Novell
NetWare® 6.5

WAN OVERVIEW

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2002-2003 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,854; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,810; 6,002,398; 6,014,667; 6,016,499; 6,023,586; 6,029,247; 6,052,724; 6,061,726; 6,061,740; 6,061,743; 6,065,017; 6,081,774; 6,081,814; 6,094,672; 6,098,090; 6,105,062; 6,105,069; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,216,123; 6,219,652; 6,233,859; 6,247,149; 6,269,391; 6,286,010; 6,308,181; 6,314,520; 6,324,670; 6,338,112; 6,345,266; 6,353,898; 6,424,976; 6,466,944; 6,477,583; 6,477,648; 6,484,186; 6,496,865; 6,510,450; 6,516,325; 6,519,610; 6,532,451; 6,532,491; 6,539,381. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

WAN Overview
April 2003

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

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc in the United States and other countries.

Internetwork Packet Exchange is a trademark of Novell, Inc.

IPX is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

NetWare Loadable Module is a tademark of Novell, Inc.

NLM is a trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Cluster Services is a trademark of Novell, Inc.

Novell Directory Services is a registered trademark of Novell, Inc in United States and other countries.

NDS is a registered trademarks of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

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

Contents

About This Guide

This guide provides the information you need to configure and manage the Novell® Internet Access Server 4.1 routing software. This guide provides overall troubleshooting tips, techniques, and tools, as well as the symptoms of and solutions to commonly occurring problems for the common components of Novell Internet Access Server 4.1.

This guide is divided into the following sections:

- Chapter 1, "Setting Up," on page 5
- Chapter 3, "Troubleshooting," on page 47
- Chapter 2, "Managing," on page 25

Documentation Updates

For the most recent version of the *WAN Overview* guide, see the NetWare® 6.5 Documentation Web site (http://www.novell.com/documentation/lg/nw65).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Also, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Setting Up

The Novell® Internet Access Server 4.1 routing software offers an extensive set of configurable parameters for all supported protocols. You can use these parameters to

- Modify the default characteristics of the initial configuration
- Configure advanced features and optimize router and WAN link performance options

The initial configuration of Novell Internet Access Server 4.1 provides the basis for most routing needs. The initial configuration is based on the configured boards, the enabled and configured protocols, and the supported WAN protocol. If you followed the instructions when you installed Novell Internet Access Server 4.1, you set most protocol parameters during the initial configuration at their default values.

Configuration Overview

To configure a router to run on a LAN or a WAN, you need to perform the following tasks using the Novell Internet Access Server Configuration utility (NIASCFG):

1. Configure the LAN or WAN board.

   - For a LAN board, you only need to configure the board.
   - For a WAN board, you need to configure the board and the WAN network interfaces.

   For information about configuring LAN or WAN boards, refer to Setting Up in the *Boards* documentation.

   For information about configuring WAN network interfaces for the NetWare® Link/PPP™ software, refer to Configuring a Permanent PPP Connection in the *NetWare Link/PPP* documentation or Configuring an On-Demand PPP Connection in the *NetWare Link/PPP* documentation.

2. For a WAN link, configure the PPP WAN call destination.

   For information about setting up permanent WAN call destinations, refer to Configuring a Permanent PPP Connection in the *NetWare Link/PPP* documentation or Configuring an On-Demand PPP Connection in the *NetWare Link/PPP* documentation.

3. Configure the network protocols that will run over the LAN or WAN connection.

   - For a LAN connection, you can configure the routing protocol (for the Internetwork Packet Exchange™ [IPX™] protocol and TCP/IP protocol), tunneling (for IPX and AppleTalk*), filtering, static routes (for TCP/IP only), and other expert configurations.
   - For a WAN connection, you can configure the routing protocol (for IPX and TCP/IP), tunneling (for IPX and AppleTalk), filtering, static services or routes (for on-demand links), and other expert configurations.

4. If necessary, configure the source route bridge.

5. Bind the network protocols, or source route bridge, to the network interfaces through which you want them to connect.

Understanding Configuration

Configuring the router involves some planning and decision-making along the way. You must know the details of the network where you are placing the router, the type of connectivity you want, and the configuration details of the peers to which you are connecting the router. For example, deciding whether you need to bridge rather than route a protocol over a specific interface depends on the type of network to which you are attaching the router.

Deciding the characteristics of each protocol you are routing (or bridging) over a LAN or WAN interface is based on the topology and existing characteristics of the network. For every protocol you configure to run over a LAN or WAN link, you must determine which routing protocol to use, whether to tunnel packets, whether you need or want to configure static routes, and which type of filtering to use.

This section discusses the basic concepts you must know to make the right decisions when configuring the network protocols you want to route using Novell Internet Access Server 4.1. Each network protocol you want to support must be bound and must run over a configured link.

This topic contains the following sections:

Routing Protocols

NetWare IPX and TCP/IP configurations offer options for setting the routing protocols. There are two general types of routing protocols available: *distance vector* and *link state*. Your choice of routing protocols is determined largely by which routing protocols are currently used in your network. For example, in older networks, such as NetWare 2, there might be several routers that can support only distance vector routing.

If your network contains routers that support both link state and distance vector routing, your router will need to support both. In networks that have only newer routers, it is best to configure the routers to use only link state routing protocols. In networks with older routers, you can gradually update your routers and migrate to the exclusive use of link state routing protocols.

Table 1 shows the distance vector and link state protocols that are supported by Novell Internet Access Server 4.1.

Table 1   Distance Vector and Link State Protocols

Network Protocol	Distance Vector Routing Protocol	Link State Routing Protocol
IPX	RIP	NetWare Link Services Protocol™ (NLSP™) software with RIP/SAP compatibility (default)
TCP/IP	RIP (default)	OSPF
AppleTalk	RTMP and AURP	not applicable

Source Route Bridge

The source route bridge enables you to use your router to link token ring networks and create an extended network. Source route bridging allows end stations to discover routes dynamically and determine which one to use when sending data to any particular destination.

Novell Internet Access Server 4.1 supports concurrent routing and bridging of all major protocols, including IPX, TCP/IP, and AppleTalk, and bridges unroutable protocols, such as the IBM* NetBIOS and SNA protocols. However, because you cannot bridge and route the same protocol on the same interface, the software provides a mechanism for automatically disabling bridging for the protocols that are being routed.

On-Demand Links and Static Routes

NetWare Link/PPP on-demand links are WAN circuits that become active only when there is traffic on the link. 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 exchange routing information dynamically and, in the case of IPX, to receive service advertising updates. These periodic exchanges identify the network routes and services that are known on each remote LAN accessed over the WAN connections.

Because on-demand connections do not exchange routing or service information, both ends of the link must have enough information to be able to call each other. Because no routing traffic crosses an on-demand link, you must configure remote routes manually on the local router as *static routes*. This way, the connection can remain inactive until data needs to cross it.

Static routes are configured at the network protocol level, such as IPX or AppleTalk. They let the protocol know the WAN call destination to use to reach that route, as well as information about the remote router, such as IP address, number of hops, and so on.

For example, if an IP router needs to reach a remote destination, it sends packets to the local IP router that advertises the routes, and assumes the packets can reach their destination. The local router then stores the packets and, using the static route information, uses the appropriate WAN call destination to establish a connection to the remote router. After the local router completes the call and negotiates on-demand service, it forwards the stored packets to the remote router, which then forwards them to their destination.

Permanent Links and Static Routes

In TCP/IP and IPX, static routes are not limited to on-demand WAN calls; you can also use them for permanent WAN calls and connections. You use a static route for a permanent WAN connection if you want to eliminate routing protocol traffic over the connection, making more bandwidth

available for data, or to have a backup route for dynamic routes. You can also use static routes to limit user access to one portion of the network, or to gain access to isolated areas of the network. You can also use routed on-demand links for IPX.

Tunneling

Novell Internet Access Server 4.1 provides the IPRELAY and IPTUNNEL drivers for tunneling IPX packets through IP internetworks, and provides the AppleTalk Update-based Routing Protocol (AURP) to tunnel AppleTalk packets through IP internetworks.

IPRELAY is configured as a WAN board driver that simulates a collection of point-to-point Permanent Virtual Connections (PVCs) between routers. IPRELAY uses the User Datagram Protocol (UDP) encapsulation to send IPX packets through an IP internetwork to a remote IPRELAY peer. The remote IPRELAY peer then strips the UDP encapsulation and sends the IPX packet through an IPX network to its destination.

Similarly, AURP encapsulates AppleTalk packets to send them through an IP internetwork to a remote AURP peer. The remote AURP peer then strips the encapsulation and sends the packet through the AppleTalk network to its destination.

The IPTUNNEL driver enables IPX to use a TCP/IP network to communicate with other IPX nodes. The IPTUNNEL driver models the IP internetwork as a single IPX LAN. To IPX, IPTUNNEL performs the same functions as a typical NetWare LAN driver. The TCP/IP network operates as if it were a hardware network, passing packets among the IPX nodes connected to it.

Filtering

Novell Internet Access Server 4.1 supports filtering to control the service and route information that is accepted or advertised by a router. Filters are useful when you want to limit specific types of traffic to certain parts of your network and when you want to provide a certain level of security. The Filter Configuration utility (FILTCFG) enables you to configure the filters for IPX, IP, AppleTalk, and the source route bridge, to selectively discard packets sent or received by a router. The following types of filters are supported:

- *Packet forwarding* —Prevents or allows selected data packets from being forwarded by the router. Packet forwarding filtering is available for IPX and TCP/IP.

- *Service information* —Prevents or allows packets that advertise services destined for particular parts of the network from being advertised by the router. Service information filtering is available for IPX and AppleTalk.

- *Routing information* —Limits the routes added to the routing tables of specified routers. Routing information filtering is available for IPX, AppleTalk, and TCP/IP.

- *Protocol ID* and *Ring Number* —Only available for source route bridge, the Protocol ID filter is used for packets of certain protocol types received by the bridge, and the Ring Number filter is used for packets received from specific rings in a token ring network.

Configuration Utilities and Commands

You use the following utilities to configure and manage your router:

- Configuration and management utilities to configure and optimize the router. These include NIASCFG, FILTCFG, STATICON, CALLMGR, and CPECFG.

- Command-line utilities to implement configuration changes to your router. These utilities include the INITIALIZE SYSTEM and REINITIALIZE SYSTEM commands.

    NOTE: You use monitoring utilities to check how each protocol is functioning and to help you identify potential problems. These include PPPCON, IPXCON, ATCON, and TCPCON.

Configuration and Management Utilities

The utilities you use to configure and manage Novell Internet Access Server 4.1 work in conjunction with the monitoring utilities to configure, monitor, and optimize the router and its connections.

NIASCFG

NIASCFG enables you to configure Novell Internet Access Server 4.1. You can set up and customize your internetworking configuration for PPP, IPX, IP, AppleTalk, and the source route bridge by performing the following tasks:

- Select and configure a board.
- Select and configure a network interface.
- Create a WAN call directory.
- Create a backup call association.
- Select and configure a network protocol.
- Bind a network protocol to an interface.
- Manage the configuration.
- View the configuration.
- Switch to the fast setup method.

NIASCFG records information in various configuration (*.CFG) files located in SYS:\ETC. Some of these files are present at system startup; others are created by NIASCFG, depending on the parameters you configure. The following is a partial list of these files:

- AURP.CFG
- TCPIP.CFG
- IPXSPX.CFG
- NLSP.CFG
- NETINFO.CFG

    WARNING: NIASCFG creates these files strictly for its own use; do not delete them or change their contents.

FILTCFG

You use the Filter Configuration utility (FILTCFG) to set up and configure filters for the IPX, TCP/IP, and AppleTalk protocols and the source route bridge.

Filters provide a way to control the kind of information that is sent and received by a router by selectively discarding packets and routes of specified types. Filters are useful when you want to limit specific kinds of traffic to a certain part of your network topology, or when you want to provide a level of security. To configure filters, refer to Setting Up in the *Filters* documentation.

STATICON

You use the Static Routing Configuration utility (STATICON) to open a connection to a remote IPX router and configure static routes and services at each end of the connection. To configure static routes with STATICON, refer to Configuring Static Routes and Services in the *IPX* documentation.

You can use STATICON to perform the following tasks:

- Initiate configuration of static routing tables with a remote router.
- Configure local static services from gatekeepers.
- Configure local and remote static services and routes.
- Save static routing tables to permanent storage.
- Restore static routing tables from permanent storage.

CALLMGR

You use the Call Manager utility (CALLMGR) to monitor the status of your WAN connections or to initiate and terminate WAN calls manually. When you start CALLMGR, you see a list of the current WAN connections. Each line displays the status of the call, the network interface, and the protocol used for the call. Outgoing calls display the name of the WAN call destination specified for the call. The name of the remote system might also be displayed.

Call error detailed information is available for calls that terminate while you are in CALLMGR.

CPECFG

You use the CPE Configuration utility (CPECFG) to configure and manage communications equipment from the server console. You can use CPECFG to establish communications with your communications equipment, such as a DSU/CSU or a modem, through the existing serial port on a server or standalone router.

TECHWALK

You use the TECHWALK utility to record your Novell Internet Access Server 4.1 configuration. The TECHWALK utility records all information in NIASCFG or other console utilities by walking through the configuration parameters and saving them to the SYS:/ETC/TECHWALK.OUT file. All enabled items and summary lists are recorded.

You can access TECHWALK by typing one of the following command variations:

- **LOAD TECHWALK**
- **LOAD TECHWALK** *console NLM name*

The console option runs TECHWALK to record only the information for the console utility you specified in the command.

Depending on the information you want to record, you should exit NIASCFG or the specific console before you run TECHWALK. Running TECHWALK might take from 5 to 60 minutes, depending on your configuration and the network traffic, and dedicates your machine to the process.

Command-Line Utilities

Novell Internet Access Server 4.1 also includes the commands described in this section to enhance the configuration and management utilities.

INITIALIZE SYSTEM

The INITIALIZE SYSTEM command lets you enable the Novell Internet Access Server 4.1 configuration by executing all commands in the system NETINFO.CFG file.

To use INITIALIZE SYSTEM, type the following command at the server prompt:

```
INITIALIZE SYSTEM
```

This command is typically executed from the INITSYS.NCF file during server startup.

NOTE: Executing INITIALIZE SYSTEM on a system that has already been initialized can generate errors as the system discovers that the commands in the NETINFO.CFG file have already been executed.

REINITIALIZE SYSTEM

The REINITIALIZE SYSTEM command lets you enable configuration changes made since the commands in the NETINFO.CFG file were executed.

To use REINITIALIZE SYSTEM, type the following command at the server prompt:

```
REINITIALIZE SYSTEM
```

NOTE: The REINITIALIZE SYSTEM command is also available from the Internetworking Configuration menu.

REINITIALIZE SYSTEM compares the current NETINFO.CFG file with the previous one, which became effective with the execution of the INITIALIZE SYSTEM command. If REINITIALIZE SYSTEM finds any new or changed commands in the current NETINFO.CFG file, it executes them.

REINITIALIZE SYSTEM also informs any SNMP-registered NetWare Loadable Module™ (NLM™) file that it is executing. This callback mechanism enables NLM files that store configuration information *outside* the NETINFO.CFG file to recognize that changes to the configuration have taken place.

Dynamic Reconfiguration

With dynamic reconfiguration, any changes you make to a router take place automatically without the router being restarted.

Any protocol parameter changes (from the Protocols menu in NIASCFG) to TCP/IP, IPX, or AppleTalk parameters take place dynamically at reinitialization. Status changes and configuration changes in any routing protocol take place dynamically without affecting other routing protocols.

All bind configuration changes (from the Bindings menu in NIASCFG) cause an automatic unbind and rebind to the interface.

This topic contains the following sections:

IPX

The following conditions are true for IPX:

- All global configuration changes will cause an automatic unload and reload of IPX.

- Port-specific parameter changes or WAN call profile changes might or might not bring the affected connection down, depending on the type of change being made. Only permanent connections will be brought up again.

- Any configuration changes to the static routes or services for a circuit will delete and refresh all static routes and services for that circuit without disconnecting the call.

TCP/IP

The following conditions are true for TCP/IP:

- All configuration changes, except to WAN Call Destinations, RIP Bind Options, and OSPF Bind Options, cause an automatic unbind and rebind of IP to the interface.

- Any configuration changes to RIP Bind Options and OSPF Bind Options will simply reconfigure the respective routing protocol without affecting other routing protocol bind parameters.

- Any configuration changes to WAN Call Destinations, except changes to Static Routing Table and RIP Bind Options, will bring the connection down. Only permanent, automatic connections will be brought up again.

- Any configuration changes to RIP Bind Options or Static Routing Table under WAN Call Destinations will reconfigure RIP or the static routes for the specified connection without affecting other parameters, and without disconnecting the call for the given connection.

AppleTalk

The following conditions are true for AppleTalk:

- All AppleTalk configuration parameter changes are dynamically reconfigured immediately, except changes to the WAN Protocol ID (PID). You must restart the router to use a new Protocol ID.

- Binding configuration changes, except those made to WAN call destinations, automatically unbind and rebind AppleTalk to the interface.

- Any configuration changes to the zone(s) list for an external interface will cause an automatic unbind. You must enter the REINITIALIZE SYSTEM command to rebind AppleTalk to the interface 10 minutes later.

- Any configuration changes to the zone(s) list of the internal network and the static routes will make AppleTalk not advertise the changed routes for 10 minutes.

- Any configuration changes to the WAN interface or WAN call destinations, except changes to the static routes, will bring the connection down. Only permanent, automatic connections are brought up again.

- Any configuration changes to static routes will reconfigure the static routes for the specified connection without affecting other parameters, and without disconnecting the call for the given connection.

- Any configuration changes to the AURP parameters will make AURP unload and reload internally, and all connected AURP peers will be disconnected and reconnected.

Configuring Router Management

The Manage Configuration menu within the Internetworking Configuration menu provides options to copy and transfer common configuration files, configure server access, and perform other network management tasks. Sets of preconfigured files can be imported or exported to specified server destinations. These files can also be loaded as part of the Novell® Internet Access Server 4.1 installation process.

Manage Configuration menu options are

- ◆ Configure SNMP Parameters
- ◆ Configure SNMP Information
- ◆ Export Configuration
- ◆ Import Configuration
- ◆ Configure Remote Access to This Server
- ◆ Edit AUTOEXEC.NCF

The Simple Network Management Protocol (SNMP) enables network management clients to exchange information about the configuration and status of nodes on an internetwork. The information available is defined by a set of managed objects referred to as the Management Information Base (MIB).

The Manage Configuration menu provides two options for configuring SNMP parameters and information: Configure SNMP Parameters and Configure SNMP Information.

This topic contains the following sections:

- ◆ "Configuring SNMP Parameters" on page 13
- ◆ "Configuring SNMP Information" on page 15
- ◆ "Export Configuration" on page 16
- ◆ "Import Configuration" on page 17
- ◆ "Configuring Server Access" on page 17
- ◆ "Edit AUTOEXEC.NCF" on page 18

Configuring SNMP Parameters

To configure SNMP parameters, complete the following steps:

1 From the Internetworking Configuration menu, select Manage Configuration.

The Manage Configuration menu is displayed.

2 From the Manage Configuration menu, select Configure SNMP Parameters to configure SNMP for this server only.

The SNMP Parameters menu is displayed.

3 From the SNMP Parameters menu, select Monitor State.

The following options allow you to indicate how the SNMP agent handles SNMP read operations coming from outside this node.

Option	Description
Any Community May Read	Allows all read operations, no matter what community name is provided in the incoming read request.
Leave as Default Setting	Avoids changing the Monitor Community name from its default (which is usually public). The default Monitor Community can still be changed manually through SNMP command-line options.
No Community May Read	Disables all read operations, no matter what community name is provided in the incoming read request.
Specified Community May Read	Allows only read operations that contain the name specified in the Monitor Community field.

4 Select one of the options previously listed.

5 If you selected Specified Community May Read, enter a name in the Monitor Community field.

Enter the name of the community that is permitted to read management information. SNMP management stations that belong to this community can read the network management database.

6 Select Control State.

The following options enable you to indicate how the SNMP agent handles SNMP write operations coming from outside this node.

Option	Description
Any Community May Write	Allows all set operations, no matter what community name is provided in the incoming set request.
Leave as Default Setting	Avoids changing the Control Community from its default, which usually is to not allow any set requests. The default can be changed manually through SNMP command-line options.
No Community May Write	Disables all set operations, no matter what community name is provided in the incoming set request.
Specified Community May Write	Allows only set operations that contain the name specified in the Control Community field.

7 Select one of the options previously listed.

8 If you selected Specified Community May Write, enter a name in the Control Community field.

Enter the name of the community that is allowed to read and write management information. SNMP management stations that belong to this community can read or modify (write) any value in the network management database.

9 Select Trap State.

The following options allow you to indicate how the SNMP agent handles SNMP trap operations coming from outside this node.

Option	Description
Do Not Send Traps	Disables all SNMP traps.
Leave as Default Setting	Avoids changing the Trap Community from its default, which is usually public. The default can still be changed manually through SNMP command-line options.
Send Traps with Specified Community	Specifies the community name that is included in trap messages in the Trap Community field.

10 Select one of the options previously listed.

11 If you selected Send Traps with Specified Community, enter a name in the Trap Community field.

Enter the community name to be included in trap messages.

12 Select Other SNMP Parameters and press Enter.

The SNMP Other Parameters window is displayed.

13 Enter the following SNMP command-line parameters in the window that is displayed.Enter

13a Verbose=Yes/No

Entering Verbose=Yes enables SNMP parameter configuration messages to the console.

13b Enter AuthenticationTraps=Yes/No

Entering AuthenticationTraps=Yes causes SNMP to send traps to trap targets when an authentication failure occurs in GET, GET-NEXT, or SET operations. These targets are configured using the SYS:\ETC\TRAPTARG.CFG file.

Enter SNMP parameters in the same format in which they appear when entered on the LOAD SNMP command line. For more information, refer to "Configuring SNMP Information."

14 When you are finished, press Esc. If prompted, select Yes to save changes, then press Enter.

The Manage Configuration menu is displayed.

15 Select another option from the Manage Configuration menu to continue, or press Esc to return to the Internetworking Configuration menu.

Configuring SNMP Information

To configure SNMP information, complete the following steps:

1 From the Internetworking Configuration menu, select Manage Configuration.

The Manage Configuration menu is displayed.

2 From the Manage Configuration menu, select Configure SNMP Information to configure SNMP for this server only.

3 Select Node Name for SNMP and press Enter.

4 Enter the name SNMP reports to the management client for this node, then press Esc.

By convention, this is the IP hostname for the node. If the node does not have an IP hostname, we recommend that you use the NetWare® file server name for this node.

5 Select Hardware Description and press Enter.

6 Enter the hardware description for this node, then press Esc.

The hardware description can include the CPU type; bus speed; size of memory; and size and type of disks, printers, tape drives, and so on. This description, combined with the information about the software taken from the system, makes up the SNMP system description.

7 Select Physical Location and press Enter.

8 Enter the location description for this node, then press Esc.

9 Select Human Contact and press Enter.

10 Enter the contact information for the person (or persons) responsible for this node, then press Esc.

The contact information should include phone numbers and mailing addresses.

11 When you are finished, press Esc. If prompted, select Yes to save the changes to the SNMP parameters, then press Enter.

The Manage Configuration menu is displayed.

12 Select another option from the Manage Configuration menu to continue, or press Esc to return to the Internetworking Configuration menu.

Export Configuration

To move configuration files among network servers, NIASCFG provides an option to export files to diskette or a specified server destination. Exported routing configuration files can be used as a set of preconfigured files for product installation on another system, product reinstallation on this system, or as a routing configuration backup. To copy files to a remote destination, remote server access and adequate disk space are required.

To create and transfer a routing configuration file set to a specified server volume, complete the following steps:

1 From the Internetworking Configuration menu, select Manage Configuration.

The Manage Configuration menu is displayed.

2 From the Manage Configuration menu, select Export Configuration.

The Configuration Export window is displayed.

3 Indicate the export destination by specifying a DOS device or NetWare volume.

4 Select Export Entire Server Configuration and press Enter. Select Yes and press Enter to export the entire server configuration.

You can select No and specify a partial export by selecting from the X.25 Profiles, Call Destinations, or PPP Authentication Files menu options. Not all files are exported for some configurations.

NOTE: If you export an entire server configuration, information specific to that server is exported (for example, IPX addresses). This information must be modified when imported to another server.

5 Select Export to copy the routing configuration files to the specified destination.

The exported routing configuration file can be used during installation as a preconfigured file set or it can be imported, as explained in the section that follows.

Import Configuration

To move routing configuration files among network servers, NIASCFG provides an option to import files from diskette or a NetWare volume. To copy routing configuration files from a remote destination, remote server access and adequate disk space are required. The Import Configuration option backs up the original routing configuration before transferring new files.

To import a routing configuration file set, complete the following steps:

1 From the Internetworking Configuration menu, select Manage Configuration.

The Manage Configuration menu is displayed.

2 From the Manage Configuration menu, select Import Configuration.

The Configuration Import window is displayed.

3 Specify the location of the files to be imported.

NOTE: If you import an entire server configuration, use NIASCFG to modify information specific to this server (for example, IPX addresses).

4 Select Import and press Enter to copy routing configuration files from the specified source.

The original routing configuration is backed up to the SYS:\ETC.BAK directory. This configuration can be restored using the Import Configuration option and specifying SYS:\ETC.BAK as the source.

Configuring Server Access

To configure a server for RCONSOLE access, complete the following steps:

1 From the Internetworking Configuration menu, select Manage Configuration.

The Manage Configuration menu is displayed.

2 From the Manage Configuration menu, select Configure Remote Console Access To This Server.

The Configure Remote Console Access To This Server window is displayed.

3 Configure the remote parameters as described below.

Option	Description
Remote Console Access	Enables RCONSOLE access to this server. This option must be enabled to provide access to any of the other options listed in this table.
Password	Enter a password to secure remote communications. When enabled, this node requires the password of any user accessing this node through RCONSOLE, ACONSOLE, or XCONSOLE.

Option	Description
RCONSOLE Connection (SPX™)	Enables remote console access to this node through RCONSOLE. RCONSOLE allows access to the file server console from a workstation.
ACONSOLE Connection (ASYNC)	Enables remote console access to this node through ACONSOLE or RCONSOLE Async (4.x RCONSOLE).
COM Port Baud Rate	ACONSOLE allows access to the file server console through a modem. When you enable this option, you also need to specify the communications port and baud rate used by the system.
Expert Modem Setup	You might also have to set up special commands for modems that do not respond to the standard modem AT command set through the Expert Modem Setup option.
TELNET Connection	Enables remote administration from a remote workstation running an X Window System* interface or a remote workstation that has VT100* or VT220* terminal emulation.
Maximum Sessions	When you enable the TELNET connection, you also need to specify the maximum number of concurrent TELNET sessions you want this node to support.
Timeout	Specifies an interval for the ASCII Esc key to take effect.

4 When you are finished, press Esc. If prompted, select Yes to save the changes to the remote server access configuration, then press Enter.

5 Press Esc to return to the Internetworking Configuration menu.

Edit AUTOEXEC.NCF

This option displays the View or Edit AUTOEXEC.NCF window, which contains the AUTOEXEC.NCF file.

As stated in this file, the LOAD and BIND commands are contained in the NETINFO.CFG file.

2 Managing

This section provides an overview of the diagnostic utilities provided with the Novell® Internet Access Server 4.1 software. These utilities enable you to manage, optimize, and troubleshoot the product and its connections.

NIASCFG

NIASCFG enables you to configure and check the status and statistics of Novell Internet Access Server remote access, protocols, and routing. NIASCFG also enables you to use the various Novell Internet Access Server 4.1 console utilities from the NetWare® server console or by using RCONSOLE.

To launch NIASCFG, enter **load niascfg** at the NetWare server console. The NIASCFG main menu offers the following four options.

- ◆ Configure NIAS
- ◆ View Status for NIAS
- ◆ Manage Licenses
- ◆ Exit

NIASCFG offers access to console utilities in much the same way as INETCFG did previously with a few exceptions. Most notably, after launching NIASCFG, you can view status or use a console utility, but you cannot allow a utility to continue to run while you check other screens. If you launch a console utility from NIASCFG, you have to exit that utility before doing anything else.

This topic contains the following sections:

- ◆ "Configure NIAS" on page 25
- ◆ "View Status for NIAS" on page 26
- ◆ "Manage Licenses" on page 27
- ◆ "Protocols and Routing Console Utilities" on page 27

Configure NIAS

After you select Configure NIAS, select Remote Access, Protocols and Routing, or Virtual Private Network. Then select a component to configure from the displayed list. The Remote Access Options are listed below.

- ◆ Configure Ports
- ◆ Configure Port Groups
- ◆ Configure Synchronous Interfaces

- ◆ Configure Security
- ◆ Configure Services
- ◆ Set Up ...
- ◆ Generate Configuration Report

If you select Protocols and Routing, the Internetworking Configuration Window is displayed and lists the following options.

- ◆ Boards
- ◆ Network Interfaces
- ◆ WAN Call Directory
- ◆ Backup Call Associations
- ◆ Protocols
- ◆ Bindings
- ◆ Manage Configuration
- ◆ View Configuration
- ◆ Reinitialize System
- ◆ Go To Fast Setup

If you select Virtual Private Network (VPN), the Virtual Private Network Server Configuration Window is displayed and lists the following options:

- ◆ Master Server Configuration
- ◆ Slave Server Configuration
- ◆ Update VPN Filters
- ◆ Display VPN Server Configuration
- ◆ Remove VPN Server Configuration

NOTE: When you first attempt VPN configuration after software installation, you must log in to Directory Services and extend the schema for the Novell Core Protocol (NCP) server object. To extend the schema, a user must have administrative rights including Write rights to the root's access control list (ACL) attribute.

View Status for NIAS

After you select View Status for NIAS, select either Remote Access or Protocols and Routing. If you select Remote Access, the Status Options Window is displayed, offering the following options.

- ◆ Display Port Status
- ◆ Display Service Status
- ◆ Display Alerts
- ◆ Display Audit Trail

If you select Protocols and Routing, the Protocol and Routing Status Options Window is displayed, offering the following options.

- ◆ AppleTalk* Protocol Stack

- IPX Protocol Stack

- TCP/IP Protocol Stack

- X.25

- ATM

- Frame Relay

- PPP

Manage Licenses

After you select Manage Licenses, NIASCFG displays the Installed Licenses Window which displays any licenses already installed and enables you to add new licenses or remove existing licenses.

Protocols and Routing Console Utilities

The Protocols and Routing Console Utilities can be loaded individually or launched by loading NIASCFG and following this path:

Select View Status for NIAS > Protocols and Routing

NOTE: NIASCFG replaces the INETCFG NLM. INETCFG is still functional.

The following utilities can be used in NIASCFG:

- ATCON—To verify the configuration of the AppleTalk router and the connectivity to the rest of the AppleTalk internetwork.

- IPXCON—To view status and configuration about the Internetwork Packet Exchange™ (IPX™) protocol stack, including information about Simple Network Management Protocol (SNMP) access configuration, router, NetWare Link Services Protocol™ (NLSP™), Mobile IPX™, address mapping gateway, circuits, forwarding, and services.

- TCPCON—To monitor the TCP/IP protocol stack, including TCP/IP configuration, parameters, and real-time statistics.

- X25 CON—To access interface configuration and statistical information for all X.25 interfaces reported by the specified host.

- ATMCON—To monitor and troubleshoot Asynchronous Transfer Mode (ATM) traffic.

- FRCON—To view NetWare Link/Frame Relay™ interface configuration and statistical information.

- PPPCON—To view Point-to-Point Protocol (PPP) interface configuration and statistical information.

For more information about using a specific utility, refer to the management information for the appropriate protocol.

Using the CONLOG Utility

The CONLOG utility enables you to capture all console messages generated at the server while CONLOG is loaded and write the messages to the default SYS:\ETC\CONSOLE.LOG file or to another file of your choice.

You can use the CONSOLE.LOG file to check that all modules have been loaded without any errors during the startup of the Novell Internet Access Server. To view the CONSOLE.LOG file, load NIASCFG and follow this path:

Select Configure NIAS > Protocols and Routing > View Configuration > Console Messages

To load CONLOG, type the following command at the server prompt:

load conlog [file=*log filename* **] [save=***backup filename* **] [maximum=***max file size* **] [archive=***yes* **] [next=***hh:mm* **] [entire=***yes* **] | help**

where

file=*log filename* is the name of the file you want to use as the log file. CONLOG writes console messages to this file instead of CONSOLE.LOG. The *log filename* parameter must be used with SFT III™ servers, whose three engines must each write to a different log file.

save=*backup filename* is the name of the file in which you want to save the preexisting console log. This enables the AUTOEXEC.NCF file to load CONLOG without overwriting the previous console log. Use this parameter if you want to examine the old console log for troubleshooting purposes.

maximum=*max file size* is the maximum size of the log file in kilobytes. If the log file exceeds *max file size*, it is deleted—or renamed if *backup filename* was specified. In either case, logging is restarted with an empty log file.

archive=*yes* saves logs numerically. Instead of saving the console log into a file called CONSOLE.BAK, CONLOG creates CONSOLE.000, CONSOLE.001, ..., CONSOLE.999. After creating CONSOLE.999, if all 1,000 console log files exist, CONLOG reuses the number of the oldest file.

next=*hh:mm* archives the console log at the 24-hour time specified. If no time is specified, the console log is saved when it reaches the length limit.

entire=*yes* captures the lines already on the window at the time CONLOG is loaded. Without this parameter, CONLOG starts logging with the next output to the console after it is loaded.

help displays a description of each CONLOG command parameter.

The **load conlog** command is typically added to the AUTOEXEC.NCF file, as shown in the following example:

```
FILE SERVER NAME NETW41_SVR

IPX INTERNAL NET C92556E

LOAD CONLOG

LOAD REMOTE

LOAD RSPX
```

You can view the console log in one of three ways:

- Loading NIASCFG and following this path:

  Select Configure NIAS > Protocols and Routing > View Configuration > Console Messages

  NIASCFG enables you view the log file any time, even while the CONLOG.NLM is loaded.

- Using the EDIT.NLM utility by typing the following command:

  load edit sys:\etc\console.log

The EDIT.NLM utility does not let you view the log file if the CONLOG.NLM is loaded. If you want to see the log file using the EDIT.NLM utility, unload CONLOG first.

◆ Using any text editor from a LAN workstation to open the file (if CONLOG is not loaded). If you attempt to view the console.log file with a text editor while CONLOG is loaded, the file will appear empty.

Console messages can reveal errors that occur during system initialization. Table 2 shows how to use CONLOG.

Table 2   How to Use CONLOG

To...	Type...
Start capturing console messages during system initialization	**LOAD CONLOG**
Load CONLOG, but save the current log file as CLOG.BAK and limit the size of CONSOLE.LOG to 100 KB	**LOAD CONLOG SAVE=CLOG.BAK MAXIMUM=100**
Stop capturing console messages	**UNLOAD CONLOG**
Get syntax for CONLOG	**LOAD CONLOG HELP**

Using the WMDMMGR Utility

WMDMMGR is a windows-based modem script editing tool used to create and modify modem descriptions and PPP login scripts used with Novell Internet Access Server 4.1. If you need additional information, you can obtain detailed context-sensitive online help for WMDMMGR by pressing the F1 key.

After installing Novell Internet Access Server 4.1, the WMDMMGR utility and message files are located in the SYS:SYSTEM\UTILS directory. Files containing modem descriptions and login scripts are located in the SYS:SYSTEM directory.

Modem descriptions, saved in files with .MDC extensions, define the commands and capabilities of a modem. By using modem description files, Novell Internet Access Server 4.1 components offer modem independence to applications and users, enabling support for new modems without waiting for a new version of the software.

The Novell Internet Access Server 4.1 components execute scripts in the modem description files to perform modem operations as the application requires. Neither the modem control components nor the software products are specific to any one modem or set of modems. Any details specific to modems are contained in the modem description files.

Login scripts, saved in files with .LSC extensions, are PPP login scripts customized to match the sequences expected by online service providers.

This topic contains the following sections:

Launching WMDMMGR

To use WMDMMGR, start your Windows* 3.1 or Windows 95* operating system and follow these steps:

1 Log in to Novell Directory Services™.

2 Map a network drive to the SYS: volume.

3 Change directory to SYS:SYSTEM\UTILS.

Novell recommends that you copy the WMDMMGR.EXE file and the MDC files to your workstation and launch WMDMMGR there.

4 Double-click the WMDMMGR.EXE icon.

WMDMMGR is launched and the File Open window is displayed.

5 Select the drive mapped to the SYS: volume and select the SYSTEM directory.

All available modem script files are displayed in the File Name column. Change the List Files of Type field to Login Script Files to see a list of existing login script files.

Existing Modem Description Files

Novell Internet Access Server 4.1 has three modem description files created by Novell Labs™ and installed in the SYS:SYSTEM directory. These three modem description files define over 400 modems. Table 3 lists the modem description files provided with Novell Internet Access Server 4.1.

Table 3   Existing Modem Description Files

Modem Description File	Contains Modem Scripts
NIASCERT.MDC	that are certified by Novell Labs
NIASMDM1.MDC	for modems named from A-L
NIASMDM2.MDC	for modems named from M-Z

If the modem you have is not already defined in one of these files, you will need to create a new modem description. If your modem is defined but the description does not work, refer to Modifying a Modem Description to make the appropriate changes.

Compatibility Issues When Upgrading

If you have upgraded to Novell Internet Access Server 4.1 from the 4.0 release, NetWare MultiProtocol Router™ 3.1 software, or NetWare Connect™ 2.0 software, you might find that the

modem you were using is not defined in the modem scripts for Novell Internet Access Server 4.1. If this happens, consider one of the following solutions:

- Continue using the *older version.* Novell Internet Access Server 4.1 supports the older scripts. You should not have problems unless the modem is not analog or the description file has other modems with the same name as modems in the Novell Internet Access Server 4.1 MDC files.

- If the modem is not an analog modem, use WMDMMGR to set the modem's Link Type to the correct value. (For example, an ISDN terminal adapter link type should be ISDN-Async.)

- If the modem is defined in a file that contains other modems, one or more of which is already defined in NIASMDM1.MDC, NIASMDM2.MDC, or NIASCERT.MDC, use WMDMMGR to delete the duplicate modems from the file before using the file in Novell Internet Access Server 4.1.

NOTE: During Novell Internet Access Server 4.1 installation, modem description files for Novell Internet Access Server 4.0 and versions of MultiProtocol Router are backed up to the SYS:SYSTEM\BACKUP directory. Modem description files for NetWare Connect 2.0 are left in to SYS:SYSTEM\AIO. Novell Internet Access Server 4.1 uses the modem description files in SYS:SYSTEM.

Creating a Modem Description File

WMDMMGR enables you to create modem descriptions and to customize the modem descriptions to match the behavior of your modem. To create a modem description, launch WMDMMGR and follow these steps:

NOTE: Make sure you have the operation manual for your modem available for reference.

1 Select New from the File menu.

WMDMMGR opens the New dialog box and prompts you to choose Modem Script or Login Script.

2 Select Modem Script.

WMDMMGR opens the List of Modems dialog box. You can now enter the optional file version and manufacturer/copyright information.

3 Click Add.

WMDMMGR opens the Modem Description dialog box. Many of the fields that appear are set with default values that might or might not be appropriate for the modem you are defining. Refer to your modem manual to obtain the correct values and commands for each modem feature.

4 Make entries for the modem being defined.

Enter the name of the modem being defined in the Name field. Enter the appropriate values for Default, Maximum, and Fixed rates. Check the Single Fixed Rate box if the modem being defined can only use the rate specified in the Fixed Rate field when using the Fixed DTE Rate feature. Specify the Output Delay and Link Type.

NOTE: For ISDN terminal adapters (TA), make sure you use the configuration program that comes with the TA before using it in Novell Internet Access Server 4.1. It might be necessary to configure the service profile identification number (SPID) or D-channel protocol as specified by your ISDN service provider.

5 Click Initialization to edit the list of operations for initializing the modem.

The initialization disables all features shown in the dialog box (autoanswer, compression, etc.). When an application uses the modem, the features that are requested are enabled using the individual scripts defined for the feature. Refer to the modem's operation manual for information about disabling each of the features shown on the dialog box.

6 Click Hang-up to edit the list of operations for hanging up a call.

7 Click other Control Strings group buttons to edit the list of operations and enable the feature named by the button.

8 Click Responses to bring up the dialog box to edit the responses generated by this modem.

9 Click OK to save changes to this modem script entry.

The List of Modems dialog box is displayed.

10 Select either File > Save or File > Save Copy As to save changes to this modem description file.

To make the newly created modem description available to the Novell Internet Access Server 4.1 software, refer to "Installing a Modem Description or PPP Login Script."

Modifying a Modem Description

WMDMMGR enables you to customize the modem descriptions to match the behavior of your modem.

NOTE: By default, the modem description files installed by Novell Internet Access Server 4.1 are read-only. Before modifying a file, coy it to a local drive and modify it there to eliminate any effect on the server.

To modify a modem description, launch WMDMMGR and follow these steps:

1 Select File > Open from the WMDMMGR main window to select a modem description.

2 Select the name of the modem that you want to modify from the List of Modems dialog box and click Modify.

You can double-click the modem name instead of clicking the Modify button.

NOTE: For ISDN terminal adapters, make sure you use the configuration program that comes with the TA before using it in Novell Internet Access Server 4.1. It may be necessary to configure the SPID or D-channel protocol as specified by your ISDN service provider.

3 Enter a new name for the modem being defined in the Name field.

By entering a new name, you retain the original modem description.

4 Change the Default, Maximum, and Fixed rates as required for this modem type.

5 Check the Single Fixed Rate box if this modem can only use the rate that is specified in the Fixed Rate Field when using the Fixed DTE Rate feature.

6 Modify the Output Delay and Link Type fields as required for this modem type.

7 Click Control Strings group buttons to edit the list of operations and enable the feature associated with each button.

IMPORTANT: Be sure to verify the output strings in the script with the modem specification provided in the modem manual.

8 Click Responses to bring up the dialog box for editing the responses generated by this modem.

9 Click OK to save changes to this modem script entry.

WMDMRGR displays the List of Modems dialog box.

10 Choose File > Save or File > Save Copy As to save the changes to this modem description file.

To make the newly created modem description available to the Novell Internet Access Server 4.1 software, refer to "Installing a Modem Description or PPP Login Script" on page 36 and perform the steps described.

Modem Responses

Response strings in modem descriptions enable recognition and interpretation of data sent from the modem. This recognition and interpretation informs the modem control software of the success or failure of a command and enables modem control to detect a call's arrival.

Because responses generated by modems differ, the modem description must supply sufficient information to enable modem control to recognize the modem responses. Response strings contain one or more pairs of substrings. The first substring of the pair, the modem response, gives the input string to be recognized. The second substring of the pair represents the meaning of the string.

Because of the complex responses found in newer modems, it is sometimes necessary to perform multistage matching of modem response strings.

For example, when using negotiation progress monitoring to capture added information about connections, the Protocol response can be received. The first stage of recognition would identify the input as the Protocol message. The second stage of recognition identifies the particular substrings that may be present in this message. Up to four stages of recognition are allowed.

Modem control accumulates ASCII characters received from a modem until a carriage return character (hexadecimal D 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.

Editing Modem Responses

The Modem Responses dialog box displays the list of modem responses configured for each modem. Each line in the table describes one modem response. To view the responses for a modem, follow these steps:

1 Launch WMDMMGR.

Double-click the WMDMMGR icon or select Run and designate the path to the WMDMMGR.EXE file.

2 Select the modem description file (.MDC) that contains the modem you want to modify.

3 Select the modem description and click Modify.

The modem description dialog box is displayed. The Responses button is displayed in the bottom right corner of this window.

4 Click Responses.

The Responses dialog box is displayed, listing all of the currently defined responses for the selected modem.

The left-most column, Modem Responses, contains characters sent by the modem to the DTE. When modem control monitors modem responses, it collects characters received until it receives a carriage return. It then compares the input string with all match strings.

NOTE: The input string is not case-sensitive, and the compare operations occur in the order they are listed.

Only the initial characters of a response must match the match string. For example, the match string ERR matches response strings for both ERROR and ERRONEOUS, but not ERASE. This makes the order in which the match strings occur important.

The rest of the columns on this window are known as *meanings strings* and convey status, transfer rate, features, and match chaining. These columns define what the recognized response means to modem control, such as

- Connection success, failure, or some intermediate indication
- Recognition of certain optional connection features
- Indication of transfer rates

Adding a New Modem Response

To add a new response for a modem, go to that modem's Responses window, decide where to place the new response in the list of currently defined responses, and follow these steps:

1 Click a response either in front of or after the location where you want to place the new response, and click Add before... or Add after...

  The Modem Response Meaning window is displayed.

2 In the Response field, enter a string of ASCII characters that represent the expected modem response.

3 In the Status field, select a status that the expected modem response should convey to modem control.

4 In the Rate field, select a transfer rate if applicable for this response.

5 In the Feature field, select a feature to associate with this connection, if applicable.

6 Click OK to save the new modem response.

Modifying a Modem Response

To modify a response for a modem, go to that modem's Responses window, select the response to modify, and double-click that entry. The Modem Response Meaning window is displayed, enabling you to modify the response. Click OK to save your changes, or click Cancel to abandon.

Deleting a Modem Response

To delete a response for a modem, go to that modem's Responses window, select the response to delete, and click the Delete button.

Creating a PPP Login Script

WMDMMGR enables you to create customized PPP login scripts to match the sequences expected by online service providers. Login script files can contain one or more login scripts. You can have a different login script for each service provider you use. Novell Internet Access Server 4.1 has a sample login script file, ISPLOGIN.LSC, installed in the SYS:SYSTEM directory. You can modify the scripts contained in that file or create a new login scripts file.

IMPORTANT: Ensure that you have a sequence of interactions for communicating with the online service provider. This information might be available from your the online service provider or you may gather this information by using a workstation terminal program or dialer software to call the online service provider and capture the input and output sequences.

To create a new login script file, launch WMDMMGR and follow these steps:

1 Select File > New > Login Script.

  WMDMMGR opens the List of PPP Login Scripts dialog box. You can enter optional file version information.

2 Click Add.

WMDMMGR displays the Sample Login Script dialog box. When a new script is created, some fields are seeded with default values that might or might not be appropriate for the script you are defining. Refer to the online service provider for information relevant to your setup.

3 Enter the name of the login script being defined in the Name field.

4 Enter the prompts for the substitution tags that will be used in the script in the fields in the Prompts group. Clear any prompts that will not be used.

5 Click Configure to configure the operations that make up the script.

WMDMMGR displays the Script Operations list.

6 Add and delete operations from the list of operations as required by the online service provider. Click OK.

When adding operations to the list, be sure to consider any timing parameters required by the online service provider. For example, a service provider may require a delay after receiving a response.

7 Click OK to save the changes to the current script entry and return to the List of PPP Login Scripts dialog box.

8 Select File> Save or File > Save Copy As to save the changes to this login script.

To make the newly created login script available to the Novell Internet Access Server 4.1 software, refer to "Installing a Modem Description or PPP Login Script" on page 36 and perform the steps described. An example of a PPP login script follows.

Figure 1   PPP Login Script

```
Operation        Time     Value

Pause            20
Output                    `M`J
Wait for Input   50       ISP login:
Pause            20
Output                    [1]`M`J
Wait for Input   50       password:
Pause            20
Output                    [2]`M`J
Pause            20
Output                    `M`J
```

Modifying a PPP Login Script

WMDMMGR enables you to modify customized PPP login scripts to match the sequences expected by online service providers. Login script files can contain one or more login scripts. You can have a different login script for each service provider you use. Novell Internet Access Server 4.1 has a sample login script file, ISPLOGIN.LSC, installed in the SYS:SYSTEM directory. You can modify the scripts contained in that file or create a new login scripts file.

NOTE: By default, the login description files installed by Novell Internet Access Server 4.1 are read-only. Before modifying a file, copy it to a local drive and modify it there to eliminate any effect on server operations.

IMPORTANT: Ensure that you have a sequence of interactions for communicating with the online service provider. This information might be available from your the online service provider or you can gather this information by using a workstation terminal program or dialer software to call the online service provider and capture the input and output sequences.

IMPORTANT: If you have previously installed Novell Internet Access Server 4.0 or MultiProtocol Router 3.1 and used login scripts, they are backed up to the SYS:SYSTEM\BACKUP directory during the installation of Novell Internet Access Server 4.1. You must upgrade the scripts to 4.1 format using WMDMMGR before using them. WMDMMGR might request additional configuration information before the scripts can be saved in 4.1 format.

To modify a login script file, launch WMDMMGR and follow these steps:

1 Select File > Open.

2 Change the List Files of Type field to Login Scripts (.LSC).

3 Select the login script file that you want to modify and click OK.

4 Select the login script within the login script file and click Modify.

5 Make selected changes to the parameters listed in the Login Script Parameter Prompts window.

6 Click Configure to configure the operations that make up the script.

   WMDMMGR displays the Script Operations list.

7 Add and delete operations from the list of operations as required by the online service provider. Click OK.

   When adding operations to the list, be sure to consider any timing parameters required by the online service provider. For example, a service provider may require a delay after receiving a response.

8 Click OK to save the changes to the current script entry and return to the List of PPP Login Scripts dialog box.

9 Select File > Save to save changes to this login script or File > Save Copy As to save this file as a new login script file.

To make the modified login script available to the Novell Internet Access Server 4.1 software, refer to Installing a Modem Description or PPP Login Script and perform the steps described.

Installing a Modem Description or PPP Login Script

To install a new or modified modem description or login script, copy the file containing it to the SYS:SYSTEM directory of the Novell Internet Access Server. You should not use duplicate names for modem descriptions or login scripts within the modem description (.MDC) or login script (.LSC) files. If modem scripts have duplicate names, the software checks for the Novell Labs certification and script version number to decide which to use. However, if login scripts have duplicate names, an error is reported.

If you modified a file to create a new file, remove any old copies of the file so that there are no script duplications.

After you copy the files into SYS:SYSTEM, enter **reinitialize system** from the NetWare server console. This command causes the Novell Internet Access Server 4.1 software to reload the modem descriptions and login scripts.

NOTE: Because the reinitialize system command affects other software components such as protocol stacks and LAN/WAN boards on the server, you might want to wait until the system is not in heavy use before issuing the command.

Deleting Modem Descriptions or Modem Description Files

Use the Delete button from the List of Modems dialog box to delete unwanted modem description entries. Use the DOS command DEL or Window File Manager to delete unwanted modem description files.

Deleting Login Scripts

Use the Delete button from the List of PPP Login Scripts dialog box to delete unwanted PPP login script entries. Use the DOS command DEL or Window File Manager to delete unwanted login description files.

Viewing the Hardware Configuration of a LAN or WAN Interface

To find out the hardware configuration information for a LAN or WAN interface, load MONITOR and follow this path:

Select LAN/WAN Information > interface you want to view

When you examine the displayed window, you will see all of the available information about that interface including the following information:

- ◆ Interface name
- ◆ Node address
- ◆ Frame type

    NOTE: If more than one frame type is used on an interface, MONITOR shows a separate entry for each frame type used on the same interface. You can view each entry for that interface to find out all the frame types being used.

- ◆ Generic statistics
- ◆ Custom statistics

Viewing Binding Configuration for a LAN or WAN Interface

You can find out which network protocols are bound to an interface and which are currently operational by using one of the following methods:

- ◆ Typing **CONFIG** at the command line of the NetWare® server console.
- ◆ Loading MONITOR and selecting the following path:

    Select LAN/WAN Information > desired interface's information

    Look at the Protocols window to see the network protocols that are bound to that interface.

    NOTE: If more than one frame type is used on an interface, MONITOR shows a separate entry for each frame type used on the same interface. You can view each entry for that interface to find all the protocols bound to the interface.

    You can look at the state of ATCP, BRIDGECP, IPCP, and IPXCP. Protocols with the value of 9 (Opened) or 2 (Listening) are bound to this interface. Protocols currently in operation stay in the Opened state. It is possible for multiple protocols to be bound to the same interface and to operate concurrently.

- ◆ Loading NIASCFG and following this path:

Select Configure NIAS > Protocols and Routing > Bindings

Select the interface you want to view and press Enter.

Determining Processor Utilization and Memory Utilization

Use MONITOR to determine the processing time and memory use of a router. When you load MONITOR, two windows are displayed. The upper window displays general information for the router, including utilization, cache, and packet buffer information. The lower window is the Available Options window. Select Processor Utilization or Memory Utilization from the Available Options window.

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 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.

Monitoring Error Counters

Error counters are monitored to make sure they are not increasing rapidly, because a rapid increase indicates a problem. For information about troubleshooting these problems, refer to the troubleshooting information for the appropriate protocol. You can monitor error counters in one of 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.

3 Troubleshooting

This section contains general troubleshooting information for the Novell® Internet Access Server 4.1 routing software. Before you proceed to specific troubleshooting information in other sections, read the general suggestions and troubleshooting tips presented in the first two topics of this section.

Before Calling Technical Support

Before you call technical support, complete the following steps:

1. Ensure that the most recent releases, patches, modem scripts, drivers, and other software have been obtained from one of the following sources:

   - WWW location http://support.novell.com

   - WWW location http://labs.novell.com

   - WWW location http://labs.novell.com/wan (for driver support)

   - WWW location http://ftp.novell.com (for retrieving patches)

   - 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.)

2. Read the README files and Release Notes for information about known product limitations and bugs. The README files can be viewed from the SETUP menu during installation. They can also be printed from the Install directory on the CD-ROM.

3. Examine the contents of the following configuration and log files:

   - STARTUP.NCF

   - SYS:SYSTEM\AUTOEXEC.NCF

   - SYS:ETC\CONSOLE.LOG

   - SYS:ETC\NETINFO.CFG   *(Do not manually edit this file!)*

   - SYS:SYSTEM\INSTALL.LOG

   Examining these files should help you to identify network configuration errors. If you need to call technical support, run CONFIG.NLM, which will automatically redirect these files to SYS: SYSTEM\CONFIG.TXT. Also, having a network map or drawing enables the technical support staff to examine the entire configuration and the surrounding environment.

4. Examine the contents of the CONFIG command by performing the following actions:

   - Log in to the router from a workstation using RCONSOLE. Refer to RCONSOLE for more information about RCONSOLE.

   - Enter **CONFIG** at the console prompt.

Troubleshooting Tips

Check the following areas to ensure that they are not the source of the problem:

- "Interface Boards" on page 48
- "Installation" on page 49
- "Automatically Restarting the Server" on page 49
- "Configuration" on page 50

Interface Boards

The following list contains suggestions for solving problems with interface boards.

- Use boards that are certified by the Novell Labs™ group. Novell Labs bulletins are available at the WWW location
  http://support.novell.com and on the Novell Support Connection CD-ROM.

- If you are using IBM* token ring boards, a shared RAM size of 16 KB is recommended.

- In most cases, the router-associated LAN and WAN boards can be installed with the Video Memory Addressing set to the factory default settings. However, the default settings for some boards might conflict with already installed VGA/EGA boards. To eliminate the conflict, reconfigure either the VGA/EGA board or the network interface board.

- If you are routing on an Ethernet board, set the maximum physical receive packet size to at least 1524 in the STARTUP.NCF file. If you are routing on a token ring board, set the value to at least 4540. These values include 10 bytes for PPP overhead.

- Before you install a LAN or WAN board, make sure that you check all the available interrupts, I/O base addresses, and memory map addresses for all boards. To avoid conflicts between board parameter settings, verify that the same values are not being used by multiple boards. For reference, the values typically used by a PC are as follows:

  COM1 uses IRQ-4, port=3F8-3FF
  COM2 uses IRQ-3, port=2F8-2FF
  LPT1 uses IRQ-7, port=378-37F
  LPT2 uses IRQ-5, port=278-27F

  To determine valid settings for IRQ, I/O base, and memory locations, refer to the hardware documentation for each device. As you configure the router and WAN links, record this information on a worksheet to avoid any conflicts.

- The Novell NW2000 and Synchronous/+ boards have switches for changing only the I/O base address. The interrupt and memory are software-driven. When you use the Novell Internet Access Server Configuration utility (NIASCFG) to configure WAN boards, you can configure the I/O base address, interrupt, and memory map address. Verify that the NIASCFG I/O base settings match the jumper settings on the board.

  The Synchronous/+ and NW2000 boards use a shared memory interface to the PC. Multiple Synchronous/+ boards can share the same memory address and multiple NW2000 boards can share the same memory address; however, different types of boards cannot be assigned the same address. When assigned an address below 1 MB, a Synchronous/+ board uses 64 KB of shared memory and an NW2000 board uses 16 KB of shared memory. When assigned an

address above 1 MB, a Synchronous/+ board uses 512 KB of shared memory and an NW2000 board uses 256 KB of shared memory.

- When a command is issued to unload a board driver, all instances of that driver are unloaded. For example, if two Synchronous/+ boards are loaded, an UNLOAD SYNCPLUS command unloads both boards and all calls on these boards are terminated.

Installation

The following list contains suggestions for solving problems with the product installation.

- For new installations of the routing features, you must choose to convert the commands in your AUTOEXEC.NCF file to NIASCFG commands automatically when you are prompted to do so within NIASCFG. However, if you choose to convert the AUTOEXEC.NCF file commands manually, all LOAD commands for LAN and WAN drivers and all BIND commands must be commented out within, or removed from, the AUTOEXEC.NCF file. Table 4 shows the protocol LOAD and BIND commands that must be commented out of the file.

Table 4   **LOAD and BIND Command Removal**

Protocol	LOAD and BIND Commands to Comment Out
Internetwork Packet Exchange (IPX)	IPX
AppleTalk*	APPLETLK
	ATLKSNMP
TCP/IP	TCPIP
	TCONFIG
	IPCONFIG
Other	ROUTE (LOAD commands only)

- Do *not* remove other services from the AUTOEXEC.NCF file if they are present; for example:
  - NFS*
  - AFP*
  - ATPS
- If you plan to use this software in combination with another Novell product, refer to the README file of that product for any special installation instructions required for your version of the product. The order of installation is especially important if you are using NetWare for Macintosh*, NetWare for SAA*, or NetWare for NFS with the Novell Internet Access Server 4.1 routing software.

Automatically Restarting the Server

You can configure your router/server to restart automatically by creating a .NCF file (located in SYS: SYSTEM) that contains these commands:

```
REMOVE DOS
```

```
DOWN
EXIT
```

The .NCF file is created with any text editor, and can be created remotely using RCONSOLE. To restart the router/server, use RCONSOLE to attach to that router and run the appropriate .NCF file. Make sure that you have the SERVER command in the AUTOEXEC.BAT file of the router/server so that when you run the .NCF file to restart the server, the server comes up automatically.

Configuration

The following list contains suggestions for solving problems with the product configuration.

- Obtain the latest .LAN files and .LDI files from the WWW location http://support.novell.com, CompuServ, or your network interface board vendor.

- Always use NIASCFG to configure the routing and remote access software.

- NIASCFG will not run if INETCFG is loaded.

- NIASCFG provides a series of easy-to-use menus for router configuration. It also allows you to view and, in some cases, edit for troubleshooting purposes the configuration information file (NETINFO.CFG), the AUTOEXEC.NCF file, and the messages generated during a system restart. Finally, NIASCFG provides several layers of context-sensitive help to make the configuration process quicker and easier.

- Do *not* modify the NETINFO.CFG file found in the SYS:ETC subdirectory.

- The NETINFO.CFG file contains the LOAD and BIND commands you configured with NIASCFG. If you use the INSTALL utility to create an AUTOEXEC.NCF file after completing your configuration with NIASCFG, the LOAD and BIND commands in your system memory are written to the AUTOEXEC.NCF file. We do not recommend this procedure because it can create duplicate entries of the LOAD and BIND commands already in your NETINFO.CFG file.

- If the NETINFO.CFG file is flagged READ ONLY, and if you change a field in NIASCFG (for example, IPX Network Number under Configure NIAS > Protocols and Routing > Bindings), NIASCFG reflects the change but NETINFO.CFG does not. No change can be made to the NETINFO.CFG file because it is flagged READ ONLY. However, NIASCFG warns you when this occurs, indicating that the NETINFO.CFG file cannot be changed. To save the change, flag NETINFO.CFG as READ/WRITE, return to NIASCFG, and reenter the change.

- Make sure that you configure the proper frame types when you are binding IP, IPX, and AppleTalk to a LAN interface. Note that the default frame type for IPX is Ethernet_802.2.

- Do not load and bind the bridge from the command line.

Troubleshooting WAN Hardware

The following sections present techniques that you can use when troubleshooting your WAN hardware:

- "Network Interface Board Self-Diagnostics" on page 51

- "Remote Management of Communication Devices" on page 51

- "DSU/CSU Issues" on page 51

- "Back-to-Back Testing" on page 51

Network Interface Board Self-Diagnostics

Standalone test programs (DOS or NetWare version) might be supplied by a WAN board manufacturer for component and board level self-diagnostics.

A board diagnostic utility called SD.EXE is included with the Synchronous/+ board package. This utility can be used for troubleshooting when board problems occur. For more information about the SD diagnostic utility, refer to the *Synchronous/+ Adapter Installation Guide*.

A diagnostic program called WANDIAG.EXE is also provided on the distribution diskette received with the NW2000 board. WANDIAG.EXE is run from the DOS prompt and uses five different tests to test up to two boards.

If data is not sent, run the available hardware diagnostic tests on the WAN board. Change any settings and ensure that the board passes the hardware diagnostic tests.

Remote Management of Communication Devices

CPECFG (Customer Premises Equipment Configuration), a NetWare Loadable Module™ (NLM™) utility installed on your router or server, provides expanded control of your data circuit-terminating equipment (DTE). You can now control customer premises equipment (if a supervisor port exists on the communications equipment) from any workstation on your internetwork through RCONSOLE, ACONSOLE, or VT100* XCONSOLE. This feature allows you to configure, control, and troubleshoot the DCE remotely from any workstation on the internetwork. A standard null modem cable is used from the router's serial port to the supervisory port or terminal on the DCE. Refer to the documentation provided with the DCE for more information.

DSU/CSU Issues

Observe the following guidelines when using a DSU/CSU.

◆ Always make sure that only one source supplies the transmit and receive clocks on the line. Either the DCE (such as a modem or DSU/CSU) or the DTE (the WAN interface board) on one side of the link should supply the transmit and receive clocks.

◆ If your clocking is being provided by either the DSU/CSU or telco, make sure the Interface Speed option is set to External in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > a specific interface). Do not set this option to reflect the speed of the line; this setting would be incorrect. Selecting an interface speed initializes the clocks built into the WAN board and confuses the DSU/CSU. The built-in clocks are commonly used for back-to-back testing.

Back-to-Back Testing

Perform back-to-back testing of all WAN interfaces before you install the router on-site. To implement a back-to-back test, complete the following steps:

1 Construct the appropriate crossover cable (as shown in Figure 2, Figure 3, or Figure 4) and attach it between the routing systems to be tested.

IMPORTANT: A modem eliminator can also be used in place of a crossover cable. When a modem eliminator is used, it provides the clocking. Configure the Line Speed option to External in NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > a specific interface). Because an incorrectly constructed crossover cable can cause problems that are difficult to isolate, we recommend using a modem eliminator.

2 Using NIASCFG, change the Line Speed option on *one* of the routers to an appropriate line speed (baud rate) other than External (parameter path: Select Configure NIAS > Protocols and Routing > Network Interfaces > a specific WAN interface).

3 On the other router, leave the speed setting to the default External and save both settings.

4 Configure any other needed IPX, TCP/IP, AppleTalk, or source route bridge parameters.

5 Restart both machines.

6 Use CALLMGR to initiate a call between the two routers.

7 Use MONITOR to verify that the connection is working properly. You can also load PING.NLM (TCP/IP) or IPXPING.NLM to verify connectivity.

NOTE: All crossover cables shown in Figure 1-1, Figure 1-2, and Figure 1-3 can be used with the Synchronous/+ board, but only the RS-232 and RS-422 cables can be used with the NW2000 board. Other WAN boards and drivers might require variations of these cables. Refer to your WAN board documentation for more information.

Figure 2 shows pinouts for constructing an RS-422 crossover cable, which can be used for back-to-back testing on any of the RS-422 ports.

Figure 2   RS-422 Crossover Cable
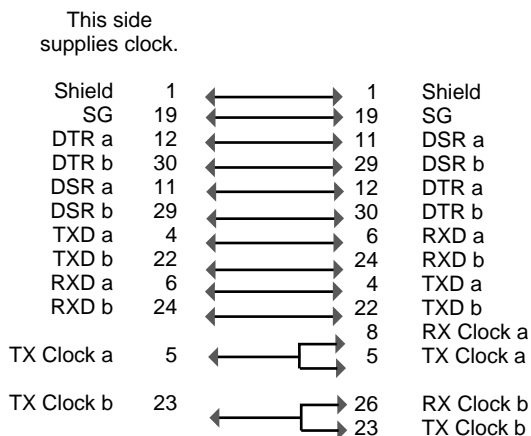
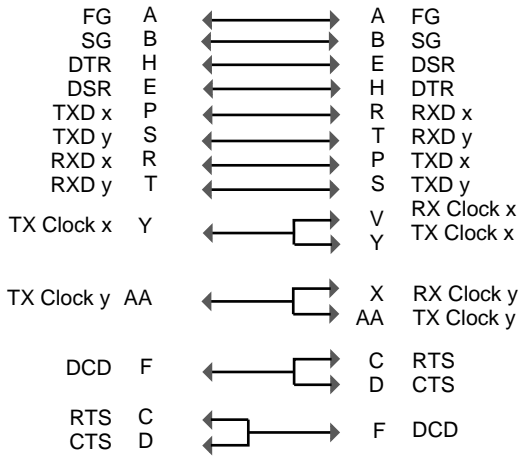| CTS | Clear To Send | RTS | Ready To Send |
DCD	Data Carrier Detect	SG	Signal Ground
DSR	Data Set Ready	TX Clock	Transmit Clock
DTE Clock	Data Terminal Equipment Clock	TXD	Transmit Data
DTR	Data Terminal Ready	RX Clock	Receive Clock
FG	Frame Ground	RXD	Receive Data

Figure 3 shows pinouts for constructing a V.35 crossover cable, which can be used for back-to-back testing on any of the V.35 ports.

Figure 3   V.35 Crossover Cable

V.35 34-Pin Connector
Female End

V.35 34-Pin Connector
Female End

This side
supplies clock.

FG	A	A	FG
SG	B	B	SG
DTR	H	E	DSR
DSR	E	H	DTR
TXD x	P	R	RXD x
TXD y	S	T	RXD y
RXD x	R	P	TXD x
RXD y	T	S	TXD y

TX Clock x   Y

V   RX Clock x
Y   TX Clock x

TX Clock y   AA

X   RX Clock y
AA   TX Clock y

DCD   F

C   RTS
D   CTS

RTS   C
CTS   D

F   DCD

CTS	Clear To Send	RTS	Ready To Send
DCD	Data Carrier Detect	SG	Signal Ground
DSR	Data Set Ready	TX Clock	Transmit Clock
DTE Clock	Data Terminal Equipment Clock	TXD	Transmit Data
DTR	Data Terminal Ready	RX Clock	Receive Clock
FG	Frame Ground	RXD	Receive Data

Figure 4 shows pinouts for constructing an RS-232 crossover cable, which can be used for back-to-back testing on any of the RS-232 ports.

Figure 4   RS-232 Crossover Cable

**DB-25 Connector
Female End**

**DB-25 Connector
Female End**
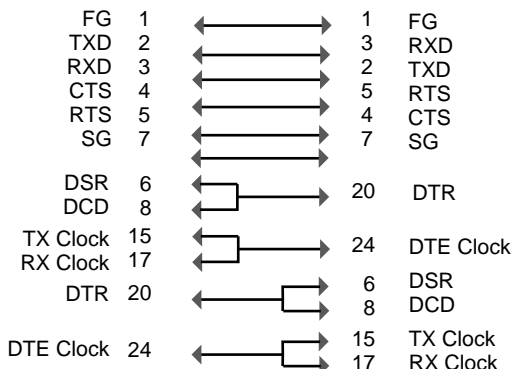
This side
supplies clock.

FG	1	1	FG
TXD	2	3	RXD
RXD	3	2	TXD
CTS	4	5	RTS
RTS	5	4	CTS
SG	7	7	SG
DSR	6	20	DTR
DCD	8		
TX Clock	15	24	DTE Clock
RX Clock	17		
DTR	20	6	DSR
		8	DCD
DTE Clock	24	15	TX Clock
		17	RX Clock

CTS	Clear To Send	RTS	Ready To Send
DCD	Data Carrier Detect	SG	Signal Ground
DSR	Data Set Ready	TX Clock	Transmit Clock
DTE Clock	Data Terminal Equipment Clock	TXD	Transmit Data
DTR	Data Terminal Ready	RX Clock	Receive Clock
FG	Frame Ground	RXD	Receive Data

General System Troubleshooting Tools

This topic describes several utilities that you can use to troubleshoot any problems you might have with your routing and remote access software. In addition to these general tools, LAN and WAN protocol-specific utilities are also available. These tools are summarized in Table 5 on page 56.

This topic contains the following sections:

- "CONLOG" on page 54

- "MONITOR" on page 55

- "Call Connection Manager" on page 55

- "RCONSOLE" on page 55

- "XCONSOLE" on page 55

- "SNMPLOG" on page 55

- "ManageWise" on page 56

CONLOG

CONLOG is an NLM utility that logs console messages in an ASCII file called CONSOLE.LOG. This ASCII file is stored in the SYS:ETC subdirectory on the server on which CONLOG has been loaded. You can use the CONSOLE.LOG file to check during the startup of the router or server that all modules have been loaded without any errors. CONSOLE.LOG can be viewed from NIASCFG (parameter path: Select Configure NIAS > Protocols and Routing > View Configuration > Console Messages).

MONITOR

MONITOR is an NLM utility that enables you to monitor various system statistics, including those for the following:

- Processor utilization and overall activity
- Cache memory status
- Connections and their status
- LAN and WAN board drivers
- Loaded modules
- Memory usage

In addition, under the LAN/WAN Information option, you can find a list of all the configured network boards in the machine. If a board does not appear on that list, it has not been initialized, probably because the settings for the board do not match the hardware settings or a conflict exists with other boards in the machine. Refer to the Utilities Reference for more details about MONITOR.

Call Connection Manager

Call Connection Manager (CALLMGR) is an NLM utility that displays information associated with IP, AppleTalk, source route bridge, and IPX connections. For each destination remote system, there is one connection entry per protocol (IP, IPX, AppleTalk, and source route bridge) per virtual circuit. The operation status of a connection entry indicates whether the connection has been established or disconnected.

Because multiple protocols can be multiplexed over a single permanent virtual circuit (PVC) connecting the same remote destination, multiple connection entries can be associated with the same PVC. You can initiate a disconnect call manually by deleting a connection entry.

RCONSOLE

RCONSOLE is a client utility that allows access to a Novell Internet Access Server 4.1 console from an IPX workstation and enables the workstation to operate as a virtual console.

XCONSOLE

XCONSOLE is an NLM utility that allows access to a routing console from an IP workstation (for example, a LAN WorkPlace® for DOS workstation) and enables the workstation to operate as a virtual console.

SNMPLOG

When loaded, SNMPLOG is an NLM utility that creates SNMP log files for trap capture. These log files can be viewed under the Display Traps option in the protocol console utilities (such as ATCON, IPXCON, TCPCON, FRCON, PPPCON, and X25CON). You must enter the LOAD SNMPLOG command at the server prompt before traps can be displayed.

ManageWise

ManageWise® software provides a Microsoft* Windows*-based SNMP management station. Its Management Information Base (MIB) browser allows remote access of the NetWare Link/Frame Relay™ MIB, as well as other routing software MIBs.

Specific Troubleshooting Tools

Table 5 lists the available diagnostic tools for routing and remote access. For a detailed explanation of each tool, refer to the troubleshooting section for the appropriate protocol.

Table 5   Specific Troubleshooting Tools

Protocol or Feature	Troubleshooting Tools
AIO ports	AIO port trace
	Identify Port
	Terminal Mode
	TRACEROUTE
Modem script files	WMDMMGR
ISDN	CAPITRCE
Remote Access	NWCRPAIR
	Port Status
Mobile Client	NWCWARN
IPX	IPXCON
	IPXPING
	DISPLAY SERVERS command
	DISPLAY NETWORKS command
	RESET ROUTER command
	TRACK ON command
IP	TCPCON
	PING
	TPING
AppleTalk	ATCON
Source route bridge	BRGCON
PPP	PPPCON
	PPPTRACE
	SPFCON
	Mobile Monitor Icon

Protocol or Feature	Troubleshooting Tools
ATM	ATMCON
	ATMTRACE
Frame relay	FRCON
	FRTRACE
X.25	X25CON
	X25TRACE

Resolving Memory Problems

To make more memory available on your server until you can add more memory to your system, perform one or more of the following tasks:

- Use the SET MINIMUM PACKET RECEIVE BUFFERS command to reduce the number of buffers used.

- Use the FILER (or NetWare® Administrator utility) to purge deleted files on the specified directory that cannot be purged automatically. (Deleted files are using up directory table space.)

- Use the REMOVE DOS or SECURE CONSOLE command to make more memory available in the server that has been reserved for DOS.

- Unload the NetWare Loadable Module™ (NLM™) programs, such as INSTALL or MONITOR, that are not currently required.

- Dismount volumes that are not being used.

- Delete unused files and directories on the specified volume.

- Change the Minimum File Delete Wait Time SET command parameter in the AUTOEXEC.NCF file so that files can be purged immediately rather than being retained in a salvageable state on the volume.

- Reduce the size or number of volumes that the server supports.

- As a last resort, back up all files in your volume, bring down your server, and use the INSTALL command to reinitialize the volume. Specify a block size of 64 KB and turn the Block Suballocation option to Off. (This setting uses a large amount of disk space but increases the amount of memory available.)