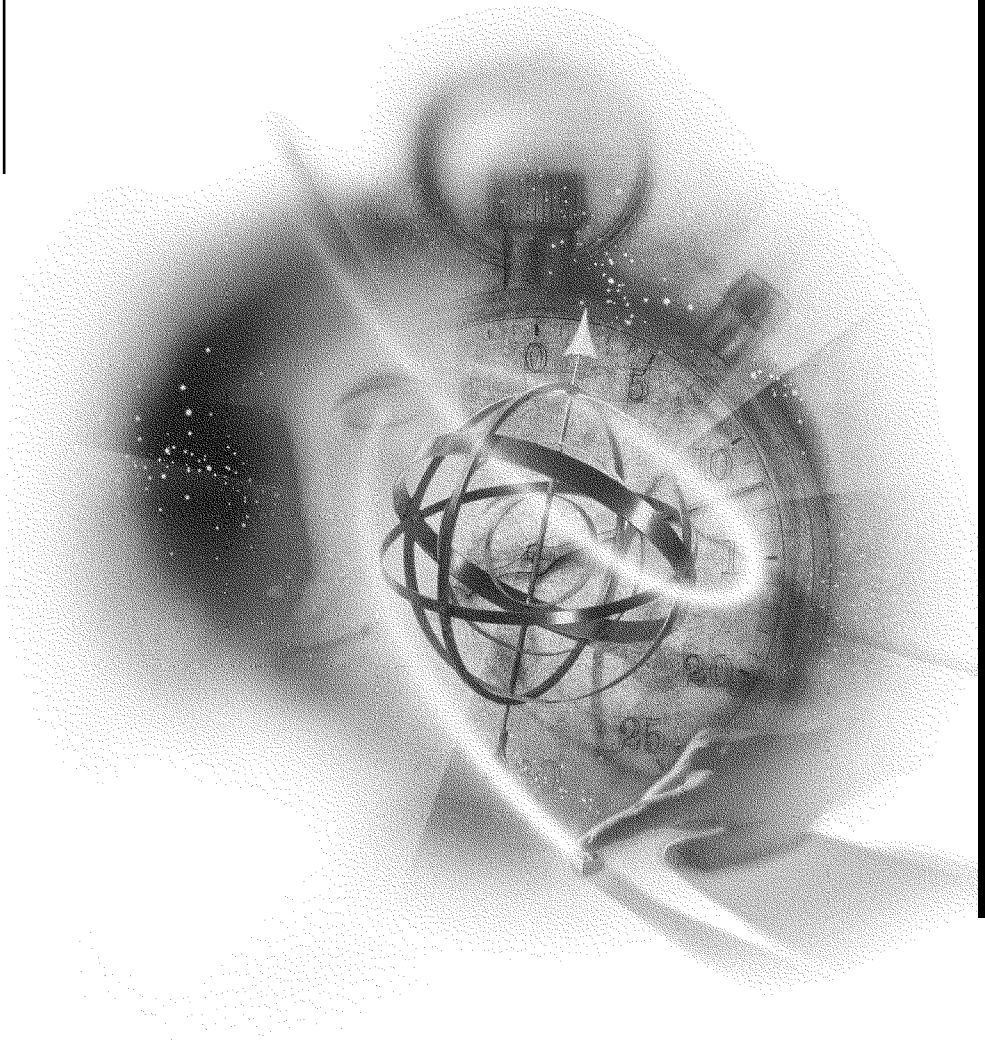
Connectivity Services

NetWare Link/PPP



Novell®

Legal Notices

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

NetWare Link/PPP
January 2000
104-001257-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

For a list of Novell trademarks, see the final appendix of this book.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

About This Guide . . . 9

1 Understanding . . . 11

How NetWare Link/PPP Works . . . 11
Communications Medium . . . 13
NetWare Link/PPP Features . . . 14
WAN Connectivity with PPP . . . 17
Permanent WAN Connections . . . 17
On-Demand WAN Connections . . . 18
Static Route and Service Databases and Routed On-Demand Calls . . . 20
Call Authentication . . . 21
Authentication Protocols . . . 22
Remote System Authentication . . . 23
Interface Groups . . . 24
PPP over ISDN . . . 25
External Device Management . . . 26
Factors that Affect PPP Performance . . . 27
Address and Control Field Compression . . . 27
Protocol ID Compression . . . 28
Data Compression . . . 28
Data Compression Concepts . . . 29
Maximizing Performance . . . 31
Typical Compression Performance . . . 32

2 Planning . . . 35

Permanent PPP Connection Configuration Decisions . . . 35
Leased-Line or Dial-Up Connection . . . 35
Transport . . . 36
Call Authentication . . . 37
Login Script . . . 37
On-Demand PPP Connection Configuration Decisions . . . 38
Transport . . . 38
Static Route and Service Databases . . . 38
Call Authentication . . . 39
Interface Groups . . . 40
Login Script . . . 41

3 Setting Up . . . 43

Configuring a Permanent PPP Connection . . . 43

How to Configure a Permanent PPP Data Link over a Synchronous Leased-Line Interface . 43
How to Configure a Permanent PPP Data Link over an ISDN Interface 45
How to Configure a Permanent PPP Data Link over a Dial-Up Line Interface. 48
How to Configure a WAN Call Destination for a Permanent PPP Connection. 51
Where to Go from Here 55
Configuring an On-Demand PPP Connection 56
How to Configure an On-Demand PPP Data Link over a Synchronous or Asynchronous Interface 56
How to Configure an On-Demand PPP Data Link over a Synchronous ISDN Interface. . . . 60
How to Configure a WAN Call Destination for an On-Demand PPP Connection 62
Where to Go from Here 65
Configuring Backup Calls 66
Configuring a Backup Call Association 67
Where to Go from Here 69
Configuring Data or Header Compression 70
Using Data Compression 71
Using Header Compression 72
How to Configure Data or Header Compression. 73
Maximizing Performance with the Packet Burst Protocol and Large Internet Packet Protocol . . 74
Configuring Maximum Receive Unit Parameters to Adjust the Frame Size 74
How to Configure MRU Parameters to Adjust the Frame Size 75
Configuring Call Retry and Timeout Parameters 76
Retrying Failed WAN Connections 77
Terminating Inactive On-Demand Connections 78
How to Configure WAN Call Retry and Timeout Parameters 78
Configuring Matching Inbound and Outbound Authentication 79
How to Configure Matching Inbound and Outbound Authentication 80
Configuring Additional Inbound Call Options 80
How to Configure Additional Inbound Call Options 81
Configuring the Bandwidth Allocation Control Protocol and the Multilink Protocol 82
Configuring Enterprise-Specific Traps 84
Configuring Interface Physical Options 86
How to Configure Interface Physical Options 86
Where to Go from Here 87
Customizing PPP Login Scripts 88
Customizing a PPP Login Script 88
Login Script Operation 89
Login Script Syntax 89
Using Modem Description Files 91
Customizing a Modem Description File 92
Limited Public-Switched Telephone Support 92
Modem Description Files 96
Environments 111

4 Optimizing . . . 113
Overview of WAN Optimization . . . 113
Payload Capacity . . . 114
Line Overhead . . . 114
Network Optimization Tools . . . 114
General PPP WAN Connection Optimization Techniques . . . 115
Understanding Data Compression and Header Compression . . . 115
Packet Burst and LIP Protocol . . . 120
Bandwidth/Benefit Ratios of Data Compression and Packet Burst . . . 121
Diminishing Traffic over a Slow Link . . . 122
Optimizing Permanent and On-Demand WAN Connections . . . 123
Optimizing PPP Multilink Performance . . . 123

5 Managing . . . 125
Using the PPPCON Utility . . . 125
PPP Multilink Information . . . 126
Using the CAPITRCE Utility . . . 127
Using the DTRACE Utility . . . 129
Using the PPPTRACE Utility . . . 131
Using PPPDISP . . . 134
Using the XLOG Utility . . . 134
Verifying the Router Configuration . . . 136
Viewing Authentication Configuration for a PPP WAN Link . . . 137
Viewing Data Compression Configuration for a PPP WAN Link . . . 137
Viewing Negotiated Options Configuration for a PPP WAN Link . . . 138
Monitoring Performance . . . 138
Monitoring Overall Link Performance . . . 138
Determining the PPP WAN Link Quality . . . 139
Determining PPP WAN Link Congestion . . . 140
Determining the Traffic Utilization for a PPP WAN Interface . . . 140
Determining the Traffic Utilization for a PPP Multilink Interface . . . 140
Determining the Number of Links in a Multilink Group . . . 140
Determining the Available Bandwidth for a PPP WAN Interface . . . 141
Checking the Connection between Routers . . . 142
Determining Whether a LAN or PPP WAN Link Is Active . . . 142
Determining Whether a Remote Router Is Reachable over a PPP WAN Link . . . 142
Monitoring PPP Packet Exchanges . . . 143
Monitoring Communications Equipment . . . 145
Monitoring Error Counters . . . 148
Monitoring PPP Multilink Information . . . 150
PPP Multilink Information . . . 150
Member Links Information . . . 150

6 Troubleshooting . . . 151
Troubleshooting Tools . . . 151
PPPTRACE . . . 151
CAPITRCE . . . 152
PPPCON . . . 154
Configuration Tips . . . 156
Troubleshooting Checkpoints . . . 160
Isolating NetWare Link/PPP Problems . . . 161
Verify the Proper Setup of Connecting Hardware . . . 161
Verify that the Modem is Set Up Properly for Initialization . . . 164
Verify Your Interface Speed . . . 166
Verify that the Modem Initialized Properly . . . 167
Create or Change a Modem Script . . . 168
Common Problems . . . 169
WAN link does not come up or immediately disconnects . . . 171
The trace is blank . . . 171
The link is established but then is disconnected . . . 172
On-demand link is not dropped . . . 172
On-demand link from an IP or IPX workstation is not working . . . 173
Connection can be made only through CALLMGR.NLM . . . 173
Synchronous connections do not connect . . . 173
Asynchronous connections do not connect . . . 174
Authentication error messages are received . . . 178
Remote system ID already exists . . . 179
LCP failure has occurred . . . 179
Incoming call is rejected . . . 179
Link goes up and down often . . . 179
PPPTRACE does not show packets . . . 180
Connection to a third-party PPP is dropped . . . 180
ISDN layer does not come up or ISDN layer goes down . . . 180
ISDN interface fails to connect . . . 181
Driver does not load . . . 182
CRC errors are excessive . . . 183
DTR dialing does not work . . . 184
DSR and DCD serial signals are incorrect . . . 184
IPCP has failed . . . 185
LAPB or data compression problems occur . . . 185
Cables are incorrect . . . 186
Remote system ID is duplicated . . . 186
Workstation connection problems occur . . . 186
Permanent WAN connection attempts to reestablish the link . . . 187
Connections are established but certain types of data are not being forwarded . . . 187
Data is sent but not received . . . 187

A Novell Trademarks . . . 189

About This Guide

This guide provides the information you need to configure and manage the Novell Internet Access Server 4.1 NetWare Link/PPP routing software. In addition to planning information, this guide provides troubleshooting tips, techniques, and tools, as well as the symptoms of and solutions to commonly occurring problems for the NetWare Link/PPP components of Novell Internet Access Server 4.1.

1 Understanding

The NetWare® Link/PPP™ software subsystem is based on the Point-to-Point Protocol (PPP), a protocol standardized by the Internet Engineering Task Force (IETF). When configured with a synchronous or asynchronous serial interface on a NetWare standalone router or file server, NetWare Link/PPP enables point-to-point transmissions of routed data across transmission facilities between interconnected LANs.

NetWare Link/PPP corresponds to the Data-Link layer of the Open Systems Interconnection (OSI) model, with additional services provided on behalf of the Network layer. It defines the automatic establishment and configuration of serial links, or connections, within router- and bridge-based network topologies.

Data transfer rates of up to 2.048 Mbps are possible, depending on the serial interface used. The only requirements are a full-duplex WAN link and modem status signals. You can use any physical interface, including RS-232, RS-422, RS-423, V.35, or X.21. Additionally, you can use copper, fiber-optic, microwave, Integrated Services Digital Network (ISDN), or satellite leased lines.

NetWare Link/PPP contains mechanisms for link configuration negotiation, call authentication, link error detection and correction, protocol multiplexing, and link header compression and data compression.

How NetWare Link/PPP Works

NetWare Link/PPP corresponds to the Data-Link layer of the Open Systems Interconnection (OSI) model, with additional services provided on behalf of the Network layer. It defines the automatic establishment and configuration of

serial links, or connections, within router- and bridge-based network topologies.

NetWare Link/PPP comprises three main components:

- A method for encapsulating datagrams over serial links
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection
- A group of Network Control Protocols (NCPs) for establishing and configuring logical connections on behalf of various Network-layer protocols

NetWare Link/PPP defines encapsulation methods supporting bit-synchronous and character-asynchronous serial communication links. NetWare Link/PPP supports the use of both types of links and operates across many standard models of modems and data terminal equipment/data circuit-terminating equipment (DTE/DCE) interfaces (for example, EIA RS-232, EIA RS-422, EIA RS-423, X.21, and International Telecommunication Union [ITU] V.35). The links must be full-duplex and can be either dedicated or switched.

NetWare Link/PPP uses a variant of HDLC that provides basic data-link delivery services over point-to-point serial connections. Typically, PPP uses HDLC unnumbered information frames providing low overhead and high throughput exchange of control and data packets. In this case, error detection is based on the CRC-16 frame check sequence (FCS). Data delivery is considered *best effort* , with error recovery left to higher-level Network- and Transport-layer protocols.

When NetWare Link/PPP data compression is enabled, HDLC sequenced information frames provide reliable delivery of control and data packets. In this case, both error detection and retransmission error recovery is provided by the data link.

A mechanism allows control data to be transmitted transparently, and removes spurious control data that can be injected into the link by intervening hardware and software. Recovery is left to higher-layer protocols.

PPP is a point-to-point service, but is capable of supporting multiple Network-layer protocols simultaneously over the same link. Because PPP provides for multiplexing of multiple Network-layer protocols (such as the Internetwork Packet Exchange™ [IPX™] protocol, IP, AppleTalk, and source route bridging) simultaneously over one link, NetWare Link/PPP provides a means

of easy connection at the Data-Link layer for a variety of hosts, bridges, and routers.

For more information about how NetWare Link/PPP works, refer to:

- Communications Medium
- NetWare Link/PPP Features

Communications Medium

NetWare Link/PPP can use any synchronous full-duplex point-to-point leased lines at speeds up to 2.048 Mbps. It also supports the use of switched-circuit lines (such as switched/56 service) and asynchronous communications over Public Switched Telephone Network (PSTN) lines, as well as synchronous communication over ISDN lines. Switched services and PSTNs provide additional flexibility by allowing on-demand and permanent connections. On-demand connections are established by the router when data must be passed to a remote system, and are terminated when idle. On-demand connection management minimizes the costs associated with serial line connectivity.

Character asynchronous and bit synchronous HDLC framing is supported by PSTNs. Device management allowing connection (circuit) establishment and termination over the PSTN is also supported using various modem command sets. Because PSTN access is unrestricted, authentication of the calling party during inbound connection attempts is provided. Because bandwidth available over most PSTNs is less than that of dedicated circuits, both PPP header compression and payload data compression is provided; however, only one compression method can be used per circuit, not both.

Within the United States, Australia, and Japan, T1 is a digital two-way telecommunications medium that operates at a clock rate of 1.544 Mbps. In Europe, E1 is the telecommunications medium and operates at a clock rate of 2.048 Mbps. The T1 data rate of 1.544 Mbps is digital signal level one, otherwise known as DS-1. The term *T1* actually refers to the hardware (usually a system of copper wire cables and amplifiers or generators) used to transport data at the DS-1 rate; however, in common use, T1 has come to mean a transmission line or connection running at 1.544 Mbps.

Traditionally, telephone companies have used these high-speed backbone trunk lines to carry long distance and local voice traffic between their central offices. In addition to voice, T1/E1 is used to transmit facsimile, graphics, and other digital data. In recent years, T1/E1 lines have been used increasingly to implement WAN connectivity.

To access T1/E1 links, the router PC or file server that is running NetWare Link/PPP must be connected to a digital service unit/channel service unit (DSU/CSU) that encodes data for transmission over the WAN link. A DSU converts a serial bit stream into a DS-1 signal; a CSU provides an interface between T1 signaling and the local loop, provided by the local telephone company (telco). The WAN board that you install in the router or file server connects to the DSU/CSU multiplexer or modem.

NetWare Link/PPP Features

PPP is recognized throughout the routing industry as a standardized serial line data-link protocol providing an efficient multivendor interoperable means of establishing WAN connections in internetwork topologies. NetWare Link/PPP includes the following advantages:

- Routing of multiple protocols simultaneously across a single WAN link. Sites can use the routing software (at both ends of each link) and gain the ability to simultaneously route IPX, IP, and AppleTalk protocols, and to route protocols routable through source route bridge, as well as nonroutable protocols.
- Removing single-vendor routing system requirements. Internetwork communities wanting to extend connectivity to new sites can configure a NetWare file server or router/bridge PC with the NetWare Link/PPP software and route IPX, TCP/IP, and AppleTalk packets across a WAN link to a non-NetWare router that also employs PPP as its data-link protocol. (The IPX over NetWare Link/PPP uses the IPXWAN™ II protocol specification, which has been published as RFC 1634 to allow other vendors to conform to the Novell NetWare Link/PPP-IPX implementation.)
- Providing a basis for supporting WAN routing of additional network protocols implemented in the future because of the extensible nature of PPP. Such enhancements, as well as enhancements to the PPP data link itself, are achieved through software upgrades; no hardware upgrade is required.
- Providing an easier and more consistent method of configuring NetWare Link/PPP, along with other Novell Internet Access Server 4.1 modules, using NIASCFG. The boards used by NetWare Link/PPP, the protocols it multiplexes across WAN links, and the parameters of the various Network-layer calls made across the WAN links are all configured

through NIASCFG. You do not need to enter commands at the server console prompt manually.

- Support of source route bridging of token ring packets over PPP.

All compliant PPP implementations are not alike. Because of the wide range of point-to-point connectivity requirements, the PPP specification, by design, specifies more capabilities and services than any single implementation might provide. However, differences in PPP implementation capabilities are reconciled at link establishment time when the two PPP peer nodes negotiate a common set of supported services.

Novell has chosen the following options:

- Any given implementation of PPP can include either asynchronous or synchronous framing, or both. NetWare Link/PPP supports both framing types. Bit synchronous framing is required for high-speed leased lines and switched circuits, whereas asynchronous framing supports the use of low-speed modems with PSTNs.
- Any given implementation can support one or more Network-layer protocols. There is no specific prescribed set of protocols that must be supported. Currently, Novell supports AppleTalk, TCP/IP, IPX, and source route bridging.
- PPP does not require modem control signals (such as RTS, CTS, DCD, and DTR), even though such signals do allow greater functionality. However, NetWare Link/PPP uses these modem control signals to provide switched-circuit device management.
- Scripted logins are provided for users who use asynchronous PPP connections to log in to online services. With minimum modification, these standard scripts enable many common logins. It is also possible to develop customized login scripts tailored to meet the needs of a specific site.
- Backup call associations ensure that new connections are made successfully and that permanent connections are maintained, even if a primary WAN call destination goes down. When a backup call association is configured, two previously configured WAN call destinations are specified to have an association with one another. One destination is defined as the primary call destination; the other, as its backup. In the event that the primary destination becomes unavailable, NetWare Link/PPP switches automatically to the backup destination.

- The NetWare Link/PPP Link Control Protocol (LCP) implementation includes the following options:
  - Maximum Receive Unit (MRU)—Allows the sender to inform the peer that it can receive larger frames than the default, or to request that the peer send smaller frames. Even if smaller frames are sent, the ability to receive 1,500-octet LCP frames is required in case link synchronization is lost.

    NetWare Link/PPP supports MRU values with the range of 128 to 4,500 bytes.
  - Magic Number —Provides a way to detect failure of a remote peer node, as well as loopback links and other Data-Link layer anomalies.
  - LCP Echo Request —Provides a positive method of verifying the presence of a remote PPP peer or detecting a loopback line. Echo requests, generated on a periodic basis, serve to elicit *keep-alive* echo responses from the remote peer.
  - PAP and CHAP Call Authentication —Limits dial-in access to authorized remote systems only. PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) are authentication protocols that protect against unauthorized access. This option is an integral part of the NetWare Link/PPP on-demand routing implementation, providing identification of each remote system.
  - Asynchronous Control Character Map (ACCM) —Allows user-configured hardware control character mapping on behalf of a variety of manufacturers' modems.
  - Address and Control Field Compression —Provides a 2-byte per packet performance optimization by eliminating the fixed HDLC address and control fields from each PPP header.
  - Protocol Field Compression —Provides a 1-byte per packet performance optimization by eliminating one of the two PPP protocol ID bytes.
- Data Compression —Provides a major performance optimization by encoding Network-layer payload data into more compact character sequences based on recurring patterns.
- Compression Control Protocol (CCP) —Supports CCP for the negotiation and selection of a common data compression protocol between systems.

In addition, Novell Internet Access Server 4.1 maintains backward compatibility with NetWare MultiProtocol Router™ 3.1 software, NetWare MultiProtocol Router 3.0, and NetWare MultiProtocol Router 2.11 PPP data compression.

- Bandwidth Allocation Control Protocol and Multilink Protocol — Greatly increase your total available bandwidth. Bandwidth Allocation Control Protocol and Multilink Protocol enable you to use multiple physical ports on one or more WAN boards to represent a single logical link to one location. When the bandwidth threshold of one port is reached, the bandwidth of the next port becomes available. More ports are added to the connection if bandwidth requirements continue to increase beyond the threshold of the ports currently in use.

WAN Connectivity with PPP

NetWare Link/PPP takes advantage of switched-circuit networks to provide a cost-effective alternative to dedicated data networks that permanently connect remote LANs. To understand the advantages provided by on-demand links created by NetWare Link/PPP, you must understand WAN connectivity with PPP.

The following sections discuss NetWare Link/PPP connectivity concepts that impact Novell Internet Access Server 4.1 network protocol configuration:

- Permanent WAN Connections
- On-Demand WAN Connections
- Static Route and Service Databases and Routed On-Demand Calls
- Call Authentication
- Remote System Authentication
- Interface Groups
- PPP over ISDN
- External Device Management

Permanent WAN Connections

Permanent WAN connections connect geographically separated LANs. The WAN connection typically uses leased lines for the physical connection between the separated LANs, and typically uses a router to establish and

maintain the connection across the line, as long as the router is operational. There is no cost savings for disconnecting the link because the service provider of a leased line charges a fixed cost.

Network protocols use a permanent WAN connection in a manner similar to the way they use a LAN connection. The protocols exchange both user data and maintenance data, including dynamic route and service updates, across the connection. The bandwidth of a leased line usually ranges from about 56 Kbps to 2.048 Mbps, which is much less than that of a LAN. However, this bandwidth is usually sufficient because not all the traffic that occurs on a LAN needs to be routed across a WAN.

For example, when a user at a branch office needs to access a file on the local branch office server, the data traffic generated by the user accessing the file is not routed across the WAN. Data is routed across the WAN only when requests are made for services accessible through the WAN connection.

Dedicated network connections have the following disadvantages:

- **Cost** —Permanent WAN connectivity is expensive because of the monthly service charge required by the service provider for the permanent circuits. Charges for permanent services are based on the bandwidth provided, not on how much of the bandwidth is actually used.
- **Setup time** —Permanent network connections are set up by the service provider between fixed points. There is a time factor involved in setting up a permanent circuit and, once the circuit is established, a similar time factor is required to change the end points of the circuit.

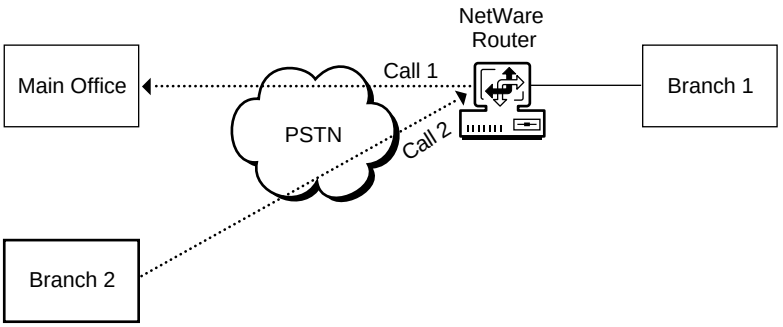
On-Demand WAN Connections

NetWare Link/PPP on-demand WAN connections are established at the request of network protocols, based on the presence of user data that must be routed to a destination across the connection. If no data is flowing across an on-demand WAN connection for a preset configurable period of time, then the connection is terminated.

On-demand WAN connections are similar to the way a telephone is used. An outbound call to a remote party is placed by dialing the phone number, and a connection is made when the remote party picks up the phone. A conversation takes place and terminates when one of the parties hangs up the receiver. When a telephone is not in use, it is available to place other outbound calls or accept inbound calls from remote parties. The costs for using the telephone are based on the duration and distance of each call.

Figure 1 illustrates on-demand WAN connections between offices. When Branch 1 has data to send to the Main Office, it uses on-demand call 1, named Call_Main_Office. After the router transfers the data and the link reaches the idle link timeout, the call is disconnected. When Branch 2 has data to send to Branch 1, it uses on-demand call 2, named Call_Branch_1.

Figure 1 On-Demand Connections



The analogy between NetWare Link/PPP on-demand connections and telephone calls is not superficial. Voice-grade telephone lines can be used to establish low-bandwidth (typically 2,400 bps to 28,800 bps) on-demand connections. ISDN lines can be used to establish medium-bandwidth (56/64 Kbps to 112/128 Kbps) on-demand connections. Depending on bandwidth requirements, on-demand connections placed over PSTNs (Public Switched Telephone Networks) can be a simple and quick way to establish temporary connectivity between remote LANs.

If low-bandwidth connections do not suffice, you can consider a switched data service, such as switched/56 or switched/256. Switched services can offer significant cost savings over dedicated circuits with the same bandwidth.

Synchronous interfaces operating over ISDN lines are excellent for on-demand connections because they provide 5 to 10 times the bandwidth of analog connections at significantly lower error rates.

On-demand connections have the following advantages:

- **Cost** —On-demand connections terminate when there is no data to route across the connection. This means that you pay only for the time the connection is in use, not for idle time, as in the case of a permanent WAN connection.

- **Flexibility** —You might initially use a single interface to establish an on-demand call to a remote LAN. After the connection terminates, you can use the same interface to establish another on-demand connection to a different remote LAN. Unlike permanent WAN connections, no service provider involvement is necessary to connect to a different destination.

Static Route and Service Databases and Routed On-Demand Calls

As described earlier, NetWare Link/PPP on-demand connections are initiated at the request of network protocols when data is present that must be routed to a remote LAN, and they are terminated when the NetWare Link/PPP WAN connection is determined to be idle. Standard network protocols generally expect each WAN circuit to provide permanent connections to all remote systems. The reason is that the network protocols rely on periodic communication with remote systems to dynamically exchange routing updates and, in the case of IPX, service advertising updates. These periodic exchanges identify the network routes and services that are known on each remote LAN accessed over the WAN connections.

Depending on the size of each remote LAN and the speed of the WAN connection, periodic maintenance exchanges can result in a constant stream of data across the NetWare Link/PPP connection, which prevents on-demand connections from terminating using idle-link detection. However, without the maintenance exchanges, Network-layer protocols do not have the information required to route data to the proper remote systems, and on-demand connections are never established because the local network protocols are not aware of the accessible WAN routes and services.

To provide the required route and service information without tying up the on-demand connection, the Novell Internet Access Server 4.1 routing software offers two alternatives:

- **Static route and service databases** —Each database is network protocol-specific and contains a manually configured subset of the route and service information. Manual configuration eliminates the need for periodic maintenance updates because the required route and service information is already available in the static databases of each system. When the Novell Internet Access Server 4.1 routing software receives a request for a manually configured static route or service, it supplies the routes and services information to other network nodes and makes a WAN call to the configured node.

A single static route is also useful as a default route for IPX or TCP/IP hosts. In this way, the only routing information crossing the link is that required by users to access a specific set of services.

Static routes and services are configured using NIASCFG. In the case of IPX, the Static Routing Configuration utility (STATICON) provides a simplified method to configure static routes and services. STATICON accesses information from the router across the WAN link if the router supports the IPX Management Information Base (MIB) provided with the Novell Internet Access Server 4.1 routing software and Simple Network Management Protocol (SNMP) over IPX. Documentation for the IPX MIB is provided in the IPXMIB.TXT file on the product CD-ROM.

- **Routed on-demand calls (with IPX and IP protocols)** —A routed on-demand call runs the IPX or IP routing protocol over the link. The timeout for a routed on-demand call is based on the receipt of Network-layer data packets. In this way, the Novell Internet Access Server 4.1 routing software is able to get the benefit of running routing protocols over the on-demand link without the IPX or IP packet traffic keeping the link continuously active.

  Routed on-demand calls are well-suited for large corporate networks that have many branch offices. For more information on routed on-demand calls, refer to Understanding in the *IPX* documentation and Understanding in the *TCP/IP* documentation.

Call Authentication

Using public-switched data or telephone networks provides a high level of communication flexibility that is not possible with dedicated circuit data networks. You can quickly reconfigure WAN connections to support changes in network topology requirements without incurring the delays often experienced when working with external service providers.

However, along with this flexibility there is the potential for unauthorized access. Dedicated circuits implicitly ensure the identity of the connection peers because of the fixed circuit between local and remote systems. However, switched circuits introduce the possibility of call attempts by unauthorized remote systems. Anyone with a modem, phone number, and knowledge of the PPP data-link protocol can potentially establish a rogue connection to a router, and thereby gain access to the attached networks.

To provide protection against unauthorized router access over public-switched data or telephone networks, PPP uses the optional authentication protocols described in the next section.

Authentication Protocols

The PPP protocol specification defines two authentication protocols to protect against unauthorized access: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). During the link establishment phase, a PPP node can request that its data-link peer provide authentication information using one of these authentication protocols. If the remote peer does not agree to provide the requested authentication information, the PPP link is not established. If the peer does agree, the link establishment phase is completed and the authentication phase is entered.

Using the previously negotiated authentication protocol, information is exchanged between the two peers, allowing the local system to authenticate the remote peer. Successful authentication allows the peers to proceed to the NCP negotiation phase. Authentication failure results in termination of the link and the physical circuit.

PAP was the initial mechanism specified by PPP for peer identification. It defines exchange of peer ID/password pairs that are validated by the node requesting authentication of the remote peer. Upon receipt by the requesting node, the ID/password pair is compared against a local list of authorized ID/password pairs. A match results in successful authentication and allows the node to proceed with NCP negotiation. A nonmatch results in termination of the link and the physical circuit.

CHAP was developed to overcome a deficiency in PAP: that is, the password is sent over the link in clear text. CHAP addresses this problem by maintaining a common secret at both peer systems. One system issues a challenge sequence that must be modified using the secret and returned to the challenging peer. The challenging system must validate the response sequence by applying its secret to the original challenge and comparing the result to the response sequence. Authentication successes and failures are processed similar to PAP.

Inbound Authentication

With NetWare Link/PPP, you can configure either PAP or CHAP as the inbound call authentication protocol type for each interface. The system maintains one or more user-configured authentication databases. The database contains entries for each authorized peer represented as ID/password pairs for

PAP and ID/secret pairs for CHAP. In both cases, the ID portion, which is exchanged by the over-the-wire protocol, specifies the remote system ID. The remote system ID is used as a database key to access the associated password or secret.

By default, one inbound authentication database is maintained for all NetWare Link/PPP ports; however, you have the ability to specify alternative authentication databases on a per-port basis. This permits any number of ports to share a single database.

The NetWare Link/PPP port configuration allows the configuration of the authentication protocol type (None , PAP , CHAP , Either PAP or CHAP), the name of the authentication database (the default is PPP-AUTH), and the contents of the specified database.

Outbound Authentication

With NetWare Link/PPP, you can also configure PAP or CHAP as the outbound call authentication protocol type for each interface. Support for PAP and CHAP is provided by the Call Support Layer (CSL) WAN call destination entries, which allow specification of authentication information for outbound calls. This information includes the authentication type (None , PAP , CHAP , Either PAP or CHAP) and password or encrypted password, as appropriate.

For on-demand connections, you must configure outbound calls to specify an authentication protocol type, an ID, and a password. To accept inbound on-demand connections, you must configure the PPP interface to validate the authentication information supplied by the calling system. Using PAP or CHAP authentication is recommended for all permanent switched-circuit connections and is required for on-demand connections.

Remote System Authentication

Using PAP or CHAP authentication also provides a method of remote system authentication. When the local system accepts an inbound on-demand connection, the remote system must be identifiable so the local system can reestablish the connection if it is terminated before the data transfer is complete. This is similar to asking telephone callers for their phone numbers, in case you need to call them back.

On-demand connections work reliably only if the called system can establish a return connection. This requires proper configuration of static routes and services, WAN call destinations, and network interface authentication at both

ends of the connection. Therefore, if a called Novell Internet Access Server 4.1 system does not have the required configuration information necessary to reestablish a connection to the calling system, it does not accept the initial connection attempt.

For example, your router initiates an on-demand connection to a remote server on behalf of a local client workstation. After the connection is established, the client initiates a database search on the remote server. Before the database search is completed, the on-demand connection is terminated because an idle data-link timeout occurs. Later, when the response to the database search is eventually available, the remote server no longer has a connection to your router. The client operation fails unless the static routing database at the remote server contains the information needed to reestablish the connection. The remote server uses the router's system ID and static route information to reestablish the connection.

Because the ID strings used by PAP and CHAP authentication provide a peer system identification mechanism that solves this problem, PAP or CHAP authentication is required for on-demand connections. The local and remote system ID strings associated with PAP and CHAP authentication typically represent the NetWare server names of the local and remote NetWare Link/PPP connection peers.

Interface Groups

Each permanent outbound call configuration identifies a specific NetWare Link/PPP interface that is used to place the call to a remote system. However, when supporting on-demand connections, you might want to have a group of interfaces that can be shared between outbound connections. If each interface in the group provides the same capabilities, any available interface can be used to establish an on-demand outbound connection to a remote system. Furthermore, if all the interfaces are attached to switched circuits that represent the same telephone number, inbound calls placed to that telephone number can be accepted over any available interface in the interface group. This is similar to a multiple-line business telephone. To place an outbound call, you select any available line. Multiple inbound calls placed to the main office number are directed to any available line.

NetWare Link/PPP lets you assign a symbolic name to a group of interfaces that can be used interchangeably. All interfaces in a group must have similar framing characteristics. NetWare Link/PPP outbound call configuration lets you select an interface group name rather than a specific interface name for

making outbound calls. Selecting an interface group name directs NetWare Link/PPP to use any available interface within the group to establish the connection.

Defining an interface group (with the Interface Group parameter) lets you make an on-demand call on any of several network interfaces without creating an individual WAN call destination for each interface. All you need to do is specify the interface group name in place of the interface name in the WAN call destination. When the call is made, the specific interface is selected from the group. Because an interface is selected automatically when the call is made, you do not need to dedicate interfaces to specific destinations. This flexibility in selecting interfaces lets you use your WAN hardware more efficiently.

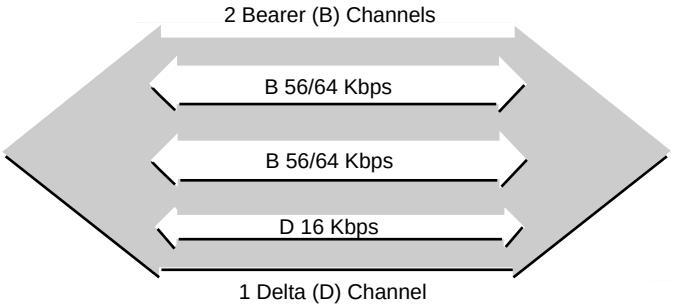
PPP over ISDN

NetWare Link/PPP supports connections over ISDN lines. ISDN is a digital network technology being deployed by international and domestic service providers to replace outdated analog technology. ISDN service is already widely available in Europe and the Pacific Rim, and is becoming widely available in the United States.

Collectively, ISDN is a set of digital transmission protocols defined by the ITU. ISDN provides both voice and data services over two types of lines: a Basic Rate Interface (BRI) and a Primary Rate Interface (PRI). Each type of line consists of a number of 64-Kbps bearer channels (or B channels) and one 16-Kbps or 64-Kbps delta channel (or D channel). B channels are clear-channel connections that can be used for voice and data communication. The D channel is used for signaling and X.25 packet networking.

A BRI line contains two 64-Kbps B channels and one 16-Kbps D channel. In some telco networks, inbound signaling is done by a technique known as bit robbing, and the B channel rate adapts down to 56 Kbps for interoffice traffic. Figure 2 illustrates a BRI line.

Figure 2 ISDN BRI Line



A PRI line in North America and Japan contains 23 64-Kbps B channels and one 64-Kbps D channel. It has a total bandwidth of 1.544 Mbps and is designed for transmission through a standard North American T-1 trunk. (In other locations, the PRI line contains either thirty or thirty-one 64-Kbps B channels and one 64-Kbps D channel.)

PPP over ISDN offers inexpensive and reliable WAN connectivity. Dial-up ISDN connectivity is significantly less expensive than leased synchronous lines. In addition, communication over ISDN lines is faster and more accurate than that attainable over analog telephone lines using modems for digital-analog conversion.

External Device Management

A variety of choices of modems or other externally attached devices can be used to provide physical connectivity between link peers. Control of these devices is typically achieved by using the interface port to exchange character-based command/response sequences between the external device and the local node. These command/response exchanges allow configuration of the device, as well as control of operations such as dialing, answering, and terminating PSTN circuits.

The Customer Premises Equipment Configuration utility (CPECFG) provides a terminal interface to a serial port on the router or server to the DSU/CSU or modem. for each ROUTE.NLM parameter using, refer to “Setting Up” in the routing documentation for Source Route Bridge. For more information about CPECFG, refer to “Setting Up” in the routing documentation for NetWare Link/PPP.

Command set support differs based on device type; therefore, identification of the attached external device is necessary to the local device management logic that is responsible for physical connection control. For best results, you might want to use the same brand of modem on the local and remote ends.

The WAN device management provided is script-driven and supports multiple modem types. Modem description (MDC) files define modems used by the router. The MDC files reside in the SYS:SYSTEM directory on the router or server.

Factors that Affect PPP Performance

To maximize the bandwidth available from the Public Switched Telephone Network (PSTN) connections, NetWare Link/PPP supports a number of PPP compression options intended to eliminate nonessential information from the data-link frame format:

- Header compression
  - Address and control compression
  - Protocol ID (PID) compression
- Data compression

These options can be negotiated at connection establishment between peers supporting similar functionality. However, data compression cannot be used simultaneously with either address and control compression or protocol ID compression.

For more information about factors that affect PPP performance, refer to:

- Address and Control Field Compression
- Protocol ID Compression
- Data Compression

Address and Control Field Compression

NetWare Link/PPP is intended as an unreliable, point-to-point data link, as opposed to a sequenced multipoint data link. Therefore, it uses constant values for the HDLC Address (All Stations Address) and Control (Unnumbered Information) fields. This is consistent with HDLC framing, but it does add a level of unneeded overhead when low-bandwidth data links are used.

To overcome this inefficiency, NetWare Link/PPP provides the option of generating or eliminating (through compression) the HDLC address and control fields for each data link. When successfully negotiated between peers, these constant HDLC header fields can be eliminated from subsequent data-link exchanges. Configuration of this option is provided on a per-port basis.

The address and control compression field (PPP Header Compression field in NIASCFG) displays the option's configured state (Enabled or Disabled); the default is Disabled. Note that enabling this option results in a negotiation attempt with the remote peer. It does not guarantee that compression is actually used; that is determined by the peer-to-peer negotiation process at link establishment time. However, you can validate whether compression is used by examining the PPP negotiated parameters in the PPP console (PPPCON.NLM).

Protocol ID Compression

To further reduce the PPP header overhead, there is an option to compress the Protocol ID field. Protocol ID values can be compressed into a single-byte form clearly distinguishable from the standard 2-byte form. In cases where the leading byte of the protocol ID is zero (network data traffic), the MSB (most significant bit) value can be omitted. Configuration of the protocol ID compression is provided on a per-port basis. Enabling compression does not guarantee that protocol ID compression is actually used; that is determined by the peer negotiation process at link establishment time. However, you can validate whether compression is used by examining the PPP negotiated parameters in PPPCON.

When address, control, and protocol ID compressions are enabled and successfully negotiated between peer data-link nodes, the result is to reduce the PPP header overhead associated with network data traffic from 9 to 5 bytes. In low-bandwidth links passing interactive traffic, this can be a savings.

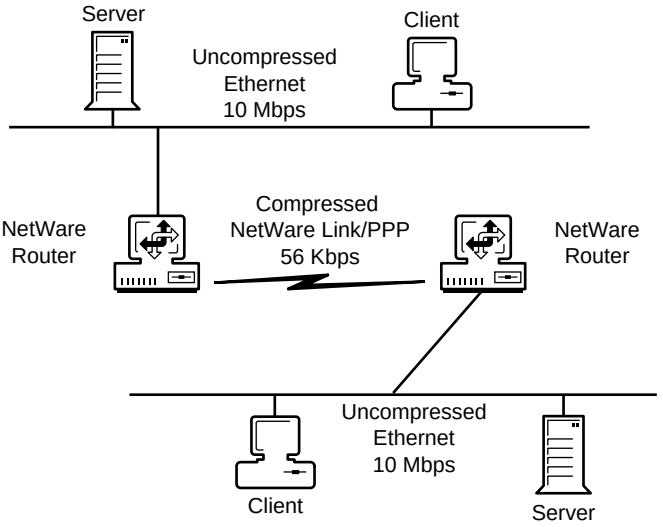
Data Compression

Data compression reduces the amount of information transferred over a communications link by replacing previously observed data sequences with more compact sequences. This increases the apparent speed of the link, at the cost of some additional router CPU load. Enabling data compression allows negotiation by CCP of compression with the remote peer. Data compression

is used if both the local and remote peers support a common compression technique.

This support for data compression allows more effective PPP link utilization when packets are routed between remote LANs. Figure 3 illustrates a simple network configuration showing NetWare Link/PPP operating over a 56-Kbps leased line to connect two Ethernet LANs operating at 10 Mbps. Note that data compression is necessary only over the PPP link connecting two LANs because this is the slowest portion of the end-to-end network traffic.

Figure 3 Two LANs over a 56-Kbps Leased Line



For more information about data compression, refer to:

- Data Compression Concepts
- Maximizing Performance
- Typical Compression Performance

Data Compression Concepts

Proper operation of most data compression algorithms requires that no data corruption be permitted on the communications link because each bit of the

compressed data is much more significant than the uncompressed data. One incorrect bit can result in thousands of bytes of incorrect output.

NetWare Link/PPP is, by default, an unreliable or *best effort* data link that does not guarantee data delivery. Retransmission of lost or corrupted data is the responsibility of higher-level protocols. Therefore, to ensure data integrity of the compressed data exchange, the unreliable PPP data link is replaced with a reliable data-link protocol when data compression is negotiated successfully by CCP. This reliable data-link protocol is ITU *Link Access Protocol-Balanced (LAPB)*. LAPB significantly increases the reliability of the communications link when used in conjunction with error checking after the received data is uncompressed.

Data compression is performed on network data only. NetWare Link/PPP LCP and NCP data is passed uncompressed. LCP and NCP data exchanges are used for connection management and configuration negotiation. They are typically used only during the connection establishment and termination operations. These protocol exchanges have their own error recovery mechanisms and, as such, do not benefit from the LAPB reliable data-link services.

NetWare Link/PPP supports the Pattern Predictor and Stac LZS compression algorithms. The Pattern Predictor compression technique provides useful data compression over a wide range of line speeds, from 1,200 baud through E1 data rates. Future versions of NetWare Link/PPP might include additional compression algorithms tailored to provide higher compression at specific line speeds.

As currently implemented, the data compression capability permits a best case 8:1 compression ratio with highly compressible data. A realistic figure for a typical mix of graphic, text, and binary data is on the order of a 2:1 compression ratio. This increases the apparent throughput of a 56-Kbps link, for example, to almost 112 Kbps. Furthermore, the Predictor Type 2 algorithm surpasses the Predictor Type 1 algorithm by filling the PPP packets to the maximum transmission unit (MTU) size with the compressed payload data. This payload data can be from different types of Transport-layer packets, such as IP, IPX, or AppleTalk packets.

Generally, as the communications link speed increases, the ability of data compression to enhance throughput performance decreases. The reason is that on a higher-speed line, the output buffers are emptied faster and compression cannot keep up, whereas on a lower-speed line, the output buffers are emptied more slowly and the compression algorithm can keep the buffers full. Therefore, although data compression provides some benefit at speeds up to E1 (2.048 Mbps), the performance improvement is not as great as that on a

lower-speed 56-Kbps link. Refer to "On-Demand WAN Connections" on page 18 and "PPP over ISDN" on page 25 for a comparison of typical compression improvements at 56 Kbps and 1.536 Mbps.

Actual results, of course, vary depending on a number of factors, including the type of data being transferred, the type of PC systems NetWare Link/PPP runs on, and the speed of the communications link.

Maximizing Performance

NetWare Link/PPP data compression works best when a constant supply of transmit data is available at the interface. This allows the compression logic to maximize the replacement of data sequences with the more compact sequences. Therefore, when using IPX with NetWare Link/PPP data compression, the IPX Packet Burst™ protocol and the Large Internet Packet (LIP) protocol should also be used. The Packet Burst protocol enhances IPX by allowing larger data transactions, composed of multiple IPX packets, to be transmitted as a single burst (or logical operation). Acknowledgments are issued for the complete burst rather than for individual IPX packets. For best results, the Packet Burst protocol and the LIP protocol must be enabled on each client and server end node system. Although the LIP protocol is included in the Packet Burst software for NetWare servers, it must be enabled separately on the clients.

WARNING: The IPX client workstation Packet Burst protocol support provided by BNETX.COM is out of date and must not be used.

Packet Burst protocol support for NetWare 3.1*x* or NetWare 4 clients is provided by the Novell Client™ files on the Novell Client CD-ROM. Alternately, for NetWare 3.11 clients, you can use the NetWare Client for DOS and Windows (VLM™) files on the Novell Client CD-ROM. Packet Burst protocol support is provided for NetWare 3.11 servers by the PBURST.NLM included in the PBURST.EXE file. Search for the PBURT.EXE file at the following locations:

- WWW location http://support.novell.com
- WWW location http://ftp.novell.com
- CompuServe* (Enter GO NOVELL.)
- Novell Support Connection Library CD-ROM (Call 1-800-377-4136 to order in the U.S. and Canada. In all other locations, call 888-321-4272.)

Typical Compression Performance

Actual compression ratio and effective throughput varies, depending on the amount and type of data being sent. For example, encrypted data does not compress at all (and might even increase the amount of data sent), whereas ASCII text documents might compress significantly.

Figure 4 is an example of compression statistics displayed by the Monitor utility.

Figure 4 Compression Statistics Displayed by Monitor

```
          AIOCOMX_1 [WHSMAIO slot=FF frame=PPP]

Custom statistics
  Line Speed                                        19,200
  Line Rx Byte Count Low                       130,714,401
  Line Rx Byte Count High                                0
  Line Rx Utilization (percent)                         94
  Line Tx Byte Count Low                       127,198,793
  Line Tx Byte Count High                                0
  Line Tx Utilization (percent)                         93
  Compression Algorithm (none=0)                         2
  Send Comp Throughput (bits/second)                92,340
  Recv Comp Throughput (bits/second)               101,574
  Send Comp Ratio (1000 * uncomp/comp)               6,998
  Recv Comp Ratio (1000 * uncomp/comp)               6,771
```

In the example shown in Figure 4, the send compression ratio is 6,998:1, meaning that for every 6,998 bytes of input data, 1,000 bytes of compressed data are sent over the link. The send compressed throughput figure shows the actual, real-time effective throughput of the line, expressed in bits per second. In the example, the link is capable of 19,200 bits per second, and with the compression enabled, you can see an effective throughput of 92,340 bits per second. The receive compressed throughput is 101,574 bits per second.

Data compression can significantly increase the apparent link speed of all protocols supported, including the IPX protocol. Data compression is of greater value if the link is already busy (for example, when many workstations are using a remote server).

Table 1 and Table 2 graph the performance of links, as tested with the PERFORM3, a network testing program (located on the NetWire(SM) electronic bulletin board), using AST* 486/33E servers and workstations. The test program was run using the following command:

```
PERFORM3 filename  12 128 4096 1024
```

Data is expressed as Kbps.

Table 1 Compression Performance for 56-Kbps Links

Scenario	Performance (Kbps)
One workstation, no compression	49.60
One workstation, compression	149.76
Five workstations, no compression	41.28
Five workstations, compression	176.32

Table 2 Compression Performance for T1 (1.5-Mbps) Links

Scenario	Performance (Kbps)
One workstation, no compression	891.52
One workstation, compression	1,252.08
Five workstations, no compression	1,405.36
Five workstations, compression	2,337.04

Each compression algorithm offers a slightly different advantage in either the compression ratio or the compression/decompression speed. Table 3, Table 4, and Table 5 show the benchmark values for all three algorithms. The benchmark tests used 1,024-byte blocks from a 3-MB file that consists of 20 smaller files of differing data types. Table 3 compares the compression ratios of the three algorithms. Table 4 compares the time in microseconds to compress data, and Table 5 compares the time in microseconds to decompress data. Note that the values listed in these three tables are numerator values where the denominator is one. A value of less than one indicates expansion. Expansion is caused by the compression of data that does not contain redundant sequences of characters. This condition causes the compression algorithm to produce more bytes than the original data size.

Table 3 Compression Ratio Comparisons

	Novell Predictor	Stac LZS
Minimum ratio	0.996	1.224
Maximum ratio	4.266	6.243
Average ratio	1.744	1.894
Expansion	0.996	1.000

Table 4 Compression Time Comparisons

Time in Microseconds	Novell Predictor	Stac LZS
Minimum ratio	3,332	20,306
Maximum ratio	1,662	10,455
Average time	2,632	18,620
Minimum time	1,576	10,455
Maximum time	3,332	23,574

Table 5 Decompression Time Comparisons

Time in Microseconds	Novell Predictor	Stac LZS
Minimum ratio	2,824	17,110
Maximum ratio	1,218	9,128
Average time	2,249	14,419
Minimum time	1,098	9,128
Maximum time	2,833	17,110

2 Planning

This section describes the decisions that you must make before you can configure permanent or on-demand PPP WAN connections.

Permanent PPP Connection Configuration Decisions

How you configure a permanent PPP connection depends on the following decisions:

- Whether you will use a leased-line or dial-up connection
- The transport over which your permanent connection will be made
- What form of call authentication you will use
- Whether you will need to use a login script

These configuration decision topics are covered in the following sections:

- Leased-Line or Dial-Up Connection
- Transport
- Call Authentication
- Login Script

Leased-Line or Dial-Up Connection

The following sections describe the two types of permanent PPP connections you can make.

Leased-line Connection

In a permanent connection over a synchronous leased-line interface, a leased line is used for the physical connection between the separated LANs. There is

no cost savings for disconnecting the link because the service provider of a leased line charges a fixed cost.

The bandwidth of a leased line usually ranges from about 56 Kbps to 2.048 Mbps, which is much less than that of a LAN. However, this bandwidth is usually sufficient because not all the traffic that occurs on a LAN needs to be routed across a WAN.

To configure this kind of connection, refer to "How to Configure a Permanent PPP Data Link over a Synchronous Leased-Line Interface."

Dial-Up Connection

In a permanent connection over a dial-up line interface, a modem is configured to keep the permanent connection active. If the connection goes down, the modem reestablishes the connection.

To configure this kind of connection, refer to "How to Configure a Permanent PPP Data Link over a Dial-Up Line Interface."

Transport

You should choose the transport that will best serve the needs of your NetWare® Link/PPP™ connection.

Voice-grade telephone lines can be used to establish low-bandwidth (typically 2,400 bps to 28,800 bps) permanent connections. Integrated Services Digital Network (ISDN) lines can be used to establish medium-bandwidth (56/64 Kbps to 112/128 Kbps) permanent connections. Depending on bandwidth requirements, permanent connections over Public Switched Telephone Network (PSTN) lines can be a simple and quick way to maintain connectivity between remote LANs.

If low-bandwidth connections do not suffice, you can consider a switched data service, such as switched/56 or switched/256. Switched services can offer significant cost savings over dedicated circuits with the same bandwidth.

Note that although synchronous interfaces operating over ISDN lines are a viable solution for your permanent connection needs, this kind of solution might not be as cost-efficient as other alternatives, depending on the service provider rates for permanent ISDN lines in your area.

To configure a connection over an ISDN line, refer to "How to Configure a Permanent PPP Data Link over an ISDN Interface."

Call Authentication

To provide protection against unauthorized router access, the PPP specification defines two optional protocols that authenticate inbound call attempts: the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP). These protocols ensure that the local system can accept calls from only authorized remote systems. Authentication is based on a remote system identified by a user ID and a password.

With NetWare Link/PPP, you can configure each interface to support one of the following methods for inbound call authentication:

- PAP
- CHAP
- Either PAP or CHAP, with CHAP attempted initially

The main difference between PAP and CHAP is that PAP sends the password string across the WAN in clear text, whereas CHAP is a more secure authentication protocol because it uses the password to encrypt a challenge string. Note, however, that not all PPP products currently support CHAP authentication.

For more information about NetWare Link/PPP and call authentication, refer to "Understanding."

Login Script

For users or systems dialing up and logging in to asynchronous service providers, login scripts facilitate the process by defining a command/response dialog that takes place between a router and a remote server at dial-up. According to syntactical conventions, certain login script strings are interpreted as output to be sent by the router (a command to the remote server), whereas others are interpreted as input to be listened for by the router (an expected response from the remote server).

NetWare Link/PPP provides a login script for logging in to a network. For information about customizing a login script to meet your site's needs, refer to "Customizing PPP Login Scripts."

On-Demand PPP Connection Configuration Decisions

How you configure an on-demand PPP connection depends on the decisions you make concerning the following topics:

- Transport
- Static Route and Service Databases
- Call Authentication
- Interface Groups
- Login Script

Transport

You should choose the transport that will best serve the needs of your NetWare® Link/PPP™ connection.

Voice-grade telephone lines can be used to establish low-bandwidth (typically 2,400 bps to 28,800 bps) on-demand connections. Integrated Services Digital Network (ISDN) lines can be used to establish medium-bandwidth (56/64 Kbps to 112/128 Kbps) on-demand connections. Depending on bandwidth requirements, on-demand connections placed over Public Switched Telephone Network (PSTN) lines can be a simple and quick way to establish temporary connectivity between remote LANs.

If low-bandwidth connections do not suffice, you can consider a switched data service, such as switched/56 or switched/256. Switched services can offer significant cost savings over dedicated circuits with the same bandwidth.

Synchronous interfaces operating over ISDN lines are excellent for on-demand connections because they provide 2 to 30 times the bandwidth of analog connections at significantly lower error rates.

Static Route and Service Databases

Standard network protocols generally expect each WAN circuit to provide permanent connections to all remote systems. The reason is that the network protocols rely on periodic communication with remote systems to dynamically exchange routing updates and, in the case of the Internetwork Packet Exchange™ (IPX™) protocol, service advertising updates. These periodic exchanges identify the network routes and services that are known on each remote LAN accessed over the WAN connections.

Depending on the size of each remote LAN and the speed of the WAN connection, periodic maintenance exchanges can result in a constant stream of data across the NetWare Link/PPP connection. This constant stream of data prevents on-demand connections from terminating using idle-link detection. However, without the maintenance exchanges, Network-layer protocols do not have the information required to route data to the proper remote systems, and on-demand connections are never established because the local network protocols are not aware of the accessible WAN routes and services.

To provide the required route and service information without tying up the on-demand connection, the Novell Internet Access Server 4.1 routing software offers two alternatives:

- **Static route and service databases** —Each database is network protocol-specific and contains a manually configured subset of the route and service information. Manual configuration eliminates the need for periodic maintenance updates because the required route and service information is already available in the static databases of each system.

  A single static route is also useful as a default route for IPX or TCP/IP hosts. In this way, the only routing information crossing the link is that required by users to access a specified set of services.

  For information about configuring static routes and services, refer to the documentation that describes configuration for the network protocol that will run over the WAN connection.

- **Routed on-demand calls (with IPX and IP protocols)** —Rather than using static routing information, a routed on-demand call runs the IPX or IP routing protocol over the link. Because routing protocols would produce steady traffic over a link, the timeout for a routed on-demand call is based on the receipt of Network-layer data packets.

  Routed on-demand calls are well-suited for large corporate networks that have many branch offices. For information about protocol configuration for routed on-demand calls, refer to "Setting Up" in the appropriate protocol documentation.

Call Authentication

The use of public-switched data or telephone networks introduces the possibility of call attempts by unauthorized remote systems. To provide protection against unauthorized router access, the PPP specification defines two optional authentication protocols that authenticate inbound call attempts: the Password Authentication Protocol (PAP) and the Challenge Handshake

Authentication Protocol (CHAP). These protocols ensure that the local system can accept calls from only authorized remote systems. Authentication is based on a remote system identified by a user ID and a password.

With NetWare Link/PPP, you can configure each interface to support one of the following methods for inbound call authentication:

- PAP
- CHAP
- Either PAP or CHAP, with CHAP attempted initially

The main difference between PAP and CHAP is that PAP sends the password string across the WAN in clear text, whereas CHAP is a more secure authentication protocol because it uses the password to encrypt a challenge string. Note, however, that not all PPP products currently support CHAP authentication.

For on-demand connections, you must configure outbound calls to specify an authentication protocol type, an ID, and a password. To accept inbound on-demand connections, you must configure the PPP interface to validate the authentication information supplied by the calling system.

For more information about NetWare Link/PPP and call authentication, refer to "Understanding."

Interface Groups

Each permanent outbound call configuration identifies a specific NetWare Link/PPP interface that is used to place the call to a remote system. However, when supporting on-demand connections, you might want to have a group of interfaces that can be shared between outbound connections. If each interface in the group provides the same capabilities, any available interface can be used to establish an on-demand outbound connection to a remote system. Furthermore, if all the interfaces are attached to switched circuits that are represented by the same telephone number, inbound calls placed to that telephone number can be accepted over any available interface in the interface group. This is similar to a multiple-line business telephone. To place an outbound call, you select any available line. Multiple inbound calls placed to the main office number are directed to any available line.

NetWare Link/PPP lets you assign a symbolic name to a group of interfaces that have similar characteristics. At configuration, you can select an interface group name rather than a specific interface name for making outbound calls.

Selecting an interface group name directs NetWare Link/PPP to use any available interface within the group to establish the connection.

Defining an interface group (F4 from the Network Interfaces screen in NIASCFG) lets you make an on-demand call on any of several network interfaces without creating an individual WAN call destination for each interface. All you need to do is specify the interface group name in place of the interface name in the WAN call destination. When the call is made, the specific interface is selected from the group. Because an interface is selected automatically when the call is made, you do not need to dedicate interfaces to specific destinations. This flexibility in selecting interfaces lets you use your WAN hardware more efficiently.

Login Script

If you are dialing up and logging in to a dial-up service provider, you must decide whether you need to use a login script. Login scripts facilitate this process by defining a command/response dialog that takes place between a router and a remote server at dial-up. According to syntactical conventions, certain login script strings are interpreted as output to be sent by the router (a command to the remote server), whereas others are interpreted as input to be listened for by the router (an expected response from the remote server).

NetWare Link/PPP provides a login script for logging in to a network. For information about customizing a login script to meet your site's needs, refer to "Customizing PPP Login Scripts."

3 Setting Up

This section describes how to use the Novell® Internet Access Server Configuration utility (NIASCFG) to configure NetWare® Link/PPP™ connections.

Configuring a Permanent PPP Connection

The following sections provide instructions for configuring different types of permanent PPP data links and for configuring WAN call destinations for PPP connections.

For more information about NetWare Link/PPP and permanent PPP connections, refer to "Permanent WAN Connections."

This topic contains the following sections:

- How to Configure a Permanent PPP Data Link over a Synchronous Leased-Line Interface
- How to Configure a Permanent PPP Data Link over an ISDN Interface
- How to Configure a Permanent PPP Data Link over a Dial-Up Line Interface
- How to Configure a WAN Call Destination for a Permanent PPP Connection
- Where to Go from Here

How to Configure a Permanent PPP Data Link over a Synchronous Leased-Line Interface

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Identify the physical type of the interface adapter.

To configure a permanent PPP connection over a synchronous leased-line interface, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

   If you are configuring a new interface and the appropriate WAN board has been configured, then continue with Step 2.

   If you are changing the data-link protocol associated with an existing WAN interface, select that interface, then press Del to delete the current interface configuration. This changes the interface's status to Unconfigured. Press Esc to exit, then select Reinitialize System and select Network Interfaces once again.

   The Network Interfaces screen displays a list of network interfaces associated with each configured board with the following information:

   - Board Name —Name you gave to the board when you configured it.
   - Interface —Name of the network interface. Each interface is identified as *boardname_n* , where *n* is the interface number.
   - Group —Interface group, if any, that the network interface belongs to.
   - Media —Network medium or WAN protocol selected.
   - Status —Current status of the interface.

2. Scroll to an unconfigured network interface, then select it.

   The Select A Medium screen is displayed.

3. Select PPP Routing to assign the protocol to the selected network interface.

   The PPP Network Interface Configuration menu is displayed.

   Verify that the physical type is correct for the interface adapter installed. The default value is RS-232.

   Leave all other parameters at their configured default values.

4. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

The Network Interfaces screen is redisplayed with the interface you just configured. The interface status is Enabled ; you can use the Tab key to toggle between Enabled and Disabled. (Note that disabled interfaces are not unconfigured, but are configured interfaces that are not enabled.)

The default configuration for a permanent PPP connection over a synchronous leased-line interface has the following attributes:

- Bit synchronous High-level Data-Link Control (HDLC) framing
- RS-232 interface
- Externally clocked line speed
- NRZ data encoding
- 1,500-byte Maximum Receive Unit (MRU) size (payload data)
- Inbound callers authentication required (PAP or CHAP)
- No modem or data circuit-terminating equipment (DCE) device configuration required
- No PPP data compression
- Generation of SNMP traps disabled
- PPP RFC-defined defaults for all other option values

You can selectively change the values of these parameters, if needed. Refer to the appropriate topics in this section for detailed information.

5. To configure another interface, repeat Step 1 through Step 4.
6. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

After you have configured the desired PPP interfaces for WAN boards, you should configure one or more WAN call destinations as described in "How to Configure a WAN Call Destination for a Permanent PPP Connection."

How to Configure a Permanent PPP Data Link over an ISDN Interface

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Identify the switch type you will be using.

To configure a permanent PPP connection over a synchronous dial-up line ISDN interface, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

   If you are configuring a new interface and the appropriate WAN board has been configured, continue with Step 2.

   If you are changing the data-link protocol associated with an existing WAN interface, select that interface, then press Del to delete the current interface configuration. This changes the interface's status to Unconfigured. Press Esc to exit, then select Reinitialize System and select Network Interfaces once again.

   The Network Interfaces screen displays a list of network interfaces associated with each configured board with the following information:

   - Board Name —Name you gave to the board when you configured it.
   - Interface —Name of the network interface. Each interface is identified as *boardname_n* , where *n* is the interface number.
   - Group —Interface group, if any, that the network interface belongs to.
   - Media —Network medium or WAN protocol selected.
   - Status —Current status of the interface.

2. Scroll to an unconfigured network interface, then select it.

   The Select a Medium screen is displayed.

3. Select PPP Routing to assign the protocol to the selected network interface.

   NOTE: For an ISDN configuration, PPP Routing is the only available medium.

   The PPP Network Interface Configuration menu is displayed.

   Because your configuration is using an ISDN board, the following parameters are automatically set:

   - Framing Type —SYNC
   - Physical Type —ISDN

   The Interface Speed field is grayed out because the interface speed will be determined at dial-up by the format of the telephone number you enter when you configure the WAN call destination (refer to "How to

Configure a WAN Call Destination for a Permanent PPP Connection" on page 51).

4 Select Modem/DCE Type.

A list of the PPP modem and DCE device types is displayed.

5 Select ISDN (AT Controlled) if you are using a NetWare CAPI ISDN driver or if the manufacturer of your AT ISDN driver does not provide a driver-specific terminal adapter script.

6 If you are configuring multiple ports and you want an incoming call to be answered by a particular port, select Local ISDN Address and enter the appropriate ISDN address.

If this parameter is configured, the port will accept incoming calls only from clients that have a matching ISDN address.

7 Optionally, if your services provider uses subaddresses, you can determine which port will answer an incoming call by selecting Local ISDN Sub-Address and entering the appropriate ISDN subaddress.

If this parameter is configured, the port will accept incoming calls only from clients that have a matching ISDN address. This parameter is usually not used in the United States.

8 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

The Network Interfaces screen is redisplayed with the interface you just configured. The interface status is Enabled ; you can use the Tab key to toggle between Enabled and Disabled.

The default configuration for a PPP connection over a synchronous dial-up line ISDN interface has the following characteristics:

- Character synchronous HDLC framing
- ISDN interface
- Line speed determined by the type of ISDN connection
- 1,500-byte MRU (payload data) size
- Inbound callers authentication required (PAP or CHAP)
- No PPP data compression
- PPP RFC-defined defaults for all other option values

You can selectively change the values of some of these parameters, if needed. Refer to the appropriate topics in this section for detailed information.

9 To configure another interface, repeat Step 1 through Step 8.

10 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

After you have configured the desired PPP interfaces for WAN boards, you should configure one or more WAN call destinations as described in "How to Configure a WAN Call Destination for a Permanent PPP Connection."

How to Configure a Permanent PPP Data Link over a Dial-Up Line Interface

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Identify the modem or DCE device you will be using.
- Optionally, if your modem supports Data Terminal Ready (DTR) controlled dialing, configure the modem for DTR dialing (refer to the manufacturer's instructions and refer to Setting Up in the *Modems and DTR-Controlled Devices* documentation).
- Optionally, if your device will be using V.25bis dialing, do one of the following:
  - Configure the modem so that the dialing mode is set to V.25bis dialing mode (refer to the manufacturer's instructions).
  - Use CPECFG to configure the device for V.25bis dialing (refer to the manufacturer's instructions and refer to Setting Up in the *Modems and DTR-Controlled Devices* documentation).

To configure a permanent PPP connection over an asynchronous dial-up line interface, complete the following steps:

1 Load NIASCFG, then select the following parameter path:

Select Configure NIAS > Protocols and Routing > Network Interfaces

If you are configuring a new interface and the appropriate WAN board has been configured, continue with Step 2.

If you are changing the data-link protocol associated with an existing WAN interface, select that interface, then press Del to delete the current interface configuration. This changes the interface's status to Unconfigured. Press Esc to exit, then select Reinitialize System and select Network Interfaces once again.

The Network Interfaces screen displays a list of network interfaces associated with each configured board with the following information:

- Board Name —Name you gave to the board when you configured it.
- Interface —Name of the network interface. Each interface is identified as *boardname_n* , where *n* is the interface number.
- Group —Interface group, if any, that the network interface belongs to.
- Media —Network medium or WAN protocol selected.
- Status —Current status of the interface.

2 Scroll to an unconfigured network interface, then select it.

The Select A Medium menu is displayed.

3 Select PPP Routing to assign the protocol to the selected network interface.

The PPP Network Interface Configuration menu is displayed.

4 The Modem/DCE Type field is already highlighted; press Enter.

A list of the PPP modem and DCE device types is displayed.

5 Scroll through the list and do one of the following:

If your modem/device type is listed:

- Select that modem/device type.
- Select Interface Speed , then select an interface speed from the pop-up menu.

NOTE: For PPP over AIO connections, if you cannot determine the speed of the UART from the documentation provided with the AIO interface, enter the load command for the AIO driver from the server prompt.

You should select the highest data terminal equipment (DTE) speed supported by that modem/device type or UART.

If your modem/device type is not listed, but it uses Hayes* AT commands:

- Select Hayes Compatible.
- Select Modem/DCE Options , then select Dialing Mode.

  A list of the available dialing modes is displayed. Options include AT Commands , DTR Controlled , and V.25bis.
- Ensure that Dialing Mode is set to AT Commands (the default), then press Esc.
- Select Interface Speed , then select an interface speed from the pop-up menu.

  You should select the highest DTE speed supported by that modem/device type or UART.

If you want V.25bis dialing or DTR-controlled dialing:

- Select NO MODEM INSTALLED. (Press Del if a modem is already installed.)
- Select Modem/DCE Options , then select Dialing Mode.

  A list of the available dialing modes is displayed. Options include AT Commands , DTR Controlled , and V.25bis.
- Set Dialing Mode to V.25bis or DTR Controlled , as applicable, then press Enter.
- Ensure that Framing Type is set to SYNC (the default when V.25bis or DTR Controlled is specified).
- Ensure that Interface Speed is set to External (the default when V.25bis or DTR Controlled is specified).

The default modem type of None (NO MODEM INSTALLED) should be used with only leased lines, V.25bis dialing, DTR-controlled devices, null modems, and other directly connected communications links.

NOTE: For DTR-controlled dialing, the dedicated answering modems must be configured with a Framing Type of SYNC , an Interface Speed of External , and a Dialing Mode of None.

All other parameters can be left at their configured default values.

6 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

The Network Interfaces screen is redisplayed with the interface you just configured. The interface status is Enabled ; you can use the Tab key to toggle between Enabled and Disabled. (Note that disabled interfaces are not unconfigured, but are configured interfaces that are not enabled.)

The default configuration for a PPP connection over an asynchronous dial-up line interface has the following characteristics:

- Character asynchronous HDLC framing
- RS-232 interface
- Internally clocked line speed (user-specified)
- 1,500-byte MRU (payload data) size
- Inbound callers authentication required (PAP or CHAP)
- No PPP data compression
- PPP RFC-defined defaults for all other option values

You can selectively change the values of these parameters, if needed. Refer to the appropriate topics in this section for detailed information.

7 To configure another interface, repeat Step 1 through Step 6.

8 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

After you have configured the desired PPP interfaces for WAN boards, you should configure one or more WAN call destinations as described in "How to Configure a WAN Call Destination for a Permanent PPP Connection."

How to Configure a WAN Call Destination for a Permanent PPP Connection

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Configure the appropriate PPP data link (refer to "How to Configure a Permanent PPP Data Link over a Synchronous Leased-Line Interface," "How to Configure a Permanent PPP Data Link over an ISDN Interface," or "How to Configure a Permanent PPP Data Link over a Dial-Up Line Interface" on page 48).

To configure a WAN call destination for a permanent PPP connection, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > WAN Call Directory

2. Press Ins to configure a new WAN call destination.

   The prompt `New Call Destination Name` , allows you to enter a name of up to 47 alphanumeric characters for the new WAN call destination.

   The WAN call destination name entered here is used in several other menu options when a WAN call destination name needs to be identified. You should use a descriptive name, such as the name of the remote destination or a branch or store number.

3. Enter a name for the new WAN call destination.

   A list of supported wide area media is displayed. These are media available on previously configured interfaces.

4. Select PPP as the wide area medium.

   The PPP Call Destination Configuration menu is displayed. The Call Type selection is highlighted. This selection specifies the type of connection to be made: permanent (continuously active) or on-demand (when activated by the presence of data traffic to the remote peer).

5. Ensure the call type is set to Permanent (the default).

   This sets a WAN call destination for permanent calling through the specified interface.

6. Select Interface Name , then select an interface name from the pop-up menu.

   This field allows you to select the name of the configured WAN interface through which this WAN call destination can be accessed.

7. For the Telephone Number field, do one of the following:

   If you are using a dial-up line or V.25bis (but not DTR-controlled dialing), specify a telephone number.

   The ASCII string you enter in the Telephone Number field can be up to 32 alphanumeric characters. This string is used by device (modem) management when initiating the outbound call to this destination.

If you are using a dial-up line with DTR-controlled dialing, leave this parameter blank.

The DTR-controlled device should have been configured with the telephone number offline, as specified by the modem manufacturer.

If you are using a leased line, leave this parameter blank.

8 Select Outbound Authentication , then select the appropriate authentication option from the pop-up menu.

This lets you specify the authentication protocol to use for an outbound connection. You can disable authentication for a permanent call if the remote system does not require either authentication type.

You can choose from the following options:

NOTE: If you choose Either PAP or CHAP , PPP will provide CHAP authentication if CHAP is requested or will provide PAP authentication if PAP is requested.

- CHAP —Allows CHAP to be used.
- Either PAP or CHAP —(Default) WAN call uses either protocol based on what the remote peer requests. This setting offers the most flexibility. If both sides use this setting, then CHAP is used.
- None —WAN call does not provide authentication.
- PAP —Allows PAP to be used.

9 Select Password , then enter a password of up to 47 alphanumeric characters.

NOTE: This field is case-sensitive.

The value specified in this field must be the PAP password (or the CHAP secret value) expected by the remote peer during the PPP authentication. If Outbound Authentication is set to anything other than None , then a password must be specified; this field cannot be left blank.

For the WAN call destination to succeed, this password and the local system ID must also be configured in the inbound authentication database of the called router.

10 Select Local System ID , then enter a local system ID of up to 47 alphanumeric characters.

NOTE: This field is case-sensitive.

During outbound authentication, this name is sent to the remote system to identify the local system for authentication and connection purposes. The default value is the local system server name.

11 Select Remote System ID , then enter a remote system ID of up to 47 alphanumeric characters.

NOTE: NetWare server names should be all uppercase. TCP/IP hostnames are usually lowercase.

This field allows you to specify the name of the remote peer associated with this WAN call destination. Typically, this name is the remote system server name. By default, the Remote System ID is blank.

Leave all other parameters in the PPP Call Destination Configuration menu at their default values. For a complete discussion of the other parameters in this menu, refer to the appropriate topics in this section for detailed information.

12 If the media type is ISDN, select ISDN Parameters and configure the following parameters as needed.

12a Select Remote Address and enter the telephone number of the destination of the call.

This field must be configured if you are using ISDN.

12b If your service provider requires a destination subaddress (usually a telephone extension number), select Remote Sub-Address and enter the desired number.

Your service provider might not require a subaddress to be configured. Contact your service provider for more information.

12c If your service provider requires a local subaddress (usually a telephone extension number), select Local Sub-Address and enter the desired number.

The local subaddress is assigned by your ISDN service provider and might not be required. Contact your service provider for details. The default is the value you configured under Network Interfaces.

12d Select ISDN Call Rate and select a rate of 56 Kbps, 56 Kbps over voice, or 64 Kbps.

Contact your service provider for this information.

13 Press Esc.

14 Select Special Options and configure the following parameters as needed.

If the remote system requires a login script and the medium is not ISDN, select Login Script Name and select the desired login script from the list

of supported scripts or enter the values for the parameters required by the login script, such as the username, password, and so on. Login scripts are not supported for ISDN.

To update the inbound authentication database so that the interface associated with this WAN call destination reflects the connection information entered here, select Inbound Authentication Update and select Enabled.

15 Press Esc until you return to the Internetworking Configuration menu; save your changes when prompted.

16 If prompted, select Yes to synchronize the inbound authentication database.

The inbound authentication database is made to agree with the outbound call authentication parameters in this WAN call destination configuration. This is useful if you expect to receive calls from systems you make calls to.

The WAN call destination you configured is listed in the Configured WAN Call Destinations screen.

17 To configure another WAN call destination, repeat Step 2 through Step 16.

18 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Where to Go from Here

If you want to further customize and optimize your connection, refer to the appropriate topics in this section for detailed information about the following parameters:

- Configuring data or header compression
- Configuring MRU parameters to adjust the frame size
- Configuring call retry and timeout parameters
- Configuring matching inbound and outbound authentication
- Configuring other inbound call options
- Configuring interface physical options

Before your WAN connection works, you must also complete the following tasks:

- Configure network protocols that will run over the WAN connection. These might include the Internetwork Packet Exchange™ (IPX™) protocol, IP, and AppleTalk.
- Bind the network protocols to the configured WAN interfaces.

For information about these two tasks, refer to "Setting Up" in the appropriate protocol documentation.

For information about configuring backup call associations to permanent PPP connections, refer to "Configuring Backup Calls."

Configuring an On-Demand PPP Connection

The following sections provide instructions for configuring on-demand PPP data links over synchronous or asynchronous interfaces, for configuring on-demand PPP data links over ISDN lines, and for configuring WAN call destinations for PPP connections.

For more information about NetWare Link/PPP and on-demand PPP connections, refer to "On-Demand WAN Connections."

This topic contains the following sections:

- How to Configure an On-Demand PPP Data Link over a Synchronous or Asynchronous Interface
- How to Configure an On-Demand PPP Data Link over a Synchronous ISDN Interface
- How to Configure a WAN Call Destination for an On-Demand PPP Connection
- Where to Go from Here

How to Configure an On-Demand PPP Data Link over a Synchronous or Asynchronous Interface

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).

- Identify the serial interface frame type (synchronous or asynchronous) based on the requirements of the connection.
- Identify the physical type of the serial interface.
- Determine the speed at which the interface will communicate.
- Identify the modem or data circuit-terminating equipment (DCE) device you will be using.
- Optionally, if your device will be using V.25bis dialing, do one of the following:
  - Set the dip switch on the device so that the dialing mode is set to V.25bis dialing mode (refer to the manufacturer's instructions).
  - Use CPECFG to configure the device for V.25bis dialing (refer to the manufacturer's instructions and refer to Setting Up in the *Modems and DTR-Controlled Devices* documentation).

To configure an on-demand PPP connection over a synchronous or asynchronous interface, complete the following steps:

1 Load NIASCFG, then select the following parameter path:

Select Configure NIAS > Protocols and Routing > Network Interfaces

If you are configuring a new interface and the appropriate WAN board has been configured, continue with Step 2.

If you are changing the data-link protocol associated with an existing WAN interface, select that interface, then press Del to delete the current interface configuration. This changes the interface's status to Unconfigured. Press Esc to exit, then select Reinitialize System and select Network Interfaces once again.

The Network Interfaces screen displays a list of network interfaces associated with each configured board with the following information:

- Board Name —Name you gave to the board when you configured it.
- Interface —Name of the network interface. Each interface is identified as *boardname_n* , where *n* is the interface number.
- Group —Interface group, if any, that the network interface belongs to.
- Media —Network medium or WAN protocol selected.
- Status —Current status of the interface.

2. Scroll to an unconfigured network interface, then select it.

   The Select A Medium screen is displayed.

3. Select PPP Routing to assign the protocol to the selected network interface.

   The PPP Network Interface Configuration menu is displayed.

4. The Modem/DCE Type field is already highlighted; press Enter.

   A list of the PPP modem and DCE device types is displayed.

5. Scroll through the list and do one of the following:

   If your modem/device type is listed, select it.

   If your modem/device type is not listed, but it uses Hayes AT commands:

   - Select Hayes Compatible.
   - Select Modem/DCE Options , then select Dialing Mode.

     A list of the available dialing modes is displayed. Options include AT Dialing , DTR Controlled , and V.25bis.
   - Ensure that Dialing Mode is set to AT Commands (the default), then press Esc.

   If you want V.25bis dialing:

   - Select NO MODEM INSTALLED. (Press Del if a modem is already installed.)
   - Select Modem/DCE Options , then select Dialing Mode.

     A list of the available dialing modes is displayed. Options include AT Commands , DTR Controlled , and V.25bis.
   - Set Dialing Mode to V.25bis , then press Enter.
   - Ensure that Framing Type is set to SYNC (the default when V.25bis is specified).
   - Ensure that Interface Speed is set to External (the default when V.25bis is specified).

6. Select Framing Type , then select a framing type from the pop-up menu.

   If you use synchronous services such as switched/56 with external digital service unit/channel service unit (DSU/CSU) equipment, select SYNC (synchronous).

If you use switched telephone services with asynchronous modems, select ASYNC (asynchronous).

7 Select Physical Type, then select the appropriate physical type from the pop-up menu.

Options presented depend on the WAN driver that was selected. Options might include RS-232 , RS-422 , V.35 , and X.21.

8 Select Interface Speed , then select the appropriate speed from the pop-up menu.

Synchronous interfaces default to, and should use, external timing provided by the modem or DSU/CSU.

NOTE: For PPP over AIO connections, if you cannot determine the speed of the UART from the documentation provided with the AIO interface, enter the load command for the AIO driver from the server prompt.

Asynchronous interfaces do not use external timing and should use a matching interface speed for both ends of the connection. Asynchronous interfaces default to 9,600 bps.

9 Optionally, do the following:

9a Select Interface Group.

A list of defined interface groups is displayed. If no interface groups have been defined, the list is empty.

9b Select an interface group from the list or press Ins and enter up to 17 alphanumeric characters to create an interface group.

An interface group is a grouping of several interfaces with similar characteristics, such as framing type and line speed. A symbolic name identifies an interface group. All interfaces in a group have similar characteristics and can be used interchangeably.

10 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

The Network Interfaces screen is redisplayed with the interface you just configured. The interface status is Enabled ; you can use the Tab key to toggle between Enabled and Disabled. (Note that disabled interfaces are not unconfigured, but are configured interfaces that are not enabled.)

11 To configure another interface, repeat Step 1 through Step 10.

12 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

After you have configured the desired PPP interfaces for WAN boards, you should configure one or more WAN call destinations as described in "How to Configure a WAN Call Destination for an On-Demand PPP Connection."

How to Configure an On-Demand PPP Data Link over a Synchronous ISDN Interface

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Identify the switch type you will be using.

To configure a permanent PPP connection over a synchronous ISDN interface, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

   If you are configuring a new interface and the appropriate WAN board has been configured, continue with Step 2.

   If you are changing the data-link protocol associated with an existing WAN interface, select that interface, then press Del to delete the current interface configuration. This changes the interface's status to Unconfigured. Press Esc to exit, then select Reinitialize System and select Network Interfaces once again.

   The Network Interfaces screen displays a list of network interfaces associated with each configured board with the following information:

   - Board Name —Name you gave to the board when you configured it.
   - Interface —Name of the network interface. Each interface is identified as *boardname_n* , where *n* is the interface number.
   - Group —Interface group, if any, that the network interface belongs to.
   - Media —Network medium or WAN protocol selected.
   - Status —Current status of the interface.

2. Scroll to an unconfigured network interface, then select it.

The Select A Medium screen is displayed.

3 Select PPP Routing to assign the protocol to the selected network interface.

NOTE: For an ISDN configuration, PPP Routing is the only available medium.

The PPP Network Interface Configuration menu is displayed.

Because your configuration is using an ISDN board, the following parameters are automatically set:

- Framing Type —SYNC
- Physical Type —ISDN

The Interface Speed field is grayed out because the interface speed will be determined at dial-up by the format of the telephone number you enter when you configure the WAN call destination (refer to "How to Configure a WAN Call Destination for an On-Demand PPP Connection" on page 62).

4 Select Modem/DCE Type.

A list of the PPP modem and DCE device types is displayed.

5 Select ISDN (AT Controlled) if you are using a NetWare CAPI ISDN driver or if the manufacturer of your AT ISDN driver does not provide a driver-specific terminal adapter script.

6 If you are configuring multiple ports and you want an incoming call to be answered by a particular port, select Local ISDN Address and enter the appropriate ISDN address.

If this parameter is configured, the port will accept incoming calls only from clients that have a matching ISDN address.

7 Optionally, if your service provider uses subaddresses, you can determine which port will answer an incoming call by selecting Local ISDN Sub-Address and entering the appropriate ISDN subaddress.

If this parameter is configured, the port will accept incoming calls only from clients that have a matching ISDN address. This parameter is usually not required in the United States.

8 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

The Network Interfaces screen is redisplayed with the interface you just configured. The interface status is Enabled ; you can use the Tab key to toggle between Enabled and Disabled.

The default configuration for a PPP connection over a synchronous dial-up line ISDN interface has the following characteristics:

- Character synchronous HDLC framing
- ISDN interface
- Line speed determined by the type of ISDN connection
- 1,500-byte MRU (payload data) size
- Inbound callers authentication required (PAP or CHAP)
- PPP data compression enabled
- PPP RFC-defined defaults for all other option values

You can selectively change the values of some of these parameters, if needed. Refer to the appropriate topics in this section for detailed information.

9 To configure another interface, repeat Step 1 through Step 8.

10 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

After you have configured the desired PPP interfaces for WAN boards, you should configure one or more WAN call destinations as described on this page.

How to Configure a WAN Call Destination for an On-Demand PPP Connection

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Configure the appropriate PPP data link (refer to "How to Configure an On-Demand PPP Data Link over a Synchronous or Asynchronous Interface" on page 56 or "How to Configure an On-Demand PPP Data Link over a Synchronous ISDN Interface" on page 59).

To configure a WAN call destination for an on-demand PPP connection, complete the following steps:

1 Load NIASCFG, then select the following parameter path:

Select Configure NIAS > Protocols and Routing > WAN Call Directory

2 Press Ins to configure a new WAN call destination.

At the prompt `New Call Destination Name` , enter a name of up to 47 alphanumeric characters for the new WAN call destination.

The WAN call destination name entered here is used in several other menu options when a WAN call destination name needs to be identified. You should use a descriptive name, such as the name of the remote destination or a branch or store number.

3 Enter a name for the new WAN call destination.

A list of supported wide area media is displayed. These are media available on previously configured interfaces.

4 Select PPP as the wide area medium.

The PPP Call Destination Configuration menu is displayed. The Call Type selection is highlighted. This selection specifies the type of connection to be made: permanent (continuously active) or on-demand (when activated by the presence of data traffic to the remote peer).

5 Press Enter , then select On-Demand from the pop-up menu.

6 To specify an interface name or an interface group, do one of the following:

If you are specifying an interface name, select Interface Name, *then select an interface name from the pop-up menu.*

If you are specifying an existing interface group, select Interface Group, *then select an interface group from the pop-up menu.*

When you specify an interface group, the system selects any available interface associated with the group for outbound connection attempts. For more information on interface groups, refer to "Interface Groups."

7 For the Telephone Number field, specify a telephone number.

The ASCII string you enter in the Telephone Number field can be up to 32 alphanumeric characters. This string is used by device (modem) management when initiating the outbound call to this destination.

8 Select Idle Connection Timeout , specify a value that is appropriate for your system, then press Enter.

9 Select Outbound Authentication , then select the appropriate authentication option from the pop-up menu.

This lets you specify the authentication protocol to use for an outbound connection. You can choose from the following options:

NOTE: If you choose Either PAP or CHAP , the called PPP system will determine through negotiation which authentication protocol is used.

- CHAP —Allows CHAP to be used.
- Either PAP or CHAP —(Default) WAN call uses either protocol based on what the remote peer requests. This setting offers the most flexibility. If both sides use this setting, then CHAP is used.
- None —WAN call does not provide authentication.
- PAP —Allows PAP to be used.

  You cannot choose the option None for an on-demand call. A form of authentication must be enabled.

10 Select Password, then enter a password of up to 47 alphanumeric characters.

The value specified in this field must be the PAP password or the CHAP secret value expected from the remote peer during the PPP inbound authentication. The value cannot be a null string.

For the WAN call destination to succeed, this password and the local system ID must also be configured in the inbound authentication database of the called router.

NOTE: This field is case-sensitive.

11 Select Local System ID , then enter a local system ID of up to 47 alphanumeric characters.

During outbound authentication, this name is sent to the remote system to identify the local system for authentication and connection purposes. The name is also used by some remote protocol stacks to determine whether the call can be accepted as an on-demand call.

NOTE: This field is case-sensitive.

The default value is the local system server name.

12 Select Remote System ID , then select an ID from the pop-up menu or press Ins and enter a remote system ID of up to 47 alphanumeric characters.

This field lets you specify the name of the remote peer system associated with the WAN call destination entry. This name is typically the remote system server name. You must specify this option.

This name is accessed by some local protocol stacks to identify the WAN call destination needed to restore an on-demand connection to a remote system that previously initiated a connection to the local system.

NOTE: When you configure the protocol you will use for an on-demand PPP connection, you must configure static routes and services. Some protocol stacks do not accept an inbound connection unless they have a configured static route or service to an identified remote system.

Leave all other parameters in the PPP Call Destination Configuration menu at their default values. For a complete discussion of the other parameters in this menu, refer to the appropriate topics in this section for detailed information.

13 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

14 If prompted, select Yes to synchronize the inbound authentication database.

The inbound authentication database is made to agree with the outbound call authentication parameters in this WAN call destination configuration. This is useful if you expect to receive calls from systems you make calls to.

The WAN call destination you configured is listed in the Configured WAN Call Destinations screen.

15 To configure another WAN call destination, repeat Step 2 through Step 14.

16 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Where to Go from Here

If you want to further customize and optimize your connection, refer to the appropriate topics in this section for detailed information about the following parameters:

- Configuring data or header compression
- Configuring MRU parameters to adjust the frame size
- Configuring call retry and timeout parameters
- Configuring matching inbound and outbound authentication

- Configuring other inbound call options
- Configuring interface physical options

Before your WAN connection works, you must also complete the following tasks:

- Configure network protocols that will run over the WAN connection. These might include IPX, IP, and AppleTalk.
- Bind the network protocols to the configured WAN interfaces.

For information about these two tasks, refer to "Setting Up" in the appropriate protocol documentation.

Configuring Backup Calls

This section describes how to use the Novell® Internet Access Server Configuration utility (NIASCFG) to configure a backup call for a WAN connection.

A backup call enhances the reliability of your WAN. It ensures that permanent connections are maintained even if your primary WAN call destination goes down. As a result, you avoid unnecessary delays and maintain high reliability over your WAN connection.

Backup calls are also useful for ensuring filtering reliability. By default, all filters that currently affect a primary call will affect a configured backup call. If a primary call should go down, the configured backup call will maintain your filtering configurations.

You can configure additional filtering for the backup link to meet the specific needs of your site (refer to Setting Up in the *Filters* documentation). If you configure additional filtering, that filtering will be maintained on the backup link in addition to the automatically mapped filtering.

Optionally, the automatic mapping of filtering can be disabled with the LOAD FILTSRV NOBACKUP command. With automatic mapping of filtering disabled, you can configure a selective filtering scheme that is specific to the needs of the backup link (refer to Setting Up in the *Filters* documentation).

Backup calls must be PPP-based and the circuit information must be correctly specified. When you configure a backup call, you specify a backup WAN call destination to be used in the event that the primary WAN call destination becomes unavailable. The Novell Internet Access Server 4.1 routing software

switches automatically to the backup WAN call destination if the primary WAN call destination goes down. When the primary connection is restored, the routing software switches to the primary WAN call destination and terminates the backup.

You specify a backup WAN call destination by configuring two existing WAN call destinations to have an association by which the routing software recognizes one as the primary destination and the other as its backup.

Primary connections can be over fixed or switched circuits. Backups are always over switched circuits.

This section describes the configuration of backup calls through the use of WAN call associations. It contains the following topics:

- "Configuring a Backup Call Association" on page 66
- "Where to Go from Here" on page 69

Configuring a Backup Call Association

This section provides instructions for configuring backup calls.

For more information about the NetWare® Link/PPP™ software, refer to "Understanding."

How to Configure a Backup Call Association

NOTE: A backup call destination can be configured for the same interface as the primary call destination if there is only one physical interface available. Note, however, that in such a configuration, when the backup call is connected, the primary call destination will not be able to reconnect because the interface will be in use.

NOTE: If a primary and backup call are to the same host and that remote host is running the NetWare MultiProtocol Router™ 2.11 or 3.0 software, you must configure different local system IDs in the primary and backup WAN call destination records.

Before you begin, you must complete the following tasks:

- Configure the appropriate WAN board (refer to Setting Up in the *Boards* documentation).
- Configure the appropriate WAN connection (refer to Configuring a Permanent PPP Connection).
- Configure two WAN call destinations to the same destination so that you can associate one as the backup for the other (refer to How to Configure a WAN Call Destination for a Permanent PPP Connection).

To configure a backup call association, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Backup Call Associations

   The Backup Call Associations screen lists all currently configured backup call associations with the following information:

   - Primary Call Destination —A WAN call destination name that has been configured to be a primary call destination.
   - Backup Call Destination —A WAN call destination name that has been configured to be a backup call destination to the primary call destination.
   - Status —Current status of the backup call association.

   This screen has no entries if no backup call associations are configured.

2. Press Ins to create a new backup call association.

   The Backup Association Configuration menu is displayed. The Primary Call Destination field is highlighted.

3. Press Enter to display a list of configured WAN call destinations that are available to be primary call destinations.

   A list of WAN call destinations is displayed. These are the configured WAN call destinations that are available to define as primary call destinations. Destinations that have already been configured to be primary or backup call destinations are not listed here. Only WAN call destinations with a call type of permanent are listed here.

4. Select a primary call destination.

   The Backup Association Configuration menu is displayed again. The Primary Call Destination field is filled in, and the Backup Call Destination field is highlighted.

5. Press Enter to display a list of configured WAN call destinations that are available to be backup call destinations.

   The list of WAN call destinations is displayed again. The destination you selected as a primary call destination is no longer contained in this list.

   NOTE: Only permanent PPP connections can be used as backup call destinations.

6. Select a backup call destination.

The Backup Association Configuration menu is displayed with the Backup Call Destination field filled in.

7 Ensure that Association Status is set to Enabled.

To change the displayed status, select Status , select the desired status from the pop-up display, then press Enter.

8 Optionally, do the following to modify the connect and disconnect timer values:

8a Enter a new value, in seconds, in the Connect Delay Timer field, then press Enter.

When the primary call destination fails, this value is the number of seconds to delay before attempting to connect to the backup call destination.

8b Enter a new value, in seconds, in the Disconnect Delay Timer field, then press Enter.

When the backup call destination is up and the primary call destination reconnects, this value is the number of seconds to delay before disconnecting the backup call.

9 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

The backup call association you configured is listed in the Configured Backup Call Associations menu.

10 To configure another interface, repeat Step 2 through Step 9.

NOTE: When binding to a backup call destination, select WAN Call Destinations and set Type to Manual to keep the backup call from coming up when the router is restarted. This setting does not keep the backup call from coming up automatically when the primary call goes down.

11 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Where to Go from Here

If you want to further customize and optimize your connection, refer to the appropriate topics in this section for detailed information about the following parameters:

- Configuring data or header compression
- Configuring MRU parameters to adjust the frame size
- Configuring call retry and timeout parameters
- Configuring matching inbound and outbound authentication
- Configuring other inbound call options
- Configuring interface physical options

Before your WAN connection works, you must also complete the following tasks:

- Configure network protocols that will run over the WAN connection. These might include the Internetwork Packet Exchange™ (IPX™) protocol, IP, and AppleTalk.
- Bind the network protocols to the configured WAN interfaces.
- Specify an automatic permanent WAN call destination in order to make the primary call initially.

For information about these tasks, refer to "Setting Up" in the appropriate protocol documentation.

Configuring Data or Header Compression

NetWare Link/PPP supports compression of either the data or the header field of the Point-to-Point Protocol (PPP) packet. Both cannot be enabled at the same time because PPP data compression uses fields that are usually deleted by PPP header compression. With either method, you can also use Internetwork Packet Exchange™ (IPX™) header compression or TCP/IP header compression for further optimization.

This topic contains the following sections:

- Using Data Compression
- Using Header Compression
- How to Configure Data or Header Compression
- Maximizing Performance with the Packet Burst Protocol and Large Internet Packet Protocol

Using Data Compression

When you select data compression, you are specifying that you want data to be transmitted in a more compact form. Using data compression has the following effect:

- Reduces the amount of data transferred over a communications link by replacing previously observed data sequences with more compact sequences
- Increases the apparent speed (bandwidth) of the link, at the cost of some additional router CPU usage and memory usage
- Allows for a more effective use of a PPP link when packets are routed between remote LANs

  NOTE: When you enable data compression, it is used only if both the local and remote peers support a common compression technique. The Control Compression Protocol (CCP) handles the negotiation and selection of a common data compression protocol between systems. NetWare Link/PPP supports the Pattern Predictor algorithm, as well as other CCP-compliant data compression algorithms. Note that the Novell Internet Access Server 4.1 routing software maintains backward compatibility with NetWare MultiProtocol Router™ 3.1 PPP data compression if the PTFs are installed. PPP data compression is not compatible with NetWare MultiProtocol Router 2.11 or 3.0.

By default, PPP does not guarantee data integrity. Retransmission of lost or corrupted data is the responsibility of higher-level protocols. However, when CCP successfully negotiates data compression, a reliable data-link protocol replaces the unreliable PPP data link to ensure the integrity of the compressed data exchange. This reliable data-link protocol is the International Telecommunication Union (ITU) Link Access Protocol-Balanced (LAPB). LAPB significantly increases the reliability of the communications link when used in conjunction with rigorous error checking after the received data is uncompressed.

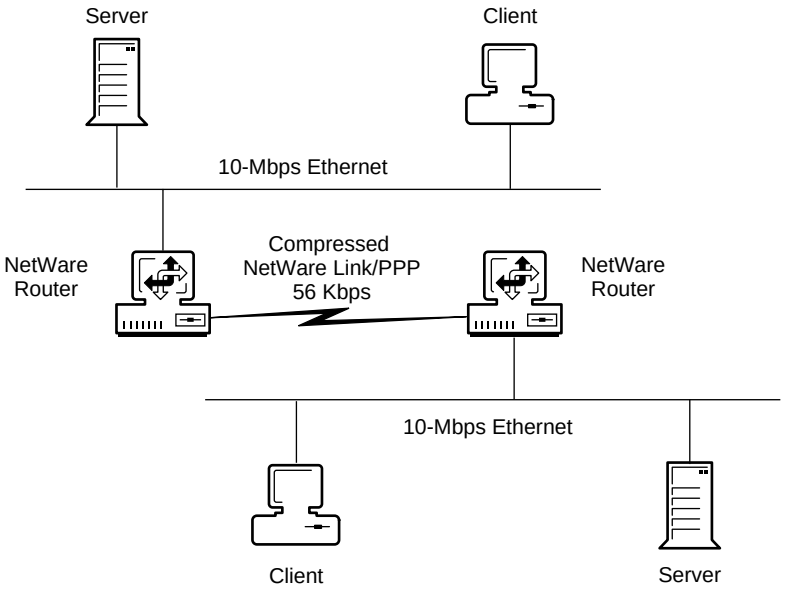
Most data compression algorithms do not permit data corruption on the communications link because each bit of the compressed data is much more significant than the uncompressed data. One incorrect bit can result in thousands of bytes of incorrect output. This, in turn, results in retransmission requests and lower overall throughput.

Data compression is performed on network data only. NetWare Link/PPP Link Control Protocol (LCP) and Network Control Protocol (NCP) data is passed uncompressed. LCP and NCP data exchanges are used for connection management and configuration negotiation. They are typically used only during the connection establishment and termination operations.

NetWare Link/PPP supports the Pattern Predictor algorithm, as well as other CCP-compliant data compression algorithms. The Pattern Predictor compression technique provides useful data compression over a wide range of line speeds, from 1,200 baud through E1 data rates. Future versions of NetWare Link/PPP might include additional compression algorithms tailored to provide higher compression at specific line speeds.

Figure 5 illustrates a simple network configuration in which NetWare Link/PPP is operating over a 56-Kbps leased-line interface to connect two Ethernet LANs operating at 10 Mbps. Note that data compression is necessary only over the PPP link connecting two LANs, because this link is the slowest portion of the end-to-end network traffic.

Figure 5 PPP Data Compression for LAN-to-LAN Routing



Using Header Compression

When you use header compression, you are specifying that you want the following two fields in the header to be compressed:

- Address and Control
- Protocol ID

Compressing these fields reduces PPP header overhead. Note, however, that enabling this compression does not guarantee that header compression is actually used. Header compression is negotiated when the link is established.

How to Configure Data or Header Compression

To configure data or header compression, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

2. Scroll to a configured PPP interface, then select it.

   The PPP Network Interface Configuration menu is displayed.

3. Select PPP Negotiations Options.

   The PPP Negotiations Options menu is displayed.

   WARNING: Data and header compression cannot be enabled at the same time. PPP data compression uses fields that are usually deleted by PPP header compression.

4. Do one of the following:

   If you are configuring header compression, select PPP Header Compression, *then select* Enabled.

   This option specifies whether compression of the PPP Address and Control and PPP Protocol fields is enabled. PPP header compression is disabled by default.

   Enabling this option does not guarantee that header compression is used. It indicates only that the local PPP interface attempts to negotiate its use.

   If you are configuring data compression, do the following:

   - **Select** PPP Data Compression, *then select* Enabled.

     This option specifies whether PPP data compression is used. PPP data compression is enabled by default.

     NOTE: PPP data compression uses 150 KB of memory per port. If the router is short of memory, disable PPP data compression to decrease memory usage.

     Enabling this option does not guarantee that data compression is negotiated with the remote peer. If the remote peer does not support compression, negotiation for the option fails, but the connection is still established.

- **If you are configuring data compression, select** Preferred Compression Algorithm, *then select the desired algorithm.*

  The interface starts the compression algorithm negotiation process with the selected algorithm. However, the algorithm might not be used. If the selected algorithm is not supported by the peer router, negotiation continues until a common data compression algorithm is found. The default algorithm is Predictor II.

5. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.
6. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Maximizing Performance with the Packet Burst Protocol and Large Internet Packet Protocol

NetWare Link/PPP data compression works best when a constant supply of transmitted data is available at the interface. This maximizes the replacement of data sequences with more compact sequences. Therefore, when using IPX with NetWare Link/PPP data compression, you should also use the IPX Packet Burst protocol and the Large Internet Packet (LIP) protocol.

The Packet Burst protocol enhances IPX by allowing larger data transactions, composed of multiple IPX packets, to be transmitted as a single burst (or logical operation). Acknowledgments are issued for the complete burst rather than for individual IPX packets. The Packet Burst and LIP protocols are included in the NetWare 3.12 and NetWare 4™ operating systems. LIP and Packet Burst are enabled separately on IPX clients.

Packet Burst protocol support is provided for IPX client workstations by the latest version of the Virtual Loadable Module™ (VLM™) software update. Refer to this update for instructions on how to configure the protocols.

Configuring Maximum Receive Unit Parameters to Adjust the Frame Size

NOTE: If you choose to configure a high Maximum Receive Unit (MRU) range for NetWare Link/PPP, you might need to edit the STARTUP.NCF file to redefine the

Maximum Physical Receive Packet parameter. The Maximum Physical Receive Packet parameter defined in the STARTUP.NCF file must be large enough to accommodate the configured NetWare Link/PPP MRU Maximum Size value plus 10 bytes.

NetWare Link/PPP ensures that both send and receive data frames are never outside the configured MRU range. Through negotiation with the remote peer, the data frames are never smaller than the configured minimum MRU or larger than the configured maximum MRU. If the remote PPP peer requires frames outside the range, the connection is not established.

NetWare Link/PPP provides three parameters that control MRU negotiation with the remote data-link peer. The minimum and maximum MRU parameters establish a window or range of MRU values that are acceptable to the NetWare Link/PPP interface. The optimal MRU value establishes the preferred MRU value that the NetWare Link/PPP interface tries to establish.

The Internet PPP specification defines a default MRU size of 1,500 bytes. IP can run with 1,500-byte datagrams because it can support fragmentation of the stream to fit the data-link MRU. However, source route bridging does not support fragmentation. Therefore, when providing connectivity between bridged token ring LANs, you should reconfigure the NetWare Link/PPP interface to support a 4,500-byte MRU for the token ring LANs.

Using the bridged token ring example, the minimum and optimal MRU values should be set to 4,500 bytes. This configuration change forces the negotiated MRU value to 4,500 bytes, or the connection is not established.

If you are using IPX routing over NetWare Link/PPP to connect two token ring LANs, a negotiated MRU size of 4,500 bytes is preferred because it allows full-size token ring packets to be exchanged. A smaller MRU is still usable because the IPX packet size is automatically adjusted to the smaller NetWare Link/PPP MRU. In this case, you could configure the MRU Optimal Size parameter to 4,500 and leave the MRU Maximum Size and MRU Minimum Size parameters at their default values of 4,500 and 600, respectively. This approach starts the MRU negotiation with the remote PPP system at 4,500, but allows the acceptance of any value proposed by the remote system within the range of 600 to 4,500.

How to Configure MRU Parameters to Adjust the Frame Size

To configure MRU parameters, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

2. Scroll to a configured PPP interface, then select it.

   The PPP Network Interface Configuration menu is displayed.

3. Select PPP Negotiations Options.

   The PPP Negotiations Options menu is displayed.

4. Select MRU Maximum Size , then enter a value.

   This parameter specifies the largest MRU size that PPP accepts for the local interface during link negotiation with a remote peer. This value, combined with the MRU Minimum Size value, defines the upper and lower limits used during MRU negotiation. The remote PPP peer must agree to a value within these limits to establish a connection.

5. Select MRU Optimal Size, then enter a value.

   This parameter specifies the preferred MRU size that PPP proposes for the local interface during link negotiation with a remote peer. The actual negotiated MRU value can be anywhere within the range established by the MRU Minimum Size and the MRU Maximum Size parameters.

6. Select MRU Minimum Size , enter a value, then press Esc to confirm your configuration entries and return to the PPP Network Interface Configuration menu.

   This parameter specifies the smallest MRU size that PPP accepts for the local interface during link negotiation with a remote peer. This value, combined with the MRU Maximum Size value, defines the upper and lower limits used during MRU negotiation. The remote PPP peer must agree to a value within these limits to establish a connection.

7. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

8. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Configuring Call Retry and Timeout Parameters

When you create WAN connections, you can establish the following outbound call attributes for permanent and on-demand calls:

- For either type of connection, the conditions for retrying failed connections
- For on-demand connections, the amount of time for links to remain active when no data has been transmitted

This topic contains the following sections:

- Retrying Failed WAN Connections
- Terminating Inactive On-Demand Connections
- How to Configure WAN Call Retry and Timeout Parameters

Retrying Failed WAN Connections

By default, a PPP WAN connection retries all self-correcting failures at increasing intervals until the call is established, with a retry interval limit of 10 minutes for permanent connections and 2 minutes for on-demand connections.

You can use the Retry Mode parameter to specify the conditions under which a failed permanent connection is retried automatically. Its default setting, Retry Self-Correcting Failures , uses error information from NetWare Link/PPP to differentiate between errors that are self-correcting, such as a busy telephone number, and errors that require user intervention, such as a call authentication failure.

Alternatively, you can set up your system to retry all failures (Retry All) or to never retry at all (Never Retry). Retrying all failures is used for unattended environments and for situations in which configuration changes are not easily made to the router. For example, it might be easier to correct problems at the peer system or WAN service provider system, and simply let the router continue to retry until the problem is corrected. However, this is not advisable when a cost is associated with each connection attempt.

Retrying failed connections results in successive connection attempts with an increasing delay between each attempt. By default, the delay is set initially to 1 second, and it is increased exponentially until the maximum delay specified by the Retry Interval Limit parameter is reached.

WARNING: Some retry intervals might be slightly longer than expected because NetWare Link/PPP employs a random backoff interval to decrease the chance of collisions between calling systems.

The Retry Limit Handling parameter defines connection attempt behavior after the retry interval limit has been reached. Retries can continue indefinitely

at the configured interval limit, or retry attempts can be terminated and the connection failed. For permanent connections, keep the default, Continuous At Limit , to support unattended operation. Otherwise, use Stop At Limit if a cost is associated with each connection attempt.

For on-demand connections, the default is Stop At Limit.

Terminating Inactive On-Demand Connections

You can specify the amount of time that an on-demand connection remains active without the presence of data by setting the Idle Connection Timeout WAN call destination parameter. The default timeout of 10 minutes is usually a reasonable compromise between performance and cost effectiveness when using public-switched telephone networks.

WARNING: Setting this value too low can cause the connection to terminate before data is actually sent. This forces multiple-connection establishment and degradation of data transfer performance.

Consider switched-circuit connection billing policies when modifying the value of the timeout. If a large percentage of the connection cost is based on the call duration, reduce the value to minimize costs. If a large percentage of the connection cost is based on establishing the initial connection, and if the call duration is less of a factor, increase the value.

How to Configure WAN Call Retry and Timeout Parameters

To configure WAN call retry and timeout parameters, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > WAN Call Directory

2. Scroll to the WAN call you are configuring, then select it.

   The PPP Call Destination Configuration menu is displayed.

3. To set the idle connection timeout, do the following:

   - Select Idle Connection Timeout.
   - Specify a value for hours, minutes, and seconds in the pop-up menu, then press Enter.

4. Select Call Retry Options and do one or more of the following:

   To set the retry mode, do the following:

   - Select Retry Mode.

- Select one of the modes displayed in the pop-up menu, then press Enter.

To set retry limit handling, do the following:

- Select Retry Limit Handling.
- Select one of the options displayed in the pop-up menu, then press Enter.

To set the retry interval limit, do the following:

- Select Retry Interval Limit.
- Specify a value for hours, minutes, and seconds in the pop-up menu, then press Enter.

5. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.
6. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Configuring Matching Inbound and Outbound Authentication

By default, every time a NetWare Link/PPP outbound call is configured, the authentication information for that outbound call is also entered into the inbound authentication database for the selected interface. The reason is that connectivity between systems is usually bidirectional. For example, if you need to call system X, chances are great that system X also needs to call you. If the same password is used by both systems, you do not need to configure the information for the outbound and inbound authentication entries separately.

You can specify that outbound authentication should match its information with inbound authentication. This causes an inbound authentication entry to be made with the remote system ID and password entered for the WAN call destination. If a group is selected, the database for each interface in the group is updated. If you change either the remote system ID or the password in a WAN call destination, and that remote system ID was previously added to the authentication database, you are prompted to determine whether it will be added to the inbound authentication database.

NOTE: Disable Inbound Authentication Update for a more secure method of authentication. This way, the inbound authentication information is not created or updated automatically for a WAN connection and its related interface, enabling you to maintain the inbound and outbound authentication entries separately.

How to Configure Matching Inbound and Outbound Authentication

To configure matching inbound and outbound authentication, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > WAN Call Directory

2. Select a configured WAN call destination.

   The PPP Call Destination Configuration menu is displayed.

3. Select Special Options.

4. Select Inbound Authentication Update , then select Enabled from the pop-up menu and press Enter.

5. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

6. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Configuring Additional Inbound Call Options

You can also configure the following inbound call options:

- Inbound Call Processing —Controls the processing of inbound connection attempts. When Disabled is selected, no inbound connections are allowed. If a modem is attached to the interface, it is initialized not to answer when called.

  Disabling inbound calls on an interface is a good way to reserve the interface for outbound call attempts.

- Local System ID for CHAP —Provides a common local system ID that can be used by multiple connected NetWare Link/PPP systems that are using CHAP authentication. This option allows a remote system to maintain a single CHAP authentication secret instead of having to maintain a separate CHAP authentication secret for each local system.

Note that the Local System ID for CHAP parameter is used only for CHAP challenges issued to remote systems that are calling in. The local system ID specified in the WAN call destination configuration is used for the name field value in a CHAP response to authenticate a local system to a remote system.

- Authentication Database Name —Maintains caller authentication information in named databases. Each interface can have a unique database, or multiple interfaces can share a single database. Each database can contain any number of inbound authentication entries. By default, all NetWare Link/PPP interfaces share a single database name of PPP-AUTH.
- Authentication Database —Accesses the inbound authentication database specified in the Authentication Database Name parameter. You can select an inbound authentication entry from the list, then delete, view, or edit it. You can also create new entries. New entries use a remote system ID from the list or a new remote system ID you create by pressing Ins while in the Remote System ID list.

How to Configure Additional Inbound Call Options

To configure inbound call processing, modify the authentication database name, or modify authentication database contents, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

2. Scroll to a configured PPP interface, then select it.

   The PPP Network Interface Configuration menu is displayed.

3. Select Authentication Options.

   The PPP Inbound Authentication Options menu is displayed.

4. Do one or more of the following:

   To configure inbound call processing, select Inbound Call Processing, *then select* Enabled *or* Disabled *from the pop-up menu.*

   To configure a common local system ID for CHAP authentication, select Local System ID for CHAP, *then enter a unique name of up to 45 alphanumeric characters.*

To configure a common local system ID for multiple NetWare Link/PPP systems using CHAP for authentication, select Local System ID for CHAP, *then enter a unique alphanumeric name.*

If your network configuration consists of multiple routers and third-party PPP systems, using a common local system ID for CHAP minimizes authentication processes and is easier to maintain.

To modify the authentication database name, select Authentication Database Name, *then enter a new name of up to eight characters.*

To modify the authentication database contents, do the following:

- Select Authentication Database.
- To modify an existing entry, select a remote system ID from the list displayed in the pop-up menu, then enter a new password.

  To delete an existing entry, select a remote system ID from the list displayed in the pop-up menu, then press Del.

  To create a new entry, press Ins , enter a new remote system ID of up to 47 ASCII characters, then enter a password.

5. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.
6. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Configuring the Bandwidth Allocation Control Protocol and the Multilink Protocol

The Bandwidth Allocation Control Protocol and the Multilink Protocol are used in conjunction with each other. The Bandwidth Allocation Control Protocol and the Multilink Protocol enable you to use multiple physical ports on your WAN boards to represent a single logical link to one location. When the bandwidth threshold of one port is reached, the bandwidth of the next port becomes available. More ports are added to the connection if bandwidth requirements continue to increase beyond the threshold of the ports currently in use. This feature greatly increases the total available bandwidth.

To configure the Bandwidth Allocation Control Protocol and the Multilink Protocol, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

2. Select or create a PPP WAN interface.

3. Select Local Telephone Number and enter the local (inbound) telephone number of this interface.

4. Press Esc and save your changes.

5. Select WAN Call Directory.

   The Configured WAN Call Destinations screen is displayed.

6. Select the appropriate PPP destination.

7. Select Multilink Configuration.

   The PPP Multilink Protocol Configuration menu is displayed.

8. Configure the Total Member Links parameter.

   This parameter represents the maximum number of physical WAN ports you want to make available for use in the multilink connection. You can use up to 32 ports.

9. Configure the following parameters as needed.

   To bring up additional ports as needed, set Member Link Activation Type *to* Bandwidth-On-Demand. *To have all available ports active at the same time, set* Member Link Activation Type *to* Static.

   When the Member Link Activation Type parameter is set to Bandwidth-On-Demand , you must configure the next two parameters to specify the bandwidth utilization that causes the next port to be added to the WAN connection and the time period that is used to calculate the utilization percentage.

   To configure the percentage aggregate utilization for the connection that must be exceeded to activate an additional port, set Bandwidth Threshold Level *to the desired value.*

   The default is 80%.

   To configure the time in seconds that will be used to compute the real-time bandwidth utilization, set Bandwidth Measurement Time *to the desired value*.

The default is 30 seconds.

To use a single interface as a secondary interface, set Interface Selection *to* Interface. *To use multiple interfaces as a secondary interface, set* Interface Selection *to* Group Interface.

To specify which interface or interface group will be used as a secondary interface when the bandwidth threshold of the primary interface is exceeded, select Interface/Group Name.

When this field is selected, a list of configured interfaces and groups from which to choose is displayed.

To specify the outbound phone numbers that will be used to establish secondary links, select Phone Number Configuration.

If the media type is ISDN, one phone number can be used for multiple calls.

10 Press Esc.

11 If needed, configure Call Retry Options as described in "How to Configure WAN Call Retry and Timeout Parameters."

12 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

13 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Configuring Enterprise-Specific Traps

You can also configure enterprise-specific traps so that particular SNMP traps will be generated to provide diagnostic information about events such as failed PPP connections. This diagnostic information appears in console notifications.

To configure enterprise-specific traps, complete the following steps:

1 Load NIASCFG, then select the following parameter path:

Select Configure NIAS > Protocols and Routing > Network Interfaces

2 Scroll to a configured PPP interface, then select it.

The PPP Network Interface Configuration menu is displayed.

3 Select Enterprise Specific Traps.

The Enterprise Specific Traps Configuration menu is displayed.

4 Do one or more of the following:

To enable an SNMP trap for failed PPP connections, select PPP Call Attempt Failure Trap, *then select* Enabled *from the pop-up menu.*

The failed PPP connections trap is disabled by default.

To enable an SNMP trap for PPP connection terminations, select PPP Call Termination Trap, *then select* Enabled *from the pop-up menu.*

The PPP connection terminations trap is disabled by default.

To enable an SNMP trap for when the physical layer's send and receive utilization exceeds its threshold, select Physical Bandwidth Threshold Trap, *then select* Enabled *from the pop-up menu.*

The physical bandwidth threshold trap is disabled by default.

To force PPP to generate an SNMP trap if the LCP experiences an up or down transition of the link, select PPP Link Up/Down Trap, *then select* Enabled *from the pop-up menu.*

The PPP link up/down trap is disabled by default.

If the Physical Bandwidth Threshold Trap *is enabled, to modify the bandwidth, enter new percentage values for* Bandwidth Lower Threshold *and* Bandwidth Upper Threshold.

After bandwidth threshold traps begin to be sent because the upper threshold has been exceeded, traps will continue to be sent until utilization falls below the lower threshold.

By default, the upper threshold is 80 and the lower threshold is 60. The upper threshold can be any integer less than 100 and greater than the lower threshold.

5 Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.

6 If you want these changes to take effect immediately, select Reinitialize System.

If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Configuring Interface Physical Options

You can also configure the following low-level serial interface parameters:

- Send Queue Limit —The maximum number of outbound data frames that can be queued to the interface for transmission. When the queue limit is exceeded, frames are returned to the Network layer.

  The Send Queue Limit functionality provides transmit time limiting with a random drop mechanism, as well as an item count limit with a random drop.

- Data Encoding —The serial data encoding technique, specified as Non-Return to Zero (NRZ) or Non-Return to Zero Inverted (NRZI). Data encoding is meaningful only when the interface framing type is synchronous.

- Idle Line State —The serial line interframe idle line transmission state, specified as either Flags (repeated transmission of the High-level Data-Link Control [HDLC] 7E synchronous pattern) or Marks (holding the data line in the marking state).

- Simulate DSR ON: , Simulate DCD ON: , Simulate CTS On: —These three options should be used only when the attached modem or communication device does not provide the signal or an equivalent.

How to Configure Interface Physical Options

To configure authentication and call management parameters, complete the following steps:

1. Load NIASCFG, then select the following parameter path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces

2. Scroll to a configured PPP interface, then select it.

   The PPP Network Interface Configuration menu is displayed.

3. Select Physical Options.

   The PPP Physical Configuration Options menu is displayed.

4. Do one or more of the following:

   To configure the send queue limit, select Send Queue Limit, *then enter a value.*

   Set the limit to zero for unlimited queueing, but keep in mind that this can result in NetWare system buffer depletion.

To configure data encoding, select Data Encoding, *press* Enter, *then select one of the displayed options.*

Use NRZ encoding unless the remote PPP node supports only NRZI. Make sure that data encoding types are configured to be the same at both ends of the link.

To configure the serial line interframe idle line transmission state, select Idle Line State, *then select one of the displayed options.*

Select Flags for repeated transmission of the HDLC 7E synchronous pattern. Select Marks to make the transmitter hold the data line in the marking state.

NOTE: The idle line state must be the same at both ends of the link. Not all drivers support both Flags and Marks. If the selected driver does not support both options, only the supported option is offered. Make sure you select the idle line state that you know the remote PPP node supports.

To configure the WAN driver to assume the interface signal is on, do one or more of the following:

NOTE: Use these options only when the attached modem or communication device does not provide the signal or an equivalent.

- Select Simulate DSR On: , then select Yes.
- Select Simulate DCD On: , then select Yes.
- Select Simulate CTS On: , then select Yes.

5. Press Esc to return to the Internetworking Configuration menu; save your changes when prompted.
6. If you want these changes to take effect immediately, select Reinitialize System.

   If you want to configure other parameters, do so now, then reinitialize the system when you are finished.

Where to Go from Here

Before your WAN connection works, you must also complete the following tasks:

- Configure network protocols that will run over the WAN connection. These might include IPX, IP, and AppleTalk.
- Bind the network protocols to the configured WAN interfaces.

For information about these two tasks, refer to "Setting Up" in the appropriate protocol documentation.

Customizing PPP Login Scripts

For users or systems dialing up and logging in to asynchronous service providers, login scripts facilitate the process by defining a command/response dialog that takes place between a router and a remote server during the dial-up sequence. Login scripts can also be used to convey additional information, such as a request to connect to a specific destination.

This topic provides information about how you can create or customize login scripts to dial in to other types of networks. It contains the following sections:

- "Customizing a PPP Login Script" on page 88
- "Login Script Operation" on page 89
- "Login Script Syntax" on page 89

Customizing a PPP Login Script

The Novell® Internet Access Server 4.1 routing software provides a Windows-based utility that enables you to create a customized PPP login script. To create, edit, or install a PPP login script, start the WMDMMGR utility the same way you would start any Windows 3.1, Windows 95, or Windows NT utility. This utility can be run only at a Windows workstation and cannot be run from the DOS prompt.

WMDMMGR is located in the SYS:\SYSTEM\UTILS directory on your server. A sample PPP login script, called ISPLOGIN.LSC, is provided in the SYS:\SYSTEM directory of your router. This sample file can be modified to meet your requirements. Multiple scripts can be stored in one .LSC file. WMDMMGR lists all scripts in the selected .LSC file. The name defined in the utility is the script name used by the Novell Internet Access Server 4.1 routing software and has no relation to the filename.

All scripts from earlier releases of the Novell routing software are saved in SYS:\SYSTEM\BACKUP during installation. These old scripts can be converted to the new format using WMDMMGR. In some cases, warning messages might occur if the old script has syntax errors. After the errors are corrected, the script can be modified or used as is. The conversion process is described in the online help.

To create a new login script, select New from the File menu. To modify an existing login script, select Open from the File menu. After editing the login script as described in the online help, save your changes by selecting Save or Save As from the File menu. To edit existing files, copy the files to the SYS:\SYSTEM directory.

Your login script must contain at least one of the words contained in the login prompt received from your Internet Service Provider (ISP). For example, if the prompt from your ISP is Enter user name, then your login script must have at least one of these words in the expected input string from the remote system.

The remaining sections in this appendix provide the background information you need to understand the operation of PPP login scripts.

Login Script Operation

Login scripts define a command/response dialog that takes place between a router and a remote server at dial-up.

The syntax of the Novell Internet Access Server 4.1 login script allows you to define specific strings to be interpreted as output to be sent by the router (a command to the remote server) or as input to be listened for by the router (an expected response from the remote server). Delays can also be specified to ensure that commands complete successfully.

This design allows any string to be designated as a command from router to server and any other string to be designated as a response. It provides a flexibility that will enable you to create new login scripts or to modify existing ones to meet your site's specific needs. The customization you will need to do is determined by the specifications provided by the ISP.

Login Script Syntax

Login scripts consist of a series of one-line entries that define the script name, certain script parameters, and the dialog of expected interaction between the router and the remote server.

WMDMMGR allows for multiple login scripts to be put in one .LSC file. The login script file must contain the name of the login script so that NIASCFG can list it as an available login script when you select Login Script Name at configuration. The maximum length of the script name is 39 characters. The script name can be multiple words separated by spaces (for example, SILICON VALLEY NET).

Each script contains a series of script prompts labeled Param[1] through Param[5]. These tags represent up to five placeholders to define arguments that can be embedded in output lines. For instance, a typical login script might use these parameters to define a user ID, a password, and a service to be selected. These three pieces of information can then be treated as three arguments in the login script that supply the rest of the information specific to the router/server dialog. With generic parameters such as these, one common login script can be used for all users and configured in the PPP WAN call destination.

When a login script is configured in the PPP WAN call destination, you are shown the prompts that are defined in the Param[1] through Param[5] fields in the script. You are then prompted to enter a value for each parameter. For example, if Param[1] is defined as username and Param[2] is defined as password, you are prompted to enter values for the username and password. The values are stored in the WAN call destination configuration and are substituted into the login script when the call is made and the script is executed. The maximum tag length is 25 characters.

The login script file consists of a series of script operations. These are the lines in a login script that specify the command/response exchanges to take place between the router and the remote server. The following are examples of operations used in a typical login script:

- **OUTPUT**

  This operation signifies the beginning of an output string, a command sent by the router to the remote server.

  STRING is a command string that the remote server recognizes. This command string can contain the following:

  - A literal command known to the remote host
  - ASCII control characters \1 through \0x1a

    These are specified with entries of **'A** through **'Z** (the letters *A* through *Z* preceded by a back-quote character [**'**]).

    Common control characters to embed in the output operations include **'I** or **\0x9** (the Tab character), **'M** or **\0xd** (the Carriage Return character), and **'J** or **\0xA** (the Line Feed character).

  - **[1] . . . [***5***]**

    Any of the parameters specified in the login script can be embedded in an output string. For instance, if **[1]** is specified as equal to the

prompt for the username in the script, **[1]** can be entered as part of the output string. This entry instructs the router to substitute the value for the User Name entered during the configuration of the PPP call destination and sends it to the remote server. No more than five tags can be defined and used in the script. Any defined parameter, however, can be embedded more than once, if necessary.

- **WAIT FOR INPUT**

  This operation signifies the beginning of an expected input string, a response from the remote server that the router will listen for.

  STRING is a remote server response that the router recognizes. It is an input line terminated by Enter (**'M**).

- **Pause**

  This operation signifies a delay, or pause. The interval for the delay is specified as *N* tenths of a second.

- **Quiet Wait**

  This operation signifies a quiet period, an interval of no input. The interval for the quiet period is specified as *N* tenths of a second.

  Quiet periods are generally the interval of time required for the current input to conclude.

Using Modem Description Files

This topic discusses the use of modems with the Novell® Internet Access Server 4.1 routing software. It contains the following sections:

- "Customizing a Modem Description File" on page 91

  This topic describes the utility used to create or modify modem description files for the Novell Internet Access Server 4.1 routing software.

- "Limited Public-Switched Telephone Support" on page 92

  This topic describes using dial-up synchronous modem connections for limited public-switched telephone support.

- "Modem Description Files" on page 96

  This topic describes modem description files, modem-specific files that enable modem support in the Novell Internet Access Server 4.1 routing

software. This section describes the information provided by these files. It also explains file syntax and provides sample files.

- "Environments" on page 110

  This topic describes how Novell's modem control is implemented in the NetWare® server environment.

Customizing a Modem Description File

The Novell Internet Access Server 4.1 routing software provides a Windows-based utility that enables you to create a customized modem description file. To create, edit, or install a modem description file, start the WMDMMGR utility the same way you would start any Windows 3.1, Windows 95, or Windows NT utility. This utility can be run only at a Windows workstation and cannot be run from the DOS prompt.

WMDMMGR is located in the SYS:\SYSTEM\UTILS directory on your server. Three sample modem description files, with an .MDC extension, are provided in the SYS:\SYSTEM directory of your router. These files contain modem scripts that are certified by the Novell Labs™ group (NIASCERT.MDC), as well as scripts for commonly used modems (NIASMDM1.MDC and NIASMDM2.MDC). You can modify these modem scripts to meet your requirements, although this is not recommended for scripts in the NIASCERT.MDC file.

To create a new modem description file, select New from the File menu. To modify an existing login script, select Open from the File menu. After editing the modem description file as described in the online help, save your changes by selecting Save or Save As from the File menu. To edit existing files, copy the files to the SYS:\SYSTEM directory. If you have any problems editing or using existing modem description files, refer to Using the WMDMMGR Utility in the *Modems and DTR-Controlled Devices* documentation.

The remaining sections in this topic provide the background information you need to understand the operation of modem description files.

Limited Public-Switched Telephone Support

This topic describes the pseudopermanent connection feature supported by the router using dial-up synchronous modems. The dial-up synchronous connection is established automatically by the modems when the routers at both ends are turned on. The connection is terminated when either of the two routers is turned off or otherwise stopped.

Pseudopermanent Link Operation

The pseudopermanent link is a dial-up link established over the Public Switched Telephone Network (PSTN) using a pair of synchronous modems. By its very nature, this connection is asymmetrical because one modem originates the call and the other modem answers the call. Therefore, the calling end needs to be programmed to automatically dial the stored telephone number of the remote modem, and the remote modem needs to be programmed to automatically answer the incoming call.

Initial Connection Establishment

When the routers are turned off, the Data Terminal Ready (DTR) signal is set low, thereby prohibiting any connection between the modems. When the router at the calling end is turned on, it turns on the DTR, triggering the modem to automatically dial and establish a connection. When the calling modem detects the DTR off-to-on transition, it goes off-hook, dials the remote modem, and waits for the connection to occur. If, after a certain programmed period (in units of number of rings), the connection fails to materialize, the modem goes on-hook and terminates the connection. If the connection does occur (that is, the remote end answers), the modem turns on the carrier, exchanges a training sequence, and reaches a ready state. These events are indicated by the modem turning on the Data Set Ready (DSR), Data Carrier Detect (DCD), and Clear-to-Send (CTS) signals, in that order.

The answering modem waits for an incoming call and answers it, if the local router has set the DTR signal high. Here again, the modem turns on DSR, DCD, and CTS signals to indicate call connection, carrier detect, and ready state.

Call Disconnection and Reconnection

Call disconnection can occur because of telephone line failure, because one of the routers was turned off or was taken down, or because of a power failure. Each modem detects the call disconnection by the absence of the carrier. Following this detection, the modem disconnects the call and turns off the DSR, DCD, and CTS signals.

The modem signals DSR, DCD, and CTS are tracked by the router, and the router, in turn, turns off the DTR when any of these signals are off. The router keeps the DTR low for a few seconds to allow the modem to complete the actions needed for terminating the call, and raises the DTR to trigger redialing. When the modem detects the DTR off-to-on transition, it goes through the procedure for reconnection; on successful reconnection, the modem raises the

DSR, DCD, and CTS signals. Should the reconnection attempt fail, the modem resets any signals it might have raised during the reconnection.

Even when the reconnection attempt fails, the router has the DTR on for approximately two minutes before taking it down. This delay spaces the reattempts to connect two minutes apart, preventing excessive telephone traffic. If the connection does occur, the DTR remains on indefinitely, and the dialed connection then simulates a permanent connection.

The router actions remain the same, whether the router is connected to a calling modem or an answering modem. Hence, the router code is unaware of the asymmetry in the dialed connection.

Note that although the preceding description is based on the experience gained from using Hayes* smart modems, it is valid for a wide variety of compatible modems.

Modem Requirements

Following are the dial-up synchronous modem requirements:

- The modem should hold the configuration for the autodial of stored numbers in nonvolatile memory. The configuration for the modem is programmed offline using an asynchronous terminal in asynchronous mode.
- The modem should dial the stored number when the DTR off-to-on transition occurs, connect to the remote modem, and switch to the synchronous mode. The modem should terminate the connection if the DTR is turned off by the router.
- Both modems should be programmed to establish the connection at the user-defined rate rather than at the asynchronous speed used to program the modem.
- The answering modem should be programmed to answer the call only if the DTR is turned on. Therefore, even if the modem is turned on, if the router has not turned on the DTR (indicating its readiness), the modem should ignore the call.
- After the modems are programmed, both modems should be disabled from recognizing synchronous data as modem control commands. This is done by forcing the modem into dumb mode.

Modem Programming Example

The following example illustrates the programming needed to set the Hayes ULTRA* 14,400-bps modem for dialed synchronous operation. To do this, connect the modem to a terminal device or PC with a terminal emulation program. The router provides a method of addressing the modem through the CPECFG program (refer to "Configuring Modems and DTR-Controlled Devices" on page 87 for information about using CPECFG).

Dip Switch Setting

The left dip switch (*sw 1* , seen when the front cover is removed) has the following settings:

- UP—Puts the modem in smart mode (command recognition mode is enabled)
- DOWN—Puts the modem in dumb mode (characters are treated as data, not commands)

This switch is set to DOWN after the modem is configured for autodial/ autoanswer. This prevents the synchronous data from accidentally being interpreted as commands (for example, when the DTR is turned off).

Modem Script for Call Originating Modem

```
AT&F; &F - Recall Factory settings
AT&Z0=&lt;dest tel no>; &Z0 - store no to be called
AT&Q2&C1&D2; &Q2 - Stored No redial on DTR OFF -> ON
; &C1 - Track status of DCD
; &D2 - Track DTR, DTR ON -> OFF go to cmd state
ATS37=11 S37=11 - Connect to remote modem at 14400bps speed
ATE0Q1&Y0&W0 E0 - Disable character echoing
; Q1 - DO not return result codes
; &Y0 - Select profile ‘0’ as power on config
; &W0 - store as profile ‘0’
```

Modem Script for Call Answering Modem

```
AT&F; &F - Recall Factory settings
AT&Q1&C1&D2S0=2; &Q1 - Sync mode 1 (async to sync on connect)
; &C1 - Track status of DCD (don’t ignore)
```

```
; &D2 - Monitor DTR, DTR ON -> OFF enter cmd state
Call automatically answered only if DTR is ON
; S0=2 Auto Answer after 2 rings
ATS37=11; S37=11 - Connect to remote modem at 14400bps speed
ATE0Q1&Y0&W0; E0 - Disable character echoing
; Q1 - DO not return result codes
; &Y0 - Select profile '0' as power on config
; &W0 - store as profile '0'
```

Reprogramming the Modem

Should the need arise to reprogram the modem (for example, to change the destination telephone number), the following procedure should be adopted. Because character echoing and result code returns have been disabled, the modem does not respond to a user's attempt to communicate with it (in asynchronous mode). To reprogram the modem, complete the following steps:

1. Turn off the modem.
2. Set dip switch 1 to the UP (smart mode) position.
3. Turn on the modem.
4. Enter the following modem command:

   ```
   ATE1Q0; E1 - Enable character echoing
   ; Q0 - Enable returning of result codes
   ```

Modem Description Files

Novell's most recent products, and those in development, are designed to be *modem independent*. This enables new modems to be supported by these Novell products without a new version of the software being released. All that is required is to load the appropriate modem description file onto the specified system.

Novell products can interpret modem description files and execute script commands in the files to perform modem operations as the application requires. Neither the modem control components nor the software products themselves are specific to any one modem or set of modems. Any details specific to modems are contained in the modem description files.

When Novell products are installed, modem description files are copied along with other product files. As users configure the software, they identify the

modems to be used from lists of modem names. Any modem that has a modem description is presented in these lists for the user to select.

When a port is configured from the Network Interfaces screen of the Novell Internet Access Server Configuration utility (NIASCFG), the type of modem attached to the port is specified in the Modem/DCE Device field. This option enables you to select a modem initialization script that is specified in the compiled NIASCERT.MDC, NIASMDM1.MDC, and NIASMDM2.MDC files in the SYS:SYSTEM directory.

Because these files are compiled, they require a special modem script editing tool, WMDMMGR, to read them and make changes to them. Multiple *.MDC (Modem Definition Compiled) files can exist in SYS:SYSTEM; however, if a description of a particular type of modem appears in multiple *.MDC files, there is no guarantee as to which description is used. To avoid confusion, a modem description should appear in only one *.MDC file. When Novell Internet Access Server 4.1 is installed, any previously installed *.MDC files are moved to the SYS:SYSTEM\BACKUP directory. Only files included in Novell Internet Access Server 4.1 remain in the SYS:SYSTEM directory.

If you create new modem description files, copy them to the SYS:SYSTEM directory so that they are available to the routing software. If the routing software is running, issue the REINITIALIZE SYSTEM command to have the modem script changes take effect

This section discusses the format and content of the information present in the modem description files. The method of defining the capabilities of a modem is specified, and the process of constructing scripts to accomplish modem operations is outlined. Several examples illustrate uses of the details presented.

Modem Description File Information

A modem description file includes information describing both a modem vendor and individual modems. The information about the modem vendor is specified first, with from one to many descriptions of modems following.

One way to organize modem descriptions is to collect information about all modems from one vendor into a single file. This makes it easy to register the single filename with Novell. Another possibility is to group modems by family, as might be done with all the *XYZ Xxxx* sample models. We suggest that all modems manufactured by a vendor be located in a small number of files.

A typical modem description file includes the following:

- Vendor description

  The vendor information begins with the vendor's name, which identifies the company creating the description file. A copyright notice can be included to protect the company's rights. Version information should be added to allow tracking of additions or corrections to description information.

- Modem description
  - Modem name

    Modem-specific information begins with a line specifying the modem name. This name must be unique within the entire set of modem names known to Novell and should include some form of the vendor's name to avoid conflicting with any other vendor's descriptions.

  - Modem options

    Modem option lines supply information regarding the features, capabilities, and default values of the modem. This information is needed by the modem control components to determine which logical operations can be performed. The information would include the highest interface bit rate possible for the modem, the link types the modem can use (analog, ISDN, and so on), and whether the modem supports a fixed rate.

  - Modem scripts

    Modem scripts that perform particular operations are specified. These scripts are simply strings encoding suboperations to be executed that together accomplish the desired operation. Multiple sequences of commands can be combined, if required.

  - Modem responses

    The final section of a modem description file contains the strings used to decode a modem's responses when the modem answers an incoming call. For example, the string returned by a modem when a call is successful might be associated with the CONNECT response. Additional response recognition allows modem control components to record the options that are negotiated for this call.

Modem Description File Components

This section describes the components that can be used in modem description files.

Vendor Description

The following fields are part of the vendor description:

- **MANUFACTURER** : A descriptive name of the modem vendor.
- **COPYRIGHT** : A vendor's copyright notice.
- **VERSION** : A version number of the modem descriptions.

The manufacturer and copyright string values can be up to 80 characters long. The version numbers can have numeric values from 0 to 99. Currently, the values are not used directly by modem control components, but they are provided for use by modem vendors.

Modem Description

This section explains the modem keywords and how to use them.

Modem Name

The modem name string value can be up to 39 characters and must be unique within the entire set of modem names known to Novell.

There can be multiple descriptions for the same modem, with each appropriate for distinct circumstances. For instance, it might be found that most revisions of a particular modem can be initialized quickly, but that some ROM levels require delays between output characters. Rather than force all users to wait for a lengthy initialization operation, it is possible to create two descriptions, as follows:

```
XYZ Modem Xxxx

XYZ Modem Xxxx (Slow Init)
```

Rate Options

The following rate options require values to be defined:

- **DEFAULT** : Best typical bit rate used to communicate with the modem.

  When a modem operation specifies the use of fixed rate mode, the **FIXED** rate option supplies the bit rate used to communicate with the modem.

When that mode is not selected, modem control uses this option to determine the default bit rate for the interface to the modem.

- **FIXED** : Best bit rate for use with fixed rate usage.

  Modems can be initialized to use one unchanging bit rate between themselves and the data terminal equipment (DTE). This bit rate is usually set to a value high enough to permit use of compression, no matter what line speed is used on a connection. The numeric value is the bit rate to be used when the modem is put into fixed rate mode.

  NOTE: This option also implies that fixed rates are supported by the modem.

- **SINGLE FIXED RATE** : Modem can use only one bit rate.

  Some modems permit the use of the FIXED DTE RATE feature, but with only one allowable bit rate, as specified by the FIXED option. This option specifies that this restriction is true for this modem.

- **MAXIMUM** : Maximum bit rate used to communicate with the modem.

  The set of interface bit rates that can be used to communicate from the DTE to a modem usually has an upper bound. This option supplies the maximum interface bit rate to be used with a modem. The numeric value for this option is the maximum rate in bits per second.

Other Options

Depending on how your modem is being used, two of the following options might have to be configured. The first two of the following options are configurable; the last two options are not configurable. These options are described as follows:

- **OUTPUT DELAY** : Delay between command characters.

  Some modems require a greater amount of time to process complex commands. Complex commands that are sent to these modems one character at a time are successful. This option enables you to specify the amount of time to insert between characters of selected commands.

  The numeric value is the time, in tenths of a second, that modem control should wait between sending characters. There are two script operations for output: one inserts delays between characters; the other does not insert delays between characters. If this option is not specified, the default delay is zero (no delay).

- **LINK TYPE** : Connection method used by the modem to establish a link.

  Possible values are as follows:

- **ANALOG** for asynchronous modems
- **ISDN-Synchronous** for ISDN adapters
- **ISDN-Asynchronous** for ISDN terminal adapters
- **X.25** for X.25 connection types such as AIOPAD
- **TCP** for TCP/IP connection types such as AIOPPTP

- **VERSION** : Version of this modem script entry.
- **NOVELL CERTIFIED** : Indication that this modem script has been certified by Novell Labs.

Modem Scripts (Control Strings)

Modem scripts are text strings that are sent to the modem to cause a particular behavior. They are associated with a particular modem capability and are transmitted to the modem when the application software wants to invoke that operation.

More information on the content and creation of modem scripts is given later in "Login Script Operation" on page 89 Individual scripts are summarized here:

- **ERROR CORRECTION** : Enable error control protocols.

  This script enables the use of any of the error correcting protocols implemented by a modem when the next data connection is begun. Because which protocols might be activated depends on the remote modem, this script only specifies that the best possible protocol for each connection be used. Through monitoring the negotiation progress responses, the modem control components can be informed of the characteristics of the protocol activated.

- **AUTO ANSWER** : Place modem into autoanswer mode.

  This script places the modem in the mode of automatically answering incoming telephone calls. A connection can begin without intervention by modem control. Modem control monitors the progress of connection initiation and detects when the connection is complete and data transfer can begin.

- **COMPRESSION** : Enable data compression method.

  This script enables the use of any of the data compression methods implemented by the modem when the next data connection is begun. Because the particular compression method employed depends partly on

the remote modem, this script specifies only the preferred method to be used. Through monitoring the negotiation progress responses, the modem control components can be informed of the characteristics of the method activated.

- **DIAL** : Make an outgoing call.

  This script is executed when a call origination operation is requested on a switched line. The operation request parameters include whether the dialing should use pulse or touch-tone signaling, and the destination telephone number. These parameters are inserted into the dial script string using the substitution tags **[T]** and **[P]**. These tags are described in detail in "Login Script Operation."

- **FIXED DTE RATE** : Place modem into fixed interface bit rate mode.

  This script places the modem into fixed interface bit rate mode. This allows the interface to be programmed to one bit rate that can be used for all subsequent connections. The actual rate used is determined by the associated **FIXED** rate value and **SINGLE FIXED RATE** rate flag.

- **HANGUP** : Disconnect any call in progress.

  This script causes the modem to disconnect any call that might be in progress (that is, place the modem on-hook). This script should specify all required operations that ensure that the call is disconnected, irrespective of the current modem state.

- **ESCAPE** : First string sent to the modem to initiate a hangup.

  This string is part of the overall **HANGUP** script for the modem. To change only the **ESCAPE** output string, you can type directly into the edit box. To modify the overall **HANGUP** script and sequence, select the HANGUP button.

- **FLOW CONTROL** : Place modem into hardware flow-controlled mode.

  This script places the modem into a hardware flow-controlled mode. In this mode, data transfer between modem and interface is controlled through the use of the Request-to-Send (RTS) and Clear-to-Send (CTS) RS-232 signals. Each signal controls data transfer in one direction.

- **RESET** : String send to the modem to reset it.

  This string is part of the overall **INIT** script for the modem. To change only the **RESET** output string, you can type directly into the edit box. To modify the overall initialization script and sequence, select the INIT button.

- **INIT** : Initialize the modem to a known state.

  This script causes the modem to be initialized to a known state. This state must have all optional features disabled. That is, the purpose of the **INIT** script is to put the modem into a state in which any of the other features can then be added by individually executing scripts.

  The **INIT** script is usually the first script executed when a modem operation is begun; the only script that could precede it is the **HANGUP** script to disconnect a call in progress. The **INIT** script can make no assumptions about the previous state of the modem. Indeed, the previous user of a modem might not have been Novell's modem control; therefore, not even modem control knows the state of a modem.

  The script must reset everything that can be affected by modem commands. This includes features like echo, call progress, result code, modem signal usage, flow control modes, and so forth. The script must set the correct modes so that modem response strings can be recognized.

- **LEASED INIT** : Place modem into leased-line mode.

  When a modem initialization operation is requested and the leased-line feature is requested, this script is executed to place the modem into leased-line mode. In some cases, this feature is not under control by commands, but rather, some switches must be set. In this case, the script might be absent.

- **LEASED ANSWER** : Accept a leased-line connection.

  This script is executed when a call answer operation is requested on a leased line. The modem should attempt to connect to the remote modem using answering frequencies. Once this script is completed, modem control monitors the local modem's responses to detect when a connection has begun.

- **LEASED DIAL** : Originate a leased-line connection.

  This script is executed when call origination is requested on a leased line. The modem should attempt to connect to the remote modem using origination frequencies. Once this script is completed, modem control monitors the local modem's responses to detect when a connection has begun.

- **MANUAL ANSWER** : Accept manually answered switched connection.

  This script is executed when a manual call answer operation is requested. The modem should attempt to connect to the remote modem using answering frequencies. Once this script is completed, modem control

monitors the local modem's responses to detect when a connection has begun.

- **`MANUAL DIAL`** : Originate manually dialed switched connection.

  This script is executed when manual call origination is requested. The modem should attempt to connect to the remote modem using origination frequencies. Once this script is completed, modem control monitors the local modem's responses to detect when a connection has begun.

- **`SYNCHRONOUS`** : Initialize modem for a synchronous connection.

  This script is executed when a modem is initialized for a synchronous connection. Certain modems allow synchronous mode connections, especially when trying to connect to mainframes and UNIX-based systems.

Script Operations

A modem script contains a sequence of nano-operations that inform modem control about which actions to perform. These actions include output of ASCII characters, controlling interface signals, checking for expected input, and so forth. There is no facility for conditional execution of nano-operations; the entire script is executed unless an error occurs.

Each nano-operation consists of an alphabetic character optionally followed by parameters for that operation. These values can be string or time values, or other modifiers for that basic operation.

Following are the operations summaries:

- Toggle Break— Control asynchronous break signal

  This operation turns on the asynchronous break signal momentarily. Toggling the break signal can be used to switch a modem into command mode.

  The break operation can be qualified by a decimal number giving the length of time, in tenths of a second, for which break is to be turned on. If a time value is not given, the default break of 0.5 second is used.

- Toggle DTR— Control the DTR signal

  This operation controls the DTR signal to the modem. The DTR signal is turned off momentarily and then turned on again. Turning off this signal can be used to switch a modem out of data transfer mode.

An optional parameter, *TIME* is the duration, in tenths of a second, for the DTR signal to be turned off.

If a time value is not given, the default DTR off time of 0.5 second is used.

- Flush Buffers— Flush Transmit/Receive buffers

  Characters that have been buffered for output or input but not yet processed can be discarded by this operation. This might be useful when modem responses, up to a point, can safely be ignored, or if prior output should be discarded when new commands are entered.

  The flush operation must specify which streams should be flushed.

- Input String—Wait for input (must match) or conditional input (optional match)

  This operation allows a script to check for a specific string to be received from a modem. For example, after most modem commands, a script should check for the returned indication of success, usually OK. There are two variants: *must match* or *optional match*.

  The operation can optionally be qualified by a decimal number specifying the maximum time to wait for this response. This value is specified in tenths of a second. If it is not given, the default value of 5 seconds is used.

  Modem control continues receiving characters from the modem until one of two occurrences. If a matching string from the modem is completed, the nano-operation finishes and the script continues. If a match is not completed and the timeout period has elapsed since the last character was received from the modem, an input timeout is declared.

  If this was a must match input string operation, the timeout causes the script to be terminated with a bad modem response error code. Otherwise, the timeout simply terminates the optional match operation and continues with the rest of the script.

- Output String—Output or output with delay

  This operation allows output of character strings from the script to a modem. The output string can contain any non-null, noncontrol ASCII characters.

  If a delay must be inserted between characters, the Output with Delay operation uses the delay time specified by the **`OUTPUT DELAY`** option value.

  The string to be output is bounded by a delimiter character chosen by the script creator. The script creator should choose a string delimiter

character that is not used for any interactions with the modem. This character should not be an alphanumeric character because this would make reading descriptions difficult. A survey of several modems has identified the many punctuation characters that are used within modem commands and responses. The following set of characters is recommended for use:

```
` < ^ _ { } | : ' ,
```

By convention, a colon (:) is used.

Control characters can be inserted into output strings using the back-quote character (**`**).

Variable strings can be substituted in output or input strings with the use of a substitution marker. A substitution is indicated by a substitution tag name surrounded by brackets ([ ]). For example, the substitution of the tone or pulse modifier and the phone number in a dial-out command might be coded as follows:

```
ATD[T][N]
```

where **[T]** is replaced with **T** or **P** , and **[N]** is replaced with a dial number.

Only a limited number of substitution tags are defined, and the substituted strings are not variable by modem type. The predefined tags are as follows:

- **T** : dial tone/pulse modifiers: **T** or **P**
- **N** : dial phone number: supplied by application
- **R** : ring count: used on initialization
- **W** : seconds to wait for a connection

Care should be taken that the longest command sent to a modem does not exceed what the modem can handle. Many modems are limited to a maximum of 40 command characters, excluding the leading **AT** , spaces, hyphens, and final carriage return. The input command can be used to break up long command-output sequences.

- Pause— Pause script execution

  This operation allows a script to pause execution for a period of time. This is useful when modems might require additional time to complete complicated modem commands.

An optional parameter, *TIME* is the pause time in tenths of a second. If a time value is not given, the default time value of 1 second is used (time = 10).

- Quiet Wait— Wait for end of input

  This operation skips all the responses from a previous command before issuing a new command. It causes a wait until the modem remains continuously quiet for the specified time.

  An optional parameter, *TIME* is the pause time in tenths of a second. If a time value is not given, the default time value of 1 second is used (time = 10).

  This nano-operation discards any data received from the modem. Whenever a character is received, the elapsed time timer is reset to 0. When the elapsed time timer reaches the specified wait time value, the nano-operation completes successfully. An additional timer records the total time since the nano-operation began. If this timer reaches the sum of the specified wait time plus 5 seconds, a timeout is declared and the nano-operation completes unsuccessfully, causing the script to be terminated with an error.

- Change Data Rate— Set new interface rate

  This operation allows scripts to change the data rate used to communicate with the modem. This is used with modems that do not automatically resynchronize interface data rates after switching back to command mode from data transfer mode.

  After execution of this operation, any further output or input through the interface uses this data rate. Some asynchronous equipment must flush one or both of the input and output streams when changing data rates.

Modem Responses

The response strings in a modem description allow recognition and interpretation of data sent from the modem to the DTE. Response strings inform the modem control software of the success or failure of a command. These strings also let modem control detect when a call is arriving.

As the responses generated differ between modems, the modem vendor must supply information to allow modem control to recognize responses. Response strings contain from one to many pairs of substrings, the first giving the input string to be recognized and the second representing the standard meaning of the string.

With the ever more complex responses found in newer modems, it is sometimes necessary to perform multistage matching of response strings. An example would be when the modem is using negotiation progress monitoring to capture added information about connections. When the **PROTOCOL** response is received, the first stage of recognition would identify the input as the **PROTOCOL** message. The second stage of recognition would then identify the particular substrings that might be present in this message. This progression from one stage to the next is called chaining.

Modem control accumulates ASCII characters received from a modem until a carriage return character (**\x0D** or decimal **13**) is received; all other control characters are ignored. The accumulated string is then compared to the match strings in the **RESPONSES** keyword string. When a match is found, the meaning is interpreted and the appropriate action is taken.

Modem Response Strings

Modem response strings can comprise two string elements: the *match string* and the *meanings string* .

- Match string

  The first of each pair of strings in the **RESPONSES** string is known as the *match string*. When modem control is monitoring modem responses, characters received from a modem are collected until a carriage return is received. The input string is then compared against all the match strings found in Modem Responses. This matching operation is case-insensitive and proceeds in the same order in which the string occurred in the description file.

  Match strings do not need to be the entire response string to declare a match. Only the initial characters of a response must match the match string. Thus, the match string **ERR** matches both the response strings **ERROR** and **ERRONEOUS** , but not **ERASE**. However, this might make the order in which match strings are tried even more important.

- Meanings string

  The second string of each pair of strings is known as the *meanings string*. The interpretation of this string defines what the recognized response means to modem control. This includes whether the response is a success, a failure, or some intermediate indication. When certain optional connection features are recognized, they can be signaled to modem control by this method. Finally, this is the way that bit rates are given to modem control.

There are four types of meanings information, as shown in Table 6 : status, rate, feature, and match chaining. The status and feature values are decimal indices into tables used by modem control. The rate decimal value is the actual data rate in bits per second. The match chaining value is described in “Match Chaining” on page 110

Table 6 Meanings String Types

Type	Meaning
STATUS	Reports a status; might terminate scanning.
RATE	Reports a data rate.
FEATURE	Reports an enabled feature for this connection.
CHAINING	Continues scanning using another string.

Status Meaning

Status information is used to notify modem control when something of significance has been discovered in a response, or to report that scanning should continue. Possible status types are as follows:

NONE	CONNECT
RESERVED 1	BUSY
RESERVED 2	NO_ANSWER
RESERVED 3	NO_CARRIER
RESERVED 4	ERROR
RESERVED 5	NO_DIALTONE
OK	VOICE
RING	UNKNOWN
RRING	

Rate Meaning

The rate meaning tells modem control what the current line data rate is in bits per second. For most modems that implement negotiation progress messages, this rate value can be captured from the **CARRIER** response by using the **<R>** construct, as in **CARRIER <R>** or **CONNECT <R>**. This construct matches any speed response from the modem and captures that value to return it in the rate definition command.

Feature Meaning

The feature values indicate to modem control when optional connection features have been enabled on the current connection. Information about which features are enabled or disabled is made available to applications. Applications can use this information to determine whether they must independently perform error control or data compression for a connection. The features are as follows:.

NONE	V.42BIS
ERROR_CONTROL	UNBALANCED
MNP5	SYNCHRONOUS

Match Chaining

The match chaining directs modem control to continue matching using the remainder of the input string (after the initially matched portion) and using a different modem response string. This permits the multistage matching that is so useful with complex sets of responses, such as negotiation progress messages. The following example illustrates this approach:

```
RESPONSE = PROTOCOL

RESPONSES STRING 1 = ERROR-CONTROL

Input from modem: PROTOCOL: ERROR-CONTROL/LAP-B
```

The first string is part of the first stage matching string formed from all the **RESPONSES** keyword strings. Modem control interprets it to mean that the response beginning with **PROTOCOL** is not a final response; rather, that additional matching must be performed using **RESPONSES STRING 1**.

Modem control begins checking the remainder of the input string repeatedly against the **RESPONSES STRING 1** match strings. Each time the match strings are used up, modem control advances to the next character in the input

string and tries again. This process continues until all the characters in the input string have been exhausted. In this manner, modem control finds the **ERROR-CONTROL** substring and notes that feature one, **ERROR CONTROL**, is enabled for this connection.

Environments

Novell's modem control is implemented in multiple environments. This section briefly describes how modem description files are used in each environment.

Modem description files on a NetWare server are placed in a subdirectory accessible to NetWare Loadable Module™ (NLM™) files. The files for both the routing and the remote access components of Novell Internet Access Server 4.1 are located in the SYS:SYSTEM directory. You should work in this directory when adding new scripts, editing existing scripts, and compiling scripts. Novell Internet Access Server 4.1 uses all compiled scripts with the .MDC extension that exist in the SYS:SYSTEM directory.

Novell Internet Access Server 4.1 Remote Access Software

The modem control components of the remote access software exist in a subdirectory called SYS:SYSTEM. All files containing compiled modem descriptions are copied to this subdirectory. When NetWare Asynchronous I/O (AIO) is loaded, it searches this subdirectory for files with the extension .MDC. AIO then creates a list of all modem names defined in these files and indicates which file contains the description for each modem. When one of the remote access services attempts a modem operation on a port, AIO determines which modem is attached to that port and ensures that the modem's description has been read into memory. AIO then starts the execution of the operation using the service's request parameters and the modem description.

The standard set of scripts that are included in the remote access software are contained in the following three files:

- SYS:SYSTEM\NIASCERT.MDC (scripts certified by Novell Labs)
- SYS:SYSTEM\NIASMDM1.MDC and NIASMDM2.MDC (scripts for commonly used modems)

Novell Internet Access Server 4.1 Routing Software

The routing software uses modem definition files that are placed in the SYS:SYSTEM directory. It interprets these files as required for modem

control. The standard set of scripts that are included in the routing software are contained in the following three files:

- SYS:SYSTEM\NIASCERT.MDC (scripts certified by Novell Labs)
- SYS:SYSTEM\NIASMDM1.MDC and NIASMDM2.MDC (scripts for commonly used modems)

4 Optimizing

Although many optimization techniques can be used on a LAN or WAN, optimization is less an issue for a LAN because bandwidth is inexpensive. On a WAN, performance optimization is critical because WAN media use slower transmission speeds than LAN media.

Because the potential for performance improvement is greater for a WAN than for a LAN, this section focuses on techniques that you can use to optimize the performance of your PPP links.

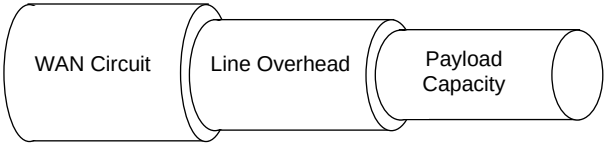
Overview of WAN Optimization

Although LAN performance is measured in packets per second, WAN performance is more accurately measured by the amount of throughput on a link. To optimize performance on a WAN, you must optimize the WAN circuit.

As shown in Figure 6 , WAN circuits are made up of two components:

- Payload capacity
- Line overhead

Figure 6 WAN Pipe



This topic contains the following sections:

- Payload Capacity
- Line Overhead
- Network Optimization Tools

Payload Capacity

Payload capacity is the speed at which data moves through a circuit. If your network is very large (over 4000 network segments and services) and uses only the Internetwork Packet Exchange™ (IPX™) protocol and T1 (1.544-Mbps) connections, maximizing payload capacity can increase network performance significantly.

Because very large networks have minimal line overhead—for example, less than 5 percent of network capacity is associated with in-band maintenance traffic—decreasing line overhead does not significantly increase bandwidth. However, you can overcome transport protocol inefficiencies and increase capacity of a circuit by using data compression.

NOTE: If the link is not already fully using the line speed, adding data compression produces minimal performance improvement.

Line Overhead

Line overhead contains the media's framing, routing protocol, and Network-layer protocol overhead. Line overhead is similar to an envelope in that it restricts the capacity of the system. To increase a circuit's capacity, you must minimize line overhead.

Reducing line overhead in a multiprotocol environment is critical because it increases circuit capacity for all protocols, not only the protocol being optimized. For example, reducing Service Advertising Protocol (SAP) traffic increases the available bandwidth for IPX, IP, and AppleTalk clients.

If your network is large (1000 network segments and services) and consists of small sites and branch offices connected by 64-Kbps or slower circuits, your line overhead can be at 25 percent or more of circuit capacity. In this case, reducing line overhead is critical. Without optimization of line overhead, circuits are saturated and payload optimization produces only minimal improvement.

Network Optimization Tools

By optimizing both the line overhead and the payload capacity, you can dramatically improve network throughput and transmit more user data over

WAN connections. Novell® Internet Access Server 4.1 routing software provides several optimization tools.

For payload optimization, consider using the following:

- PPP data compression
- Packet Burst™ protocol and Large Internet Packet (LIP) protocol

For line optimization, consider using the following:

- Header compression
- RIP and SAP filtering
- Link state routing (NetWare® Link Services Protocol™ [NLSP™] software and OSPF protocol)
- AURP tunneling

General PPP WAN Connection Optimization Techniques

Although some optimization techniques are best suited for either permanent or on-demand connections, the following techniques are applicable to either type:

- PPP data compression
- PPP header compression
- Packet Burst and LIP
- Diminishing Traffic

This topic contains the following sections:

- Understanding Data Compression and Header Compression
- Packet Burst and LIP Protocol
- Bandwidth/Benefit Ratios of Data Compression and Packet Burst
- Diminishing Traffic over a Slow Link

Understanding Data Compression and Header Compression

Novell Internet Access Server 4.1 routing software provides two types of compression: PPP data compression and PPP header compression.

PPP data compression allows data to be transmitted in a more compact form. Enabling data compression reduces the amount of data transferred over a

communications link by replacing previously observed data sequences with more compact sequences. This data compression causes the apparent speed (bandwidth) of the link to increase—at the cost of some additional router CPU overload—and allows for a more effective use of a PPP link when packets are being routed between remote LANs.

Header compression allows fields in the header of each data packet to be compressed and is used to reduce Data-Link-layer or Network-layer header overhead. Data-link header compression reduces the size of a header at the Data-Link layer. Network-layer header compression, available for the IPX and TCP/IP protocols, reduces the size of the header at the Network layer. Although enabling header compression reduces network overhead, PPP data compression provides much greater performance improvement.

NOTE: PPP header compression and PPP data compression cannot be enabled at the same time. Because data compression provides greater performance improvement than header compression, use data compression when you are connecting NetWare Link/PPP™ systems.

PPP Data Compression

Novell Internet Access Server 4.1 uses software-based data compression based on the STAC LZS and Novell's Pattern Predictor algorithm that enables you to compress data over a wide range of interface speeds from 1200 bps to T1/E1.

Although data compression provides some benefit at speeds up to E1, the performance improvement is greater on links with speeds of 56 Kbps or less. The reason is that as link speed increases, the percentage of throughput improvement decreases as a result of the additional CPU execution time required in the compression process.

Transmitting data in a more compact form provides several benefits. Because it reduces the amount of data transferred over a communications link, data compression increases the apparent speed (bandwidth) of the link, at the cost of some additional router CPU overload. Data compression also enables more effective use of a PPP link when packets are routed between remote LANs.

NOTE: When data compression is enabled, it is used only if both the local and remote peers support a common compression technique for the link speed.

NetWare Link/PPP data compression works best when a constant supply of transmitted data is available at the interface. This constant supply of data maximizes the replacement of data sequences with more compact sequences.

Therefore, when using IPX with NetWare Link/PPP data compression, you need to also use the IPX Packet Burst protocol and the LIP protocol.

You can optimize the performance of the link by configuring the parameters in the Timeouts and Retries window. The default PPP configuration parameter values conform to the values recommended by the Internet PPP specification; it should not be necessary to change them.

The default timeout and retry values are appropriate for most dedicated and switched circuits. If you are using satellite circuits that introduce significant increases in propagation delay, you might need to increase the LAPB timeout values to enable the data links to operate properly. LAPB retry parameters control data-link error detection and recovery.

The default LAPB T1 (LAPB T1 Ack Timeout) and T4 (LAPB T4 Idle Link Timeout) parameter values of Automatic make NetWare Link/PPP calculate the appropriate T1 and T4 timeouts based on the interface speed and the Maximum Transmission Unit (MTU) size, as follows:

T1 ms = T4 ms = MTU x 8 x 1000/interface speed + overhead

If the line speed is greater than 56K, the overhead equals 1750 ms; otherwise, the overhead equals 3000 ms.

PPP echo request generation enables you to detect a remote peer that is no longer responding. When PPP data compression is working, the LAPB T1 timeout provides a similar service. Although you can disable PPP echo request generation when data compression is working, the benefits are minor.

To configure interface timeout and retry parameters, load NIASCFG and follow this path:

Select Configure NIAS > Routing and Protocols > Network Interfaces > PPP Network Interface > Timeouts and Retries

The PPP Timeouts and Retries window is displayed, from which you can configure the following parameters:

- Echo Requests—Enables or disables generation of PPP echo requests on a periodic basis. LCP echo requests provide a way to detect a failing remote PPP peer, along with loopback links and other Data-Link-layer anomalies.

  Note that responses to received LCP echo requests are always generated, regardless of the state of this option. Disable this option for a busy link.

- Echo Retries—Specifies the maximum number of times the data link retransmits an LCP echo request before it determines that the link is bad. Increase the value if the link is congested.
- Echo Timeout—Specifies the maximum number of seconds the data link waits for a peer to respond to an LCP echo request. Increase the value if the link is congested.
- LAPB T1 Ack Timeout—Specifies the maximum number of seconds that this LAPB interface waits to receive an acknowledgment for a previously transmitted information frame. Expiration of this timer causes the LAPB interface to retransmit the information frame. If the frame is retransmitted for LAPB N2 times without an acknowledgment, the interface is declared *down* and the link is disconnected.

  Set this value high for a delayed link or set it low for a noisy link.
- LAPB T4 Idle Link Timeout—Specifies the maximum number of seconds this LAPB interface can remain idle (without send or receive exchanges) before an RR (Receiver Ready) or RNR (Receiver Not Ready) supervisory frame is sent to the remote LAPB peer.

Press Esc until you return to the main NIASCFG menu; save your changes when prompted.

If you want these changes to take effect immediately, exit NIASCFG, then bring down and restart the router. If you want to configure other parameters, do so now and restart the router when you are finished.

NOTE: Refer to the online help for information about the following available timeout and retry parameters: Request Retries, NAK Retries, Terminate Retries, Response Timeout, and LAPB N2 Retransmissions.

For information about configuring PPP data compression, see "Configuring Data or Header Compression."

Network-Layer Header Compression

Except for TCP/IP, Network-layer header compression supports all WAN media, including PPP, X.25, frame relay, and SNA. TCP/IP compression supports PPP only. Header compression is best for line speeds of 64 Kbps or less. As link speed increases, the percentage of throughput improvement decreases because the compression process requires additional CPU execution time.

There are two common Network-layer header compression algorithms: Van Jacobson IP Header Compression for the TCP/IP protocol, and compressed IPX for the IPX protocol.

TCP/IP Header Compression

Van Jacobson published *Compressing TCP/IP Headers for Low-Speed Serial Links* as a Request for Comment (RFC) 1144. This method of header compression reduces the TCP/IP header from 40 bytes to between 3 and 5 bytes. TCP/IP compression supports only PPP.

User Datagram Protocol (UDP) and other IP traffic cannot take advantage of Van Jacobson compression because the protocol does not specify a method to compress only the IP header.

For information about configuring TCP/IP header compression, see "Configuring Data or Header Compression."

IPX Header Compression

Telebit* Corporation extended the Van Jacobson algorithm to the IPX protocol. They published RFC 1533—*Compressing Headers over WAN Media*. This specification shows how to compress any IPX header. It also enables you to (optionally) compress the transport header of NetWare Core Protocol™ (NCP™) type 2222 (NCP Request) and type 3333 (NCP Reply) packets.

IPX header compression reduces the header from 30 bytes to 1 byte in the best case, or to 7 bytes in the worst case. NCP header compression reduces IPX and NCP overhead from 36 bytes to 2 bytes in the best case, or to 8 bytes in the worst case.

For information about configuring IPX header compression, see "Configuring Data or Header Compression."

Data-Link Layer Header Compression

Data-link header compression is available only for PPP because leased or switched lines used for PPP connections do not manipulate PPP packets. For header compression to be effective on X.25 and frame relay, all intermediate switches must also implement header compression. This implementation requires changes in a service provider's infrastructure on a regional, national, and global basis.

With header compression, PPP has the option of eliminating the leading byte of the protocol field in the header when it is not used, thereby reducing this field from 2 bytes to 1. The PPP specification also allows the address and control fields of the Data-Link layer to be eliminated, because the High-level Data Link Control (HDLC) fields always contain the static values of 0xFF (all stations address) and 0x03 (unnumbered information). Eliminating these fields reduces the PPP data-link header by another 2 bytes.

NOTE: The HDLC address and control fields cannot be eliminated if you are using PPP data compression because the compression control protocol uses LAPB to provide reliable delivery of compressed data. LAPB uses both the address and control fields dynamically. In addition, the PPP protocol field is always 2 bytes for a compressed frame; therefore, it cannot be compressed either.

PPP header compression can be used on either uncompressed lines or lines with hardware data compression, such as dial-up lines with modems supporting V.42 bis or Microcom* Networking Protocol (MNP*).

For information about configuring PPP header compression, see "Configuring Data or Header Compression."

Packet Burst and LIP Protocol

The Packet Burst protocol enhances IPX by allowing larger data transactions, composed of multiple IPX packets, to be transmitted as a single burst. Acknowledgments are issued for the complete burst of packets instead of for individual IPX packets. Packet Burst can be used alone or with LIP, a combination that allows large IPX packets. For best results, you can enable Packet Burst and LIP on each client and server end node system. Although LIP and Packet Burst are included with NetWare 3.12 and NetWare 4™ servers, they can be enabled separately on the clients.

With Packet Burst and LIP, you can obtain dramatic improvements in performance over a WAN. Over a WAN, adding data compression further increases performance. Some benchmark results are included in the next section, "Bandwidth/Benefit Ratios of Data Compression and Packet Burst." Similar performance gains can also be obtained when Packet Burst and LIP are combined with other vendors' data compression solutions, such as modems and DSUs that offer data compression.

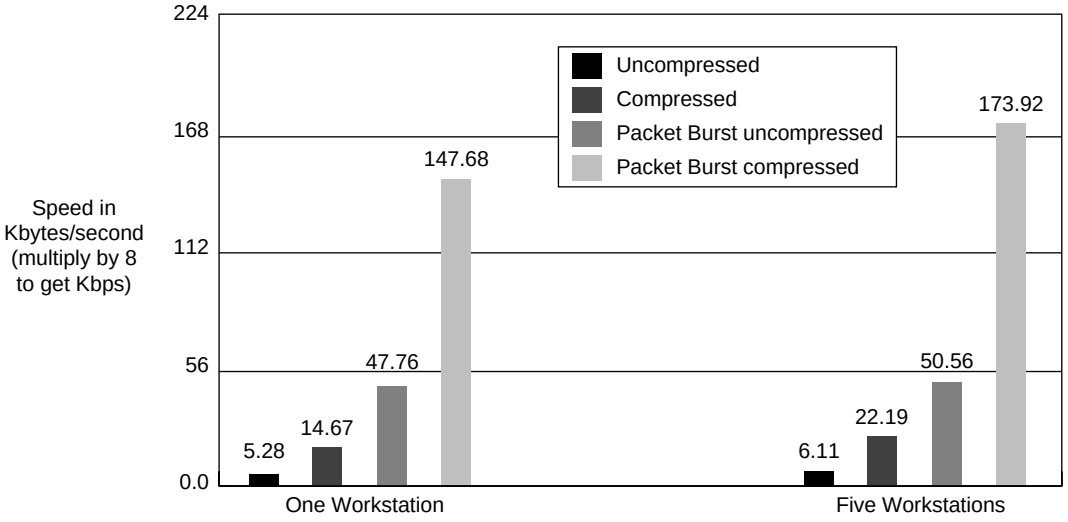
For more information about how Packet Burst and LIP work, see Packet Burst Update: BNETX vs. VLM™ Implementations in the November 1993 *NetWare Application Notes*.

Bandwidth/Benefit Ratios of Data Compression and Packet Burst

Data compression alone provides some increased performance, but you can get much better improvement by combining data compression with Packet Burst and LIP. It is now possible to drive the 56-Kbps circuit at two or three times its rated capacity.

Figure 7 shows the results of tests using Perform3™ and the following test parameter values with 486/33 clients and servers: 12, 128, 4096, 1024. The server sends 4096-byte packets for 12 seconds; 3072-byte packets for 12 seconds; 2048-byte packets for 12 seconds; and finally, 1024-byte packets for 12 seconds.

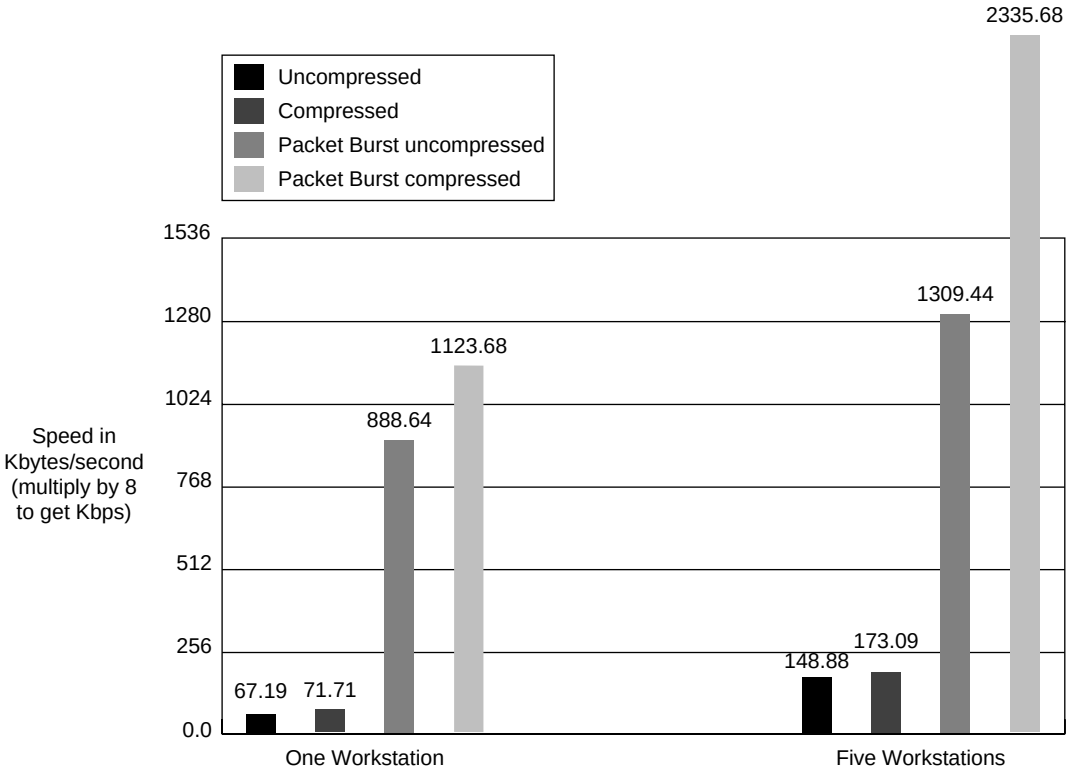
Figure 7 56-Kbps Circuit—Packet Burst and Compression versus Baseline



NOTE: These are benchmark results—performance gains with the NCP and Sequenced Packet Exchange™ (SPX™) protocols might not be the same. NCP and SPX are both sensitive to latency, and it might be that the additional processing time of compression does not offset the gains in bandwidth reduction.

Data compression used without Packet Burst provides modest results, but compression gives exponential results when coupled with Packet Burst and LIP, as shown in Figure 8.

Figure 8 T1 Circuit—Packet Burst and Compression versus Baseline



Data compression alone gives a gain of less than a 20 percent with five workstations. When given a Packet Burst stream, compression increases the result by more than 75 percent. Improvements in line efficiency with a single stream range from less than 7 percent to more than 25 percent.

Diminishing Traffic over a Slow Link

NOS utilities can be a major source of the traffic that congests an on-demand connection. These utilities include login.exe, logout.exe, map.exe, and other utilities usually found on SYS:\public.

When using a slow WAN, you can reduce WAN congestion and avoid loss of client connection if you install the most frequently used NOS utilities on the client. For example, when the login.exe is found only on the server, logging in requires from 350 to 1000 small frames. When the LOGIN.EXE file is copied to the client, logging in requires only up to 250 frames.

Optimizing Permanent and On-Demand WAN Connections

For more information about optimizing any type of permanent or on-demand WAN connection, refer to Optimizing in the *WAN Overview* documentation.

Optimizing PPP Multilink Performance

Using PPP Multilink is, in itself, an optimization of PPP connections. You may obtain additional bandwidth by increasing the member links in a PPP Multilink group. There are two ways to do this, static and bandwidth-on-demand.

If you choose static, every time a connection is made the number of member links assigned to the multilink group are used. This can be costly, but it does provide immediate bandwidth. However, you pay a price for this performance optimization in the cost of your line use. You might not be using all of the bandwidth available, thereby wasting the unused bandwidth.

Bandwidth-on-demand offers the benefit of increasing bandwidth (when needed) by activating another line in the multilink group when the utilization of the first line exceeds the value set in the Bandwidth Threshold Level.

When using bandwidth-on-demand, the server monitors the utilization of the first line connection over the period of time set in Bandwidth Measurement Time field. The default value is set at 30 seconds. If the utilization of the line exceeds the Bandwidth Threshold Level at any time during that 30 seconds, the next line in the multilink group is activated, and both lines share transfers to the PPP connection. (The splitting of packets and overhead is done at the PPP level, and the multilink connection is perceived as a single connection by network protocols such as IP or IPX.)

If a multilink group is configured for three or more lines and the average utilization of the two lines exceeds the Bandwidth Threshold Level during the next measurement period (for example, the next 30 seconds), another line would be activated.

If, however, during the subsequent measuring period, the average utilization of the active member links were to be below the Bandwidth Threshold Level, the most recently activated line would drop out of the connection.

If you decide that the increased performance is required, you have to experiment and monitor the performance of the multilink group to decide on

the bandwidth threshold level at which to trigger the connection of another line and the total number of member links to include in the multilink group.

5 Managing

This section describes how to monitor PPP connections using the available router management consoles and utilities.

Using the PPPCON Utility

PPPCON is a diagnostic console utility that provides access to both NetWare Link/PPP™ interface statistics and information about the status of various components of the PPP data-link protocol. PPPCON uses SNMP to access this information from any local or remote system on the network.

To launch PPPCON, enter **`LOAD PPPCON`** at the system console prompt or load NIASCFG and follow this path:

Select View Status for NIAS > Protocols and Routing > PPP

You can use PPPCON to perform the following tasks:

- Reset a modem that has entered an error state
- Reset a PPP interface
- Display the configured parameters for each PPP interface
- Display PPP interface statistics dynamically
- Display the status of serial interface signals
- Monitor the states of the Link Control Protocol (LCP), NetWare Core Protocol™ (NCP™), and Link Access Protocol-Balanced (LAPB) layers
- Display parameters negotiated by PPP LCP
- Test the PPP link by temporarily establishing the PPP LCP connection with a PPP Echo test

- View the status of Multilink member links

PPP Multilink Information

PPPCON displays information about PPP Multilink in the PPP Multilink Group Information window and the Members Links Information window. Table 7 lists and describes each of the fields of the PPP Multilink Group Information window. To display the PPP Multilink Group Information window, enter **`load pppcon`** at the server console prompt and follow this path:

Select PPP Interfaces > interface you want to view > PPP Multilink Group Information

Table 7 PPP Multilink Group Information

Field	Meaning
Interface Name	Name of the primary link interface in this multilink group.
Aggregate Receive Utilization	Percentage of serial interface bandwidth currently in use receiving for this multilink group. This value includes network-layer datagram and PPP overhead.
Aggregate Transmit Utilization	Percentage of serial interface bandwidth currently in use transmitting for this multilink group. This value includes network-layer datagram and PPP overhead.
Average Receive Utilization	The average of the receive utilization of all active member links.
Average Transmit Utilization	The average of the transmit utilization of all active member links.
Call Destination Name	Destination name for the out-going call, but could be listed as in-coming call.
Total Member Links	Maximum number of links defined by the user.
Member Link Activation Type	Multilink type, either Static or Bandwidth on Demand
Bandwidth Threshold Level	Aggregrate receive or transmit bandwidth utilization level when member links will be activated or deactivated. (Valid only if the link activation type is Bandwidth on Demand.)
Bandwidth Measurement Interval	Interval to calculate the average bandwidth utilization. (Valid only if the link activation type is Bandwidth on Demand.)

Field	Meaning
Active Member Links	Number of currently active links.
Peak Member Links	Number of links ever active for this multilink group. This value may not be the same as the active count.
Last Multilink Console Error	Select this option to view the system console log output of the last error that occurred for this multilink group, including a timestamp.
Member Links Information	Select this option to view the Member Links Information window.

To display the Member Links Information window defined in Table 8 , enter **`load pppcon`** at the server console prompt and follow this path:

Select PPP Interfaces > interface you want to view > PPP Multilink Group Information > Member Links Information

Table 8 Member Links Information

Field	Meaning
Call Destination	Destination name for the outgoing call, but could be listed as incoming call.
Receive Utilization	Percentage of serial interface bandwidth currently in use receiving for this member link.
Transmit Utilization	Percentage of serial interface bandwidth currently in use transmitting for this member link.
Interface Name	Interface name of each member link in the multilink group.

Using the CAPITRCE Utility

CAPITRCE is a utility that captures and displays decoded packet communication between the following:

- The CAPI Manager (CAPIMGR) and the CAPI adaptation component (WHSMCAPI)
- The ISDN CAPI driver (each ISDN interface) and the CAPI Manager

If a problem with a PPP over ISDN connection cannot be traced to the PPP layer, CAPITRCE can be used to observe and debug negotiation between the

CAPI Manager and its upper and lower layers (the CAPI adaptation layer and CAPI driver, respectively).

NOTE: If your network uses Eicon* Technology adapters, refer to "Using the XLOG Utility" on page 134 for information on the XLOG utility. If your network uses U.S. Robotics adapters, refer to "Using the DTRACE Utility" on page 129 for information on the DTRACE utility.

To view packets exchanged between the CAPI Manager and its upper and lower layers, complete the following steps:

1. Type **`LOAD CAPITRCE`** , select the CAPI Manager or one of the displayed ISDN drivers for tracing, then select Yes when asked if you want to create a new trace.

   The Select Trace Function window is displayed.

2. If needed, select Options and specify an alternate name for the log file or specify that new data will be appended to an existing log file (select Append for the File Mode option), press Enter , then press Esc.

3. Select Start to begin the trace, and, after a desired interval, select Stop to end the trace. Then select Convert.

4. If needed, modify the default settings for the following trace options:

   - Output file—You can change the name of the output file to any other filename.

   - Convert filter options—For messages, the default, Yes specifies that CAPI messages will be included in the trace. Specify No if you do not want CAPI messages included.

     For functions, the default, No, specifies that a detailed trace of each CAPI function will not be included. If you want a detailed trace of all CAPI functions, specify Yes.

   - B3 HEX data—The default, Yes, specifies that the hexadecimal data portion of the DATA_B3_REQ and DATA_B3_IND CAPI messages will be included in the trace. Specify No to exclude this information.

   - B3 ASCII data—The default, No, specifies that the ASCII data portion of the DATA_B3_REQ and DATA_B3_IND CAPI messages will be excluded. Specify Yes to include this information.

   - Data size—You can modify the size of the data packets being traced to fit your needs. The default is sufficient for identifying the packet type.

- Times—The default, No, specifies that the time stamp for each packet will not be included in the trace. This time stamp is based on the time kept by the server and indicates when the packet is received by the CAPI Manager or ISDN driver. Specify Yes to include this information.
- Start (hh:mm:ss) and stop (hh:mm:ss)—You can specify a starting and stopping time for a section of the trace that you want to view.

5 Complete the conversion and exit CAPITRCE.

Select <Select>. At the Select Trace Function window, press Esc , then select Yes when prompted if you want to exit.

6 Enter **`LOAD EDIT SYS:FILENAME`** , where *FILENAME* is the name of the converted log file.

The trace file is displayed.

7 Press Esc to exit the trace file.

Using the DTRACE Utility

DTRACE is a menu-driven trace utility used with U.S. Robotics ISDN Allegra adapters with FXPRI.LAN and FXBRI.LAN ISDN drivers.

To load DTRACE, enter the following command at the server prompt:

```
load dtrace
```

The DTRACE main menu is displayed. Table 9 describes the fields of the DTRACE main menu. To select a menu item, use the cursor control keys (arrow keys) to move the cursor to the field you want to select.

Table 9 DTRACE Main Menu

Menu Field	Description
Board Selection	Name of board to trace
Buffer Size	Size of the file to store the trace data, default is 4 KB
Start Background Trace	Press Enter to begin trace of selected board

Menu Field	Description
Display Current Trace	Displays the Display Current Trace menu
Save Current Trace Data	Saves current trace data in a file you designate

After the trace has started, DTRACE will record all transfers between the adapter and the ISDN switch. If the file exceeds the buffer size, entries will wrap to the beginning of the file. Press Esc to stop the trace.

To display the current trace, select Display Current Trace from the DTRACE Main Menu. The Display Current Trace window is displayed. Table 10 describes the fields of the Display Current Trace window.

Table 10 Display Current Trace Window

Field	Description
Display Current Trace	Displays the current trace
Select Layer or Layers to Trace	Displays the selected layers
Layer 1	Select Yes to filter, No to include
Layer 2	Select Yes to filter, No to include
Layer 3	Select Yes to filter, No to include
Save Current Trace Data	Saves current trace data in a file you designate

After selecting a trace to display, DTRACE decodes the recorded data and displays it in ASCII packets. The output of the trace shows all incoming and outbound data between the ISDN driver and the ISDN switch.

If you choose to filter a layer's data, that layer's transfers will not be included in the trace data. This can be helpful when you are trying to diagnose problems in a specific layer. For example, filter layers 1 and 2 to diagnose a connection problem occurring only in layer 3.

Using the PPPTRACE Utility

The PPPTRACE utility enables you to debug PPP data link problems. PPPTRACE fully decodes and displays PPP protocol exchanges. You can also examine network protocol data that flows through the PPP link in a partially decoded format. Because each captured frame is time stamped to an accuracy of one tenth of a second, PPPTRACE can also provide valuable timing information.

This topic describes the interface for PPPTRACE. You can use PPPTRACE to perform the following tasks:

- Observe real-time samples of data as it flows through the PPP interface.
- Capture the PPP protocol exchanges and troubleshoot any PPP connectivity problem. You can display and capture every LCP and NCP protocol exchange. This lets you pinpoint the cause of failure for a PPP connection, including the following:
  - Failure to negotiate LCP options
  - Failure to negotiate NCP options
  - Failure to authenticate a user or remote system ID
  - Delays in replying to LCP/NCP requests and verification of consequent retransmissions
  - Isolate problems as belonging to the hardware driver or the PPP data link
- Capture to RAM (fast capture) or to disk (for viewing at a later time on the same or different machine)
- Examine raw packet data in ASCII or hexadecimal format
- Switch monitoring among different PPP interfaces by pressing a single key

To start PPPTRACE, type the following command at the server prompt:

```
load ppptrace
```

The PPPTRACE Available Options menu enables access to the features of PPPTRACE. These features are described in Table 11.

Table 11 PPPTRACE Options

Option	Description
Network Interface Information	Displays the hardware parameters for all configured PPP interfaces in the system. This option displays the following information: I/F Name—Symbolic name used by the Link Support Layer™ (LSL™) software to refer to this interface. LSLBoardNo—Interface index used by SNMP to refer to this interface. I/O—Specifies the base input/output (I/O) port address of the interface. IRQ—Specifies the primary interrupt request level. MEM—Specifies the shared base memory address where the board memory that is shared between the adapter and the host system is located. Port—Identifies the specific port on the adapter that is associated with this interface.
Real-Time Monitor	Enables the dynamic view and capture of all NetWare Link/PPP traffic through a PPP interface. You can capture the dynamic data that is displayed on window to either a disk file or to RAM and replay it later for diagnostic analysis. This option displays the following information: Dir—Specifies whether the data is being received from the network (Rcv) or being sent from the routing software. TIme—Specifies the time the data is sent or received (in 24-hour format). Size—Specifies the size of the sent or received data (in bytes). PPP Data—Displays the actual data being transmitted or received. Status—Specifies the current configuration display settings.
PlayBack	Enables playback of any captured data traffic session from RAM or a disk file using the following options: PlayBack Device—Specifies the captured data session to be played back from either a disk file or from RAM. Disk Filename—Specifies the name of the file to be played back. You can have several files to which you saved several real-time sessions. This option enables you to pick one session and play it back. PlayBack Speed—Specifies the speed at which you want to view the session: Fast, Medium, or Slow. You can change the speed and view the session again at another speed, if needed.

Option	Description
Configuration	Enables configuration of the capture device to meet your specific needs. Use this option to set up the various Trace parameters before you start a capture session. For example, to capture a session to a file, first specify the capture device and the filename using the Configuration window. This option enables you to configure the following parameters: Capture Device—Specifies the device that should be used with the capture option in the Real-Time Monitor window: either Disk or RAM (default). If you choose Disk, you must specify a filename in the next parameter. Disk Filename—Specifies the name of the file to which you want to capture the data. Use a standard DOS filename.

Note that the Real-Time Monitor does not show all the frames on the display. Instead, it shows a sampling of frames and ignores the frames that came in while the display of a frame was in progress. If you capture the output to a disk file or RAM and display it later, all frames that were processed by the PPP interfaces are displayed.

WARNING: The Real-Time Monitor can consume a large portion of your router CPU resources.

For example, a status value of [Raw Mode, Short, Hex] tells you that the data is being shown in Raw Mode (no decode of any PPP frames), Short Display (one line of data), and Hex. Use function keys F3 , F4 , or F5 to change any of the three configuration parameters dynamically.

WARNING: When Multilink is used, all data frames are shown only on the first member of the Multilink group, though LCP packets are still shown for each link.

The Real-Time Monitor provides its functions through the following keys:

F2 —Enables you to select an interface. Identify your interface (LSL board number) by viewing the port status window in NWCCON.

F3 —Toggles the display between Raw Mode (no decode of any PPP frames) or Decode Mode (PPP frames fully decoded).

F4 —Toggles the display between complete and short display format.

F5 —Toggles the display between Hex or ASCII format.

F6 —Enables you to freeze and resume the continuous display of data.

F7 —Enables you to begin and stop capturing the continuous display of data to either a disk file or to RAM.

F8 —Goes to next interface.

F9 —Returns to preceding interface.

Using PPPDISP

PPPTRACE works with PPPDISP to provide a way to analyze the output of PPPTRACE. PPPDISP is a DOS executable utility that decodes the PPPTRACE output file and generates an ASCII format file. PPPDISP.EXE is located in SYS:SYSTEM\UTILS.

For example, to write the captured data to an output file to display in ASCII, complete mode, and frame mode, enter the following command:

PPPDISP *source_filename destination_filename*

If the destination filename is not specified, data is displayed on the console server window. The contents of the source file are converted so that they are displayed in ASCII or hex format, in complete or short display mode, and in one of three decode modes: raw, frame, or packet mode. Table 12 shows the arguments that can be used with this DOS executable file. These arguments are case-sensitive.

Table 12 PPPDISP Arguments

Argument	Meaning
PPPDISP	Runs the DOS executable file
source filename	Specifies the name of the input file
destination filename	Specifies the name of the output file

Using the XLOG Utility

Use the XLOG utility to help diagnose ISDN-related connection problems with Eicon Technology ISDN adapters. The following Eicon adapters maintain a log of connection events in a buffer:

- SCOM Basic Rate Adapter
- Quadro Four-Port Basic Rate Adapter

- S2M Primary Rate Adapter
- Amadeo Basic Rate Adapter

The XLOG utility is located in the SYS:SYSTEM directory. XLOG reads, formats, and writes the buffer contents to an ASCII text file, also stored in SYS:SYSTEM, or displays the buffer contents on the server console window.

To load XLOG, type the following command at the server prompt:

load xlog [adapter] [+|-] [s|d] ***filename***

where

adapter is the name of the ISDN adapter, as specified in NIASCFG.

[+|-] indicates the type of output. The + flag causes XLOG to write continuously to the log file (specified *filename*) until interrupted by a keystroke. The - flag causes XLOG to write continuously to the server console window until interrupted by a keystroke.

[s|d] indicates the type of information to record. The s flag causes XLOG to record SIG events only. The d flag causes XLOG to record D-channel events only.

filename is the name of the file where XLOG stores the recorded information. If the file already exists, the new trace overwrites the previous contents of the file.

Use any text editor to view the ASCII-text log file. Each line in the trace contains one event and the time of its occurrence in hours, seconds, and milliseconds (relative to the time XLOG was loaded). The following line shows the format of a recorded event:

HH:SSS:MMM - *Event name*

Table 13 provides a general sequence of events and a description of the event when a line establishes an outgoing connection.

Table 13 Key Events in ISDN Connections

Event	Description of Event
Sync_Gained	Physical link established.
L1_UP	LAPD RR frames are being sent and layer 1 is active.

Event	Description of Event
D-X, D-R	The D-channel is transmitting and receiving data.
SIX-x ... SPID	SPID is sent to the switch.
SIG-r	TEI number is received from switch.
EVENT:Layer-2 Failed, resend SPID	Incorrect SPID sent to switch; make sure correct SPID is configured.
EVENT:SPID Accepted	Switch accepted the SPID.
Q.931 ... SETUP	A call is being placed.
SIG-R ... CALL_PROC	Switch indicates the call is proceeding.
SIG-R ... CONN	An end-to-end connection is established.
SIG-R ... CONN_ACK	Local acknowledgment of the connection is received.
B1-X, B1-R	The first B-channel is transmitting and receiving.
B2-X, B2-R	The second B-channel is transmitting and receiving.

Verifying the Router Configuration

After you configure the Novell® Internet Access Server 4.1 routing software, verify that your router is configured in the way you intended. Using the monitoring and management tools available, you can view whether your router is working correctly according to your configuration. This topic contains the following sections:

- "Viewing Authentication Configuration for a PPP WAN Link" on page 137
- "Viewing Data Compression Configuration for a PPP WAN Link" on page 137
- "Viewing Negotiated Options Configuration for a PPP WAN Link" on page 138

Viewing Authentication Configuration for a PPP WAN Link

To view the Remote System ID and Password parameters at the receiving end, complete the following steps:

1. Load NIASCFG and follow this path:

   Select Configure NIAS > Protocols and Routing > Network Interfaces > PPP interface you want to view

   The PPP Network Interface Configuration window appears.

2. Select the following path:

   Authentication Options > Authentication Database > system entry you want to view

   The PPP Inbound Authentication window appears.

3. Look at the Remote System ID parameter.

   To view the Remote System ID parameter at the calling end, load NIASCFG and follow this path:

   Select Configure NIAS > Protocols and Routing > WAN Call Directory > local system ID

4. Look at the Password parameter.

   To view the Remote Password parameter at the calling end, load NIASCFG and follow this path:

   Select Configure NIAS > Protocols and Routing >WAN Call Directory > Remote Password

Viewing Data Compression Configuration for a PPP WAN Link

To find out whether data compression is turned on and what the compression ratio is for an active interface, load MONITOR and follow this path:

Select LAN/WAN Information > interface you want to view

If the Compression Algorithm in the Custom Statistics field on the MONITOR window has a value other than 0, you can also find the Send Compression Ratio and Receive Compression Ratio fields if data is being sent or received.

You can use PPPCON to determine which compression algorithm is being used. Load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Negotiated Parameters

The PPP Negotiated Parameters window displays the Data Compression Algorithm in use, if applicable.

Viewing Negotiated Options Configuration for a PPP WAN Link

To see which options were negotiated for a PPP WAN link, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Negotiated Parameters

Monitoring Performance

Monitoring the performance of the router and connections is an important management task. If the router or links are not performing efficiently, they could cause problems for users or could signal a larger problem in your network. This topic contains the following sections:

- Monitoring Overall Link Performance
- Determining the PPP WAN Link Quality
- Determining PPP WAN Link Congestion
- Determining the Traffic Utilization for a PPP WAN Interface
- Determining the Traffic Utilization for a PPP Multilink Interface
- Determining the Available Bandwidth for a PPP WAN Interface

Monitoring Overall Link Performance

To monitor the performance of a particular interface, load MONITOR and follow this path:

Select LAN/WAN Information > interface you want to view

Check the following fields:

- Send Line Utilization
- Receive Line Utilization
- Receive Overruns
- Data Q Backup in 1/1000 second

Consistently high values in these fields indicate that the link is busy and that performance has probably degraded. In this case, consider using a higher line speed. Note that occasional increases in the values for these fields are normal in all networks.

Determining the PPP WAN Link Quality

You can determine the quality of a PPP WAN link by loading PPPCON and selecting PPP Interfaces.

If the Exceptions field in the PPP Interfaces window shows a value other than 0, select the interface, then PPP Error Statistics. A high value in the Bad FCS Values counter indicates problems on a link.

Select the interface you want to view. If LAPB and Data Compression is enabled, select LAPB Interface Information > Traffic Flow Statistics

High values in the Transmit REJs, Receive REJs, and T1 Timeout counters indicate a poor connection.

You can also determine the quality of the link by checking the following counters in MONITOR:

- Send Packet Retry under PPP Generic Statistics
- Checksum Errors under PPP Generic Statistics
- LAPB Retransmissions under PPP Custom Statistics
- Compression Reset under PPP Custom Statistics
- RxDataPktDropped under PPP Custom Statistics
- Receive CRC Errors under NW2000 (or other board) Statistics
- Receive Aborts under SYNC Only Statistics
- Receive Char Framing Errors under ASYNC Only Statistics
- Receive Chars out of Frame under ASYNC Only Statistics

The higher the values of the counters, the lower the link quality. If only the LAPB Retransmission counter is high, use NIASCFG to adjust the T1 timer to a larger value.

The LAPB parameters are meaningful only if PPP data compression is enabled and successfully negotiated with the remote PPP peer.

NOTE: High values for the Receive CRC Errors and Receive Aborts statistics are normal if the Dialing Mode parameter is set to V.25bis.

Determining PPP WAN Link Congestion

To determine whether the PPP data link is congested, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > General Interface Information

The Interface Statistics window is displayed.

Look at the Queue Length fields. If these fields consistently contain a high value, consider using a higher bandwidth modem or leased line. Occasional increases in the amount of WAN traffic are normal for any network.

Determining the Traffic Utilization for a PPP WAN Interface

To determine the traffic utilization for an interface, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view

Look at the Receive Utilization and Transmit Utilization fields. These numbers can exceed 100 percent if you have compression turned on.

Determining the Traffic Utilization for a PPP Multilink Interface

To determine the traffic utilization for a PPP Multilink interface, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Multilink Group Information

The Aggregate Receive and Transmit Utilization percentage values represent the sum of the utilization of all active links in the Multilink group.

The Average Receive and Transmit Utilization percentage values represent the average utilization of all active links in the Multilink group.

Determining the Number of Links in a Multilink Group

To determine the number of links in a PPP Multilink group, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Multilink Group Information

Table 14 shows the fields of the PPP Multilink Group Information window needed to determine the number of links in a PPP Multilink group. For more detailed information, please refer to "PPP Multilink Information."

Table 14 PPP Multilink Information

Field	Meaning
Call Destination Name	Call destination (for outgoing calls)
Active Member Links	Number of current active links of this multilink group
Peak Member Links	Shows the greatest number of links established by this multilink group
Last Multilink Console Message	Shows the last console message received regarding this multilink group
Member Links Information	Shows each interface of the active member links of this multilink group, receive and transmit utilization, and destination of call

Determining the Available Bandwidth for a PPP WAN Interface

You can determine the available bandwidth of the PPP link for an active interface by loading PPPCON and following this path:

Select PPP Interfaces > interface you want to view > General Interface Information

The Interface Statistics window is displayed.

Look at the Speed field. Note that for an asynchronous line, the value might not reflect the real bandwidth; the real bandwidth might be 80 percent or less than the apparent value.

You can also check the available bandwidth by loading MONITOR and looking at Interface Speed under Custom Statistics.

Checking the Connection between Routers

You can check that the connection between routers is active by performing the following tasks:

- Use MONITOR to determine whether a link is active
- Run an Echo or Ping test to determine whether a remote router or services are reachable
- Use PPPTRACE to monitor the PPP protocol exchanges that occur during PPP data-link establishment
- Use MONITOR and the consoles to monitor the error counters

This topic contains the following sections:

- "Determining Whether a LAN or PPP WAN Link Is Active" on page 142
- "Determining Whether a Remote Router Is Reachable over a PPP WAN Link" on page 142
- "Monitoring PPP Packet Exchanges" on page 143
- "Monitoring Communications Equipment" on page 145
- "Monitoring Error Counters" on page 148

Determining Whether a LAN or PPP WAN Link Is Active

To determine whether a link is active, load MONITOR and follow this path:

Select LAN/WAN Information > interface you want to view

Under Generic Statistics, look at the Total Packets Sent and Total Packets Received counters. The link is active if these counters are increasing.

Determining Whether a Remote Router Is Reachable over a PPP WAN Link

To determine whether a remote router is reachable, you can run an Echo test. To run an Echo test, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Echo Test

The following information is displayed:

- Interface Name—Symbolic name used by the Link Support Layer™ (LSL™) software to refer to this interface.

- Interface—Interface index used by SNMP to refer to this interface. This is the same as the board number assigned by the LSL to this interface.
- Echo Test Results—Displays the results for the Echo test. Displays None if the test has not been run, Success if the test is successful, Failure if the test fails, and In Progress if the test is in progress.
- Current Call Destination—Displays the PPP WAN call destination name if the interface is connected to a PPP peer or None if the local interface is not connected. To select the WAN call destination, press Enter to display a list of destinations, select a destination and press Enter again.
- Number of Echo Test Iterations—Number of times the Echo test is repeated. The default is 1. To specify a different number, press Enter and type a new number.
- Echo—Press Enter on this field to perform the Echo test.

Monitoring PPP Packet Exchanges

You can determine the location of a failure point by capturing PPP packet exchanges. To do this, load PPPTRACE and complete the following steps:

1. From the Available Options window, select Configuration.
2. Select Capture Device.

   Select whether you want to capture the data to RAM or to Disk. If you select Disk, specify the filename in the Disk Filename field.
3. Press Esc to go back to the Available Options window.
4. Select Real-Time Monitor to view and capture the PPP protocol exchanges.

   The Real-Time Monitor window is displayed.
5. Press F7 to begin capturing the information.

   Press F7 when you want to end the capture.

   You can also use the following keys:

   F2 —Displays the statistics for the next interface.

   F3 —Toggles the display between raw mode (no decode of any PPP frames) and decode mode (PPP frames fully decoded).

   F5 —Toggles the display between Hex and ASCII.

   F6 —Enables you to freeze and resume the continuous display of data.

F8 —Selects the next interface.

F9 —Selects the preceding interface.

6. Establish the call.

   If you are testing outgoing calls, use CALLMGR on the local router to initiate the call. If you are testing incoming calls, use CALLMGR on the remote router to initiate the call.

7. Press F7 to stop the capture when the desired data has been sent.

8. Press Esc to return to the PPPTRACE menu.

9. Select Playback to view the captured data at your convenience.

   The captured data might show one of the following problems:

   - Failure to negotiate LCP options—Shown by the LCP Config-Reject or the LCP Config-NAK packet. Check the LCP negotiated parameters in PPPCON and make sure that the maximum and minimum MRU values are set within the negotiable range between routers. For more information, see "Viewing Negotiated Options Configuration for a PPP WAN Link."

   - Failure to authenticate a user—Shown by the LCP Authentication Config-Reject packet and the LCP PAP NAK packet or the LCP CHAP Fail packet. An LCP Config-NAK packet might also appear, but it does not indicate a problem with authentication. Look at the system console for messages. Check that authentication is enabled at the calling end, and make sure that both sides are using the same authentication method. Also, confirm that the Remote System ID and the Password parameters at the receiving end are set to the same value as the Local System ID and the outbound Password parameters at the calling end. For more information, see "Viewing Authentication Configuration for a PPP WAN Link."

   - Failure to negotiate NetWare® Core Protocol™ (NCP™) options—Shown by the NCP Config-Reject and the NCP Config-NAK packet. Ensure that the interface is bound to the same protocol on both sides. Use CALLMGR to find out which network protocol is used to make the call, then use PPPCON to check whether the same protocols are bound to the interfaces at both ends.

   Figure 9 shows a sample PPP packet exchange.

Figure 9 Real-Time Monitor Capturing PPP Packet Exchanges

```
        Real-Time Monitor [I/F Name=DNLTEST_2  LSLBoardNo=5    Port=2

Dir Time         Size PPP Data  [PPP Decode, Complete, ASCII]
Rcv 10:46:10.7 20    [cr][lf]CONNECT 9600/ARQ[cr][lf]
Snd 10:46:12.3 20    Adr Ctl LCP  CnfgReq Id Len  ACCM Len AsyncMap Mg
                     FF  03  C021 01      0B 0010 02   06  000A0000 05
                     Data..
                     0003CCFC
Rcv 10:46:13.0 25    Adr Ctl LCP  CnfgReq Id Len  ACCM Len AsyncMap AU
                     FF  03  C021 01      0B 0015 02   06  000A0000 03
                     CHAP MD5 MgkNo Len Data..
                     C223 05  05    06  000288B0
Rcv 10:46:13.0 20    Adr Ctl LCP  CnfgAck Id Len  ACCM Len AsyncMap Mg
                     FF  03  C021 02      0B 0010 02   06  000A0000 05
                     Data..
```

Monitoring Communications Equipment

Monitoring your communications equipment can help you identify the source of some common problems with your local modem or data circuit-terminating equipment (DCE) device, including the following:

- The modem or DCE does not answer incoming calls.
- The modem or DCE does not initiate outgoing calls.
- The modem or DCE initiates outgoing calls but does not successfully connect.

If the modem or DCE device cannot answer an incoming call or cannot initiate an outgoing call, you might need to reset it. Before resetting the device, check the following information:

- If the modem cannot answer incoming calls, check the AA (Auto Answer) light on your device. If it is off, reset the modem by using PPPCON or cycling the power.
- If the modem cannot answer incoming calls or initiate outgoing calls, use PPPTRACE to capture and decode modem or DCE device dialogs. Look at the send and receive exchanges to determine whether it is responding to the command properly (see the next section, "Capturing Modem/DCE Device Dialogs" on page 146). If the modem does not respond properly, reset it by using PPPCON or cycling the power.

If the modem or DCE device can initiate an outgoing call but cannot connect, you might need to change the settings or the hardware. To determine your course of action, check the following information:

- Use PPPTRACE to capture and decode modem or DCE device dialogs. Look at the dial command to determine whether the correct phone number for the remote modem was used. If the number is incorrect, use NIASCFG to change the number.
- Use MONITOR to look at the serial signals. If data set ready (DSR) or data carrier detect (DCD) are off, the modem cannot connect. Check the cable between the router and the modem. If the cable is properly connected, try another modem. If this does not resolve the problem, enable the Simulate DSR On parameter. Load NIASCFG and follow this path:

  Select Configure NIAS > Protocols and Routing > Network Interfaces > Physical Options

Capturing Modem/DCE Device Dialogs

To capture and decode modem or DCE device dialogs, load PPPTRACE and complete the following steps:

1. From the Available Options window, select Configuration.
2. Select Capture Device.

   Select whether you want to capture the data to RAM or to Disk. If you select Disk, specify the filename in the Disk Filename field.
3. Press Esc to go back to the Available Options window.
4. Select Real-Time Monitor to view and capture the modem or DCE device dialog.

   The Real-Time Monitor window appears.
5. Press F7 to begin capturing the modem or DCE device dialog.

   Press F7 when you want to end the capture.

   You can also use the following keys:

   F2 —Displays the statistics for the next interface.

   F5 —Toggles the display between Hex and ASCII.

   F6 —Enables you to freeze and resume the continuous display of data.

   F8 —Goes to the next interface.

F9 —Returns to the preceding interface.

6 Establish the call.

If you are testing outgoing calls, use CALLMGR on the local router to initiate the call. If you are testing incoming calls, use CALLMGR on the remote router to initiate the call.

7 Press F7 to stop the capture when the desired data has been sent.

8 Press Esc to return to the PPPTRACE menu.

9 Select Playback to view the captured data at your convenience.

You can expect to see the response OK or an echoed command for each initialization string sent to the modem. If the modem does not respond, check the power and cable connections.

Figure 10 shows a sample modem dialog.

Figure 10 Real-Time Monitor Capturing a Modem Dialog

```
        Real-Time Monitor [I/F Name=DNLTEST_2  LSLBoardNo=5

Dir Time         Size PPP Data  [PPP Decode, Complete, ASCII]
Snd 10:46:55.6 10 +++ATE1H0[cr]
Rcv 10:46:55.7 6  [cr][lf]OK[cr][lf]
Snd 10:46:57.5 1  [cr]
Snd 10:46:58.0 5  AT&F[cr]
Rcv 10:46:58.1 8  [cr]AT&F[cr][cr][lf]
Rcv 10:46:58.1 4  OK[cr][lf]
Snd 10:46:59.9 15 ATE0N1Q0V1W1X4[cr]
Rcv 10:47:00.0 17 ATE0N1Q0V1W1X4[cr][cr][lf]
Rcv 10:47:00.0 4  OK[cr][lf]
Snd 10:47:01.1 18 AT&C1&D2&K0&Q5%C0[cr]
```

Viewing Modem/DCE Serial Signals

To monitor the serial interface signals raised by the modem or the DCE device, load MONITOR and follow this path:

Select LAN/WAN Information > interface you want to view

Under the specific board's statistics section, look for serial interface signals such as DTR, DSR, RTS, CTS, and DCD (1=on, 0=off).

Resetting a Modem or DCE Device

To reset the modem or DCE device, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Reset Modem > Reset Modem

The following information is displayed on the PPP Reset Modem window:

- Interface Name—Symbolic name used by the LSL to refer to this interface.
- Interface—Interface index used by SNMP to refer to this interface. This is the same as the board number assigned by the LSL to this interface.
- Reset Modem Results—Displays None if the test has not been run, Success if the modem reset correctly, Failure if the modem did not reset correctly, and In Progress if the test is in progress.
- Reset Modem—Pressing Enter on this field resets the modem or DCE device.

Monitoring Error Counters

Error counters are monitored to make sure they are not increasing rapidly, because a rapid increase indicates a problem. You can monitor error counters for PPP interfaces in the following ways:

- By using MONITOR to view counters such as Checksum Errors, Send and Receive Packet Errors, and interface-specific errors. To view these counters, load MONITOR and follow this path:

  Select LAN/WAN Information > interface you want to view

- By using PPPCON to view the following PPP counters:
  - Bad Address Fields
  - Bad Control Fields

- Bad FCS Values
- Packets Too Long

To view these counters, load PPPCON and follow this path:

Select PPP Interfaces > interface you want to view > PPP Error Statistics

- By using IPXCON to view the following IPX counters:
  - Too Many Hops
  - Header Errors
  - Unknown Sockets
  - Decompression Errors
  - Malformed Requests
  - Compression Errors
  - Open Socket Failures
  - Maximum Sockets

  To view these counters, load IPXCON and follow this path:

  Select IPX Information > Detailed IPX Information
- By using TCPCON to view the following TCP/IP counters:
  - IP Errors
  - IP Address Errors
  - Unknown Protocol Errors
  - Local Errors
  - Reassembly Failures Detected
  - Fragmentation Failures Detected

  To view these counters, load TCPCON and follow this path:

  Select Statistics > IP > More IP Statistics
- By using ATCON to view the following AppleTalk counters:
  - Bad DDP Length
  - Bad DDP Checksum
  - No Route Found
  - Too Many Hops

To view these counters, load ATCON and select Packet Statistics.

Monitoring PPP Multilink Information

Monitor PPP Multilink information to view status and determine whether the Novell Internet Access Server routing software is configured properly. Monitoring this information can also be helpful in troubleshooting and optimizing the network.

This topic contains the following sections:

- "PPP Multilink Information" on page 150
- "Member Links Information" on page 150

PPP Multilink Information

The PPP Multilink Group Information window provides specific information about selected interfaces. To display the PPP Multilink Group Information window, enter **`load pppcon`** at the server console prompt and follow this path:

Select PPP Interfaces > interface you want to view > PPP Multilink Group Information

For more detailed information, please refer to Table 7 on page 126.

Member Links Information

The Member Links Information window provides specific information about a selected multilink group. To display the Member Links Information window, enter **`load pppcon`** at the server console prompt and follow this path:

Select PPP Interfaces > interface you want to view > PPP Multilink Group Information > Member Links Information

For more detailed information, please refer to Table 8 on page 127.

6 Troubleshooting

This section contains NetWare Link/PPP™ and CAPI ISDN software troubleshooting information that is divided into four topics:

- Troubleshooting tools
- Configuration tips
- Troubleshooting checkpoints
- Common problems

If a problem that is general in nature occurs, the procedure described in Troubleshooting Checkpoints will help you isolate and resolve the problem. If a problem with a specific symptom occurs, refer to "Common Problems."

Troubleshooting Tools

The utilities that can be used to troubleshoot NetWare Link/PPP are described in the following sections:

- PPPTRACE
- CAPITRCE
- PPPCON
- MONITOR

PPPTRACE

PPPTRACE is a utility that captures and displays decoded PPP packets; encoded IPX, IP, AppleTalk, and source route bridge packets; and modem control packets. PPPTRACE can be used to determine the contents and validity of modem initialization scripts and login initialization scripts, to

observe and debug Link Control Protocol (LCP) and NetWare Control Protocol (NCP) negotiation, and to debug problems with communications links.

To view packets generated by NetWare Link/PPP, complete the following steps:

1. Enter **LOAD PPPTRACE** at the console prompt.
2. Select Real-Time Monitor, then press F8 until the interface you want to view is displayed.
3. To capture the data to RAM, press F7.

   You can view the captured data by watching the PPPTRACE Real-Time Monitor window, using the Play Back option, or using the print utility. Remember that the PPPTRACE Real-Time Monitor window will probably not show all the packets; use the Play Back window or the print utility to see all the captured packets.

   The PPPTRACE print utility reads a capture file, converts the file contents from hexadecimal to ASCII, and writes the contents to an output file that can be printed or viewed with an ASCII editor or browser. The command for this DOS executable file has the following format:

   PPPDISP <*saved_file*> <*output_file*>

CAPITRCE

CAPITRCE is a utility that captures and displays decoded packet communications between the following:

- The CAPI Manager (CAPIMGR) and the CAPI adaptation component (WHSMCAPI)
- The ISDN physical layer (each ISDN interface) and the CAPI Manager

If a problem with a PPP over ISDN connection cannot be traced to the PPP layer, CAPITRCE can be used to observe and troubleshoot negotiation between the CAPI Manager and its upper and lower layers (the CAPI adaptation layer and CAPI driver, respectively).

To view packets exchanged between the CAPI Manager and its upper and lower layers, complete the following steps:

1. Enter **LOAD CAPITRCE** , select CAPI Manager or one of the displayed ISDN drivers for tracing, then select Yes when prompted if you want to create a new trace.

The Select Trace Function window is displayed.

2. If required, select Options and specify an alternative name for the log file or specify that new data will be appended to an existing log file (select Append for the File Mode option), press Enter , then press Esc.

3. Select Start to begin the trace, and, after a desired interval, select Stop to end the trace. Then select Convert.

4. If required, modify the default settings for the following trace options:

   - Output File—You can change the name of the output file to any other *.TXT filename.
   - Convert Filter Options—For Messages, the default, Yes, specifies that CAPI messages will be included in the trace. Specify No if you do not want CAPI messages included.

     For functions, the default, No, specifies that a detailed trace of each CAPI function will not be included. If you want a detailed trace of all CAPI functions, specify Yes.
   - B3 HEX Data—The default, Yes, specifies that the hexadecimal data portion of the DATA_B3_REQ and DATA_B3_IND CAPI messages will be included in the trace. Specify No to exclude this information.
   - B3 ASCII Data—The default, No, specifies that the ASCII data portion of the DATA_B3_REQ and DATA_B3_IND CAPI messages will be excluded. Specify Yes to include this information.
   - Data Size—You can modify the size of the data packets being traced to meet your requirements. The default is sufficient for identifying the packet type.
   - Times—The default, No, specifies that the time stamp for each packet will not be included in the trace. This time stamp is based on the time kept by the server and indicates when the packet is received by the CAPI Manager or ISDN driver. Specify Yes to include this information.
   - Start (hh:mm:ss) and stop (hh:mm:ss)—You can specify a starting and stopping time for a section of the trace that you want to view.

5. Complete the conversion and exit CAPITRCE.

   At the Select Trace Function window, press Esc , then select Yes when prompted if you want to exit.

6. Enter **LOAD EDIT SYS:***FILENAME* , where *FILENAME* is the name of the converted log file (the *.TXT file).

   The trace file is displayed.

7. Press Esc to exit the trace file.

PPPCON

PPPCON is a diagnostic console utility that provides access to both NetWare Link/PPP interface statistics and information about the status of various components of the PPP data-link protocol. PPPCON uses SNMP to access this information from any local or remote system on the network.

You can use PPPCON to perform the following tasks:

- Reset a modem that has entered an error state
- Reset a PPP interface
- Display the configured parameters for each PPP interface
- Display PPP interface statistics dynamically
- Display the status of serial interface signals
- Monitor the states of the Link Control Protocol (LCP), Network Control Protocol (NCP), and Link Access Protocol-Balanced (LAPB) layers
- Display parameters negotiated by PPP LCP
- Test the PPP link by temporarily establishing the PPP LCP connection with a PPP Echo test

Using PPPCON to Reset a Modem

You can use this option when a modem is not answering an incoming call or when you need to check the modem initialization script. To use this option, complete the following steps:

1. Enter **LOAD PPPCON** at the console.
2. Select the PPP Interfaces option.
3. Select the interface on which the modem you want to reset resides.
4. Select the PPP Reset Modem option.
5. Press Return to reset the modem.

6 Wait 15 seconds or longer for the script to finish. The Status field changes to Success if the initialization is successful or Failed if the initialization is unsuccessful. If the initialization failed, proceed to "Create or Change a Modem Script."

MONITOR

You can use MONITOR to check the state of PPP connectivity by viewing the statistics for the PPP driver. Statistics for each port are displayed on a per-port basis.

Following are examples of some of the statistics:

- Baud Rate
- Transmit Packets
- Transmit Packets Miscellaneous Errors
- Compression Algorithm

Each port on the PPP board also has states listed for the following protocols:

- LCP
- AppleTalk
- IP
- IPX
- Bridge (source route bridge, SNA/NetBIOS Translation Bridge, or both)

Each link state has a number associated with it. State 2 indicates that you have configured the protocol and it is listening for a response on the line. State 9 indicates that the protocol has opened the connection and is transmitting across the line. State 0 indicates that the protocol has closed the connection and is not listening.

LCP

A PPP link is established after the originating PPP interface first sends LCP packets to configure the data link. In the MONITOR window, the selected interface LCP state should indicate 9, which represents the LCP Open state. If a connection has been attempted and LCP is not in state 9, there is probably a data communications problem on the line or the LCP negotiation options are preventing the completion of the call.

If there is a problem, load NIASCFG to verify that the WAN interface has the Physical Type option set to the correct value (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > Selected WAN Interface). If you are using a DSU/CSU, verify that the data encoding (NRZ or NRZI) is set to the same value as that used by the router interface on the other side of the WAN connection. Also verify that the data encoding is set to the same value as that used by the DSU/CSU or other communications device to which the port is connected. Finally, verify that all other NIASCFG parameters are configured correctly.

Run the SD.EXE program (refer to the *Novell Synchronous/+ Adapter Installation Guide*) to test the Synchronous/+ board. Contact your telco to have it check the line and perform loopback testing with the DSU/CSU.

AppleTalk, IP, IPX, and Source Route Bridge

If LCP is in state 9 and the desired protocol is not connecting, the problem probably exists in the configuration of the protocol. If the desired protocol is in state 0, you might not have enabled the protocol and it is not listening on this line. If the desired protocol is in state 2, the protocol has been configured and is waiting for a response from the other side.

Configuration Tips

We recommend the following guidelines for configuring NetWare Link/PPP:

- The routing software can be used to set up a PPP connection to an Internet Service Provider (ISP) provided there is TCP/IP routing to the Internet over a dial-up modem, ISDN card, or synchronous WAN link.
- Some configuration options require special attention when connecting to an ISP. Ensure that you have already configured the appropriate board and interface for a PPP connection. Also, obtain a PPP account with an ISP and at least one assigned STATIC IP address. The routing software currently does not support dynamically assigned local addresses.
- If you will be routing to a local LAN that uses IP addresses, these addresses must also be obtained from your ISP, or otherwise registered with your company. You cannot make up your own addresses.
- Asynchronous modems on a serial port use the driver WHSMAIO. CAPI-compliant ISDN boards use the driver WHSMCAPI. All other boards have a board-specific driver. Novell Internet Access Server 4.1 does not currently support ISDN modems or Terminal Adapters. Check with the

manufacturer to see if it provides its own ISDN scripts for the Novell Internet Access Server 4.1 routing software.

- For WAN interface configuration, set Interface Speed to External if you are using DSU/CSU devices. Disable Inbound Authentication under Authentication Options because you will be originating the call. Under Negotiation Options, set PPP Header and Data Compression to Disabled. To make these changes, load NIASCFG and select Configure NIAS > Protocols and Routing > WAN Call Destinations > select the WAN Interface Driver. Changes can be made in the ISDN Parameters and Special Options windows. You can enable these options later if your ISP supports compression.

- Your ISP should inform you if you must use a login script. Login Script Name allows you to select a script that can be used to specify a login name, a password, or other keywords expected by your ISP. Some ISPs might require this type of exchange before you access their system, or they might require that you inform them that you will be using PPP. These steps might be necessary if you must actually log in to the ISP's system or send data through a firewall. In most cases, a login script is not necessary. You probably will be given a username and password by your ISP, but this information is used later in the Outbound Authentication setup.

- The Outbound Authentication option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > ISDN Interface Driver > Outbound Authentication) specifies the PPP authentication protocol to be used. On-demand links require authentication, but it is optional on permanent links. The type of authentication is determined by the ISP.

  For on-demand links, set Outbound Authentication to either PAP or CHAP. Either type of authentication is used, depending on the ISP requirements. If you are setting up a permanent link and are certain that the ISP uses no authentication, set Outbound Authentication to None.

  The ISP will give you a PAP or CHAP login name and password (the ISP might refer to it as your account username and password). For Local System ID, enter the username or login name assigned to you by the ISP. The username and password are case-sensitive. For Remote System ID, enter a name you want to use to identify the remote system. This can be any name, such as ISP.

- For TCP/IP protocol configuration, load NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > TCP/IP). Make sure

that both TCP/IP Status and IP Packet Forwarding are enabled. Other settings can be left at their defaults.

- If you plan to bind TCP/IP to the WAN interface, your ISP should have assigned you an IP address for your side of the link and/or a block of addresses for your own use. The binding configuration will vary, depending on the addresses assigned to you and the type of link the ISP has set up. There are two ways the link can be set up: numbered single point-to-point and unnumbered single point-to-point.

  - Numbered single point-to point—This type of connection uses an IP address for each end of the WAN link. The link is treated as its own network, so the two IP addresses must conform to the same network address. An example follows:

    Local IP address: 137.65.45.17 (subnet mask 255.255.240)

    Remote IP address: 137.65.45.19 (subnet mask 255.255.240)

    Block of addresses: 150.3.56.64 through 150.3.56.95 (subnet mask 255.255.255.224)

    The local and remote IP addresses for the WAN link are in the same network. If the local and remote IP addresses are not in the same network, do not use a numbered link. Set up a numbered link and bind 137.65.45.17 to the WAN interface and specify 137.65.45.19 as the remote IP address. Use the block of addresses assigned to you to bind to the network interface in the server and the clients on the LAN.

    To configure a numbered single point-to-point connection, load NIASCFG, select Configure NIAS > Protocols and Routing > Bindings, and then press Ins to add a new binding. Select TCP/IP and then select the WAN interface set up previously. For WAN Network Mode, select Numbered Single Point-to-Point. For Local IP Address, enter the local IP address assigned by the ISP (for example, 137.65.45.17). For Subnetwork Mask, enter the subnet mask assigned by the ISP (for example, 255.255.255.240). Select WAN Call Destination, then press Ins. Press Enter and select the defined WAN call destination. For Remote IP address, enter the ISP's remote address (for example, 137.65.45.19). Press Enter on Static Routing Table and then press Ins to add a new static route. Under Route to Network or Host, select Network for the IP Address of Network/Host and enter `0.0.0.0`. The static routing entry sets up a default route that points to the ISP. Leave all other settings at their defaults values.

- Unnumbered single point-to-point—This type of connection does not use an IP address for either end of the WAN link. No IP address is bound to the WAN interface. Instead, it is bound to the local NIC in the routing software. The local IP address bound to the NIC is on a network different from the one that the remote IP address of the ISP is on. Sample ISP-provided addresses follow:

  Local IP addresses: 150.3.56.64 through 150.3.56.95 (subnet mask 255.255.255.224)

  Remote IP address: 137.65.45.19 (subnet mask 255.255.255.240)

  Because the local and remote IP addresses for the WAN link are in different networks, you must use an unnumbered WAN link. Bind the local address (or the first address in a block of addresses) to the local NIC.

  To configure an unnumbered single point-to-point connection, load NIASCFG and select Configure NIAS > Protocols and Routing > Bindings. Press Ins to add a new binding. Select TCP/IP and then select the WAN interface set up previously. For WAN Network Mode, select Unnumbered Single Point-to-Point, then select WAN Call Destination and press Ins. Press Enter and select the WAN call destination defined earlier. Press Enter on Static Routing Table and press Ins to add a new static route. Under Route to Network or Host, select Network for the IP Address of Network/Host and enter `0.0.0.0`. The static routing entry sets up a default route that points to the ISP. Leave all other settings at their default values.

- After you have completed the setup, reinitialize your system and test the WAN link. Load CALLMGR.NLM at the server console. For a permanent link, the call should come up automatically with a status of Out-Connecting, then Out-Connected. A console message appears stating that an IP connection was established to the WAN call destination. For an on-demand link, bring up the link manually. Press Ins , select WAN Call Destination, and select IP. The status should show Out-Connecting, then Out-Connected. A console message appears stating that an IP connection was established to the WAN call destination. Load PING.NLM at the server console and enter the IP address of the ISP. Press Esc to begin the ping. Packets should be sent and received. The IP clients connected to the LAN side of the routing software server should also be able to access the Internet through the router's WAN link.
- To route IPX over a WAN, you must always bind IPX to a WAN board.

- You can define only one WAN call destination for all protocols going to the same destination. Each protocol can use the same WAN call destination name when it is bound to the WAN interface.
- When routing IPX or AppleTalk over a permanent PPP link, you must specify the permanent WAN call destination under Bindings on only one side of the WAN connection (the originating side).
- When routing AppleTalk or IPX over an on-demand PPP link, you must specify a WAN call destination in the static routes or static services configuration on both sides of the WAN connection (parameter path: Select Configure NIAS > Protocols and Routing > Bindings > a specific binding > WAN Call Destination > Static Routes).
- When using IP RIP over a WAN in Multi-Access mode, you must configure at least one neighbor in the Neighbor List option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Bindings > Select a specific TCP/IP binding > Expert TCP/IP Bind Options/RIP Bind Options).
- When configuring source route bridging over a WAN, make sure that you enable and configure the route end station on all WAN ports that allow clients to access the NetWare file server. If the node is a dedicated router, the route end station is not required.
- When you are routing or source route bridging over NetWare Link/PPP, you must configure a WAN call destination.
- If your DCE device (DSU/CSU, modem, multiplexer, and so on) has both single and dual clocking configuration options, make sure you configure your DCE to provide both transmit and receive clocks when a Synchronous/+ or NW2000 board is being used.

Troubleshooting Checkpoints

This topic contains the following sections:

- Isolating NetWare Link/PPP Problems
- Verify the Proper Setup of Connecting Hardware
- Verify that the Modem is Set Up Properly for Initialization
- Verify Your Interface Speed
- Verify that the Modem Initialized Properly
- Create or Change a Modem Script

Isolating NetWare Link/PPP Problems

To isolate and resolve problems with NetWare Link/PPP, complete the following steps:

1. Check the Status option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select a port) to verify that the port is enabled.
2. For ports configured as ISDN connections, verify that the ISDN address and the ISDN subaddress entered for the interface are correct.
3. Verify that the Inbound Call Processing option is enabled in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > Authentication Options).
4. Verify that the WAN board driver and PPPTSM are loaded by reading the CONSOLE.LOG file. You can also enter **`modules`** at the console prompt. The system returns the names of modules that are loaded.
5. Verify that the desired protocols are bound to the WAN interface by entering **`CONFIG`** at the server prompt.
6. Use MONITOR to verify that LCP and the appropriate NCP (IPCP, IPXCP, ATCP, or BRIDGECP) are running. Select the appropriate interface under LAN/WAN Information and look under the custom statistics to verify that the desired NCP is in state 9 (Open).
7. Verify your software configuration with back-to-back testing, as described in Back-to-Back Testing in the *Overview* documentation. If the test is successful, the interfaces are ready for use.
8. Verify that the hardware is set up properly, as described in "Verify the Proper Setup of Connecting Hardware."
9. Verify that the modem is set up properly for initialization, as described in "Verify that the Modem is Set Up Properly for Initialization."
10. Verify that the modem initialized properly, as described in "Verify that the Modem Initialized Properly."

Verify the Proper Setup of Connecting Hardware

This section lists checkpoints for the hardware required for both on-demand connections (modems) and permanent connections (crossover cables, modem eliminators, or leased lines).

For Modems

To verify connections that use modems, complete the following steps:

1. Verify that the modem is receiving power.
   - Verify that the power switch on the modem is turned to the On position.
   - Verify that the power cord is properly connected to both a reliable source of power and the modem.
   - Verify that you are using the correct power cord. Many modems have power cords that are physically interchangeable, but not electrically. If you think the power cord is correct, but the lights on the modem do not come on, check that the voltage and amperage (sometimes listed on the power cord) exactly match the specifications listed on the modem or in the modem manual.
2. Check the phone cables.
   - Verify that the phone line has a dial tone by plugging a telephone line into the phone line and listening through the headset. If you cannot hear a dial tone, use a valid line or contact your phone service provider to fix the line.
   - Verify that the phone cord is plugged into the modem in the Line or Telco slot, not the Phone or Telset slot.
   - Verify that the phone cable is plugged in securely and that the connector is not broken.
3. Check the cables to the WAN board.
   - Verify that the WAN board (Synchronous/+, NW2000, and so on) is properly connected to the modem. Tighten the connectors.
   - Verify that there are no damaged pins on either end of the cable. If the cable is damaged in any way, replace it.
   - Verify that you are using the correct cables. Rev. D and Rev. E of the Synchronous/+ boards use different cables. Check all cables using a null modem.
   - For the NW2000 board, verify that the V.35 jumper on the board is closed if you are using a V.35 cable and open if you are using any other type of cable (such as RS-232).

For Permanent Links

To verify connections that use permanent links connected by crossover cables, modem eliminators, or leased lines, complete the following steps:

1. Verify that both Data Set Ready (DSR) and Data Carrier Detect (DCD) signals are active.

   There might be lights for these signals on the devices indicating that the signals are active. If the signals are active, go to Step 6. Otherwise, continue with the next step.

2. Load MONITOR at the NetWare console.

3. Select the LAN/WAN Information option and select the appropriate WAN port.

   This unique address is displayed in the window that appears after the interface is selected in MONITOR. To determine the node address that is assigned to a specific port, enter **`CONFIG`** at the NetWare console and look at the node address listed below the desired port. The LSL board number, which is the first four digits of the node number, can also be used to identify the port.

4. Check that the DCE Signal - DSR statistic is in state 1 and the DCE Signal - DCD option is in state 0 before the call is initiated.

   After the call is made, DCD should be in state 1.

5. For synchronous ports, verify that a clock is supplied.

   Crossover cables used with synchronous ports require that the transmit clock is generated internally. Typically, the transmit clocks for modems, DSU/CSUs, and modem eliminators are supplied by the DCE device.

6. Verify that the PPP port is not connected to an X.25 or frame relay network access point.

   In such a case, the driver is functional, but PPP receives invalid frames. PPP discards these frames, and the frames sent by PPP are also discarded by the switch.

7. Verify that the crossover cable cross-connects the signals, as described in Back-to-Back Testing in the *Overview* documentation.

For Outgoing Calls

To verify connections for outgoing calls that use permanent links connected by crossover cables, modem eliminators, or leased lines, complete the following steps:

1. Load NIASCFG to verify that the WAN call destination record has the correct phone number (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > Selected LAN/WAN Driver).

   Calls going through a PBX might require a 9 dialed first.

2. For calls dialed from a phone line within the same PBX, verify whether only the extension is required.

3. For a call made in Data Terminal Ready (DTR) Dialed mode (the modem dials the preconfigured number), pulse dialing is generally required.

   Usually, an internal PBX does not support pulse dialing. If this is the case, use an outside line.

4. For calls dialed from an external line to an extension on an internal PBX, verify that the extension can be reached without the intervention of an operator.

Verify that the Modem is Set Up Properly for Initialization

If you are using AT commands and your modem is not DTR controlled, you must specify the type of modem attached to the port in the Modem/DCE Device field when you configure a port through NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces). This option selects a modem initialization script that is stored as an .MDC file in the SYS:SYSTEM\ directory. For information on these files and the modem vendors to which they correspond, refer to Table 15 on page 168.

These initialization scripts are sent to the corresponding modem under the following circumstances:

- The router is restarted.
- PPPCON issues a RESET MODEM command to that port.
- A call is terminated.
- A REINITIALIZE SYSTEM command is entered at the console or issued by NIASCFG after a WAN board parameter or critical network interface parameter is changed.

For an initialization script to work, several elements must be set up properly. To verify the modem setup, complete the following steps:

1. Verify that the correct cables are attached to the modem.

   - The correct power cable must be plugged into a reliable power source and into the modem.
   - The correct cable from a WAN board in the router must be connected firmly to the modem. Screw the cable in tightly. Make sure the number on the cable matches the number of the port you configured in NIASCFG under Network Interfaces. If the cables are not numbered, put labels on them.
   - A phone line must be attached to the Line or Telco port of the modem. The phone port is for an auxiliary phone and is not used for modem calls.

2. Specify the correct modem in the Modem/DCE Device type (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > a specific PPP interface > Modem/DCE type).

   If you specify the wrong modem or neglect to specify a modem, it is *very* unlikely that the modem will initialize correctly. Look on the front of the modem or underneath for the model number. If there is no exact match, select a simpler modem from the same manufacturer.

   If you have a modem that is not supported in the list of modems in the Modem/DCE Device types, try Hayes compatible for a short-term solution. Also, refer to the WWW location http://support.novell.com.

   In the long term, it is better to create your own modem script. Refer to "Create or Change a Modem Script" on page 168 for details.

3. Verify that the interface speed configured in NIASCFG is accepted by the modem (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > a specific PPP interface > Interface Speed).

   Use the highest interface speed your modem supports without excessive CRC errors. Refer to the modem manual to determine the supported interface speeds. Often this information is difficult to find; therefore, experimenting with different values might be the easiest way to determine the supported interface speeds. Follow the instructions in "Verify Your Interface Speed."

4. For a port using the WHSMAIO (WAN HSM™ [Hardware Specific Module™] Asynchronous Input/Output) driver, verify that the Interface

Speed option is set to a speed that the board's UART is capable of handling.

For example, if you are using AIOCOMX, one of the last lines displayed during initialization states the speed, in bps, that is acceptable to the UART. For the 16450 UART, this rate is 2,400 bps. Therefore, if you use an interface speed greater than 2,400 with a 16450 UART, the WHSMAIO driver does not load. To determine which UART is in your PC, enter **LOAD AIOCOMX** at the console. If AIOCOMX is already loaded, enter **UNLOAD AIOCOMX** at the console prompt and then load it again.

If the modem does not initialize properly after you have completed this procedure, the initialization script might be the source of the problem and you must create your own script. Refer to "Create or Change a Modem Script" on page 168 for details.

Verify Your Interface Speed

To verify that you are using the correct interface speed, complete the following steps:

1. Change the interface speed in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > a specific PPP interface > Interface Speed).
2. Restart the server or issue the REINITIALIZE SYSTEM command from the console or NIASCFG.
3. Watch the initialization in PPPTRACE to verify that the interface speed is acceptable.

   If the modem replies OK after the issuance of each AT command from PPP, the speed is probably correct.
4. If you are still uncertain about the interface speed, or if the modem replied OK after a large group of AT commands, decrease the interface speed and repeat Step 2 and Step 3. Keep the following points in mind:

   Most modems *require* that the interface speed be the same on both ends of the connection.

   Some modems (those without automatic speed buffering or connect speed functionality) require that the Interface Speed option be the same as the connect speed. To check the connect speed, watch in PPPTRACE as a connection is made. This speed can change between (or during) calls, according to the quality of the phone lines.

If you are using a high-speed WAN board (such as Synchronous/+ or NW2000) and the modem accepts only a low interface speed (4,800 or lower), the performance is poor. The best solution is to use a faster modem. However, even with fast modems, bad phone lines cause low connect speeds.

Verify that the Modem Initialized Properly

To verify that the modem initialized properly, complete the following steps:

1. Verify that the AA light on the front panel of the modem is on.

   This is generally, but not always, an indication that the initialization script worked. Most, but not all, modems have this light. If this light is on, the initialization script probably worked and the modem should function properly.

   The first commands sent by the router are a <CR> and +++ATE1H0. DTR is then toggled on the modem. After the +++ATE1H0 command, the modem should issue the response <CR><LF> OK<CR><LF> or OK<CR><LF>.

2. Verify that the modem issued the OK response.

   If this OK response is not sent by the modem and the modem has been set up properly, as described in "Verify that the Modem is Set Up Properly for Initialization" on page 164 the modem might be the source of the problem.

   If you have another modem of the same type, try using it. If it works, then the first modem was faulty. You can also use a communications package to check whether the modem is functional.

3. If the modem returns OK to the +++ATE1H0 command at a given interface speed, you must verify that the commands sent to the modem are understood by the modem.

4. When a line of commands is sent, there should be a response for every few lines sent.

   If there is no response, the interface speed might be too high. If there is still no response at the lowest interface speed, recheck the modem setup. If you cannot resolve the problem, try a different modem.

5. If you see a receive line that has an ERROR response, one of the settings in that line is not understood by the modem. Here is an example:

   ```
   snd     ATE0N1Q0V1X4&C1&D2&Q5&U0&K0&L0&R0
   ```

```
rcv     ERROR
```

To correct this error, refer to the modem manual to find out which command is not supported by the modem. In the previous example, the &U0 command was not in the manual and was not supported by this modem. In some cases, an update from the manufacturer might be required to support this parameter. Decide whether you want to get an update or omit the parameter and continue. If you choose to omit the parameter, follow the instructions described in "Create or Change a Modem Script."

6 The routing software requires that the modem raise a DSR signal.

If the modem does not raise this signal, the initialization script appears to finish successfully, but any calls originated from this interface go into an Out-Queued state in CALLMGR and are never made. You can simulate a DSR signal by setting the Simulate DSR option in NIASCFG to Yes (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > Physical Options). Alternatively, you can use the AT&S0 command to force the modem to raise DSR. However, this command is not supported by all modems. To send this command to the modem, follow these instructions:

- Verify that the Dialing Mode option in NIASCFG is set to AT Commands (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > Modem/DCE Options).
- In Initialization String #1, put in the command that you want to send to the modem after the regular initialization script has finished. In this case, enter **`AT&S0`** to force the modem to raise DSR. Some modems have DIP switches that control DSR. These DIP switches are explained in the manual that came with the modem. If your modem does not have DIP switches and does not support the AT&S0 command, follow the instructions in "Create or Change a Modem Script." Append the string NODSR after the modem name.

Create or Change a Modem Script

When you configure a port through the Network Interfaces option in NIASCFG, you must specify the type of modem attached to the port in the Modem/DCE Device field. This option selects a modem initialization script that is stored as an .MDC file in the SYS:SYSTEM\ directory. Table 15 lists the modem script files in this directory.

Table 15 Modem Script Files

Modem Script File	Contents
NIASMDM1.MDC	Modem script files for vendor names beginning with A through L.
NIASMDM2.MDC	Modem script files for vendor names beginning with M through Z.
NIASCERT.MDC	Novell-certified modem script files.

You can use the new Windows-based modem script tool WMDMMGR to edit these script files or to create new modem scripts.

To Change a Modem Script

The following is an example of an error resulting from the execution of a sample modem script.

```
snd     ATE0N1Q0V1X4&C1&D2&Q5&U0&K0&L0&R0
rcv     ERROR
```

In this example, the &U0 command is not supported by the modem; therefore, the following steps must be completed to correct the script:

1. Copy the modem script from SYS:SYSTEM to another location to make modifications.
2. Start the Windows-based program WMDMMGR.
3. Select File > Open, then select the modem script file containing the modem definition.
4. Select the modem script containing the &UO command and make modifications.
5. Select File > Save, then copy the updated file back to SYS:SYSTEM.
6. Enter **`REINITIALIZE SYSTEM`** to reload the new script.
7. Try to initialize the modem again with PPPCON, then use PPPTRACE to determine whether the new script worked.

Common Problems

This topic discusses the following common problems and their associated solutions:

- WAN link does not come up or immediately disconnects.
- The trace is blank.
- The link is established but then is disconnected.
- On-demand link is not dropped.
- On-demand link from an IP or IPX workstation is not working.
- Connection can be made only through CALLMGR.NLM.
- Synchronous connections do not connect.
- Asynchronous connections do not connect.
- Authentication error messages are received.
- Remote system ID already exists.
- LCP failure has occurred.
- Incoming call is rejected.
- Link goes up and down often.
- PPPTRACE does not show packets.
- Connection to a third-party PPP is dropped.
- ISDN layer does not come up or ISDN layer goes down.
- ISDN interface fails to connect.
- Driver does not load.
- CRC errors are excessive.
- DTR dialing does not work.
- DSR and DCD serial signals are incorrect.
- IPCP has failed.
- LAPB or data compression problems occur.
- Cables are incorrect.
- Remote system ID is duplicated.
- Workstation connection problems occur.
- Permanent WAN connection attempts to reestablish the link.
- Connections are established but certain types of data are not being forwarded.

- Data is sent but not received.

WAN link does not come up or immediately disconnects.

Load CALLMGR.NLM and manually try to initiate a call. Press Ins , select WAN Call Destination, then select IP. Check the Status column for the call.

If the status is Out-Queued, this means that the Novell Internet Access Server 4.1 server cannot communicate with the interface. If you are using a modem, check the physical connections and board and driver settings. For leased lines, make sure the DSU/CSU is set up correctly and all connections are working. Check the console log to make sure that the drivers for the board are loaded properly.

If the status is Out-Connecting and then Out-Disconnect, this indicates that a physical connection was established to the ISP; however, PPP did not successfully negotiate, so the call was disconnected. Load PPPTRACE.NLM and select Real-Time Monitor. Initiate the call with CALLMGR and then toggle back to PPPRTRACE by pressing Ctrl+Esc.

Both send (Snd) and receive (Rec) data should appear as PPP traffic before the IP connection is negotiated. If you see only send data and no receive data, the other side is not responding to the PPP requests. You might need to set up a login script, or the ISP might not be set up for PPP. Typically, you will see both send and receive data in the form of Configuration Requests (CnfgReq), Configuration Acknowledgments (CnfgAck), and Configuration Rejection (CnfgRej). You might also see other protocol-specific packets. Eventually, when the link terminates, you will see a Terminate Request (TermReq) and then a Terminate Acknowledge (TermAck). By viewing the negotiation exchange in PPPTRACE, you might be able to see where the negotiation fails. When the link terminates, a message appears on the system console stating why the link was terminated. For a more detailed explanation of the error message, refer to Novell Internet Access Server 4.1 Messages. The message often points you directly to the solution of the problem. Common causes for negotiation failure include incorrect PAP or CHAP negotiation, or incorrect setup of IP addresses for the connection.

The trace is blank.

If the trace is blank (no data), load MONITOR and select LAN/WAN Information. Check the Data Send Ready (DSR) value.

If the DSR is set to 0, the modem might not raise DSR. Load PPPCON to verify that the DSR is set to Off (parameter path: Select PPP Interfaces >

Serial Interface). Load NIASCFG to set the Simulate DSR option to Yes (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > Physical Options). Restart the server or issue the REINITIALIZE SYSTEM command.

The link is established but then is disconnected.

Use the Real-time Monitor option to generate a trace. If several packets appear and then the link is disconnected, verify that there is only one source of clocking between the routing software and any CSU/DSUs. Also, ensure that the router interface speed settings on the routers match.

In addition, verify that Outgoing Authentication in WAN Call Destination specifies the same authorization protocol that is configured on the remote side. You might need to load NIASCFG and select Configure NIAS > Protocols and Routing > Network Interfaces > PPP card option to set the Inbound Authentication option on both routers to None.

On-demand link is not dropped.

Load PPPTRACE and select Real-time Monitor to verify that data is being sent and received, then complete the following steps:

1. Ensure that Time Synchronization and NDS Synchronization are configured for on-demand links.
2. If the on-demand link is also configured for routing IP, ensure that RIP is disabled on the WAN interfaces.

   Continue with the following steps if the ManageWise® software is installed in your environment.
3. Close all ManageWise windows that are polling an agent when they are no longer needed. Also, ensure that the network segments are not being monitored unnecessarily.
4. Run the NetExplorer™ software during nonbusiness hours, or configure a NetExplorer server at each site and use IPX and IP scoping in NXPCON to limit the discovery to networks that are not across the on-demand link.
5. Limit the number of alarms sent across the on-demand link. For servers running the NetWare Management Agent™ software, the NWTRAP.CFG file can be configured to transmit only critical alarms.

On-demand link from an IP or IPX workstation is not working.

Load CALLMGR.NLM and verify the link connection. If the link is up, enter **`DISPLAY SERVICES`** at the server console to view the available services. Load STATICOM.NLM to automatically create static routes and services.

Connection can be made only through CALLMGR.NLM.

Load NIASCFG and check the Physical Type option (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces). Change this setting to the correct physical type.

Synchronous connections do not connect.

- A synchronous connection does not connect, and the following console message appears:

  ```
  LCP is down: **Maximum reached for Configure-Request
    retries - remote rejected the call**.
  ```

  Cause 1— Data Encoding option does not match on both ends of the link.

  Change the Data Encoding option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Physical Options) to be the same on both ends of the link. For example, a port with the Data Encoding option set to NRZI connects only to another port with the Data Encoding option set to NRZI.

  Restart the server or issue the REINITIALIZE SYSTEM command.

  CALLMGR shows Out-Connecting status until the connection attempt times out.

  Cause 2— Physical Type (V.35, RS-232, and others) was configured incorrectly.

  Configure the correct type in the Physical Type option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Physical Type).

  Restart the server or issue the REINITIALIZE SYSTEM command.

- A synchronous connection does not connect.
  - Set the Interface Speed option to External on both ends of the PPP link.

- Verify that the connecting device is supplying a clock. Refer to the documentation provided by the manufacturer of the connecting device.

NOTE: Make sure that both ends of the synchronous PPP connection have been configured to use external clocking. Otherwise, one end operates in synchronous mode and the other end operates in asynchronous mode. This causes the PPP link to fail to connect.

Asynchronous connections do not connect.

- An asynchronous connection does not connect, and the following console message appears:

  ```
  Could not make WAN connection to call_name  on interface
    interface_name. Call is rejected by the remote WAN node,
    or the media failed.
  ```

  Cause 1— Physical Type option is configured incorrectly.

  Configure the correct type in NIASCFG for both ends of the connection (parameter path: Configure NIAS > Select Protocols and Routing > Network Interfaces > select an interface >Physical Type).

  Restart the server or issue the REINITIALIZE SYSTEM command.

  Cause 2— Inbound Call Processing option is disabled on the receiving end.

  At the called router, change the Inbound Call Processing option to Enabled in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Authentication Options).

  Restart the server or issue the REINITIALIZE SYSTEM command.

- A connection does not connect, and the following console message appears:

  ```
  Could not make WAN connection to call_name  on interface
    interface_name. Call is rejected by the remote WAN node,
    or the media failed.
  ```

  On the called router, the following message appears:

  ```
  **Peer rejected authentication negotiation.**
  ```

  On the router originating the call, change the Outbound Authentication option to Either PAP or CHAP in NIASCFG under WAN Call Directory. On the router receiving the call, make entries in the Local System ID and Password fields of the calling router in NIASCFG (parameter path: Select

Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Authentication Options > Inbound Authentication). The Password and Local System ID fields are case-sensitive. Restart the server or issue the REINITIALIZE SYSTEM command.

- The answering modem answered, but it did not connect.

  Check in PPPTRACE for the LCP data that was sent and the generated responses. If you are using a slow link, increase the Response Timeout in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Timeouts & Retries).

- Both modems call each other, but neither connect.

  There is a call collision. Static routes or permanent WAN call destinations are configured on both routers, and both routers are attempting to set up the call at the same time. Using CALLMGR at the router making the call, delete the call by pressing Del or speed up the retry by pressing F3. If you do not delete the call manually in CALLMGR by pressing Del , the retry mechanism eventually connects the calls.

- The calling modem rings and rings, but the call is never answered.

  Cause 1— Interface on the receiving end is disabled.

  In NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces), press Tab on the desired interface to toggle the status to Enabled.

  Issue the REINITIALIZE SYSTEM command.

  Cause 2 —Wrong phone number is being dialed.

  - Make sure the phone line is attached to the plug marked Line or Telco on each modem.
  - On the answering modem, check that the AA light is on. When the calling modem rings, check that the OH (off-hook) light is turned on for both modems.
  - If the OH light of the answering modem stays on, then refer to the problem discussed in The answering modem answered, but it did not connect.
  - If the OH light does not go on, check that the phone number being dialed at the calling modem is correct.

- If you think the phone number is correct, try attaching a regular phone on the answering end. Check for a dial tone, then verify that the phone rings after the calling modem dials.
- If the phone does not ring, the phone number is incorrect.
- If the phone rings, try the solution for the problem discussed in *Cause 3*—Answering modem is not properly configured.

Cause 3— Answering modem is not properly configured.

- If the answering modem has an AA light, verify that this light is on.
- If the AA light is not on or if there is no AA light on the modem, verify that the modem initialization script is valid, as described in "Verify that the Modem Initialized Properly."
- If the modem script is valid, then try another modem.

- All calls on that port go into Out-Queued state and never get made.

  Cause 1— Outgoing phone line has no dial tone or is in the wrong plug.

  Follow the procedures in "Verify the Proper Setup of Connecting Hardware."

  Cause 2— In CALLMGR, the outgoing call shows a status of Out-Queued and the status does not change.

  - If DSR = 0 in MONITOR, it is possible that the modem does not raise DSR. PPPCON also shows DSR = Off (parameter path: Select Configure NIAS > Protocols and Routing > PPP Interfaces > Serial Interface Information). Set the Simulate DSR option in NIASCFG to Yes (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > Physical Options). Issue the REINITIALIZE SYSTEM command.
  - If the problem continues, you can force a modem to raise DSR by using the AT&S0 command. Specify this in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Bindings > a specific binding > Modem/DCE Options > Initialization String #1). After saving the new configuration, either restart the server or issue the REINITIALIZE SYSTEM command. If your modem does not support the AT&S0 command, it might have DIP switches that control DSR. These DIP switches are explained in the manual that came with the modem. If your modem does not have DIP switches and does not support the AT&S0 command, follow the instructions

in "Create or Change a Modem Script." For additional information, refer to the modem's documentation.

- If you use the AT&S0 command, watch in PPPTRACE to verify that the command is accepted by the modem. Not all modems understand this command.

  If the problem continues, check the modem manual for a listing of DIP switch settings. Sometimes there is a switch setting to raise DSR.

- If the problem continues, try another modem. The routing software does not make a call unless DSR = 1. Load PPPCON to verify that DSR = On (parameter path: Select PPP Interface > select an interface > Serial Interface Information).

- If the problem continues, check for problems with DSR, as described in DSR and DCD serial signals are incorrect.

Cause 3— The modem answered, but it did not connect.

Watch the LCP negotiation using PPPTRACE. If any error messages are displayed on either console, refer to Novell Internet Access Server 4.1 Messages for information about the appropriate solutions. If PPPTRACE only shows Send packets, check the interface speed, as described in "Verify Your Interface Speed."

- Two routers cannot connect through a modem.

  If two routers are connected through a modem with servers on either side of the network and the routers have been set up for on-demand calls, you can set up a static route to the remote server on the local router to attempt to establish a connection. Use one of the following methods to set up a static route.

  - Load NIASCFG and select Configure NIAS > Protocols and Routing > Protocol > IPX > Static Services for On-demand Calls and Protocol > IPX. Select Static Routes for On-demand Calls to specify the proper services and internal IPX number for the remote server.

  - Load NIASCFG and select Configure NIAS > Protocols and Routing > Manage Configuration > Configure SNMP > Configure SNMP Information > Configure SNMP Parameters. Ensure that the Monitor State is set to Any Community May Read and the Control State is set to Any Community May Write. Load STATICON and select Configure Local Static Services > Configure Local Static Routes to set up one static service and routing entry for the remote router in the

local router tables. Load CALLMGR and connect to the remote router. Select Dynamically Configure Static Routing Table > Autoconfigure Local and Remote Routing Tables. This option updates the service and routing table of both routers to include all the services and routing entries for the entire network.

Authentication error messages are received.

- A connection is not established, and the following console message appears:

  ```
  Could not make WAN connection to call_name  on interface
    interface_name. Call is rejected by the remote WAN node,
    or the media failed.
  ```

  On the called router, the following message appears:

  ```
  **Illegal peer ID/Password in the Authenticate-Request
    packet.**
  ```

  The entries in the Inbound Authentication Database and the WAN Call Directory do not match. On the calling end, verify that the Password and Local System ID (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > entry for the affected call) are entered exactly the same as in the Inbound Authentication Database (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Authentication Options) of the called router. The Password and System ID fields are case-sensitive.

- A call does not connect, and the following console message appears:

  ```
  Could not make WAN connection to call_name  on interface
    interface_name. Call is rejected by the remote WAN node,
    or the media failed.
  ```

  On the called router, the following message appears:

  ```
  **Peer rejected authentication negotiation.**
  ```

  The outbound authentication protocol and inbound authentication protocol do not match. On the calling end, verify that the Outbound Authentication option (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > select an interface > entry for the affected call > Outbound Authentication Option) matches the Inbound Authentication option on the receiving interface (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > Authentication Options) of the called router.

Remote system ID already exists.

CALLMGR displays the following message:

```
A call could not be established. See the console messages for
  further information.
```

The console message states the following:

```
Will not make WAN Connection to call_name. A connection to
  that remote WAN node Remote System ID  already exists.
```

The remote system ID is duplicated on two WAN calls. If you require two active calls between two machines running the routing software, specify a unique remote system ID for each call in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > select an interface).

LCP failure has occurred.

PPPTRACE shows that there is an LCP failure.

The PPP negotiated parameters are not configured properly. In NIASCFG, verify that the MRU Maximum Size and MRU Minimum Size for both routers are in a range in which an MRU can be negotiated (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Negotiation Options).

Incoming call is rejected.

The following error message is displayed on the NetWare console of the Novell Internet Access Server 4.1 routing software receiving the call:

```
An incoming call for protocol protocol  on interface
  interface_name  was rejected. Check Protocol binding to
  interface.
```

The protocol specified in the incoming call is not bound to the port on which this call has been accepted. Bind the protocol to the port and issue the REINITIALIZE SYSTEM command. Enter the CONFIG command at the NetWare console and verify that the desired protocol is now bound to the port. To find out the protocol, use PPPTRACE to see the incoming NCP Configure-Request packets.

Link goes up and down often.

An on-demand link goes up and down too often.

The Idle Link Timeout value is too short. The console of the router making the call displays the following message:

```
Link termination due to inactivity.
```

Load NIASCFG to increase the Idle Connection Timeout value (parameter path: Select Configure NIAS > Protocols and Routing > WAN Call Directory > select an interface).

PPPTRACE does not show packets.

- PPPTRACE Real-Time Monitor does not show any packets.

  Cause 1 —Window is not displaying the correct interface.

  Press F2 to change interfaces until the desired interface is displayed.

  Cause 2— No data is being sent on the interface.

  Send some data.

- PPPTRACE Real-Time Monitor does not show all the packets.

  PPPTRACE cannot show all packets in Real Time-Monitor. Use F7 to save the packets, then use the Play Back window to display them.

Connection to a third-party PPP is dropped.

The connection to a third-party PPP implementation is being dropped after it has been established for a few minutes.

Link quality monitoring is not supported in Novell Internet Access Server 4.1. Disable link quality monitoring in the third-party implementation of PPP. Alternatively, if a third-party implementation supports using Echoes as the link quality monitoring method, use Echoes.

ISDN layer does not come up or ISDN layer goes down.

- The ISDN layer does not come up.

  Observe the lights on the NT1.

  If the Terminal Error light is on, this indicates a local problem. Refer to Cause 1 and, if necessary, Cause 2.

  If the Line Error light is on, this indicates a network problem. Refer to Cause 3.

  Cause 1 —There is a problem with the cable from the ISDN adapter to the NT1.

Determine whether the cable from the ISDN adapter to the NT1 is undamaged and is connected properly.

Cause 2 —There is a problem with the ISDN driver.

Verify that the ISDN driver is loaded and is configured properly.

Cause 3 —There is a problem with equipment on the network side of the connection.

Report the problem to your ISP.

- The ISDN layer goes down.

  Observe the lights on the NT1.

  If the Line Error light is on, this indicates a network problem. Refer to Cause 1.

  If the Terminal Error light is on, this indicates a local problem. Refer to Cause 2 and, if necessary, Cause 3.

  Cause 1 —There is a problem with equipment on the network side of the connection.

  Report the problem to your ISP.

  Cause 2 —There is a problem with the cable from the ISDN adapter to the NT1.

  Determine whether the cable from the ISDN adapter to the NT1 is undamaged and is connected properly.

  Cause 3 —There is a problem with the ISDN driver.

  Verify that the ISDN driver is loaded and is configured properly.

ISDN interface fails to connect.

An ISDN interface fails to connect. You can determine whether the AT command for dialing out failed by using PPPTRACE.

Cause 1— The receiving end rejects the call after the CONNECT_IND message is received.

- Load CAPITRCE on both routers and use CALLMGR to make a call. After the CONNECT_IND message is received and the call is rejected by the receiving end, stop CAPITRCE and convert the captured trace to ASCII format.

- Verify that the ISDN address and subaddress for this interface match those provided by the CONNECT_IND message.

Cause 2— The receiving end does not receive the CONNECT_IND message.

- Load CAPITRCE on both routers and use CALLMGR to make a call. Watch the trace to determine whether a CONNECT_IND message is received. You might need to stop CAPITRCE and convert the captured trace to ASCII format to verify that no CONNECT_IND message was received.
- Verify that the ISDN driver is configured correctly. Verify that the service profile ID (SPID) at both ends of the connection match.

Driver does not load.

- CALLMGR displays the following message:

```
A call could not be initiated because the selected
  interface is not loaded or is not bound to the selected
  protocol.
```

Cause 1— WAN driver did not load.

- Check in NIASCFG for the messages displayed when the driver is loaded (parameter path: Select Configure NIAS > Protocols and Routing > View Configuration > Console Messages).
- Correct any conflicts with memory, I/O port, or interrupts.
- Verify that the WAN board driver (for example, NW2000.LAN) exists in SYS:SYSTEM and is not corrupt. Use the DOS COMP command to verify that the driver is valid. Check for out-of-memory conditions that prevent the driver from loading.

Cause 2— PPPTSM did not load.

- Check in NIASCFG for the messages displayed when PPPTSM is loaded (parameter path: Select Configure NIAS > Protocols and Routing > View Configuration > Console Messages). PPPTSM automatically loads several other modules. If these modules do not exist, PPPTSM does not load.
- Verify that PPPTSM exists in SYS:SYSTEM, load MODULES on the server console to display version information, and ensure that the version is correct.
- Use the DOS COMP command to verify that the driver is valid.

- Check for out-of-memory conditions that prevent PPPTSM from loading.

Cause 3 —LAN protocol was not bound to the outgoing interface.

Bind the desired protocol to the port (network interface) on the WAN board from which the call will be made.

Cause 4 —Outgoing PPP port is disabled.

- In NIASCFG, select Configure NIAS > Protocols and Routing > Network Interface, then press Tab on the desired interface to toggle the status to Enabled.
- Issue the REINITIALIZE SYSTEM command.

- When NIASCFG is loading, the following message is displayed:

```
Cannot recognize driver driver_name. Disabled boards for
  this driver. Delete board or install and reenable
  boards.
```

The driver file does not exist in SYS:SYSTEM. Verify that the WAN board driver (for example, NW2000.LAN) exists in SYS:SYSTEM and is not corrupt. Use the DOS COMP command to verify that the driver is valid.

- WHSMAIO driver did not load. The following message appears:

```
AIO FAILURE: data bit rate not supported. Fatal error:
  Unable to initialize AIO Board.
```

The interface speed specified in NIASCFG for the WHSMAIO interface is too high. Decrease the Interface Speed option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface) and issue the REINITIALIZE SYSTEM command.

CRC errors are excessive.

MONITOR shows many CRC errors.

CRC errors indicate either noise on the phone line or a mismatched interface speed. Check the Interface Speed option in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface) on both sides of the connection. Usually, this speed should match. If matching the interface speed does not improve the number of CRC errors, the phone lines or the modems might be at fault. Use modems of the same

type, or at least from the same vendor. Use different phone lines if you can. Complete the steps in "Verify Your Interface Speed."

NOTE: High values for the Receive CRC Errors and Receive Aborts statistics are normal if the Dialing Mode parameter is set to V.25bis.

DTR dialing does not work.

- The modem is not dialing.

  The modem is not configured properly for DTR dialing mode. Make sure the modem is configured for DTR dialing by verifying the positions of the DIP switches. For some modems, the DTR dialing mode can be set on the front panel. Consult the modem operation manual. Use MONITOR to monitor the DTR signal and make sure it is changed from the OFF to ON state (0 to 1).

- The DTR dial modem goes off hook but does not dial the number.

  The modem is not preprogrammed with a phone number to be dialed, or it is programmed with the wrong phone number. Make sure that the phone number is stored correctly and is the correct number. Depending on the modem type, the preprogrammed phone number can be stored by using the front panel or by sending AT command strings. Refer to the modem operation manual. CPECFG can be used to send AT command strings to the attached modem.

DSR and DCD serial signals are incorrect.

- The state change counters for the DSR and DCD signals (in MONITOR) are updated frequently.

  Make sure that both ends of the cable are screwed in tightly.

- CALLMGR shows that a link is connected, but the link is actually not connected.

  The DSR and DCD signals are not in the correct state. Use PPPCON or MONITOR to look at the DSR and DCD signals. The DSR signal must be in state 1 and the DCD signal must be in state 0 before a call can be initiated. The ON (1) state for these two signals indicates that the connection is established. If the modem raises both DSR and DCD signals prior to the connection, disable this feature with the modem's DIP switches or use a different modem.

IPCP has failed.

An IPCP failure has occurred.

The local IP address of the router is not configured properly. Use the Bindings option in NIASCFG to make sure that the ports (network interfaces) at each end of the link are configured with IP addresses that are in the same subnet (parameter path: Select Configure NIAS > Protocols and Routing > Bindings > select an interface). The subnet masks must be identical. This topic is complex; refer to Understanding in the *TCP/IP* documentation for a complete explanation of subnet masks.

LAPB or data compression problems occur.

- MONITOR or PPPCON shows that the LAPB Retransmission counter is high.

  The LAPB T1 Retransmission Timer option is too short. Use NIASCFG to review and adjust the LAPB T1 Retransmission Timer option to a larger value.

- MONITOR or PPPCON shows that the LAPB Compression Reset counter is high.

  The connection link is not reliable. LAPB is finding transmission errors in the compressed data. Try different modems or different phone lines. Reducing the Interface Speed option might help also.

- PPP Data Compression is not working. MONITOR shows that the PPP Data Compression statistic is in state 0 when the connection is up.

  Cause 1— One end of the connection has the PPP Data Compression option set to Disabled.

  Set PPP Data Compression in NIASCFG to Enabled for the correct port on both ends of the connection (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > select an interface > Negotiation Options).

  Cause 2— The type of data compression used is not supported by another vendor's routing software.

  Novell Internet Access Server 4.1 supports the following types of data compression:

  - Predictor I
  - Predictor II

- State LZS
- Microsoft Point-to-Point Compression (MPPC)

Cables are incorrect.

Verify that you are using the correct cables. Rev. D and Rev. E of the Synchronous/+ boards use different cables. After verifying your configuration, use a null modem to check all cables as described in Back-to-Back Testing in the *Overview* documentation.

Remote system ID is duplicated.

When two or more IPX WAN connections exist between two routers, verify that the connections are not assigned the same remote system ID in the WAN Call Directory option of the originating router.

Workstation connection problems occur.

- A workstation receives an error message or timeout response while it is accessing a file server over a PPP WAN connection.
  - Use PPPCON to look at the following counters: Bad CRC, Transmit REJ, and Received REJ. If the counters are too high, there is a problem with line quality. Use a different line or contact your ISP.
  - Use MONITOR to look at the following counters: Send Packet Retry Count, Checksum Errors, LAPB Retransmission, Compression Reset, Rx Data Pkt Dropped, Receive Abort, Receive Char Frame Errors, and Receive Char out of Frame. If the counters are too high, there is a problem with line quality. Use a different line or contact your ISP. If only the LAPB Retransmission counter is high, use NIASCFG to adjust the T1 Timer value.
- A workstation takes too long to access a file server (copy file) over a PPP WAN connection.
  - Use MONITOR to verify that Data Compression is set to Enabled on all intervening routers. If it is set to Disabled on an intervening router, use NIASCFG to enable Data Compression and issue the REINITIALIZE SYSTEM command at the server console prompt.
  - Use PPPCON to check whether the T1 Timeouts counter is high. If it is, use NIASCFG to increase the value of the T1 Timer.
  - Use PPPCON to check whether the Interface Speed option is too low or too high compared to the bandwidth capacity of the modem.

Permanent WAN connection attempts to reestablish the link.

A permanent WAN call destination has the Retry Mode option set to Never Retry; however, when the link goes down, there is one attempt to reestablish the link.

This is normal operation. The Retry Mode option does not influence the operation of the network protocol stacks. Therefore, when a permanent link goes down, the network protocols make one attempt to reestablish the link.

Connections are established but certain types of data are not being forwarded.

Established links will forward most data, but the packets for certain protocols or between certain destinations are being blocked.

You have filters configured on the router. Use FILTCFG to delete the appropriate filters. In the case of backup calls, FILTCFG might not display the filters that are causing the problem. All filters for backup calls are automatically mapped from the primary call, but they are not displayed in FILTCFG. You can disable this automatic mapping by entering the FILTSRV NOBACKUP command. You must configure a remote system ID to enable filter support for backup calls. To delete a filter from a backup call, you must delete it from the primary call. You can configure additional services on a backup call by adding filters on the circuit (interface and remote system ID) that is configured in the backup call.

Data is sent but not received.

If the trace shows data being sent but not received, run a loopback test and hardware diagnostics to verify that the WAN card, cabling, and CSU/DSU devices are working.

If the loopback test between the CSU/DSU devices is successful, try configuring one of the CSUs as the clocking source. Not all telco lines provide clocking.

Load the PPP driver from NIASCFG. Configured WAN call destinations might not recognize the PPP driver loaded manually from the server console.

A Novell Trademarks

Access Manager is a registered trademark of Novell, Inc. in the United States and other countries.

Advanced NetWare is a trademark of Novell, Inc.

AlarmPro is a registered trademark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppTester is a registered service mark of Novell, Inc. in the United States and other countries.

BrainShare is a registered service mark of Novell, Inc. in the United States and other countries.

C-Worthy is a trademark of Novell, Inc.

C3PO is a trademark of Novell, Inc.

CBASIC is a registered trademark of Novell, Inc. in the United States and other countries.

Certified NetWare Administrator in Japanese and CNA-J are service marks of Novell, Inc.

Certified NetWare Engineer in Japanese and CNE-J are service marks of Novell, Inc.

Certified NetWare Instructor in Japanese and CNI-J are service marks of Novell, Inc.

Certified Novell Administrator and CNA are service marks of Novell, Inc.

Certified Novell Engineer is a trademark and CNE is a registered service mark of Novell, Inc. in the United States and other countries.

Certified Novell Salesperson is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

LAN WorkGroup is a trademark of Novell, Inc.

LAN WorkPlace is a registered trademark of Novell, Inc. in the United States and other countries.

LAN WorkShop is a trademark of Novell, Inc.

LANalyzer is a registered trademark of Novell, Inc. in the United States and other countries.

LANalyzer Agent is a trademark of Novell, Inc.

Link Support Layer and LSL are trademarks of Novell, Inc.

MacIPX is a registered trademark of Novell, Inc. in the United States and other countries.

ManageWise is a registered trademark of Novell, Inc. in the United States and other countries.

Media Support Module and MSM are trademarks of Novell, Inc.

Mirrored Server Link and MSL are trademarks of Novell, Inc.

Mobile IPX is a trademark of Novell, Inc.

Multiple Link Interface and MLI are trademarks of Novell, Inc.

Multiple Link Interface Driver and MLID are trademarks of Novell, Inc.

My World is a registered trademark of Novell, Inc. in the United States and other countries.

N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Natural Language Interface for Help is a trademark of Novell, Inc.

NDS Manager is a trademark of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE/2T is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2000T is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NE32HUB is a trademark of Novell, Inc.

NEST Autoroute is a trademark of Novell, Inc.

NetExplorer is a trademark of Novell, Inc.

NetNotes is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Link/PPP is a trademark of Novell, Inc.

NetWare Link/X.25 is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWare LU6.2 is trademark of Novell, Inc.

NetWare Management Agent is a trademark of Novell, Inc.

NetWare Management System and NMS are trademarks of Novell, Inc.

NetWare Message Handling Service and NetWare MHS are trademarks of Novell, Inc.

NetWare MHS Mailslots is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Mirrored Server Link and NMSL are trademarks of Novell, Inc.

NetWare Mobile is a trademark of Novell, Inc.

NetWare Mobile IPX is a trademark of Novell, Inc.

NetWare MultiProtocol Router and NetWare MPR are trademarks of Novell, Inc.

NetWare MultiProtocol Router Plus is a trademark of Novell, Inc.

NetWare Name Service is trademark of Novell, Inc.

NetWare Navigator is a trademark of Novell, Inc.

NetWare Peripheral Architecture is a trademark of Novell, Inc.

NetWare Print Server is a trademark of Novell, Inc.

NetWare Ready is a trademark of Novell, Inc.

NetWare Requester is a trademark of Novell, Inc.

NetWare Runtime is a trademark of Novell, Inc.

NetWare RX-Net is a trademark of Novell, Inc.

NetWare SFT is a trademark of Novell, Inc.

NetWare SFT III is a trademark of Novell, Inc.

NetWare SNA Gateway is a trademark of Novell, Inc.

NetWare SNA Links is a trademark of Novell, Inc.

NetWare SQL is a trademark of Novell, Inc.

NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.

NetWare Telephony Services is a trademark of Novell, Inc.

NetWare Tools is a trademark of Novell, Inc.

NetWare UAM is a trademark of Novell, Inc.

NetWare WAN Links is a trademark of Novell, Inc.

NetWare/IP is a trademark of Novell, Inc.

Novell Gold Partner is a service mark of Novell, Inc.

Novell Labs is a trademark of Novell, Inc.

Novell N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Novell NE/2 is a trademark of Novell, Inc.

Novell NE/2-32 is a trademark of Novell, Inc.

Novell NE3200 is a trademark of Novell, Inc.

Novell Network Registry is a service mark of Novell, Inc.

Novell Platinum Partner is a service mark of Novell, Inc.

Novell Press is a trademark of Novell, Inc.

Novell Press Logo (teeth logo) is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Replication Services is a trademark of Novell, Inc.

Novell Research Reports is a trademark of Novell, Inc.

Novell RX-Net/2 is a trademark of Novell, Inc.

Novell Service Partner is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

Novell Support Connection is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Technical Services and NTS are service marks of Novell, Inc.

Novell Technology Institute and NTI are registered service marks of Novell, Inc. in the United States and other countries.

Novell Virtual Terminal and NVT are trademarks of Novell, Inc.

Novell Web Server is a trademark of Novell, Inc.

Novell World Wide is a trademark of Novell, Inc.

NSE Online is a service mark of Novell, Inc.

NTR2000 is a trademark of Novell, Inc.

Nutcracker is a registered trademark of Novell, Inc. in the United States and other countries.

OnLAN/LAP is a registered trademark of Novell, Inc. in the United States and other countries.

OnLAN/PC is a registered trademark of Novell, Inc. in the United States and other countries.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Open Look is a registered trademark of Novell, Inc. in the United States and other countries.

Open Networking Platform is a registered trademark of Novell, Inc. in the United States and other countries.

StarLink is a registered trademark of Novell, Inc. in the United States and other countries.

Storage Management Services and SMS are trademarks of Novell, Inc.

Technical Support Alliance and TSA are collective marks of Novell, Inc.

The Fastest Way to Find the Right Word is a registered trademark of Novell, Inc. in the United States and other countries.

The Novell Network Symbol is a trademark of Novell, Inc.

Topology Specific Module and TSM are trademarks of Novell, Inc.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

Universal Component System is a registered trademark of Novell, Inc. in the United States and other countries.

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

Writer's Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

Yes, It Runs with NetWare (logo) is a trademark of Novell, Inc.

Yes, NetWare Tested and Approved (logo) is a trademark of Novell, Inc.

ZENworks is a trademark of Novell, Inc.