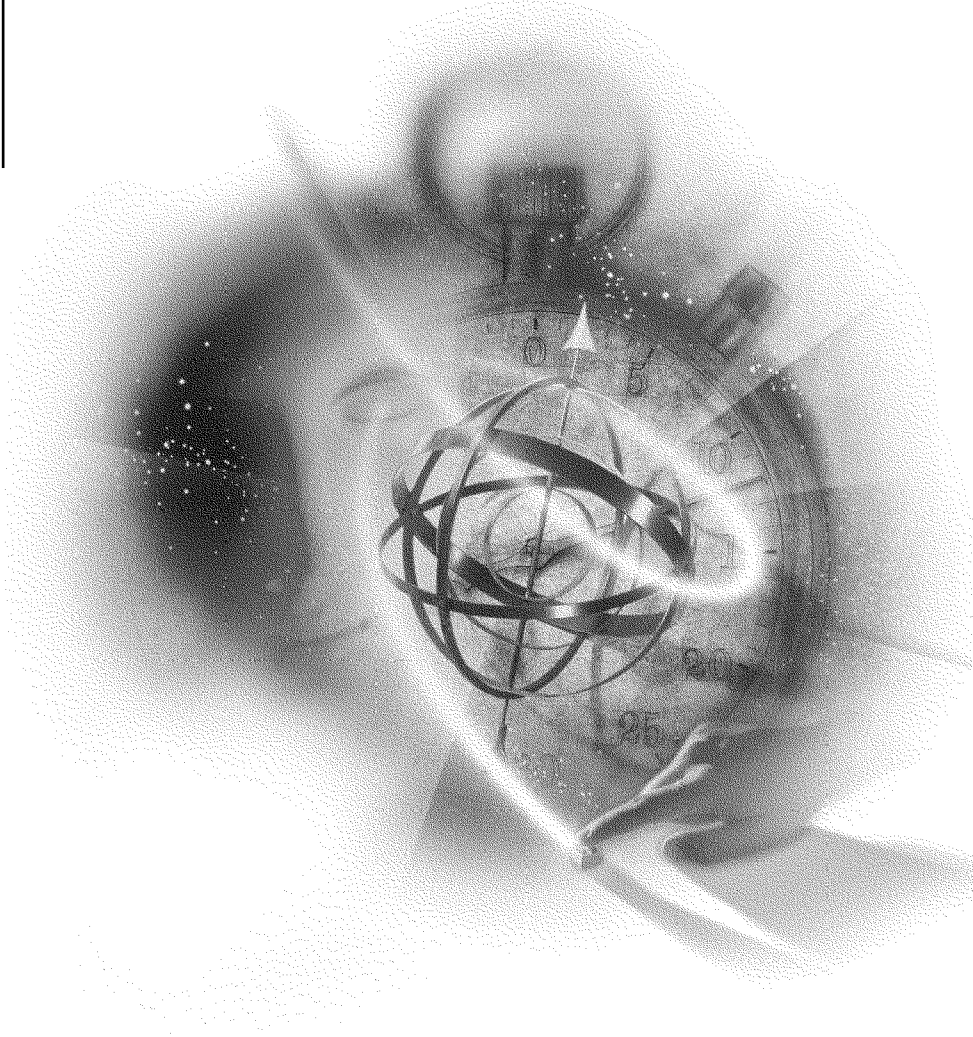


Remote Access Configuration



Connectivity Services

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.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1993-2000 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 Nos. 4,555,775; 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,594,863; 5,608,903; 5,633,931; 5,652,854; 5,671,414; 5,677,851; 5,692,129; 5,758,069; 5,758,344; 5,761,499; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,275; 5,832,483; 5,832,487; 5,859,978; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,893,118; 5,903,650; 5,905,860; 5,913,025; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,467; 5,956,718; 5,974,474. U.S. and Foreign Patents Pending.

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

www.novell.com

Remote Access Configuration
January 2000
104-001259-001

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

Novell Trademarks

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

Third-Party Trademarks

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

Contents

1	Understanding	15
	Inbound and Outbound Services	15
	Dialing In to the Network	17
	Dialing Out of the Network	17
	Remote Node Versus Remote Control	17
	Remote Access Architecture	18
	X.25 Support for Remote Access	21
	AIOPAD	21
	NetWare Link X.25	22
	NCS and NASI	23
	PPPRNS and Remote Dialer Software	23
	Remote Access Security	24
	Usernames	25
	Passwords	25
	Restrictions	28
	The Role of ConnectView	29
	ConnectView 2.1 Features	30
2	Planning	39
	NetWare Rights for Remote Access	39
	Allowing Access for Existing Users	39
	Adding New Users	40
	Restricting User Access	40
	Remote Access Client Software Distribution and Licensing	40
	Support for Apple Remote Access and Mac2NCS	41
	Installing Novell Client for Macintosh	41
	Installing and Using Mac2NCS	42
	X.25 Support	42
	Hardware Requirements	42
	Software Requirements	42
	Remote Access Security	43
	Types of Access Security	43
	Security Options	49
	Remote Access Server Management with ConnectView	51
	Software Requirements	51
	Hardware Requirements	51
	Network Requirements	52
	Server Requirements	52
	Preparing to Use ConnectView for Trend Analysis and Accounting	52

3	Setting Up	55
	Using the Automated Setup Program	56
	Loading PPPRNS	60
	Specifying Load Parameters for PPPRNS	60
	Loading NCS	61
	Loading ARAS	62
	Step 1: Loading AppleTalk	62
	Step 2: Specifying Load Parameters for ARAS	63
	Verifying the Automated Configuration	64
	Remote Access Drivers and Ports	65
	Configuring Boards for Running PPP over Asynchronous Ports	66
	Sharing AIO Ports with the NetWare Routing Software	67
	How to Configure Boards for Running PPP over Asynchronous Ports	68
	Configuring Boards for Point-to-Point Tunneling Protocol (PPTP)	70
	Installing and Configuring X.25 Adapters	71
	Step 1: Install an X.25 Adapter	71
	Step 2: Configure the X.25 Interface Board	72
	Step 3: Configure the Network Interface	75
	Step 4: Configure the WAN Call Directory (Optional)	77
	Loading the AIO Drivers	79
	Loading the X.25 Driver and AIOPAD.NLM	80
	Configuring Ports	81
	Configuring Ports for ISDN	81
	Configuring Ports for Remote Access	83
	Removing a Port from the List of Configured Ports	85
	Creating Port Groups	86
	Configuring AIOPAD and X.25 Ports	87
	Configuring AIOPAD	87
	Configuring Remote Access Ports for X.25 Support	89
	Support for Remote Nodes	90
	Remote IPX Nodes	91
	Remote IP Nodes	92
	Remote AppleTalk Nodes	95
	Support for Dial-Out Nodes	97
	Loading NCS	98
	Distributing the Client Software	98
	Configuring for a Modem-Independent Port Group	100
	Setting Up Security	101
	Configuring Clients Dialing Out	101
	Support for Remote Control Dial-in Connections	103
	Configuring the Host	104
	Configuring the Remote Workstation	104
	Support for Remote Control Dial-In Connections Through IPX	105
	Configuring the Host	105

6 Remote Access References

Configuring the Remote Workstation	105
Remote Access Services	105
Configuring PPRNS	106
Specifying Optional IPX Parameters	107
Specifying Optional IP Parameters	109
Specifying ISDN Short-Hold Parameters	112
Specifying PPP Multilink	113
Configuring ARAS	113
Verifying Data Integrity	115
Configuring NCS	115
General Names	116
Specifying the NCS Configuration	119
Remote Access Security	121
Authorizing Users for Specific Services	121
Authorizing Ports for Specific Services	122
Setting Global Security	123
Setting Remote Client Passwords	125
Configuring for Third-Party Security	128
Remote Access Parameters in NetWare Administrator	129
Setting Remote Access User Parameters	129
Setting Remote Access Service Parameters	130
Setting Remote Access IP Filtering	132
Support for SNMP and ConnectView	133
Remote Access Management Agent Overview	133
Configuring the SNMP Agent	134
Loading RAMA	138
ConnectView	138
Starting ConnectView	140
Exiting ConnectView	140
Installing with ManageWise	140
Using ManageWise SNMP Options	143
Starting from ManageWise	143
4 Optimizing	145
Port Configuration	145
Advanced Port Configuration	146
Port Groups	149
Ports Available for Remote Access	150
Ports for Unidirectional Support	150
Port Access Time	151
User-Specific Remote Access Security	152
Service-Specific Remote Access Security	155
Configuring PPP Remote Node Service Security	155
Configuring NAS1 Connection Service Security	156

Configuring AppleTalk Remote Access Service Security	157
Third-Party Dialers for Use with Remote Access Services	160
Setting Up the Windows 95 Dial-Up Networking Dialer	160
Dialing In to the Server Using the Windows 95 Dial-Up Networking Dialer	161
Setting Up the Windows NT 3.51 Remote Access Services Dialer	161
Dialing In to the Server Using the Windows NT 3.51 Remote Access Services Dialer	162
Setting Up the Windows NT 4.0 Dial-Up Networking Dialer	162
Dialing In to the Server Using the Windows NT 4.0 Dial-Up Networking Dialer	163
Macintosh Dial-In and Dial-Out Connections	163
Apple Remote Access Clients Dialing in to the Network	164
Before Connecting	164
Establishing a Connection	164
Logging In to the Network	165
Setting the Remote Access Password	166
Saving Memory after Connecting	169
Disconnecting from the Network	169
Mac2NCS Dial-In and Dial-Out Connections	169
Installing Mac2NCS	169
Installing IPXNetStat	171
Configuring Mac2NCS	171
Using Mac2NCS	178
NetWare Link/X.25 Configurations	179
Network Interface Configuration Parameters	180
Viewing and Configuring Profile Parameters	182
Profile	182
Profile Type	182
Frame Level Parameters	182
Packet Level Parameters	185
Virtual Circuit Setup	188
User Facility Setup	190
Conformance Options	193
Frame Node Type	196
Packet Size (In/Out)	196
Frame Window Size	196
Packet Window Size (In/Out)	196
Number of VCs (PVC/In/Two-Way/Out)	197
Expert PVC Configuration Parameters	197
Authentication Options Parameters	198
WAN Call Directory Configuration Parameters	200
Call Destination Name	200

5	Managing	207
	Remote Access Using RCONSOLE	207
	Starting Remote Access	208
	Bringing Down Remote Access	208
	Remote Access Soft Shutdown	209
	Resuming Remote Access	209
	Remote Access Using Console Utilities	209
	Remote Access Using NIASCFG	210
	The Configure NIAS Option	211
	The View Status for NIAS Option	211
	Modifying Set Up Parameters for Remote Access Management	212
	Setting Directory Context	212
	Specifying Server Information	213
	Specifying Audit Trail Parameters	213
	Generating Remote Access Configuration Reports	214
	Viewing Remote Access Status Options	217
	Viewing Remote Access Port Status	218
	Viewing Remote Access Port Statistics	220
	Current Settings	221
	Port Information	221
	Port Statistics	221
	Saving Information to a File	221
	Activating Remote Access Port Traces	221
	Starting a Port Trace	221
	Stopping a Port Trace	222
	Viewing Trace Files	222
	Resetting Remote Access Ports or Sessions	222
	Viewing Remote Access Port Identification	223
	Changing Remote Access Port Configuration	224
	Viewing Remote Access Service Status and Statistics	224
	Viewing NCS Status	225
	Viewing Service Statistics	226
	Viewing Remote Access Alerts	229
	Saving Alerts to a File	229
	Managing Alerts with Display Options	229
	Viewing the Remote Access Audit Trail	229
	Remote Access Using ConnectView	230
	Displaying and Managing Servers and Their Resources	230
	Managing and Monitoring Connections and Ports	232
	Managing Port Connections	233
	Viewing Port Status	234
	Setting Port Thresholds	235
	Managing NASI Connection Service (NCS) Sessions	235
	Accessing Log Files and Log Reports	237

Configuring Audit Trail Recording	237
Using Alerts Files	238
Using Audit Trail Files	241
Loading and Unloading Services	243
Setting Application Preferences	244
Displaying and Using Trend Analysis Data	246
Setting the Trend Analysis Display Options	247
Using the Trend Analysis Split Window	247
Saving Trend Analysis Data	248
Outputting Trend Analysis Data	248
Interpreting Trend Analysis Data	249
Maximum Ports Usage Graphs	249
Connections by Direction Graphs	252
Connections by Service Graphs	254
Connection Attempts Graphs	255
Connection Duration Graphs	256
Traffic Statistics Graphs	258
Usage by Media Graphs	261
Setting Up Accounting Profiles and Generating Billing Charges	262
Setting the Rate per Minute Charge	265
Setting the Rate per Connection Charge	266
Setting the Overhead Rate Charge	267
Entering Billing Rates	268
Setting Up a Time of Day Rate Table	269
Setting Holidays	270
Setting Up a Baud Rate Table	271
Setting Up a Port Rate Table	272
Setting Up a Service Rate Table	273
Viewing Sample Billing Charges	274
Assigning Accounting Profiles and Account Numbers to Users	276
Adding Users and Removing Users from a Profile Assignment	276
Selecting an Accounting Profile	278
Setting Up Account Numbers	278
Displaying Billing Charges	279
Specifying a Billing Period and Accessing the Accounting Log Window	280
Accessing the Accounting Report Window	285
Customizing the Accounting Report	286
Displaying Incomplete Connections and Connections with Duplicate IDs	286
Printing, Copying, and Exporting Accounting Data	288
Copying Accounting Data	289
Printing Accounting Data	289
Exporting Accounting Data	289
Remote Access from the ManageWise Console	289
Managing Alerts	290

Monitoring Alerts from the NetView Console	292
NetWare Link/X.25	293
Using the X.25 Console Utility	294
SNMP Access Configuration	295
X.25 Network Interfaces	296
X.25 Interface Menu	297
Active Virtual Circuit Summary	298
Cleared Virtual Circuit Summary	300
Logical Channel Range Summary	301
Packet Layer Operating Parameters	302
Packet Layer Statistics	304
Link Layer Flow Table	306
Link Layer Operating Parameters	307
Link Layer Statistics	308
Physical Layer Status	309
Physical Layer Operating Parameters	310
Physical Layer Statistics	311
X.25 Call Target Summary	312
X.25 Call Target Database	312
X.25 Ping Remote System	314
Display Traps	316
Using the X.25 Trace Utility	316
Network Interface Information Window	317
Real-Time Monitor Window	317
Play Back Window	318
Configuration Window	319
Exiting X25TRACE	319
6 Troubleshooting	321
Using Terminal Mode, NCS Debug, or NWCRPAIR Utilities	322
Using the Terminal Mode Option	322
Using the NCS Debug Utility	323
Running NWCRPAIR	325
Remote Access Cabling	325
Common Problems	326
Ports and Modems	329
Troubleshooting Tools	329
Configuration Tips	329
Common Problems	332
Remote Access Server Configuration Problems	336
AppleTalk zones do not appear on the network	336
Data transfer errors or a PC lockup occurs	336
More than one server is running Novell Internet Access Server 4.1, and one server does not show up on the network	336

A remote access server halts unexpectedly.	336
You have restarted a server after loading the remote access software, and the server cannot find the license data, the server has corrupted the audit trail database, or the Remote Access Supervisor (NWCSU.NLM) reports problems logging in to the network.. . . .	337
When you start the remote access software, error messages appear that indicate your server has insufficient memory.	337
AIOPTTP Problems	338
Remote Node (PPRNS and ARAS) Connections	338
Troubleshooting Tools	338
Configuration Tips	339
Troubleshooting Checkpoints	339
Common Problems	342
Remote Control (NCS) Connections	345
You cannot see ports under Win2NCS.	345
Users dialing in with a remote control application have trouble connecting.. . . .	345
No NCS service names are displayed when a user dials in to remote access.	346
Windows 95 Connections	346
Configuration Tips	346
Troubleshooting Checkpoints	348
NCS Dial-Out Connections	349
Configuration Tips	349
Win2NCS Connections	350
Configuration Tips	350
Common Problems	351
Mac2NCS Connections	355
Configuration Tips	355
Troubleshooting Checkpoints	356
Common Problems	356
Login Problems	360
A Novell Trademarks	363

Overview of the Remote Access Software

The remote access software provided with NetWare 5 is a server-based software solution for remote computing. The remote access software runs on a NetWare[®] server and provides a common platform for remote node and remote control technologies. With remote access, multiple remote users can access IPX- and IP-based networks, and network workstations can access host computers through telephone lines (including ISDN), leased lines, X.25 packet-switched networks, or direct connections.

NOTE: You must install the Novell[®] Internet Access Server 4.1 product option on your NetWare 5 server to copy the remote access software. If you install Novell Internet Access Server 4.1 on a server that was upgraded from a NetWare 4.11 server that ran NetWare Connect 2.0, all previously defined groups, restrictions, and other definitions from NetWare Connect 2.0 are retained. However, RNS services are no longer supported.

1

Understanding

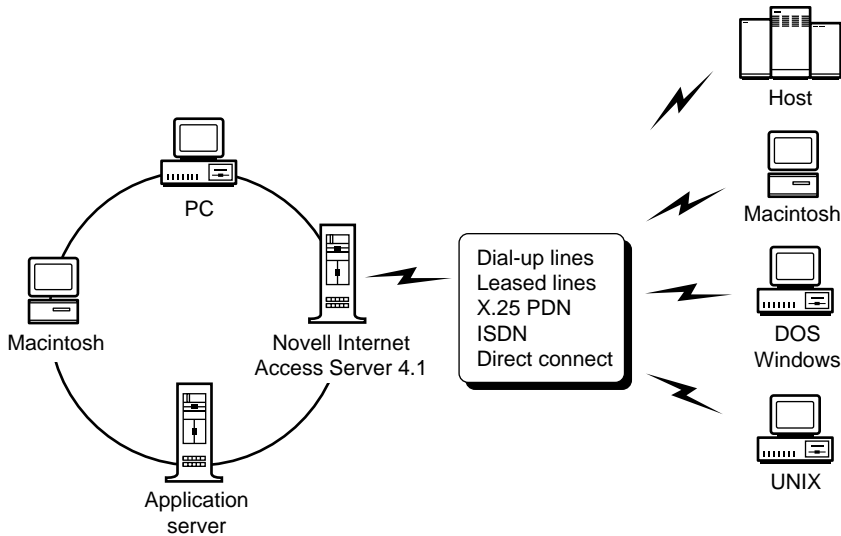
Use this section to familiarize yourself with the difference types of remote access connections supported, the remote access architecture for NetWare servers, and remote access security requirements.

Inbound and Outbound Services

NetWare 5 remote access supports inbound and outbound services. It lets a wide range of different clients dynamically share common ports, thereby eliminating the need for dedicated ports or separate communications servers for each client type.

Figure 1 shows examples of inbound and outbound communications. The PC and Macintosh* computers on the network require remote access ports to access bulletin boards or a host computer. At the same time, the remote Macintosh computer and remote PC running Windows* are using other available remote access ports to access network resources.

Figure 1 Examples of Inbound and Outbound Communications



Remote access services includes the following client software:

- ◆ Windows-to-NCS (Win2NCS)
- ◆ Macintosh-to-NCS (Mac2NCS)
- ◆ Novell Remote Access Dialer for Windows 3.x

The remote access services dial-out service for Macintosh* (Mac2NCS) requires application packages that support the standard serial driver interface.

The remote access services dial-out service for Windows* (Win2NCS) requires application packages that support the standard Microsoft* Communications API.

Users can access remote access services using the following dialer software:

- ◆ Windows NT* 3.51 Remote Access Services
- ◆ Windows NT 4.0 Remote Access Services
- ◆ DOSDIAL
- ◆ Windows Dialer
- ◆ LAN Workplace[®] 5.0
- ◆ Novell[®] Mobile Services (for Windows 95* and Windows 3.x)

Remote access services also supports Apple* Computer's Apple Remote Access software. Apple Remote Access provides user interfaces for connecting to a remote access services port.

Dialing In to the Network

A dial-in connection can be made through a modem dialing directly to a modem that is attached to a NetWare server. Once remote users have established a connection to the network, they have access to any resources available on the network. These resources can include mainframe hosts, UNIX* networks, application servers, etc. There are two types of dial-in connections: remote node connections and remote control connections.

Dialing Out of the Network

As with remote control connections, there are two ways to dial out of the network. If you have a modem attached to your machine, you can dial out using your local modem. If you do not have a modem attached, you can dial out of the network through the modem pool to such remote services as bulletin boards or host computers.

For information on using Win2NCS to dial out of the network or to create a remote node connection, see the help file (DIALOUT.HLP) included with Win2NCS. For information on using Mac2NCS, refer to Mac2NCS Dial-In and Dial-Out Connections.

Remote Node Versus Remote Control

PC dial-in connections can be of two types: remote node and remote control.

With remote node connections, the remote PC functions as if it were a workstation directly connected to the LAN. All data required for a session (file data and application packets) is transferred over the communications link. Data processing occurs on the remote PC. Remote node connections are accomplished by using dial-in software to dial in to the network access resources. Macintosh remote node connections are made through Apple* Remote Client and the AppleTalk* Remote Access Service (ARAS) server.

With remote control connections, the remote PC controls a dedicated workstation on the LAN. Only keystrokes and screen updates are transferred over the communications link. Data processing occurs on the dedicated workstation on the LAN.

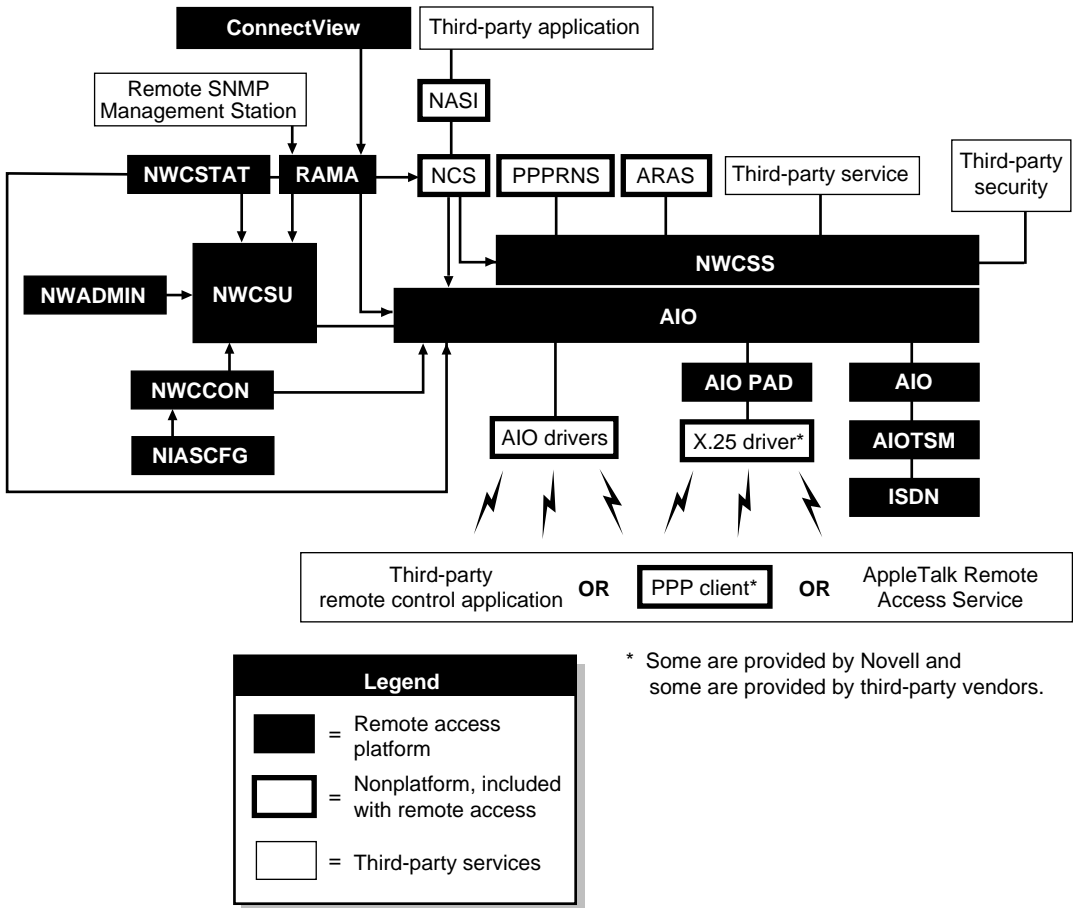
If you have a modem attached to your workstation on the network, you can dial directly in to your computer and remotely control it using third-party software such as pcAnywhere*, ReachOut*, PROCOMM*, LapLink*, and CarbonCopy. If you do not have a modem attached to your workstation, you can dial in to your workstation through the modem pool attached to your server using Win2NCS or Mac2NCS and third-party software.

For information on using Win2NCS to remotely control a computer, see the help file (DIALOUT.HLP) included with Win2NCS. For information on using Mac2NCS, see Mac2NCS Dial-In and Dial-Out Connections.

Remote Access Architecture

The remote access software provides an open platform for third-party development. Figure 2 illustrates the remote access architecture and its primary components.

Figure 2 Remote Access Architecture



The remote access components shown in Figure 2 include the following:

- Asynchronous Input/Output (AIO)** —AIO.NLM controls a group of NetWare Loadable Module™ (NLM™) files that provide an interface between the serial port (COM or other AIO port), the communications drivers, and the remote access services, and is independent of the hardware used. You install and configure the AIO software as part of the remote access configuration. AIO facilitates port sharing, independent modem control, logical port management, and automatic port acquisition. AIO.NLM. When AIO drivers load, they register their capabilities and the number of ports with AIO.NLM. All AIO drivers automatically load AIO.NLM.

- ♦ **NetWare Connect Service Selector (NWCSS)** —Because remote access supports diverse client types, it features NWCSS.NLM, which automatically routes incoming calls to the appropriate service. The Service Selector interfaces with AIO and monitors ports on behalf of the registered services. The Service Selector determines the appropriate destination of the incoming data, then relinquishes port control to the appropriate service. In a remote control dial-in connection, the Service Selector queries the caller for the available session (network workstation) to which the caller wants to connect.
- ♦ **NetWare Connect Supervisor (NWCSU)** —NWCSU.NLM provides configuration and dynamic reconfiguration support. It also supports security, license checking, and network management, and it updates port status. NWCSU.NLM provides a library of functions, including dialback, audit trail, and alert logging.
- ♦ **NetWare Connect Configuration (NWCCON)** —NWCCON is a utility that is launched by NIASCFG, which you use to configure and manage remote access.
- ♦ **NetWare Administrator (NWADMIN) snap-in for remote access** — Novell Internet Access Server 4.1 contains Windows 3.x, Windows 95*, and Windows NT* snap-ins for NetWare Administrator that enable you to set remote access configuration information for users and servers.
- ♦ **Point-to-Point Protocol Remote Node Service (PPRNS)** —PPRNS provides PPP support for remote Windows clients using the Internetwork Packet Exchange™ (IPX™) protocol or Internet Protocol (IP).
- ♦ **NASI™ Connection Service (NCS)** —NCS establishes a logical connection between a remote access port and a network workstation. This connection enables network workstations (PCs and Macintosh computers) to dial out of the network with third-party applications using a pool of modems on the server.

Similarly, dial-in users (PC or Macintosh) can use third-party *remote control* applications to remotely control a dedicated workstation or an application server on the network through NCS. NCS manages the connection between the calling PC and the network workstation.
- ♦ **AppleTalk Remote Access Service (ARAS)** —ARAS supports remote Macintosh clients using Apple's ARA 1.0 or ARA 2.0. The Macintosh clients dial in to become *remote nodes* on the network.
- ♦ **AIOPAD** —Remote access supports the transmission of asynchronous data over synchronous protocols such as X.25. With remote access,

network workstations can use an X.25 packet-switched network to dial out to host computers, and remote users can dial in and access network resources. This module provides an AIO interface to an X.25 driver.

- ◆ **Remote Access Management Agent (RAMA)** —RAMA (NCMA.NLM) enables you to manage remote access from any Simple Network Management Protocol (SNMP)-based console on the network. RAMA interfaces with other management consoles through SNMP. It provides all remote access information to the ManageWise™ software or to any SNMP-based console on the network.

X.25 Support for Remote Access

The remote access software allows LAN workstations to use an X.25 packet-switched network to dial out to synchronous host computers and allows remote users to dial in and access network resources. The following remote access software components provide this capability:

- ◆ AIOPAD
- ◆ NetWare® Link/X.25™ software
- ◆ The NetWare Asynchronous Services Interface™ (NASI™) Connection Service (NCS) and NASI
- ◆ Point-to-Point Remote Node Service (PPRNS) and its remote client software

AIOPAD

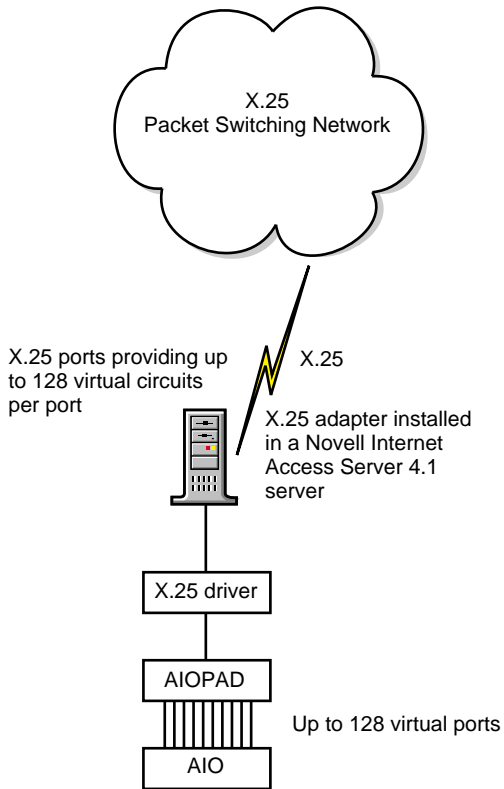
AIOPAD, a NetWare Loadable Module™ (NLM™) file included with remote access, provides an asynchronous input/output (AIO) interface to support an X.25 driver. AIOPAD mediates between the AIO NLM and the X.25 driver to provide up to 128 virtual circuits for each physical port on the X.25 adapter. AIO and the remote access software interact with each virtual circuit as if it were a physical port. The number of circuits that can be active at one time is limited by the number of remote access licenses installed on the server and by port availability.

AIOPAD's X.25 implementation is based on the X.3 and X.29 ITU-T (International Telecommunications Union, Telecommunications Standardization Sector), formerly CCITT, standards and a subset of the X.28 ITU-T standard.

The AIOPAD NLM is installed automatically when remote access X.25 support is installed.

Figure 3 shows the relationship between AIO, AIOPAD, and an X.25 board driver.

Figure 3 Relationship Between AIO, AIOPAD, and an X.25 Driver



NetWare Link X.25

NetWare Link/X.25 is a software subsystem that operates in the remote access environment and also with other Novell communications server products.

NetWare Link/X.25 is installed automatically when remote access X.25 support is installed.

NCS and NASI

The NetWare Asynchronous Services Interface (NASI) Connection Service and its client software, NASI, allow NASI users on the NetWare LAN to establish a connection to an X.25 network and access resources available through the network. Remote NASI users can also dial in to remote access through an X.25 network.

PPPRNS and Remote Dialer Software

The remote access PPPRNS service supports the following dialers:

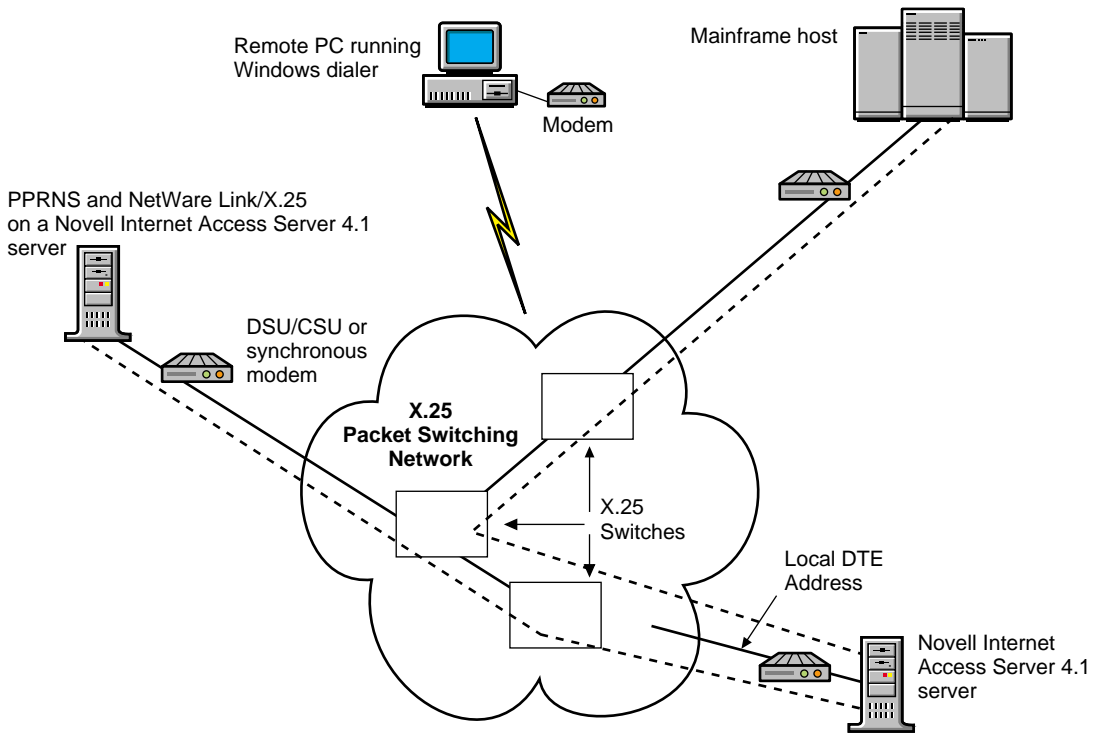
- ◆ Novell Client™ Remote Access Dialer (Windows* 3.x)
- ◆ Windows* 95 Dial-Up Networking dialer
- ◆ Windows* NT Remote Access Server dialer

NOTE: PPPRNS is also backward-compatible with older Novell dialers, such as DOSDIAL and Windows Dialer, which were shipped with NetWare Connect™ 2.0; NetWare Mobile™ software; and LAN WorkPlace® 5.0 software. The NetWare Connect 1.0 RNR dialer is no longer supported.

Using these dialers, remote users can dial in to remote access through an X.25 network.

Figure 4 shows a remote workstation running the Windows dialer to dial in to a remote access server running PPPRNS and NetWare Link/X.25.

Figure 4 Remote Dialer Software and Remote Access X.25 Connections



Remote Access Security

There are several ways you can set up remote access security to prevent unauthorized access. In addition to supporting NetWare[®] security (verifying NetWare password expiration), remote access provides port security at connection time.

Remote access security controls access to the remote access ports and services and determines the following:

- ◆ Which callers can establish connections
- ◆ When callers can establish connections
- ◆ Which resources callers can use on the network

You can authenticate remote access security both logically and physically. Logical authentication involves assigning usernames and passwords, and setting up restrictions. Physical authentication involves installing third-party hardware devices between the remote access ports and the modems.

Username

Username provide the first level of security. In a NetWare 4™ or later environment, by default, all users in the container that you specified as having the Connect Rights Level can access the remote access server and establish a logical connection to the network. The user's access rights depend on the user's physical location in the tree and the trustee rights assigned to the CONNECT object.

Another way to restrict access by username is to use the console SET commands **SET NWC CHECK CONTEXT=ON** and **SET NWC CHECK CONTEXT NAME=<context>**. Only users with names of *context* are allowed access.

Password

Before establishing a connection, remote access authenticates clients by prompting them for one of the following passwords:

- ◆ NetWare password
- ◆ Remote Client password

NOTE: Remote access allows you to disable security and the prompt for the remote access Remote Client password.

Remote Client Password

The Remote Client password is designed so that NetWare security is not compromised by passing NetWare passwords in plain text or any other form over the wire. Remote Client passwords are used in the following cases:

- ◆ Remote AppleTalk nodes.
- ◆ Remote Windows or IP nodes using the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP) method of authentication. (The Windows 95 and Windows NT dial-up networking support uses PAP or CHAP.) The passwords for PAP and CHAP are case-sensitive.

Remote Client passwords are not required if you are using the default NetWare Connect™ Authentication Protocol (NWCAP) security.

- ◆ Remote control dial-in users.

NOTE: If a Remote Client password is not assigned, the remote user using PAP or CHAP cannot gain access without a password. The remote user can gain access without a password only if the administrator enters `set PPPRNS AdmitNoConfig=ON` at the server console. Set this flag to OFF to require a Remote Client password. By default, this flag is set to OFF and a Remote Client password is required.

Initially, you assign Remote Client passwords and then allow callers to choose and change their passwords. You can enhance security for Remote Client passwords by requiring the following:

- ◆ Minimum password length
- ◆ Limited number of connection attempts

If you allow callers to change their passwords, you can increase password security by requiring users to change passwords periodically. Remote access provides Windows and Macintosh tools to enable remote node users to change Remote Client passwords. Refer to the Novell Internet Access Server 4.1 remote access online help for more information about these tools. The NetWare Connect Service Selector (NWCSS) also provides an option for remote control dial-in users to change their Remote Client passwords. Passwords can contain up to 16 characters if the extended password feature is enabled.

Figure 5 , Figure 6 , and Figure 7 illustrate how security is implemented for each of the remote access services: PPP Remote Node Service (PPRNS), AppleTalk Remote Access Service (ARAS), and NASITM (NetWare Asynchronous Services InterfaceTM) Connection Service (NCS), respectively.

Figure 5 PPPRNS Security

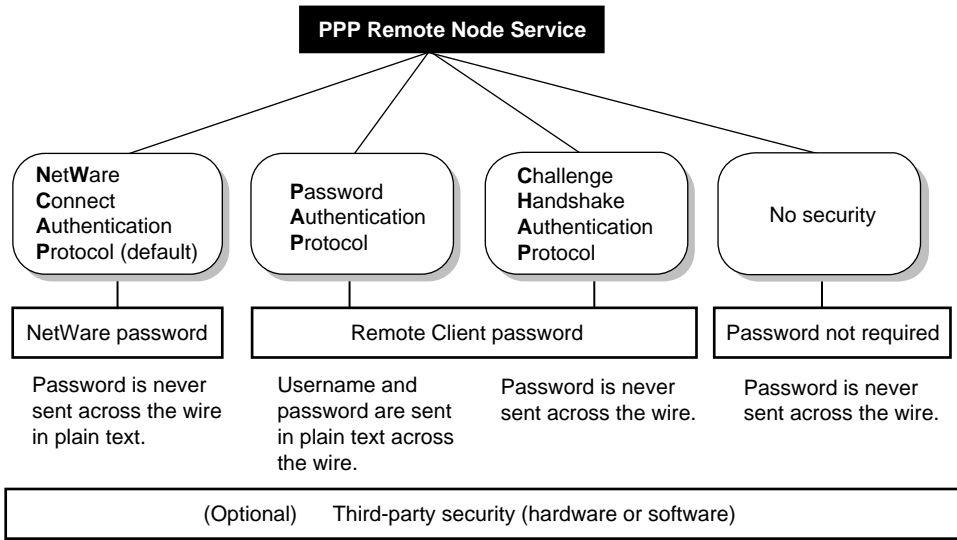


Figure 6 ARAS Security

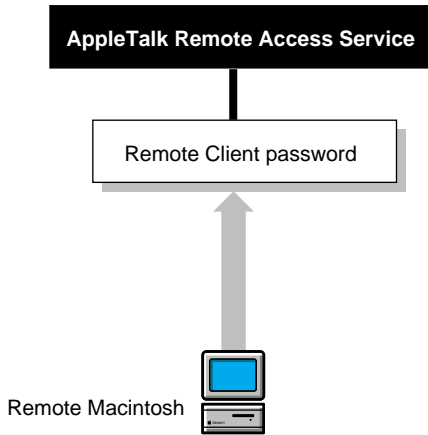
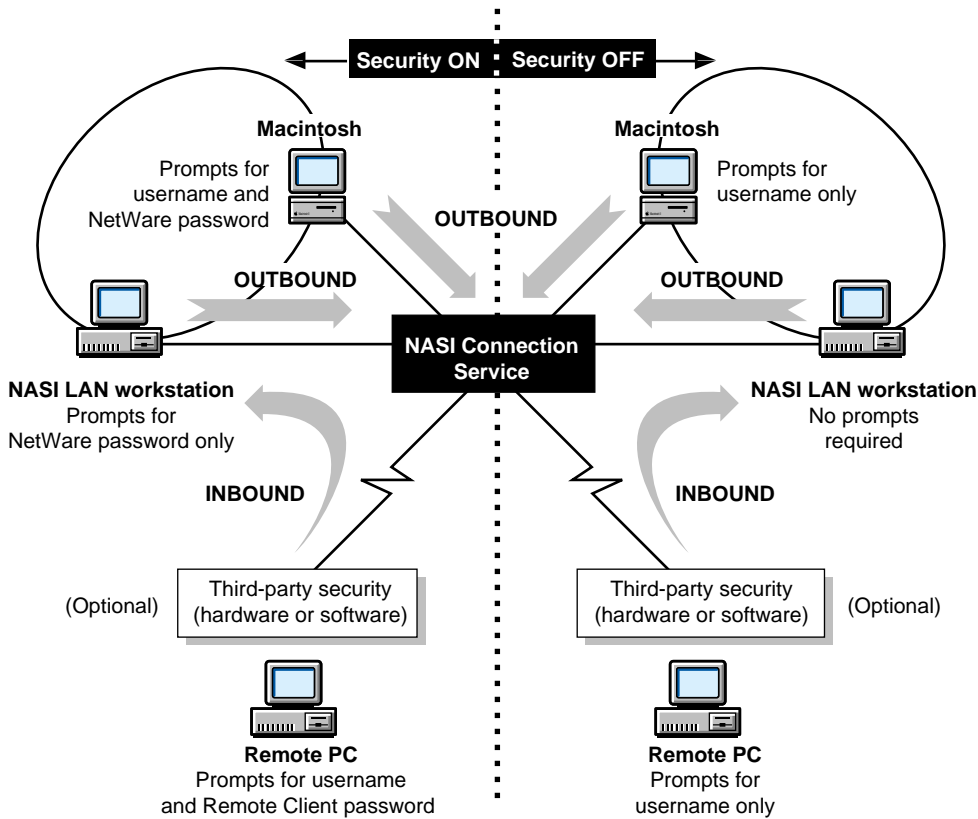


Figure 7 NCS Security



Restrictions

Restrictions control when and where a caller can connect, and they protect your network from unauthorized access. The following restrictions are configurable within remote access; however, after you establish a connection, NetWare security applies during login:

- ♦ **Port restrictions** —These restrictions limit users or services from accessing all ports.
- ♦ **Service restrictions** —These restrictions limit users or ports from accessing all services.
- ♦ **Time restrictions** —These restrictions limit the amount of time users can remain connected, disconnect a user if a connection remains idle for

a set time, and limit the hours (the time of day and week) that a service can access a port.

- ◆ **Zone restrictions** —These restrictions limit callers from accessing specific AppleTalk zones on the network.
- ◆ **Dial-out restrictions** —These restrictions limit users to dialing out to authorized telephone numbers. This applies only when a modem-independent group is used; refer to Configuring NCS.
- ◆ **Dialback restrictions** —These restrictions enforce network security and allow the user to reverse charges by having a service call back. Dialback occurs when a remote user calls in, the call is validated, and remote access disconnects the call and dials back.
- ◆ **Account restrictions** —These restrictions lock a user's account when certain limits are exceeded.

When an account is locked, no one can connect using that username. You specify that an account is locked automatically when the password expires and the three grace logins are used up, or when a set number of incorrect passwords is used.

To unlock an account locked by intruder lockout, you can modify the user's security parameters or Remote Client password. To unlock an account locked by password expiration and running out of grace logins, modify the user's Remote Client password.

The Role of ConnectView

ConnectView 2.x benefits include

- ◆ Novell Internet Access Server 4.1 remote access and NetWare Connect 2.0 server management with a server list defined from the Server Advertising Protocol (SAP)
- ◆ Real-time port and connection management to enable you to quickly view and monitor the status of each server's ports and connections
- ◆ Graphical display of port status to enable you to quickly determine port utilization and verify important configuration data and modem status
- ◆ NetWare Asynchronous Services Interface (NASITM) Connection Service (NCS) session management to enable you to dynamically monitor and manage NCS sessions

- ◆ Trend analysis graphs to enable you to evaluate resource utilization, perform capacity planning, proactively anticipate performance problems, and efficiently distribute server usage
- ◆ Accounting charges and reporting to enable you to create an accounting system, apply charges to your remote access users, and display and/or export accounting data and reports for further analysis
- ◆ Service management to enable you to dynamically load and unload remote access services
- ◆ Port threshold setting to enable you to receive proactive notification when port usage reaches a specified level on each managed server
- ◆ Generated alerts and audit trail reports with summary and daily information to enable you to print and store histories of network events and records of remote access service access and usage

ConnectView uses the remote Btrieve client to access records stored in the server-based audit trail log file for the Trend Analysis, Accounting, Audit Trail, and Alerts windows. To display this data, users must have READ/SCAN rights to the server and SYS:\SYSTEM\CSLIB directories and files.

For users already logged in to a Novell Directory Services™ (NDS™) tree, ConnectView attempts background authentication the first time an Accounting, Trend Analysis, Audit Trail, or Alerts window is opened. If the authentication is successful, ConnectView displays the data. If the authentication is unsuccessful, ConnectView displays a Bindery login box. The user must enter a valid username and password to display the data. Subsequent access to servers in the same NDS tree will occur without a login prompt.

For users not logged into an NDS tree, ConnectView displays a Bindery login box. The user must enter a valid username and password before the data will be displayed.

ConnectView 2.1 Features

ConnectView 2.1 includes the following enhancements:

- ◆ Management of Novell Internet Access Server 4.1 remote access software and existing NetWare Connect 2.0 servers
- ◆ Port media type (Asynchronous, X.25, ISDN) displayed in the View All and View windows
- ◆ Trend analysis for usage by media

- ◆ Report preferences to enable you to customize accounting, alert, and audit trail report data
- ◆ Enhanced accounting features
 - ◆ Additional fields for connected time and baud rate in the Accounting Log window.
 - ◆ An accounting log display option to enable you to limit data in the Accounting Log window by date, account number, and username.
 - ◆ Additional fields for the total dial-in connections and charges, total dial-out connections and charges, baud rate, and dial type in the Accounting Report window.
 - ◆ An additional overhead rate option to enable you to apply the overhead charge to all users, including users who did not connect to the remote access software. Previously, the overhead charge was limited to users with valid remote access connections.
 - ◆ ISDN short hold support.

Management Features

ConnectView uses a combination of the Simple Network Management Protocol (SNMP) and the remote Btrieve* client to manage your remote access servers.

To implement the SNMP connectionless management protocol, each server running the remote access software must run the Remote Access Management Agent (RAMA) and the NetWare[®] SNMP Agent (SNMP.NLM). The Remote Access Management Agent registers the IDs of the NetWare Connect[™] objects it manages with the SNMP Agent. When a request is received for data, the SNMP agent forwards the request to the RAMA service, which processes the request and returns the information to the SNMP Agent. The SNMP Agent then returns the data to ConnectView. The server's SNMP community strings are compared to the workstation's community string settings for that server. If they match, the request is performed. Otherwise, the request is denied. By default, ConnectView sets the workstation community strings to public (monitor=public control=public).

IMPORTANT: Ensure that the most up-to-date versions of NCMA.NLM and SNMP.NLM are loaded on the managed servers. ConnectView does not install the Novell TCP/IP stack and does not support SNMP over IP. Also, ensure that BSPXCOM.NLM is loaded on the managed servers and BREQUEST.EXE is running on the ConnectView workstation

ConnectView copies the necessary SNMP files to your workstation. This includes the WLIBSOCK.DLL file. If a different version of this file exists on your workstation, ConnectView displays a warning message.

However, ConnectView does not install the Novell TCP/IP stack and does not support SNMP over IP.

IMPORTANT: ConnectView SNMP options are available only when ConnectView is run in standalone mode.

ConnectView uses the remote Btrieve client to access records stored in the server-based audit trail log file for the Trend Analysis, Accounting, Audit Trail, and Alerts windows. To display this data, users must have Read/Scan rights to the server's SYS:\SYSTEM\CSLIB directories and files.

For users not logged in to a Novell Directory Services™ (NDSTM) tree for NetWare 4.1 or later servers, ConnectView displays a Bindery login box. The user must enter a valid username and password before ConnectView displays trend analysis, accounting, audit trail, and alert data.

ConnectView displays a list of all available servers in the View All window. Available servers are servers that respond to the SAP of the server you are logged in to. If you are not logged in to a server, ConnectView uses the SAP notification from the server to which you are attached.

Unavailable servers that become available after ConnectView is started can be added to the View All window by choosing View >Update (F5).

IMPORTANT: If you want to manage a server that is active but not displayed in the View All window, log in to either the desired server or a server that can receive SAP notification of the desired server. Then, from the View All window choose View > Update.

Accounting Features

To calculate billing charges, ConnectView

- ◆ Matches start connection records with end connection records to determine the valid connections that occurred during the billing period.
- ◆ Applies the rates from the rate tables to the hourly intervals of the connection durations.

Matching Start Connection and End Connection Records

ConnectView determines valid connections within the specified billing period by matching start connection records and end connection records.

If both a start connection record and an end connection record are found within the billing period for the same connection ID, ConnectView logs the connection as valid. Otherwise, ConnectView considers the connection incomplete and does not use the connection in the accounting process.

If a start connection record is found, but a matching end connection record cannot be located within the specified billing period, ConnectView searches for the end connection record one day beyond the end date of the billing period. If the matching end connection record is found within this 1-day buffer, ConnectView logs the connection as valid. If the matching end connection record is not found during the one day buffer, ConnectView considers the connection invalid and logs the connection in the Discarded Connections dialog box.

NOTE: Checking for end connection records during this 1-day buffer helps eliminate incomplete connections that might occur when connections are started near the end of the billing period.

If an end connection record without a matching start connection record is found within the specified billing period, ConnectView considers the connection invalid and logs the end connection record in the Discarded Connections dialog box. Logging the unmatched end connection records avoids duplicating billing and invalid connections across billing periods.

NOTE: The grace period, by default set to 30 seconds, determines the minimum connection duration required for a connection to be valid.

The following table summarizes the process of determining valid connections for a connection that began on 3/1/96 at 8:00 a.m. and ended at 3/4/96 at 3:00 p.m.

Billing Period	Accounting Result
3/1/96 to 3/4/96	Valid Connection The connection is included in the accounting data, because both the start time and the end time are within the billing period.
3/1/96 to 3/3/96	Valid Connection The connection is included in the accounting data, because the start time is within the billing period and the end time is outside the billing period by less than one day.

Billing Period	Accounting Result
3/1/96 to 3/2/96	Invalid Connection. The connection is counted as an incomplete connection, because the start time is within the billing period, but the end time is outside the billing period by more than one day. The start connection record is logged in the Discarded Connections dialog box.
3/2/96 to 3/2/96	Invalid Connection The connection is not included in the accounting data, because neither the start time nor the end time is within the billing period.
3/2/96 to 3/4/96	Invalid Connection The connection is not included in the accounting data and is not counted as an incomplete connection, because the start time is outside the billing period, even though the end time is within the billing period. The end connection record is logged in the Discarded Connections dialog box.

Applying Rates to Connection Durations

After the valid connections are determined, ConnectView applies the billing rates from the assigned accounting profiles to the connection durations.

For charges based on the rate per minute, ConnectView determines the amount of time in seconds that applies to each hourly interval within the connection duration. Next, ConnectView checks the hourly rates in the assigned accounting profile and applies the rates. The cost of each hourly interval is then added together to equal the total charge for the connection.

For charges based on rate per connection and overhead rate, ConnectView checks the assigned accounting profile for rates and charges, determines the connected time in seconds for each hourly interval of the billing period, and applies the assigned rates. The costs of each hourly interval are then added together to equal the total charge for the connection.

The following connection example illustrates this process.

Connected Time	Hourly Intervals	Rates per Minute	Rates per Second	Connected Seconds per Interval	Total Charges
3:30:35 p.m.-	3:00-3:59	0.60	0.01	1765	1765 x .01 =
5:30:10 p.m.	4:00-4:59	0.60	0.01	3600	17.65
	5:00-5:59	0.50		1790	3600 x .01 =
			0.008		36.00
					1790 x .008 =
					14.32
					Total Charge =
					\$67.97
09:00:10 a.m.-	9:00-9:59	0.30	0.005	3281	3281 x .005 =
09:54:31 a.m.					16.40
					Total Charge =
					16.40
11:30:15 a.m.-	11:00-	0.85	0.01	1815	1815 x .01 =
2:45:03 p.m.	11:59	0.85	0.01	3600	18.15
	12:00-	0.85	0.01	3600	3600 x .01 =
	12:59	0.85	0.01	2703	36.00
	1:00-1:59				3600 x .01 =
	2:00-2:59				36.00
					2703 x .01 =
					27.03
					Total Charge =
					117.18

IMPORTANT: Baud rate and port name rates assigned in accounting profiles do not apply to NCS dial-out and AIOPAD connections. NCS and AIOPAD do not report the baud rate used during these connections.

Handling Invalid Connections and Duplicate Connection IDs

Invalid connections are connections for which ConnectView can find only one connection record, but cannot locate the matching start or end connection record.

ConnectView automatically checks for end connection records up to one day after the end date of the billing period. If a matching end connection record is found in the one day after the billing period end data, ConnectView logs the connection as valid and includes the connection in accounting data for the

specified billing period. If the matching end connection record is not found, ConnectView counts the connection as invalid. Invalid connections are not included in the accounting data for the specified period, but they are logged in the Invalid Connections dialog box.

NOTE: Because of the checking one day beyond the end date of the billing period and to avoid duplicate billing, ConnectView discards any end connection records for which a matching start connection record cannot be found.

Duplicate connection IDs occur when a new connection record contains the same connection ID as an existing connection record of the same type. When this occurs, ConnectView displays a warning message and allows you to terminate or continue the accounting process.

If the accounting process is continued, ConnectView cannot guarantee the integrity of the accounting data.

Security Features

ConnectView uses SNMP to retrieve data with GET requests and to control the remote access software with SET requests. These management operations affect a large number of windows and are dependent on the SNMP community string settings on each managed server and the ConnectView workstation.

On the server side, you can set the desired community strings on the command line either when you are loading SNMP.NLM or through the NIASCFG utility.

IMPORTANT: By default, SNMP.NLM on your servers grants public access to the MonitorCommunity (monitor=public) but disables access to the ControlCommunity.

Table 1 describes the server SNMP community strings.

Table 1 Server SNMP Community Strings

Community String	Description
MonitorCommunity	Controls security for the read-only GET and GET NEXT operations. The default is <i>public</i> .
ControlCommunity	Controls security for the read-write SET operations. By default, this operation is disabled.
TrapCommunity	Controls security for receiving SNMP-trap messages. The default is <i>public</i> .

IMPORTANT: The ConnectView use of community strings follows SNMP v1 security.

Your workstation's community string settings must match the community string settings on the managed servers. By default, ConnectView sets the workstation community strings to public (monitor=public control=public).

To configure workstation community strings for each server, choose File > Preferences and click the SNMP Options tab button. This dialog box also contains options for SNMP time-out and retry values.

IMPORTANT: ConnectView does not support SNMP over the NetWare Core Protocol™ (NCP™) or SNMP over IP. An SNMP workstation can still access the Management Information Base (MIB) objects using the MIB browser over an IP stack.

Performance Considerations

When using ConnectView, it is important to keep several performance issues in mind:

- ◆ If large amounts of data are involved in trend analysis, accounting, audit trail, or alert log viewing, ensure that sufficient memory is available.

A substantial amount of time may be required to process large amounts of data. The time required to process the data depends on the available disk space, the number of records, and your Windows configuration. During low memory conditions, Windows may begin to swap data to disk, increasing the amount of time required to process the data. In extremely low memory conditions, you may not be able to complete the operation.

- ◆ If ConnectView is running with other Windows applications, ConnectView competes with the other applications for Windows resources and memory, especially if many windows are open.

2

Planning

This section describes the requirements for supporting remote access, which include the following:

- ◆ Assigning the appropriate NetWare rights for remote access
- ◆ Distributing client software
- ◆ Supporting Apple remote access and X.25 users
- ◆ Planning for remote access security

NetWare Rights for Remote Access

All NetWare users in the Connect container (or Connect Rights Level) can use remote access, except users in the containers that are blocked with the Inheritance Rights Filter. The Connect container (or Connect Rights Level) is the container specified during the installation of the CONNECT object in the Directory tree. Refer to your configuration report to see the Connect container context.

Allowing Access for Existing Users

To allow existing users in other containers to use remote access, you must grant the following rights to the CONNECT object:

- ◆ Browse entry rights to the container in which these users are defined
- ◆ Read attribute rights to the container in which these users are defined

NOTE: In addition to Read attribute rights, if the CONNECT object has Write attribute rights to that container, then the remote access server administrator can configure the users' remote access parameters.

Adding New Users

For a new user to be able use remote access, he or she must be added to the Directory tree. To add new users to the Directory tree, use the appropriate NetWare administrative utility from any LAN workstation. If you add the users to the Connect container, then they have immediate access to remote access; otherwise, you must grant the rights listed previously to the CONNECT object to allow those users to access remote access.

Restricting User Access

You can restrict users from accessing remote access by modifying the CONNECT's object rights to the users' container.

Modify the CONNECT object's rights using the appropriate NetWare administrative utility by removing the following rights to that container:

- ◆ Browse rights to objects
- ◆ Read attribute rights
- ◆ Write attribute rights

Remote Access Client Software Distribution and Licensing

Remote access services allows the network supervisor to distribute the remote access client software to any number of remote users.

The remote access dialer software is installed automatically when you install the Novell Client.

The software for MAC2NCS (RAMAC.EXE) is available on the Novell Client CD-ROM and is located in the PRODUCTS\MAC2NCS directory. RAMAC.EXE is a DOS formatted, compressed version of the Remote Access Mac Client folder. This folder contains the installer for Mac2NCS and the Set Remote Access Password utility. Instructions for making these files available to users are included in the RAMAC.TXT file included in the same directory.

To improve the performance of Point-to-Point Protocol (PPP) connections, NetWare files—LOGIN.EXE, LOGOUT.EXE, ATTACH.EXE, MAP.EXE, CX.EXE, NLIST.EXE, and SLIST.EXE—should be distributed to the remote PCs.

Any other program that is invoked in the user login script should also be distributed to the remote PCs.

PPP-based remote node support is provided with the remote access software. Apple Remote Access is available from Apple Computer, Inc.

Support for Apple Remote Access and Mac2NCS

To use Apple Remote Access, you need the following:

- ◆ A Macintosh computer running system software version 7.0 or later
- ◆ At least 2 MB of memory and a hard disk
- ◆ If you are using Novell Client for Macintosh, at least 4 MB of memory
- ◆ A Hayes*-compatible modem with a data rate of at least 2400 bps

HINT: We recommend that you always use the latest ARA modem scripts. Contact Apple or the modem manufacturer for the most current ARA modem scripts for your modem. If your modem is not listed in ARA, Apple offers a utility to create your own ARA modem scripts.

- ◆ Apple Remote Access software
- ◆ The Set Remote Access Password utility to modify the remote access password

This utility is shipped as a DOS executable on the Novell Client CD-ROM. Contact your network supervisor for access to this utility.

- ◆ If you will be logging in to a Novell Internet Access Server 4.1 server, you need the Novell Client for Macintosh program, including the MacIPX[®] program.

Installing Novell Client for Macintosh

If you will use the Apple Remote Access software to access a NetWare server, you need to install the Novell Client for Macintosh utility on your remote Macintosh, if it is not already installed. Contact your network supervisor for access to this utility.

To install this utility, access a Novell server through AppleTalk* or a remote connection, locate the folder where Novell Client for Macintosh is located, and then drag the folder icon to a folder on your Macintosh.

After transferring the files, click the Novell Client for Macintosh Installer icon. The utility installs automatically and is available the next time you start your Macintosh.

Installing and Using Mac2NCS

The Mac2NCS component of the remote access software allows you to redirect the input from Macintosh communications applications to NASI ports on a server. You can use Mac2NCS connections for both dialing out from and in to the network.

To dial out using Mac2NCS, you need to install Mac2NCS and a Macintosh communications application which uses the standard serial driver interface on a LAN workstation. To dial in using Mac2NCS, you need to set up a Macintosh workstation on the network and install a supported third-party application on both the workstation and the remote PC.

X.25 Support

To enable remote users to dial in or dial out through an X.25 packet-switched network, you must have the appropriate hardware and software installed.

Hardware Requirements

To support X.25 connections, you must have an X.25 adapter installed in the communications server.

A list of third-party X.25 adapters certified by the Novell Labs™ group can be found at the Novell WWW location <http://labs.novell.com>.

NOTE: The Novell labs document, How to select WAN Hardware for your Novell product, can help you to select the appropriate hardware for X.25, as well as for other WAN and dial-up adapters. This document can be found at the Novell WWW location <http://labs.novell.com/wan/certinfo.htm>.

Software Requirements

X.25 support for remote access requires the following software:

- ◆ NetWare 3.12 or later
- ◆ The remote access X.25 support files

The files for X.25 support are installed during the Novell Internet Access Server 4.1 installation. The X.25 support files include the drivers from the NetWare Link/X.25 product, the AIOPAD NLM, and other required files.

Remote Access Security

Before you install the remote access software, you should create a security plan for remote users dialing in to your network. This involves selecting the type of access security you want to implement and whether the restrictions will be placed globally or for selected users only.

Types of Access Security

Remote access provides the following levels of access security:

- ◆ Default Security
- ◆ User-, Port-, and Service-Level Security
- ◆ Global Security for All Users
- ◆ User-Specific Security
- ◆ Service-Specific Security
- ◆ Third-Party Security

Default Security

Default security is in effect when you first install and set up a basic configuration. The default security for each service is explained in Table 2.

Table 2 Default Security Requirements

PPP Remote Node Service	AppleTalk Remote Access Service	NASI Connection Service
NetWare username and NetWare password	NetWare username and Remote Client password	NASI, Win2NCS, or Mac2NCS workstation: NetWare password Remote workstation: NetWare username and Remote Client password

The default security parameters specify the following:

- ◆ All users have access to all services and ports.
- ◆ All services have access to all ports at all times.
- ◆ Users can remain connected for an unlimited amount of time.

- ◆ Users cannot use the dialback feature.
- ◆ User sessions can remain idle for an unlimited amount of time.
- ◆ Users can dial out to any number.
- ◆ There are no restrictions on defining Remote Client passwords.

After the remote client establishes a connection, the remote client must log in to the NetWare network. The system does not prompt for a NetWare login until the user runs the login command.

User-, Port-, and Service-Level Security

As an administrator, you can customize the level of security by restricting the following:

- ◆ Users from accessing certain ports
- ◆ Users from accessing specific services
- ◆ Ports to a particular service for a specified time

Global Security for All Users

You can define the following security options globally for all users:

- ◆ **Maximum connection time** —You can limit the time online for all users. If you set this value to 0 minutes, remote access will immediately disconnect the user when the user dials in. If you set this value to -1, there is no limit. Connections that are already established are not affected.
- ◆ **Idle time before disconnection** —Remote access disconnects a user after the connection has been idle for a specified amount of time, in minutes. This helps you manage line usage costs by disconnecting inactive connections. This option is not valid for ARAS connections.
- ◆ **Password restrictions** —These restrictions apply to the Remote Client password that is set for each user. You can specify the number of times a user can enter an incorrect password, as well as the minimum length of the password.
- ◆ **Dialback** —You can require users to specify a dialback number at connection time. Or, you can allow users to request dialback at connection time.
- ◆ **Dial-out restrictions** —You can restrict users from dialing out to a specific number by specifying a list of authorized numbers. Dial-out restrictions apply only to modem-independent ports.

NOTE: Frame=26:/2.0 internal insetSetting a value for a security option for a user overrides, in order, the nearest container, remote access server, and global settings for that option.

User-Specific Security

You can define remote access security for each user. If you have more than one remote access server on the network, you can customize user security from a single server console. Note, however, that you must specify dial-out restrictions on each remote access server.

You can configure the following options for each user:

- ◆ **Maximum connection time** —You can limit the time online for a user. If you set this value to 0 minutes, remote access will immediately disconnect the user when the user dials in. If you set this value to -1, there is no limit. Connections that are already established are not affected. This parameter overrides any global defaults.
- ◆ **Idle Timeout** —Remote access disconnects the user after a connection has been idle for a specified amount of time. You can set the idle timeout value for a user or a container. This option is not valid for ARAS connections.
- ◆ **Dialback** —Forced dialback enables you to enforce maximum security by preconfiguring a dialback number for each caller. You can also require users to specify a dialback number at connection time, or you can allow users to choose to dial back and specify a dialback number at connection time.
- ◆ **Dial-out restrictions** —You can restrict a user from dialing out to any number by creating a list of authorized numbers for that user. Dial-out restrictions apply to modem-independent ports.
- ◆ **Remote Client password** —You can set a Remote Client password for ARAS, NCS, and PPRNS clients using the PAP or CHAP method of authentication. By default, there is no Remote Client password, and ARAS, NCS, and PPRNS services are denied without a password. The NetWare password is still required for PPRNS with NWCAP selected.

You can set the password to be valid for a specific number of days and require users to change their passwords when they expire. Remote access provides users with the tools to change their Remote Client passwords.

Once a user's Remote Client password has expired, the user must use these tools to change the Remote Client password. The user is allowed three grace logins after the password has expired. If the user logs in using

the three grace logins without changing the password, the user is denied logon to remote access. The administrator must then use NIASCFG or the NetWare Administrator utility in Windows to assign a new password to the user.

Service-Specific Security

You can configure service-specific security options for each of the following services:

- ◆ PPP Remote Node Service
- ◆ NASI Connection Service
- ◆ AppleTalk Remote Access Service

PPP Remote Node Service

You can disable PPPRNS security or enable one or more of the three supported protocols used to establish a connection:

- ◆ NetWare Connect Authentication Protocol (NWCAP)

This type of authentication is the default method for maintaining network security. With this method, users must specify the NetWare password to successfully establish a connection. This type of authentication is supported by the PPPRNS client for the remote access dialer. The NetWare password is encrypted and is not sent in plain text across the wire.

NOTE: The PPPRNS client for DOS (DOSDIAL) and Windows (Windows Dialer) NetWare Connect™ 2.0 dialers are also supported.

- ◆ Password Authentication Protocol (PAP)

This type of authentication offers minimum security. It is not enabled by default. If you enable this protocol, users must specify the Remote Client Password to successfully establish a connection. The Remote Client password is sent in plain text across the wire.

This method is supported by the PPPRNS client for the remote access dialer. Enable this option if you have UNIX clients that support PAP, such as the LAN WorkPlace® software.

NOTE: The PPPRNS client for DOS (DOSDIAL) and Windows (Windows Dialer) NetWare Connect 2.0 dialers are also supported.

- ◆ Challenge Handshake Authentication Protocol (CHAP)

This type of authentication allows third-party PPP clients that support CHAP to connect to remote access. It is disabled by default, and is used by Windows 95 and Windows NT. This method is not supported by the PPPRNS client that is shipped with Novell Internet Access Server 4.1.

This method of authentication requires users to specify the Remote Client password to establish a connection. The Remote Client password is used for encryption and is not sent across the wire.

If the default NWCAP authentication is enabled, users must specify a NetWare username and password. If you enable PAP or CHAP, users must specify Remote Client passwords.

PPPRNS negotiates the security modes in the following order (when enabled): CHAP, PAP, and NWCAP. For example, the server is configured to support both NWCAP and CHAP. If the client supports CHAP, CHAP is used. If the client supports NWCAP, NWCAP is used. If the client supports both CHAP and NWCAP, CHAP is used because it is negotiated first.

When PAP or CHAP is used, a Remote Client password must be defined to allow users access. To allow users access without Remote Client passwords, either turn off PPPRNS security or use the Set PPPRNS AdmitNoConfig=ON command at the server console to validate users without Remote Client passwords.

NOTE: To use the native Windows 95 or Windows NT dialer to connect to a Novell Internet Access Server 4.1 server, you must enable CHAP or PAP on Novell Internet Access Server 4.1 and either assign a Remote Client password to each user or allow users without Remote Client passwords to be validated.

If you want your Windows 95 dialer to use NetWare passwords instead of Remote Client passwords, you must install the latest Novell Client for Windows 95 from the client CD-ROM. Refer to the Novell Internet Access Server 4.1 remote access online help for more information. From the server console, type `SET PPPTSM NWCAPFIRST=ON`. This does not affect Windows 95 or Windows NT clients using the Microsoft client or older NetWare clients.

If security is disabled at the server side, the remote client must specify None for the security type.

NASI Connection Service

For NASI Connection Service (NCS), you apply security to the network workstation dialing out and to the remote workstation dialing in. Enabling security for the network workstation means that NASI workstations must specify a password. Enabling remote security means that remote workstations must specify a username and a Remote Client password.

AppleTalk Remote Access Service

For AppleTalk Remote Access Service (ARAS), you can restrict access to AppleTalk zones globally for all users or on a per-user basis.

Third-Party Security

Remote access supports third-party security products that implement token-based challenge/response types of security. These products have both hardware and software components. Remote access supports the software by providing a configuration option in the configuration utility. The hardware components are installed between the remote access port and the modem.

When third-party security is enabled, PPPRNS and NCS users must be validated through third-party security. After third-party security passes, call selection takes place. Any configured security for a service is applied to the call before the session is established.

PPPRNS users must configure their dialers to enter terminal mode to process the third-party security validation and transfer the call to PPP mode. If the dialer is configured incorrectly, that is, the call goes into PPP mode right away, the call will be rejected. Refer to the Novell Internet Access Server 4.1 remote access online help for information about how to use scripts for the dialers.

When the services available on a port are PPPRNS, NCS, or both, the incoming call executes third-party security as soon as the call is received. If additional services (such as ARAS) are also available on a port, the usual call selection will take place first. This enables services that do not support third-party security to accept calls even when third-party security is enabled. After the initial call selection, third-party security is executed.

If third-party security passes, a second call selection process takes place to determine which service the call is destined for.

If PPPRNS clients are configured incorrectly and the call is selected during the initial call selection process, the call is terminated.

If you have services other than PPPRNS or NCS selected, you can minimize the call establishment time for PPPRNS and NCS calls by restricting ARAS (and other services that do not support third-party security) to using specific ports.

Security Options

You use the security options in the Remote Access Configure Security menu in NIASCFG to set up remote access security. The options for security are explained in Table 3.

Table 3 Security Options

Options	Description
Restrict Ports by User	Restricts users to access a specific port or ports.
Restrict Service by User	Restricts users to a specific service.
Restrict Service by Port	Restricts ports to a specific service. Restricts port access time by service.
Set Global Parameters	Sets the following global security parameters for all users: Default maximum connection time Idle time before disconnection Default dialback mode Dialback parameters, including wait time, busy retry count, and busy retry interval Dial-out restrictions
Set User Parameters	Customizes the following user security parameters: Users allowed to change remote client passwords Remote client password expiration Idle timeout per user or container Default maximum connection time Dialback mode options Dial-out restrictions
Set User Remote Client Password	Specifies a Remote Client password for a user.

Options	Description
Set Remote Client Password Restrictions	Disables a password after a number of failed logins. Enables long passwords and sets the minimum password length.
Set Third-Party Security Parameters	Enables/disables third-party security. Selects a third-party security product. Applies third-party security to a direct connection.

NOTE: Set Third-Party Security Parameters is available only if at least one third-party security product is installed.

You can set the time allowed online, dialback options, and dial-out restrictions globally for all users or customize them for selected users. If you need a secure system, implement all the appropriate security features.

In addition to the features listed in Table 3 , service-specific security options are provided for each service. Table 4 lists the service-specific security options.

Table 4 Service-Specific Security Options

Service	Security You Can Enable	Default
PPP Remote Node Service	PPPRNS security	On
	NetWare password (NWCAP)	Yes
	Password Authentication Protocol (PAP)	No
	Challenge Handshake Authentication Protocol (CHAP)	No
NASI Connection Service	NCS dial-in security	On
	NASI security	On
AppleTalk Remote Access Service	Default zone restrictions	Access to all zones

Service	Security You Can Enable	Default
	User zone restrictions	Access to all zones
	Prompting users for password	No

Remote Access Server Management with ConnectView

This section summarizes the prerequisites for using ConnectView and how you should prepare to use it.

Software Requirements

- ◆ MS-DOS* 5.0 or higher
- ◆ Windows 3.1 or higher
- ◆ NetWare Client™ (VLMTM) 1.2 or later Novell Client™ software

IMPORTANT: If you are using the NetWare Client (VLM) 1.2 software, you can run ConnectView in both Windows 3.1 and Windows 95 environments. If you are using the Novell Client for DOS and Windows 3.1x software, you can run ConnectView in the Windows 3.1x environment. If you are using the Novell Client for Windows 95 software, the statement that loads BREQUEST.EXE is moved from your AUTOEXEC.BAT file to the WINSTART.BAT file, to enable you to run ConnectView in a Windows 95 environment.

Hardware Requirements

The ConnectView workstation must include the following hardware:

- ◆ An 80386- or 80486-based IBM PC/AT* compatible or higher computer
- ◆ A LAN adapter that, together with the drivers provided by the NetWare workstation shell, connects the ConnectView workstation to a LAN by use of SNMP over the Internetwork Packet Exchange™ (IPX™) protocol.
- ◆ A VGA or super VGA graphics card and monitor
- ◆ A mouse supported by Windows 3.1
- ◆ 8 MB of RAM
- ◆ 6 MB of disk space

NOTE: If you have removed ManageWise® from your workstation, ensure that the NMS.INI file is removed from the WINDOWS directory.

Network Requirements

If ConnectView is to operate in a WAN environment, you must have a ConnectView workstation and the hardware and software capable of connecting the WANs. This hardware and software could be a router capable of routing IPX traffic.

IMPORTANT: ConnectView does not support SNMP over IP.

Server Requirements

ConnectView manages the Novell Internet Access Server 4.1 remote access software and NetWare Connect 2.0 servers.

IMPORTANT: The BSPXCOM.NLM and NCMA.NLM files must be loaded on the managed servers.

Preparing to Use ConnectView for Trend Analysis and Accounting

ConnectView's trend analysis enables you to monitor resource usage, proactively distribute resource utilization, and perform capacity planning. To effectively use this ConnectView feature, ensure that

- ◆ Audit trail files or archived files are available
- ◆ Server and workstation software is running
- ◆ An effective display period is used

The ConnectView accounting feature allows you to create account profiles with specific billing formulas and rates, apply profiles to users, and generate accounting data in accounting log and accounting report format. To effectively use this feature, ensure that

- ◆ Audit trail file and/or archived files are available
- ◆ Server and workstation software is running
- ◆ Data processing and display requirements are considered

Maintaining Audit Trail and Archive Files

Before displaying trend analysis data or starting the accounting process, ensure that the audit trail option is enabled and sufficient data has been

recorded. Trend analysis data can be viewed only after the remote access software has recorded data in the current server's audit trail file, or there is access to data stored in an archived file. The audit trail file and/or archived files must be available before any trend analysis data can be displayed.

Because ConnectView uses the remote Btrieve client to access audit trail records, you must have READ/SCAN rights to the server's SYS:\SYSTEM\CSLIB directories in which the audit trail file and archived files are stored.

IMPORTANT: Ensure that only the audit trail file and archived files for the Novell® Internet Access Server 4.1 are used. ConnectView will not display data from other files.

Ensuring That Server and Workstation Software Is Running

For ConnectView to display trend analysis data or process accounting data, ensure that the following NetWare® Loadable Module™ (NLMTM) files are loaded on the managed server:

- ◆ BSPXCOM.NLM
- ◆ NCMA.NLM (NetWare Connect™ Management Agent)
- ◆ SNMP.NLM (NetWare SNMP Agent)

Also, ensure that BREQUEST.EXE is running on the ConnectView workstation.

Planning for Data Display

Because accessing large amounts of data could require a substantial period of time and trend analysis graphs are not scrollable horizontally, plan the display of data in manageable amounts. For example, displaying trend analysis data from 8 a.m. to 5 p.m. in hourly intervals for one day or displaying data in daily intervals for 30 days results in manageable displays of data. However, displaying data in hourly intervals for a large number of days (60, for example) could result in long delays in data processing and data that is difficult to view.

If you are accessing large amounts of data in the current audit trail file and/or archived files, displaying trend analysis data could require a substantial amount of time and memory. Also, if low memory conditions occur and Windows is configured to swap data to disk, this could increase the amount of time required to process the data.

3

Setting Up

As you complete the product installation, the remote access software runs an automated setup procedure that lets you quickly and easily set up and configure your remote access server for basic operation. The automated procedure runs the first time you select Remote Access Configuration from the NIASCFG menu. The remote access software basic configuration process automatically loads AIO hardware drivers, selects modem types, and modifies the NETINFO.CFG file.

The automated setup prompts you to do the following:

- ◆ Identify the communications adapters installed in your server
- ◆ Identify the modem types connected to your server
- ◆ Select the remote access services to load

Before you start configuring the remote access software, make sure you have

- ◆ Installed the communications adapters
- ◆ Installed Novell Internet Access Server 4.1
- ◆ Connected modems to the ports on the adapter and *turned them on*

When you have completed the basic configuration, the remote access software assigns the basic profile to authorized users to

- ◆ Access all remote access ports
- ◆ Access all active remote access services
- ◆ Set ports for bidirectional use
- ◆ Log in for an indefinite amount of time
- ◆ Dial out to any number

- ◆ Access all AppleTalk* zones on the network

If you bypass or quit the automated setup, you can configure the remote access software manually. Refer to Remote Access Drivers and Ports.

Using the Automated Setup Program

The remote access software takes you through an automated setup program the first time you configure it. If you quit this automated setup procedure, any subsequent changes to the configuration must be made using the configuration utility, NIASCFG. Refer to the subsequent chapters in this book for detailed information about subsequent remote access configuration.

- 1** Enter **LOAD NIASCFG** at the server prompt.

A window is displayed prompting you to move all driver LOAD and BIND commands from the AUTOEXEC.NCF file to the NETINFO.CFG file.

- 2** Select Yes and press Enter to continue.

One or more messages might be displayed indicating that duplicate LOAD commands were not imported. Skip these messages until a message is displayed indicating that NIASCFG has completed copying all the LOAD and BIND commands to NETINFO.CFG.

- 3** Press Enter to continue.

The NIAS Options menu is displayed.

- 4** Select Configure NIAS from the NIAS Options menu and press Enter.

The Select Component to Configure menu is displayed.

- 5** Select Remote Access from the Select Component to Configure menu and press Enter.

The Remote Access Configuration NetWare Loadable Module™ (NLM™) file is loaded and the Connect Object Installation Requirement menu is displayed. This menu allows you to automatically extend the directory schema to install the Connect object (the remote access object name).

- 6** Specify the Connect Rights level and press Enter.

This is the container below which the Connect object is granted administrative rights. Users in this container, and below, can access this remote access server. The default value is [ROOT].

NOTE: If you do not choose [ROOT] during installation, you can use NetWare Administrator to allow other users access to the remote access object, or to explicitly grant the Connect object administrative rights to other containers. Refer to NetWare Rights for Remote Access.

7 Enter an Administrator name and password.

This user must have the required rights to extend the schema and install the Connect object.

At this point, you are asked if you want to review the instructions.

8 If you want to review the instructions, select Yes and press Enter.

The instructions contain an overview of the steps that are performed during the automated configuration process. To return to the automated configuration program, press Esc. Press F8 at any time during the setup procedure to display these instructions or press F1 to display the help screens for the window or field being displayed.

9 A message is displayed asking if your server contains any synchronous adapters, such as X.25 or ISDN. If it does, select Yes and press Enter. If your server contains only asynchronous adapters, select No and press Enter. Go to Step 15.

When you select Yes, the MultiProtocol Router Fast Setup menu is displayed; however, remote access does not support Fast Setup.

10 Select No and press Enter to continue.

An abbreviated version of the Internetworking Configuration menu is displayed.

11 From the Internetworking Configuration menu, select Boards and press Enter.

The Configured Boards window is displayed.

12 Perform the following steps to configure asynchronous adapters:

12a Press Ins and select the appropriate driver from the list displayed.

NOTE: SYNCPLUS is the Novell-provided X.25 driver that supports the Novell synchronous /V.35+, RS-422+, and RS-232+ adapters.

WHSMCAPI is the Novell-provided driver for ISDN adapters that support NetWare CAPI, such as the Eicon SCOM adapter.

Consult your hardware documentation for other drivers.

12b Enter the appropriate board parameters.

Save the board parameters.

- 12c** Press Esc to return to the Internetworking Configuration menu.

The Internetworking Configuration menu is displayed.

- 13** Select Network Interfaces and press Enter.

For each interface that you defined in Step 12a that you want to use for remote access, select the interface, select PPP Remote Access for the medium, and specify the ISDN address and ISDN subaddress, if applicable.

HINT: For examples on how to configure X.25/ISDN boards and network interfaces, refer to Configuring Ports for ISDN.

- 14** Press Esc to return to the Internetworking Configuration menu. Press Esc again to exit INETCFG.

A prompt is displayed informing you that the system must be reinitialized and offering you the option of terminating the automated setup, which means that you must repeat this procedure from the beginning.

- 15** Load the AIO drivers.

The configuration program prompts you to identify the communications adapters installed in your server. When you select the adapter, it automatically loads the appropriate driver with the factory default settings.

NOTE: You must select an AIO driver to continue with the installation. If you do not have an asynchronous adapter in your server, select Serial Port (COMx) to continue.

If there is an address conflict, you will be prompted for the load parameters, such as IRQ, I/O address, memory address, board name, and board number. For information about supported values, refer to your adapter documentation or the AIODISK.DOC provided with the remote access software.

- 16** Identify remote access ports.

NOTE: Make sure the modems are connected to the ports and are turned on.

The configuration program automatically identifies ports that have modems attached.

- 17** Select modem types.

The automated setup program can automatically detect some modem types attached to a port. If it is unable to detect the modem type, the program prompts you to identify the modem type on each port.

HINT: Select the modem type whose DTR signal is blinking. The highlighted port sets the DTR signal of the modem attached to it to blink.

Highlight the next port on the list and select the modem whose DTR signal is blinking. Repeat the process for all ports in the list.

When modem information has been defined for a previous installation, this information is retained and the modem discovery process is not required.

18 Select remote access services.

Select the services that you want loaded. Some services, such as Point-to-Point Protocol Remote Node Service (PPPRNS) and ARAS. See AppleTalk Remote Access Service (ARAS), require load-time configuration; others, such as NASIT[™] Connection Service (NCS), simply confirm if you want the service loaded immediately.

Select	To allow...
PPPRNS	DOS, Windows, and UNIX* clients to dial in and become remote IP or IPX (Internetwork Packet Exchange) nodes on the LAN. Refer to Loading PPPRNS.
NCS	LAN workstations to dial out to remote host computers or bulletin boards. NCS also allows remote PCs to dial in using third-party remote control applications and access a dedicated host PC or application server on the LAN. Refer to Loading NCS.
ARAS	Macintosh* clients to dial in and become remote AppleTalk nodes on the LAN. Refer to Loading ARAS.

After you have successfully completed the automated setup procedure, remote access is ready for remote clients to dial in or LAN workstations to dial out. If you want to stop the remote access software from running, enter **NWCSTOP** at the NetWare console prompt. To start the remote access software again, enter **NWCSTART**.

After setting up a basic configuration with the automated setup program, do the following:

1. Verify your configuration. Refer to *Verifying the Automated Configuration*.
2. Distribute the client software to your remote users
3. Install and configure the client software for the remote users.
4. Test your configuration by trying to establish a connection.

Loading PPRNS

Loading Point-to-Point Protocol Remote Node Services (PPRNS) allows users to dial in to the LAN from remote IPX or IP nodes.

To support IPX connections, your server must have IPX protocol packet forwarding enabled. This is the default setting; however, if you receive a message stating that IPX packet forwarding is disabled, enable it by loading INETCFG, then selecting Protocols > IPX > Packet forwarding and enable it.

To support TCP/IP connections, you must configure the server as an IP router. If your LAN has remote IP nodes, make sure your server is configured as an IP router.

Specifying Load Parameters for PPRNS

To specify load parameters for PPRNS, complete the following steps:

- 1** Select the protocol.

PPRNS supports IPX and TCP/IP protocols. Select IP if the remote users require access to an IP application. The default protocol is IPX.

- 2** Enter a network address.

Enter any valid, unique network address. Specify the network address based on the protocol selected in Step 1.

Protocol	Network Address
IPX	An IPX network address is a unique hexadecimal number one to eight digits long. All remote node users connected to this server are placed on the virtual LAN segment associated with this IPX network address. This address must be unique, that is, no two servers can have the same IPX network address.

Protocol	Network Address
IP	This address is the local IP address for the WAN interface. An IP address is a 4-byte (32-bit) numeric value that identifies both a network and a local host or node on that network. The address is represented in dotted decimal notation. Each byte is represented by a decimal number and dots separate the bytes (for example, 130.57.45.240). Each byte can range from 0 through 255. Do not represent IP addresses in hexadecimal numbers.

IMPORTANT: The IP address must have its own IP address range. It must not be in the same address range as that specified for the LAN, for example, 128.37.172.xxx for the LAN and 128.37.173.xxx for PPPRNS.

3 For TCP/IP connections only, specify other IP parameters.

3a Specify a subnet mask.

The mask is a 4-byte numeric value represented in dotted decimal notation. Each byte ranges from 0 through 255 and dots separate the bytes, for example, 255.255.255.0.

3b (Optional) To specify a client address range, select Yes and press Enter.

Additional fields are displayed for entering the starting and ending client addresses for the range. Enter the starting and ending IP addresses of the range for remote IP clients. The client address range must be on the same network or subnet as the server address specified in the Local Address field.

You can also enter a secondary client address range using this procedure.

4 Press Esc and respond Yes when prompted to save your changes.

Loading NCS

NASI Connection Service (NCS) does not require any configuration parameters at load time; therefore, remote access simply confirms whether you want the service loaded.

Loading ARAS

AppleTalk Remote Access Service (ARAS) enables Macintosh* users to dial in to the LAN from remote locations using a modem. Further configuration is required to provide other capabilities, including the following:

- ♦ To use a NetWare 5 server as a router to an existing Macintosh environment, you must load AppleTalk on to the server and configure it to be an AppleTalk router.
- ♦ To enable remote Macintosh clients to log in to the remote access server, you must load AppleTalk and NetWare for Macintosh AppleTalk Filing Protocol (AFP*).
- ♦ To enable users to log in to the Novell Directory Services™ (NDS™) software, you also must configure the MacIPX® gateway.

Loading ARAS consists of the following tasks:

1. Loading AppleTalk

Load AppleTalk to configure your server as an AppleTalk router. If your server is already configured to route AppleTalk packets, refer to Step 2: Specifying Load Parameters for ARAS.

2. Specifying parameters to load ARAS

Step 1: Loading AppleTalk

AppleTalk is loaded on the remote access server to route AppleTalk packets between the AppleTalk network and the remote Macintosh computers. This does not enable remote Macintosh computers to log in to the remote access server. If you want the users to be able to log in to the remote access server, you must load AppleTalk Filing Protocol (AFP), which is part of NetWare for Macintosh.

Use the Routing and Protocols option of NIASCFG to load AppleTalk and configure your server as an AppleTalk router. When you configure the server as an AppleTalk router using NIASCFG, the appropriate LOAD and BIND commands are added to the INITSYS.NCF and NETINFO.CFG files in the SYS:ETC subdirectory.

Novell Directory Services Considerations

If your remote users are logging in to the Novell Directory Services (NDS) software, you must load the MacIPX gateway on the remote access server and

the remote client must load the MacIPX control panel on the workstation. If your NetWare server has bindery emulation turned on, then the server can accept non-NDS logins.

Use NIASCFG to load the MacIPX gateway on the server.

Step 2: Specifying Load Parameters for ARAS

To specify the LOAD parameters for ARAS, complete the following steps:

1 Select a frame type.

ARAS supports the following frame types:

- ◆ Ethernet_SNAP
- ◆ Ethernet_II

The default is Ethernet_SNAP.

If you have already loaded AppleTalk, select a frame type that is identical to that loaded with the LAN driver for the AppleTalk LAN. Refer to your AUTOEXEC.NCF file for more information. Typically, Ethernet_SNAP is selected for EtherTalk* 2.0 networks, and Ethernet_II is selected for EtherTalk 1.0 networks.

IMPORTANT: ARAS allows only a single frame type (Ethernet_SNAP or Ethernet_II) to be loaded at one time.

2 Enter network numbers and AppleTalk zone names.

Configure the following parameters for binding the ARAS driver to AppleTalk:

2a Enter the starting range of the network number.

The starting range of the network number must be an integer between 1 and 65,279.

2b Enter the ending range of the network number.

The ending range of the network number must be an integer between 1 and 65,279.

NOTE: The difference between the two integers must be between 0 and 10. The network range, however, must be unique on the LAN. Each group of ports on the server running ARAS is considered to be a network.

2c Enter AppleTalk zone names.

A valid zone name is a string of up to 32 characters that can include hyphens (-), underscores (_), and spaces (.). You can specify one or

more zone names separated by commas, for example, *Novell Engr* , *Novell Mktg*. If any Macintosh on the LAN is a resource for the remote Macintosh calling in, specify the zone name to which the Macintosh on the LAN belongs. In a NetWare environment, you can enter **LOAD ATCON** at the NetWare console prompt to find existing AppleTalk zone names.

- 3** Press **Esc** and respond **Yes** when prompted to save your changes.

You are asked if you want to restart the service at this time.

- 4** Select **Yes** and press **Enter** to restart ARAS.

Restarting the service causes any users currently using the service to be disconnected.

Verifying the Automated Configuration

After you install and configure the remote access software, generate a configuration report to verify your port configuration and maintain server records. To verify the configuration, complete the following steps:

- 1** Select **Generate Configuration Report** in the **Remote Access Options** menu.
- 2** (Optional) Press **F2** to display a list of report options that you can select (or deselect) to customize the configuration report.

Press the **Up-arrow** or **Down-arrow** key to highlight an option, and press **Enter** to toggle the option on (**Yes**) or off (**No**).

You are prompted for the output device.

- 3** Select the device you want to send the report to and press **Enter**.

Select **Screen** if you want the output to be displayed on the screen, or select **Disk File** if you want to view the entire contents later. The report is saved in the **NWCRPT.TXT** file in the **SYS:** volume. This file is overwritten each time you select this option. You can change the default pathname to create a different file.

The configuration report appears.

- 4** Check the entries in the report.

Make sure your configuration is set up properly by verifying the following:

- ◆ Warning messages

The consistency check warnings are displayed at the beginning of the report. These warnings might display inconsistencies with port configurations and licenses.

- ◆ Directory context
- ◆ Container context

This context represents the username display.

- ◆ Services loaded

If you do not see the proper services loaded, refer to the instructions for loading the services.

5 Generate the report again if you made changes to the configuration.

Remote Access Drivers and Ports

You are required to configure the remote access drivers and ports if you did not use the automated setup program. You might also need to reconfigure the software when you add ports or change modems after the initial configuration.

Before you load drivers and configure the ports, you must do the following:

1. Install the communications adapters. Make sure your multiport adapters are installed and the modems are connected to the ports and turned on.
2. Configure the boards and drivers you will be using.

Refer to the following special procedures if you will be running PPP over asynchronous ports, PPTP, or dialing in to or out of a packet-switched X.25 network:

- ◆ Configuring Boards for Running PPP over Asynchronous Ports
- ◆ Configuring Boards for Point-to-Point Tunneling Protocol (PPTP)
- ◆ Installing and Configuring X.25 Adapters

To configure drivers, refer to *Loading the AIO Drivers* or *Loading the X.25 Driver and AIOPAD.NLM*.

To configure ports, refer to *Configuring Ports* or *Configuring AIOPAD and X.25 Ports*.

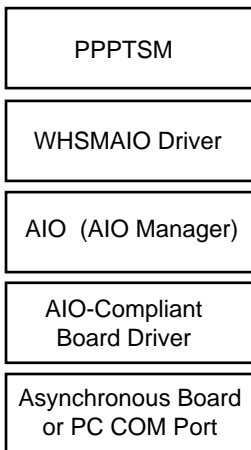
Novell certifies third-party communications adapters with their AIO drivers for use with remote access. For a current list of certified adapters, contact the Novell Labs™ FAX Back System. For U.S. customers, the number is 1-800-

414-LABS; for customers outside the United States, the number is 801-429-2776, extension 2. Or you can access the Novell Labs World Wide Web site for current information at <http://labs.novell.com>. The Novell Labs certification bulletins also list certified communications adapters. For your convenience, the AIO drivers for some of the certified third-party communications adapters, as well as Novell's AIOCOMX.NLM (COM port driver), are supplied with remote access.

Configuring Boards for Running PPP over Asynchronous Ports

To run PPP over asynchronous ports, such as your PC's COM ports, you must use a board driver that is compliant with the AIO standard. An AIO-compliant driver can communicate with the AIO Manager (AIO.NLM), which then communicates with the WHSMAIO driver. The WHSMAIO driver converts the AIO character stream into the asynchronous HDLC framing service required by the NetWare Link/PPP™ software. WHSMAIO also converts PPP asynchronous HDLC frames into an AIO character stream. Finally, the WHSMAIO driver provides a WHSM interface with the PPP Data-Link layer (PPPTSM.NLM). The relationship of these modules is shown in Figure 8.

Figure 8 Modules Required to Run PPP over Asynchronous Ports



Because the structure shown in Figure 8 contains two separate drivers, two boards must be configured, one for the AIO-compliant driver and one for the WHSMAIO driver. This section does not explain how to configure a board for

the AIO-compliant driver because this board is configured just like any other physical WAN board. However, the WHSMAIO board is not a physical board. Instead, it is a software entity that is used to represent one or more AIO ports as one or more WHSM interfaces. The WHSMAIO driver can also be applied to many different physical AIO boards using different AIO-compliant drivers. With NIASCFG, you can configure several ports that have the same parameter settings using just one screen. However, each port's configuration is shown as a separate board under Network Interfaces.

The Novell Internet Access Server 4.1 routing software includes an AIO-compliant driver, AIOCOMX, that runs over your PC's COM ports.

Refer to the Novell Labs WWW location http://labs.novell.com/infosys/mastr_06.htm for more information about the following topics:

- ◆ Selecting WAN hardware based on performance
- ◆ Determining whether to run PPP over an asynchronous or synchronous port
- ◆ Understanding the advantages and disadvantages of running PPP over your PC's COM ports
- ◆ Getting the most current Novell-certified boards and drivers

Sharing AIO Ports with the NetWare Routing Software

The NetWare routing and remote access components can coexist on a single server and can share serial interfaces provided by AIO drivers. However, the following information should be taken into consideration.

The AIO ports for the routing software are configured under the Protocols and Routing option in NIASCFG, whereas the AIO ports for the remote access software are configured under the Remote Access option. Typically, AIO ports used by the WHSMAIO driver do not require configuration by the remote access software. However, when both products are enabled, you can reserve all AIO ports for the exclusive use of the remote access product. This causes the WHSMAIO driver to fail with the following error message:

```
Fatal Error: Unable to initialize the AIO board.
```

To correct this problem, use NIASCFG to enable the WHSMAIO driver access to the specified AIO ports.

To configure an AIO port for use by the WHSMAIO driver, complete the following steps:

- 1 If Novell Internet Access Server 4.1 remote access software is running, stop the remote access software by entering the following command at the NetWare console prompt:

NWCSTOP

- 2 Load NIASCFG, then select the following parameter path:
Select Configure NIAS > Remote Access > Set Up ... > Select Remote Access Ports

- 3 Select any listed remote access ports that you want to be dedicated to WHSMAIO and press Del.

Repeat this step on each port to be dedicated to WHSMAIO.

- 4 Start the remote access software by entering the following command at the NetWare console prompt:

NWCSTART

- 5 From this point, use *only* the path NIAS Options > Protocols and Routing to configure Novell Internet Access Server 4.1 routing ports. Use *only* the path NIAS Options > Remote Access to configure remote access ports.

The following NIASCFG remote access options should not be used for AIO ports that use the WHSMAIO driver:

- ♦ Manage Ports
- ♦ Reset Port
- ♦ Unconditional Reset Port

If you use any of these options, the port becomes inoperative. If this occurs, unload the WHSMAIO driver and enter the REINITIALIZE SYSTEM command to restore normal operation.

How to Configure Boards for Running PPP over Asynchronous Ports

Before you begin, you must configure a physical WAN board.

To configure a WHSMAIO board, complete the following steps:

- 1 Load NIASCFG, then select the following parameter path:
Select Configure NIAS > Protocols and Routing > Boards

- 2 Do one of the following:

If you are configuring a new WHSMAIO board:

- ◆ Press **Ins** to display the list of available drivers.
- ◆ Select the **WHSMAIO** driver.
- ◆ Enter a name for the new board.

The **WHSMAIO** Configuration menu appears.

If you are changing an existing **WHSMAIO board configuration, select that board.**

3 Select AIO Board Options.

If you are configuring a new AIO board, the following message appears:

Should NIASCFG automatically load the AIO driver?

If you are configuring an existing board, a message is displayed that explains that you can change only the configuration of the board that was previously configured with NIASCFG. You cannot select another AIO board unless you delete the existing **WHSMAIO** board and add a new one. To reconfigure the existing board, press **Enter** and proceed to Step 5.

4 Select Yes or No.

NOTE: If possible, always select **Yes** to load the AIO driver using NIASCFG.

Select *No if your system has an AIO board that has already been configured for another product using **LOAD** commands in the **AUTOEXEC.NCF** file. A window containing information about all available AIO boards is displayed. Select the board you want to use.*

This window displays the following information for each AIO board: AIO board name, number of ports, port speed, manufacturer, and version. Select a board that is likely to have some ports available for use by PPP. This board does not necessarily have to be currently used by another product. If no drivers are displayed, you must load the board driver at the console or restart the router.

Select *Yes if you are using a board that is being configured for the first time through NIASCFG. A list of AIO drivers is displayed. Select a driver from the list. A menu with driver-specific parameters is displayed. Enter the appropriate values for these parameters.*

These parameters are vendor-specific and vary depending on which third-party AIO driver is being used. Parameters that are commonly displayed include **Interrupt**, **I/O Base**, and **Memory Base**. Refer to the documentation supplied with the third-party driver for more information about the displayed parameters.

Some AIO drivers have interface speed limits that prevent you from configuring the interface to a speed above the default limit. If a console error message indicates that the WHSMAIO port configured in Step 5 failed to load because the default speed limit has been exceeded, you might be able to increase the AIO driver speed limit. Refer to the documentation supplied with the third-party driver for more information about the parameter to configure to increase this speed limit.

5 Enter a value for the First AIO Port Number parameter.

Enter the number of the first port that is available for use by PPP. The reason is to distinguish the ports available for use by PPP from the other ports on this board that are being used by another product.

6 Enter a value for the Number of AIO Ports parameter.

This number is used in conjunction with the previous parameter to determine the total number of ports, starting with the first port, that are available for use by PPP.

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

8 If you want these changes to take effect immediately, you must first configure a PPP network interface for this board as described in Setting Up in the *NetWare Link/PPP* documentation.

After configuring a network interface, you can make the changes take effect by restarting the router or selecting Reinitialize System. If you want to configure other parameters, do so now, then restart the router or reinitialize the system when you are finished.

The AIOCOMX.NLM and AIO.NLM files are used by many Novell products. If you install another product that uses the COM ports on the server running Novell Internet Access Server 4.1 routing software, check the versions of these files before and after the installation of the new product. If problems occur with the WHSMAIO ports after the installation of a new product that uses the AIOCOMX.NLM and AIO.NLM files, try using the versions of these files that are supplied with Novell Internet Access Server 4.1.

Configuring Boards for Point-to-Point Tunneling Protocol (PPTP)

You can also use the Protocols and Routing option in NIASCFG to configure the Point-to-Point Tunneling Protocol (PPTP) on a remote access server. PPTP

allows Novell Internet Access Server 4.1 to accept PPP calls from remote users through any Internet service provider (ISP) by tunneling PPP packets through an IP tunnel.

NOTE: Your Internet Service Provider (ISP) must have a PPTP access concentrator, and your network must have access to a port on that concentrator. Talk to your ISP for details.

To configure a board for PPTP, complete the following steps:

1 Configure a WHSMAIO board as described in *How to Configure Boards for Running PPP over Asynchronous Ports* except select AIOPTTP for the driver in Step 4.

2 Select the Number of AIOPTTP Ports parameter and select a value.

This number is used in conjunction with the First AIO Port Number parameter to determine the total number of ports, starting with the first port, that are available for use by PPTP.

Valid values range from 4 to 256.

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

4 If you want these changes to take effect immediately, you must first configure a PPP network interface for this board as described in *Setting Up* in the *NetWare Link/PPP* documentation.

After configuring a network interface, you can make the changes take effect by restarting the router or selecting Reinitialize System. If you want to configure other parameters, do so now, then restart the router or reinitialize the system when you are finished.

Installing and Configuring X.25 Adapters

Step 1: Install an X.25 Adapter

Install a certified X.25 adapter in the remote access server.

A list of third-party X.25 adapters certified by the Novell Labs™ group can be found at the Novell WWW location <http://labs.novell.com>.

NOTE: The Novell labs document, *How to select WAN Hardware for your Novell product*, can help you to select the appropriate hardware for X.25, as well as for other WAN and dial-up adapters. This document can be found at the Novell WWW location <http://labs.novell.com/wan/certinfo.htm>.

You can install more than one X.25 adapter in the server; however, the number of adapters might be limited depending on the manufacturer and available interrupts.

For installation instructions, refer to your X.25 adapter documentation.

Step 2: Configure the X.25 Interface Board

Use the Novell Internet Access Server Configuration (NIASCFG) utility to configure the X.25 boards installed in the remote access server. After you have run NIASCFG to configure one or more X.25 drivers, the remote access software automatically loads the driver for the board when a session is initiated on an X.25 port.

NOTE: The name of the X.25 support driver provided with Novell Internet Access Server 4.1 is SYNCPLUS.LAN.

Each X.25 driver that works with remote access has a driver description file (sometimes called a load driver information file or .LDI file) that specifies the parameters for the driver load. When you run NIASCFG, you accept default settings in the .LDI file or modify them according to your requirements.

The parameters for the load command vary for different drivers. For example, some drivers require an I/O port address, memory address, and interrupt, whereas other drivers require other parameters to interface with the data-link layer.

To run NIASCFG and configure an X.25 interface board, complete the following steps:

- 1 At the server prompt, enter

LOAD NIASCFG

If this is the first time that you have run NIASCFG on the server, the following prompt appears.

Transfer LAN driver, protocol and remote access commands?

IMPORTANT: Make sure that you really want to do this before responding Yes to this prompt. If you respond Yes to the prompt, NIASCFG comments out any load and bind commands for LAN drivers in the server's AUTOEXEC.NCF file and transfers them to its own initialization file, the NETINFO.CFG file in the SYS:\ETC directory. You can view this file but cannot edit it. Subsequently, when you start the server, the NetWare® Link/X.25™ software automatically issues the `initialize system` command to initialize X.25 ports on the server.

- 2 If you want NIASCFG to modify your AUTOEXEC.NCF file, select Yes in response to the prompt; otherwise, select No.

The Internetworking Configuration menu appears.

3 From the Internetworking Configuration menu, select Boards.

The Configured Boards window appears.

If you are setting up a new configuration, no existing boards are shown. Otherwise, boards that have already been configured are shown.

Table 5 explains the fields shown on the Configured Boards window.

4 Press Ins.

5 Scroll through the list of available drivers that appears.

6 Do one of the following:

- ◆ If you find the driver for your board in the list, highlight the driver name and press Enter.
- ◆ If you do not find the driver for your board in the list, follow the procedure listed under Copying a Driver File to the Server.

The Board Configuration window appears.

7 Specify the X.25 interface board parameters.

7a If the parameters are listed as separate fields, highlight each field and accept the default value shown or select an appropriate value for the parameter.

All drivers require a board name. However, the additional fields on the Board Configuration window vary, depending on the driver.

Table 2-1 describes the most common driver configuration parameters. If your driver requires other parameters, highlight the field for that parameter and press F1 to display information about the field or refer to your driver documentation.

Table 5 Common Driver Configuration Parameters

Field	Description
Board Name	Enter a name for the board. You can use up to 10 alphanumeric characters for the board name.
Driver	Select the name of the driver associated with the board.

Field	Description
Int	The interrupt request level (IRQ) used by the board. Make sure that the setting you use matches the settings enabled by the board's jumpers or DIP switches. This setting should not conflict with the interrupts used by any other boards in the server.
IOAddr	The base input/output port address for the board. Make sure that the setting you use matches the settings enabled by the board's jumpers or DIP switches. This address should not conflict with the I/O addresses used by any other boards in the server.
MemAddr	The base memory address used by the board. This address range should not conflict with the I/O addresses used by any other boards in the server.
Slot	If the driver configuration for the board requests this information, enter the number of the slot where the board is installed.
Comment	A comment about the board or its configuration.

7b If the Board Configuration window for your board's driver provides only a *Board Parameters* field, type the required parameters in this field.

For example, if your adapter board requires a port I/O address, a memory address, and an interrupt number, type

PORT=258 MEM=D000 INT=3

8 Press **Esc** to exit the Board Configuration window.

9 Select **Yes** to save changes to the X.25 interface board configuration, then press **Enter**.

If the configuration you specified conflicts with the configuration for other boards, one or more messages appear describing the conflicting parameters. If you believe that the conflict might cause a problem with the system, change the configuration of one or more boards to resolve the conflict.

The Configured Boards window appears and lists the interface you just configured. The Status field is **Enabled**.

10 To configure any additional boards, repeat Step 3 through Step 8.

NOTE: If you have run **NIASCFG** previously and it modified the **AUTOEXEC.NCF** file to include load commands for LAN drivers, you will have to modify the

AUTOEXEC.NCF file manually if you want additional load driver commands to be in the file.

- 11** When you are finished, press `Esc` to return to the Internetworking Configuration menu.

Copying a Driver File to the Server

If you try to add a driver configuration from the Configured Boards window and do not find the correct driver for the board you are configuring, you must copy the driver description file for the board to the server before you can configure it.

To copy a driver file to the server, complete the following steps:

- 1** From the Configured Boards window, press `Ins`.

The Available Drivers window appears.

- 2** Press `Ins`.

The New Driver window appears.

- 3** Make sure that the system can find the driver file.

- ◆ If the driver is on a diskette, insert the diskette containing the driver into an available drive slot.
- ◆ If the driver is not on the server, make sure that you have copied it to the server.

- 4** Type the full pathname of the new driver and press `Enter`.

The new driver appears in the list of Available Drivers.

If NIASCFG cannot find the driver file you specify, the message `Driver file not found` appears.

- 5** To configure the driver, go to Step 1.

Step 3: Configure the Network Interface

To configure network interface parameters for NetWare Link/X.25, complete the following steps.

- 1** From the NIASCFG Internetworking Configuration menu, select Network Interfaces.

The Network Interfaces window appears.

- 2** Select an unconfigured port on an X.25 board.

A pop-up menu listing the available media appears.

3 Select X.25-Host.

The X.25 Network Interface window appears.

The first field in the Network Interface window is the *Interface Name* field. This field is a read-only field that displays the interface name assigned by NIASCFG. This name is a combination of the board name that was specified in the Board Configuration window plus the number of the port on the adapter.

4 Configure the remaining fields on the Network Interface window as indicated in Table 2-2.

Table 6 Network Interface Configuration Fields

Field	Explanation
Interface Group	Accept the default value (None).
Interface Status	Specifies whether the port is Enabled or Disabled. Accept the default value (Enabled) by pressing the Down-arrow key to skip to the next field. If you need to disable the field to test your board configuration, refer to "Network Interface Configuration Parameters".
Profile	Specifies a standard profile used by X.25 service providers. Press Enter to display a list of standard profiles and then select the standard profile for your X.25 service provider from the list. If you need to modify the profile, refer to "Viewing and Configuring Profile Parameters" for instructions.
DTE Address	Enter the address assigned by your local X.25 network service provider.
Statistics Period	Specifies the interval, in seconds, at which the interface board is polled by the driver to gather statistical data that is displayed on the monitor. Accept the default value (6 seconds).
User Data Size	Specifies the maximum user data size, in bytes, that the interface supports. Accept the default value (1500 bytes).
Interface Queue Limit	Specifies the maximum number of data packets that can be queued to this port. Accept the default value (100 packets). The range of values is 0 (unlimited) through 1024 packets.
Physical Type	Specifies the port's electrical interface standard (RS-232, RS-422, or V.35). This parameter must match the actual interface used with the port.

Field	Explanation
Port Connection	Specifies the physical connection between the local DTE and the remote end. Accept the default value (Hard-wired). If you need to change the default, refer to "Network Interface Configuration Parameters".
Interface Speed	Specifies the line speed, in bits per second, for this port. Accept the default value (External). If you need to change the interface speed, refer to "Viewing and Configuring Profile Parameters".
Authentication Options	Limits acceptance of incoming calls to those specified in a DTE address database. Press Enter to display the X.25 Authentication Options window. Then make sure that the Inbound Authentication field in this window reads Disabled.

5 Press Esc to return to the Network Interface window.

6 When prompted to save the configuration, select Yes.

7 Press Esc to return to the Internetworking Configuration menu.

Step 4: Configure the WAN Call Directory (Optional)

When you use remote access to communicate through an X.25 network, you must specify a DTE number. To avoid having to remember the DTE number, you can configure a WAN call destination configuration for each remote destination the server will communicate with. WAN call destination configurations contain parameters that NetWare Link/X.25 uses when establishing and maintaining calls to the destination.

To configure WAN call destinations for X.25 interfaces, complete the following steps.

1 From the NIASCFG Internetworking Configuration menu, select WAN Call Directory.

The Configured WAN Call Destinations window appears. This window has no entries if no WAN call destinations are configured.

2 Press Ins to configure a new WAN call destination.

The following prompt appears:

New Call Destination Name:

3 Enter a name for the new WAN call destination.

The WAN call destination name can be up to 47 alphanumeric characters in length.

A list of supported wide area media appears.

4 Select X.25 Host.

NOTE: If you have not installed an X.25 board and configured an interface before attempting to configure a WAN call destination, an error message appears.

The X.25 Call Destination Configuration window is displayed.

The first field in the X.25 Call Destination Configuration window is the *Call Destination Name* field. This field is a read-only field. It displays the name of the WAN call destination that you entered in Step 3.

5 Specify information for the remaining fields in the X.25 Call Destination window, as described in Table 2-3.

Table 7 X.25 Call Destination Window Fields

Field	Explanation
Call Type	Press the Down-arrow key to accept the default value (Permanent <active continuously >).
Interface Group	This field is not used with remote access X.25 support.
Interface Name	Press Enter to display a list of available X.25 interfaces (ports on installed X.25 adapters). Then select the interface that the call destination configuration will be used with.
Circuit Type	Press Down-arrow to accept the default value (Switched Virtual Circuit).
PVC Number	This field is not used with remote access X.25 support.
Destination DTE Address	Enter the DTE address for the remote call destination. The address can be up to 15 decimal digits long.
Retry Mode	Press Down-arrow to accept the default value (Retry Self-Correcting Failures). If you need to change the value, refer to "WAN Call Directory Configuration Parameters".
Retry Limit Handling	Press Down-arrow to accept the default value (Continuous at Limit). If you need to change the value, refer to "WAN Call Directory Configuration Parameters".
Retry Interval Time	Press Down-arrow to accept the default value (00:10:00). If you need to change the value, refer to "WAN Call Directory Configuration Parameters".

Field	Explanation
Idle Line Timeout field	This field is not used with remote access X.25 support.
Remote System ID	Press Down-arrow to accept the default value (<None>).
Expert Call Configuration	Normally, you do not need to specify an expert call configuration. If you need to specify one, refer to "Expert Call Configuration Parameters".

6 Press Esc.

7 When prompted to save your changes, select Yes.

The new WAN call destination appears in the list of configured WAN call destinations.

8 To configure another WAN call destination, repeat Step 3 through Step 7.

9 Press Esc to return to the Internetworking Configuration menu.

Loading the AIO Drivers

When you first install the Novell Internet Access Server 4.1 remote access software or when you add a serial adapter board, the automated setup procedure helps you configure your ports automatically. If you exited the automated setup without completing the port configuration, you must load the drivers manually.

To load the appropriate driver, complete the following steps:

1 Load NIASCFG, then select the following path:

Select Configure NIAS > Remote Access > Set Up... > Add a Serial Adapter Board

2 For each communications adapter you have installed, load its AIO driver once by selecting the appropriate serial adapter entry from the list.

3 If no AIO ports are defined or the board cannot be loaded, you see a warning message. Press Enter and step through configuring the board. Otherwise, skip to Step 5.

To configure a board, you must enter its name and other specific information. Follow the prompts on the screen.

4 Press Ins and select the WHSMCAPI driver for ISDN.

NOTE: Some ISDN boards, such as the US Robotics Allegra series for NetWare, use WAN ODI drivers instead of WHSMCAPI. Select the appropriate driver, or press Ins and use your manufacturer-supplied driver diskette. Specify your board parameters, then continue with Step 5.

- 5 Select Continue with Automated Setup after remote access has determined which ports have modems attached. Select Try Modem Discovery Again if modems were not discovered (not turned on).

Loading the X.25 Driver and AIOPAD.NLM

After you complete the X.25 driver configuration using the NIASCFG utility, load the X.25 driver and the AIOPAD NetWare Loadable Module™ (NLM™) file.

The X.25 driver communicates between the X.25 adapter and the server. AIOPAD.NLM is the AIO driver that provides X.25 support for remote access.

To load the X.25 driver and the AIOPAD NLM, complete the following steps:

- 1 At the NetWare console prompt, enter
`initialize system`
- 2 For each X.25 port in the server, load AIOPAD. To load AIOPAD, enter
`load aiopad x25board=interface name [prompt=string] [/
pass]`

interface name

This is the interface name that you specified for the X.25 driver in NIASCFG. See Interface Name in Step 3: Configure the Network Interface.

prompt

The optional **prompt** parameter allows you to specify a string that specifies a prompt that is displayed to NAS!™ users when they acquire a port using AIOPAD. The prompt can be up to 16 characters.

/pass

The optional pass parameter disables AIO PAD from performing X.3 processing in data transfer mode. It prevents the user from going into command mode and changing the X.3 PAD parameters. However, using the option enables PPPRNS to operate more efficiently.

AIO PAD initializes each port for which it is loaded. Note, however, that remote access can limit the number of active connections.

HINT: Once you have performed your initial configuration of remote access for X.25 support, you might want to modify the AUTOEXEC.NCF file. To edit the AUTOEXEC.NCF file, at the NetWare console prompt, load the NetWare INSTALL utility and select System Options. Then select Edit AUTOEXEC.NCF File

Configuring Ports

After the AIO drivers are loaded, you can configure ports for remote access. If you used the automated setup program, you do not need to configure ports unless you introduced new hardware after you first ran the automated setup program.

Refer to the following procedures:

- ◆ Configuring Ports for ISDN
- ◆ Configuring Ports for Remote Access
- ◆ Removing a Port from the List of Configured Ports
- ◆ Creating Port Groups

Configuring Ports for ISDN

If you did not configure one or more ISDN ports during the remote access automated installation and setup procedure, you can configure an ISDN port manually. An ISDN port must be configured before it can be used for remote access.

To configure a port for ISDN, complete the following steps:

- 1** Load NIASCFG, then select the following path:

Select Configure NIAS > Remote Access > Configure Synchronous Interfaces

An abbreviated version of the Internetworking Configuration (INETCFG) menu is displayed.

2 Select Boards.

The Configured Boards window is displayed.

3 Do the following to configure an ISDN board:

3a Press `Ins` and select the WHSMCAPI driver for ISDN.

3b Enter a name for the board.

The WHSMCAPI Board Configuration window is displayed.

3c Select CAPI Board Options and press `Enter`, then select `Yes` to have INETCFG automatically load the CAPI driver.

3d Select the appropriate CAPI driver from the list, based on the board you have.

3e Enter the number of MAXPORTS.

3f Press `Esc` to return to the WHSMCAPI Board Configuration window.

3g Select Driver-Specific Configuration to configure the ISDN driver. If you are prompted to enter a name for the ISDN board, be sure to use the same name that you used in Step 3b.

3h Press `Esc` again, save your changes, and return to the INETCFG menu.

4 Select Network Interfaces.

The Network Interfaces window is displayed.

5 Do the following to configure the ISDN interface:

5a Select the ISDN interface and press `Enter`.

5b Select PPP Remote Access.

5c Enter the local ISDN address and local ISDN subaddress, if applicable.

5d Toggle the ISDN interface status by pressing `Tab` to change the status from RMT Access to Enabled.

5e Press `Esc` and save the changes.

6 Press `Esc` to exit the INETCFG menu and return to the Remote Access Options menu.

7 Continue with Configuring Ports for Remote Access.

NOTE: The ISDN board and interface configuration does not take effect until you reinitialize the system.

Configuring Ports for Remote Access

You use the NIASCFCG utility to configure the remote access ports. When the utility starts, function keys are enabled. The keys that are enabled for a particular remote access window are displayed at the bottom of the utility window. Table 8 summarizes the key functions.

Table 8 Remote Access Function Key Definitions

Function Key	Operation
F1	Open context-sensitive help
F2	Customize a configuration report; save port statistics to file; write an audit report to file
F3	Rename; modify the field
F4	Copy from
F5	Mark/unmark (select multiple items from a list)
F6	Copy to
F7	Clear all marks
F8	Display instructions; identify the port
F10	Activate the AIOPAD configuration; run a service-specific NLM
Alt+F1	Display additional key help
Alt+F5	Mark all
Alt+F7	Abort the configuration report

To configure ports for remote access, complete the following steps:

- 1 Load NIASCFCG, then select the following path:
Select Configure NIAS > Remote Access

The Remote Access Options window is displayed. If you are loading NIASCFG for the first time, the program prompts you with instructions to configure remote access.

2 Select Configure Ports.

A window listing port information by port name is displayed. The window lists the ports that the AIO NLM recognizes. Default port names are assigned, depending on the existing configuration.

The Status column displays the status of the port: Available, Unavailable (the driver is not loaded), or Port_Acquired.

3 Select the port that you want to configure and press Enter.

4 Specify the following port parameters:

- ◆ Port Name—Enter a unique port name of up to 15 characters, or up to 14 characters if you will use the port for the NASI™ (NetWare Asynchronous Services Interface™) Connection Service (NCS). Only alphanumeric characters, underscores (_), hyphens (-), and periods (.) are allowed. Port names must be unique on a server and begin with a letter in the first character position. The port name can indicate the type of connection, the telephone number of the port, or other information for troubleshooting purposes. (In NASI applications, port names are called *specific names*. Refer to Support for Dial-Out Nodes and for more information.) Default port names are supplied based on the driver type.
- ◆ Port Description—(Optional) Enter a description for the port. For example, if you plan to use the port to manage remote access, you can describe it as System admin's private line.
- ◆ Modem Type—Select Modem Type and press Enter. A list of modem types is displayed. Select the type of modem that is attached to the port.

If your modem is not listed, select a similar modem. If no similar modems are listed, select Hayes* Compatible. Select Automatic Detection to have remote access determine the modem type for you. The default is None, which means that the line is a direct connection and does not use a modem.

For direct connections, select None. For X.25 ports, select AIOPAD. For ISDN adapters (not ISDN terminal adapters that connect to a serial port like a modem), select ISDN (AT Controlled). For PPTP ports, select AIOPPTP.

NOTE: For a list of supported modems and the current support file, download NWCMOD.EXE from the Novell World Wide Web site or from the Netwire NWGENFILES Forum (library 3) on CompuServe*. Note that the modem script files in NIASMOD.EXE are not backwards-compatible with NetWare Connect 2.0.

5 (Optional) Select Additional Parameters and press Enter.

The Port Configuration window displays additional port configuration parameters. Usually, you can keep the defaults for most of these parameters. For more information on configuring these parameters, refer to "Advanced Port Configuration".

6 When you have configured the port, press Esc and select Yes to save the changes.

7 Configure the rest of the ports in the port list panel by repeating Step 3 through Step 6.

You can use the following keys to configure a similar port or port groups:

- ◆ F4 —Copies the port configuration from another port.
- ◆ F6 —Copies the port configuration to another port or port group.

8 Review your port assignments.

9 Press Esc to return to the Remote Access Options window.

After you have configured the remote access ports, you will need to do one or more of the following additional tasks:

- ◆ Create port groups. Refer to Creating Port Groups.
- ◆ Configure remote node support. Refer to Support for Remote Nodes.
- ◆ Configure dial-out and remote control dial-in connections. Refer to Support for Dial-Out Nodes.

Removing a Port from the List of Configured Ports

To delete a port from a list of configured ports, complete the following steps:

1 Select Configure Ports from the Remote Access Options window.

2 Select a port from the list of ports and press Del.

To delete multiple configured ports, press F5 to select multiple ports, then press Del.

3 Press Esc to exit.

- 4 To remove the configuration from the deleted port, unload the AIO driver, then reload it.

Creating Port Groups

You can give a group name to a set of ports. Group names help pool resources and manage ports on the remote access server. Group names are useful when they describe the type of service that the port provides.

Typically, network users require access to a resource but are not interested in knowing the resource's location or phone number. If you name a port for the resource to which it is assigned, users can request that resource quickly and intuitively. For example, you can assign the group name MODEMS96 to a group of remote access ports that establish a connection at 9,600 bps. For access to a host line, you can assign a name that describes the host. For example, assign the group name HP_ACCT to an HP* minicomputer that belongs to the accounting department. Users can then access the device by requesting it with the group name HP_ACCT.

The default port group is ANY_PORT. This group contains all remote access ports and is created so that all NCS, PPPRNS, and ARAS users can access a port on the server in a basic configuration environment.

To create a new port group, complete the following steps:

- 1 Select Configure Port Groups from the Remote Access Options window.

The Group Names window is displayed with the default group name ANY_PORT.

- 2 Press **Ins** to create a new group.

- 3 Enter a new group name of up to 15 characters.

NOTE: Do not create a group name of DIALIN. This name is already used by NCS. Refer to General Name for Shared DIALIN Ports.

The name must be unique for the remote access server. Use only alphanumeric characters, underscores (**_**), hyphens (**-**), and periods (**.**). The first character must be a letter.

NOTE: The group name in remote access is the same as the General Name used by NASI applications. Group names used for NCS must be limited to eight characters.

- 4 Select the new group name from the Group Names list and press **Enter**.

A list of group members for the port is displayed. Initially, this list is blank.

5 Press **Ins**.

A list of other remote access ports is displayed.

6 Press **F5** or **Enter** to select the ports that you want to be members of the group.

Press **Alt+F5** to select all ports in the list. The ports you selected are highlighted.

7 Press **Enter** to save the group assignments.

8 Press **Esc** twice to exit the Configure Port Groups window.

Configuring AIOPAD and X.25 Ports

After the X.25 driver and AIOPAD are loaded, you can configure AIOPAD and the X.25 ports installed in the remote access server.

Configuring AIOPAD allows you to configure AIOPAD profiles. AIOPAD profiles are defined to set X.3 PAD parameters according to the specification of the X.25 public data network (PDN). The profiles enable users to connect to different host computers with different profiles.

Configuring AIOPAD

After you have configured the X.25 ports on the server using NIASCFG, you might want to configure AIOPAD to include site-specific profiles.

Configuring AIOPAD involves copying one of the provided profiles, saving it under another name, and then modifying the profile as required by your installation.

The remote access software provides four predefined X.3 profiles that are used when AIOPAD is communicating with X.25 hosts. You can edit these profiles directly or copy them under another name and then edit them. Note, however, that we do not recommend editing the profiles. The following predefined profiles are provided:

- ◆ **DEFAULT**. When the remote access software initializes X.25 ports on the server, it automatically uses the **DEFAULT** profile.
- ◆ **DIALIN**. When the remote access Service Selector initializes an X.25 port for a dial-in call from PPRNS or RNS, it automatically uses the **DIALIN** profile.
- ◆ **SIMPLE**. This profile contains a set of basic X.3 settings that can be used to communicate with an X.25 host.

- ♦ **TRANSPARENT.** Some X.25 installations require that data be transferred in transparent mode. If your installation requires this capability, you can use the **TRANSPARENT** profile.

To use the **SIMPLE** profile, the **TRANSPARENT** profile, or a custom profile that you have created, at the **AIOPAD** prompt issue the **PROF** command, followed by a blank space, followed by the profile name. For a description of the **PROF** command, refer to *AIOPAD Commands in the AIOPAD Commands, Service Signals, and PAD Parameters Reference.*

If necessary, complete the following steps to configure **AIOPAD**:

- 1** At the NetWare console prompt, enter

```
LOAD NIASCFG
```

- 2** From the **NIAS** options menu, select **Configure NIAS**.

The **Select Components to Configure** menu appears.

- 3** Select **Remote Access**.

- 4** From the **Remote Access Options** menu, select **Set Up**.

The **System Setup Options** menu appears.

- 5** Select **Configure AIOPAD Parameters**.

A list of predefined **AIOPAD** profiles appears.

- 6** Press **Ins** to create a new profile.

A **Profiles Details** form appears.

- 7** Specify a unique profile name and a profile number.

HINT: Use the context-sensitive help text if you need an explanation of either of these parameters. Highlight the parameter and press **F1** to display the help text. Press **Esc** to exit the help window.

- 8** Set the **PAD** parameters as required.

The remaining options in the **Profiles Details** form consist of **X.3 PAD** parameters. For an explanation of these parameters, refer to *PAD Parameters in the AIOPAD Commands, Service Signals, and PAD Parameters Reference.*

To set a parameter, move the cursor to the field and enter the new parameter information.

- 9** If you need to set the AIOPAD Extended Parameters, move the cursor to the <Extended Parameters> field at the bottom of the window and press Enter.

The Extended Parameters window appears.

- 10** Set the Extended Parameters as required.

- 11** Press Esc.

If you changed any parameters, the system prompts you to save your changes.

- 12** If you changed any parameters, select Yes.

- 13** Press F10 to activate the configuration.

This instructs AIOPAD to read the configuration file and update its internal table of profile information.

Configuring Remote Access Ports for X.25 Support

This section outlines the procedure for configuring remote access ports for X.25 support.

To configure remote access for X.25 support, complete the following steps:

- 1** Define port usage for the X.25 ports.

- ◆ Define any X.25 ports that NASI users will use to dial out from the LAN as Dial-Out Only or Both Dial-In and Dial-Out.
- ◆ Define any X.25 ports that remote users will access using the Windows dialer and PPRNS as Dial-In Only or Both Dial-In and Dial-Out.

- 2** Configure the X.25 ports.

Select AIOPAD for the Modem Type for any remote access X.25 port.

Configure the other parameters as required for your installation.

- 3** Restrict port usage to NCS, PPRNS, or both.

- ◆ For ports that you want to be dial-out only, restrict port usage to NCS.
- ◆ For ports that you want to be dial-in only, restrict port usage to PPRNS.
- ◆ For ports that you want to use as both dial-in and dial-out ports, restrict port usage to NCS and PPRNS.

Support for Remote Nodes

The remote access server software supports remote IPX, remote IP, and remote AppleTalk nodes.

To configure support for remote IPX nodes, refer to Remote IPX Nodes.

To configure support for remote IP nodes, refer to Remote IP Nodes.

To configure support for remote AppleTalk nodes, refer to Remote AppleTalk Nodes.

To set up your server to support remote Windows-based IPX clients, you must do the following:

- ◆ Load Point-to-Point Protocol Remote Node Service (PPPRNS).
- ◆ Configure PPPRNS for Internetwork Packet Exchange™ (IPX™) support.

To configure your server to support remote IP users, you must do the following:

- ◆ Configure the server as a TCP/IP router.
- ◆ Load PPPRNS.
- ◆ Configure PPPRNS for IP support.

To configure your remote access server to support remote AppleTalk nodes, you must perform the following tasks:

- ◆ Load AppleTalk and configure the server as an AppleTalk router.
- ◆ Load ARAS.
- ◆ Set Remote Client passwords.
- ◆ Configure ARAS (optional).

You might have already performed some of these tasks if you set up the remote access server for basic operation, as described in Using the Automated Setup Program.

Remote IPX Nodes

Loading PPPRNS allows remote Windows clients to dial in and become IPX nodes on the network. The software automatically adds a command to execute the NWCSTART.NCF file in AUTOEXEC.NCF.

To load PPPRNS, complete the following steps:

- 1** Load NIASCFG, then select the following path:

Select Configure NIAS > Remote Access > Set Up... > Select Remote Access Services > PPPRNS > IPX

- 2** Enter a valid, unique network address in the Net Address field.

This is the network address used by the remote workstations dialing in. An IPX network address is a hexadecimal number, one to eight digits long, for example, CF104009. This address must be unique, that is, no two servers can have the same IPX network address. Refer to <http://support.novell.com> for information on obtaining addresses.

Remote access uses this network address to create a virtual network (LAN segment) containing remote IPX nodes. A virtual network is created to decrease network traffic. This restricts the amount of broadcast messages to the remote clients.

IMPORTANT: Modifications to an existing network address take effect the next time you load IPXRTR.NLM or enter the `REINITIALIZE SYSTEM` command.

- 3** Press Enter then Esc and save your changes.
- 4** Press Esc and select Yes to save the current settings to a file.
- 5** Press Enter to activate the current configuration.
- 6** Select Yes to restart the service now.

The service is selected, but is not necessarily running. When a service is selected, it is added to the NWCSTART.NCF file. To verify that the service is running, you can view the statistics for that service. Refer to Viewing Service Statistics for more information.

After you have completed the procedure to support remote IPX nodes, you can do the following:

- ◆ **Configure IPX parameters.** Refer to Configuring PPPRNS.
- ◆ **Configure client software.** The Windows client software for PPPRNS is available on a separate client CD-ROM. Install and configure the client software on the remote PC and try to establish a connection. For more

information, refer to the Novell Internet Access Server 4.1 remote access online help.

- ♦ **Configure remote access security.** If you want to specify dialback, maximum connection time, or the idle timer, or if you want to restrict PPPRNS to specific ports or users, refer to "Service-Specific Remote Access Security".
- ♦ **Specify Remote Client passwords.** Refer to Setting Remote Client Passwords. Distribute the passwords to the respective users.

Remote IP Nodes

Loading PPPRNS with IP support allows IP clients to dial in and become remote nodes on the network. This procedure adds the appropriate LOAD and BIND commands to the NETINFO.CFG file.

Table 9 describes the IP parameters that you configure for PPPRNS with IP support.

Table 9 PPPRNS IP Parameters

Parameter	Description
Local IP Address	<p>Specifies the local IP address for the WAN interface on the remote access server. This is a 4-byte (32-bit) numeric value that identifies both a network and a local host or node on that network. The address is represented in dotted decimal notation. Each byte is represented by a decimal number, with periods separating the bytes, for example, 130.57.45.240. Each byte can range from 0 through 255. Do not use hexadecimal numbers.</p> <p>The local IP address must be on the same subnet as the client address range. The remote access software creates a virtual LAN segment (network) for all IP clients accessing this server.</p> <p>The IP address on the remote node can be configured statically or dynamically:</p> <p>Statically—The user explicitly specifies the IP address in the client software.</p> <p>Dynamically—The remote access software assigns IP addresses through IPCP. Specify a client range.</p> <p>Dynamically—The remote access server is a BOOTP server and assigns IP addresses. Configure the remote access server as a BOOTP server.</p>

Parameter	Description
Subnet Mask	A 4-byte numeric value in dotted decimal notation. Each byte ranges from 0 through 255, with periods separating the bytes.
Use Header Compression	<p>Specifies whether to use header compression over the WAN link with the remote client. The default is No.</p> <p>If you specify Yes, the remote access IP service will use TCP header compression with all remote access clients connecting to this address. Make sure that the settings for header compression on the server and the client agree: both are enabled or both are disabled. If the client is not configured to use header compression but the server is, TCP will not run between the remote access server and the client.</p>
Specify Client Address Range	<p>Specifies whether the remote access software assigns IP addresses to the remote nodes. Once you have specified the range and a client requests an address, remote access chooses an address that is not in use by another client from the address range and assigns it to the requesting client.</p> <p>Address assignments can be made through either IPCP (Internet Protocol Control Protocol) or BOOTP if the remote access server is configured as a BOOTP server. If the remote access server is not configured as a BOOTP server and a client address range is specified, IPCP address assignment is used.</p>
Client Address Range Start	Specifies the starting address for the remote IP client address range. The client address range must be on the same network or subnet as the server address specified in the Local IP Address parameter.
Client Address Range End	Specifies the ending address for the remote IP client address range.
Specify Secondary Client Address Range	Note: You configure a user to use the primary or secondary client address range with the NetWare Administrator utility. The secondary client address range feature might or might not be available on your system; it is an optional part of the standard Novell Internet Access Server 4.1 software.
Secondary Local IP Address	Specifies an additional (secondary) local IP address on the remote access server.
Secondary Subnet Mask	Specifies an additional (secondary) subnet mask on the remote access server.
Secondary Address Range Start	Specifies the starting address for the secondary remote IP client address range. This is a separate group of addresses that you can specify to limit or restrict access to network locations.

Parameter	Description
Secondary Address Range End	Specifies the ending address for the secondary remote IP client address range. This is a separate group of addresses that you can specify to limit or restrict access to network locations.

To load PPRNS with IP support, complete the following steps:

- 1** Load NIASCFG, then select the following path:
Select Configure NIAS > Remote Access > Set Up... > Select Remote Access Services > PPRNS > IP
- 2** Select Local IP Address and enter a valid, unique local IP address.
NOTE: The local IP address must be on the same subnet as the client address range.
- 3** Select Subnet Mask and enter a 4-byte value in dotted decimal notation.
- 4** Select Use Header Compression, then specify Yes to use TCP header compression. Otherwise, specify No.
NOTE: Make sure the settings for header compression on the server and the client agree, that is, both are enabled or disabled.
- 5** Select Specify Client Address Range and do the following:
NOTE: The Client Address Range parameters must be set when the remote access server is configured as a BOOTP server.
 - 5a** Specify Yes if you want the remote access server to assign IP addresses to the remote nodes. Otherwise, specify No and continue with Step 6.
 - 5b** Specify the Client Address Range Start and Client Address Range End parameters.
NOTE: The address range is for address assignment only, and is not for authenticating the remote IP address. If the client already has an address configured locally and does not need address assignment from the remote access server, the remote access software will not check the client address against the address range to make sure it is within the range.
- 6** (Optional) Select Specify Secondary Client Address Range and do the following:
 - 6a** Specify Yes if you want the remote access server to assign secondary IP addresses to the remote nodes. Otherwise, specify No and continue with Step 7.

6b Specify the Secondary Subnet Mask, Secondary Address Range Start, and Secondary Address Range End parameters.

NOTE: The secondary address parameters might not be available on your system. If these parameters are available, you can use them to limit access to certain network locations.

7 Press Esc and specify Yes to save your changes.

The service is selected, but is not necessarily running. When a service is selected, it is added to the NWCSTART.NCF file. To verify that the service is running, you can view service statistics, as described in Viewing Service Statistics.

The changes take effect the next time you start the PPPRNS service.

Once you have completed the procedure to support remote IP nodes, you can do the following:

- ◆ **Configure IP parameters.** Refer to Configuring PPPRNS.
- ◆ **Configure client software.** The Windows client software for PPPRNS is available on a separate client CD-ROM. Install and configure the client software on the remote PC and try to establish an IP connection. For more information, refer to the Novell Internet Access Server 4.1 remote access online help.
- ◆ **Specify remote access security.** If you want to specify dialback, maximum connection time, or the idle timer, refer to Setting Global Security. If you want to restrict PPPRNS to specific ports or users, refer to Authorizing Ports for Specific Services and Authorizing Users for Specific Services.
- ◆ **Specify Remote Client passwords.** Refer to Setting Remote Client Passwords. Distribute the passwords to the respective users.

Remote AppleTalk Nodes

When you configure the server as an AppleTalk router using NIASCFG, the appropriate LOAD and BIND commands are added to the INITSYS.NCF and NETINFO.CFG files in the SYS:ETC subdirectory.

Loading AppleTalk Remote Access Service (ARAS) allows Macintosh users to dial in to the LAN from remote AppleTalk nodes. This procedure adds the appropriate LOAD and BIND commands to the NWCSTART.NCF file.

To load ARAS, complete the following steps:

1 Load NIASCFG, then select the following path:

Select Configure NIAS > Remote Access > Set Up... > Select Remote Access Services > ARAS

2 Select a frame type from the list.

- ◆ Ethernet_SNAP—Select for EtherTalk* 2.0 networks (the default).
- ◆ Ethernet_II—Select for EtherTalk 1.0 networks.

Select a frame type that is identical to that loaded with the network driver for the AppleTalk network. Refer to your AUTOEXEC.NCF file for more information.

IMPORTANT: ARAS allows only a single frame type (Ethernet_SNAP or Ethernet_II) to be loaded at a time.

3 Select Starting Range of Net Number and enter a starting number between 1 and 65279.

4 Select Ending Range of Net Number and enter an ending number between 1 and 65279.

NOTE: The difference between the starting and ending range integers must be between 1 and 10. Ensure that the network range is unique on the network. Each group of ports on the server running ARAS is considered to be a network.

5 Select Zone List and enter one or more AppleTalk zone names.

A valid zone name is a string of up to 32 characters, including hyphens (-), underscores (_), and spaces. You can specify one or more zone names separated by commas, for example, Novell Engr, Novell Mktg. If any Macintosh computer on the network is a resource for the remote Macintosh calling in, then specify the zone name to which the Macintosh on the network belongs. These names must match names that have already been created.

IMPORTANT: We recommend that you specify the same zone to which your server belongs. The server belongs to the first zone that you specified when loading AppleTalk.

6 Press Esc and specify Yes to save your changes.

The service is selected, but is not necessarily running. When a service is selected, it is added to the NWCSTART.NCF file. To verify that the service is running, you can view service statistics, as described in Viewing Service Statistics.

Once you have completed the procedure to support remote Macintosh nodes, you can do the following:

- ◆ **Configure ARAS.** (Optional) Refer to Configuring ARAS.
- ◆ **Configure client software.** The client software, Apple Remote Access Client 2.0, must be purchased from Apple resellers. Install and configure the client software on the remote Macintosh computers and try to establish a connection. For more information, refer to the Novell Internet Access Server 4.1 remote access online help.
- ◆ **Specify remote access security.** If you want to specify dialback or maximum connection time, refer to Setting Global Security. If you want to restrict ARAS to specific ports or users, refer to Authorizing Users for Specific Services and Authorizing Ports for Specific Services.
- ◆ **Specify Remote Client passwords.** Refer to Setting Remote Client Passwords. Distribute the passwords to the respective users.

Further configuration is required to provide the following capabilities:

- ◆ To use remote access as a router to an existing Macintosh environment, load AppleTalk on the server and configure it as an AppleTalk router. This does not enable remote Macintosh computers to log in to the remote access server. For information on configuring the AppleTalk module, refer to Setting Up in the *AppleTalk* documentation.
- ◆ To enable remote Macintosh clients to log in to the remote access server, load AppleTalk and NetWare for Macintosh AppleTalk Filing Protocol.
- ◆ To enable users to log in to the Novell Directory Services™ (NDS™) software, configure the MacIPX® gateway on the remote access server. The remote client must load the MacIPX control panel on the workstation. If your remote access server has bindery emulation turned on, the server can accept non-NDS logins.

For more information about using the Protocols and Routing option of NIASCFG to configure an AppleTalk router for use with remote access and to load the MacIPX gateway, refer to Setting Up in the *AppleTalk* documentation and Configuring the MacIPX Gateway in the *IPX* documentation.

Support for Dial-Out Nodes

The remote access software supports network workstations (PCs and Macintosh computers) dialing out to access host computers or electronic bulletin boards.

On your remote access server, you enable PCs or Macintosh computers to dial out of the network by:

- ◆ Loading NASITM (NetWare® Asynchronous Services Interface™) Connection Service (NCS). Refer to Loading NCS.
- ◆ Distributing the Client Software
- ◆ (Optional) Configuring for a Modem-Independent Port Group
- ◆ (Optional) Setting Up Security
- ◆ Configuring Clients Dialing Out from a workstation

Loading NCS

You might have already loaded NCS when you first installed the remote access software. You can perform the following procedure to verify that NCS is running.

To install NCS, complete the following steps:

- 1** Load NIASCFG, then select the following path:

Select Configure NIAS > Remote Access

The Remote Access Options window is displayed.

- 2** Select Set Up.

The System Setup Options window is displayed.

- 3** Choose Select Remote Access Services.

A list of services is displayed.

- 4** Select NCS.

The LOAD NCS command is inserted into the NWCSTART.NCF file. The Yes and No prompts indicate that the service is selected, but they do not necessarily mean that it is running. To verify that the service is running, view service statistics, as described in Viewing Service Statistics.

Distributing the Client Software

The client software is installed on the remote access server during installation and is provided on CD-ROM. The following table shows the subdirectories to which the client software is copied.

Client Software	Server Subdirectories
For Windows clients (Windows 3.1x , Windows 95, and Windows NT)	SYS:SYSTEM\WIN2NCS
For Macintosh clients	SYS:SYSTEM\MAC2NCS

NOTE: NASI DOS clients are not shipped with Novell Internet Access Server 4.1; however, earlier versions of DOS clients are still supported. You can download the earlier NASI files from the Novell World Wide Web site: <http://www.novell.com>.

You can distribute the client software by copying the contents of the previously listed directories onto diskettes, or by providing access to users by copying the files to the SYS:PUBLIC directory.

The Macintosh client software is provided as a DOS-formatted, compressed version of the remote access MAC Client folder (named NetWare Connect™ MAC Client). This folder contains the Set Remote Access Password utility and the Installer for Mac2NCS. It is installed on F:\SYSTEM\MAC2NCS. To uncompress the software, use DOS to open the directory and enter **NWCMAC** . When the processing is complete, the NWCMAC.SIT file appears.

Now you can distribute the software in the following ways:

- ◆ Make the directory that contains NWCMAC.SIT accessible to all Macintosh users, allowing them to unstuff the file and extract Mac2NCS and Set Remote Access Password.
- ◆ Locate a Macintosh that has a Chooser mapping to the same directory. Use this machine to invoke NWCMAC.SIT to create the remote access MAC Client at an accessible hard drive (SYS:PUBLIC directory).
- ◆ Make a copy of the NetWare Connect MAC Client folder on diskette. Do not change the name of the folder; the folder name must be NetWare Connect MAC Client.

DOS Clients

NASI for DOS clients is not shipped with the Novell Internet Access Server 4.1 release; however, earlier versions of NASI are still supported. You can download earlier versions of NASI, including documentation, from the Novell World Wide Web site.

Windows Clients

Win2NCS is a redirector program that redirects the modem or printer port I/O for Windows communications applications to a NASI port on a remote access server. It runs on Windows 3.1, Windows for Workgroups 3.11, Windows 95, and Windows NT (3.51 and 4.0).

Distribute Win2NCS to the network workstations. From Windows, run the SETUP program to install Win2NCS.

In addition to Win2NCS provided with remote access, the dial-out nodes require a third-party communications program that uses the Windows Communications API. Almost all Windows communications applications support the Windows Communications API. Refer to <http://www.novell.com> for a list of supported third-party applications.

Macintosh Clients

Mac2NCS is a redirector program that redirects the COM port I/O for Macintosh communications applications to a NASI port on a remote access server.

In addition to the client software (NASI redirector for Macintosh computers, Mac2NCS) provided with remote access, the dial-out nodes require a third-party communications program that makes use of the Macintosh serial ports for communication. Refer to the MAC2NCS Readme file for a list of tested third-party applications.

Configuring for a Modem-Independent Port Group

Defining a modem-independent port group allows remote access to control modem initialization, instead of allowing the NASI application running on the network workstation to control it. This modem-independence feature is implemented by emulating the basic AT commands from a small set of industry-standard modem commands.

A modem-independent port group simplifies making dissimilar modems operate the same way. It also enables third-party applications to specify Hayes Compatible and ignore the exact modem type.

For information about creating a modem-independent port group, refer to *Specifying the NCS Configuration*.

Setting Up Security

The default NASI security for the network workstation is enabled. This means that if the NASI user is logged in to the network, NASI will prompt for a NetWare password only. With Macintosh users, however, the program prompts for a password only the first time, when users set up Mac2NCS.

If NASI security is disabled, NASI users will *not* be prompted for a password. To change the default, refer to *Configuring NCS*.

NOTE: If you disable NASI security on a single remote access server, you must disable security on all remote access servers on the network. This is necessary because the NASI client determines the security mode to use by requesting this information from the nearest NCS server, which might or might not be its target NCS server.

Configuring Clients Dialing Out

A user can dial out of the network from one of the following workstations:

- ◆ Windows 3.1x, Windows 95, and Windows NT 3.51 and 4.0 clients using Win2NCS
- ◆ Macintosh clients using Mac2NCS

NOTE: NASI DOS clients are not shipped with Novell Internet Access Server 4.1; however, earlier versions of DOS clients are still supported. You can download the earlier NASI files from the Novell World Wide Web site at <http://www.novell.com>.

Windows Clients

Before you start this procedure, make sure that you have installed the NASI redirector for Windows and that the local COM ports are enabled. For more information, refer to the WIN2NCS online help.

To set up a dial-out connection from the Windows clients, complete the following steps:

- 1** Attach to the network and start Windows.
- 2** (Optional) Click the Win2NCS redirector icon if you want to map a specific COM port.
- 3** Start any Windows communications program.

The Windows program must support the Windows Communications API.

- 4** From your communications program, use the appropriate COM port.
- 5** Specify a username, password, and session name for Win2NCS.

The username and password do not have to be the same as the login name and password you specified in Step 1.

NOTE: The session name is used for remote control dial-in connections.

A list of NASI services available on the network is displayed.

6 Select a NASI service from the list.

When you are dialing out to a host computer or a bulletin board, select any port except the port with the specific name *NCSname* DIALIN or the general name DIALIN. When setting up for a dial-in session, select the *NCSname* DIALIN session to facilitate port sharing.

If your application fails to connect, use the Terminal program that comes with Windows to verify the configuration of the application.

Macintosh Clients

Refer to the Novell Internet Access Server 4.1 remote access online help for a complete description of how to configure Mac2NCS. To set up a dial-out connection from the Macintosh client workstation, complete the following steps:

1 Run the Mac2NCS redirector.

1a From the Apple menu, select Chooser.

1b Click the Mac2NCS icon in the upper left window.

1c Click ON for redirection.

The port defaults to the modem. This is not required if the third-party Macintosh communications application is Communication Toolbox-Enabled. Refer to the Novell Internet Access Server 4.1 remote access online help for more information.

2 Click Setup.

A dialog box displays the currently selected port.

3 Select the servers you want.

4 Specify the User ID, Password, and Directory Context.

5 Click Server Options.

This button is labeled Continue the first time you use the application, and is labeled Options thereafter.

- 6 Select the server you want, the general name, and the specific name for the new default.

When you are dialing out to a host computer or bulletin board, select any port except the port with the specific name *NCSname* DIALIN.

- 7 Click OK twice to return to the Chooser.

- 8 Start your Macintosh communications program and begin a session.

Most applications default the Macintosh port selection to the modem port. To use NASI, make sure the application's port selection matches the Mac2NCS port selection. For example, if the application chose the modem port, the Mac2NCS redirection must be for the modem port. If your application is Communication Toolbox-Enabled, do not redirect the modem or the printer port. The application allows you to select the Mac2NCS port.

Refer to your application documentation to dial out from your port and establish a connection with the host computer.

For more information about the tasks in this section, refer to the Novell Internet Access Server 4.1 remote access online help.

Support for Remote Control Dial-in Connections

Remote control dial-in connections consist of one of the following:

- ◆ PCs dialing in and remotely controlling dedicated workstations or application servers on the network
- ◆ Macintosh computers dialing in and connecting to Macintosh computers or PCs on the network

To set up remote control connections, you must have third-party remote control applications that support NASI or the Windows communication driver. Third-party remote control applications supporting NASI or Win2NCS use NCS to establish a dial-in connection. The remote control application includes a host and a remote component. The remote component is installed on the calling PC, and the host component is installed on the network workstation or the application server. NCS manages the connection between the host and the remote components of the third-party application.

Configuring the Host

To set up a remote control connection, complete the following steps on the network workstation:

- 1** Distribute the client software. Refer to *Distributing the Client Software*.
- 2** Configure the client network workstation. Refer to *Configuring Clients Dialing Out*.

For Win2NCS, make sure you specify a unique name. If you want all callers to access this session, you can make the session public by selecting the Public Session check box in the Win2NCS program. If the session is private, the caller must specify the same username and password that were specified on the host when Win2NCS was started.

- 3** If the host session on the network selects a DIALIN port, enter a username and session name. If NCS dial-in security is enabled, also enter the Remote Client password.

If the host session on the network selected a dedicated port, the caller is automatically connected to the host session. For more information, refer to the Novell Internet Access Server 4.1 remote access online help.

- 4** Make sure your third-party application supports remote control connections.
- 5** From the server console, specify Remote Client passwords for callers dialing in.

Refer to *Setting Remote Client Passwords*. If you do not want the caller to specify a password, turn off NCS dial-in security. Refer to *Specifying the NCS Configuration* to disable NCS dial-in security.

Configuring the Remote Workstation

To configure the remote workstation, complete the following steps on the remote workstation dialing in:

- 1** Start the remote component of the third-party application and dial in to remote access.
- 2** If the host session on the network selected a DIALIN port, enter a username and session name. If NCS dial-in security is enabled, also enter the Remote Client password.

If the host session on the network selected a dedicated port, the caller is automatically connected to the host session.

Support for Remote Control Dial-In Connections Through IPX

Third-party remote control applications that support the Internetwork Packet Exchange™ (IPX™) protocol can use PPRNS to establish a dial-in connection. The remote control application includes a host and a remote component. The remote component is installed on the calling PC, and the host component is installed on the network workstation or the application server. PPRNS manages the connection between the host and the remote components of the third-party application.

Configuring the Host

To set up a remote control connection, complete the following steps on the network workstation:

- 1** Log in to the network.
- 2** Bring up the host component of your application and establish an IPX connection.
- 3** Specify a name for your host IPX session.

Configuring the Remote Workstation

To configure the remote workstation, complete the following steps on the remote workstation dialing in:

- 1** Run the remote access dialer and establish a connection to remote access.
- 2** Start your third-party application from your local drive and select IPX.
- 3** Select your IPX host session from the displayed list.

Remote Access Services

Before you begin configuring the remote services, make sure you have installed and loaded PPRNS, ARAS, or NCS. For information about loading PPRNS or ARAS, refer to *Loading PPRNS* or *Loading ARAS*. For information about loading NCS, refer to *Loading NCS*.

You can verify that the services are installed by selecting *Generate Configuration Report* from the *Configuration Options* window.

Do one of the following to determine which services are running:

- ◆ Select Display Service Status from the Status window.
- ◆ Enter **MODULES** at the server console prompt. If the services are loaded, you will see PPRNS, NCS, or ARAS in the list of modules.

Refer to Configuring PPRNS for the following PPRNS configuration tasks:

- ◆ Specifying Internetwork Packet Exchange™ (IPX™) parameters (optional)
- ◆ Specifying IP parameters (optional)
- ◆ Specifying ISDN short-hold parameters
- ◆ Specifying PPP multilink
- ◆ Configuring PPRNS security

Refer to Configuring ARAS for the following ARAS configuration tasks:

- ◆ Forwarding packets to AppleTalk with Cyclic Redundancy Check (CRC) embedded
- ◆ Specifying Apple remote access client versions

ARAS supports both types of Apple Remote Access (ARA) clients: ARA 2.0 and ARA 1.0.

Refer to Configuring NCS for how to specify the following information:

- ◆ List of general names from the port groups
- ◆ Modified general name for shared DIALIN ports
- ◆ Modem-independent group (optional)
- ◆ Server alias
- ◆ NCS remote dial-in security
- ◆ NASI network security
- ◆ Command Interpreter (CI) prompt
- ◆ Break duration

Configuring PPRNS

Refer to the following procedures:

- ◆ Specifying Optional IPX Parameters

- ◆ Specifying Optional IP Parameters
- ◆ Specifying ISDN Short-Hold Parameters
- ◆ Specifying PPP Multilink

Specifying Optional IPX Parameters

You can assign the following parameters for a user or a container:

- ◆ **IPX address** —A unique hexadecimal number up to 12 hexadecimal digits.
- ◆ **IPX address mask** —The IPX address mask allows you to create a range of IPX addresses for the user or container based on the specified IPX address. This address is assigned to the user when the user dials in from a remote workstation. If you provide a range of addresses for a container, then all users in the container inherit the range. Users might require more than one IPX address if they want to dial in more than once to establish multiple sessions.

When you define the mask, make sure that the 1 bit is contiguous. You cannot have leading zeros or zeros in the middle of the mask. For example, the masks FFFFFFFC00FF00 and FFFFFFFF4 are invalid. In the second mask, 4 in binary is 0100 (zeros in the middle of the mask). Substituting 0, 8, C, E, or F for 4 would provide valid masks because in binary the corresponding values are 0000, 1000, 1100, 1110, and 1111, respectively. Other valid masks are FFFFFFFF80, FFFFFFFFC00, and so on.

If you set the IPX address to 123ABC456780 and you want 16 IPX addresses, change the mask to FFFFFFFF0. This means that the selected user or all users in the selected container are assigned IPX addresses ranging from 123ABC456780 to 123ABC45678F.

If you modify the IPX address to 123ABC456784 for the same mask (FFFFFFF0), the IPX addresses would still range from 123ABC456780 to 123ABC45678F.

- ◆ **List of home servers** —When a remote node dials in, it attaches to a NetWare server and retrieves network information from that server. This parameter enables the remote node to attach to a server in the client's local site, thereby providing the remote node with the same view of the network through both local and remote access.

NOTE: Servers on the home server list must be reachable from all remote access servers into which the user will be dialing. If, for some reason, the home server is not running IPXRTR.NLM or is not reachable by a remote access server, the dial-

in user will not be able to establish an IPX connection. IPXRTR.NLM is a part of NetWare 4.1 or later, and the NetWare MultiProtocol Router™ 3.0 and 3.x software. Home servers running NetWare 4.1x or later must have bindery emulation. For NetWare 3.12 servers that are not using NetWare MultiProtocol Router, install the latest version of the NetWare 3.12 IPXRTR software that is available on the NetWare® service on CompuServe and the Novell support World Wide Web site at <http://support.novell.com>.

To configure PPPRNS, complete the following steps:

- 1** Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

- 2** Select PPPRNS.

The PPPRNS Configuration Options window is displayed.

- 3** Select Set IPX Parameters.

A list of users and containers in the default Directory context is displayed.

Select the single period (.) to set IPX information for the current container. If users are distributed over multiple contexts, select the double period (..) to move up the Directory tree to a common branch. Select names with a plus (+) prefix to move down the tree.

If the CONNECT object does not have Browse rights to move up the Directory tree, press **Ins** and enter a new Directory context. This enables you to jump to another branch of the tree where the CONNECT object does have rights.

- 4** Select a user or container.

The IPX parameters window is displayed. You can set the parameters if the CONNECT object, in addition to having Browse and Read attribute rights, has Write attribute rights to that container.

- 5** Select Specify IPX Address and specify Yes.

The User IPX Parameters window is displayed.

- 6** Specify the following IPX parameters:

- ◆ IPX Address—Enter an IPX address for the user or container. The IPX address must be a unique hexadecimal number, for example, 123ABC456780.
- ◆ IPX Address Mask—Enter a mask for the previous IPX address to provide a range of IPX addresses for the user or container. The default, FFFFFFFF, specifies a single IPX address to be used.

NOTE: If the highest-order byte of the IPX address is an odd number, it indicates a multicast address. Windows 95* clients (running the Novell Client™ for Windows 95) might not be able to connect using such an address. For example, an IPX address mask of FFFFFFFF0 and address of A112233445566 will cause the connection to fail. However, the address CCBBDDDEEFFAA can be used.

NOTE: You can assign a *fixed* IPX address for a user or a container by entering a *unique* address in the IPX address field and not providing a range (keeping the default for the IPX address mask).

7 Create a list of home servers by doing the following:

7a Select See List and press Enter.

Initially, the list is empty for the selected user or container.

7b Press Ins.

A list of server names on the network is displayed.

7c Select one or more home servers for the user or container.

If you select more than one home server, the user attaches to any one of the servers in the list.

7d Press Ins and enter the server address if the server name is not displayed in the list.

If the server is down, the server name is displayed as an IPX address.

8 Press Esc to exit.

The changes take effect immediately and apply the next time the user dials in.

Specifying Optional IP Parameters

You can set up your remote access server to function as a BOOTP server for remote clients. Use this option to assign IP addresses to remote access clients from the remote access server address range through BOOTP. You can also use this option when the clients want to obtain client information such as the domain name server from the remote access server. When your remote access server is configured as a BOOTP server, specify the following parameters per user or container:

- ◆ Domain Name Server Address
- ◆ Domain Name
- ◆ Boot Filename (used for diskless clients)

NOTE: DHCPD must be loaded for these parameters to apply.

To install the BOOTP server, complete the following steps:

- 1** Enter the following command at the console prompt on the remote access server:

LOAD DHCPD

- 2** When setting up the remote access server as a BOOTP server, make sure you set the following parameters.

- ◆ Set the Client Address Range parameter to Yes.
- ◆ Enter the IP addresses for the Client Address Range Start and Client Address Range End parameters. If necessary, enter IP addresses for the Secondary Local IP Address, Secondary Address Range Start, and Secondary Address Range End parameters.

- 3** If your clients want to receive domain information from the BOOTP server, specify the Domain Name Server Address and Domain Name parameters when you specify IP parameters.

NOTE: The DHCPD NetWare Loadable Module™ (NLM™) file can be used only for remote node clients. It cannot be used for LAN clients. You must set up a separate DHCP server for LAN clients.

To configure IP addresses for PPRNS, complete the following steps:

- 1** Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

- 2** Select PPRNS.

The PPRNS Configuration Options window is displayed.

- 3** Select Set IP Parameters.

A list of users and containers in the default Directory context is displayed.

Select the single period (.) to set IP information for the current container. If users are distributed over multiple contexts, select the double period (..) to move up the Directory tree to a common branch. Select names with a plus (+) prefix to move down the tree.

If the CONNECT object does not have Browse rights to move up the Directory tree, press **Ins** and enter the new Directory context. This enables you to jump to another branch of the tree where the CONNECT object does have rights.

4 Select a user or container.

The User IP Parameters window is displayed. You can set the remote access parameters if the CONNECT object, in addition to having Browse and Read attribute rights, has Write attribute rights to that container.

5 Select Set Domain Information and specify Yes.

The domain information can be specified when the remote access server is set up as the BOOTP server for remote clients and the clients want to receive this information.

NOTE: The following parameters are available to clients only if the remote access server is a BOOTP server and the clients request the information using BOOTP. If the remote access server is not set up as a BOOTP server (refer to Support for Remote Nodes) or the clients do not use BOOTP to request information, these parameters are not used.

6 Specify the following domain parameters:

- ◆ Domain Name Server Address—Enter the address of the domain name server to resolve hostnames for client requests.
- ◆ Domain Name—Enter the suffix to append to local hostnames. For example, if the domain name is novell.com, the client appends this name to ca (the local hostname) to provide the complete name of ca.novell.com.

NOTE: You can specify the Domain Name Server Address without specifying the Domain Name if the client uses complete hostnames. Specifying the Domain Name without the server address is not useful.

7 Select Set Boot Parameters and specify Yes.

The Boot parameters enable a diskless client machine to transfer a boot file to the client's memory and execute the boot file to start the client.

8 Specify the following boot parameters:

- ◆ TFTP Server Address—Specify the IP address of the TFTP server for this user or container.
- ◆ Boot File Name—Specify the name or pathname of the boot file that the client uses to start the remote workstation.

You are not required to set these parameters if the client does not need this information. For example, the client usually does not require a boot filename. Few client workstations must transfer a boot file from a remote site in order to start workstation operation (boot up). Most PCs have their boot files in local memory.

NOTE: When the BOOTP service is used, the client dialer application must be configured to use BOOTP for address assignment. Refer to the Novell Internet Access Server 4.1 remote access online help for information about setting up the client application network parameters.

- 9 Press Esc twice to save your changes.

The changes take effect when you have saved them.

Specifying ISDN Short-Hold Parameters

Specifying short-hold parameters for a PPP ISDN connection enables a remote node client to disconnect the line temporarily when no traffic is on the line and to reconnect when required. This minimizes telephone charges by reducing the actual connection time. Note that when the line is temporarily disconnected, the line is dropped but the session remains. The line is reconnected when either side has data to send.

If you have configured the short-hold parameters, the remote node client can determine whether to activate the feature when establishing the link.

NOTE: Although ISDN short-hold is most useful for connections for which call setup time is relatively short, it can be used for any PPP connection, including telephone dial-up lines.

To specify ISDN short-hold parameters, complete the following steps:

- 1 Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

- 2 Select PPRNS.

The PPRNS Configuration Options window is displayed.

- 3 Select Configure ISDN Short-Hold Parameters.

The ISDN Short-Hold Configuration window is displayed.

- 4 Select Idle Time Before Temporary Disconnect and enter a value.

This specifies the amount of time, in hours, minutes, and seconds, of link inactivity before the link is temporarily disconnected. The default is 5 minutes. The range is 1 second through 23 hours, 59 minutes, and 59 seconds.

- 5 Select Maximum Call Suspension Time and enter a value.

This specifies the maximum amount of time, in hours and minutes, that the connection can be left suspended before it is permanently disconnected. The actual amount of time the call is left in a suspended

state is negotiated with the remote client when the connection is established. The two sides negotiate for the smallest value proposed by each. The default is 30 minutes. The range is 1 minute through 23 hours and 59 minutes.

NOTE: If the remote client is configured and has negotiated short-hold with the server, both the Idle Time Before Temporary Disconnect and Maximum Call Suspension timers are used. The other timers associated with the connection, Maximum Connect Time and Idle Time Before Disconnect (each configured on a global or individual user basis), are ignored.

If the remote client does not negotiate short-hold with the server, both the Idle Time Before Temporary Disconnect and Maximum Call Suspension timers are ignored. The other timers associated with the connection, Maximum Connect Time and Idle Time Before Disconnect, are used.

Currently, only the Novell mobile client supports short-hold.

6 Press **Esc** to save your changes.

Specifying PPP Multilink

PPP multilink enables you to group multiple physical links into one logical link. With PPP multilink, you can group two physical ISDN channels or modems into one logical link to increase bandwidth. This feature allows you to use multiple channels between a remote access server and a client to increase the bandwidth for a logical connection.

NOTE: PPP multilink is automatically enabled for remote access. Additional links are initiated by the remote client. Check your hardware documentation to determine whether your ISDN device supports PPP multilink.

To specify PPP multilink, complete the following steps:

- 1** Select **Configure Services** from the **Remote Access Options** window.
The **Remote Access Services** window is displayed.
- 2** Select **PPPRNS**.
The **PPPRNS Configuration Options** window is displayed.
- 3** Select **Configure PPP Multilink**.
- 4** Press **Enter** to toggle between **Enabled** and **Disabled**.

Configuring ARAS

To configure ARAS, complete the following steps:

1 Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

2 Select ARAS.

The ARAS Configuration Options window is displayed.

3 Select Setup Options.

The Setup Options window is displayed.

4 Select Support Apple Remote Access Client Version.

4a Select one of the following options:

- ◆ 2.0 Only—Select this option if you have only ARA 2.0 clients. Continue with Step 4b.
- ◆ 1.0 and 2.0—Select this option if some clients dial in with ARA 1.0 and some dial in with ARA 2.0. Skip to Step 5.

IMPORTANT: When you select 1.0 and 2.0, the remote access software disables hardware compression on all ports that can be accessed by ARAS. We recommend that you either restrict ARAS to using specific ports (to minimize the number of ports with hardware compression disabled) or update your ARA 1.0 clients to ARA 2.0 clients. To restrict ARAS to using specific ports, refer to Authorizing Ports for Specific Services.

4b If you select ARA 2.0 Only, specify the following parameters:

- ◆ Prompt User for Remote Client Password—Select Yes if you want the user to enter the password manually. Select No if a stored password can be used by the client. The default is No.
- ◆ ARAS Greeting—Enter the text that is displayed when the remote user establishes a connection with remote access. The default is blank.

5 Select Forward Packet to AppleTalk with CRC Embedded, and specify Yes or No.

If this parameter is enabled (Yes), data packets from the remote node are forwarded with CRC embedded. If the AppleTalk network is sending frames with CRC embedded, then this option must be enabled for the remote nodes as well. The default is disabled (No). Refer to the following section for more information.

Verifying Data Integrity

To verify that the data packets on the AppleTalk network have CRC embedded, check the LOAD command for loading the AppleTalk protocol stack. If the AppleTalk protocol stack is loaded with the following command line parameter, then the AppleTalk network is sending frames with CRC embedded:

checksum=yes

An alternate way to verify that the data packets are sending frames with CRC enabled is by using INETCFG. Select Protocols and AppleTalk, then check the DDP Checksum field. It should be enabled.

The CHECKSUM parameter is used to detect data corruption in the AppleTalk packets. When this parameter is enabled, AppleTalk calculates the CHECKSUM value for the outbound packet, stores the value in the packet, then sends the packet out. When the packet is received at the destination, AppleTalk verifies the value to find out if the packet is good or bad. If the packet is bad, AppleTalk discards it. CHECKSUM helps to ensure data integrity; however, extra CPU time is required to compute the value.

If the network media has a high rate of data corruption, we recommend that you enable CHECKSUM; otherwise, leave it disabled for better performance. To enable CHECKSUM, select the DDP Checksum option in the AppleTalk section of the Protocols and Routing option of NIASCFG.

Configuring NCS

Refer to the descriptions of the following parameters:

- ◆ General Names
- ◆ General Name for Shared DIALIN Ports
- ◆ Modem-Independent Groups
- ◆ Server Alias Names
- ◆ NCS Remote Dial-in Security
- ◆ NASI Network Security
- ◆ CI Prompt
- ◆ Break Duration

General Names

A general name is a port group name that NCS recognizes. Most third-party NASI applications are written to the NASI specification that supports general names defined with eight or less characters. Remote access, however, supports group names that have up to 15 characters. To enable the third-party NASI applications to recognize the group names, you must create a list of general names that have no more than eight characters. Refer to *Support for Dial-Out Nodes* for more information about NASI.

General Name for Shared DIALIN Ports

Use of the shared DIALIN port enables multiple remote control hosts to share ports and prevents a single user from holding up a line.

Remote access automatically creates the general name DIALIN, which includes all ports defined for dial-in usage. The specific name of the ports in the DIALIN group has the form *NCSname* DIALIN, where *NCSname* is the first eight letters of the remote access server name or the alias server name.

NOTE: If your access or alias server name is less than eight characters, underscores are used for the remaining characters. For example, FS1_ _ _ _ _DIALIN. The first eight characters of the server name are used by default. Refer to the section *Server Alias Names* for information on alias server names longer than eight characters.

When remote control hosts select the specific virtual port *NCSname* DIALIN, dial-in users using NASI, Win2NCS, or Mac2NCS share all available dial-in ports. If remote control hosts acquire a non-DIALIN port, the workstation owns the port and cannot share the port with other users. The port is free for other users only when the network workstation disconnects the port. Refer to *Support for Dial-Out Nodes* for more information about NASI.

Modem-Independent Groups

A modem-independent group enables you to group modems from different vendors under a single group. The modem-independent feature is implemented by emulating the AT Commands set from a small set of industry-standard modems. All modem commands for the ports that belong to a modem-independent group are handled the same way.

The general advantage to using the modem-independent group is that the user does not have to know the modem type being used so that NASI applications can specify Hayes Compatible. Another advantage is that you can set dial-out restrictions only for a modem-independent group. In addition, the numbers

that users of modem-independent groups dial out to appear in the audit trail. However, a disadvantage is the limited support of the Hayes command set.

HINT: Group similar modems together in a modem-independent group. For example, you can group all V.34 modems. However, do not group a 2,400-bps modem with 28.8-Kbps modems.

However, NASI, Win2NCS, or Mac2NCS applications on a network workstation can modify the port settings (data rate, parity, data bits, stop bits, and flow control) of the ports in a modem-independent group. The remote NASI application user must specify Hayes Compatible for modem type.

Notify the NASI, Win2NCS, or Mac2NCS user of the highest data rate supported by the modem-independent group. The highest data rate supported is the speed of the slowest modem in the group. A NASI, Win2NCS, or Mac2NCS application on a network workstation must not have its data rate configured higher than the speed of the slowest modem in the group.

When using the modem-independent group, a NASI, Win2NCS, or Mac2NCS applications user should specify Hayes Compatible for the modem type. The default port settings are configured based on the modem type you select in NIASCFG. Refer to "Port Configuration" for more information.

NOTE: Specifying Hayes Compatible in your NASI, Win2NCS, or Mac2NCS application does not mean that your connection is set for 2,400 bps. Typically, users might experience a short connection delay as remote access translates between the generic modem command and the actual modem commands.

The default port speed is set when remote access initializes the port. The port settings are configured on the remote access server using NIASCFG.

Server Alias Names

If a remote access server name has more than eight characters, NASI truncates it and displays the first eight characters. A problem arises if two or more remote access servers on the network have the same first eight characters. To overcome this limitation, NCS allows you to specify a unique alias server name of eight or less characters.

NCS Remote Dial-in Security

The NCS dial-in security applies to users dialing in through the Service Selector (using the shared DIALIN port) to access dedicated remote control host sessions on the network. The default requires users to specify the Remote Client password. If NCS dial-in security is disabled, users are prompted only for the username.

NASI Network Security

NASI security applies to network workstation connections to an NCS port. The default requires users to specify the NetWare password. If NASI network security is disabled, users are not prompted for a username or password. This applies only to workstations using the NASI DOS TSR. Win2NCS workstations must always specify the NetWare password.

CI Prompt

Whenever a user starts an application that supports the Command Interpreter (CI), NASI displays the CI prompt. Refer to the Novell Internet Access Server 4.1 remote access online help for more information on the commands that can be used at the CI prompt. The default prompt looks like this:

```
nas i 1:1>
```

The default CI prompt contains the following elements:

- ♦ `nas i` —The name of the software.
- ♦ `n :n` —The number of currently active NASI sessions, followed by the currently active logical circuit. For example, 1:1 indicates that there is one NASI session and the logical circuit number 1 is active; 3:3 indicates that there are three active sessions and the currently active session is on logical circuit 3. To modify the number of logical circuits, refer to the Novell Internet Access Server 4.1 remote access online help.

Some third-party applications provide a method for connecting to the communications ports. With other applications, the user must rely on the CI or write an application using the NASI Basic functions that accept CI commands.

The CI enables users to issue commands that control access to the NASI Application Programming Interfaces (APIs). For example, users can list the available resources on the network, connect to a particular communications port, and set parameters for communicating with that port. For more information, refer to the Novell Internet Access Server 4.1 remote access online help.

Break Duration

Break duration is the elapsed time that a break signal is sent to the remote host computer. Generally, break signals are used in time-sharing systems that require a signal to initiate login.

The default value is 0.55 seconds. Some systems require a specific amount of time for the break signal to expire. The default value ensures maximum compatibility between applications. Keep the default value or change the value, depending on the application. Refer to the documentation that came with the application.

Specifying the NCS Configuration

To start configuring for NCS, complete the following steps:

- 1** Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

- 2** Select NCS.

The NCS Configuration Options window is displayed.

- 3** Select General Name List and do the following to specify a general names list.

A list of general names is displayed. Initially, the default group name ANY_PORT is displayed. This group contains all remote access ports.

You can select, insert, or delete a general name. Deleting a general name deletes the name from the list but retains it in the port groups list.

IMPORTANT: Selecting a general name displays its group members, which you can add or delete. To add a group member, press `Ins`, and a list of other ports is displayed. To delete a group member, move the member to the other ports list.

- 3a** Press `Ins` to display additional port group names.

- 3b** Select a port group to add to the list of general names, or press `Ins` to create a new port group and add it to the port groups list.

- 3c** Press `Esc` to save your changes.

The group members in the general names list are the only ports that NCS recognizes (with the exception of the DIALIN group).

- 4** Select General Name for Shared Dial-In Ports, then press `Enter` and modify the name.

For example, you can modify the general name to INBOUND or REMCTRL (for remote control).

WARNING: Users should not select the DIALIN general name for dialing out to bulletin boards or host computers.

- 5** Select Modem-Independent Group, then do the following.

A list of known port groups is displayed. If this list is empty, you must create a general names list as described in Step 3a through Step 3c.

5a Select a group to be modem-independent.

5b Press Esc to save your changes.

IMPORTANT: Do not select a group with X.25 ports.

6 Select Alias Server Name, then enter a unique server name of eight characters or less.

7 Select Enable NCS Dial-In Security, then specify Yes to require remote users to enter the Remote Client password.

If this parameter is disabled (No), users will be prompted only for their usernames.

IMPORTANT: If security is enabled, you must specify Remote Client passwords for users who are dialing in. For information about specifying Remote Client passwords, refer to Setting Remote Client Passwords.

8 Select Enable NASI Security, then specify Yes to require LAN users to enter a NetWare password.

If this parameter is disabled (No), users will not be prompted for their usernames or passwords when they bring up NASI on their workstations. Disable this parameter if you do not want NASI workstations to be prompted for a password. This applies only to workstations using the NASI DOS TSR. Workstations using Win2NCS must specify a password.

IMPORTANT: If this field is disabled on a single remote access server, make sure you disable this option on *all* other remote access servers on the network.

9 Select Command Interpreter Prompt, then enter a new NASI prompt.

The new prompt does not take effect until the next time you start the NCS service.

10 Select Break Duration, then enter a new value.

The default is 0.55 seconds. Some systems require a specific amount of time for the break signal to expire. The default value ensures maximum compatibility between applications. Refer to the application documentation to determine the correct value.

11 Press Esc to save your changes.

Remote Access Security

Setting up basic remote access security consists of the following tasks:

- ◆ Authorizing Users for Specific Services
- ◆ Authorizing Ports for Specific Services
- ◆ Setting Global Security
- ◆ Setting Remote Client Passwords
- ◆ Configuring for Third-Party Security

For information on how to optimize user-specific and service-specific remote access security options, refer to the security-related topics under Optimizing.

Authorizing Users for Specific Services

To authorize users for specific services, complete the following steps:

- 1** Select **Configure Security** from the **Remote Access Options** window.

The **Configure Security** window is displayed.

- 2** Select **Restrict Service by User**.

A list of services is displayed.

- 3** Select a service.

A list of users authorized to use that service is displayed.

Initially, this list shows **(Any User)** to indicate that all users can access this service. If you have already authorized users for a specific service and you want to configure other services with an identical port configuration, use the following function keys:

- ◆ **F4** —Copies a configuration from another service.
- ◆ **F6** —Copies the selected port configuration to one or more services.

- 4** Press **Ins** to display additional users.

A list of additional NetWare users is displayed.

- 5** Select a user or press **F5** to select multiple users.

If users are distributed over multiple contexts, select the double period (..) to move up the Directory tree to a common branch. Select any other container object to move down the tree.

If the CONNECT object does not have Browse rights to move up the Directory tree, press **Ins** and enter the new Directory context. This allows you to jump to another branch of the tree where the CONNECT object does have rights.

- 6** Press **Enter** to add the users to the list of authorized users.
- 7** Press **Esc** to save the changes.
- 8** Repeat Step 2 through Step 7 to authorize user access to other services.

Authorizing Ports for Specific Services

To authorize ports for specific remote access services, complete the following steps:

- 1** Select **Configure Security** from the **Remote Access Options** window.
The **Configure Security** window is displayed.
- 2** Select **Restrict Service by Port**.
A list of installed services is displayed.
- 3** Select a service.
A list of ports authorized to use that service is displayed.
Initially, this list shows **(Any Port)** to indicate that all ports can access this service. If you have already authorized ports for a specific service and you want to configure other services with an identical port configuration, use the following function keys:
 - ◆ **F4** —Copies a configuration from another service.
 - ◆ **F6** —Copies the selected port configuration to one or more services.
- 4** Press **Ins** to display additional ports.
A list of additional remote access ports is displayed.
- 5** Select a port or press **F5** to select multiple ports.
- 6** Press **Enter** to add the ports to the list of authorized ports.
- 7** Press **Esc** to save the changes.
- 8** Repeat Step 2 through Step 7 to authorize port access for other services.

Setting Global Security

Use the procedure in this section to set or specify the following global security options:

- ◆ Default maximum connection time
- ◆ Idle time before disconnection (not applicable for ARAS connections)
- ◆ Default dialback mode
- ◆ Dialback mode parameters
- ◆ Dial-out restrictions

To set the global security parameters for remote access, complete the following steps:

- 1** Select **Configure Security** from the **Remote Access Options** window.

The **Configuration Options** window is displayed.

- 2** Select **Set Global Parameters** from the **Configure Security** window.

The **Global Parameters** window is displayed.

- 3** Select **Default Maximum Connection Time** and enter a value between -1 and 100,000 minutes.

Enter a value of -1 to allow all users to remain connected for an indefinite amount of time. You can set this parameter to 0 and customize the value for each user with the **Set User Parameters** window to prevent unauthorized users from accessing the network. Refer to "User-Specific Remote Access Security".

NOTE: If the remote client is configured and has negotiated short-hold with the server, both the **Idle Time Before Temporary Disconnect** and **Maximum Call Suspension** timers are used (refer to *Specifying ISDN Short-Hold Parameters*). The other timers associated with the connection, **Default Maximum Connection Time** and **Idle Time Before Disconnection** (each configured on a global or individual user basis), are ignored.

If the remote client does not negotiate short-hold with the server, both the **Idle Time Before Disconnection** and **Maximum Call Suspension** timers are ignored. The other timers associated with the connection, **Default Maximum Connect Time** and **Idle Time Before Disconnection**, are used.

- 4** Select **Idle Time Before Disconnection** and enter a value between -1 and 100,000 minutes.

The default value of -1 indicates that the idle timer is not set and connections can remain idle for any amount of time. The timer is reset

whenever data is sent or received through the port. This includes any broadcast or watchdog traffic that might be sent or received.

5 Select Default Dialback Mode and press Enter.

5a Select one of the following modes:

- ◆ No Dialback Allowed—Dialback is globally disabled for all users. You can configure specific users for dialback. Skip to Step 7.
- ◆ Allow User to Request Dialback to Any Number—The user can request remote access to dial back to any number specified at connection time. Continue with Step 5b.
- ◆ Forced dialbackForce Dialback to a Caller-Specified Number—Users are required to use the dialback feature. The dialback number is not preconfigured on remote access; the user specifies the dialback number at connection time. Continue with Step 5b.

5b Specify a port for dialing back.

To have remote access dial back on the same port that the caller used to dial in, select Use Dial-In Port for Dialback and specify Yes. Specify No to have remote access dial back on a different port. Dialing back on a different port is useful if, for example, users dial in on a 1-800 line, and you want to keep that line free for other users. If you specify No, you must specify a dialback port group.

To have remote access dial back to a port group, select Dialback Port Group, press Enter , and specify a port group. Select a dialback port group if you specified to have remote access dial back on a different port.

6 Specify the following dialback parameters:

- ◆ Dialback Wait Time—Specifies the amount of time, in seconds, that remote access waits before attempting to dial back. Enter a value between 0 and 3,600. The default is 30 seconds.
- ◆ Dialback Busy Retry Count—Specifies the number of times remote access retries a failed dialback operation. Enter a value between 0 and 100. The default is 3.
- ◆ Dialback Busy Retry Interval—Specifies the amount of time, in seconds, that remote access waits between redials. Enter a value between 0 and 3,600. The default is 30 seconds.

7 Select Dial-out Restrictions and press Enter.

A list of authorized dial-out numbers is displayed. Initially, the list shows the default, Any Number, indicating that users can dial out to any number.

8 Press **Ins** and enter a dial-out number.

If you only want certain users to dial out, enter an invalid phone number here, then enter valid numbers for individual users to enable them to dial out. Refer to "User-Specific Remote Access Security".

Press **Ins** again to enter another number. You can add or delete telephone numbers. Use the **F5** key to delete multiple entries. Deleting the last number on the list redisplay the Any Number option.

9 Press **Esc** to exit and save your global security settings.

Setting Remote Client Passwords

The Remote Client password is required to establish a connection, and the NetWare password is required for logging in to the NetWare network. Both passwords are specified for the same username.

You can set Remote Client passwords for the following types of callers:

- ◆ Remote user on a Macintosh computer
- ◆ Remote user on a PC using the PAP or CHAP method of authentication
- ◆ Remote user accessing a remote control host session on the network

You assign Remote Client passwords at first, then later allow callers to choose and change their own passwords. Remote access has Windows and Macintosh tools to enable users to change their passwords. Refer to the Novell Internet Access Server 4.1 remote access online help for more information about these tools. Refer to *Setting Remote Access User Parameters* for more information on using the NetWare Administrator utility to assign and change Remote Client passwords.

NOTE: After the connection is established, ARA 2.0 clients can use the ARA 2.0 client software to modify the passwords set by the administrator. ARA 1.0 clients, however, must run the Macintosh Set Remote Client Passwords utility to modify the administrator-specified password.

Enhance security for Remote Client passwords by requiring the following:

- ◆ Minimum password length
- ◆ Limited number of connection attempts
- ◆ Periodic password change

NOTE: The user has a grace login limit of three logins after a password has expired. During this grace period, the password must be changed by either the user or the administrator. NCS dial-in users can see the number of grace logins remaining as they authenticate with the Service Selector (if their password has expired) before they select a host session. A separate utility on the remote access client allows the user to check for the number of remaining grace logins. Refer to the Novell Internet Access Server 4.1 remote access online help for more information.

To set Remote Client passwords, complete the following steps:

- 1** Select **Configure Security** from the **Remote Access Options** window.

The **Configure Security** window is displayed.

- 2** Select **Set User Remote Client Password**.

A list of authorized users is displayed.

If users are distributed over multiple contexts, select the double period (..) to move up the Directory tree to a common branch. Select any other container object to move down the tree.

If the **CONNECT** object does not have **Browse** rights to move up the Directory tree, press **Ins** and enter the new Directory context. This allows you to jump to another branch of the tree where the **CONNECT** object does have rights.

- 3** Select a username.

The current status of the user's password is displayed, for example, never set or expired.

- 4** Enter a password.

The password must be alphanumeric and can contain up to 16 characters. The password is case-sensitive.

NOTE: You must enable password restrictions in order to specify passwords longer than 8 characters. Refer to **Setting Password Restrictions** for more information.

You can configure user passwords if the **CONNECT** object, in addition to having **Browse** and **Read** attribute rights, has **Write** attribute rights to the container.

NOTE: The Remote Client password is less secure than the NetWare password. Make sure it is not the same as the NetWare password.

- 5** Reenter the password.
- 6** Press **Esc** to save your changes.

7 Distribute the passwords to the corresponding users.

A user must enter this password to establish an initial connection with remote access.

An NCS dial-in user is prompted for a Remote Client password when dialing into remote access. If no Remote Client password is defined for this user, access will be denied.

NOTE: An undefined password is not the same as a NULL password. If the password is set to NULL, the user must press Enter when prompted for a password.

The Service Selector indicates when a Remote Client password has expired and enables the NCS dial-in user to change the password at login time.

Setting Password Restrictions

To set password restrictions on Remote Client passwords, complete the following steps:

- 1 Select Configure Security from the Remote Access Options window.

The Configure Security window is displayed.

- 2 Select Set Remote Client Password Restrictions.

- 3 Select Enable Long Passwords, then specify Yes or No to enable or disable this option.

NOTE: You cannot disable the long passwords feature once you have enabled it. If you enable long passwords, you must upgrade all your servers to Novell Internet Access Server 4.1. Users will no longer be able to use NetWare Connect 2.0. You must also set the Enable Long Passwords parameter on each server.

- 4 Enter a value between -1 and 20 for the Maximum Invalid Login Attempts parameter.

This sets the number of times the user can enter the wrong password before being disconnected. The Remote Client password is disabled and cannot be used after the specified number of failed tries. The default of -1 allows the user to reenter an incorrect password indefinitely.

- 5 Enter a value between -1 and 16 for the Set Minimum Password Length parameter.

This sets the minimum number of characters for a password. The change takes effect the next time the password is set. To increase security, have users specify passwords of five or more characters. The default of -1 means no limit is set.

6 Press Esc to save your changes.

Allowing Users to Change Passwords

You can allow or disallow users to change their passwords. If you allow users to change passwords, you can increase password security by requiring them to change passwords periodically. Refer to "User-Specific Remote Access Security" for information on how to do this.

NOTE: The user has a grace login limit of three logins after a password has expired. During this grace period, the password must be reset or changed by either the user or the administrator. NCS dial-in users can see the number of grace logins remaining if their passwords have expired during authentication with the Service Selector.

Remote access has Windows tools that enable users to change their Remote Client passwords and Windows and Macintosh tools that enable users to check for the remaining number of grace logins. Refer to the Novell Internet Access Server 4.1 remote access online help for more information. Refer to Remote Access Parameters in NetWare Administrator for more information on using the NetWare Administrator utility to assign and change Remote Client passwords.

The Service Selector also has a menu option for changing the Remote Client password. This option is available to NCS dial-in users or PPP dialers using the Terminal Window After Dial-in option.

Configuring for Third-Party Security

To configure for third-party security, complete the following steps:

- 1** Install the third-party security product. Follow the installation steps in the product documentation.
- 2** Select Set Third-Party Security Parameters from the Configure Security window.

NOTE: The Set Third-Party Security Parameters option is displayed only if a third-party security product is installed.

The Third-Party Security Parameters window is displayed.

- 3** Select Enable Third-Party Security and specify Yes.
- 4** Select Security Product Name, press Ins , then select a name from the list.

NOTE: When you install a third-party security product for remote access, the name of the third-party security product will remain in the Security Product Name list even after you have removed it.

- 5 Select Apply Third-Party Security to Direct-Connect Ports and specify Yes or No, depending on your configuration.

If you select No, third-party security will be enforced only for dial-in ports with modems attached. If you select Yes, third-party security will be enforced for all dial-in ports.

- 6 Press Esc to save your changes.

Third-party security is now enabled.

Remote Access Parameters in NetWare Administrator

You can use the NetWare Administrator utility to configure many of the same remote access parameters that you configure using NIASCFG. These parameters include AppleTalk Remote Access Service (ARAS) zones, IPX™/IP settings, Remote Client password, maximum connection time, dialback mode and number, and idle timeout. It might be easier for you to configure or change these parameters from a PC using the NetWare Administrator utility if the parameters affect a user, organization, organizational unit, country, or locality.

NOTE: If you still have NetWare Connect 2.0 servers on your network, you should be able to use the new NetWare Administrator snap-ins to administer NetWare Connect 2.0. If you do use the new snap-ins, you should apply the snap-ins to the NetWare Administrator version that comes with NetWare 5.

Setting Remote Access User Parameters

Perform this procedure to configure remote access user parameters, including the Remote Client password, connection time, idle timeout, and dialback.

To set remote access user parameters, complete the following steps:

- 1 Select a user from the Novell Directory tree in the NetWare Administration main window by double-clicking the username, or right-clicking the username and selecting Details from the pop-up menu.

The NetWare Administrator Details window is displayed. You can view or modify object properties from this window.

- 2 Scroll down the list of choices on the right side of the window and click Remote Access 1.

The Remote Access 1 dialog box is displayed.

- 3** For the Remote Client password, specify one or more of the following options:
 - ◆ Allow User to Change Remote Client Password—Select this check box to permit users to change their Remote Client passwords.
 - ◆ Disable Remote Client Password—Select this check box to invalidate the Remote Client password after a specified number of days. Enter the number of days in the text box.

NOTE: You must enable the Remote Client password if NASITM (NetWare Asynchronous Services InterfaceTM) Connection Service (NCS) dial-in security is enabled.
- 4** To change the Remote Client password, click Change Remote Client Password, then enter the new password.
- 5** For the Connect Time, do one of the following:
 - ◆ Select the Use Default Maximum Connect Time check box to select the default of no limit.
 - ◆ If you did not select the Use Default Maximum Connect Time check box, enter the number of minutes (between -1 and 100,000) in the Maximum Connect Time text box. A value of -1 indicates no limit.
- 6** Select Specify Idle Timeout and enter a number for the timeout, in minutes, between 1 and 100,000.

A value of -1 indicates no limit.
- 7** In the Dialback box, do the following:
 - 7a** Select a dialback mode.
 - 7b** Enter a dialback number, if Force Dialback to a Specific Number is selected as the dialback mode.
 - 7c** Select the Use Dial-In Port for Dialback check box, if applicable to the dialback mode selected.

NOTE: If you select a forced dialback option, Windows and DOS callers must specify a blank for the dialback number or the call will be rejected.
- 8** Click OK and save your changes, or continue with the next procedure.

Setting Remote Access Service Parameters

Perform this procedure to configure remote access service parameters for a user, organization, organization unit, country, or locality, including the ARAS

zone and IPX/IP parameters. You can also set the idle timeout for an organization, organization unit, country, or locality.

To set remote access service parameters, complete the following steps:

- 1** Select an object from the Novell Directory tree in the NetWare Administration main window by double-clicking the object, or right-clicking the name and selecting Details from the pop-up menu.

The NetWare Administrator Details window is displayed. You can view or modify object properties from this window.

- 2** Scroll down the list of choices on the right side of the window and click Remote Access 2. (Click Remote Access if you selected an organization, organization unit, country, or locality.)

The Remote Access 2 or Remote Access dialog box is displayed.

- 3** For ARAS, select a user restrict zone from the list.

If the ARAS user restrict zone is not listed, click the three-dot button to the right. This displays a dialog box that lets you add or delete zones from the user restrict zone list.

NOTE: This parameter is not available if you selected an organization, organization unit, country, or locality in Step 1.

- 4** If you are working with an organization, organization unit, country, or locality, select the Specify Idle Timeout check box and enter a number for the timeout, in minutes, between -1 and 100,000.

A value of -1 indicates no limit.

NOTE: This parameter is not available if you selected a user in Step 1.

- 5** For IPX, select the Specify IPX Address for User check box, then specify the following:

- ◆ IPX Address—Enter a unique hexadecimal address containing from 1 to 12 characters. Remote access uses this address to create a virtual network containing remote IPX nodes.
- ◆ IPX Address Mask—Enter the hexadecimal address used for user IPX addresses. Make sure that the 1 bit is contiguous and there are no leading zeros or zeros in the middle of the mask.
- ◆ Home Server(s)—Select the home server to which the remote node can attach at the client's local site.

NOTE: Servers assigned as home servers must be reachable from all remote access servers to which the user will be dialing, and they must be running

IPXRTR software. If servers are not functioning when you configure this parameter, the user must enter the server's IPX address.

- 6** For IP, select the Specify Domain Information check box, then specify the following:
 - ◆ Server Address—Enter the network address of the domain name server to resolve hostnames for client requests.
 - ◆ Domain Name—Enter the suffix to append to local hostnames.
- 7** For IP, select the Set Boot Parameters check box, then specify the following:
 - ◆ TFTP Server Address—Enter the network address of the server that provides the Trivial File Transfer Protocol (TFTP) used to access the boot file.
 - ◆ Boot File Name—Enter the name of the boot file that the client uses to start the remote workstation.
- 8** Click OK and save your changes.

Setting Remote Access IP Filtering

Perform this procedure to configure remote access IP filtering parameters for a user, organization, organization unit, locality, or country. This option might or might not be available on your system.

You can set IP filtering by primary or secondary IP address pool so that users can do the following:

- ◆ Access the Internet, but not access any locations on Novell Internet Access Server 4.1.
- ◆ Access multiple locations on Novell Internet Access Server 4.1, but not any locations on the Internet.
- ◆ Access the Internet and limited locations on Novell Internet Access Server 4.1.

If no filter is set, the users will have access to all locations on the server.

To set remote access IP filtering, complete the following steps:

- 1** Select an object from the Novell Directory tree in the NetWare Administration main window by double-clicking the object, or right-clicking the name and selecting Details from the pop-up menu.

The NetWare Administrator Details window is displayed. You can view or modify object properties from this window.

- 2 Scroll down the list of choices on the right side of the window and click Remote Access 3. (Click Remote Access 2 if you selected an organization, organization unit, country, or locality.)

The Remote Access 3 dialog box is displayed.

- 3 Select whether to use the primary or secondary IP address pool.

The display box shows the IP addresses that the user can send packets to and receive packets from. You can change the filtering parameters.

- 4 Click Add to add an IP address to IP filtering.

The IP Filter dialog box is displayed.

NOTE: You can also click Edit to change IP filtering information for an IP address.

- 5 Specify the following information:

- ♦ IP Address—Enter the address of the IP network you want to filter.
- ♦ Mask—Enter the mask for the IP network.
- ♦ Packet Type—Click one of the choices: Any, TCP, UDP, or ICMP.
- ♦ Ports—Click one of the options: Any, Range, or Service.

- 6 Click OK and save your changes.

Support for SNMP and ConnectView

This section discusses setting up remote access to be managed by ConnectView® and other SNMP management tools.

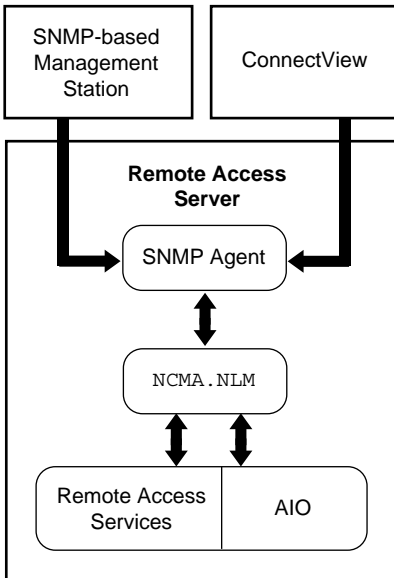
The following tasks must be performed on the remote access server to provide SNMP support:

- ♦ Configuring the SNMP Agent
- ♦ Loading RAMA

Remote Access Management Agent Overview

The remote access software can be managed from any SNMP-based management console (including ConnectView) on the network. The Remote Access Management Agent (RAMA) provides access to remote access services and the AIO ports through the NCMA.NLM file. The NCMA.NLM

file interfaces with other management consoles through NetWare SNMP (SNMP Agent), as shown below.



Configuring the SNMP Agent

NetWare SNMP loads automatically when your server starts. However, to change the SNMP options, you can manually start NetWare SNMP with the command while NetWare SNMP is running. You can also modify the LOAD SNMP line in the AUTOEXEC.NCF file to include your preferred default options. To load NetWare SNMP, use the following command format:

```
load snmp [options ]
```

The options allow you to establish the community name used in SNMP. NetWare SNMP also provides default community names for the monitor (read-only) and control (read/write) communities. NetWare SNMP uses these names for access control. The community name contained in a request message from an SNMP management station must match the name established by NetWare SNMP. By default, the control community is disabled for NetWare SNMP.

NOTE: If NetWare SNMP receives a request protocol data unit (PDU) whose community name is not authorized, NetWare SNMP does not respond to the request.

Community types can also be disabled. When a community type is disabled, no management entity can access information for that community. For example, if you disable the control community, no one can use NetWare SNMP to perform SET operations against the data NetWare SNMP manages.

Community Name Options

The LOAD command line accepts three SNMP options:

- ◆ Monitor community to enable read access
- ◆ Control community to enable read/write access
- ◆ Trap community to enable event traps

Syntax

M [onitorCommunity] = [*CommunityName*]

C [ontrolCommunity] = [*CommunityName*]

T [rapCommunity] = [*CommunityName*]

The option parameters are not case-sensitive. In addition, when specifying option parameters, you need to enter only the first character of the option name, although complete or partial names are also accepted. For example, T, TrapCom, and Trap are all interpreted as TrapCommunity.

The Community Name is an arbitrary ASCII string of up to 32 characters. It can include any characters except space, tab, open square bracket ([), equal sign (=), colon (:), semicolon (;), and number sign (#).

NOTE: Community names are case-sensitive. Therefore, the names Public, public, and PUBLIC denote three different communities.

Enabling Access by a Single Community Name

To enable access to a community for a single community name, enter the option parameter, followed by an equal sign (=), followed by the community name. Thereafter, the community name offered by the SNMP management station must match the specified value; otherwise NetWare SNMP denies access for the request.

Enabling Access by Any Community Name

If you follow the option name only by an equal sign without an argument, NetWare SNMP accepts any community name offered by an SNMP

management station for that community. For example, the following command will allow read access to any community name:

```
load snmp monitorcommunity=
```

Disabling Access to a Community

To disable access to a community, enter the associated option name without following it by an equal sign (=). For example, the following command will load SNMP and disable all read/write access:

```
load snmp controlcommunity
```

Examples

To set the read/write community to secret, use the following command:

```
load snmp controlcommunity=secret
```

To disable all read/write access, use the following command:

```
load snmp controlcommunity
```

To allow any community name to be used for read access, use the following command:

```
load snmp monitorcommunity=
```

To allow any community name to have read-only access, and to set the read/write community name to private, use the following command:

```
load snmp m= c=private
```

To set the community name for traps to *AgentTrap*, use the following command:

```
load snmp Trapcommunity=AgentTrap
```

Configuring NetWare SNMP to Send Traps to Your Application

To receive traps sent by NetWare SNMP, make sure your management station address is listed in the IP or IPX section of the `SYS:\ETC\TRAPTARG.CFG` file. Edit the file with any ASCII text editor and follow the instructions given in the file comments.

Sample TRAPTARG.CFG File

An example of the TRAPTARG.CFG file is shown in Figure 9. This file specifies all SNMP managers that are to receive SNMP trap messages generated by the SNMP Agent (SNMP.NLM).

Figure 9 Sample TRAPTARG.CFG File

```
Protocol IPX
# In this section you can put SNMP managers that want
# to receive traps from the local node over IPX.
# Managers can be identified by NetWare service name (e.g.,
# NetWare file server name, for example) or by IPX
# address. To specify by IPX address, use the following
# format:
#   IPX Network Number: MAC Address
#
# for example, c9990111:00001B555555

C1FF3691:00001B5537E7
01114144:00001B3A5ABE

Protocol UDP
# In this section you can put SNMP managers that want
# to receive traps from the local node over UDP.
# Use either IP address or logical name. (If you use a
# logical name be sure the name and its corresponding
# IP address appear in the SYS:ETC\HOSTS file.)
# By default, the local node sends traps at least
# to itself.

127.0.0.1          #send traps to the loopback address
192.20.12.100     # a sample ip address
```

Loading RAMA

The Remote Access Management Agent is loaded when you start remote access with the **nwcstart** command. You can check to see whether RAMA is already loaded using the **MODULES** command.

To enable RAMA (if it is not loaded), load NIASCFG and follow this path:

Select Configure NIAS > Remote Access > Set Up ... > Select Remote Access Services > RAMA

After you select RAMA, the necessary load and unload commands are added to the NWCSTART.NCF and NWCSTOP.NCF files.

The server asks, Do You Want to Start This Service Now? If you select Yes, the service is started. Otherwise, the service will not be started until the next **nwcstart** command.

After loading, the RAMA registers the management information bases (MIBs), NCMIB and AIOMIB, with the SNMP Agent so it knows to forward requests that are designated for remote access. The RAMA then reads the remote access and AIO configuration information and registers with the Remote Access Supervisor for notification of remote access configuration changes.

NOTE: The RAMA must run on the same server as the NetWare SNMP Agent.

ConnectView

To install ConnectView, complete the following steps:

- 1** Insert and mount the Novell BorderManager CD-ROM.
- 2** Choose File > Run from the Program Manager menu and run the ConnectView SETUP.EXE program from the \CLIENT\CVIEW\DISK1 directory.

See your Windows documentation for details about running applications within Windows.

- 3** Follow the installation program's directions.

The installation program displays a series of windows with dialog boxes that guide you through the installation process. Although the dialog boxes are self-explanatory, when you are installing ConnectView, you should be aware of the following information:

- ◆ The default directory of ConnectView is \NWCVIEW.
- ◆ You can exit the installation program any time; simply click the Exit button. A message appears to confirm the operation.
- ◆ ConnectView enables you to specify the target directory to which the Btrieve v6.15 files are copied. By default, the Btrieve files are copied to the \WINDOWS directory. If you want to copy the files to a different directory, click the Btrieve Directory button in the Welcome screen and specify the desired location.
- ◆ If any ConnectView files already exist on the target location, ConnectView lists the installation files and the existing files with check boxes for each file. If you want to overwrite the installed files, click the check boxes for the desired version of the displayed files.
- ◆ ConnectView edits your AUTOEXEC.BAT file to load the BREQUEST.EXE and SHARE files. If you change the AUTOEXEC.BAT file, the current file is saved as AUTOEXEC.SAV. If you do not change the AUTOEXEC.BAT file, the file with changes suggested by ConnectView is saved as AUTOEXEC.NEW.

IMPORTANT: If you are using the NetWare Client (VLM)1.2 software, you can run ConnectView in both Windows 3.1 and Windows 95 environments. If you are using the Novell Client for DOS and Windows 3.1x software, you can run ConnectView in the Windows 3.1x environment. If you are using the Novell Client for Windows 95 software, ConnectView moves the statement that loads BREQUEST.EXE from your AUTOEXEC.BAT file to the WINSTART.BAT file to enable you to run ConnectView in a Windows 95 environment.

- ◆ When viewing the AUTOEXEC.BAT file, click the Warning Alerts button to display possible conflicts with files existing in multiple locations. ConnectView also suggests corrective actions to avoid these conflicts.

- 4** If your AUTOEXEC.BAT file has changed, reboot your system. Otherwise, restart Windows.

If you changed your AUTOEXEC.BAT file to load the BREQUEST.EXE file after the NetWare shell but before Windows, or for any other reason, reboot your system before starting ConnectView. Otherwise, bring down Windows, ensure that the BREQUEST.EXE file is loaded after the NetWare shell, and restart Windows before starting ConnectView. However, if you do not include the statement to load the BREQUEST.EXE file in your AUTOEXEC.BAT file, the next time you

reboot the ConnectView workstation you will have to reload the BREQUEST.EXE file before starting ConnectView. If you choose to return to Windows, ensure that the proper action is taken before you attempt to start ConnectView.

5 Check the ConnectView file NWCVIEW.TXT for product notes.

ConnectView provides the NWCVIEW.TXT file for product notes and last-minute feature changes. This file is stored in \NWCVIEW. To access this file anytime, use the Microsoft* Notepad or any text editor.

Starting ConnectView

ConnectView creates a ConnectView program group in Program Manager with ConnectView, NWCV Help, and NWCV Readme Notes icons. If a ConnectView program item already exists, it is replaced with a new link to the ConnectView 2.1 program files.

To start ConnectView, double-click the ConnectView icon. ConnectView opens the application and displays a View All window with a list of the managed servers.

To manage the remote access software, select the desired server and then click the desired icons in the Tool Bar or choose the commands in the Menu Bar.

Exiting ConnectView

Exit ConnectView whenever you no longer want to monitor or manage the remote access software on the servers displayed in the View All window.

To exit ConnectView, use either of the following methods:

- ◆ Choose File > Exit (Alt+F+X).
- ◆ Issue the Windows Close command from the Application window. To do this, select the Control-menu box to display the Control menu and then choose Close (Alt+F4). For details about the Close command, see your Windows documentation.

NOTE: Double-clicking the Control-menu box also allows you to exit ConnectView.

Installing with ManageWise

When installing ConnectView with ManageWise, ensure that the following requirements are met:

IMPORTANT: ConnectView does not support the Simple Network Management Protocol (SNMP) over IP.

- ◆ ManageWise software and workstation requirements
- ◆ ConnectView product diskettes
- ◆ 8 MB of RAM in addition to the ManageWise requirement
- ◆ 4 MB of disk space in addition to the ManageWise requirement

IMPORTANT: Because ManageWise can run with multiple Windows applications, refer to the ManageWise documentation to ensure that you have sufficient DOS memory and Windows resources to run ConnectView. If you are low on DOS memory, you might not be able to launch ConnectView. You might also be unable to open numerous windows if you are low on Windows resources.

Before installing ConnectView, perform the following tasks:

- 1** Ensure that ManageWise is installed.

ConnectView can also run as a standalone application if ManageWise is unavailable.

WARNING: If the install mode does not match the runtime environment, ConnectView displays a warning message and exits the installation. The install mode does not match the runtime environment if ConnectView was installed as a standalone application but the workstation is running with ManageWise, or ConnectView was installed with ManageWise but the workstation is running without ManageWise.

- 2** Close ManageWise and exit any ManageWise applications.
- 3** Insert the Novell® Internet Access Server 4.1 CD-ROM in the workstation's CD-ROM drive.
- 4** Choose File > Run from the Program Manager menu to run the ConnectView SETUP.EXE program from Windows.

See your Windows documentation for details about running applications within Windows.

- 5** Follow the installation program's directions.

The installation program displays a series of windows with dialog boxes that guide you through the installation process. Although the dialog boxes are self-explanatory, when responding to them you should be aware of the following information:

- ◆ ConnectView is installed in \MW\NMS\BIN.

This directory also contains the NWCVIEW.TXT file and is the default location for trend analysis files (files with .TAD extension) and accounting profiles (files with .NCP extension).

- ◆ You can exit the installation program anytime; simply click the Exit button. A message appears to confirm the canceling of the installation.
- ◆ When running with ManageWise, ConnectView allows you to display all servers running the remote access software as Novell Internet Access 4.1 server icons in the ManageWise maps. If you do not wish the servers running the remote access software to appear as Novell Internet Access Server 4.1 server icons in your ManageWise maps, select the No radio button on the Welcome screen.

IMPORTANT: If you choose the option to display server icons, be sure to run the NetExplorer™ program to ensure that the ManageWise maps are updated.

- ◆ ConnectView enables you to specify to which directory the Btrieve v6.15 files are copied. By default, the Btrieve files are copied to the \WINDOWS directory. If you wish to copy the files to a different directory, click the Btrieve Directory button in the Welcome screen and specify the desired location.
- ◆ If any ConnectView files already exist on the target location, ConnectView lists the installation files and the existing files with check boxes for each file. If you wish to override this, click the check boxes for the desired version of the displayed files.

NOTE: If an older version of the WLIBSOCK.DLL file exists on your workstation, ConnectView displays a warning message.

- ◆ ConnectView enables you to edit your AUTOEXEC.BAT file to load BREQUEST.EXE and SHARE. If you change this file, the current file is saved as AUTOEXEC.SAV. If you do not change this file, the file with changes suggested by ConnectView is saved as AUTOEXEC.NEW.
- ◆ When viewing the AUTOEXEC.BAT file, click the Warning Alerts button if you want to view a display of possible conflicts with files existing in multiple locations. ConnectView also suggests corrective actions to avoid these conflicts.

- 6 If your AUTOEXEC.BAT file has changed, reboot your system. Otherwise, restart MS Windows.

If you changed your AUTOEXEC.BAT to load BREQUEST.EXE after the NetWare shell and before MS Windows or for any other reason, reboot your system before you start ConnectView. Otherwise, bring down MS Windows, ensure that BREQUEST.EXE is loaded after the NetWare shell, and restart Windows before you start ConnectView. If you choose

to return to Windows, ensure that the proper action is taken before you attempt to start ConnectView.

7 Check the ConnectView file NWCVIEW.TXT for product notes.

ConnectView provides the NWCVIEW.TXT file for product notes and last-minute feature changes. This file is stored in \MW\NMS\BIN. To access this file at any time, use the Microsoft Notepad or any similar text editor.

Using ManageWise SNMP Options

If ConnectView is installed with ManageWise, ConnectView utilizes the SNMP engine in ManageWise and does not install the SNMP files on your workstation.

You can use the ManageWise command Configure > Global Preferences > SNMP Options to configure global community strings on your workstation for all Novell Internet Access 4.1 servers running the remote access software. In addition, ManageWise offers secure SNMP over NCP. This encapsulates an SNMP PDU in a NetWare Core Protocol™ (NCP™) packet. You can also use the ManageWise SNMP Options dialog box to configure SNMP over NCP separately for GET and SET requests on individual servers. If this option is used, a login dialog box for either the Novell Directory Services™ (NDS™) program or Bindery login information appears before an SNMP GET or SET operation is performed.

Starting from ManageWise

You can start ConnectView from ManageWise in the following ways:

- ◆ Choose Tools > ConnectView from the ManageWise Menu Bar.

ConnectView opens the application and displays the View All window with a list of the available servers.

- ◆ Double-click a Novell Internet Access 4.1 server icon in a ManageWise map.

ConnectView opens the application and displays the View All window with a list of the available servers and a View window for the selected server.

4

Optimizing

The remote access ports are automatically configured when you first install and configure the remote access software. The remote access automated software installation process loads the AIO hardware drivers and selects the appropriate modem types. Refer to *Using the Automated Setup Program* for more information about the automated configuration. Use the topics in this section to optimize ports, security settings, and remote access dialers and connections.

Port Configuration

You can modify the following port configuration information:

- ◆ Port names
- ◆ Modem types
- ◆ Data rate

To modify existing port configurations, complete the following steps:

- 1** Select **Configure Ports** from the **Remote Access Options** window.
- 2** Select a port from the list of ports.
- 3** Modify the port configuration fields by doing the following:
 - ◆ To modify the port name or modem type, highlight the port you want to modify, then press **Enter** to move to the lower part of the window. To change the port name, type the new port name and press **Enter**. To change the modem type, select **Modem Type**, press **Enter**, then select from the list of modem types.

- ◆ To modify the advanced port configuration fields, select Additional Parameters and press Enter. Refer to Advanced Port Configuration for information about completing the fields.
- 4 When you have completed making the port configuration changes, press Esc.
 - 5 Press Esc to exit the port configuration window.

Advanced Port Configuration

This section contains the information you need to configure the following advanced parameters, shown in Table 10, in the Port Configuration window.

Table 10 **Advanced Port Configuration Parameters**

Parameter	Description	Default
Modem Parameters	Lets you specify the following:	
	Dial Type—Sets tone or pulse dialing.	Tone
	Leased Line—Specifies whether the port is connected to a leased line.	No (Dial)
	Modem Init String—Adds additional modem strings to be executed after the modem script. For example, specify ATM0 to turn off the modem speaker.	None; 36-character limit
Link Parameters	Lets you specify the following:	
Note: For dial-in ports, the Link Parameters option is used only for direct connections.	Initial Data Rate—Sets the port speed between the server and the modem.	9,600 bps for direct connections; otherwise, the maximum speed supported by the modem and port
	Initial Data Bits—Sets the number of data bits sent per character.	8
	Initial Parity—Sets parity checking for the parity bit.	NONE

Parameter	Description	Default
	Initial Stop Bits—Sets the number of stop bits transmitted per character.	1
	Initial Flow Control—Sets hardware and software flow control.	Based on the selected modem type
Port Mapping	Shows the relationship between the port and the physical hardware. The field has the format (x,y,z), where: x = driver name or number y = board name or number z = port number For example, (COMX,0,0) indicates that COMX is the AIO driver on the port, the first zero is the board number, and the second zero is the port number.	Not configurable by the user
Groups Assigned To	Allows you to select the groups in which the port will be a member.	ANY_PORT
Applications Allowed	Limits port access to the AIO or AIOMGR application.	Any Application
Application Parameters	Used by other applications that use the communication ports, for example, e-mail services. Refer to the application-specific documentation for information about what is required for this field.	Not applicable to remote access

To specify advanced port configuration, complete the following steps:

- 1** Access the Port Configuration window by following this path:
Select Configure NIAS > Remote Access > Configure Ports > a port name > Additional Parameters
- 2** Select Modem Parameters, press Enter , then specify the following parameters:

- ◆ Dial Type—Specify Tone or Pulse.
- ◆ Leased Line?—Specify Yes for a leased line or No for a dial line.
- ◆ Modem Init String—Enter a string of up to 36 characters.

3 Select Link Parameters, press Enter , then specify the following parameters:

- ◆ Initial Data Rate—If you are using a modem, you do not have to change this parameter. Make sure the data rate matches the communications equipment.
- ◆ Initial Data Bits—Select 5, 6, 7, or 8 bits. Set to 8 for ARAS and PPPRNS. The sizes displayed depend on the settings supported by the communications adapter controlling the port.
- ◆ Initial Parity—Set to NONE, ODD, EVEN, MARK, or SPACE.
- ◆ Initial Stop Bits—Set to 1, 1.5, or 2.
- ◆ Initial Flow Control—Set to one of the following:

HDW/OFF, SW/OFF for connections with no flow control. This is the correct setting for multiplexed connections and dial-in connections if the port is attached to modems capable of 2,400 bps or less.

HDW/ON, SW/OFF for connections with hardware flow control only. This is the correct setting for dial-in connections if this port is attached to modems capable of 9,600 bps or higher.

HDW/OFF, SW/ON for connections with software flow control only.

HDW/ON, SW/ON for connections using both software and hardware flow control.

IMPORTANT: If you are using modems, remote access automatically sets the data rate and flow control based on the selected modem type. For direct connections, make sure that the data rate, data character size, type of parity checking, and stop bits used by the remote access port match those used by the remote hardware and software.

4 Select Groups Assigned To and press Enter.

The groups that this port is a member of are displayed.

NOTE: If you have not defined any group names, you see only the default group name ANY_PORT. You must define group names before you can assign the port to a group. Refer to Creating Port Groups

4a Select one or more groups and press Enter.

- 4b** Press **Ins** to display a list of additional available groups.
- 5** Select **Applications Allowed** and press **Enter**.
- 6** Press **Ins** and enter one of the following options for the application name:
 - ◆ **AIO**—Allows AIO applications written for earlier AIO releases to access the ports.
 - ◆ **AIOMGR**—Allows new applications written to the AIOMGR interface to access the ports.
 - ◆ **CONNECT**—Allows remote access applications written to the Service Selector interface (for example, PPPRNS, ARAS, or NCS) to access ports.

The default is **Any Application**.

Port Groups

Modifying port groups consists of the following tasks:

- ◆ Renaming a group
- ◆ Deleting a group
- ◆ Deleting group members
- ◆ Adding new members to a group

To modify a port group, complete the following steps:

- 1** Select **Configure Port Groups** from the **Remote Access Options** window.
- 2** Select a group name from the **Group Names** list.
- 3** Do one of the following:
 - ◆ To rename a group, press **F3**.
 - ◆ To delete the selected group, press **Del**.
To delete multiple groups, press **F5** to select the groups, then press **Del**.
 - ◆ To delete a member of a group, select the group. From the displayed list of group members, highlight the group member that you want to delete and press **Del**.
To delete multiple group members, press **F5** to select the group members, then press **Del**.

- ◆ To add members to a group, select the group. A list of group members is displayed. Press **Ins** to display a list of ports. Select the port that you want to add to the group. Press **F5** to select multiple ports.

NOTE: The port group named ANY_PORT cannot be renamed or deleted.

- 4** When the group is configured the way you want it, press **Esc**.
- 5** Press **Esc** to exit the Configure Port Groups window.

Ports Available for Remote Access

When you first install remote access, all available ports are automatically selected. Perform this procedure to switch a port from Novell Internet Access Server 4.1 routing to remote access, or to ensure that you have identified the correct ports for remote access to use.

To select ports for remote access, complete the following steps:

- 1** Select **Set Up...** from the Remote Access Options window.

The System Setup Options window is displayed.

- 2** Choose **Select Remote Access Ports**.

- 3** Press **Ins** to display a list of configured ports.

NOTE: To make a remote access port available for routing, simply delete the port from the displayed list.

- 4** Select one or more ports for remote access to use.

Press **F5** to select multiple ports. Press **Alt+F5** to select all ports.

- 5** Press **Esc** to return to the System Setup Options window.

Ports for Unidirectional Support

By default, ports are bidirectional; each port supports both dial-in and dial-out operations. Perform this procedure to make ports unidirectional. For example, if you have a port connected to a 1-800 telephone number, enable the port for dial-in operation only.

Skip this section if you want to use all remote access server ports for dialing in and dialing out, the default port usage setting.

To set the direction of the remote access ports, complete the following steps:

- 1** Select Set Up... from the Remote Access Options window.
The System Setup Options window is displayed.
- 2** Select Define Remote Access Port Usage.
The Port Usage Options window is displayed.
- 3** Select a port usage option: Dial-In Only, Dial-Out Only, or Both Dial-In and Dial-Out.

A list of ports for that port usage option is displayed. Select an option from the Port Usage Options window to display the list of ports for that option. Press **Ins** to add ports to that option. Press **Del** to delete ports from that option.
- 4** Do one or more of the following:
 - ◆ Press **Ins**, then select a port from the list of ports and add it to the port usage list.
 - ◆ Select a port from the port usage list and press **Del** to remove it from that option and move it to another option.
- 5** Press **Esc** to return to the System Setup Options window.

Port Access Time

After you have authorized the ports for specific services, you can optimize the port access times.

To authorize port access to remote access services for a specific time of day or week, complete the following steps:

- 1** Select Restrict Service by Port from the Configure Security window.
A list of installed services is displayed.
- 2** Select a service.

A list of ports authorized to use that service is displayed. If Any Port is listed, press **Ins** and select the ports for the service to use.
- 3** Select a port.

The Access Time Restrictions window for that port is displayed.

The selected port can access the service during the times marked with an asterisk. Each asterisk denotes a half-hour block. To restrict access time, use the following keys:

- ◆ Enter —Toggles the current setting.
- ◆ Arrow keys—Move the cursor.
- ◆ Space or Delete —Turns an option off.
- ◆ * or Ins —Turns an option on.
- ◆ F5 —Marks and changes a large block at a time.
- ◆ F4 and F6 —Copy restrictions to or from other ports.

4 Press Esc and save the changes.

NOTE: This procedure only limits the time that a port can establish a connection to a service. Once connected, the port will not be disconnected unless the user requests it or an idle timeout or maximum connect time occurs.

User-Specific Remote Access Security

Use the procedure to set the following user-specific remote access information:

- ◆ Whether a user can change the Remote Client password
- ◆ How often the user must change the Remote Client password (in days)
- ◆ Idle timeout
- ◆ Maximum connection time
- ◆ Dialback mode
- ◆ Whether to use the global dial-out restrictions or create a restriction list

NOTE: For a container object, you can only configure idle timeout.

To specify security parameters for individual users, complete the following steps:

1 Select Configure Security from the Remote Access Options window.

The Configuration Options window is displayed.

2 Select Set User Parameters.

A list of authorized users is displayed.

If users are distributed over multiple contexts, select the double period (..) to move up the Directory tree to a common branch. Select any other container object to move down the tree.

If the CONNECT object does not have Browse rights to move up the Directory tree, press Ins and enter the new Directory context. This allows you to jump to another branch of the tree where the CONNECT object does have rights.

- 3 Select the name of the user that you want to customize.

The User Parameters window is displayed for that user.

As a remote access server administrator, you can configure user parameters if the CONNECT object, in addition to having Browse and Read attribute rights, has Write attribute rights to the container in which the username resides.

When a user's account is disabled by intruder lockout or an expired password, modify one of the parameters in this window or the Remote Client password to reenab the account.

- 4 Select Allow User to Change Remote Client Password, and specify Yes or No to allow or disallow the user to change the password.
- 5 Select Disable Remote Client Password After Number of Days and enter a value between -1 and 365 days.

A value of -1 indicates no limit. The default value is 30 days, indicating that the user must change the password once every 30 days. A value of 0 indicates that the user will be disconnected immediately after dialing in.

- 6 Select Specify Idle Timeout and specify Yes or No. If you select Yes, enter a value between -1 and 100,000 minutes.

The default value of -1 indicates that the idle timer is not set and connections can remain idle for any amount of time. The timer is reset whenever data is sent or received through the port, including any broadcast or watchdog traffic. A value of 0 means that the idle timeout occurs immediately. You can set this value for a user or container object.

- 7 Select Use Default Maximum Connection Time and specify Yes or No. If you select No, enter a value between -1 and 100,000 minutes.

A value of -1 allows the user to remain connected indefinitely. The default is 0 minutes. Setting the maximum connection time to 0 immediately disconnects the user when the user dials in. Changing the value does not affect current connections. The default maximum connection time is specified when global security is set.

NOTE: If the remote client is configured and has negotiated short-hold with the server, both the Idle Time Before Temporary Disconnect and Maximum Call Suspension timers are used (refer to Specifying ISDN Short-Hold Parameters).

The other timers associated with the connection, Default Maximum Connection Time and Idle Time Before Disconnection (each configured on a global or individual user basis), are ignored.

If the remote client does not negotiate short-hold with the server, both the Idle Time Before Disconnection and Maximum Call Suspension timers are ignored. The other timers associated with the connection, Default Maximum Connect Time and Idle Time Before Disconnection, are used.

8 Select Dialback Mode and press Enter.

8a Select one of the following modes:

- ◆ Use Global Default Dialback Mode—The default dialback mode specified for global remote access security is used. Skip to Step 9.
- ◆ No Dialback Allowed—Dialback is disabled for this user. Skip to Step 9.
- ◆ Force Dialback to a Specific Number—Remote access dials the caller back at a preselected telephone number. Enter a dialback number for the caller. If you select this option, make sure that the user does not specify a dialback number when establishing the connection (specify a blank in the DOS and Windows Dialers for NetWare Connect 2.0). Continue with Step 9.
- ◆ Allow User to Request Dialback to Any Number—The user can request remote access to dial back to any number specified at connection time. Continue with Step 9.
- ◆ Force Dialback to a Caller-Specified Number—The user is required to use the dialback feature. The dialback number is not preconfigured on remote access. The caller specifies the dialback number at connection time. Continue with Step 9.

8b Specify a port for dialing back.

To have remote access dial back on the same port that the caller used to dial in, select Use Dial-In Port for Dialback and specify Yes.

To have remote access dial back to a port group, select Dialback Port Group, press Enter, and specify a port group.

9 To set dial-out restrictions, select Use Global Dial-Out Restrictions and specify No.

The Restriction List field is displayed.

9a Press Enter.

A list of authorized dial-out numbers is displayed. Initially, the default Any Number is displayed, indicating that the user can dial out to any number.

9b Press Ins.

9c Enter a dial-out number.

The user is restricted to that dial-out number. Enter an invalid phone number to prevent a user from dialing out to any number at all. This restriction applies only if you use modem-independent groups.

Press Ins again to add another number. You can add or delete phone numbers. Use the F5 key to select and delete multiple entries.

Deleting the last number in the list redisplayes the Any Number entry.

10 Press Esc to exit and save your user security settings.

Service-Specific Remote Access Security

Each remote access service has its own security-related options. You must configure the service-specific security options to provide a secure system on your network.

Configuring PPP Remote Node Service Security

To configure PPPRNS security, complete the following steps:

1 Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

2 Select PPPRNS.

The PPPRNS Configuration Options window is displayed.

3 Select Configure Security.

The PPPRNS Configuration window is displayed.

4 Select Enable Security and specify Yes or No to enable or disable PPPRNS security.

NOTE: When security is disabled, callers can establish a connection successfully by entering a valid username without a password. However, callers still must log in to the network.

5 Specify Yes or No to enable or disable the NetWare Connect Authentication Protocol (NWCAP).

This method is supported by the Dialer remote access dialer. NWCAP allows the NetWare password to be used as the Remote Client password (the default).

- 6 Specify Yes or No to enable or disable the Password Authentication Protocol.

The default is No. If you enable this protocol, callers configured for PAP must specify the Remote Client password to successfully establish a connection. This method is supported by the remote access dialer. Enable this option if you have UNIX clients that support PAP.

- 7 Specify Yes or No to enable or disable the Challenge Handshake Authentication Protocol.

This method is not supported by the remote access dialer shipped with Novell Internet Access Server 4.1. This method requires callers to specify a Remote Client password to establish a connection. To set Remote Client passwords, refer to Setting Remote Client Passwords.

NOTE: Enable this option if you have the native Windows 95 or Windows NT dialers. If you want PAP or CHAP users to authenticate if they do not have a Remote Client password, enter `Set PPPRNS AdminNoConfig=ON` at the server console. The default is OFF. Setting this option to ON is not recommended.

Configuring NASI Connection Service Security

With NASI Connection Service (NCS), security requires users to specify passwords for network workstations or specify usernames and passwords for remote workstations.

To configure NCS security, complete the following steps:

- 1 Select Configure Services from the Remote Access Options window.

The Remote Access Services window is displayed.

- 2 Select NCS.

The NCS Configuration Options window is displayed.

- 3 Select Enable NCS Dial-In Security, then specify Yes or No to enable or disable this option.

This security option applies to the remote workstation dialing in through the Service Selector (using the shared DIALIN port) to access host sessions on the network. The default (Yes) requires users to specify the Remote Client password. If this field is disabled, users are prompted only for a username.

If the user is accessing a private session on the network, the dial-in username must be the same one used when NASI, Win2NCS, or Mac2NCS are loaded on the network workstation. If the user is accessing a public session on the network, the dial-in username can be different from the username used on the network workstation.

- 4** Select Enable NASI Security, then specify Yes or No to enable or disable the option.

This security option applies only to the NASI workstation on the network dialing out. The default (Yes) forces users to specify the NetWare password. If the user is not logged in to the network, NCS will also prompt for a username. If the field is disabled, users are not prompted for a username or password.

Configuring AppleTalk Remote Access Service Security

To enhance network security, you can prevent callers from accessing specific AppleTalk zones on the network in the following ways:

- ◆ **Restrict global access to AppleTalk zones.** Limit all users to specified AppleTalk zones on the network.
- ◆ **Restrict user access to AppleTalk zones.** Limit individual users to specific AppleTalk zones on the network.
- ◆ **Automate the connection.** Allow AppleTalk Remote Access Client 2.0 users to automate the connection process by sending a stored password instead of manually entering the password every time.

Setting Global Access for AppleTalk Zones

To set default zone restrictions, complete the following steps:

- 1** Select Configure Services from the Remote Access Options window.

The Services Options window is displayed.

- 2** Select ARAS.

The ARAS Configuration Options window is displayed.

- 3** Select Set Default Zone Restriction.

A restricted zone list is displayed. Initially, the Any Zone option is displayed and users have access to all zones.

- 4** Press **Ins** to add zones to the list, or press **Del** to delete zones from the list.

A list of other known zones is displayed.

- 5 Select the zone to which you want to restrict access.

Press F5 to select multiple zones.

- 6 If the zone to which you want to restrict access does not appear in the Other Zone List window, press Ins , then enter the zone name.

A valid zone name can contain up to 32 characters, including all printable characters.

- 7 Press Esc to save your changes.

All users are now limited to accessing the AppleTalk zone or zones in the restricted zone list.

Setting User Access for AppleTalk Zones

To restrict individual users to specific AppleTalk zones, complete the following steps:

- 1 Select Configure Services from the Remote Access Options window.

The Services Options window is displayed.

- 2 Select ARAS.

The ARAS Configuration Options window is displayed.

- 3 Select Set User Zone Restriction.

A list of ARAS users is displayed.

If users are distributed over multiple contexts, select the double period (..) to move up the Directory tree to a common branch. Select any other container object to move down the tree.

If the CONNECT object does not have Browse rights to move up the Directory tree, press Ins and enter the new Directory context. This allows you to jump to another branch of the tree where the CONNECT object does have rights.

- 4 Select a username.

A restricted zone list for that user is displayed. Initially, the Any Zone option is displayed and the user has access to all zones. You can use F4 and F6 to copy access settings to or from another user.

NOTE: The Any Zone option is also displayed when default zones are defined. Select this option to select the default zone specification.

The remote access server administrator can set zone restrictions for the user if the CONNECT object, in addition to having Browse and Read attribute rights, has Write attribute rights to the container in which the username resides.

- 5** Press **Ins** to add zones to the list, or press **Del** to delete zones from the list.

A list of other known zones is displayed.

- 6** Select the zone to which you want to restrict access.

Press **F5** to select multiple zones from the list.

- 7** If the zone to which you want to restrict access does not appear in the Other Zone list, press **Ins**, then enter the zone name.

- 8** Press **Esc** to save your changes.

The users now are limited to accessing only the zones in the restricted zone list.

Automating the Connection

You can let AppleTalk Remote Access Client 2.0 callers automate the connection process by sending a stored password instead of manually entering the password every time.

To automate the connection, complete the following steps:

- 1** Select **Configure Services** from the **Remote Access Options** window.

The **Services Options** window is displayed.

- 2** Select **ARAS**.

The **ARAS Configuration Options** window is displayed.

- 3** Select **Setup Options**.

The **Setup Options** window is displayed.

- 4** Select **Prompt User for Remote Client Password**, then specify **Yes** to have the user enter the password manually or **No** to have the client use the stored password.

- 5** Press **Esc** to save the changes.

Third-Party Dialers for Use with Remote Access Services

You can use several third-party dialers to remotely access a server. However, the configuration for these dialers must be set correctly to achieve a remote access connection.

Setting Up the Windows 95 Dial-Up Networking Dialer

- 1** Make sure the Windows 95 Dial-Up Networking dialer is installed and your modems are configured.

If you have not previously done this, refer to your Windows documentation for installation and configuration instructions. Once installation and configuration are complete, the Dial-Up Networking folder will appear.

- 2** Double-click the Dial-Up Networking folder.

- 3** Double-click Make New Connection.

- 4** Follow the on-screen instructions to configure your connection.

You will be prompted to enter a name and phone number for this connection.

- 5** Click Finish when you have entered the appropriate information.

A new connection icon with the information you entered now appears in the Dial-Up Networking folder.

- 6** Right-click the icon and then click Properties from the menu.

- 7** Click Server Type to configure the correct protocols for remote access services.

- 8** Uncheck Require Encrypted Password.

- 9** Uncheck NetBEUI.

- 10** Do one of the following:

- ◆ If you are using IPXTM, check Log On to the Network.
- ◆ If you are using TCP/IP only, uncheck Log On to the Network.

NOTE: It might be necessary to set the TCP/IP settings. See your network supervisor for details.

- 11** Click OK to close the Server Type window.

12 Click OK to save the changes made to your connection setup.

You are now ready to dial in to the server.

Dialing In to the Server Using the Windows 95 Dial-Up Networking Dialer

Windows 95 Dial-Up Networking dials in to the server and establishes a remote node connection.

1 In the Dial-Up Networking folder, double-click the icon for the connection to the server.

2 Enter your network user ID including the context.

3 Enter your remote access password.

NOTE: Your remote user password might be different from your network login password. See your network supervisor for more information.

4 Click Connect to dial.

Setting Up the Windows NT 3.51 Remote Access Services Dialer

1 Make sure the Windows NT 3.51 Remote Access Services dialer is installed and your modems are configured.

If you have not previously done this, refer to your Windows NT documentation for installation and configuration instructions.

2 Double-click Remote Access Services on the Desktop.

3 Double-click Remote Access.

4 Click Add.

5 Enter the name, phone number, and a description (optional) for this connection.

6 (Conditional) If your remote username or password is different from your NT username or password, uncheck **Authenticate Using Current Username and Password**.

7 Click **Advanced**.

8 Click the port that your modem is connected to.

9 (Optional) Click **Modem** to set software compression.

10 (Optional) Check **Enable software compression**, and then click **OK**.

11 Click **Network**.

- 12** Uncheck NetBEUI.
- 13** Uncheck Request LCP Extensions.
- 14** Click PPP.
- 15** Check the desired protocols (IPX, IP, or both).
NOTE: It might be necessary to set the TCP/IP settings. See your network supervisor for details.
- 16** Click OK to save the configuration settings.
- 17** Click OK again.

Dialing In to the Server Using the Windows NT 3.51 Remote Access Services Dialer

Windows NT 3.51 Remote Access Services dials in to the server and establishes a remote node connection.

- 1** Double-click Remote Access Services on the Desktop.
- 2** Double-click Remote Access.
- 3** Select the phone book entry you want to use, and then click Dial.
- 4** Enter your remote access username and password.

NOTE: Your remote user password might be different from your network login password. See your network supervisor for more information.

It is not required that you enter a domain.

- 5** Click OK.

Setting Up the Windows NT 4.0 Dial-Up Networking Dialer

- 1** Make sure the Windows NT 4.0 Dial-Up Networking dialer is installed and your modems are configured.

If you have not previously done this, refer to your Windows NT 4.0 documentation for installation and configuration instructions.

- 2** Make sure that you have set the correct protocols and bindings for IPX/SPXTM and TCP/IP.

See your network supervisor about these settings.

- 3** Double-click Dial-Up Networking.
- 4** Click New.

- 5** Enter the name and phone number.
- 6** Select the correct modem.
- 7** Uncheck Use Another Port if Busy.
- 8** Click the Server tab.
- 9** Uncheck NetBEUI.
- 10** Uncheck Enable PPP LCP Extensions.
- 11** Select the desired protocols (IPX, IP, or both).
NOTE: It might be necessary to set the TCP/IP settings. See your network supervisor for details.
- 12** Click OK to save.

This dial-up connection is now available from the phone book entry drop-down menu.

Dialing In to the Server Using the Windows NT 4.0 Dial-Up Networking Dialer

Windows NT 4.0 Dial-Up Networking dials in to the server and establishes a remote node connection.

- 1** Double-click Dial-Up Networking on your Desktop.
- 2** Select the desired connection from the phone book entry drop-down menu.
- 3** Click Dial.
- 4** Enter your remote access username and password.
NOTE: Your remote user password might be different from your network login password. See your network supervisor for more information.
It is not required that you enter a domain.
- 5** Click OK.

Macintosh Dial-In and Dial-Out Connections

Use the following procedures to optimize the following:

- ◆ Apple Remote Access Clients Dialing in to the Network
- ◆ Mac2NCS Dial-In and Dial-Out Connections

Apple Remote Access Clients Dialing in to the Network

This section describes how to use the Apple Remote Access from Apple Computer, Inc. and the Novell® Apple Remote Access Service to dial in to the network and establish a remote node connection. Apple Remote Access is the program that you run on the remote Macintosh to connect to the network. You must purchase this product from Apple Computer, Inc.

Before Connecting

Before you make a call using Apple Remote Access, complete the following steps.

- 1** Install the Apple Remote Access software.
- 2** (Conditional) If necessary, connect a modem to your Macintosh.
- 3** Indicate your modem setup in the Remote Access Setup control panel.
- 4** Verify that the remote users are authorized users on the network.
- 5** Specify the telephone number.

Establishing a Connection

To dial in to a Novell Internet Access Server 4.1 server (formerly known as the NetWare® Connect™ server) using the Apple Remote Access, complete the following steps.

- 1** Double-click the Apple Remote Access icon to open the program.

A new untitled connection window appears.

- 2** Enter your username on the server.

Make sure that you enter the full NDS™ (Novell Directory Services™) context for your username. For example, if your username is admin and your context is novell, enter **admin.novell**.

- 3** If you are prompted for a remote access password, enter your remote access password.

If you have Apple Remote Access 2.0 and the server is configured to allow the use of a password stored on disk, then you can use the Save My Password option to store your remote access password on disk so that you do not have to enter it each time that you connect.

If the server is configured to allow remote users to change their passwords, then you can change your remote access password. For more information, refer to Setting the Remote Access Password.

- 4** Enter the telephone number of the communications port.
- 5** (Conditional) If you want Apple Remote Access to remind you periodically of your connection, do the following:
 - 5a** Click Options.
 - 5b** Select one of the options in the Connection Reminder box.
 - 5c** If you select Display Alert Every, type a number between 1 and 9999 to tell Apple Remote Access how often, in minutes, to remind you of the connection.
 - 5d** Click OK.
- 6** Click Connect.

Apple Remote Access initializes the modem and starts dialing.

Once you establish a connection, the status window appears.

If the remote caller is configured for security dialback, then Apple Remote Access sets itself for autoanswer mode and waits for the communications server to call back.

Logging In to the Network

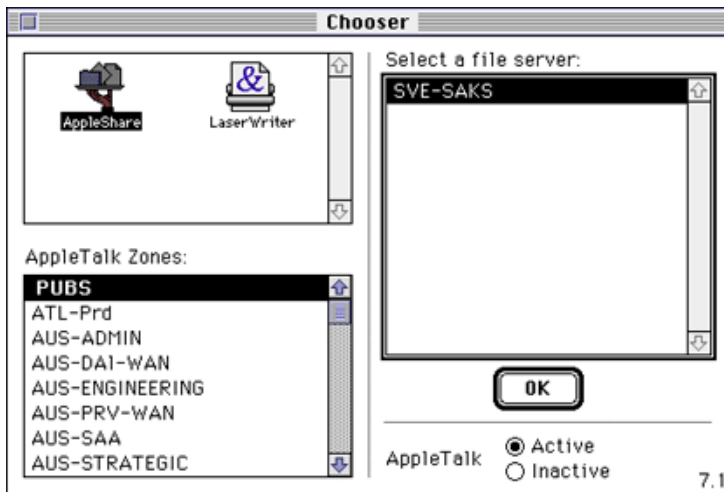
Once you have established a connection, you must log in to the network to use any of its resources.

- 1** Log in to a Novell Internet Access Server 4.1 server and do the following:
 - 1a** Open the Macintosh Control Panels folder and double-click the MacIPX icon.
 - 1b** Click the AppleTalk icon.

A list of possible AppleTalk zones and IPXTM gateways appears.
 - 1c** Select an IPX gateway that has a LAN connection to the server that you will access.
 - 1d** Exit MacIPX and close the Control Panels folder.
- 2** Select the AppleShare* icon in the Chooser window.

A list of available AppleTalk zones appears, as shown in Figure 10.

Figure 10 AppleTalk Zones and Remote Access Servers



- 3 Select the AppleTalk zone that your remote access server belongs to.
- 4 Select your remote access server and click OK.
- 5 Log in to the remote access server by specifying your username and password.

You are prompted to specify an access method.

- 6 Do one of the following:
 - ◆ If you are logging in to a server that has NDS (Novell Directory Services) installed, select Encrypted NetWare Authentication.
 - ◆ If you are not logging in to a server that has NDS installed, select Apple Standard UAMS.

You are now logged in to the server.

NOTE: Before disconnecting from your Apple Remote Access session, make sure that you log out of Novell Directory Services.

Setting the Remote Access Password

To provide additional security for the Novell Internet Access Server 4.1 server, the network supervisor can require users to enter another password for the server, in addition to the network password.

Novell recommends that the network supervisor initially configure a remote access password for you and instruct you on how to use that password.

Once you establish a connection, you can change the remote access password, if the server is configured to allow remote users to change the remote access password. You can change the remote access password in two ways:

- ◆ If you are using Apple Remote Access 2.0, you can use the Apple Remote Access program to change the remote access password.
- ◆ If you are using AppleTalk Remote Access 1.0, you can use the Set Remote Access Password utility provided with the Novell Internet Access Server 4.1 server.

If you are using a Macintosh computer that has a network connection to the server, you must have the MacIPX utility and its associated LAN drivers software installed. MacIPX and its LAN drivers can be installed during Mac2NCS installation. For instructions on installing Mac2NCS, see *Installing Mac2NCS*.

To run the Set Remote Access Password utility through a modem connection to a server, the following software must be installed on the remote Macintosh:

- ◆ MacIPX
- ◆ the MacIPX AppleTalk driver
- ◆ Novell Client for Macintosh (if you will connect to a Novell Internet Access Server 4.1 server)

To run the Set Remote Access Password utility, complete the following steps.

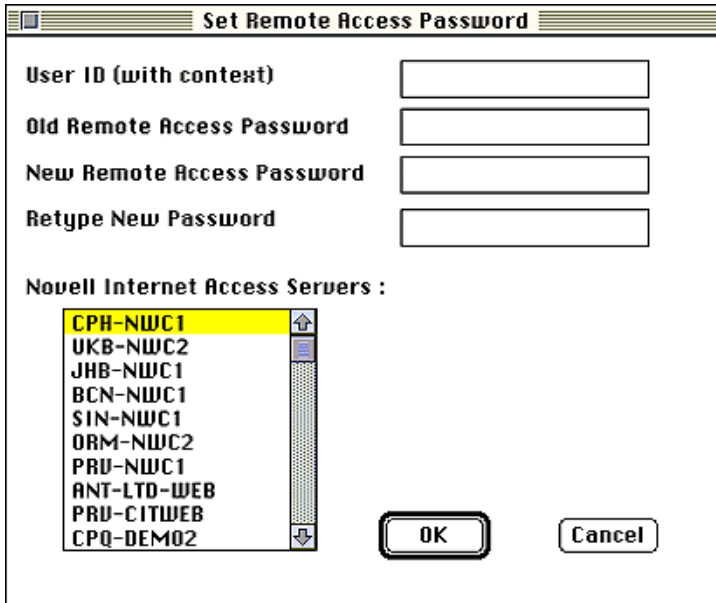
- 1** (Conditional) If you are running the Set Remote Password utility through a modem connection to a server, do the following:
 - 1a** Double-click the MacIPX icon in the Macintosh Control Panels folder.
 - 1b** Click the AppleTalk icon.

A list of AppleTalk zones and possible IPX gateways appears.
 - 1c** Select an IPX gateway that has a LAN connection to the server that you will access.
 - 1d** Exit MacIPX and close the Control Panels folder.
- 2** Open the folder where the Set Remote Access Password utility is installed.

3 Double-click the Set Remote Access Password icon.

The Set Remote Access Password window appears, as shown in Figure 11.

Figure 11 Set Remote Access Password Window



4 In the User ID field, type your username.

5 Enter your current remote access password in the Old Remote Access Password field.

6 Enter a new password in the New Remote Access Password field.

7 Retype the new password in the Retype New Password field.

8 Click OK.

The utility displays a message informing you that your remote access password has been changed.

You can now use the new remote access password to access the remote access software through Apple Remote Access.

Saving Memory after Connecting

To utilize memory to run other applications on the network, you can close the Apple Remote Access program but still remain connected.

From the File menu, select Quit to close Apple Remote Access. A dialog box appears reminding you of your connection. Click Stay Connected and Quit. Quitting the program has no effect on the connection.

To disconnect from the network, you need to reopen the program.

Disconnecting from the Network

Once you establish a connection, there are three ways to disconnect:

- ◆ From the Remote Access Windows menu, select Status and then click Disconnect.
- ◆ Quit the Apple Remote Access program while you are connected. When a dialog box appears to remind you of your connection, click Disconnect and Quit. This method frees up memory for your computer to use for other processing.
- ◆ Shut down your Macintosh while it is connected. The connection is automatically broken.

We recommend that you use the first method to disconnect from the network. Whatever method you choose, the following message is displayed:

The file server's connection has unexpectedly closed down.

This message does not necessarily mean that the communications server is having problems.

Mac2NCS Dial-In and Dial-Out Connections

This section describes how to use the Mac2NCS software and a third-party communications application to dial out from the network and access a bulletin board, host computer, or other resource—or to dial in and remotely control a dedicated LAN workstation. Mac2NCS is a redirector program that redirects the COM port I/O for Macintosh communications applications to a NASI port on a NetWare server.

Installing Mac2NCS

- 1 Locate the Remote Access Mac Client folder.

This folder might be on a diskette or a folder on a server.

- ♦ If the folder is on a server, open the Chooser, click AppleShare, and then locate a server that contains the NetWare Connect MAC Client folder. Log in to the server.
- ♦ If the folder is on a diskette, insert the diskette into a diskette drive on the Macintosh and then double-click the disk icon.

2 Double-click the Installer icon.

An informational screen appears. This screen contains basic instructions for installing Mac2NCS.

3 Click Continue.

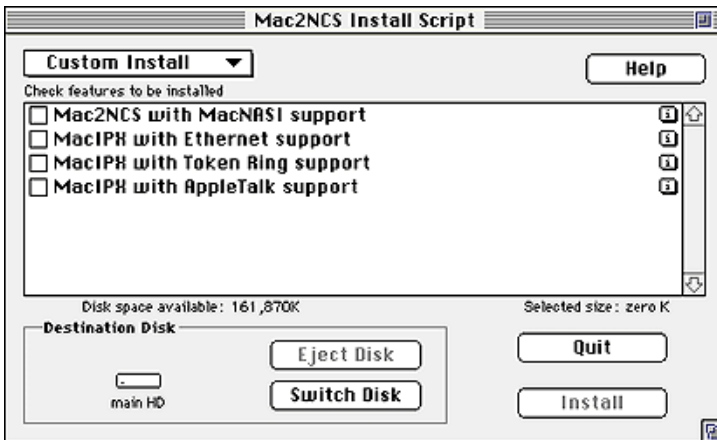
The Mac2NCS Install Script window appears.

4 Do one of the following:

- ♦ If you want to install all of the Mac2NCS options, click Install.
Mac2NCS installs automatically.
- ♦ If you need to install only some of the options listed on the Install Script window, pull down the Install menu at the upper-left corner of the window and click Custom Install.

The Custom Install options appear, as shown in Figure 12.

Figure 12 Mac2NCS Install Script Window



5 (Conditional) If you selected Custom Install, check Mac2NCS with MacNASI Support, check the other features that you want to install, and then click Install.

For example, if you have an Ethernet network, you need to install MacIPX[®] with Ethernet support (if it isn't already installed), but you do not need to install MacIPX with token-ring support.

6 Click Install.

7 Select Restart.

Installing IPXNetStat

Novell recommends that you also install the IPXNetStat diagnostic utility, if it is not already installed on the Macintosh.

To install IPXNetStat, complete the following steps.

1 Locate the Remote Access Services Mac Client folder.

This folder might be a diskette or a folder on a server.

- ♦ If the folder is on a server, open up the Chooser, click AppleShare, and then locate a server that contains the NetWare Connect MAC Client folder. Log in to the server.
- ♦ If the folder is on a diskette, insert the diskette into a diskette drive on the Macintosh and then double-click the diskette icon.

2 Open the NetWare Connect MAC Client folder.

3 Open the Mac2NCS folder.

4 Drag the IPXNetStat icon from the Mac2NCS folder to the System folder of your boot drive.

The IPXNetStat icon appears in the Apple Menu.

Configuring Mac2NCS

After you have installed Mac2NCS and restarted the Macintosh, you can configure Mac2NCS.

HINT: If you need additional help configuring Mac2NCS, you can activate the Apple balloon help system by clicking the balloon icon in the upper-right corner of your screen.

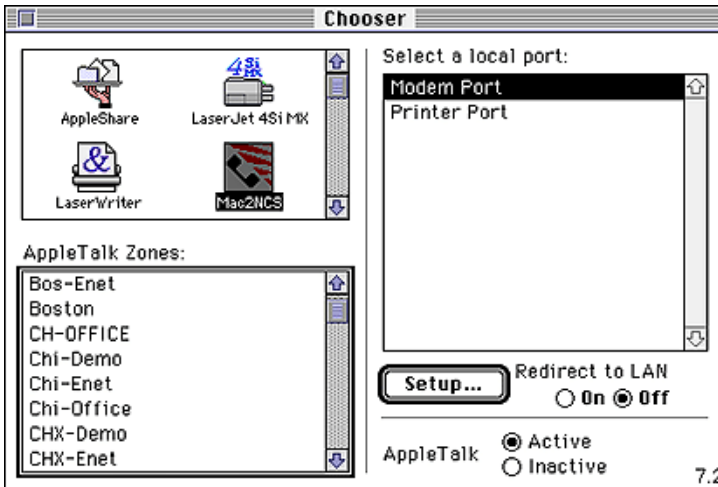
To configure Mac2NCS, complete the following steps.

1 From the Apple menu, select the Chooser.

2 Find and click the Mac2NCS icon.

The Chooser window appears, as shown in Figure 13.

Figure 13 Mac2NCS Chooser Window



The modem and printer ports are displayed in the right portion of the window.

3 Select the local port that will be used for redirection (Modem Port or Printer Port).

If the application that you will use is enabled for the Communications Tool Box, Steps 3 and 4 are not necessary. Proceed to Step 5. If you are unsure that the application that you will use is enabled for the Communications Tool Box, proceed with Steps 3 and 4.

Once a port is chosen for redirection, the port is not available to a physical device such as a printer or modem. Applications that are enabled for the Communications Tool Box allow you retain the physical port while using a virtual serial device for Mac2NCS.

4 Click On to enable redirection.

5 Click Setup.

The Login Information window appears, as shown in Figure 14.

Figure 14 Login Information Window

The Server(s) to Select window shows the available servers. The Last Port Chosen field shows the server name, general name, and specific name for the last NASI port that was chosen.

6 Specify server login information as indicated in Table 11.

Table 11 Remote Access Login Information

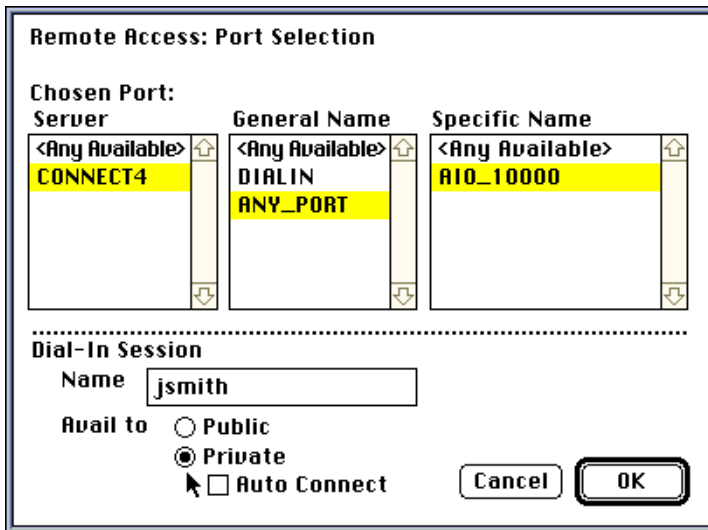
Option	Description
Server(s) to Select	<p>Select list to select the server that you want Mac2NCS to search for NASI ports.</p> <p>If you do not select any servers, then all available servers will be searched for NASI ports. This might take quite some time if you have access to several servers.</p> <p>Your selection of servers limits the servers whose ports you can access. Mac2NCS will locate ports only on servers that you have selected and can access using the user ID, context, and password that you use to log in.</p>
User ID	In the User ID field, enter your NetWare user ID on the server where you want to use a port.
Context	If you are accessing a Novell® Internet Access Server 4.1 server, enter your NDS context for the server.

Option	Description
Password	Enter your server password for the user ID you specified in the User ID field.

7 Click Continue.

The Remote Access Port Selection window appears, as shown in Figure 15.

Figure 15 Remote Access Port Selection Window



8 Specify port selection information as indicated in Table 12.

You can select from one or more lists in any order. A General Name of <Any Available> is not recommended. If you intend to dial out but your call is routed to a port in a DIALIN group, then you will be unable to dial out. A selection other than <Any Available> from the Server or Group list might limit the choice of port. If the specific port you have selected is not available, you might be unable to use Mac2NCS temporarily.

Table 12 Mac2NCS Port Selection Fields

Option	Description
Server	<p>Select the server on which to locate ports for redirection. If you want to search all available servers, select <Any Available>.</p> <p>The list of servers that appears is limited by the servers that you selected when you logged in using the Login Information window.</p>
General Name	<p>Select the Remote Access General Port name.</p> <p>If you will use the port to dial out, make sure that the port you select is <i>not</i> in the DIALIN group or the <Any Available> group.</p> <p>If you will use the port to allow a remote caller to dial in, the port can be either dial-in or dial-out. In this case, you might want to select the DIALIN General Name.</p>
Specific Name	<p>Select the specific port name of the port to use for redirection. If you want to use any port on the server or in the port group, select <Any Available>. If you will use the port to allow a remote caller to dial in, make sure that you select a port whose name ends in DIALIN.</p>
Dial-in Session Name	<p>If you will use Mac2NCS to place the Macintosh in host mode and wait for a call from a remote site, specify the username to be used to establish a session.</p>
Avail To	<p>If you want a dial-in session to be available to the specified user only, click the Private button. If you want the session to be available to all users, click the Public button.</p>
Auto Connect	<p>If you clicked the Private button and want the remote user to connect automatically without being presented with a menu of available sessions, check the Auto Connect check box.</p>

9 When you have finished making your selections, click OK to exit the Port Selection window.

10 Click OK to exit the Login Information window.

Configuring Mac2NCS to Allow Remote Users to Dial In to the Network

When you configure Mac2NCS to allow remote users to dial in to the network, you have the following two options:

- ◆ You can configure Mac2NCS so that remote users are presented with a list of sessions to choose from.
- ◆ You can configure Mac2NCS so that remote users access only one particular Macintosh session on the network.

Configuring Mac2NCS to Allow Remote Users to Select a Session

To configure Mac2NCS to allow dial-in users to select a session, complete the following steps:

- 1** Install Mac2NCS on a network workstation.

See *Installing Mac2NCS*.

- 2** (Conditional) If the application that you will use is not enabled for the Communications Tool Box, configure Mac2NCS to redirect printer or modem port I/O to a port that belongs to the NCS DIALIN group.

- 3** See *Configuring Mac2NCS*.

- 4** In the Dial-in Session options on the NetWare Connect Port Selection window, configure the following fields.

- 4a** In the Name field, enter a session name.

This can be any text that you want. The text that you enter will be used to identify the session name to remote users.

- 4b** Select one of the following Avail To options:

- ◆ If you want the session to be available to all users, click the Public button.
- ◆ If you want the session to be available only to private users (users who specify the same login information as was entered on the Login Information window), click the Private button.
- ◆ If you want the session to be available to private users, and you do not want the server to prompt the users to select a session, check the Auto Connect box.

- 5** Set the communications software on the local Macintosh to host mode or call-waiting mode.

Make sure that you configure the software to use a direct connection and do not configure it to wait for a modem to answer a call.

- 6** Make sure that the remote component of the Macintosh communications package is installed.

When you configure Mac2NCS in this manner, remote users will be presented with a menu of sessions when they access the LAN. They can then select a session on a particular Macintosh.

Configuring Mac2NCS to Allow Remote Users to Select Only One Port

You can also configure Mac2NCS to allow remote users to access only one particular Macintosh.

IMPORTANT: This configuration is not recommended because it consumes more resources, requires more knowledge of the server and modem setup, and might have a higher potential security risk. See your network supervisor before using this configuration.

To configure Mac2NCS to allow dial-in users access to only one Macintosh, complete the following steps.

- 1** Install Mac2NCS on a LAN workstation.
See *Installing Mac2NCS*.
- 2** (Conditional) If the application that you will use is not enabled for the Communications Tool Box, configure Mac2NCS to redirect Printer or Modem port I/O to a port that is configured for either dial-out or both dial-in and dial-out.
- 3** See *Configuring Mac2NCS*.
- 4** Make sure that the port that users will use has a dedicated phone number associated with it.
- 5** Set the communications software on the local Macintosh to host mode or to wait for a call to a modem.

In order to do this, your host Macintosh software must know what type of modem will be used to answer the call.
- 6** Make sure that the remote component of the Macintosh communications package is installed.
- 7** Provide remote users with the phone number for the port that will be directly connected to the host Macintosh.

When you configure Mac2NCS in this manner, remote users will interact directly with the host computer.

Using Mac2NCS

You can use Mac2NCS to dial out from the network or to allow a remote user to dial in to your Macintosh while it is in host mode.

Using Mac2NCS to Dial Out from the Network

To use Mac2NCS to dial out, start a supported Macintosh communications application and dial out.

For example, use the Apple Internet Connection Kit to dial out to an ISP or use an America Online* client application to dial out to America On-Line services. You could also use Microphone II to dial out to another PC or Macintosh with a similar communications program. Refer to your application documentation for detailed information.

HINT: See the Mac2NCS README file for more specific information and troubleshooting tips.

Using Mac2NCS with Applications that Enable the Communications Tool Box

If you are using Mac2NCS with an application that enables the Macintosh Communications Tool Box, make sure that the Redirect to LAN option on the Mac2NCS Chooser Window is set to Off.

With this type of application, Mac2NCS can appear as a directly accessible serial port. By not redirecting the printer and modem ports, you can leave them free for other uses.

Using IPXNetStat to Troubleshoot

You can use the IPXNetStat program provided with Mac2NCS to troubleshoot problems with Mac2NCS.

To use IPXNetStat, complete the following steps.

- 1** Open the folder where IPXNetStat is installed.

If IPXNetStat was installed as an Apple menu item, go to the Apple menu and select IPXNetStat.

- 2** Double-click the IPXNetStat icon.

The IPXNetStat window appears.

3 Do one of the following:

- ◆ If you are querying NetWare Connect 1.0 servers, enter **394** in the Query Type field.
- ◆ If you are querying NetWare Connect 2.0 servers, enter **591** in the Query Type field.

4 Check the Query Type check box and then click Update.

IPXNetStat displays a report indicating how many servers your Macintosh can detect.

5 If no servers are available, click Update.

If you still do not see any servers in the list, check to make sure that MacIPX is configured correctly on your Macintosh. To do this, go to the Control Panels and click the MacIPX icon. Double-click the highlighted network interface selection and make sure that the correct frame type is selected. Also, check your physical connection to the LAN.

If none of these suggestions works, then contact your network supervisor.

NetWare Link/X.25 Configurations

In most cases, the information provided in *Installing and Configuring X.25 Adapters* is sufficient to install X.25 support for the Novell Internet Access Server 4.1 file server. The additional information provided here can be used to customize your NetWare Link/X.25 configuration.

Refer to the following sections:

- ◆ Network Interface Configuration Parameters

This section provides information on the following topics:

- ◆ How to configure the network interface parameters
- ◆ How to view a network interface parameter

- ◆ WAN Call Directory Configuration Parameters

This section describes the parameters you need to set for WAN Call handling information.

Network Interface Configuration Parameters

This section summarizes the fields on the NIASCFG X.25 Network Interface menu.

To display the X.25 Network Interface menu, from the Novell Internet Access Server Configuration menu, select Network Interface.

The NIASCFG X.25 Network Interface menu appears.

The parameters enable you to configure NetWare Link/X.25 for the selected interface. Table 13 describes the X.25 Network Interface parameters.

Table 13 X.25 Network Interface Parameters

Parameter	Description	Default Value
Interface Name	Specifies the name of the interface assigned to the currently selected port. This field is read-only.	No default
Interface Group	Allows protocols such as the IP or Interent Packet Exchange™ (IPX™) protocol to request an X.25 virtual circuit be made either through a specific interface or by way of one interface from within a group of interfaces. Specifying a group name here includes this interface in a group. Press F3 or Enter to display a list of currently defined groups and to define a new group.	No default
Interface Status	Specifies the load status of the current board. You can configure the current board to load each time the server or router PC is initialized. The value can be Enabled or Disabled.	Enabled
Profile	Press Enter to display a menu that lists Novell-standard profiles for major public data networks (PDNs). Then select the standard profile for your X.25 service provider. Press Enter or Insert to view or modify the X.25 profile parameters. Refer to Viewing and Configuring Profile Parameters for more information. All standard profiles are read-only. However, you can make a copy of one of the standard profiles by pressing F2 , then you can make changes to the copy.	No default

Parameter	Description	Default Value
Local DTE Address	Specifies the X.121 DTE address (up to 15 digits) assigned to the local DTE. This should match the address assigned by your attached network. This address is included in the Calling Address field of outbound Call Request packets.	No default
Statistics Period	Specifies the rate, in 1-second increments, at which the board is polled by the driver to acquire port statistics. Range: 20 to 1024	60
User Data Size	Specifies the maximum size, in bytes, of the user data you expect to transmit and receive on this interface. Range: 500 to 4096 bytes.	1500 bytes
Interface Queue Limit	Specifies the maximum number of data packets that can be queued to each port on the board. Range: 0 to 1024 (0 = unlimited packets)	100 packets
Physical Type	Specifies the port's electrical interface standard (for example, RS-232 or V.35). Press Enter to display a list of the available interface types. This parameter must equal the actual port type installed (for example, if the board type is RS-232, setting this parameter to V.35 is invalid). The value can be RS-232, RS-422, RS-423, V.35, or X.21.	RS-232
Port Connection	Specifies the physical connection between the local DTE and the remote end. The value can be DTR Dialed, Hard-wired, or Pseudo-Switched.	Hard-wired
Interface Speed	Specifies the line speed, in bits per second, of the port. The internal board rates vary, depending on the driver. The possible values are 1200, 2400, 4800, 7200, 9600, 12000, 14400, 16000, 19200, 38400, 48000, 56000, 64000, and External.	External

Parameter	Description	Default Value
Authentication Options	<p>Presents a menu that covers the definition of the incoming call verification parameters. X.25 can be configured to accept incoming calls from a list of predefined partners, which are identified by their X.25 DTE addresses.</p> <p>Authentication Options Parameters explains the parameters that can be configured for NetWare Link/X.25 inbound authentication for this interface.</p>	No default

Viewing and Configuring Profile Parameters

When you press **Insert** when the cursor is on the **Profile** parameter on the X.25 Network Interface menu, a list of profiles is displayed. The list includes the names and Novell-standard profiles of major PDNs. All the standard profiles are read-only.

If you select a profile and press **Insert** or **F3**, the X.25 Profile Configuration window appears. This window allows you to change the profile parameters and save the changed profile under a new name.

The X.25 Profile Configuration window displays the following fields.

Profile

Specifies the name of the currently selected profile. This parameter is read-only.

Profile Type

This parameter is purely informational and has no effect on NetWare Link/X.25 operation.

Options: Enterprise, Local

Default: Local

Frame Level Parameters

Pressing **Enter** when the cursor is in the **Frame Level Parameters** field displays the X.25 Frame Level Parameters window. This window is used to define the working characteristics of the link (LAPB) between the remote access software and the DCE (typically the X.25 network).

Changing the parameters from the defaults is optional. The default configuration should be adequate for most configurations.

Table 14 describes the Frame Level parameters.

Table 14 **Frame Level Parameters**

Parameter	Explanation	Default
Profile	Specifies the name of the currently selected profile. This field is read-only.	No default
Frame Node Type	<p>Specifies which address, A or B, you allocate to the local DTE, depending on your communications configuration.</p> <p>Do not use this option with the Connection Mode parameter set to <i>Passive</i>.</p> <p>The possible options are DCE (LAPB DCE address used); DCE-A (automatically determines which LAPB address to use, beginning with DCE); DTE (LAPB DTE address used); and DTE-A (automatically determines which LAPB address to use, beginning with DTE).</p>	DTE-A
Connection Mode	<p>Specifies whether NetWare Link/X.25 waits for the calling partner to set up the actual link. Active mode continually attempts to set up the link. Passive mode waits for a partner to set up the link.</p> <p>Generally, Passive mode is not used unless you are communicating with an X.25 implementation that does not tolerate partner setup.</p>	Active
Frame Sequencing Modulo	<p>Specifies the Link layer sequence numbering that is used. The possible values are 8 (Modulo 8) and 128 (Modulo 128). All networks support Modulo 8 for normal sequence numbering, whereas some networks also support Modulo 128 for extended sequence numbering. This allows users to select a larger window size.</p> <p>For most networks, select Modulo 8. The Frame Window Size parameter is dependent on which Modulo method you select.</p>	8
Frame Window Size (K)	<p>Specifies the maximum number of information frames that can be received or sent before the server or router PC sends (or waits for) an acknowledgment.</p> <p>Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)</p>	7

Parameter	Explanation	Default
Maximum Frame Size (N1)	<p>Specifies the maximum frame size, in octets, that can be received on the link.</p> <p>Frames received on the link in excess of this number cause the link to be reset by sending a Frame Rejected (FRMR) frame. Unnecessarily specifying a large number reduces the amount of memory available for normal data operations. N1 should be greater than the specified packet size (both default and maximum).</p> <p>Range: 160 to 4103 (for 1980 X.25 version); 261 to 4103 (for 1984 or 1988 X.25 version)</p>	261
Retry Count (N2)	<p>Specifies the maximum number of times a frame is retransmitted after the Retry Timer (T1) expires. A large value for this parameter increases the probability of a correct transfer between the DTE and DCE. A smaller value permits faster detection of a permanent error condition.</p> <p>Range: 1 to 255</p>	10
Retry Timeout (T1)	<p>Specifies the time, in seconds, to wait for an acknowledgment of the oldest transmitted frame. If an acknowledgment is not received within this set time, an attempt is made to determine the status of the remote device.</p> <p>Set this parameter to a value slightly greater than twice the transmission time of the longest frame, including the anticipated delay time to the peer node.</p> <p>Range: 1 to 3200</p>	2
Disconnect Timeout (T3)	<p>Specifies the value, in seconds, of the T3 timer. When the T3 timer value expires, the Data-Link layer passes an indication of an observed, excessively long idle channel state condition to the Packet layer. The T3 timer value must be greater than T1 to ensure that the data-link channel is in a nonactive, nonoperational state, and that the data-link channel needs data-link setup, before a normal data-link operation can resume.</p> <p>Range: 0 to 3200 (0 = disabled)</p>	20

Parameter	Explanation	Default
Idle Timeout (T4)	Specifies the amount of time, in seconds, the local DTE waits when a link becomes idle before attempting to poll the partner node for status. If the partner node does not respond to the polls, the link is reset and all current virtual calls are cleared or reset. Range: 0 to 180 (0 = disabled)	10

Packet Level Parameters

Selecting **Packet Level Parameters** from the X.25 Profile Configuration window displays a submenu that accesses all the Packet Level parameters for the interface. Table 15 describes the Packet Level parameters.

Table 15 Packet Level Parameters

Parameter	Description	Default
Profile	Specifies the name of the currently selected profile. This field is read-only.	No default
X.25 Version	Specifies the specific conformance year for the X.25 specification you are using for this port. The value can be 1980, 1980-Min, 1984, or 1988.	1984
Packet Layer Role	Specifies whether DTE or DCE procedures are used for Packet layer operation. When establishing a connection to an X.25 network, you must set this parameter to DTE (the default value) to avoid call collisions. The value can be DTE or DCE.	DTE
Default Inbound Packet Size	Specifies the default packet size that is used for a call. Unless another packet size is specified when the call is made, the default value is used. Set this value to correspond to your network subscription. The value can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.	128

Parameter	Description	Default
Default Outbound Packet Size	<p>Specifies the maximum outgoing data packet size used when a call is established without the Flow Control Negotiation parameter. The Default Outbound Packet Size parameter should be a value that is agreed upon by the PDN and the remote DTE.</p> <p>The value can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.</p>	128
Packet Sequencing Modulo	<p>Specifies the control over the numbering of sequential data packets allowed in a window. For most networks, Modulo 8 should be used. For special high-propagation delay situations (for example, a satellite), you can use Modulo 128, if allowed by your network, to permit larger window sizes.</p> <p>The Default Window Size parameter is dependent on the Modulo method you select.</p> <p>Options: 8 or 128</p>	8
Default Inbound Window Size	<p>Specifies the default number of sequential incoming data packets that can be received before an acknowledgment is required.</p> <p>The Packet Sequencing Modulo and Window Size parameters are independent of the Frame Sequencing Modulo and Window Size parameters.</p> <p>Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)</p>	2
Default Outbound Window Size	<p>Specifies the default value of the maximum number of sequentially numbered data packets that the local DTE might not acknowledge at any given time.</p> <p>When a virtual circuit is established without flow control negotiation, this value is used as an outbound window size. You should set this parameter to the value that is agreed upon with the PDN.</p> <p>Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)</p>	2

Parameter	Description	Default
Default Inbound Throughput Class	<p>Specifies the default setting, in bits per second, for the incoming throughput of each virtual circuit. Set this value to correspond to your network subscription.</p> <p>Options: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 48000, 64000</p>	1200
Default Outbound Throughput Class	<p>Specifies the default outbound throughput class that is used when a call is established without throughput class negotiation.</p> <p>Options: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 48000, 64000</p>	1200
Restart Response Timer (T20)	<p>Specifies the amount of time, in seconds, that the local DTE waits when it issues a Restart Request packet to receive a restart confirmation.</p> <p>When the time limit expires, the Restart Request packet is retransmitted.</p> <p>Range: 1 to 3200</p>	180
Call Response Timer (T21)	<p>Specifies the amount of time, in seconds, that the DTE waits for a response to an outbound Call Request packet.</p> <p>Range: 0 to 3200 (0 = disabled)</p>	200
Reset Response Timer (T22)	<p>Specifies the amount of time, in seconds, that the DTE waits for a response to a Reset Request packet.</p> <p>Range: 1 to 3200</p>	180
Clear Response Timer (T23)	<p>Specifies the amount of time, in seconds, that the DTE waits for a response to a Clear Request packet.</p> <p>Range: 1 to 3200</p>	180
Ack-Send Timer (T24)	<p>Specifies the amount of time, in seconds, that a DTE waits when a packet carrying a valid acknowledgment is sent.</p> <p>This timer is used to ensure that any acknowledgments are not lost. If the timer expires, an RR (Receiver Ready) packet is sent.</p> <p>Range: 0 to 3200</p>	0 (timer not active)

Parameter	Description	Default
Data Retransmission Timer (T25)	<p>Specifies the amount of time, in seconds, that the DTE waits for the appropriate acknowledgment after transmitting a data packet.</p> <p>If the T25 timer expires, the Packet layer resets the virtual circuit.</p> <p>Range: 0 to 3200</p>	30 (timer not active)
Interrupt Response Timer (T26)	<p>Specifies the amount of time, in seconds, that the DTE waits for an interrupt confirmation when an Interrupt Request packet is sent.</p> <p>If the timer expires, the Packet layer resets the virtual circuit.</p> <p>Range: 0 to 3200</p>	0 (timer not active)
Restart Retransmission Count (R20)	<p>Specifies the maximum number of times the local DTE retransmits when the T20 timer expires before notifying the user that the associated link is inoperative.</p> <p>Range: 0 to 50</p>	5
Reset Retransmission Count (R22)	<p>Specifies the maximum number of times the local DTE retransmits a Reset Request packet after the T22 timer expires before initiating a clear procedure for an SVC or a restart procedure for a PVC.</p> <p>Range: from 0 to 50</p>	5
Clear Retransmission Count (R23)	<p>Specifies the maximum number of times the local DTE retransmits a Clear Request packet after the T23 timer expires before initiating a Restart procedure on the associated link.</p> <p>Range: 0 to 50</p>	5

Virtual Circuit Setup

When you select Virtual Circuit Setup from the X.25 Profile Configuration window, the X.25 Virtual Circuit window appears. The Virtual Circuit Setup parameters allow you to configure PVC and SVC Logical Channel Numbers (LCNs). Table 16 describes the available parameters.

Table 16 Virtual Circuit Setup Parameters

Parameter	Description	Default
Profile	Specifies the name of the currently selected profile. This field is read-only.	No default
Lowest PVC LCN	Specifies the lowest LCN that can be used for a PVC. Range: 0 to 255 (0 is for Transpac only)	1
Number of PVC LCNs	Specifies the number of logical channels supporting PVCs. This number must agree with your network subscription. Range: 0 to 256	0
Expert PVC Configuration	Press Enter to display a list of the PVCs that have been defined and can be configured for the associated interface. Select a PVC and press Enter again. Use the resulting window to configure a single PVC. Refer to Expert PVC Configuration Parameters for information on the Expert PVC Configuration parameters.	No default
Lowest Inbound-Only SVC LCN	Specifies the lowest LCN that can be used for one-way incoming logical channels for SVCs. This value must be greater than or equal to the Lowest PVC LCN parameter value. Range: 1 to 4095	1
Number of Inbound-Only LCNs	Specifies the number of incoming channels assigned for inbound-only SVCs. This number must agree with your network subscription. Range: 0 to 255	0
Lowest Two-Way SVC LCN	Specifies the lowest number of two-way channels assigned for SVCs that can be used for both inbound and outbound calls. Range: 1 to 4095	1
Number of Two-Way SVC LCNs	Specifies the lowest LCN that can be used for two-way SVCs. This number must agree with your network subscription. Range: 0 to 255	8

Parameter	Description	Default
Lowest Outbound-Only SVC LCN	<p>Specifies the lowest LCN that can be used for outgoing SVC logical channels.</p> <p>The value must be greater than or equal to the <i>Lowest Two-Way SVC LCN</i> parameter value plus the <i>Number of Two-Way LCNs</i> parameter value.</p> <p>Range: 1 to 4095</p>	9
Number of Outbound-Only SVC LCNs	<p>Specifies the number of logical channels reserved for outbound-only SVCs.</p> <p>This number must agree with your network subscription.</p> <p>Range: 0 to 255</p>	0

User Facility Setup

When you select User Facility Setup from the X.25 Profile Configuration window, the X.25 User Facility Setup window appears. This window allows you to specify user facility setup parameters. You can change or specify flow control and throughput negotiation settings, maximum inbound and outbound packet and window sizes, use of CUGs, fast select, and reverse charging.

Table 17 describes the User Facility Setup parameters.

Table 17 User Facility Setup Parameters

Parameter	Description	Default
Profile	Specifies the name of the currently selected profile. This field is read-only.	

Parameter	Description	Default
Allow Flow Control Negotiation	<p>Specifies whether to allow negotiation, per call, of the data throughput that can be transferred on a virtual circuit.</p> <p>If set to <i>Yes</i> , allows incoming calls and outgoing calls containing either the <i>Window Size</i> facility or the <i>Packet Size</i> facility to be passed to the destination application for disposition. Flow Control Negotiation is also allowed when the parameter is set to <i>Yes</i>.</p> <p>If the destination application accepts the call, NetWare Link/X.25 either accepts the <i>Window Size</i> or <i>Packet Size</i> facilities as requested, or adjusts them to the highest value allowed (less than or equal to the maximum values specified in the <i>User Facility Setup</i> menu).</p> <p>If set to <i>No</i> , an incoming call or outgoing call is cleared if the specified window size or packet size is greater than the specified maximum window size or maximum packet size, respectively.</p> <p>Options: Yes, No</p>	No
Maximum Inbound Packet Size	<p>Specifies the largest incoming packet size that can be negotiated on a per-virtual circuit basis.</p> <p>Options: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096</p>	128
Maximum Outbound Packet Size	<p>Specifies the largest outgoing packet size that can be negotiated on a per-virtual circuit basis.</p> <p>Options: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096</p>	128
Maximum Inbound Window Size	<p>Specifies the largest value, per virtual circuit, that can be negotiated for the inbound window size.</p> <p>The maximum value for this parameter depends on the <i>Packet Sequencing Modulo</i> method you selected. Refer to <i>Packet Level Parameters</i> for more information.</p> <p>Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)</p>	2

Parameter	Description	Default
Maximum Outbound Window Size	<p>Specifies the largest value, per virtual circuit, that can be negotiated for the outbound window size.</p> <p>The maximum value for this parameter depends on the Packet Sequencing Modulo method you selected. Refer to Packet Level Parameters for more information.</p> <p>Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)</p>	2
Allow Throughput Negotiation	<p>Specifies whether to allow negotiation, per call, of the data throughput that can be transferred on a virtual circuit.</p> <p>If set to <i>Yes</i>, incoming calls containing the Throughput facility are passed to the destination application.</p> <p>If the destination application accepts the call, the Throughput Class Negotiation value is set to the highest value (less than or equal to) or the maximum specified in the Packet Layer Parameters window.</p> <p>If set to <i>No</i>, an incoming call containing a Throughput Class Negotiation value that does not match the default is cleared.</p> <p>Options: Yes, No</p>	No
Maximum Inbound Throughput Class	<p>Specifies the maximum Throughput Class Negotiation value, in bits per second, that can be negotiated per virtual circuit.</p> <p>Options: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 48000, 64000</p>	9600
Maximum Outbound Throughput Class	<p>Specifies the maximum Throughput Class Negotiation value, in bits per second, that can be negotiated per virtual circuit.</p> <p>Options: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 48000, 64000</p>	9600
Allow Incoming Reverse Charge Calls	<p>Specifies whether incoming calls containing the Reverse Charging facility are passed to the destination application.</p> <p>If set to <i>Yes</i>, the call is passed to the destination application for disposition. If set to <i>No</i>, the call is cleared.</p> <p>Options: Yes, No</p>	Yes

Parameter	Description	Default
Allow Closed User Group	<p>Specifies whether CUGs are allowed for the DTE and, if so, what kind of access the CUGs will have.</p> <p>CUGs allow the DTEs to belong to a group so they can communicate with each other. However, CUGs preclude communication with all other DTEs. If a DTE belongs to more than one CUG, you must specify a preferential CUG.</p> <p>Options: Yes, No</p>	No
Allow Bilateral CUG	<p>Specifies whether to allow pairs of DTEs to form bilateral communication. This allows access between the bilateral DTEs and excludes access to (or from) other DTEs.</p> <p>Options: Yes, No</p>	No
D-Bit Procedure Authorized	<p>Specifies whether Delivery Confirmation (D-bit) procedures are allowed for any virtual call through this port. If set to <i>Yes</i>, incoming calls specifying D-bit procedures are allowed. If set to <i>No</i>, these calls are cleared.</p> <p>Options: Yes, No</p>	No
Fast Select	<p>Specifies whether Fast Select can be used for any call on this port.</p> <p>If set to <i>Yes</i>, Fast Select calls can be used. If set to <i>No</i>, incoming calls containing the Fast Select facility are cleared.</p> <p>Options: Yes, No</p>	Yes

Conformance Options

Pressing **Enter** from the X.25 Profile Configuration window displays the X.25 Conformance Options window. This window allows you to customize NetWare Link/X.25 for use on PDN implementations.

IMPORTANT: The Novell-provided profiles for the various PDNs have these options set for proper operation on your network. Consult your network representative or technical support before you modify these parameters.

Table 18 describes the Conformance Options parameters.

Table 18 Conformance Options Parameters

Parameter	Description	Default
Profile	Specifies the name of the currently selected profile. This field is read-only.	No default
Unknown Frame Option	Specifies whether to acknowledge an unknown frame. If set to <i>Yes</i> , command frames with the Poll/Final (p/f) bit set to <i>Off</i> are ignored. If set to <i>No</i> , unknown frames are not acknowledged. Options: <i>Yes</i> , <i>No</i>	No
Disconnect Answer Option	Specifies the response to Disconnect (DISC) frames in either link setup states or link disconnect states. If set to <i>Yes</i> , an Unsequenced Acknowledgment (UA) response is sent. If set to <i>No</i> , a Disconnect Mode (DM) response is sent. Options: <i>Yes</i> , <i>No</i>	No
Disconnect Action Option	Specifies the action when a Disconnect (DISC) frame is received in an SABM Sent or OFF state. If set to <i>Yes</i> , the SABM is sent immediately. If set to <i>No</i> , the link is disconnected. Options: <i>Yes</i> , <i>No</i>	No
Force FRMR Option	Specifies that any received frame is answered with an FRMR frame while in FRMR Sent state or when the link is reset. Options: <i>Yes</i> , <i>No</i>	No
Force FRMR on RR Option	Specifies an FRMR response to RR frames if in FRMR Sent state. If set to <i>Yes</i> , an FRMR response is sent. If set to <i>No</i> , it is ignored. Options: <i>Yes</i> , <i>No</i>	No
T1 Action Option	Specifies the point at which the retransmission counter is reinitialized when in T1 Sent state. If set to <i>Yes</i> , it reinitializes when any information frame (I frame) is acknowledged. If set to <i>No</i> , it is ignored. Options: <i>Yes</i> , <i>No</i>	No

Parameter	Description	Default
Call Accept Data	<p>Specifies the use of Call User Data in a positive response to an incoming call.</p> <p>If set to <i>Yes</i>, the user data accepted allows various byte lengths of data (up to 128 bytes of user data) to be sent in the Call Request packet, depending on the protocol involved and whether <i>Fast Select</i> is selected in the Call Request packet.</p> <p>Options: <i>Yes</i>, <i>No</i></p>	No
D-Bit on Call Confirm	<p>Specifies whether the D-bit in a Call Confirm packet is set.</p> <p>Options: <i>Yes</i>, <i>No</i></p>	No
General Diagnostic Code	<p>Determines whether the original diagnostic code is retransmitted when the T20 timer expires (<i>Yes</i>), or whether the T20 timer expired diagnostic code is included in the Restart packet (<i>No</i>).</p> <p>Options: <i>Yes</i>, <i>No</i></p>	No
Clear Unassigned LCN	<p>Specifies that incoming packets appearing with an unassigned LCN will generate a Clear response.</p> <p>Setting this option to <i>Yes</i> is not recommended unless your attached network requires it. This option generates a Clear response for incoming calls containing unconfigured LCNs.</p> <p>If set to <i>No</i>, such incoming calls are ignored.</p> <p>Options: <i>Yes</i>, <i>No</i></p>	No
Short Call Confirm	<p>Specifies whether a 3-byte Call Accept packet (<i>Yes</i>) or 5-byte Call Accept packet (<i>No</i>) is transmitted when a facility is not included in the Call Accept packet.</p> <p>Options: <i>Yes</i>, <i>No</i></p>	No
Facility Field	<p>Specifies whether Clear packets and Call Accept packets with full facility and user data fields are allowed.</p> <p>Options: <i>Yes</i>, <i>No</i></p>	No

Parameter	Description	Default
Clear Long Call	<p>Specifies whether user data is cleared for the pre-1984 version of X.25.</p> <p>If set to Yes , enables the Clear User Data field option in the Clear Request packet for the pre-1984 version of X.25.</p> <p>Options: Yes, No</p>	No
Force Defaults on Negotiation	<p>Specifies whether the port defaults always are selected as a negotiation response for an incoming call. Usually, this option is not set unless required by your attached network.</p> <p>If set to Yes , any negotiable facility value contained in an accepted incoming call is forced to the port's default values (rather than using the maximum, or less than or equal to port maximum).</p> <p>Options: Yes, No</p>	No

Frame Node Type

Displays the link type you use. This parameter is read-only.

Packet Size (In/Out)

Displays the current default packet sizes. The **In** packet size corresponds to the packets transmitted to a network. The **Out** packet size corresponds to the packets received from this network. This field is read-only.

Frame Window Size

Displays the current settings for the Frame level window. Defines the number of information frames (I frames) that are transmitted or received before an acknowledgment is required. This field is read-only.

Packet Window Size (In/Out)

Displays the current settings of the Packet level window size. The window size specifies how many data packets are transmitted or received before an acknowledgment is required. This field is read-only.

Number of VCs (PVC/In/Two-Way/Out)

Displays the number of PVCs and SVCs currently configured. The SVCs are further divided into outgoing, two-way, and incoming (the network can allocate to the incoming call only). This field is read-only.

Expert PVC Configuration Parameters

When you select Expert PVC Configuration from the X.25 Virtual Circuit Setup window, a window appears that allows you to configure Expert PVC parameters.

Table 19 describes the Expert PVC Configuration parameters.

Table 19 Expert PVC Configuration Parameters

Parameter	Description	Default
Profile	Specifies the name of the currently selected profile. This field is read-only.	No default
Logical Channel Number	Displays the LCN assigned to the associated PVC. Each PVC is assigned an LCN, starting from the lowest user-configured PVC LCN. This field is read-only.	No default
Inbound Packet Size	Specifies the inbound packet size that is used for the specified PVC. This value must be agreed upon by the PDN at network subscription time. Options: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096	128
Outbound Packet Size	Specifies the outbound packet size that is used by the associated PVC. This value must be agreed upon by the PDN at network subscription time. Options: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096	128
Inbound Window Size	Specifies the inbound window size that is used by the associated PVC. This value must be agreed upon by the PDN at network subscription time. Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)	2

Parameter	Description	Default
Outbound Window Size	<p>Specifies the outbound window size that is used by the associated PVC. This value must be agreed upon by the PDN at network subscription time.</p> <p>The window size must be less than the Packet Sequencing Modulo.</p> <p>Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)</p>	2
D-Bit Procedures Authorized	<p>Specifies whether Delivery Confirmation (D-bit) procedure is allowed for this virtual circuit.</p> <p>If set to <i>Yes</i> , incoming calls specifying D-bit procedures are allowed. If set to <i>No</i> , such calls are cleared.</p> <p>Options: Yes, No</p>	No

Authentication Options Parameters

When you select this option on the Network Interface Configuration menu and press *Insert* or *Enter* , a menu of inbound authentication parameters is displayed. This section describes the parameters that you can configure for X.25 inbound authentication for this interface.

Interface Name

Specifies the name of the interface assigned to the currently selected port. This field is read-only.

Inbound Authentication

Specifies whether incoming calls are subject to authentication based on specific DTE addresses in the authentication database.

If authentication is enabled, only incoming calls with a DTE address specified in the authentication database are accepted.

Options: Enabled, Disabled

Default: Disabled

Authentication Database Name

Allows you to enter the name of an authentication database. You can enter the name of an existing or a new database. You can add a new partner DTE address. For existing databases, the submenu displays a list of currently defined valid partner DTE addresses.

Authentication Database

Press **Enter** to view or edit the list of valid remote system IDs and associated DTE addresses. Each entry represents a valid partner that can communicate with this interface.

You can press **Enter** to edit an authentication entry or press **Insert** to add a new one. The X.25 Inbound Authentication Database window appears, from which you can associate a remote system ID with the DTE address from an incoming call. You can configure the following authentication entry parameters:

- ◆ **Interface Name**

Specifies the name of the interface you assigned to the currently selected port. This field is read-only.

- ◆ **Database Name**

Displays the name of the authentication database.

- ◆ **Remote System ID**

Specifies the local handle for a partner system. It is not verified or exchanged with the remote system. The remote system ID is used by protocols such as IP and IPX to identify a connection to a partner system.

Press **Enter** to list all remote system IDs.

Default: Blank

- ◆ **Remote DTE Address**

Specifies the 15-digit X.121 DTE address assigned to the remote system. This address must correspond exactly to the calling DTE address, included in the Incoming Call packet received by the remote system. Otherwise, authentication fails and the incoming call is rejected.

Default: Blank

WAN Call Directory Configuration Parameters

The WAN Call Directory is a list of WAN call destination configurations. You must create at least one WAN call destination configuration for each WAN link you want to use (one WAN call destination is one virtual circuit on one WAN link). Such a configuration contains the parameters needed by the WAN driver to establish and maintain links to a given destination. If you are routing multiple network protocols across a given WAN link, you must create one WAN call destination for each protocol that is routed on the WAN link.

Call Destination Name

Specifies the name of the WAN call destination. The name can contain up to 47 alphanumeric characters. This field is read-only.

Call Type

Specifies the type of call: permanent (active continuously) or on-demand (activated by the presence of data traffic directed to or through the remote peer system). The selection is made independent of the physical media type. You can specify permanent for switched circuits, dial-up circuits, or leased lines.

Options: Permanent, On Demand

Default: Permanent

Interface Group

Protocols such as IPX or IP can request an X.25 virtual circuit to be made either through a specific interface or by way of one interface from within a group of interfaces. Setting this parameter to a group name includes this interface in the specified group.

This parameter is available only when an on-demand call is configured.

Press Enter to display a list of currently defined groups and to define new groups.

Interface Name

Instructs NetWare Link/X.25 to establish a virtual circuit through a specific X.25 interface.

You can define call establishment through a specific interface (by setting this parameter) or through the first available interface from a group (by setting the Interface Group parameter).

NOTE: You can select an interface group or a single network interface, but not both.

Press Enter to display a list of all the available NetWare Link/X.25 interfaces, then select the interface you want.

Circuit Type

Specifies whether a PVC or an SVC is used to establish a connection to the specific destination.

NOTE: IP, Bridge, and AppleTalk protocols do not support PVCs.

Options: Permanent Virtual Circuit, Switched Virtual Circuit

Default: Switched Virtual Circuit

PVC Number

Specifies the PVC number. This number must be equal to the LCN assigned by the network to a PVC at network subscription time.

NOTE: This parameter is available only if the Circuit Type parameter is set to Permanent Virtual Circuit.

Range: 0 to 4095

Default: 1

Destination DTE Address

Specifies the X.121 DTE address assigned to the specific destination DTE. Enter up to 15 digits (in the range 0 through 9).

Default: Blank

Retry Mode

Specifies the conditions when a failed attempt at a connection (under the Call Type parameter) is retried automatically.

All connection failures are reported to the system console and to the Call Manager utility (CALLMGR). The result is successive connection attempts,

with an increasing delay between each attempt. The delay is set initially to 8 seconds and increases exponentially to the limit.

Options: Never Retry, Retry All Failures, Retry Self-Correcting Failures

Default: Retry Self-Correcting Failures

Retry Limit Handling

Specifies the action taken when the connection retry interval exceeds the configured limit. Retries can continue indefinitely at the configured interval limit or are terminated (the connections fail). The default option of Continuous At Limit supports unattended operation.

Options: Continuous At Limit, Stop At Limit

Default: Continuous At Limit (for permanent); Stop At Limit (for on-demand)

Retry Interval Limit

Specifies the maximum delay interval, in hours:minutes:seconds, between attempts to establish a permanent connection (under the Call Type parameter).

The delay is set initially to 1 second and increases exponentially. The Retry Limit Handling parameter allows retries to continue or stop when the maximum delay is reached.

Options: 00:00:00 to 23:59:59 (hh:mm:ss)

Defaults: 00:10:00 (for permanent); 00:02:00 (for on-demand)

Idle Line Timeout

Specifies the amount of time, in seconds, that a call can be inactive before closing the connection. This parameter is visible only for on-demand calls.

Range: 0 to 23:59:59

Default: 00:10:00

Remote System ID

Specifies the symbolic name of the remote peer system associated with this WAN call destination entry. This is typically the remote system server name.

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

Options: 1 to 47 ASCII characters

Default: WAN Call Destination Name

Expert Call Configuration Parameters

Pressing Enter while the cursor is on the Expert Call Configuration Parameters field displays a window listing Expert Call Configuration parameters. This window lets you configure advanced parameters for a specific WAN call destination.

You can configure the following Expert Call Configuration parameters.

Call Destination Name

Specifies the name of the WAN call destination. The name can contain up to 47 alphanumeric characters. This field is read-only.

Request Reverse Charging

Specifies whether Reverse Charging is requested for this call.

Options: Yes, No

Default: No

Window Size

Specifies the size of the window that is negotiated for a specific call. The value in this parameter overrides the default inbound or outbound window sizes specified in the X.25 Packet Level Parameters window. Refer to Packet Level Parameters for more information.

Range: 1 to 7 (Modulo 8); 1 to 127 (Modulo 128)

Default: 0 (no Window Size Negotiation Packet level)

Packet Size

Specifies the size of the packet that is negotiated for a call. If this parameter is used, it overrides the default inbound and outbound packet sizes specified in the X.25 Packet Level Parameters window.

Options: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, Not Selected

Default: Not Selected

Throughput Class

Specifies the throughput, in bits per second, that is negotiated for the call.

Options: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 48000, 64000, Not Selected

Default: Not Selected

CUG Facility

Specifies the type of CUG that is used for this specific call. A CUG permits DTEs belonging to the group to communicate with each other, but a CUG precludes communication with all other DTEs.

Options: Bilateral, Incoming, Not Selected, Outgoing

Default: Not Selected

CUG Number (hex)

Specifies a one- or four-digit hexadecimal number for a specific CUG. If the CUG Facility parameter is set to Incoming or Outgoing, you can enter a two-digit number. If the CUG Facility parameter is set to Bilateral, you can enter up to four digits.

WARNING: Refer to the ITU-T (formerly CCITT) Recommendation X.25 for more information before you set this parameter.

Fast Select

Specifies an optional parameter that a DTE can request for a virtual circuit to allow the use of up to 128 bytes of user data in Call Request packets. You can specify whether the Fast Select option is used for the call.

Options: Yes, No

Default: No

With Restriction

Addition to the Fast Select parameter that specifies whether the called DTE can accept a call with the Fast Select option.

If set to *Yes* , a call is made with Fast Select with the restriction enabled. In this case, the called DTE must clear the incoming call. This parameter is available only if the Fast Select parameter is set to *Yes*.

Options: Yes, No

Default: No

Call User Data (hex)

Specifies the actual user data that is sent in the Call Request Packet User Data field.

The length of the user data field depends on whether you configure to use Fast Select.

The following shows the lengths, in bytes, that are available, depending on two aspects: whether you are using Fast Select and the specific protocol being used.

IPX with Fast Select = 122 bytes; without Fast Select = 10 bytes

AppleTalk with Fast Select = 122 bytes; without Fast Select = 10 bytes

CLNS with Fast Select = 124 bytes; without Fast Select = 12 bytes

Generic ITU-T Facilities Entry

Lets you add new facilities codes to your current configuration in addition to the facilities already specified.

WARNING: This parameter must be entered in hexadecimal format. Refer to the ITU-T Recommendation X.25 before setting this parameter.

Generic National Facilities Entry

Provided as a convenience for customers requiring the specification of National or proprietary facilities. A provision for a Facilities Parameter Marker value is also included. This field is convenient for use across an X.25 gateway.

Entries must be in hexadecimal format consistent with the ITU-T Recommendation X.25.

Consult your network representative or technical support for further information.

Inbound Authentication Update

Specifies whether the inbound authentication database for the interface associated with this WAN call destination is updated to reflect connection information. If the parameter is set to **Enabled** , an entry consisting of the remote system ID and the password is written to the authentication database. If the parameter is set to **Disabled** , no entry is written.

Options: **Enabled**, **Disabled**

Default: **Disabled**

5

Managing

This section explains how to manage remote access after it has been installed and configured and describes the utilities used to manage remote access connections.

You have many options for managing remote access, including the use of

- ◆ RCONSOLE to start and stop remote access services remotely
- ◆ Utilities executed from the server console to monitor remote access
- ◆ NIASCFG to view the status of and change remote access parameters
- ◆ ConnectView to monitor remote access use in real-time
- ◆ ManageWise to manage remote access along with other network resources

Remote Access Using RCONSOLE

You can use RCONSOLE, the remote console utility provided with NetWare, to manage Novell[®] Internet Access Server 4.1. RCONSOLE enables you to use a workstation to access the server (on the same network or through a modem) by creating a remote server console.

During a remote console session, you can load and unload modules, execute console commands, and copy files. RCONSOLE is convenient for remote access control of your server.

NOTE: RCONSOLE will not allow remote access to a server if the network supervisor has not enabled remote connections using REMOTE. To access a server remotely, the Remote and RSPX modules must be loaded on the server, the RCONSOLE.EXE file must be loaded on the workstation, and you must know the remote password.

To launch an RCONSOLE session, type **rconsole** and press Enter. If you are starting a remote session through a direct Sequenced Packet Exchange™ (SPX™) connection, you can also designate the name of the server or the Internetwork Packet Exchange™ (IPX™) address you want to reach.

You can use the keystrokes described in Table 20 for the RCONSOLE functions shown. All other keys function as if you were at the server console.

Table 20 RCONSOLE Function Keys

Function	Press keys
Access the RCONSOLE Available Options menu	Alt + F1
Exit RCONSOLE	Alt + F2
Cycle through the console windows	Alt + F3 or Alt + F4
Show the address of the workstation you are using	Alt + F5

For complete information about using RCONSOLE to manage a server, refer to your NetWare® documentation.

Starting Remote Access

To start remote access, enter the following command at the NetWare® console prompt (:):

```
nwcstart
```

This command executes all the statements in the NWCSTART.NCF file that contains the LOAD commands for remote access services.

The NWCSTART.NCF file is created during the Novell Internet Access 4.1 installation and configuration. The NWCSTART command is automatically added to the AUTOEXEC.NCF file.

Bringing Down Remote Access

After installation and configuration have been completed, remote access is up and running. To bring it down or stop remote access from running, enter the following command at the NetWare system console prompt (:):

```
nwcstop
```


Remote Access Soft Shutdown

When in soft shutdown mode, the remote access server will not accept new connections, a condition useful when preparing to issue the **nwcstop** command. To put the remote access server into soft shutdown mode, enter the following command at the NetWare system console prompt (:):

```
nwcshutd
```

After issuing the NWCSHUTD command, all unused ports are disabled and dial-in ports are not monitored for incoming calls. Ports that were in use at the time the command was issued are not affected until released by the application. At that time, the port will also become unavailable.

Disabled ports show a status of Shutdown. Any attempts by applications to acquire a dial-out port will fail. You must issue the NWCRSUME command to resume normal remote access operation.

An alert is generated when the NWCSHUTD command is executed. To view the alert report, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Alerts

Resuming Remote Access

To exit soft shutdown mode and resume normal remote access operation, enter the following command at the NetWare system console prompt (:):

```
nwcrsume
```

After issuing the NWCRSUME command, all ports that were shut down become available again. All dial-in ports are reinitialized and go into a waiting state.

An alert is generated when the NWCRSUME command is executed. To view the alert report, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Alerts

Remote Access Using Console Utilities

The Remote Access Console Utilities can be launched from NIASCFG and are intended to be viewed as part of that program. The following list describes the NetWare® Loadable Module™ (NLM™) programs that make up the remote access console utilities.

- ◆ NWCCON—Configure remote access options. You can use this utility by loading NIASCFG and following this path:
Select Configure NIAS > Remote Access
- ◆ NWCSTAT—Display remote access status. You can use this utility by loading NIASCFG and following this path:
Select View Status for NIAS > Remote Access
- ◆ AIOCON—Configure low-level port information. You can use this utility by loading NIASCFG and following this path:
Select Configure NIAS > Remote Access > Configure Ports
- ◆ AIOPDCON—Create Packet Assembler Disassembler (PAD) profiles used to configure PAD parameters for X.25 connections. You can use this utility by loading NIASCFG and following this path:
Select Configure NIAS > Remote Access > Set Up... > Configure AIOPAD Parameters
- ◆ PPPRNCN—Configure Point-to-Point Protocol Remote Node Service (PPRNS) options. You can use this utility by loading NIASCFG and following this path:
Select Configure NIAS > Remote Access > Configure Service > PPPRNS
- ◆ ARASCON—Configure AppleTalk Remote Access Service (ARAS) options. You can use this utility by loading NIASCFG and following this path:
Select Configure NIAS > Remote Access > Configure Service > ARAS
- ◆ NCSCON—Configure NetWare Asynchronous Services Interface™ (NASI™) Connection Service (NCS) options. You can use this utility by loading NIASCFG and following this path:
Select Configure NIAS > Remote Access > Configure Service > NCS

Remote Access Using 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.

The Configure NIAS Option

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

Refer to *Setting Up* in the *Remote Access* documentation for the configuration procedures. For information about using the Set Up option to set parameters to simplify remote access management, refer to *Modifying Set Up Parameters for Remote Access Management*.

The View Status for NIAS Option

You can monitor remote access from the View Status for NIAS option. For more information, refer to the individual management procedures:

- ◆ Generating Remote Access Configuration Reports

- ◆ Viewing Remote Access Status Options
- ◆ Viewing Remote Access Port Status
- ◆ Viewing Remote Access Port Statistics
- ◆ Activating Remote Access Port Traces
- ◆ Resetting Remote Access Ports or Sessions
- ◆ Viewing Remote Access Port Identification
- ◆ Changing Remote Access Port Configuration
- ◆ Viewing Remote Access Service Status and Statistics
- ◆ Viewing Remote Access Alerts
- ◆ Viewing the Remote Access Audit Trail

Modifying Set Up Parameters for Remote Access Management

As part of remote access management, you might find it useful to set certain parameters to make your administration tasks easier, such as setting a directory context, specifying server information, and specifying audit trail parameters.

Setting Directory Context

Setting a default directory context helps you to easily traverse the Directory tree when you configure user-related menu options. This does not change the object's directory context, it just makes it easier to modify user-related configuration. To set the default directory context, load NIASCFG and follow this path:

Select Configure NIAS > Remote Access > Set up... > Set Directory Context

Specify the context in which most of your users appear. If your users are distributed over multiple contexts, then move up the Directory Tree to a common branch of the tree.

To move up the tree, select the double-period (..) entry; select any other container to move down the tree. If the CONNECT object does not have browse rights to move up the Directory tree, press Insert and enter the new directory context. This allows you to jump to another branch of the tree where the CONNECT object has rights.

Specifying Server Information

Specifying the server information requested on the Set Server Information window is useful for administering remote access from a remote console. It helps other administrators identify the server and also appears on the configuration reports. Entering this information is optional, but it is very useful in network management.

To specify the server information, load NIASCFG and follow this path:

Select Configure NIAS > Remote Access > Set Up... > Set Server Information

Enter the server installation location and description information.

Specifying Audit Trail Parameters

Remote access maintains an audit trail that stores a record of each connection and each user action. Configuring the audit trail consists of enabling or disabling the audit trail. If you enable the audit trail, you must specify the time of archival, the interval between two archives, and the number of archived files that you want retained before the audit trail is purged.

The audit trail information is used for accounting by the ConnectView[®] management application. You can also use the audit trail information to determine how effectively your resources are being used. You can view the audit trail and manage it from the Remote Access Status Options menu.

To set audit trail options, load NIASCFG and follow this path:

Select Configure NIAS > Remote Access > Set Up... > Define Audit Trail

Table 21 on page 213 describes the parameters of audit trail configuration. After you specify the audit trail parameters, press Esc to save your changes.

Table 21 **Audit Trail Parameters**

Audit Trail Parameter	Function
Enable Audit Trail	Enables (or disables) audit trail log entries to the currently active log file.
Archive Hour	Time of day when the contents of the current log file are to be moved to an archive file for storage. Specify a time when the communications server activity is low. The default time is 3:00 a.m.

Archive Interval	Set to a number of days (0-90) that log entries are to be accumulated in the current log file. At the end of the archive interval, log entries are moved to an archive file for storage. A value of zero indicates no archive. The default is one.
Archive Files Retained	Set to a maximum number of archive files to be retained for storage. When the maximum is exceeded, the oldest log file is deleted as the current log file is archived. The default is seven.

Generating Remote Access Configuration Reports

Each time you make changes to your configuration, generate a configuration report to verify your configuration. You can also use the configuration report for subsequent troubleshooting efforts. To generate a configuration report, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Generate Configuration Report

You are given the option of sending the report to the screen or a disk file. If you save the configuration report to a file, you can print the file or save it to compare with future reports. Table 22 on page 215 shows the information generated for a configuration report.

By default, all options are enabled. The F2 key enables you to customize options. For example, if you have many users, you can turn off User Information to generate a shorter, quicker report. You can enable or disable options before running the configuration report.

Table 22 Configuration Report Information

Report Entry	Description
Warning messages	<p>Consistency. These warnings display inconsistencies in port configurations, licenses, user restrictions to ports and services, and service restrictions to ports. These service-specific consistency checks help you determine configuration errors in the Configure Service windows:</p> <p>ARAS-specific messages. Make sure valid zone names are specified for user and global restrictions.</p> <p>PPRNS-specific messages. Make sure the correct protocol is selected for security.</p> <p>NCS-specific messages. Group names and port names defined in NIASCFG are equivalent to general names and specific names (with a slight difference) of NetWare Asynchronous Services Interface™ (NASI™) users. The difference is in the number of characters supported. NIASCFG supports a maximum of 15 characters for group and port names. NCS/NASI supports a maximum of 8 characters in general names and 14 characters in specific names.</p> <p>The inconsistency exists because third-party NASI applications are written to the specification defined for general and specific names; remote access is enhanced to support more characters.</p>
Directory context and container context	<p>Specifies the Directory context. Verify that it is set to the container in which most of your remote access users exist. This context is useful when you must browse NIASCFG menus to set up user configuration parameters. The Directory context is set in NIASCFG in the remote access Set Up... window.</p> <p>The Container context (Connect Rights Level) is defined when you create the CONNECT object in the Novell Directory Services™ (NDS™) tree during remote access installation. All NetWare users in the Connect container and below can access remote access, except users in the containers that are blocked with the Inheritance Rights Filter. A user who does not belong to the Container context might fail to establish a connection.</p> <p>You cannot change the Container context to allow users to establish connections. However, you can modify the CONNECT object's rights to the user's container. Use the appropriate NetWare administrative utility to grant the CONNECT object Browse rights and Read attributes to the container. This allows the users in that container to access remote access. To allow the CONNECT object to manage the user's connect parameters, also grant the CONNECT object Write attribute rights to the container.</p>

Report Entry	Description
Installed and loaded remote access services	Displays the installed and loaded remote access services. These are installed automatically when you install remote access. However, load only the services that you require. If you do not see the proper services loaded, choose Select Remote Access Services from the Set Up... window and load the required services.
Installed and enabled third-party security services	Displays the installed and enabled third-party security services. Third-party security devices are installed separately from remote access. When at least one third-party security device is installed, the third-party security entries appear in the configuration report. Verify that the third-party security product is enabled or disabled as required by your installation.
Defined communication ports	<p>Displays the port mapping, modem type, and link parameters for the list of defined ports.</p> <p>Defined Remote Access Ports. Verify that the ports are defined correctly for dialing in, dialing out, or both.</p> <p>Port groups defined. If a port group is named incorrectly or contains the wrong port, refer to Port Groups for instructions on changing the name or configuration.</p>
Authorized users for ports and services	Displays the authorized users for the ports and services. Make sure that only valid user IDs are allowed to access these ports and services. Any User means all valid users not restricted by the Connect Rights Level. If you want to restrict some users to ports or services, refer to Remote Access Security.
Authorized ports for services	If Any Port is defined to use the service, then all remote access ports can use that service. If you want to restrict specific ports to a service, refer to Remote Access Security.
Services configured to use ports	Displays the same information as Authorized ports for services, but in a different format. The ports and the services each has access to are listed in alphabetic order.
System defaults	<p>Displays the global defaults: maximum connect time, default dial-back mode, idle timeout, dial-out restriction, and remote access password restriction.</p> <p>The system defaults for maximum connect time, dial-back mode, and dial-out restrictions are overridden by the defaults set for the individual user.</p>
User information	Displays the configuration parameters for each user.

Report Entry	Description
Configuration reports for NCS, PPPRNS, and ARAS	<p>Displays the configuration parameters for NCS, PPPRNS, and ARAS.</p> <p>For NCS, this is the list of general names that NASI, WIN2NCS, and MAC2NCS users see on their workstations. The default group in the list is ANY_PORT; this group contains all remote access ports. The default general name for DIALIN ports is DIALIN. To make any changes to the NCS configuration parameters, refer to <i>Configuring NCS</i>.</p> <p>For PPPRNS, this is the list of configured options including Enabled Security, enabled IP and IPX interfaces, ISDN short hold parameters, and whether PPP ISDN Multilink is enabled.</p> <p>For ARAS, this is the list of configured options for all ARAS clients. The list of Setup Options includes Forward Packets to AppleTalk with CRC Embedded, Support Version for Remote Access Clients, whether to prompt users for remote client password, and the optional ARAS greeting. The Default Restriction Zone List and User Restricted Zone List are also included.</p>

Viewing Remote Access Status Options

To view the remote access status options, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access

The remote access Status Options menu is displayed, showing four display options. Table 23 lists the options, what each displays when selected, and other information about each option.

Table 23 Remote Access Status Options

Option	Information Displayed
Display Port Status	Displays real-time port information such as the port name, port status, service accessing the port, username, elapsed time, port description, and maximum connection time. This option allows you to reset a session.
Display Service Status	Displays statistics for each of the loaded services. Service statistics can be divided into general and custom statistics.
Display Alerts	Displays real-time and current alerts. This option also enables you to archive current alerts and to save alerts to a file.

Option	Information Displayed
Display Audit Trail	When auditing is enabled, displays audit event's time of occurrence, username, workstation ID (if applicable), port name, telephone number dialed (if applicable), dialback number, service used, and session names (for modem-independent ports only). This option enables you to display the active log file, select and view an archived file, output to an ASCII file, and display entries in descending order.

Viewing Remote Access Port Status

Monitoring port status gives you real-time information about the port name, status of the port, service accessing the port, username, elapsed time, port description, and maximum connection time.

To view the port status, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status

The Port Status Window is displayed. Each port is listed with the following Headings: port name, status, service, user, and time. Table 24 defines each Heading.

Table 24 Port Status Window

Heading	Meaning
Port Name	The name assigned to a port during port configuration.
Status	The status of the selected port. Table 5-3 shows the possible values and their meanings.
Service	The service that has acquired the port.
User	The name of the user accessing the port. The full username appears at the bottom of the screen when the port is highlighted. If it is more than 10 characters, the name is truncated.
Time	The duration of the connection.

The status of the selected port is displayed in the second column from the left. Table 25 shows the possible values and their meanings.

Table 25 Port Status

Port Status	Meaning
Acquired	The port was acquired by remote access.
Acquired Other	The port was acquired by an application other than remote access.
Answering	The port is responding to an incoming call.
Broken	Remote access failed to initialize the modem attached to this port.
Connected	The remote connection established successfully.
Connecting	The remote caller is attempting to establish a remote access connection.
Dialing	Remote access is dialing out.
Disconnected	The connection has been completely terminated.
Disconnecting	The connection is being reset.
Idle	The port is available for dial-out use.
Initializing	The modem-to-port connection is being initialized.
Shutdown	The port is not available because the system is in soft shutdown state.
Startup	Remote access is being loaded.
Unavailable	The port cannot be used because the driver providing this port is not loaded or has not registered this port with remote access.
Waiting	The port is ready for an incoming call.

For more information and options, highlight a port name and press Enter. The Port Operations menu is displayed, offering six options. Table 26 describes the available options.

Table 26 Port Operations

Option	Action or Information Displayed
Display Port Statistics	Views current settings, configuration information, and statistics for the selected port.
Start Trace on Port	Starts a trace of this port's bidirectional data that is saved to a binary file. This option is helpful if you have problems with a modem initializing or if an incoming application fails to connect. Starting a trace adds the Stop Trace on Port option to the Port Operations menu.
Stop Trace on Port	Stops a port trace. This option is present only after a trace has been begun. After the trace has been stopped, you can view the captured trace data using the VIEWTRC utility from a workstation.
Reset Port	Reinitializes a port that has failed to initialize or whose configuration parameters have been changed. Use this option to forcibly disconnect a user.
Identify Port	Use this option to identify which physical port is referenced by this port name. When you select this option the remote access software toggles the port's DTR signal, causing the TR or DTR light on the attached modem to blink. You cannot use this option if the port is in use by an application.
Terminal Mode	Use this option to diagnose a modem or cabling problem. This option sends data to the selected port from the keyboard or a file and enables you to view the response.
Configure Port	Enables you to change a port's name, modem type, or link parameters.

Viewing Remote Access Port Statistics

Viewing port statistics gives you real-time information about the port name, status of the port, service accessing the port, username, elapsed time, port description, and maximum connection time.

To view a port's statistics, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status

Select the port you want to view and press Enter.

The information window for the selected port is displayed showing detailed information about current settings, port information, and port statistics. You will have to scroll down the window to view all the information presented.

Current Settings

Verify that the current settings are what you expect. The settings listed on the information window include bit rate, data bits, parity, flow control and port signals and reflect what the driver is currently using for this port.

Port Information

The information window displays general and configuration information about the selected port. You can view the hardware type, board number, port number, application owning and monitoring the port, configured default bit rate, and data bits (for the port and modem, if applicable).

Port Statistics

The information window displays data bytes received and transmitted, parity errors, framing errors, and hardware and software overrun errors.

Saving Information to a File

The contents of the information window can be saved to a file by pressing the F2 key. The data is written to the file `SYS:\SYSTEM\AIO\AIOMON.TRC`. If the file already exists, the current data is appended to the file. You can view and print the file using an ASCII text editor.

Activating Remote Access Port Traces

If you have problems with a modem initializing or if an application fails to connect to a port, you can start a trace on the port to get more information about the problem.

Starting a Port Trace

To start a trace on a port, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status > port you want to trace > Start Trace on Port

Select the port you want to trace, press Enter , then select Start Trace on Port from the Port Operations menu.

You are prompted for the Output File Name. After you enter the trace filename, the Port Operations menu is removed and the server captures the information flow. All data packets sent to and received from the port are saved into the trace file. The trace is active until you stop it.

NOTE: If you do not specify a path with the trace filename, the file will be saved on the root of the SYS volume.

Stopping a Port Trace

To stop a trace, select the desired port, then select Stop Trace on Port.

Use the VIEWTRC utility to convert the file into readable form for viewing.

Viewing Trace Files

Novell Internet Access Server 4.1 provides a DOS-based utility, VIEWTRC.EXE, that converts the trace files you have saved to ASCII text files that you can read with any text editor.

VIEWTRC.EXE is installed in the SYS:SYSTEM\UTILS subdirectory. Copy this file to a DOS workstation and enter the following command at the DOS prompt:

```
viewtrc source destination
```

Replace *source* with the pathname and filename of the trace file, and replace *destination* with the pathname and filename of the converted file.

Resetting Remote Access Ports or Sessions

You can reset a port if you have problems with a modem initializing or if an application does not recognize a port.

To reset a port, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status

Select the port you want to reset, press Enter, then select Reset Port from the Port Operations menu. The Port Reset Options menu is displayed, offering the three options shown in Table 27.

Table 27 **Port Reset Options**

Option	Resulting Action
Reset Session	Terminates the connection by notifying the application using the port to disconnect the session. Use this option in the case of malfunctioning hardware or software or for security purposes. Generally, the remote user is not notified that the connection will be terminated, but this behavior depends on the application.
Conditional Port Reset	Initializes the port in an orderly way. If the port is not in use, the port will be re-initialized. Use this option to guarantee that you will not reset a port that is in use.
Unconditional Reset of Port	Causes AIO to release the port and notify the application. Use this option in the event of a malfunctioning application and only if the Reset Session or Conditional Port Reset options fail.

WARNING: Use the Unconditional Reset of Port option with extreme caution because data loss could occur.

Viewing Remote Access Port Identification

You can use the Identify Port option to identify which physical port is referenced by this port name. The remote access software will toggle the port's DTR signal, which causes the TR or DTR light on the attached modem to blink. You cannot use this option if the port is in use.

You can use this option to quickly find the modem attached to a port. For example, if users report that they are having trouble dialing in to a certain port and you suspect a problem with the modem, use the Identify Port option to determine which modem to replace without having to trace cables.

You can also use the Identify Port option to find out the name of the port that a particular modem is attached to. Select the ports in sequence and request the Identify Port option until the modem in question blinks.

To use this feature, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status

Select the port you want to identify, press Enter, then select Identify Port from the Port Operations menu.

Changing Remote Access Port Configuration

You can use the Configure Port option to change the configuration parameters for a selected port, including the port's name, modem type, and link parameters.

To change a port's configuration, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status > port you want to configure > Configure Port

When you select the Configure Port option, the initial window displays the highlighted Port Name, the port description and the modem type in use. Use the cursor control keys (arrow keys) to highlight the parameter you want to change. After making a change, press Enter or F3 to save your changes.

When you modify the modem type, select a specific modem name or select Automatic Detection to have the remote access software attempt to find out which modem is connected to the port.

You can modify more parameters by selecting Additional Parameters. The additional parameters include link parameters, port mapping, groups assigned to, applications allowed, and application parameters.

Viewing Remote Access Service Status and Statistics

The Display Service Status option enables you view statistics for each of the loaded services. Service statistics can be divided into general and custom statistics.

The Service Statistics window lists the service name, whether it is running, whether statistics are available, and the port number. A description of the service is displayed below the Service Statistics window with an explanation of the service's function.

To view a service's statistics, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Service Status

Select the service you want to view and press Enter. The statistics for the selected service are displayed.

Viewing NCS Status

Highlight NCS and press F10 to view more status information about the NetWare Asynchronous Services Interface™ (NASI™) Connection Service (NCS), as shown in Figure 16. This window also displays remote control hosts on the LAN waiting for calls (if configured to use the dial-in group). The other services (ARAS and PPRNS) do not provide any additional status information.

Figure 16 NCS Status

NCS Status 1.0						NetW
Session	Port Name	Dial	Status	CallerID	NASI	
ENG	SVE-ENG DIALIN	IN	ACTIVE	JOE	SUPERV	
IN1	AIO_10001	IN	IDLE		SUPERV	
IN1	AIO_10002	IN	ACTIVE	RAY	TESTE	
OUT	AIO_10003	OUT	ACTIVE	RAY		
OUT	AIO_10004	OUT	IDLE			
OUT	AIO_10005	OUT	ACTIVE	OLAF		

Session ID: ENG	
Port Name: SVE-ENG_DIALIN	
Caller ID: JOE	
NASI USER ID: SUPERVISOR	
Network Address: c1fc0000	Node Address

Viewing Service Statistics

You can monitor service statistics to diagnose internal problems with the services. To view the service statistics, select the service you want to view from the those listed and press Enter. To reset the statistics counters to zero, press Delete.

PPPRNS Statistics

Service statistics for PPPRNS can be divided into general and custom statistics. Only the custom statistics are explained in this section. For an explanation of general statistics, refer to information on the MONITOR utility in the NetWare documentation. To view the PPPRNS statistics, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Service Status > PPPRNS Statistics

Table 28 defines the PPPRNS custom statistics.

Table 28 PPPRNS Custom Statistics

Statistic	Meaning
Number of Connected Ports Monitored	The number of active sessions that PPPRNS is monitoring.
Reset Statistics Counter	The number of times you pressed Delete to reset the counters.
Total Bytes Transmitted	The total number of bytes that PPPRNS sent from all ports.
Data Packets Transmitted	The number of packets transmitted by PPPRNS.
Total Bytes Received	The total number of bytes PPPRNS received from all ports.
Data Packets Received	The number of packets PPPRNS received from all ports.
Receive Framing Errors	The number of invalid frames that PPPRNS received.
Receive CRC Errors	If you have cyclic redundancy check (CRC) errors, then you might have data loss. The data loss could be from hardware overrun or corrupted data. Hardware overruns occur if data is arriving too fast for the server to process and the data is being overwritten. During disturbances in the asynchronous link, the incoming byte might be altered, resulting in corrupted data.

Statistic	Meaning
Received Frames Too Big	If your receive buffer cannot handle the bigger frames from the client, this counter is incremented. This shows problems with the client negotiation.
No RCB to receive frame	The number of times PPRNS cannot acquire a receive buffer to accept an incoming frame. Incoming frames are discarded. This could happen if resources are running low.
Number of Transmit Frames Tossed	The number of transmitted frames that were discarded because PPRNS was too busy.
TSM Tx Flow Control Errors	This counter is incremented if PPPTSM sends information when PPRNS is busy. The problem could be with the flow control handshake.

NCS Statistics

To view the NCS statistics, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Service Status > NCS Statistics

Table 29 defines the custom statistics for NCS.

Table 29 NCS Custom Statistics

Statistic	Meaning
Command Interpreter Users	The number of NASI applications using NCS that have active Command Interpreters (CIs)
Query Name Requests	The number of requests to query a general port name or a specific port name
Packets Input	The total number of packets input to NCS by NASI applications
Packets Output	The total number of packets output by NCS to NASI applications
Total Connections	The total number of connections to the NCS ports

ARAS Statistics

Service statistics for ARAS can be divided into general and custom statistics. Only the custom statistics are explained in this section. For an explanation of general statistics, refer to information about the MONITOR utility in the NetWare documentation.

To view the ARAS statistics, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Service Status > ARAS Statistics

Table 30 explains the custom statistics for ARAS.

Table 30 Custom ARAS Statistics

Statistic	Meaning
Number of Ports Monitored	Number of active ports that ARAS is controlling
Total Bytes Transmitted	Total number of bytes that ARAS sent out of the serial ports
Data Packets Transmitted	Number of packets transmitted by ARAS
Data Packet Bytes Transmitted	Number of bytes in all the packets transmitted so far
Total Bytes Received	Total number of bytes ARAS received from the serial ports
Data Packets Received	Number of packets ARAS received from the serial ports
Data Packet Bytes Received	Number of bytes in all the packets received so far
Receive Framing Errors	Number of framing errors that ARAS received
Receive CRC Errors	Number of cyclic redundancy check (CRC) errors received by ARAS
Out-of-Sequence Packets Received	Number of packets ARAS retransmitted because it did not receive an acknowledgment
Out-of-Sequence Packet Bytes Received	Number of bytes ARAS retransmitted because it did not receive an acknowledgment
Requested Retransmits	Number of times the remote end requested retransmission because data was lost during transmission
Timeout Retransmits	Number of times the remote end timed out and ARAS had to retransmit the data

Viewing Remote Access Alerts

An alert is a record of a network event alerting you to problems and conditions on the network. To view the remote access alerts, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Alerts

A list of alerts is displayed.

Saving Alerts to a File

To save an alert to a file, select the alert and press F2. You are prompted to specify a filename in the (default) path, SYS:\SYSTEM. You can specify a different path. This file can be copied to a LAN workstation to be viewed or printed with an ASCII text editor.

Managing Alerts with Display Options

The Display Options menu offers four options for managing alerts. To view and use the Display Options menu from the Manage Alerts window, press Insert. Table 31 defines the display options.

Table 31 Manage Alerts Display Options Menu

Display Option	Meaning
Display Active Log File	Displays a list of current audit trail entries if any are available.
Select from Archived File List	Lists all archived files, depending on the settings in the Audit Trail Configuration window. Select a file from the list and press Enter to display all alerts archived in that file.
Output to ASCII File	Prompts you for a filename in which to save the displayed list of alerts. You can print this ASCII file from any LAN workstation.
Display Entries in Descending Order	Sorts the displayed alerts in ascending or descending chronological order.

Viewing the Remote Access Audit Trail

An audit trail contains information about who used which service or port and for how long. You can view and manage the audit trail from the Remote

Access Options menu if you enabled the audit trail when you configured remote access.

To view and manage the audit trail, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Audit Trail

A list of logged events is displayed. To save a logged event to a file and print, select the entry and press F2. Specify a different pathname and filename if you do not want the program defaults.

You can press Insert to manage the audit trail with the Display Options menu, as described in Managing Alerts with Display Options.

Remote Access Using ConnectView

ConnectView™ enables you to perform real-time management of the remote access software on multiple Novell® Internet Access Server 4.1 servers. This includes displaying multiple servers and their resources, managing ports and connections for a selected server, setting a port threshold value for each server, and displaying alerts and audit trail data for each server.

Refer to the following sections for information about

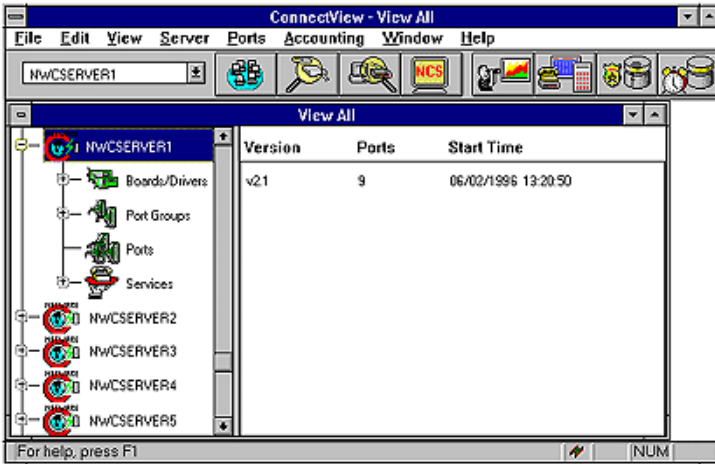
- ◆ Displaying and Managing Servers and Their Resources
- ◆ Managing and Monitoring Connections and Ports
- ◆ Accessing Log Files and Log Reports
- ◆ Displaying and Using Trend Analysis Data
- ◆ Setting Up Accounting Profiles and Generating Billing Charges

Displaying and Managing Servers and Their Resources

ConnectView opens a View All window whenever the application is started. The View All window enables you to quickly view a list of your managed servers, display and control the servers' resources, and view summary information about them. Server resources include the boards/drivers, port groups, ports, and remote access services. To view this data, you need the Simple Network Management Protocol (SNMP) MonitorCommunity (GET) access rights. Figure 17 shows an example View All window.

NOTE: Only one instance of the View All window can be opened. This window cannot be closed unless you exit the application; however, it can be minimized.

Figure 17 View All Window



You can also open View windows to display additional views of resources and data for individual servers. To open a View window, select the desired server and choose Window > New. A View window appears for the selected server.

Server and server resources appear as containers or leaf objects. Container objects (servers, board/driver groups, port groups, and service groups) can be expanded to display additional resources. A plus sign (+) appears in front of the container objects that can be expanded. A minus sign (-) appears in front of the objects that have been expanded and can then be collapsed. Leaf objects (individual boards/drivers, ports, individual port group, and service) are objects that cannot be expanded and do not have either symbol in front of them. Selecting an object causes information for the selected object to appear in the right side of the window.

To expand the objects of a container, either double-click the container or select it and choose View > Expand Object or press +. To return the objects to the container, either double-click the expanded container or select it and choose View > Collapse Object or press -.

NOTE: The message Gathering data... appears when data for the server's resources is being obtained. Also, to indicate the application is processing data, a lightning bolt flashes in the Status Bar.

By default, server polling intervals are set to 5 minutes so the data in the View All and View windows is refreshed every 5 minutes. To force an immediate update of the data displayed in the View All window or a View window, select the window and choose View >Update (F5).

If data for a server cannot be retrieved, collapse it and select another object. Then, reselecting and expanding the server icon causes ConnectView to retry retrieving the data.

Managing and Monitoring Connections and Ports

To establish a dial-in or dial-out connection, the remote access software first assigns the user a necessary port and then establishes a connection to the destination device. After the connection is established, the remote access software, and any additional software, such as third-party remote access applications, establishes a session between the calling and receiving applications so that the remote node or remote control communication can take place.

ConnectView enables you to

- ◆ Quickly display a summary of port availability through a graph
- ◆ Quickly verify the status of a server's port connections and settings information to enable you to easily monitor connections and diagnose configuration problems when they occur
- ◆ Reset ports to enable you to perform port maintenance and security functions
- ◆ Access a Port Status dialog box for each port to enable you to view port utilization, display error statistics, verify port settings, and check modem status and operation
- ◆ Display NetWare[®] Asynchronous Service Interface™ (NASITM) Connection Service (NCS) session data to enable you to manage NCS sessions

NOTE: You need the SNMP MonitorCommunity (GET) access rights to display data and the SNMP ControlCommunity (SET) access rights to perform management operations. Refer to Support for SNMP and ConnectView for more information about setting community strings.

For more information about managing connections and ports, refer to the following sections:

- ◆ Managing Port Connections
- ◆ Viewing Port Status
- ◆ Setting Port Thresholds
- ◆ Managing NASI Connection Service (NCS) Sessions

Managing Port Connections

You manage port connections in the Port Connections window. This window displays data in a graph showing the in-use and available ports, connection information, and detailed port configuration data.

To access the Port Connections window, first either select the desired server in a View All or View window or select the desired server name in the Server combo box in the Tool Bar. Then, either click the Port Connections icon in the Tool Bar or choose Server > View Port Connections. ConnectView opens the Port Connections window for the selected server.

Displaying Connections by User ID, Port Name, Port Status, or Service

ConnectView allows you to limit the display of port connections with the following display options:

- ◆ User ID
- ◆ Port
- ◆ Port status
- ◆ Service

Limiting the display of port connections helps you find information quickly and focus on connections and port problems when they occur. To access these options, choose View > Display Options (F4). ConnectView displays the Port Connections Display Options dialog box.

Specify the desired options and click OK.

Updating Port Connections Data

ConnectView updates port connection data based on the server's polling interval. By default, the server polling interval is set to 5 minutes for each

managed server. ConnectView also enables you to force an immediate update of the information when it is needed.

NOTE: To change a server's polling interval, choose File > Preferences and click the Server Information tab button.

To force an immediate update of the data in the Port Connections window, choose View > Update (F5). ConnectView replaces the current data with the most up-to-date data available from the network.

Viewing Port Status

To verify port status and configuration data, you can access a Port Status dialog box. This dialog box provides a real-time status of the selected ports, graphs for the level of traffic and errors, summary connection information, and a graphic display of modem and port signals.

To access a Port Status dialog box, first select the desired port in the View All, View, NCS Sessions, or Port Connections window. Then, either click the Port Status icon in the Tool Bar or choose Ports > View Port Status. ConnectView opens the Port Status dialog box for the selected port.

NOTE: Double-clicking a port icon, or a port connection in the above windows also opens the Port Status dialog box.

Updating Port Data

ConnectView polls the selected port every 2 seconds to update the real-time data displayed in the Port Status dialog box. ConnectView updates this data independent of the server's polling interval. ConnectView also enables you to turn off this polling by clicking the Stop Polling button or to force an immediate update of the information by pressing Update.

Resetting Port Statistics

ConnectView enables you to reset the statistics displayed in the Traffic and Errors graphs, so that you focus your analysis on current and future traffic and error rates. By default, these statistics are cumulative for all connections on this port, starting from when the remote access software was started.

To reset the statistics, click the Reset Statistics button. The current statistics are set to zero. Statistics for new traffic and errors accumulate until the dialog box is closed or the statistics are reset again.

Reopening the dialog box displays the current cumulative statistics based on the original data. The statistics return to zero when the remote access software is unloaded and restarted.

Resetting Ports

ConnectView enables you to reset the ports displayed for the current server. Reset a port to terminate an unwanted connection or to perform connection and session maintenance. Resetting a port disconnects the current users and returns the port to its original state. This is equivalent to the remote access software unconditional port reset command.

NOTE: To reset a port, you need the SNMP ControlCommunity (SET) access rights. Refer to *Support for SNMP and ConnectView* for more information about setting community strings.

To reset a port, select the desired port and choose Ports > Reset Port. ConnectView resets the selected port.

NOTE: Another way to reset a port is by selecting a port in any ConnectView window that displays ports and choosing Ports > Reset Port.

Setting Port Thresholds

ConnectView enables you to set a port usage threshold, to enable you to receive proactive notification when port usage reaches a specified limit.

When the threshold limit is reached, the remote access software generates a threshold message informing you that the port usage threshold has been reached. This proactive notification can help you efficiently distribute port usage across your servers, optimize port usage, and perform capacity planning.

NOTE: To set a port threshold, you need the SNMP ControlCommunity (SET) access rights. Refer to *Support for SNMP and ConnectView* for more information about setting community strings.

To set a port threshold, select the desired server in a View All or a View window, or select the desired server name in the Server combo box in the Tool Bar. Then, choose Ports > Set Port Usage Threshold. ConnectView opens the Threshold Settings dialog box. Enter the desired settings and click OK.

Managing NASI Connection Service (NCS) Sessions

You can manage NCS sessions in the NCS Sessions window. This window provides a status of the NCS sessions on the current server and is updated

according to the server's polling interval. By default, the server polling interval is set to 5 minutes for each managed server.

To access the NCS sessions window, first either select the desired server in the View All window or a View window, or select the desired server name in the Server combo box in the Tool Bar. Then, either click the NCS Sessions icon in the Tool Bar or choose Server > View NCS Sessions. ConnectView opens the NCS Sessions window for the selected server.

Displaying Connections by Session ID, Port, Status, or Dial Type

ConnectView allows you to filter the display of NCS session data with the following display options:

- ◆ Session ID
- ◆ Port
- ◆ Status
- ◆ Dial type

To access these options, choose View > Display Options (F4). ConnectView displays the NCS Sessions Display Options dialog box.

Updating NCS Session Data

ConnectView updates the data in the NCS Sessions window according to the server polling interval. By default, the server polling interval is set to 5 minutes for each managed server. ConnectView also enables you to force an immediate update of the information displayed in this window.

NOTE: To change the server's polling interval, choose File > Preferences and click the Server Information tab button.

To force an update of the data in the NCS Sessions window, choose View > Update (F5). ConnectView replaces the current data with the most up-to-date data from the network.

Resetting NCS Sessions

ConnectView enables you to reset the sessions displayed in the NCS Sessions window by resetting the port. This allows you to terminate unwanted connections and perform session maintenance. Resetting a port used by a session disconnects the current users and returns the port to its original state.

NOTE: You need the SNMP ControlCommunity (SET) access rights to reset a session. Only sessions with a Connected status can be reset. Refer to Support for SNMP and ConnectView for more information about setting community strings.

To reset a port, select the desired NCS session and choose Ports > Reset Port. ConnectView resets the port used by the selected session.

Accessing Log Files and Log Reports

ConnectView provides access to each managed server's alerts file and audit trail file and displays data in report format. In addition, ConnectView allows you to customize the data fields that appear in the reports. The alerts file contains a history of a server's events. The audit trail file contains a record of remote access service access and usage. These files are stored and maintained in the SYS:SYSTEM\CSLIB directories on the remote access servers on your network. Before accessing the log files, ensure that the BSPXCOM.NLM file is loaded on the managed servers and that the BREQUEST.EXE program file is running on the ConnectView workstation.

IMPORTANT: The audit trail file and/or archived files must be available to display trend analysis, accounting, audit trail, and alert data. To enable the audit trail, choose Server > Configure Audit Trail. If a large audit trail file or archived files are used, obtaining audit trail or alerts data might require a substantial period of time.

This section covers the following topics:

- ◆ Configuring Audit Trail Recording
- ◆ Using Alerts Files
- ◆ Using Audit Trail Files

Configuring Audit Trail Recording

Audit trail records in the current audit trail file or archived files are required for trend analysis and accounting and for viewing alerts and audit trail logs. ConnectView enables you to dynamically turn on and off remote access audit trail recording and set audit trail options for archiving files. By default, remote access audit trail recording is enabled; the archive hour is set to 3:00 a.m.; the archive interval is set to 1 day; the number of archived files retained is set to 7.

NOTE: To change the audit trail options, you need the SNMP ControlCommunity (SET) access rights. Refer to Support for SNMP and ConnectView for more information about setting community strings.

To toggle the remote access audit trail recording and change other audit trail options, select the desired server and choose **Server > Configure Audit Trail**. ConnectView opens the Audit Trail Configuration dialog box.

To enable remote access audit trail recording, click the **Enable Audit Trail** check box. Use the spin controls to set the desired archive hour, archive interval, and the number of archived files retained. To disable audit trail recording, clear the **Enable Audit Trail** check box.

NOTE: Enabling and disabling audit trail recording affects the recording of only remote access and NetWare Connect™ 2.0 records. However, changes to the archive options affect the server's archive files.

To apply the changes and close the Audit Trail Configuration dialog box, click **OK**. To close this dialog box without applying the changes, click **Cancel**.

Using Alerts Files

Alerts files contain information about network events detected by the remote access software. Alerts files contain a chronological record of information—such as severity, time the event occurred, port name, and service—based on the current audit trail file. You can use the display options to view the alerts data from the archived files. Data for alerts can be displayed in tabular and report format.

ConnectView provides access to the alerts files of the servers you are managing to enable you to obtain a chronological list of server events and assess server performance.

To access an alerts file, complete the following steps:

- 1** Ensure that the desired server is selected.

If the desired server is not selected, either select the server icon in the **View All** window or a **View** window or select the server name in the **Server** drop-down combo box located in the left corner of the **Tool Bar**.

- 2** Either click the **Alerts** icon in the **Tool Bar** or choose **Server > View Alerts**.

ConnectView prompts you for start and end dates. Enter the desired dates and click **OK**. ConnectView opens an **Alerts** window.

You can further limit the displayed alert data by choosing **View > Display Options (F4)** and specifying the dates within the specified start and end dates.

IMPORTANT: Due to table tool limitations, up to 8,000 alert records may be displayed at one time.

Displaying Alert Data by Entry Time, Severity Level, Port, and Service

ConnectView enables you to limit the display of alerts by entry time, severity level, port name, and service.

To limit the data displayed in the Alerts window, choose View > Display Options (F4). ConnectView opens the Alerts Display Options dialog box.

Click the Filter radio button and click the check boxes for the desired options.

To display the alerts data for the specified settings, click OK. To close the Display Options dialog box without changing the current settings, click Cancel.

To return to full display, click the Show All radio button and OK.

Updating Alert Data

Alert data is not updated automatically. However, ConnectView enables you to refresh the data whenever it is necessary.

To force an immediate update of the data in the Alerts window, choose View > Update (F5). ConnectView replaces the current data with the most up-to-date data available from the current audit trail file.

Generating Alert Reports

ConnectView enables you to generate daily and summary alert data in report format. The report format allows you to view and print formatted data for server summaries or daily alert activities. Also, by using the Alerts Display Options dialog box to limit the data in the Alerts window, you can limit the content of the report to a specified time period, severity level, port, and service.

NOTE: To limit the content of the report to a specified time period, severity, port, and service, use the display options in the Alerts window before accessing the report. Due to table tool limitations, up to 8,000 alert records may be displayed at one time.

To display alert data in report format, ensure that the desired server is selected, and from any window choose File > Generate Report > Alerts. ConnectView opens the Alerts Report window and displays the alert data in report format. The Alerts window is also opened in the background.

NOTE: Closing the Alerts window also closes the Alerts Report window.

Customizing the Alert Report

ConnectView allows you to specify which information appears in the Alert Report window and in what order the data columns appear.

To customize the data display in the Alert Report window, choose File > Report Preferences and click the Alert tab button. The Report Preferences dialog box appears with the options for the Alert Report window.

By default, the Alert Report includes summary and detailed information. Detailed information appears in the following order:

- ◆ Entry time
- ◆ Severity
- ◆ Port name
- ◆ Service
- ◆ Description

Clear the check boxes for the data you do not want to appear in the report.

To change the order of the detailed information, select the desired field and click the Up or Down button.

To save your changes, click OK. The changes take effect the next time the Alert Report window is opened and remain in effect until these options are changed. To close this dialog box without applying the changes, click the Cancel button.

Printing or Copying Alert Report Data

ConnectView allows you to print or copy report data.

To print alert report data, open an Alerts Report window and choose File > Print. ConnectView prints the displayed report.

To copy the alert report data, open an Alerts Report window and choose Edit > Copy. ConnectView copies the displayed report to the Windows clipboard.

Using Audit Trail Files

An audit trail file is integral to network security and management. This file provides information that identifies who used which remote access ports and services, when the ports and services were used, and for how long. When the Audit Trail window is first opened, the data is based on the current audit trail file. You can use the display options to view the audit trail data from the archived files. This data enhances system security and enables efficient planning and resource allocation.

Accessing Audit Trail Records

To access a server's current audit trail file, complete the following steps:

- 1** Ensure that the desired server is selected.

If the desired server is not selected, either select a server icon in the View All window or a View window or select a server name in the Server drop-down combo box located in the left corner of the Tool Bar.

- 2** Either click the Audit Trail icon in the Tool Bar or choose Server > View Audit Trail.

ConnectView prompts you for start and end dates. Enter the desired dates and click OK. ConnectView opens an Audit Trail window.

You can further limit the displayed audit trail data by choosing View > Display Options (F4) and entering dates within the specified start and end dates.

IMPORTANT: Due to table tool limitations, up to 8,000 audit trail records may be displayed at one time.

Displaying Audit Trail Data by Entry Time, User ID, Port, Port Status, and Service

ConnectView enables you to limit the data displayed by entry time, user ID, port, port status, and service.

To display audit trail information by any of the display options, choose View > Display Options (F4). ConnectView opens the Audit Trail Display Options dialog box for the Audit Trail window.

Click the Filter radio button and click the check boxes for the desired options.

To display the audit trail data for the specified options, click OK. To close the Display Options dialog box without changing the current settings, click Cancel.

To return to full display, click the Show All radio button and OK.

Updating the Audit Trail Window

ConnectView enables you to update the information displayed in the Audit Trail window so that it reflects the server's most recent audit trail information. This data is not updated automatically.

To refresh the data in the Audit Trail window, choose View > Update (F5). ConnectView replaces the data displayed in the Audit Trail window with the most up-to-date data from the current audit trail file.

Generating Audit Trail Reports

ConnectView enables you to generate audit trail reports with server and daily totals. These reports allow you to easily view and output formatted server and daily summaries of remote access service access and use.

NOTE: To limit the content of the report to a specified time period, user ID, port, port status, and service use the display options in the Audit Trail window before accessing the report. Due to table tool limitations, up to 8,000 audit trail records may be displayed at one time.

To generate an audit trail report, ensure that the desired server is selected and from any window choose File > Generate Report > Audit Trail. ConnectView opens an Audit Trail Report window with the report data. The Audit Trail window is also opened in the background.

NOTE: Closing the Audit Trail window also closes the Audit Trail Report window.

Customizing the Audit Trail Report

ConnectView allows you to specify which information appears in the Audit Trail Report window and in what order the data columns appear.

To customize the data display in the Audit Trail Report window, choose File > Report Preferences and click the Audit Trail tab button. The Report Preferences dialog box appears with the options for the Audit Trail Report window.

By default, the Audit Trail Report includes summary and detailed information. Detailed information appears in the following order:

- ◆ Entry time
- ◆ User ID

- ◆ Port name
- ◆ Service
- ◆ Description
- ◆ Connection ID (not selected)
- ◆ Event ID (not selected)

Clear the check boxes for the data you do not wish to appear in the report.

To change the order of the detailed information, select the desired field and click the Up or Down button.

To save your changes, click OK. The changes take effect the next time the Audit Trail Report window is opened and remain in effect until these options are changed. To close this dialog box without applying the changes, click the Cancel button.

Printing or Copying Audit Trail Report Data

ConnectView allows you to print or copy report data.

To print the audit trail report data, open an Audit Trail Report window and choose File > Print. ConnectView prints the displayed report.

To copy the audit trail report data, open an Audit Trail Report window and choose Edit > Copy. ConnectView copies the displayed report to the Windows clipboard.

Loading and Unloading Services

The remote access software provides the following three basic services:

- ◆ NASI Connection Service (NCS)
NCS provides PC and Mac* users dial-in capability with third-party access products and remote control technology. NCS also allows users to dial-out to host resources.
- ◆ AppleTalk* Remote Access Service (ARAS)
ARAS provides Mac users dial-in capability with remote node technology.
- ◆ Point-to-Point Protocol/Remote Node Service (PPPRNS)
PPPRNS provides Unix[®] and DOS users dial-in capability with remote node technology or ISDN connections.

ConnectView enables you to dynamically load and unload the available services on the current server.

NOTE: To load and unload services, you need ControlCommunity (SET) access rights. Refer to [Support for SNMP and ConnectView](#) for more information about setting community strings.

To load or unload a service, expand the server to display the desired service, select the desired service, and choose **Server > Load Service** or **Server > Unload Service**. ConnectView loads or unloads the selected service.

Setting Application Preferences

ConnectView provides several application preferences to enable you to customize the application for your environment. ConnectView preferences include

- ◆ Polling intervals to enable you to control how often the network is polled for data. This is especially useful to limit unnecessary traffic or traffic over slow networks. By default, the server polling interval is set to 5 minutes for each managed server.
- ◆ Grace periods to enable you to specify a minimum connection duration to be used for accounting and trend analysis data. By default, a grace period of 30 seconds is used for each service.
- ◆ SNMP options to enable you to set workstation community strings for individual servers and SNMP timeout values and retry values. By default, MonitorCommunity and ControlCommunity strings are set to public, the SNMP retry value is set to 2 retries, and the SNMP timeout value is set to 5 seconds.

NOTE: SNMP options are available only when ConnectView is run in standalone mode.

To change a ConnectView preference, choose **File > Preferences**. ConnectView opens the Preferences dialog box. Click the tab button for the desired option and specify the desired settings.

Setting Server Polling Intervals

The polling interval determines how often your network is polled for data. ConnectView displays data according to the server polling interval in the View All, View, Port Connections, and NCS Sessions windows. By default, the server polling interval is set to 5 minutes for each managed server. You can also force an immediate update of data by opening the desired window and then choosing **View > Update (F5)**.

NOTE: Data in the Port Status dialog box is updated every 2 seconds, independent of the server polling interval.

To change the polling intervals, click the Server Information tab in the Preferences dialog box. The polling options appear. Click the check box in the Polling? column for the desired servers, then enter the desired polling intervals in minutes in the Polling Interval column. Acceptable values include 1 to 60 minutes.

IMPORTANT: If you plan to manage many servers or servers over slow networks, consider using a high polling interval to reduce network traffic and improve network performance. In this case, you can always use the Update command (F5) to force an immediate update of the data as needed.

Either click another tab button to make additional changes or click OK to apply the changes and close the Preferences dialog box.

Click Cancel to close this dialog box without applying the changes.

Setting a Grace Period

ConnectView enables you to specify a minimum connection duration so that connections lasting less than the minimum duration are not used to calculate accounting and trend analysis data. By default, ConnectView sets the minimum connection duration at 30 seconds for each service.

To change the minimum connection duration, click the Grace Period tab button. The grace period options appear. Use the spin controls to set the desired grace period for each service. Valid settings include 0 to 999 seconds (approximately 17 minutes).

To make additional changes, click another tab button. To apply the changes and close the Preferences dialog box, click OK.

To close this dialog box without applying the changes, click Cancel.

Setting SNMP Options

ConnectView enables you to set workstation community strings for individual servers, SNMP time-out values, and SNMP retry values. By default, community strings on the ConnectView workstation are set for public access (monitor=public control=public). For SNMP GET and SET requests to be successful, the workstation community strings must match the community strings set on the managed server.

IMPORTANT: By default, SNMP.NLM on the server side sets the server's MonitorCommunity to public but disables access to the ControlCommunity.

To change the SNMP options, click the SNMP Options tab button in the Preferences dialog box. The SNMP options appear.

To make additional changes, click another tab button. To apply the changes and close the Preferences dialog box, click OK.

To close this dialog box without applying the changes, click Cancel.

Displaying and Using Trend Analysis Data

To access a Trend Analysis Data window, select a server in the View All window or a View window, or select a server name in the Server drop-down combo box in the left corner of the Tool Bar. Then, either click the Trend Analysis icon in the Tool Bar or choose Server > View Trend Analysis. ConnectView prompts you for starting and ending dates and then opens the Trend Analysis window for the specified period.

NOTE: Connections that terminate while the audit trail option is disabled and connections that terminate beyond the end date of the display period are not included in trend analysis data.

You can also open multiple views of the Trend Analysis window for the same server and the same display period by selecting the opened Trend Analysis window and choosing Window > New.

IMPORTANT: If you are accessing large amounts of data in the current audit trail file and/or archived files, displaying trend analysis data could require a substantial amount of time and memory. Also, if low memory conditions occur and Windows is configured to swap data to disk, this could increase the amount of time required to process the data.

Refer to the following procedures:

- ◆ Setting the Trend Analysis Display Options
- ◆ Using the Trend Analysis Split Window
- ◆ Saving Trend Analysis Data
- ◆ Outputting Trend Analysis Data

For sample Trend Analysis windows and explanations, see Interpreting Trend Analysis Data.

Setting the Trend Analysis Display Options

When you are viewing trend analysis data, ConnectView enables you to customize the display of data with several display options. These options appear in the Trend Analysis Display Options dialog box. The available options vary depending on which trend analysis category is selected.

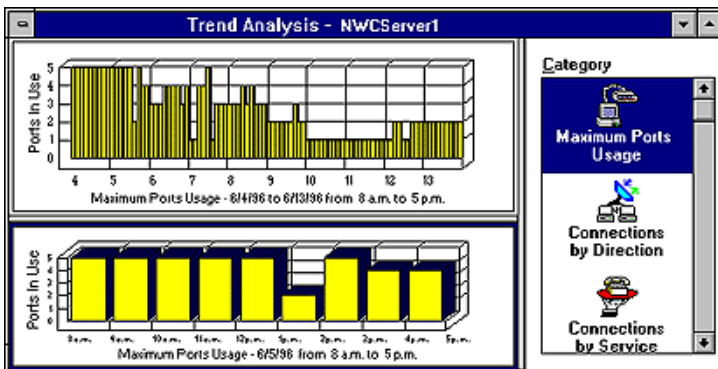
To access the Dialog boxes:Trend Analysis Display OptionsTrend Analysis Display Options dialog boxTrend Analysis Display Options dialog box, ensure that a Trend Analysis window is open and the desired graph is selected. Choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Option dialog box. Specify the desired options and click the OK button.

Using the Trend Analysis Split Window

ConnectView enables you to display two views of data from the same trend analysis category within one window, so you can easily compare data from the same category for different intervals.

To display a split trend analysis window, position the cursor over the upper gray border of the window (just under the Title Bar) until it changes shape to parallel lines with two arrows. Press and hold the left mouse button. Drag the border to the desired position and release the mouse button. Click the icon for the desired category. Figure 18 shows an example split window with maximum port usage data.

Figure 18 Trend Analysis Split Window



To limit the data display in either graph, select the desired graph. A dark border appears around the selected graph. Choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Options dialog box for the selected graph.

NOTE: If the Category list box is in focus and you have split windows, a dialog box appears so you can specify to which graph to apply the display options.

Saving Trend Analysis Data

ConnectView enables you to save trend analysis data to a file so that you can view trend analysis graphs independent of the server's audit trail and archived files.

To save trend analysis data, open the Trend Analysis window for the desired period and choose File > Save Trend Analysis. ConnectView prompts you for a path and filename and then saves the data for the specified period to a trend analysis file. Trend analysis files have a.TAD extension.

To access a previously saved trend analysis file, choose File > Open Trend Analysis. The File Open dialog box appears. Specify the desired trend analysis file (file with a.TAD extension) and click OK. ConnectView opens the Trend Analysis window and displays the saved data.

NOTE: Use the DOS command or Windows File Manager to delete trend analysis files.

Outputting Trend Analysis Data

ConnectView enables you to print the graphs from any Trend Analysis window, copy the trend analysis graph in bit map or text format to the Windows clipboard, or export trend analysis data in tab-delimited format. This capability allows you to create and maintain trend analysis records for detailed reports and analyses.

Copying Trend Analysis Data

To copy graphs from a Trend Analysis window in text or bit map format, select the category you wish to copy. A dark border appears around the selected graph. Choose Edit > Copy. ConnectView prompts you to choose graph or bit map format. Select the desired format and click OK.

ConnectView copies the graph data in the specified format to the Windows clipboard. You can then paste the text or bit map into other applications.

Printing Trend Analysis Data

To print a graph from a Trend Analysis window, select the category you wish to print. A dark border appears around the selected graph. Choose File > Print. ConnectView prints the selected graph.

IMPORTANT: To print graphs, some printers could require configuration changes.

Exporting Trend Analysis Data

To export trend analysis data, select the trend analysis category you wish to export. A dark border appears around the selected graph. Choose File > Export. ConnectView prompts you to specify a filename and path. Specify the desired path and click the OK button.

ConnectView exports data in tab-delimited format to the specified file. You can then import the data into other applications for additional analysis.

Interpreting Trend Analysis Data

This section contains sample Trend Analysis windows to help you interpret and analyze the trend analysis data you collect.

NOTE: The grace period or minimum connection duration needed for a connection to be included as trend analysis data can be set in the Grace Period page of the Preferences dialog box. To access this dialog box, choose File > Preferences. By default, the grace period is set at 30 seconds.

Refer to the following descriptions of the types of graphs available:

- ◆ Maximum Ports Usage Graphs
- ◆ Connections by Direction Graphs
- ◆ Connections by Service Graphs
- ◆ Connection Attempts Graphs
- ◆ Connection Duration Graphs
- ◆ Traffic Statistics Graphs
- ◆ Usage by Media Graphs

Maximum Ports Usage Graphs

Maximum ports usage graphs show the maximum number of ports in use simultaneously during the display period to enable you to monitor port

utilization, perform capacity planning, and evenly distribute port usage across Novell Internet Access Server 4.1 servers running the remote access software.

To obtain this data, ConnectView checks the recorded status of each port for each minute of the display period. If a port was accessed during a minute, ConnectView counts the port as used during that minute. Then, ConnectView compares the number of ports used during each minute for a 60 minute interval and selects the highest value as the maximum port usage for that hour. This process is repeated for each hour of the display period. The highest hourly value within a 24 hour period is then used as the daily maximum port usage.

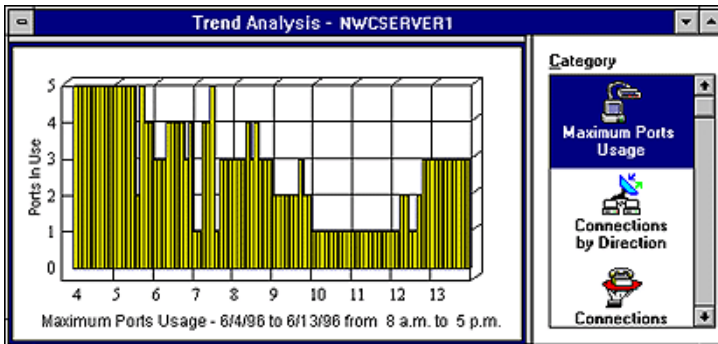
NOTE: Because it is unlikely a port will be used more than once per minute, ConnectView uses a minute interval to check for port usage. If a port happens to be used more than once during a minute, the port usage data will be inaccurate. Also, ConnectView considers only complete connections, so if a port is in use when the port usage data is calculated, it will not be counted.

If a port is accessed more than once per minute, ConnectView counts it as being used only once during the minute interval.

To display maximum ports usage data, click the Maximum Ports Usage icon in the Category list box. By default, data is displayed at hourly intervals from 8 a.m. to 5 p.m. for each day for the specified dates.

Figure 19 shows a sample Trend Analysis window for ports usage on server NWCServer1. To change the time of day and display interval, ensure the desired graph is selected and choose View > Display Options (F4).

Figure 19 Example Trend Analysis Window for Maximum Ports Usage



From this example, you can see that the maximum ports usage on the server NWCServer1 is displayed from 8:00 a.m. to 5:00 p.m. for 10 days (6/4/96 to 6/13/96). This data indicates that a maximum of five ports were in use simultaneously on 6/4. Only one port was used on 6/10 and 6/11. If the remote access software is licensed for eight ports, this data suggests that port utilization is greater than 50 percent of the available port licenses for more than two days.

NOTE: Maximum ports usage does not reflect the number of sessions using the ports.

Setting Display Options for Maximum Ports Usage, Connections by Direction, Connections by Service, and Connection Attempts Graphs

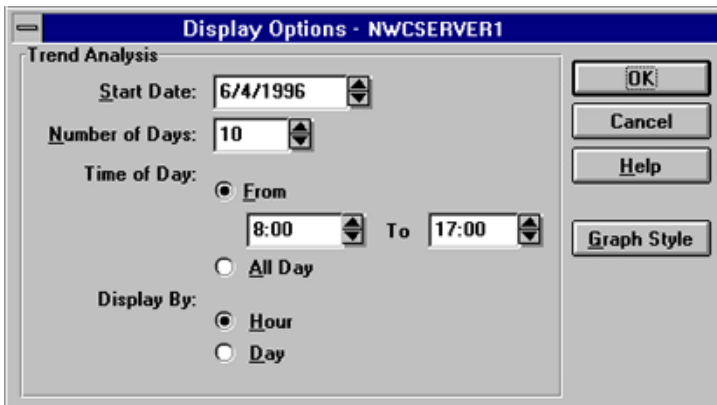
When you are viewing maximum ports usage, connections by direction, connections by service, and connection attempts data, ConnectView enables you to customize the display of data within the originally specified start and end dates by changing the

- ◆ Start date
- ◆ Number of days for which data is displayed
- ◆ Time of day for which data is displayed (individual hours or all day [24 hours])
- ◆ Interval by which data is displayed (hourly or daily)
- ◆ Graph style

IMPORTANT: Displaying connection data by hour shows the number of connections that were established during the displayed hours. If a connection crosses hours, the connection will be counted in each hourly interval that it crosses. In this case, the total number of connections could exceed the total when the data is displayed by a daily interval.

To access the Trend Analysis Display Options dialog box, ensure that the desired graph is selected and choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Option dialog box, shown in Figure 20.

Figure 20 Example Trend Analysis Display Options



Specify the desired options and click the OK button.

Connections by Direction Graphs

Connections by Direction graphs help you determine the number of dial-in, dial-out, and dialback connections made during a specified period, monitor resource usage, and evenly distribute dial-in, dial-out, and dialback users for more efficient performance.

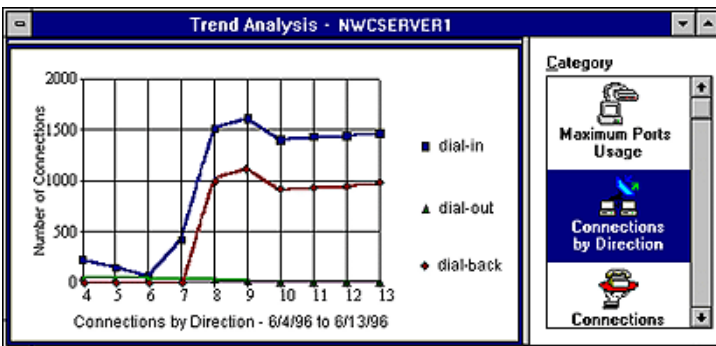
ConnectView counts the number of valid dial-in, dial-out, and dialback connections that occurred during each hour of the display period. The hourly totals for each twenty-four hour period within the display period are then added together for the daily totals. For a connection to be valid for this trend analysis category, both a start connection record and an end connection record must be found within the display period.

IMPORTANT: Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Service, Connection Attempts, and Connection Duration categories. Connection Direction graphs require both a start connection record and an end connection record within the display period. These other categories require that valid connections have only an end connection record within the display period.

To display connections-by-direction data, click the Connections by Direction icon in the Category list box. By default, this graph shows the number of connections by direction on a daily interval.

Figure 21 shows a sample Trend Analysis window with connections by direction data.

Figure 21 Example Trend Analysis Window for Connections by Direction



In this example, you can see the number of dial-in, dial-out, and dialback connections made between 6/4/96 and 6/13/96 on server NWCServer1. This data indicates that approximately 1,500 dial-in connections and 1,000 dialback connections were made each day between 6/8 and 6/13, while there were few dial-out connections during the display period.

To change the display options for connections by direction data, choose View > Display Options (F4). For an example Display Options dialog box, see Figure 20 on page 252.

Connections by Service Graphs

Connections by Service graphs provide data to enable you to track service usage and proactively plan for service expansion.

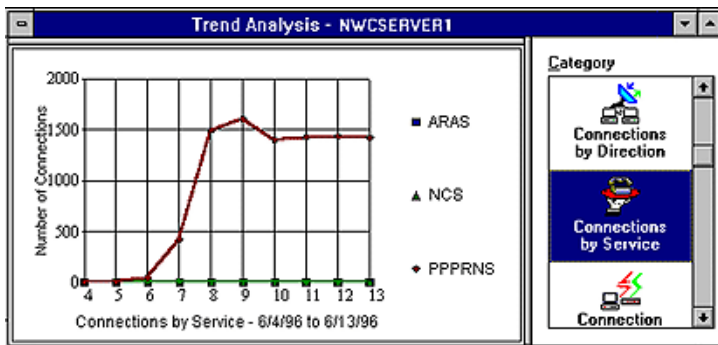
ConnectView counts the number of valid connections for each service that occurred during each hour of the display period. The hourly totals for each twenty-four hour period within the display period are then added together for the daily totals. For a connection to be valid for this trend analysis category, only an end connection record must be found within the display period.

IMPORTANT: Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Direction, Traffic Statistics, and Usage by Media categories. Connections by Service graphs require only an end connection record within the display period. These other categories require that valid connections have both a start connection record and an end connection record within the display period.

To display connections-by-service data, click the Connection by Service icon in the Category list box. By default, this graph displays the daily number of connections by service.

Figure 22 shows a sample Trend Analysis window with connections by service data.

Figure 22 Example Trend Analysis Window for Connections by Service



In this example, you can see that connections were made using the PPRNS service from 6/6/96 to 6/13/96 on the server NWCServer1. No AppleTalk

Remote Access Services (ARAS) or NASITM Connection Service (NCS) connections occurred throughout the period.

NOTE: The remote access services that are configured and loaded on the server or recorded in the audit trail file appear in this graph.

To change the display options for connections by service data, ensure the desired graph is selected and choose View > Display Options (F4). For an example Display Options dialog box, see Figure 20 on page 252.

Connection Attempts Graphs

Connection attempts graphs show the number of normal connections, abnormal connections, dial-out failures, and login failures on a server. These graphs help you monitor how successful users are in establishing their connections and assess connection and security problems during this period. Table 32 describes the connection attempt categories.

Table 32 Connection Attempt Categories

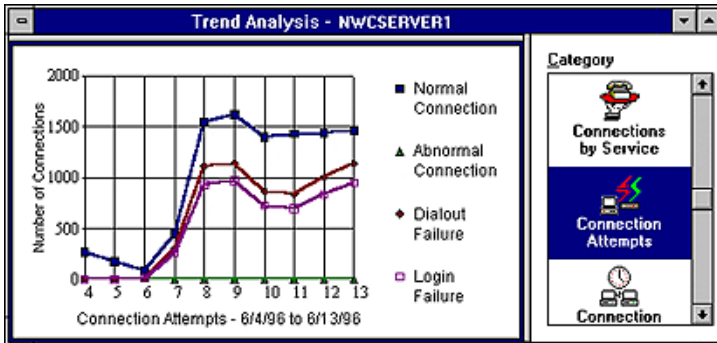
Connection Category	Description
Normal Connection	Successful dial-in, dial-out, and dialback connections that terminated in an orderly fashion.
Abnormal Connection	Connections that were terminated in a disorderly fashion, without user initiation. Possible causes are line failure, transmission error, maximum idle time or user connection time exceeded limit, port or session reset by administrator, or service or driver unloaded.
Dial-out Failure	Dial-out or dialback connection failed. Possible causes are that the number was busy, port or service was unavailable, or access was restricted.
Login Failure	User login attempt failed. Possible causes are invalid username or password, unauthorized NetWare or remote access software access, or that the login was disabled.

IMPORTANT: Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Direction, Traffic Statics, and Usage by Media categories. Connection Attempts graphs require only an end connection record within the display period. These other categories require that valid connections have both a start connection record and an end connection record within the display period.

To display connection attempts data, click the Connection Attempts icon in the Category list box. The connection attempts graph shows daily connection attempts from the specified start date to the specified end date.

Figure 23 shows a sample Trend Analysis window with connection attempts data.

Figure 23 Example Trend Analysis Window for Connection Attempts



In this example, you can see that there were approximately 1,500 successful connections each day between 6/8/96 and 6/13/96 on the server NWCServer1. Also, notice that during this period a number of dial-out failures and login failures occurred. There were no abnormal connections during the display period.

To change the display options for connection attempts data, ensure that the desired graph is selected and choose View > Display Options (F4). For an example Display Options dialog box, see Figure 20 on page 252.

Connection Duration Graphs

Connection duration graphs enable you to track connection durations and patterns in connection durations. This data can help you to set duration standards and monitor the amount of time users are connected to the remote access software.

For each day of the display period, ConnectView counts the number of connections with connected times within each duration interval. Connection

times are calculated in seconds and then converted to minutes. The number of connections within each connection duration interval provides the daily totals. For a connection attempt to be valid for this trend analysis category, only an end connection record must be found within the display period.

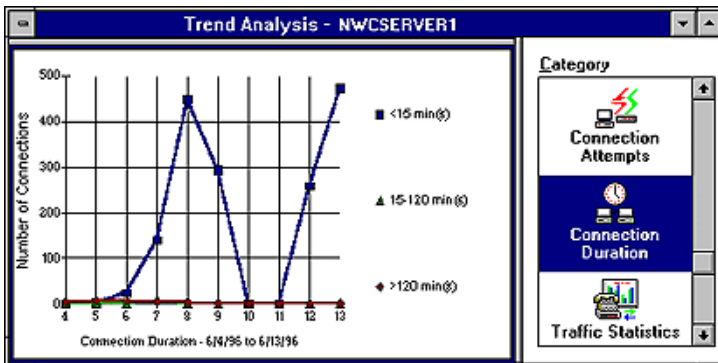
IMPORTANT: Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Direction, Traffic Statics, and Usage by Media categories. Connection Duration graphs require only an end connection record within the display period. These other categories require that valid connections have both a start connection record and an end connection record within the display period.

To display connection duration data, click the Connection Duration icon in the Category list box.

NOTE: This data can be viewed only on a daily basis.

Figure 24 shows a sample Trend Analysis window with connection duration data. By default, this graph shows the number of connections established for less than 15 minutes, between 15 and 120 minutes (2 hours), and more than 120 minutes. Also, data is displayed daily from the specified start date to the specified end date.

Figure 24 Example Trend Analysis Window for Connection Duration



In this example, you can see the duration of connections between 6/4/96 and 6/13/96 on the server NWCServer1. This data indicates that almost all connections were established for less than 15 minutes.

Setting Display Options for Connection Duration Graphs

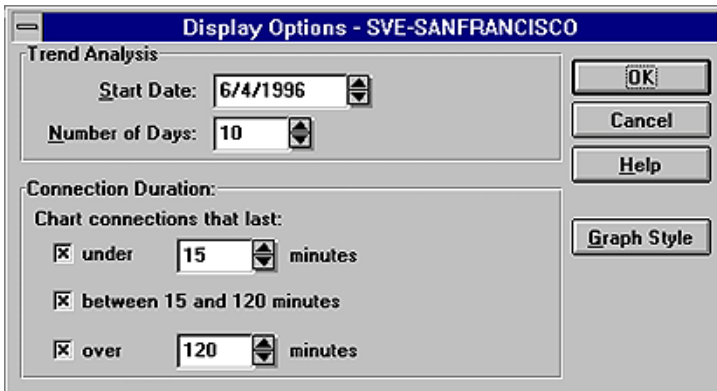
When you are viewing connection duration data, ConnectView enables you to customize the display of data within the originally specified start and end dates by changing the

- ◆ Start date
- ◆ Number of days for which data is displayed
- ◆ Under (less than) duration setting
- ◆ Over (greater than) duration setting
- ◆ Graph style

NOTE: This data can be displayed only in daily intervals.

To access the Trend Analysis Display Options dialog box, ensure that a connection duration graph is selected and choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Options dialog box, shown in Figure 25. Specify the desired options and click the OK button.

Figure 25 Example Display Options(Connection Duration)



Traffic Statistics Graphs

Traffic statistics graphs help you monitor traffic patterns, anticipate periods of heavy or light traffic, and more evenly distribute traffic across your remote access servers.

These graphs show the number of connections in groups of the average traffic patterns. Traffic consists of the number of kilobytes or kilopackets sent and received per second. To determine the level of traffic, the total number of bytes or packets is divided by the number of seconds in the connection duration. The resultant rates of traffic are then grouped according to intervals. For a connection to be valid for this trend analysis category, both a start connection record and an end connection record must be found within the display period.

IMPORTANT: Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Service, Connection Duration, and Connection Attempts categories. Traffic Statistics graphs require both a start connection record and an end connection record within the display period. These other categories require that valid connections have only an end connection record within the display period.

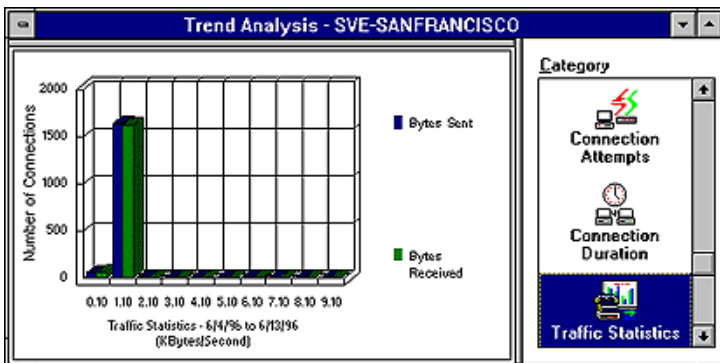
By default, the traffic intervals start at 0.1 KBps (100 bytes) and continue for 10 intervals. The display options allow you to adjust these intervals and display values and to display data for Kilopackets sent and received.

NOTE: This data can be displayed only in daily intervals.

To display traffic statistics, click the Traffic Statistics icon in the Category list box.

Figure 26 shows a sample Trend Analysis window with traffic statistics data.

Figure 26 Example Trend Analysis Window for Traffic Statistics



In this example, you can see that all connections between 6/4/96 and 6/13/96 on the server NWCServer1 had less than 2 KBps of traffic.

Setting Display Options for Traffic Statistics

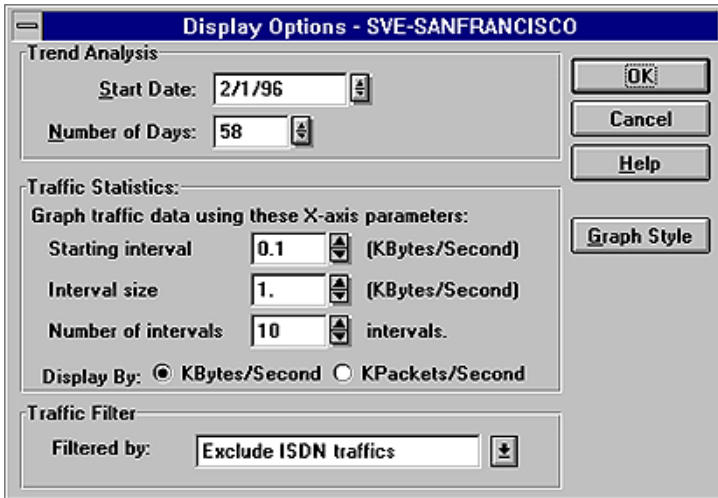
When viewing traffic statistics data, you can customize the display of data based on the originally specified start and end dates by changing the

- ◆ Start date
- ◆ Number of days for which data is displayed
- ◆ Traffic statistics
- ◆ Starting interval
- ◆ Interval size
- ◆ Number of intervals
- ◆ Data display for kilobytes per second (KBytes/Second) or kilopackets per second (KPkets/Second)
- ◆ Traffic filter (ISDN only, ISDN and others, non-ISDN only)
- ◆ Graph style

NOTE: This data can be displayed only in daily intervals.

To access the Trend Analysis Display Options dialog box, ensure that a traffic statistics graph is selected and choose View > Display Options (F4). ConnectView opens the Trend Analysis Display Option dialog box, shown in Figure 27. Specify the desired options and click the OK button

Figure 27 Example Display Options(Traffic Statistics)



Usage by Media Graphs

Usage by media graphs help you monitor media usage, analyze media usage patterns, and distribute media utilization across your remote access servers.

These graphs contain pie charts that show the percentage of data traffic and the percentage of connections by media groups. Media groups are defined as analog, ISDN, X.25, and other. Other refers to remote access connections that use a media type different from those listed.

NOTE: Media type is not supported by NetWare Connect 2.0 servers. Connections to NetWare Connect 2.0 servers will show the media type as other.

ConnectView counts the amount of traffic in kilobytes and the number of connections for each media type for each day of the display period. The resultant totals are then divided by the total amount of traffic and the total number of connections, respectively. For a connection to be valid for this trend analysis category, both a start connection record and an end record must be found within the display period.

IMPORTANT: Within the same display period, the number of valid connections for this category might not match the number of valid connections for the Connections by Service, Connection Duration, and Connection Attempts categories. Usage by Media graphs require both a start connection record and an end connection record within the

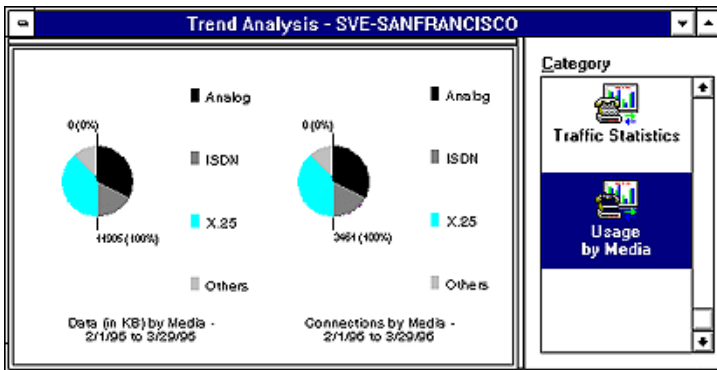
display period. These other categories require that valid connections have only an end connection record within the display period.

To display media usage data, click the Usage by Media icon in the Category list box.

NOTE: This data can be displayed only in daily intervals. You can choose View > Display Options to adjust the dates of the displayed data.

Figure 28 shows a sample Trend Analysis window with usage by media data.

Figure 28 Example Trend Analysis Window for Usage by Media



In this example, you can see that most data traffic (40%) on the server San Francisco during the period 2/1/97 to 3/29/97 was analog traffic. Also, most connections (40%) were established for analog connections.

NOTE: Because the numerical values for traffic and connections are displayed in the graphs, the hot graph feature is disabled for this trend analysis category.

Setting Up Accounting Profiles and Generating Billing Charges

Accounting profiles define how charges will be calculated with a billing formula and rates. First, specify the desired billing formula (Step 1). Then enter the desired rates (Step 2). After the billing formula and rates have been entered, view sample charges to verify that the formula and rates are correct (Step 3).

A billing formula can be based on one or more of the following categories

- ◆ Rate per minute based on connection duration

Length of the connection multiplied by the rate per minute, based on:

- ◆ Time-of-day

Intervals of 60 minutes from 0:00 a.m. to 11:59 p.m., for each day of the week and holidays

- ◆ Baud rate

Connection speeds in bits per second (bps)

- ◆ Port

Port names and available speeds

- ◆ Services

Remote access services available on the current server

- ◆ Rate per connection

Rate for each connection based on baud rate, service, or port

- ◆ Overhead Rate

A flat-rate charge applied to the users assigned to the profile with valid remote access software connections. A check box is available to apply this charge to all users assigned to the profile, including those without valid connections.

After the billing formula and rates are specified, accounting profiles are saved as files with .NCP extensions. Accounting profiles can be saved locally or on a network drive. You can then assign users to the saved profiles.

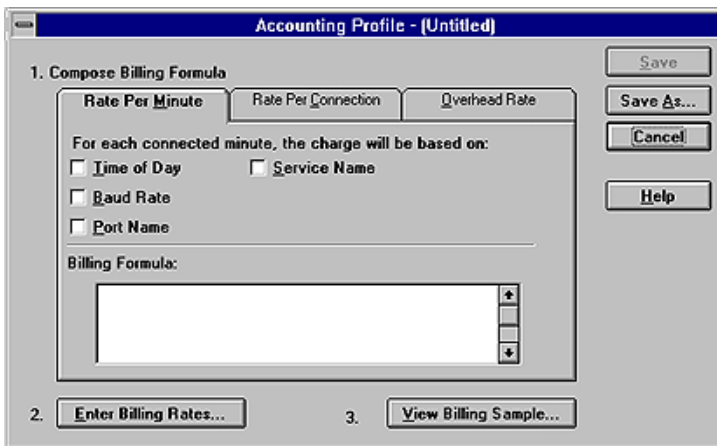
NOTE: To delete unwanted accounting profiles, use the DOS command or Windows File Manager.

You can create multiple accounting profiles and apply them to different users as necessary. By default, ConnectView creates an accounting profile called DEFAULT.NCP, with no billing formula or rates. This default accounting profile is assigned to all users. However, you must specify the desired billing formula and enter the billing rates to generate meaningful charges.

To access the Accounting Profile dialog box, select a server icon in the View All window or a View window, or select a server name in the Server drop-down combo box in the left corner of the Tool Bar. Then, choose Accounting > Create Profile or, if an accounting profile has already been saved,

Accounting > Edit Profile. ConnectView opens the Accounting Profile dialog box, shown in Figure 29.

Figure 29 Accounting Profile Dialog Box



In this dialog box, you can use the tab buttons to specify the desired billing formula. The current billing formula appears in the lower section of this dialog box.

NOTE: The display in the Billing Formula list box changes as you select or deselect the desired charges, but cannot be edited.

ConnectView enables you to create or change billing formulas based on rate tables for time of day, baud rate, port, and service, as well as an overhead rate.

For more information on billing, refer to:

- ◆ Setting the Rate per Minute Charge
- ◆ Setting the Rate per Connection Charge
- ◆ Setting the Overhead Rate Charge
- ◆ Entering Billing Rates
- ◆ Viewing Sample Billing Charges

- ◆ Assigning Accounting Profiles and Account Numbers to Users
- ◆ Displaying Billing Charges
- ◆ Printing, Copying, and Exporting Accounting Data

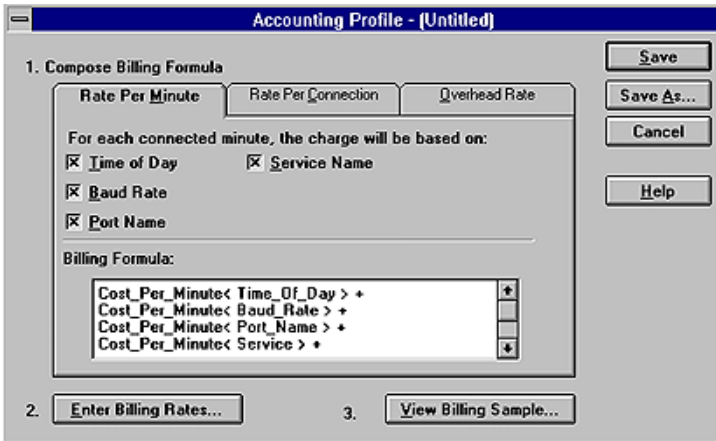
Setting the Rate per Minute Charge

Rate per minute is a charge applied to users based on any or all of the following costs:

- ◆ Time of day the connection was made
- ◆ Baud rate or connection speed
- ◆ Individual port accessed
- ◆ Remote access service used

To access the Rate Per Minute settings, click the Rate Per Minute tab button in the Accounting Profile dialog box. ConnectView displays the rate per minute options, shown in Figure 30.

Figure 30 Account Profile Dialog Box with Rate Per Minute Options



Click the desired check boxes for the rate tables you want to use. Click a tab button to display additional billing formula options.

To close this dialog box and accept all changes, click the Save or Save As button. To close this dialog box without applying any changes, click the Cancel button.

NOTE: To enter rates for the rate per minute based on baud rate, port name, time of day, and type of service, click the Enter Billing Rates button (Step 2) and then click the desired tab buttons.

Setting the Rate per Connection Charge

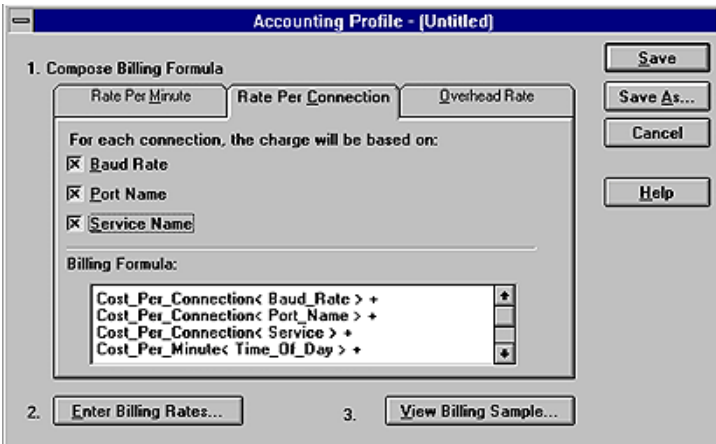
Rate per connection is a flat-rate charge based on any or all of the following:

- ◆ Baud rate of the connection
- ◆ Individual port and connection speed used in the connection
- ◆ Remote access service used for the connection

This rate is applied to all users each time they connect to the current remote access software, regardless of the duration of the connection.

To access the Rate Per Connection settings, click the Rate Per Connection tab button in the Accounting Formula dialog box. ConnectView displays the rate per connection options, shown in Figure 31.

Figure 31 Accounting Profile Dialog Box with Rate per Connection Options



Click the desired check boxes for the rate tables you want to use.

To close this dialog box and accept all changes, click the Save or Save As button. To display additional billing formula options, click a tab button. To close this dialog box without applying any changes, click the Cancel button.

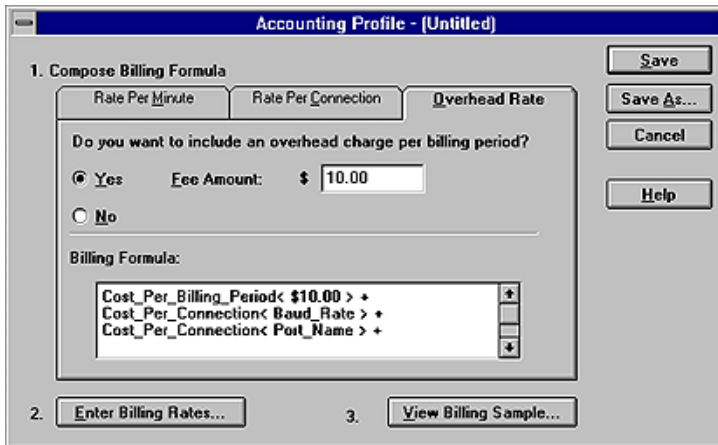
NOTE: To enter rates for the rate per connection based on baud rate, port name, and type of service, click the Enter Billing Rates button (Step 2) and then click the desired tab buttons.

Setting the Overhead Rate Charge

Overhead rate is a flat-rate charge applied to all remote access software users assigned to the profile during the specified billing period. Alternatively, this charge can be applied to all users assigned to the profile, including those without valid remote access connections during the billing period.

To enter a rate per billing period, click the Overhead Rate tab button. ConnectView displays the overhead rate options, shown in Figure 32.

Figure 32 Accounting Profile Dialog Box with Overhead Rate Options



If you want to use a flat-rate access fee or rate per billing period charge, click the Yes radio button and enter the desired charge.

NOTE: Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

To close this dialog box and accept all changes, click the OK button. To display additional billing formula options, click a tab button. To close this dialog box without applying any changes, click the Cancel button.

Entering Billing Rates

ConnectView enables you to enter rates (Step 2) for any or all of the following:

- ◆ Time of day for 24-hour intervals for each day and holiday
- ◆ Baud rates by connection speeds on a per minute or per connection basis
- ◆ Individual ports by port speeds on a per minute or per connection basis
- ◆ Remote access services on a per minute or per connection basis

NOTE: Time of day and holiday rates apply only to the rate per minute billing formula.

IMPORTANT: Because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections. Because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate and port name rate tables do not apply to these connections.

Setting Up a Time of Day Rate Table

Time of day rate tables can be used to specify different costs per minute based on the hour of the day, the day of the week, and whether or not it is a holiday.

To set up a time of day rate table, click the Enter Billing Rates button in the Accounting Profile dialog box. ConnectView displays the Time of Day rate table and the tab buttons for additional rate tables, shown in Figure 33.

Figure 33 Rate Tables (Time of Day) Dialog Box

Time of Day	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holidays
0:00 A.M. - 0:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
1:00 A.M. - 1:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
2:00 A.M. - 2:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
3:00 A.M. - 3:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
4:00 A.M. - 4:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
5:00 A.M. - 5:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
6:00 A.M. - 6:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
7:00 A.M. - 7:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
8:00 A.M. - 8:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
9:00 A.M. - 9:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30
10:00 A.M. - 10:59 A.M.	\$0.20	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.20	\$0.30

The example Time of Day rate table lists the time in hourly intervals from 0:00 a.m. to 23:59 p.m., and charges for each interval for each day of the week.

Enter the desired rates.

NOTE: To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

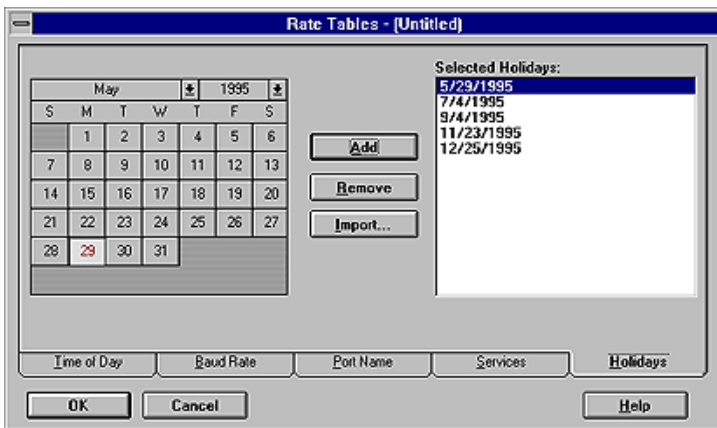
Also, enter additional rates that apply to holidays under the Holidays column. The Holidays column is the far right column.

Setting Holidays

When specifying time of day rates, ConnectView enables you to specify holidays of the year to receive special rates. When a connection occurs on a day assigned to be a holiday, holiday rates are used in place of any other rates. Enter the desired holiday rates in the Holidays column in the Time of Day rate table.

Click the Holidays tab button. ConnectView displays the holiday calendar in the Rate Tables dialog box, shown in Figure 34.

Figure 34 Rate Tables (Holiday Calendar) Dialog Box



To include dates as holidays, either double-click them in the calendar or select the desired holiday dates and click the Add button. To remove dates as

holidays, either double-click them in the Selected Holidays list or select any unwanted dates and click the Remove button.

To copy holiday settings from a previously saved profile, click the Import button. Importing holidays from another profile replaces the current holiday settings with the imported settings.

To close this dialog box and apply the holiday changes, click the OK button. To display additional accounting profile options, click a tab button.

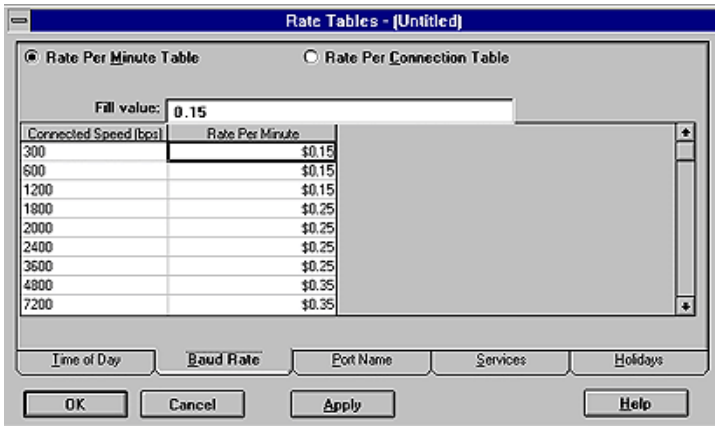
Setting Up a Baud Rate Table

ConnectView enables you to create a rate table based on cost per minute or cost per connection for baud rates used for a connection (connection speeds).

NOTE: Because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate or port name rate tables do not apply to these connections. Also, because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections.

To create a rate table for baud rates, click the Baud Rate tab button. ConnectView displays the rates in the Rate Tables (Baud Rate) dialog box, shown in Figure 35.

Figure 35 Rate Tables (Baud Rate) Dialog Box



Click the Rate Per Minute Table or Rate Per Connection Table radio button and enter the desired rates for the connection speeds in the rate column.

NOTE: To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

To close this dialog box and apply all rate changes, click the OK button. To display additional accounting profile options, click another tab button.

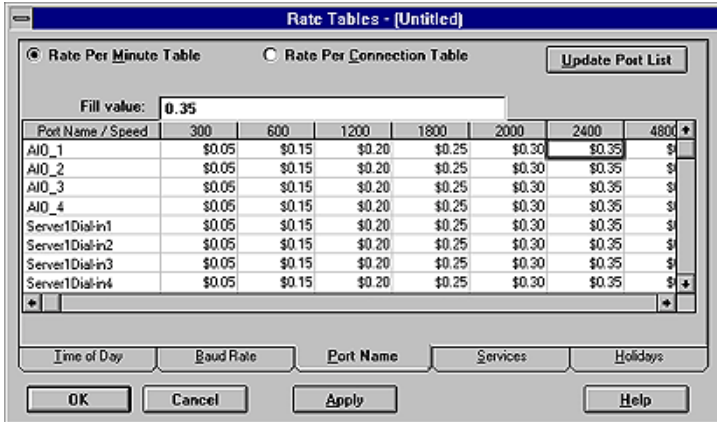
Setting Up a Port Rate Table

ConnectView enables you to create a rate table based on cost per minute or cost per connection for individual port access on the current server.

NOTE: Because an AIO PAD port cannot report the baud rate used for its connections, the rates specified in the baud rate or port name rate tables do not apply to these connections. Also, because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections.

To create a rate table for the ports, click the Port Name tab button. ConnectView displays the rates for the different speed on a port in the Rate Tables (Port Name) dialog box, shown in Figure 36.

Figure 36 Rate Tables (Port Name) Dialog Box



Click either the Cost Per Minute Table or Cost Per Connection radio button and enter the desired rates for each port and port speed. To update the list of available ports to match the available ports on the current server, click the Update Port List button.

NOTE: To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

To close this dialog box and apply all rate changes, click the OK button. To display additional accounting profile options, click another tab button.

Setting Up a Service Rate Table

ConnectView enables you to create a rate table based on cost per minute or cost per connection for each remote access service on the current server.

To create a rate table for the supported services, click the Services tab button. ConnectView displays the service rates in the Rate Tables (Services) dialog box, shown in Figure 37.

Figure 37 Rate Tables (Services) Dialog Box

Service	Rate Per Minute
ARAS	\$0.25
NCS	\$0.35
PPPRNS	\$0.30

Click the Rate Per Minute Table or the Rate Per Connection Table radio button and enter the desired rates in the rate column. To update the list of available services on the current server, click the Update Service List button.

NOTE: To enter the same amount in multiple cells, highlight the desired cells and enter the desired rate in the Fill value edit box. Click the Apply button. This fills the highlighted cells with the entered rate. Rates must begin with an integer, for example 0.50 or 1.20. A leading decimal point will not be accepted.

To close this dialog box and apply all rate changes, click the OK button. To display additional accounting profile options, click another tab button.

Viewing Sample Billing Charges

ConnectView allows you to view sample billing charges based on the current billing formula, so that you can quickly evaluate the specified billing formula and the specified rates.

To access the View Sample dialog box, click the View Sample button in the right side of the Accounting Profile dialog box. ConnectView opens the View Sample dialog box, shown in Figure 38.

Figure 38 View Sample Dialog Box

The screenshot shows a dialog box titled "View Sample - (Untitled)". It contains a "Billing Formula:" section with a list of cost components and their rates, and an "Example:" section showing a sample calculation for a billing period from 09/01/96 to 10/01/96.

Billing Formula:

- Cost_Per_Billing_Period < \$10.00 > +
- Cost_Per_Minute < Time_Of_Day > +
- Cost_Per_Minute < Baud_Rate > +
- Cost_Per_Minute < Port_Name > +
- Cost_Per_Minute < Service > +

Example:

During the billing period from 09/01/96 to 10/01/96, there is a connection made by JMOBILE

on **Friday** A Holiday

connecting from **9:00** to **17:00** \$ 30.00

at the speed of **300** \$ 120.00

on port **AIO_1** \$ 24.00

using service **PPRNS** \$ 120.00

Overhead charge for the billing period \$ 10.00

Total Charge Per Billing Period \$ 304.00

Use the spin controls to change the time of day, click the A Holiday check box to specify holiday charges, and use the combo boxes to select a connection time, baud rate, port, and/or service. ConnectView displays sample billing charges based on the current billing formula and rate tables. The current billing formula is displayed in the upper section of the dialog box.

IMPORTANT: Remote Node Service (RNS) connections that fail to log in could be included in the billing charges because a start and end record could still be logged. Because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to NCS dial-out connections. Also, because an AIOPAD port cannot report the baud rate used for its connections, the rates specified in the baud rate or port name rate tables do not apply to AIOPAD connections.

To close this dialog box, click the Close button.

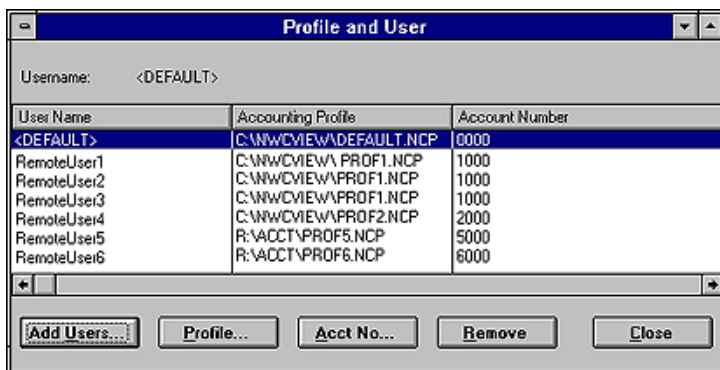
Assigning Accounting Profiles and Account Numbers to Users

ConnectView enables you to assign users to the saved accounting profiles in the Profile and User window.

To assign users to your accounting profiles, choose Accounting > Assign Profile to Users. ConnectView opens the Profile and User window, shown in Figure 39.

NOTE: By default, ConnectView creates the DEFAULT.NCP profile with account number 0000 and assigns this profile to all users (<DEFAULT>). This profile does not initially contain any billing formula or rates. The profile can be modified using Accounting > Edit Profile, but cannot be removed from the Profile and User window.

Figure 39 Profile and User Window



NOTE: No charges are applied for accounting profiles that are unavailable or cannot be found.

Adding Users and Removing Users from a Profile Assignment

You might want to assign users to different accounting profiles to enable you to apply different billing charges to different users.

To select users, click the Add Users button. ConnectView opens the Add Users dialog box, shown in Figure 40.

Figure 40 Add Users Dialog Box



To select users from the current Novell Directory Services™ (NDS™) tree, click the From DS radio button in the User List Source section. Then, either double-click the desired usernames in the Assigned Users list box or select the desired context or usernames in the Unassigned Users list box and click the Add button.

NOTE: If you assign accounting profiles using the bindery username jsmith, then record transactions using the complete NDS context (jsmith.eng.xyzcorp) the transactions will not match the bindery username (jsmith) assigned to the accounting profile and the default accounting profile will be used. NDS usernames are different than bindery usernames.

You can either double-click the objects or use the Collapse/Expand button to browse the tree and select the desired users. You can use the arrow buttons to navigate the tree.

NOTE: To select multiple users, press and hold the left mouse button while dragging the selection over the desired usernames or press and hold Ctrl while clicking the usernames. Selecting multiple users is not possible when you select users from an NDS tree.

To remove users, select the desired usernames in either the Profile and User window or the Assigned Users list box and click the Remove button.

When the desired users have been selected, click the OK button to close this dialog box and add or remove the users to the Profile and User window. To close this dialog box without applying any changes, click the Cancel button.

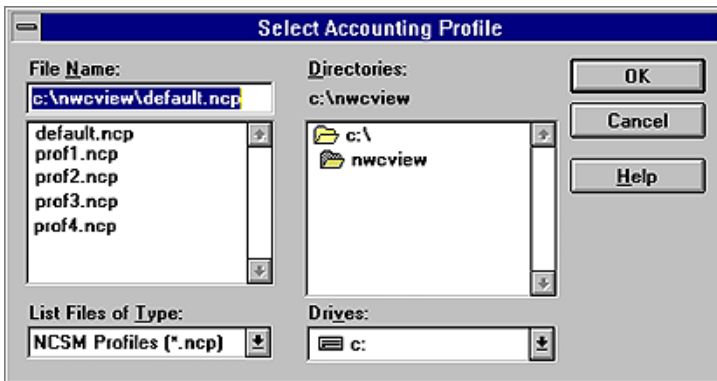
Selecting an Accounting Profile

To select a different accounting profile for a user, select the desired usernames and click the Profile button.

NOTE: To select multiple users, press and hold the left mouse button while dragging the selection over the desired usernames or press and hold Ctrl while clicking the usernames.

ConnectView opens the Select Accounting Profile dialog box, shown in Figure 41.

Figure 41 Select Accounting Profile Dialog Box



Use the file options to specify the desired drive, path, and accounting profile filename. By default, accounting profiles are stored in the \NWCVIEW directory.

To apply the accounting profile to the selected users, click the OK button. To close this dialog box without applying the profile, click the Cancel button.

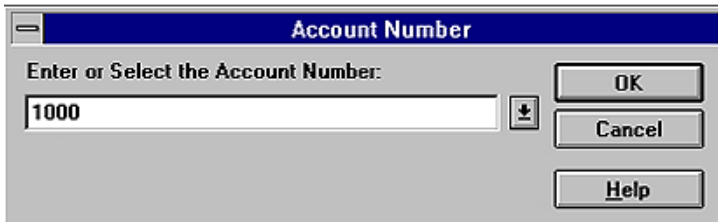
Setting Up Account Numbers

To set up or change the account number assigned to a user, select the desired usernames and click the Acct No button.

NOTE: To select multiple users, press and hold the left mouse button while dragging the selection over the desired usernames or press and hold Ctrl while clicking the usernames.

ConnectView opens the Account Number dialog box, shown in Figure 42.

Figure 42 Account Number Dialog Box



Enter the desired account number and click the OK button. Account numbers can be up to 38 alphanumeric characters, including mixed case and special characters. ConnectView applies the entered account number to the selected users.

To close this dialog box without applying the account number, click the Cancel button.

Displaying Billing Charges

ConnectView enables you to generate and display billing charges based on the accounting profiles assigned to users and remote access usage.

IMPORTANT: The audit trail file and/or archived files must be available for the display period to display accounting data. Also, ensure that the BSPXCOM.NLM file is loaded on the managed servers and the BREQUEST.EXE program file is running on the ConnectView workstation.

Only connections that begin and terminate during the display period (connections that have both a valid start record and end record) are considered in accounting data. RNS connections that fail to log in might be included in the billing charges because a start record and end record might still be logged. Because NCS cannot report the baud rate used for its dial-out connections, baud rate and port name charges do not apply to the NCS dial-out connections. Also, because a connected speed is not available for connections using an AIOPAD port, the rates specified in the baud rate and port name rate tables do not apply to AIOPAD connections.

NOTE: Connections with a duration less than the grace period, the minimum connection duration, are not included in accounting data. By default, the grace period is set to 30 seconds. To change the grace period, choose File > Preferences and click the Grace Period tab button.

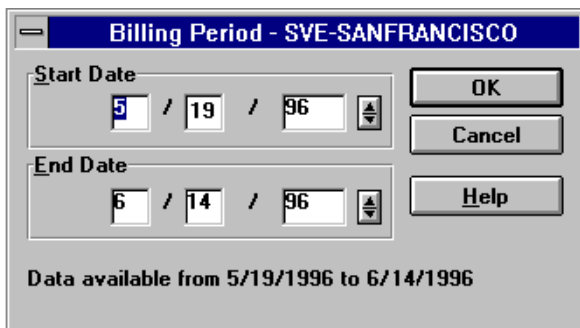
After accounting profiles are assigned and connection data is available, accounting data can be displayed in an accounting log, with data listed by username or account number or in an accounting report.

IMPORTANT: If you are accessing large amounts of data in the current audit trail file and/or archived files, displaying accounting data could require a substantial amount of time and memory. This is especially so if low memory conditions occur and Windows begins to swap data to disk, increasing the amount of time required to process the data. In extremely low memory conditions, you might not be able to complete the operation.

Specifying a Billing Period and Accessing the Accounting Log Window

To access accounting data, select the desired server icon in the View All window or a View window, or select the desired server name in the Server combo box in the left corner of the Tool Bar. Then, either click the Accounting icon or choose Accounting > View Billing Charges by User Name. ConnectView opens the Billing Period dialog box, shown in Figure 43.

Figure 43 Billing PeriodDialog Box



Enter the desired Start and End dates and click the OK button.

NOTE: Connections that are started before the billing period start date and continue past the billing period end date (span the entire specified billing period), and connections that do not start within the billing period but end within the billing period are not displayed as incomplete connections and are not included in accounting data.

By default, start and end dates are determined by the available audit trail and archived files.

To check for connections that started during the specified billing period but last beyond the end date (a start connection record is found, but not a matching end connection record), ConnectView checks for end records up to one day after the billing period. If an end connection record that matches a start connection record is found, ConnectView includes the connection in the accounting data. If not, ConnectView counts it as incomplete.

Because of this one day checking and to avoid duplicate billing, ConnectView discards any end connection records for which a matching start connection record cannot be found. The following table summarizes this accounting process for a connection that begins on 3/1/96 at 8:00 a.m. and ends on 3/4/96 at 3:00 p.m.

Billing Period	Accounting Result
3/1/96 to 3/4/96	Included. The connection is included in the accounting data, because both the start time and the end time are within the billing period.
3/1/96 to 3/3/96	Included. The connection is included in the accounting data, because the start time is within the billing period and the end time is outside the billing period by less than one day.
3/1/96 to 3/2/96	Incomplete connection. The connection is counted as an incomplete connection, because the start time is within the billing period, but the end time is outside the billing period by more than one day.
3/2/96 to 3/2/96	Not included. The connection is not included in the accounting data, because neither the start time nor the end time is within the billing period.

Billing Period	Accounting Result
3/2/96 to 3/4/96	Not included.

The connection is not included in the accounting data and is not counted as an incomplete connection, because the start time is outside the billing period, even though the end time is within the billing period.

ConnectView opens the Accounting Log window with data for the specified date. Figure 44 shows an example Accounting Log window with data displayed by user ID.

Figure 44 Accounting Log by User Name Window

Accounting Log - SVE-SANFRANCISCO					
Date:	5/19/1996 - 6/14/1996	Complete Connections:	10305		
Total Connected Hours:	1253:38:31	Incomplete Connections:	185		
Total Charges:	\$243.06	Total Bytes Transferred:	125,886,195		
User Name	Charges	Total Hours	Complete Connectio	Incomplete Connect	
ADMIN	\$30.00	139:35:14	91	0	
NWCADMIN	\$10.00	1:57:44	10	3	
JMOBILE	\$125.47	258:32:29	113	25	
Complete Transactions for Admin using cost profile C:\NWCVIEW\DEFAULT.NCP					
Date	Duration	Port Name	Service	Charges	Bytes Tran
5/19/1996 13:41:40	69:31:17	Remote1	PPRNS	\$12.00	258,833
5/6/1996 17:12:06	19:32:17	Remote5	NCS	\$6.00	175,192
5/6/1996 17:21:52	0:12:42	Remote3	PPRNS	\$1.00	342,316

From this example, you can see that the Accounting Log window is divided into three sections. The top section contains billing period summaries, the middle section shows totals by user ID, and the bottom section lists the completed transactions associated with the selected user.

IMPORTANT: The Accounting Log window can display data for up to 8,000 user IDs for the specified billing period. However, this display limitation does not apply to copying, printing, or exporting accounting data.

Displaying Accounting Data for Specific Users

ConnectView enables you to limit the data displayed in the Accounting Log window by usernames, account numbers, and dates within the display period.

To limit the display of accounting data, with the Accounting Log window open, choose **View > Display Options (F4)**. ConnectView opens the Accounting Log By Users Display Options dialog box.

Specify the desired dates. These dates cannot exceed the dates and times specified for the accounting display period.

Then, select the desired usernames in the Available Users list and click **Add**. The usernames appear in the Selected Users list.

Click **OK** to limit the data displayed in the Accounting Log window to specified options. Click **Cancel** to close this dialog box without changing the data in the Accounting Log window.

Displaying Accounting Data by Account Number

To display accounting data by account number, first open the Accounting Log window with data displayed by user ID. This is the default view of the accounting log. When this window is open, the command changes to **Accounting > View Billing Charges by Account Number**. Choose this command. ConnectView displays accounting data by account number.

Figure 45 shows an example Accounting Log window for the period from 5/19/96 to 6/14/96, with data by account number.

Figure 45 Accounting Log by Account Number Window

Accounting Log - SVE-SANFRANCISCO					
Date:	5/19/1996 - 6/14/1996	Complete Connections:	10305		
Total Connected Hours:	1253:38:31	Incomplete Connections:	185		
Total Charges:	\$1243.05	Total Bytes Transferred:	125,886,195		
Account Number	Charges	Total Hours	Connections	Average Connection	Bytes
0000	\$125.47	256:32:29	113	6:32	
1000	\$56.19	1:43:21	19	9:45	
2000	\$110.15	43:11:09	43	3:58	
Transactions for account: (0000)					
UserName	Charges	Hours	Complete Con		
ADMIN	\$19051.30	776:15:07	61		
NWCADMIN	\$20149.75	814:42:15	55		
IMOBILE	\$23391.55	996:15:10	52		

From this example, you can see that the Accounting Log window is divided into three sections. The top section contains billing period summaries; the middle section shows connections by account number; and the bottom section lists the users assigned to the selected account number along with data for each user.

IMPORTANT: The Accounting Log window can display up to 8,000 user IDs for the specified billing period. However, this display limitation does not apply to copying, printing, or exporting accounting data.

To switch back to displaying accounting data by user ID, choose Accounting > View Billing Charges by User Name.

Displaying Accounting Data for Specific Account Numbers

ConnectView enables you to limit the data displayed in the Accounting Log window account numbers and dates within the original display period.

To limit the display of accounting data, with the Accounting Log window open, choose View > Display Options (F4). ConnectView opens the Accounting Display By Account Number Options dialog box.

Specify the desired dates. These dates cannot exceed the dates and times specified for the original accounting display period.

Select the desired account numbers in the Available Accounts list and click Add. The account numbers appear in the Selected Accounts list.

Click OK to limit the data displayed in the Accounting Log window to specified options. Click Cancel to close this dialog box without changing the data in the Accounting Log window.

Accessing the Accounting Report Window

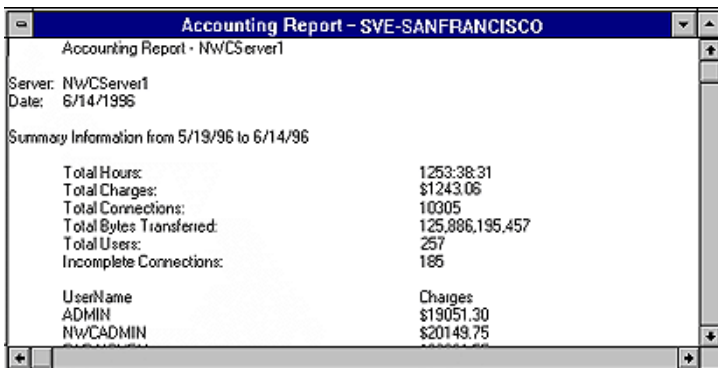
You can use the Accounting Report window to display accounting totals and daily connections in report format.

To display accounting data in report format, ensure the desired server is selected and from any window choose File > Generate Report > Accounting. The Billing Period dialog box appears so you can enter start and end dates. For a description of the Billing Period dialog box, see Figure 43 on page 280.

Enter the desired dates and click OK.

ConnectView opens the Accounting Report window shown in Figure 46.

Figure 46 Accounting Report Window



The screenshot shows a window titled "Accounting Report - SVE-SANFRANCISCO" with a subtitle "Accounting Report - NWCServer1". It displays the following information:

Server: NWCServer1
Date: 6/14/1996

Summary Information from 5/19/96 to 6/14/96

Total Hours:	1253:38:31
Total Charges:	\$1243.06
Total Connections:	10305
Total Bytes Transferred:	125,886,195,457
Total Users:	257
Incomplete Connections:	185

UserName	Charges
ADMIN	\$19051.30
NWCADMIN	\$20149.75

From this example, you can see an Accounting Report window with data for connections made between 5/19/96 and 6/14/96.

IMPORTANT: The Accounting Report window can display up to 32,000 lines of data for the specified billing period. However, this display limitation does not apply to copying, printing, or exporting accounting data.

Customizing the Accounting Report

ConnectView allows you to specify which information appears in the Accounting Report window and in what order the data columns appear.

To customize the data display in the Accounting Report window, choose File > Report Preferences and click the Accounting tab button. The Report Preferences dialog box appears with the options for the Accounting Report window.

By default, the Accounting Report includes summary information, user totals, account totals, and connection information. The following table shows the default fields for the user totals and connection information.

User Totals	Username, charges, hours, dial-in hours, dial-out hours, dial-in charge, dial-out charge, complete connections, discarded connections, account number, account profile, bytes transferred
Connection Information	Server name, date, username, hours, port name, baud rate, service, dial type, charges, bytes transferred, phone number

Clear the check boxes for the data you do not want to appear in the report.

To change the order of the detailed information, select the desired field and click the Up or Down button.

To save your changes, click the OK button. The changes take effect the next time the Accounting Report window is opened and remain in effect until these options are changed. To close this dialog box without applying the changes, click the Cancel button.

Displaying Incomplete Connections and Connections with Duplicate IDs

Incomplete connections are connections for which ConnectView can find a start connection record but cannot locate the related end connection record. Incomplete connections could be due to one of the following:

- ◆ Server was down.

- ◆ Audit trail recording was disabled or unavailable after the connection was established.
- ◆ Connection was disconnected beyond the end date of the display period.
- ◆ Connection is ongoing or the connection was disconnected and an end of connection record could not be generated.

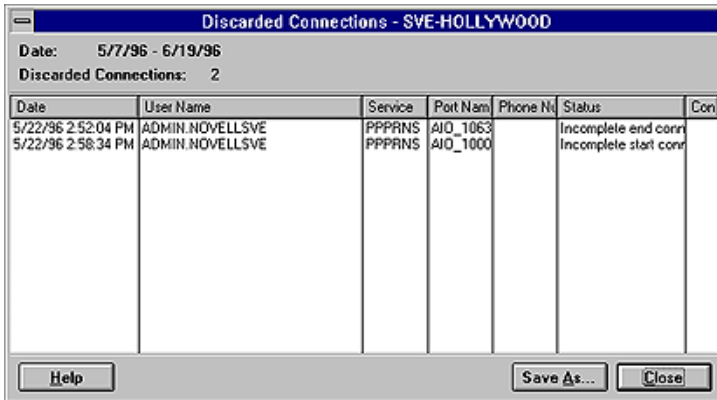
NOTE: ConnectView automatically checks for end connection records up to one day after the end date of the billing period. If an end connection record that matches a start connection record is found in the day after the billing period end date, ConnectView includes the connection in the accounting data. If the matching end connection record is not found, ConnectView counts it as incomplete. Because of this one day checking and to avoid duplicate billing, ConnectView considers any end connection records for which a matching start connection record cannot be found as incomplete connections.

Duplicate connection IDs occur when a new connection record contains the same connection ID as an existing connection record of the same type. When this occurs, ConnectView displays a warning message and allows you to terminate or continue the accounting process. If the accounting process is continued, ConnectView cannot guarantee the integrity of the accounting data.

To display the incomplete connections and connection records with duplicate connection IDs, with the Accounting Log window open, choose Accounting > View Invalid Connections.

ConnectView opens the Invalid Connections dialog box, shown in Figure 47.

Figure 47 Invalid Connections Dialog Box



From this example, you can see there were two invalid connections during the current billing period. These connections are not included in the accounting data.

NOTE: Connections that are started before the billing period start date and continue past the billing period end date (span the entire specified billing period) are not displayed as discarded connections and are not included in accounting data.

Printing, Copying, and Exporting Accounting Data

ConnectView enables you to copy, print, and export accounting data.

IMPORTANT: The amount of accounting data that can be output is not limited to the display limitations of 8,000 user IDs or account numbers in the Accounting Log window and 32,000 lines of data in the Accounting Report window.

This capability allows you to create and maintain comprehensive accounting records.

IMPORTANT: If you are accessing large amounts of data in the current audit trail file and/or archived files, generating accounting data could require a substantial amount of time and memory. This is especially so if low memory conditions occur and Windows begins to swap data to disk, increasing the amount of time required to process the data. In extremely low memory conditions, you might not be able to complete the operation.

Copying Accounting Data

To copy accounting data, open the desired Accounting Log or Accounting Report window and choose Edit > Copy. ConnectView copies the displayed data to the Windows clipboard. You can then paste this data into other applications.

Printing Accounting Data

To print accounting data, open the desired Accounting Log or Accounting Report window and choose File > Print. ConnectView prints the data from the opened window.

Exporting Accounting Data

To export accounting data in tab-delimited format, open the Accounting Report window for the desired period and choose File > Export. ConnectView prompts you for a filename and then exports the data from the opened Accounting Report window to the specified file in tab-delimited format.

Remote Access from the ManageWise Console

This section is applicable only if you have NetWare ManageWise software installed on the network. This allows the ManageWise operator to manage remote access information from within the ManageWise product.

To allow ManageWise to support remote access, complete the following steps:

1. Map a drive on your ManageWise workstation to the remote access server.
2. Copy the required remote access files from the remote access server to a subdirectory on the ManageWise workstation.

The files are located in the SYS:SYSTEM\NWCNMS subdirectory of the remote access server.

- a. Copy NWCTRAP.MIB, AIOMIB.MIB, and NCMIB.MIB from the remote access server to the MW\NMS\SNMPMIBS\CURRENT subdirectory on the ManageWise workstation.
 - b. Copy NWCTRAP.HLP from the remote access server to the NM\HELP subdirectory on the ManageWise workstation.
3. Start ManageWise under Windows on the workstation.

4. Integrate the MIB files into the Alarm Manager database.

Use the SNMP MIB compiler in the Tools menu to integrate the MIB files.

5. Configure the profiles.

Select the Add command to configure a profile for the scalar objects and for each remote access table object that you want to access. See the *Management Guide* in the ManageWise documentation set for information on using the SNMP profile editor.

This ensures that ManageWise can now recognize remote access data.

Managing Alerts

An alert is a record of a network event alerting you to problems and conditions on the network.

Remote access alerts can be viewed from any of the following management consoles:

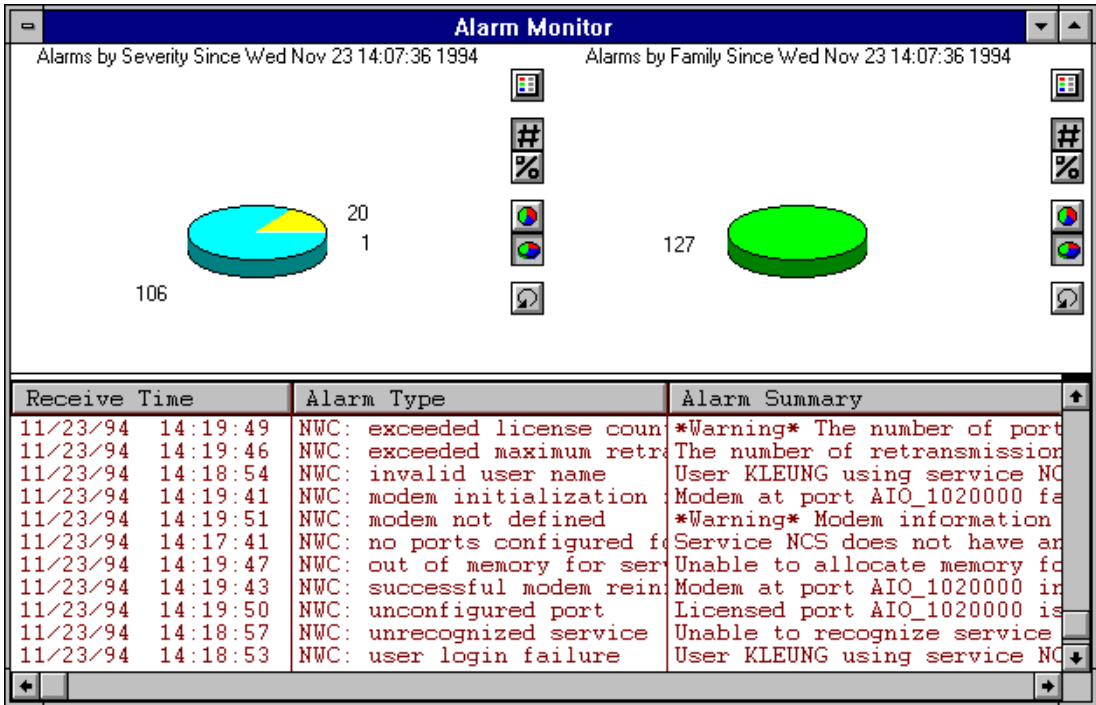
- ◆ NetView console, if installed
- ◆ Remote access
- ◆ NetWare server console
- ◆ ConnectView, if installed
- ◆ ManageWise console, if installed

You can view remote access alerts from the Alarm Monitor and the Alarm Report in the ManageWise product. For more information about the Alarm Monitor and Alarm Report, see the documentation that is shipped with the ManageWise product.

Sample Alerts from the Alarm Monitor

The Alarm Monitor displays real-time information about all the alerts that occurred since you started ManageWise. Figure 48 shows sample alerts from all the products that ManageWise manages.

Figure 48 Sample Alerts from the Alarm Monitor



If you have the Alarm Monitor window open, then remote access alerts pop up on the screen as they occur.

Sample Alerts from the Alarm Report

The Alarm Report window, shown in Figure 49 , displays information about alerts that are logged in the database.

Figure 49 Alarm Report in ManageWise

1 - All Alarms - Alarm Report		
Receive Time	Alarm Type	Alarm Summary
11/23/94 14:19:51	NWC: modem not defined	*Warning* Modem information for
11/23/94 14:19:50	NWC: unconfigured port	Licensed port AIO_1020000 is no
11/23/94 14:19:49	NWC: exceeded license c	*Warning* The number of ports c
11/23/94 14:19:47	NWC: out of memory for	Unable to allocate memory for n
11/23/94 14:19:46	NWC: exceeded maximum	The number of retransmissions o
11/23/94 14:19:44	NWC: connection drops	Connection made by users at por
11/23/94 14:19:41	NWC: modem initializat	Modem at port AIO_1020000 faile
11/23/94 14:19:40	NWC: connection time ex	User KLEUNG using service NCS o
11/23/94 14:19:39	NWC: abnormal disconnec	User KLEUNG with session WordPr
11/23/94 14:19:38	NWC: dialout failure	User KLEUNG with session WordPr
11/23/94 14:19:00	NWC: ARAS not bound	AppleTalk remote Access Service
11/23/94 14:18:58	NWC: dailback failure	Service NCS unable to dial back
11/23/94 14:18:58	NWC: abnormal disconnec	Remote user KLEUNG using servic
11/23/94 14:18:57	NWC: unrecognized serv	Unable to recognize service for
11/23/94 14:18:56	NWC: user not authorize	User KLEUNG is not authorized t
11/23/94 14:18:55	NWC: user not configura	User KLEUNG is not configured t
11/23/94 14:18:54	NWC: invalid user name	User KLEUNG using service NCS a

From the Alarm Report window, you can obtain more detailed information about a particular alert.

Monitoring Alerts from the NetView Console

Support for Open NetView allows the NetView operator to view remote access alerts from a NetView console.

To allow NetView to support remote access alerts, complete the following steps:

1. Unload the Communication Executive from the server that has NetWare for SAA or NMA for NetView installed.

This unlocks the Communication Executive master database, CSMMASTER.DBA.

2. Run the NVALTDB utility on the server on which the alerts are generated.

This utility updates the CSMMASTER.DBA file. At the system prompt (:), enter

```
load nvaltdb source [destination]
```

Replace *source* with SYS:SYSTEM\NWC_NV.CPG. Specify the volume, pathname, and filename with the extension CPG.

Replace *destination*, which is optional, with the volume and directory path in which the Btrieve formatted file is placed. The default pathname for the output file, NWC_NV.BTV, is SYS:SYSTEM.

This process allows the NetView console operator to monitor remote access alerts. Figure 50 shows a sample NetView console monitoring alerts.

Figure 50 Monitoring Alerts from the NetView Console

```
NETUIE  SESSION DOMAIN: CMM01  PQUINTO  05/26/93 14:50:40
MPDA-30A          * ALERTS-DYNAMIC *

DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
CMM01  XP17      CTRL 14:49 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:49 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:48 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:47 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:46 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:46 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:45 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:45 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:44 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:44 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:42 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:42 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:41 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
CMM01  XP17      CTRL 14:41 TIMEOUT:X.25 NETWORK
CMM01  XP17      CTRL 14:40 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK

DEPRESS ENTER KEY TO VIEW ALERTS-STATIC
```

NetWare Link/X.25

The X.25 Console utility (X25CON) is a management console that provides access to interface configuration and statistical information for all X.25 interfaces reported by the specified host. It uses the Simple Network Management Protocol (SNMP) to access this information from any local or remote system on the network. For more information about using the X.25 console utility, refer to Using the X.25 Console Utility.

The X.25 Trace utility (X25TRACE) enables you to monitor traffic over X.25 links. It enables you to capture real-time incoming and outgoing data frames and play them back to the window. For more information about using the X.25 trace utility, refer to Using the X.25 Trace Utility.

Using the X.25 Console Utility

To load X25CON, enter the following command at the NetWare® system console prompt:

```
LOAD X25CON
```

X25CON loads and displays the X.25 Console Main Menu and a summary window.

The X.25 Console Main Menu options are as follows:

- ◆ **SNMP Access Configuration.** Enables you to configure SNMP access parameters (such as the desired host, poll interval time, and timeout value).
- ◆ **X.25 Interfaces.** Displays an information summary of all X.25 interfaces reported by the specified host system.
- ◆ **X.25 Call Target Summary.** Displays all the call targets configured at the specified host.
- ◆ **Cleared Circuit Summary.** Displays an information summary of any virtual circuits that were abnormally cleared.
- ◆ **Ping Remote System.** Initiates an X.25 PING test to a remote end from the local host.
- ◆ **Display Traps.** Enables you to access the trap log file created by SNMP LOG.NLM.

To select an option on this menu, use the Up-arrow and Down-arrow keys to move the highlight bar to the option, then press Enter.

The summary window displays the following information:

- ◆ **Host.** Name of the target system.
- ◆ **Uptime.** Elapsed time since the target system was last initialized.
- ◆ **System.** Version of NetWare running on the target system.
- ◆ **Interfaces Configured.** Number of X.25 interfaces configured on the target system.
- ◆ **Interfaces Active.** Number of X.25 interfaces actually running on the target system.
- ◆ **Active VCs.** Number of virtual circuits running on the target system.

SNMP Access Configuration

You can display the SNMP Access Configuration window by selecting that option from the X.25 Console Main Menu.

The SNMP Access Configuration window allows you to specify how you obtain information about the target system.

To configure SNMP access parameters, complete the following steps:

- 1** The Transport Protocol selection is highlighted. Press Enter to display the transport mechanisms X25CON can use to obtain X.25 information.

The Transport Protocol menu appears.

- 2** Choose the transport protocol you want to use.
 - ◆ Local System. Provides direct access to the local node's X.25 information.
 - ◆ IPX. Provides access to the selected node's X.25 information using SNMP over the Internetwork Packet Exchange™ (IPX™) protocol.
 - ◆ UDP. Provides access to the selected node's X.25 information using SNMP over the User Datagram Protocol (UDP) of the TCP/IP protocol suite.

- 3** Enter the *Host Address* of the target system.

The address can be either a hostname, an IP address, or an IPX address. The default is the local host.

- 3a** If you selected IPX as the *Transport Protocol*, press Insert to display a list of the known servers. Select the desired server and press Enter.

- 3b** If you selected UDP as the *Transport Protocol*, press Insert to display a list of hostnames and their associated IP addresses. Select the desired host and press Enter.

If you type in a valid hostname, that host's IP address is displayed in this field.

- 4** Enter the *Community Name* to be included in each request message sent to the target system.

The community name is used by the SNMP agent to determine the type of management object access to be granted. The name can be from 1 to 24 ASCII characters. The default name is public (read-only access); the other valid choice is Disabled (read-write access).

5 Enter the desired timeout value.

This is the time interval that X25CON waits for a response to an SNMP request. The range of values is 0 to 7200 seconds (12 hours). The default is 5 seconds.

6 Enter the desired poll interval.

This is the time interval at which the target system is accessed to update the selected X.25 interface management information display. The range is 0 to 4,294,967,295 seconds. The default is 1 second for a local system or 5 seconds for a remote system. If you specify an interval of 0, the target system is accessed as frequently as possible.

7 Press Esc.

You are prompted to save the Network Interface Console options.

8 Select Yes to save the changes, then press Enter to return to the X.25 Console Main Menu.

X.25 Network Interfaces

You can display a list of the X.25 interfaces reported by the target system by selecting the X.25 Network Interfaces option from the X.25 Console Main Menu.

The X.25 Network Interfaces window displays the following information about each of the interfaces listed:

- ◆ Interface Name. The NetWare Link Support Layer™ (LSL™) symbolic name associated with this port. This is the name used to reference the interface during NetWare bind operations.
- ◆ VCs. Total number of virtual circuits (including PVCs) currently established on this interface versus the total number of virtual circuits that can be established on this interface.
- ◆ Phy. Current status of the physical layer of this interface.
- ◆ Link. Current status of the link layer of this interface.
- ◆ Packet. Current status of the packet layer of this interface.
- ◆ Elapsed Time Up. Total elapsed time that this interface has been up and running.

X.25 Interface Menu

In the X.25 Network Interfaces window, use the Up-arrow and Down-arrow keys to highlight an interface, then press Enter to view the X.25 Interface Menu for that interface.

NOTE: If you select an X.25 port on a remote server/router to monitor, it might take several seconds for the connection to be established.

The X.25 Interface Menu window displays a list of the windows available for each layer of the selected interface.

The X.25 Interface Menu lists the following options (the first three fields are read-only). Use the Up-arrow and Down-arrow keys to highlight the desired window, then press Enter to select it.

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface. This is the name used to reference the interface during NetWare bind operations.
- ◆ Interface Index. Unique index assigned to an interface within the target host system. A different Interface Index is assigned to each layer (packet, link, and physical). The value shown here is assigned to the packet layer.
- ◆ Version. This field is not used with the remote access software.

Packet Layer

- ◆ Active VC Summary. Displays a list of all the active virtual circuits currently established on this interface.
- ◆ Cleared VC Summary. Lists all virtual circuits that have used this interface and have been cleared abnormally.
- ◆ LCN Range Summary. Displays the currently configured Logical Channel Number ranges for various types of virtual circuits.
- ◆ Packet Layer Operating Parameters. Displays information about the configured packet level runtime parameters.
- ◆ Packet Layer Statistics. Provides a count of packet level statistics.

Link Layer

- ◆ Link Layer Flow Table. Displays some of the more important runtime link layer statistics and last used information.
- ◆ Link Layer Operating Parameters. Displays information about the configured link level runtime parameters.

- ◆ Link Layer Statistics. Displays statistics relating to the frames exchanged.

Physical Layer

- ◆ Physical Layer Status. Displays information about the physical level interface signals/leads for the X.25 interface.
- ◆ Physical Layer Operating Parameters. Displays interface card hardware related information for the X.25 interface.
- ◆ Physical Layer Statistics. Displays statistics related to the correct operation of the port for the X.25 interface.

Active Virtual Circuit Summary

You can display the X.25 Active Virtual Circuit Summary window by selecting that option from the X.25 Interface Menu window.

The X.25 Active Virtual Circuit Summary window displays a list of the active virtual circuits (both SVCs and PVCs) currently established on the selected interface.

The X.25 Active Virtual Circuit Summary window displays the following information about each of the virtual circuits listed:

- ◆ Destination Name. WAN call destination name associated with this circuit for the outgoing SVC or PVC, or the calling DTE address for the incoming SVC.
- ◆ LCN. Logical Channel Number of this virtual circuit. This value ranges from one (1) to the total number of virtual circuits configured for this interface.
- ◆ Type. Type of virtual circuit: switched (SVC) or permanent (PVC).
- ◆ Protocol ID. Protocol ID of the upper layer using this virtual circuit.
- ◆ Elapsed Time Up. Total elapsed time since the virtual circuit was established (SVC) or opened by the user (PVC).

Use the Up-arrow and Down-arrow keys to highlight a circuit, then press Enter to select it. The X.25 Active Virtual Circuit window for the selected circuit is displayed.

The X.25 Active Virtual Circuit window displays the following parameters:

- ◆ Interface Name. Name of the interface on which the VC is established.

- ◆ Remote System Name. Logical name, as defined in the Call Target database, of the remote DTE to which this active virtual circuit is logically connected for outgoing SVCs and PVCs, or the X.121 DTE address of the remote DTE for incoming SVCs.
- ◆ Elapsed Connect Time. Total time this circuit has been connected.
- ◆ Called DTE Address. Local DTE address for incoming SVCs (for PVCs this field displays blanks). The X.121 DTE address assigned to the destination DTE for outgoing packets.
- ◆ Calling DTE Address. Decimal address (up to 15 characters) of the DTE from which an incoming call is originated. For outgoing calls, this field should match the address assigned by your network. Most X.25 application users include this address in outbound Call Request packets in the Calling Address field.
- ◆ Protocol. Name of the protocol in use over this circuit.
- ◆ Direction. Indicates whether the current call is incoming or outgoing (or PVC).
- ◆ Virtual Circuit Type. Indicates whether a PVC or SVC is used to establish a connection to the specific destination.
- ◆ LCN. Logical Channel Number assigned to this virtual circuit.

Received/Transmitted

- ◆ Number of Bytes. Number of data bytes received/transmitted over this virtual circuit during the elapsed connect time.
- ◆ Data Packets. Number of data packets received/transmitted over this virtual circuit during the elapsed connect time.
- ◆ Interrupt Packets. Number of interrupt packets received/transmitted over this virtual circuit during the elapsed connect time.

Timer Timeouts

- ◆ Data Retransmission (T25). Total number of times this timer has expired on this virtual circuit during the elapsed connect time.
- ◆ Reset (T22). Total number of times this timer has expired on this virtual circuit during the elapsed connect time.
- ◆ Interrupt (T26). Total number of times this timer has expired on this virtual circuit during the elapsed connect time.

Cleared Virtual Circuit Summary

You can display the X.25 Cleared Virtual Circuit Summary window by selecting that option from the X.25 Interface Menu window.

The X.25 Cleared Virtual Circuit Summary window displays a list of the virtual circuits on the selected interface that have been cleared with a nonzero cause code or a nonzero diagnostic code.

The X.25 Cleared Virtual Circuit Summary window displays the following information about each of the virtual circuits listed:

- ◆ Destination Name. Logical name of the destination, as defined in the Call Target database for outgoing calls, or the remote X.121 DTE address for incoming calls.
- ◆ LCN. Logical Channel Number assigned to the cleared virtual circuit.
- ◆ Cause. Clearing cause code included in the clear packet.
- ◆ Diagnostic. Diagnostic code included in the clear packet.
- ◆ Up > 5 Mins. Indicates whether the cleared circuit was up longer than 5 minutes before it was cleared.

Use the Up-arrow and Down-arrow keys to highlight the desired circuit, then press Enter to select it. The X.25 Cleared Virtual Circuit window appears.

The X.25 Cleared Virtual Circuit window displays the following parameters for the abnormally cleared virtual circuit selected:

- ◆ Interface Name. Name of the interface on which the virtual circuit was established and abnormally cleared.
- ◆ Remote System Name. Remote DTE address or the logical name, as defined in the Call Target database, of the remote DTE to which this abnormally cleared virtual circuit was logically connected.
- ◆ Interface Index. Unique index assigned to the interface on which the VC was established and abnormally cleared.
- ◆ Called DTE Address. Local DTE address for incoming SVCs (for PVCs this field displays blanks). The X.121 DTE address assigned to the specific destination DTE for outgoing packets.
- ◆ LCN. Logical Channel Number assigned to this virtual circuit.
- ◆ Cause Code. Clearing cause code included in the clear packet.
- ◆ Diagnostic Code. Diagnostic code included in the clear packet.

- ◆ Time Established. Time that the connection was established.
- ◆ Connection Uptime. Total time that the connection was up.
- ◆ Data Packets Received. Number of data packets received over this virtual circuit during the elapsed connect time.
- ◆ Data Packets Transmitted. Number of data packets transmitted over this virtual circuit during the elapsed connect time.

Logical Channel Range Summary

You can display the X.25 Logical Channel Range Summary window by selecting that option from the X.25 Interface Menu.

The highest Logical Channel Number (LCN) possible is 4095; however, the maximum number of virtual circuits (or logical channels) supported by the NetWare Link/X.25™ software is 255 per port. The actual number of logical channels available is determined by the subscription with your X.25 service provider.

The Logical Channel Number ranges for the different types of circuits cannot overlap each other (two different circuits cannot use the same LCN).

The X.25 Logical Channel Range Summary window displays the user-defined ranges of logical channel numbers. The following fields appear on the X.25 Logical Channel Number Summary window:

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface.
- ◆ Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value here is assigned to the packet layer.
- ◆ PVC LCN, Lowest. Lowest LCN that can be used for a PVC. The range of values is 0 (Transpac only) through 255.
- ◆ PVC LCN, Highest. Highest LCN that can be used for a PVC. This number must agree with your network subscription. The range of values is 0 (undefined) through 6.
- ◆ Inbound SVC LCN, Lowest. Lowest LCN that can be used for one-way incoming logical channels for SVCs. The range of values is 1 through 4095. This value must be greater than the highest PVC LCN.
- ◆ Inbound SVC LCN, Highest. Highest LCN that can be used for one-way incoming logical channels for SVCs. The range of values is 0 (undefined)

through 4095. The number of incoming SVCs must agree with your network subscription.

- ◆ Two-Way SVC LCN, Lowest. Lowest LCN that can be used for two-way channels (both inbound and outbound calls) for SVCs. The range of values is 1 through 4095. This value must be greater than the highest Inbound SVC LCN.
- ◆ Two-Way SVC LCN, Highest. Highest LCN that can be used for two-way SVCs. The range of values is 0 (undefined) through 4095. The number of two-way SVCs must agree with your network subscription.
- ◆ Outbound SVC LCN, Lowest. Lowest LCN that can be used for one-way outgoing logical channels for SVCs. The range of values is 1 through 4095. This value must be greater than the highest Two-Way SVC LCN.
- ◆ Outbound SVC LCN, Highest. Highest LCN that can be used for one-way outgoing logical channels for SVCs. The range of values is 0 (undefined) through 4095. The number of outgoing SVCs must agree with your network subscription.

Packet Layer Operating Parameters

You can display the Packet Layer Operating Parameters window by selecting that option from the X.25 Interface Menu window.

The Packet Layer Operating Parameters window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface.
- ◆ Protocol Version. Conformance year for the X.25 specification used for this port. The possible values are:
 - 1976. ITU-T (formerly CCITT) X.25 1976 version
 - 1980. ITU-T X.25 1980 version
 - 1984. ITU-T X.25 1984 version (default)
 - 1988. ITU-T X.25 1988 version
 - 1987. ISO 8208 1987 version
 - 1989. ISO 8208 1989 version
- ◆ Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value here is assigned to the packet layer.

- ◆ **Local DTE Address.** X.121 address (up to 15 digits) of the local DTE. It should match the address assigned by the attached packet data network (PDN).
- ◆ **Max Number of VCs.** Maximum number of virtual circuits (SVCs and PVCs) that can be established on this interface.
- ◆ **Number of PVCs.** Total number of permanent virtual circuits (PVCs) that are configured on this packet layer interface.
- ◆ **Interface Mode.** Indicates whether DTE or DCE procedures are currently being used for packet layer operations.

When establishing a connection to an X.25 network, this parameter must be set to DTE (the default value) to avoid call collisions.

- ◆ **Modulo.** Indicates the numbering of sequential data packets allowed in a window. The options are Modulo 8 (0 through 7) or Modulo 128 (0 through 127). For most networks, the default value (Modulo 8) is used. The Default Window Size parameter is dependent on which Modulo method is selected.

Timers

- ◆ **Restart (T20).** Time, in seconds, that the packet layer waits for an acknowledgment before it initiates a recovery procedure. The range of values is 1 through 3200 seconds (0=timer disabled).

When this timer expires, the Restart Request packet is retransmitted.

- ◆ **Call (T21).** Time, in seconds, that the DTE waits for a response to an outbound Call Request packet before retransmitting. The range of values is 1 through 3200 seconds (0=timer disabled).
- ◆ **Reset (T22).** Time, in seconds, that the DTE waits for a response to a Reset Request packet before retransmitting. The range of values is 1 through 3200 seconds (0=timer disabled).
- ◆ **Clear (T23).** Time, in seconds, that the DTE waits for a response to a Clear Request packet before retransmitting. The range of values is 1 through 3200 seconds (0=timer disabled).
- ◆ **Window (T24).** Time, in seconds, within which the packet level data window must change. The range of values is 1 through 3200 seconds (0=timer disabled).

If this timer expires, the virtual circuit is considered inoperative and is cleared (SVCs) or reset (PVCs).

- ◆ Data Retx. (T25). Time, in seconds, that the DTE waits for the appropriate acknowledgment after transmitting a data packet. The range of values is 1 through 3200 seconds (0=timer disabled).

If this timer expires, the circuit is reset.

- ◆ Interrupt (T26). Time, in seconds, that the DTE waits when an Interrupt Request packet is sent for an interrupt confirmation to be received. The range of values is 1 through 3200 seconds (0=timer disabled).

If this timer expires, the circuit is reset.

Retransmission Counts

- ◆ Restart (R20). Maximum number of times a Restart Request packet is retransmitted, upon expiration of the T20 timer, before notifying the user that the associated link is inoperative. The range of values is 1 through 50 (0=disabled).
- ◆ Reset (R22). Maximum number of times a Reset Request packet is retransmitted, upon expiration of the T22 timer, before initiating a clear procedure (SVCs) or a restart procedure (PVCs). The range of values is 0 through 50 (0=disabled).
- ◆ Clear (R23). Maximum number of times a Clear Request packet is retransmitted, upon expiration of the T23 timer, before initiating a Restart procedure on the associated link. The range of values is 0 through 50 (0=disabled).

Packet Layer Statistics

You can display the Packet Layer Statistics window by selecting that option from the X.25 Interface Menu.

The Packet Layer Statistics window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface.
- ◆ Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value here is assigned to the packet layer.
- ◆ Outgoing. Total number of one-way outgoing SVCs currently established on this interface.
- ◆ Incoming. Total number of one-way incoming SVCs currently established on this interface.

- ◆ Two-Way. Total number of two-way SVCs currently established on this interface.

Received/Transmitted

- ◆ Restart. Total number of Restart Indication packets received and Restart Request packets transmitted on this interface.
- ◆ Call. Total number of Incoming Call packets received and Call Request packets transmitted on this interface.
- ◆ Reset. Total number of Reset Indication packets received and Reset Request packets transmitted on this interface.
- ◆ Clear. Total number of Clear Indication packets received and Clear Request packets transmitted on this interface.
- ◆ Interrupt. Total number of Interrupt Indication packets received and Interrupt Request packets transmitted on this interface.
- ◆ Data. Total number of data packets received and transmitted on this interface.

Timer Timeouts

- ◆ Restart. Total number of times the Restart timer (T20) has expired on this interface since the packet layer was (re)initialized.
- ◆ Call. Total number of times the Call timer (T21) has expired on this interface since the packet layer was (re)initialized.
- ◆ Reset. Total number of times the Reset timer (T22) has expired on this interface since the packet layer was (re)initialized.
- ◆ Data Retx. Total number of times the Data Retx. timer (T25) has expired on this interface since the packet layer was (re)initialized.
- ◆ Interrupt. Total number of times the Interrupt timer (T26) has expired on this interface since the packet layer was (re)initialized.
- ◆ Clear. Total number of times the Clear timer (T23) has expired on this interface since the packet layer was (re)initialized.
- ◆ Retry Count Exceeds. Total number of times the Retry count (N2) has been exceeded on this interface since the packet layer was (re)initialized.
- ◆ Clear Count Exceeds. Total number of times the Clear Request Retransmission count (R23) has been exceeded on this interface since the packet layer was (re)initialized.

Link Layer Flow Table

You can display the Link Layer Flow Table window by selecting that option from the X.25 Interface Menu.

The Link Layer Flow Table window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface.
- ◆ Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value shown here is assigned to the link layer.
- ◆ Current Mode. Current state of the link layer:
 - ◆ disconnected. Initial state or DISC received.
 - ◆ linkSetup. SABM sent.
 - ◆ frameReject. Invalid frame received and FRMR sent.
 - ◆ disconnectRequest. DISC sent.
 - ◆ informationTransfer. Normal information transfer state. SABM(E) sent and UA received, or SABM(E) received and UA sent.
 - ◆ rejFrameSent. Invalid NS received and REJ sent.
 - ◆ waitingAcknowledgement. T1 expired, and RR sent.
 - ◆ stationBusy. RNR sent.
 - ◆ remoteStationBusy. RNR received.
 - ◆ bothStationsBusy. RNR received and RNR sent.
 - ◆ waitingAckStationBusy. T1 expired, RNR sent.
 - ◆ waitingAckRemoteBusy. T1 expired, RNR received.
 - ◆ waitingAckBothBusy. T1 expired, RNR sent and RNR received.
 - ◆ rejFrameSentRemoteBusy. REJ sent and RNR received.
 - ◆ xidFrameSent. XID frame sent.
 - ◆ error. An error state other than one defined above.
 - ◆ other. A state not listed above.
- ◆ Busy Defer. Total number of times this interface was unable to transmit a frame because of perceived remote busy condition.

- ◆ T1 Expired. Total number of times the Retry timer (T1) expired and an unacknowledged frame was retransmitted or error recovery was initiated.
- ◆ Reject Frames Transmitted. Number of Reject (Rej) frames transmitted by the link layer because of the receipt of an Information (I) frame that was out of sequence.
- ◆ Reject Frames Received. Number of Reject (Rej) frames received by the link layer due to transmission of an Information (I) frame that was out of sequence.
- ◆ I Field in FRMR Transmitted. Displays the Information (I) field of the Frame Reject (FRMR) frame most recently transmitted. This field is either 3 bytes (Modulo 8) or 5 bytes (Modulo 128). When no Reject (FRMR) frame has been transmitted, this field contains all 0s.
- ◆ I Field in FRMR Received. Displays the Information (I) field of the Frame Reject (FRMR) frame most recently received. This field is either 3 bytes (Modulo 8) or 5 bytes (Modulo 128). When no Reject (FRMR) frame has been received, this field contains all 0s.

Link Layer Operating Parameters

You can display the Link Layer Operating Parameters window by selecting that option from the X.25 Interface Menu.

The Link Layer Operating Parameters window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface.
- ◆ Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value shown here is assigned to the link layer.
- ◆ Station Type. User-configured station type of this interface:
 - ◆ DTE. Local DTE plays as a DTE.
 - ◆ DCE. Local DTE plays as a logical DCE.
 - ◆ DXE. Local DTE's role, whether DTE or DCE, is dynamically determined during the link setup.
- ◆ Modulo. Modulo currently used by the associated link layer interface (Modulo 8 [0 through 7] or Modulo 128 [0 through 127]). The modulo defines the limits of Information (I) frame sequence numbers.

- ◆ Max Frame Size (N1). Maximum number of bytes in an I frame that the local DTE is willing to accept from the remote DTE or DCE (excluding flags and 0 bits inserted for transparency).
- ◆ Transmit Window Size. Maximum number of sequentially numbered Information (I) frames that the link layer can have outstanding (unacknowledged) at any time.
- ◆ Receive Window Size. Maximum number of outstanding Information (I) frames that the link layer can receive before an acknowledgment (ACK) is transmitted.
- ◆ Retransmission Count (N2). Maximum number of attempts made by the local link layer to complete the successful transmission of a frame to the remote end. If this count is exceeded, the local link layer notifies the upper layer of a link failure and initiates a link recovery procedure.
- ◆ Ack Timer (T1). Current value of the T1 timer. On expiration of this timer, the link layer retransmits the frame up to N2 times before notifying the upper layer of a link failure and initiating a link recovery procedure.
- ◆ Disconnect Timer (T3). Current value of the T3 timer. On expiration of this timer, the link layer passes an indication of an excessively long idle channel state condition to the upper layer.
- ◆ Idle Timer (T4). Current value of the T4 timer. This is the time that the local DTE waits when a link becomes idle before attempting to poll the remote end for status. If the remote end does not respond, the link is considered inoperative and all currently active virtual circuits are cleared (SVCs) or reset (PVCs).

Link Layer Statistics

You can display the Link Layer Statistics window by selecting that option from the X.25 Interface Menu.

The Link Layer Statistics window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name associated with this interface.
- ◆ Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value shown here is assigned to the link layer.

Received/Transmitted

- ◆ SABM Frames. Total number of Set Asynchronous Balanced Mode (SABM) frames received and transmitted.
- ◆ UA Frames. Total number of Unnumbered Acknowledgment (UA) frames received and transmitted.
- ◆ DM Frames. Total number of Disconnect Mode (DM) frames received and transmitted.
- ◆ DISC Frames. Total number of Disconnect (DISC) frames received and transmitted.
- ◆ I Frames. Total number of Information (I) frames received and transmitted.
- ◆ RR Frames. Total number of Receive Ready (RR) frames received and transmitted.
- ◆ RNR Frames. Total number of Receive Not Ready (RNR) frames received and transmitted.
- ◆ FRMR Frames. Total number of Frame Reject (FRMR) frames received and transmitted.

Physical Layer Status

You can display the Physical Layer Status window by selecting that option from the X.25 Interface Menu.

The Physical Layer Status window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name for this interface.
- ◆ Physical Layer Interface Index. Unique index assigned to an interface within the target host system. The value here is assigned to the physical layer.
- ◆ Interface Type. Interface type of the physical layer (RS-232, RS-422, RS-423, V35, or Other)
- ◆ Receive Speed. Speed, in bits per second, at which the physical layer can receive data.
- ◆ Transmit Speed. Speed, in bits per second, at which the physical layer can transmit data.
- ◆ State/State Changes:. Total number of times that the state of each of the following signals has changed since the physical layer was (re)initialized.

- ◆ Request to Send (RTS). When the state of this signal changes from OFF to ON, it notifies the DCE that the DTE has data to transmit and to be prepared to receive the transmission.
- ◆ Clear to Send (CTS). When the state of this signal changes from OFF to ON, it notifies the DTE that the DCE is ready to receive data.
- ◆ Data Terminal Ready (DTR). When the state of this signal changes from OFF to ON, it indicates the DTE is ready to transmit or receive data.
- ◆ Data Set Ready (DSR). When the state of this signal changes from OFF to ON, it indicates the DCE is ready to transmit or receive data.
- ◆ Data Carrier Detect (DCD). When the state of this signal changes from OFF to ON, it indicates the DCE has detected the remote end's carrier signal.
- ◆ Ring Indicator (RI). When the state of this signal changes from OFF to ON, it indicates the DCE has received a ringing signal on an SVC. This field displays N/A for PVCs.

Physical Layer Operating Parameters

You can display the Physical Layer Operating Parameters window by selecting that option from the X.25 Interface Menu.

The Physical Layer Operating Parameters window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name for this interface.
- ◆ Physical Layer Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value shown here is assigned to the physical layer.
- ◆ I/O Base. Base address of a block of I/O addresses decoded by this interface.
- ◆ I/O Length. Number of I/O addresses in the block, starting at the base I/O address.
- ◆ Memory Base. Base address of a block of shared memory space decoded by this interface.
- ◆ Memory Length. Length, in bytes, of the shared memory space, starting at the base memory address.

- ◆ Interrupt Request Level. Primary interrupt request level (vector) used by this interface.
- ◆ Adapter Slot. EISA or MCA slot that this interface card resides in. None = not supported.
- ◆ DMA Channel. Primary DMA channel used by this interface. The valid range is 0 through 255. None = not supported.

Physical Layer Statistics

You can display the Physical Layer Statistics window by selecting that option from the X.25 Interface Menu.

The Physical Layer Statistics window displays the following information:

- ◆ Interface Name. NetWare LSL symbolic name for this interface.
- ◆ Physical Layer Interface Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value here is assigned to the physical layer.
- ◆ Interface Type. Defines the port's electrical interface standard: RS-232, RS-422, RS-423, V.35, or Other.
- ◆ Receive Speed. Speed, in bits per second, at which the physical layer receives data.
- ◆ Transmit Speed. Speed, in bits per second, at which the physical layer transmits data.
- ◆ Clock Source. Source of the interface's transmit and receive bit rate clock signals. Valid entries in this field are:
 - ◆ Internal. Both clocks are internal.
 - ◆ External. Both clocks are external.
 - ◆ Split. Transmit clock internal; receive external.
- ◆ Frame Checks. Total number of frames received with an invalid frame check sequence.
- ◆ Transmit Underruns. Total number of frames that were not transmitted since the system was (re)initialized because data was not available to the transmitter in time.

- ◆ Receive Overruns. Total number of frames that failed to be received since the system was (re)initialized because the receiver did not accept the data in time.
- ◆ Interrupted Frames. Total number of frames that failed to be received or transmitted since the system was (re)initialized because of the loss of modem signals.
- ◆ Aborted Frames. Total number of frames that were aborted since the system was (re)initialized because of the receipt of an abort sequence.

X.25 Call Target Summary

You can display the X.25 Call Target Summary window by selecting that option from the X.25 Console Main Menu.

The X.25 Call Target Summary window displays the following information for each entry in the Call Target Database:

- ◆ Destination Name. Name of the target host as defined in the Call Target Database.
- ◆ Remote DTE Adrs. X.121 address assigned to the destination DTE by the public data network (PDN) to which you are attached. This field displays N/A if the associated virtual circuit is a PVC (permanent).
- ◆ Interface Name. NetWare LSL symbolic name for this interface.
- ◆ Interface Enabled. Indicates whether an interface is configured as X.25 or not.

Yes indicates that the associated interface is configured as X.25 and is enabled.

No indicates that the associated interface is disabled or has not been configured as X.25.

Use the Up-arrow and Down-arrow keys to highlight the desired destination, then press Enter to view the X.25 Call Target Database window for that destination.

X.25 Call Target Database

You can display the X.25 Call Target Database window by selecting a destination name from the X.25 Call Target Summary window. The X.25 Call Target Summary window displays the parameters associated with an SVC. If this circuit had been a PVC, only the first five parameters would be displayed.

The X.25 Call Target Database window displays the following information:

- ◆ Destination Name. Name of the target host as defined in the Call Target Database.
- ◆ Remote DTE Address. X.121 address assigned to the destination DTE by the public data network (PDN) to which you are attached. This field displays N/A if the associated virtual circuit is a PVC (permanent).
- ◆ Index. Unique index assigned to an interface within the target host system. An Interface Index is assigned to each layer (packet, link, and physical). The value here is assigned to the packet layer.
- ◆ Circuit Type. Indicates whether a PVC or SVC is used to establish a connection to the specified destination.
- ◆ Interface Enabled. Indicates whether an interface is configured as X.25 or not.

Yes indicates that the associated interface is configured as X.25 and is enabled.

No indicates that the associated interface is disabled or has not been configured as X.25.

Called/Calling

- ◆ Packet Size (bytes). Packet size for the direction of transmission that is negotiated when an SVC is established using this call destination.
- ◆ Window Size. Window size for the direction of transmission that is presented in the Flow Control parameter negotiation facility of the Call Request packet at call setup time.
- ◆ Throughput Class (bps). Throughput class for the direction of transmission that is presented in the Throughput Class negotiation facility of the Call Request packet at call setup time.
- ◆ Fast Select. Indicates whether the Fast Select user option should be specified in outgoing calls. The possible values are as follows:
 - ◆ No. Fast Select is not used.
 - ◆ No Restriction. Fast Select is used with no restrictions on response.
 - ◆ Restriction. Fast Select is used with restrictions on response.
- ◆ Reverse Charging Proposed. Indicates whether reverse charging should be used when a call setup is requested. Possible values are as follows:
 - ◆ Local. No reverse charge.

- ◆ Reverse. Reverse charge is required for all call setup requests.
- ◆ Default. Default to the value specified in the configuration table for the associated interface.
- ◆ CUG Facility. Type of Closed User Group (CUG) used for this call. The possible values are Bilateral , Incoming , Outgoing , and Not Selected.
A CUG permits DTEs belonging to the group to communicate with each other, but a CUG precludes communication with all other DTEs.
- ◆ CUG ID. One- or four-digit hexadecimal number specifying the specific CUG in the Call Request packet.

X.25 Ping Remote System

If you select Ping Remote System from the X.25 Console Main Menu, the X.25 Ping Remote System window appears.

The X.25 Ping Remote System window allows you to run a PING test that verifies the initial connection between the local X.25 interface and a remote X.25 interface.

The Destination Name field is highlighted and should be blank. Press **Ins** to display a list of Available Destinations. To select a destination, use the **Up-arrow** and **Down-arrow** keys to highlight the desired destination, then press **Enter**.

The X.25 Ping Remote System window displays the parameters listed for the selected destination (you can change the values of the last four parameters):

- ◆ Destination Name. Name of the selected destination as defined in the Call Target Database.
- ◆ Remote DTE Address. X.121 address assigned to the destination DTE by the public data network (PDN) to which you are attached.
- ◆ Interface Name. NetWare LSL symbolic name for this interface.
- ◆ Local DTE Address. Network address assigned to the local DTE.
- ◆ Number of VCs. Number of virtual circuits to be established for the PING test. The range of values is 1 through 255. The default is 1.
- ◆ Number of Messages. Total number of messages to be sent to the remote end during the test. The range of values is 0 through 2147483647. The default value is 0.

- ◆ Delay (in 100 msec). Delay between message transmissions in 100-millisecond intervals. The range of values is 0 through 1000. The default value is 1 (100 msec).
- ◆ Data Size (bytes). Amount of data to be included in each message, in bytes. The range of values is 0 through 4096. The default value is 512 bytes.

When the values of the last four parameters have been set, the prompt `Enter F3 to Start the Ping Test` appears. Press F3 to begin the PING test with the remote destination.

You can abort the PING test at any time by pressing F5.

The following parameters display the results of the PING test with the remote destination:

- ◆ Num of Active VCs. Total number of active virtual circuits configured on this interface.
- ◆ Num of Call Failures. Total number of Call Failures detected.
- ◆ Num of VCs Connected. Total number of active virtual circuits established between this interface and the destination DTE.
- ◆ Avg Call Setup Time. Average time required to set up a call to the destination DTE.
- ◆ Messages Transmitted. Total number of messages transmitted.
- ◆ Messages Received. Total number of messages received.
- ◆ Transmit Errors. Total number of transmit errors detected.
- ◆ Receive Errors. Total number of receive errors detected.
- ◆ Sequence Errors. Total number of sequence errors detected.
- ◆ Size Errors. Total number of size errors detected.
- ◆ Pattern Errors. Total number of pattern errors detected.
- ◆ Software Errors. Total number of software errors detected.
- ◆ Average Delay. Average round-trip delay between transmitting a message to and receiving a message from the destination DTE.
- ◆ Cause Code. Clearing cause code included in the clear packet if the PING test failed.

- ◆ Diagnostic Code. Diagnostic code included in the clear packet if the PING test failed.
- ◆ Result. Indicates the overall result of the PING test: `Destination is alive` or `Ping Test to Destination Failed`.

Display Traps

You can display Trap Log information by selecting the Display Traps option from the X.25 Console Main Menu.

SNMP trap messages are used to report events. The `SNMPLOG.NLM` processes messages sent to the local server and writes them to a disk file. `X25CON` reads the disk file and displays the trap messages with the most recent first. Upon exit, the trap log file can be deleted or saved.

The Trap Log window displays the following information:

- ◆ Host Name. Hostname or IP address of the node that issued the trap message. Use the Tab key to toggle between the IP address and hostname formats.
- ◆ Trap Type. Event type triggering each trap message. Six trap types are defined to report TCP/IP events, including coldstart, warmstart, link up, link down, request authentication failure, and EGP neighbor loss. In addition to the six TCP/IP traps, four X.25 trap types are defined to report X.25 events, including X.25 Link Up, X.25 Link Down, X.25 Packet Restarted, and X.25 VC Reset.
- ◆ Time Stamp. Date and time each trap message was received and processed by the local server.

Using the X.25 Trace Utility

To invoke `X25TRACE`, enter the following at the NetWare console prompt:

```
LOAD X25TRACE
```

The message `Loading module X25TRACE.NLM` appears, followed by version and copyright notices. `X25TRACE` then displays the Available Options menu.

The options displayed in the `X25TRACE` Available Options menu are as follows:

- ◆ Network Interface Information. Displays information for the configured ports. This information specifies the basic I/O port address of the interface and the channel used on the interface.
- ◆ Real-Time Monitor. Enables you to view and capture transmitted and received frames dynamically. You can capture the dynamic data displayed on the window to either a disk file or to the memory (the default), to be replayed later for diagnostic analysis.

IMPORTANT: The Real-Time Monitor can consume a large portion of your router's CPU resources.
- ◆ Play-Back. Enables you to play back to the window a captured Real-Time Monitor data session from a disk file or from RAM.
- ◆ Configuration. Enables you to configure the X25TRACE utility.

Network Interface Information Window

You can display the Network Interface Information window by selecting that option from the X25TRACE Available Options menu.

The Network Interface Information window displays the following information:

- ◆ I/O. I/O address of this interface.
- ◆ IRQ. Interrupt request level (vector) used by this interface.
- ◆ MEM. Base address of a block of shared memory space decoded by this interface.
- ◆ Port. Port number used by this interface.
- ◆ LSL Board No. EISA or MCA slot that this interface card resides in.
- ◆ I/F Name. NetWare LSL symbolic name for this interface.

Real-Time Monitor Window

You can display the Real-Time Monitor window by selecting that option from the X25TRACE Available Options menu.

The Real-Time Monitor window displays a sampling of the actual packet traffic. To view the actual traffic, you should capture the transmission to RAM or a disk file.

The options available on this window are as follows:

F2	Next Interface
F3	Decode Mode (Raw/Frame/Packet)
F4	Complete/Short Display
F5	ASCII/Hex
F6	Freeze/Resume
F7	Start/Stop Capture

Play Back Window

You can display the X25TRACE Play Back window by selecting that option from the X25TRACE Available Options menu.

The Play Back window displays the following options:

- ◆ Play Back Device. Indicates whether the captured data session to be played back originates from RAM or a disk file.
- ◆ Disk Filename. Name of the disk file to be played back if you selected Disk as the playback device. You can have several files to which you saved real-time sessions.
- ◆ Play Back Speed. Speed at which you want to view the session: Fast , Medium , or Slow. You can change the speed and view the session again at another speed, if needed.

The cursor is positioned in the Play-Back Device field. Press Enter to display the available options. Use the Up-arrow and Down-arrow keys to highlight either Disk or RAM , then press Enter to select that option.

If you select Disk as the playback device, move the highlight bar to the Disk Filename field, enter the desired filename, then press Enter to select that file.

Highlight the Play-Back Speed option, then press Enter to display the Play-Back Speed window. Use the Up-arrow and Down-arrow keys to highlight the desired option (Slow, Medium, or Fast), then press Enter to select that option.

Configuration Window

You can display configuration information by selecting the Configuration option from the Available Options menu.

The X25TRACE Configuration window enables you to configure the X.25TRACE utility. You should use the Configuration window to set up the type of capture device and the disk filename before you use any of the other options from the Available Options menu.

The cursor is positioned in the Capture Device field. Press Enter to display the available options. Use the Up-arrow and Down-arrow keys to highlight either Disk or RAM, then press Enter to select that option.

If you select Disk as the capture device, move the highlight bar to the Disk Filename field and enter a valid filename.

Exiting X25TRACE

At the X25TRACE Available Options menu, press Esc to display the Exit window. Use the Up-arrow and Down-arrow keys to highlight the desired option (Yes or No), then press Enter to select that option.

6

Troubleshooting

This section contains troubleshooting information for the remote access software. Before you proceed to troubleshoot specific problems, ensure that you have completed the following steps before you start:

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 remote access server from a workstation using RCONSOLE.
 - ◆ Enter **CONFIG** at the console prompt.

NOTE: To print the file, redirect the output to a printer by pressing Shift+PrintScr.

Using Terminal Mode, NCS Debug, or NWCRPAIR Utilities

The following paragraphs describe how to use the terminal mode option in NIASCFG, the NCS Debug utility, and NWCRPAIR to troubleshoot remote access.

Using the Terminal Mode Option

You can use the Terminal Mode option to

- ◆ Diagnose modem or cabling problems
- ◆ Verify the link between the server, modem, and the operator of the modem
- ◆ Verify the modem commands supported by the modem

To use the Terminal Mode option, load NIASCFG and follow this path:

Select View Status for NIAS > Remote Access > Display Port Status > port you want to view > Terminal Mode

When you select the Terminal Mode option, a terminal window is displayed, through which you can interact with the device connected to the selected port. Input is sent to the AIO port as you type. Any output from the port is displayed as it is received. If local echo is enabled, keyboard input is also displayed. Only ASCII input is accepted and sent to the AIO port. Use the special-function keys defined in Table 33.

Table 33 Terminal Mode User-Input Keys

Key	Function
F1	Help
Insert	Display available terminal mode options for the terminal window
F7	Clear the terminal window
F8	Stop or continue displaying output to the terminal window
F9	Enable/disable local echo
Esc	Exit the terminal window

Terminal Mode Options

After selecting Terminal Mode, press the **Insert** key to view and select the Terminal Window Options. Table 34 lists the available options.

Table 34 Terminal Mode Options

Option	Action or Result
Change Link Settings	Temporarily changes link parameter settings for the duration of the terminal port session
Capture Output to File	Captures data (from terminal window) into a file (or stops capture if already enabled)
Input from File	Takes input from a specified file (instead of the keyboard)

Using the NCS Debug Utility

The NCS Debug utility helps you debug NCS connections. Start the NCS Debug utility by entering the following command:

```
load ncs -t
```

The `-t` parameter enables the NCS Debug Window to be displayed and saves a record of all NCS port activity in an ASCII text file called `NCSTRACE.LOG` in the `SYS:SYSTEM` directory. The size of the log file is limited to 800 KB. After the file reaches that size, the entries wrap around to the beginning of the file and logging continues.

After it is loaded, the NCS Debug utility displays a window with information similar to that shown in Figure 51. (The information shown in Figure 51 displays the server in its initial start-up phase.) As data transfers occur, lines are displayed with a date, timestamp, and function control block (FCB) information.

Figure 51 NCS Debug Utility Output

```

16:29:22 02/13/97 FCB: o: 0 s: 0 l: 0 r: 0 s: 0 v: 0 n: 0 f: Network
16:29:22 02/13/97 FCB: o: 0 s: 0 l: 0 r: 0 s: 0 v: 0 n: 0 f: Port
16:29:22 02/13/97 FCB: o: 0 s: 0 l: 0 r: 0 s: 0 v: 0 n: 0 f: Connect
16:29:22 02/13/97 FCB: o: 0 s: 0 l: 0 r: 0 s: 0 v: 0 n: 0 f: CI
16:29:22 02/13/97 FCB: o: 0 s: 0 l: 0 r: 0 s: 0 v: 0 n: 0 f: Serial

```

Table 35 defines the FCB output lines and fields. Seven of the nine FCB fields are displayed; the DATAFLAGS and REVNBR fields are not displayed. The right-most field lists the FCB's destination.

Table 35 NASI Functional Control Block

FCB Field	Field Name and Description
o	OPCODE, request identification
s	SUBOPCODE, request identifier adjective (valid for some opcodes)
l	LENGTH, length (in bytes) of this FCB
r	RETURNCODE, value returned to user application
s	STATUS, function completion status
v	VCLPID, virtual circuit identifier (NASI identification information)
n	NACSCID, NCS connect table index
f	Destination of this FCB (function that will next process this FCB)

By observing the data transfers, you can determine if the sequences are correct and, possibly, determine where problems may exist.

Running NWCRPAIR

The NWCRPAIR.NCF is a troubleshooting utility that recovers corrupted Btrieve* files. Corrupted Btrieve files may be the result of a remote access server abend (terminate program execution abnormally). Use this utility if you receive an initialization failure when you bring up remote access with NWCSTART. Enter the following commands at the server console:

```
nwcstop  
unload cssysmsg  
nwcrpair
```

You will be prompted several times to press Enter as NWCRPAIR recovers the list of remote access database files. When NWCRPAIR finishes, you will be returned to the NetWare console prompt.

Then, bring up remote access with NWCSTART. Do not delete the Btrieve files unless the files are unrecoverable. If you delete the files, you will lose the remote access configuration. You will have to issue the following command to define the remote access services.

```
load svcdev sys:system\connect\svcs.def
```

After issuing the command, re-enter port and service configuration.

Remote Access Cabling

If problems occur with RS-232-C straight-through and null modem cables used to connect the adapter port or remote PC to a modem, use the information in Table 36 to select a cable type that connects properly to the computer and device you are using.

Table 36 Cable Type Capability

Cable Type	Capabilities
25-pin-to-25-pin straight-through modem cable	Connects an IBM PC or compatible computer to a straight-through standard DCE modem such as a dial-up modem, leased modem, line modem, or multiplexer.

Cable Type	Capabilities
9-pin-to-25-pin straight-through modem cable	Connects an IBM AT or compatible computer to a straight-through standard DCE modem such as a dial-up modem, leased modem, line modem, or multiplexer. You can use a 9-pin-to-25-pin cable because it converts the IBM AT's DB-9 connector to a DB-25 connector. (The male DB-25 connector of a 9-pin-to-25-pin cable is equivalent to an IBM PC or XT* serial port.)
25-pin-to-25-pin null modem	Connects an IBM PC or compatible computer directly to a standard DTE such as a communications server.
9-pin-to-25-pin null modem	Connects an IBM AT or compatible computer directly to a standard DTE device such as a communications server.

Common Problems

This section discusses various symptoms of common problems and their potential solutions.

WAN Board Loads, but It Has a Status of Down.

Ensure the board switch is set to the type of interface to which you are trying to connect. Some WAN boards can toggle between V.35 and RS-232.

Communications Adapters Installed on the Server Will Not Load or Initialize.

Each communications adapter installed on the server might not use a unique I/O port address. Ensure that each adapter uses a unique I/O port address. When you install the communications adapters used with the remote access feature, make sure you do not configure them to use the RAM allocated for your video adapter or any other adapters. For example, with WNIM+ adapters, the typical configuration is I/O port hexadecimal address 0280 for the first adapter, 0290 for the second adapter, 02A0 for the third adapter, and 02B0 for the fourth adapter. If you install other third-party communications adapters,

configure them according to their documented instructions and avoid configuring them with addresses used by other adapters in the PC. If you configure COM ports on the server for asynchronous communications, ensure that the driver program for the COM ports, AIOCOMX.NLM, does not assign addresses used by other hardware devices.

COM Ports Do Not Function or a Message Indicating They Are Not Available Is Displayed.

The IRQ values used by the I/O driver program conflict with the IRQ values used by other hardware devices in the server. Ensure that the IRQ values do not conflict. When you load the I/O driver program for the COM ports, AIOCOMX.NLM, you can specify the IRQ value used by the driver with the LOAD command. If you do not specify an IRQ value with the LOAD command for AIOCOMX.NLM, the driver assigns an IRQ value of 4 to the first port and interrupt 3 to the second port. If you are using COM2, ensure that your LAN adapter is not configured to use interrupt 3. Table 37 shows standard configurations used by hardware drivers.

Table 37 Standard Configurations Used by Hardware Drivers

Device	IRQ Number	I/O Port Address	Memory Address	DMA
COM1	4	3F8-3FF	—	—
COM2	3	2F8-2FF	—	—
COM3	—	3E8-3EF	—	—
COM4	—	2E8-2EF	—	—
LPT1	7	378-37F	—	—
LPT2	5	278-27F	—	—
AT diskette controller	14	1F0-1F8	—	—
Diskette controller	6	3F0-3F7	—	—
SCSI adapter	2, 3, 5	340-343	D0000-D7FFF	1, 3
Game I/O	—	200-20F	—	—
Hard disk controller (PC and XT)	—	B60-32F	—	—

Device	IRQ Number	I/O Port Address	Memory Address	DMA
MDA and printer adapter	—	3B0-3BF	—	—
VGA	—	3BA-3DA	—	—
EGA	—	3C0-3CF	—	—
CGA	—	3D0-3DF	—	—

If LPT3 is used, then use the values shown in Table 38.

Table 38 LPT Values

Device	IRQ Number	I/O Port Address	Memory Address	DMA
LPT1	7	3BC-3BE	—	—
LPT2	5	378-37A	—	—
LPT3	—	278-27A	—	—

Modem or Communications Adapters Take Too Long to Initialize.

Ensure that you are using Novell-certified communications adapters and that your drivers are up-to-date. Contact the manufacturer for an updated list of certified communications adapters.

The Modem Type of Your Modem Is Not Displayed in Remote Access as a Supported Modem Type.

Select a similar modem or Hayes* compatible. Hayes compatible works with most modems and is useful for troubleshooting.

You can also check the latest NWCMOD.EXE file at the WWW location <http://support.novell.com> to see if your modem has been recently added. Choose the search feature and enter NWCMOD.EXE for access to scripts. Novell updates NWCMOD.EXE periodically. Otherwise, use the modem script editing tool WMDMMGR.EXE in SYS:SYSTEM\UTILS to write your own modem scripts.

Ports and Modems

This section contains troubleshooting information for ports and modems and is divided into three categories:

- ◆ Troubleshooting Tools
- ◆ Configuration Tips
- ◆ Common Problems

Troubleshooting Tools

Load NIASCFG and select View Status for NIAS > Remote Access > Display Port Status, and then select the desired port and the following troubleshooting tools:

- ◆ Display Port Statistics—Displays current port configuration settings and potential problem areas. Take note of the Port Statistics section. Software overrun errors, framing errors, or parity errors could indicate phone line problems or PBX configuration problems. If the number of bytes received progressively increments and the number of bytes transmitted remains constant, then modem script incompatibilities or PPPRNS configuration errors might exist. Make sure that the modem type connected to the port matches the modem type configured for that port.

Check the PPPRNS configuration and verify that the Internetwork Packet Exchange™ (IPX™) address is unique across the WAN, including network segment addresses and internal IPX addresses.

- ◆ Start Trace on Port—Captures traffic sent to and received from the port.
- ◆ Terminal Mode—Verifies operation of the modem or device connected to the modem by using this operation to send data to and receive data from the AIO port.
- ◆ Identify Port—Identifies the physical port referenced by a port name by toggling the Data Terminal Ready (DTR) on the port.
- ◆ Use NWCRPAIR to repair the remote access database after a server abends.

You can view server configurations by loading NIASCFG and selecting Configure NIAS > Remote Access > Generate Configuration Report.

Configuration Tips

This section lists configuration tips that are useful for server configuration.

Inbound Port Service

Novell Internet Access Server 4.1 provides Remote Control Services—the ability of a remote workstation to dial in to the remote access modem pool and take control of a host on the LAN—through the Inbound Port Service. Use NIASCFG to configure this service (parameter path: Select Configure NIAS > Remote Access > Configure Services > NCS). The second line, General Name for Shared Dial-In Ports, displays DIALIN. This remote access service creates a modem pool used for dial-in connections. From a workstation running Win2NCS, select Options > Map Communication Ports. When you select Unique Name or Specific Name, the service name listed is a combination of the first eight characters of the Novell Internet Access Server 4.1 server name and the word DIALIN. For example, if the server name is RemoteAccess, the service name is REMOTEACDIALIN. A local workstation would not use this service for dial-out services.

You can view sessions on dial-in connections using NIASCFG (parameter path: Select View Status for NIAS > Remote Access > Display Service Status > tab to NCS > press F10).

Outbound Port Groups

For dialing out, use only the ports listed in NIASCFG in Dial-Out mode and in Both Dial-In and Dial-Out Port Usage (parameter path: Select Configure NIAS > Remote Access > Set Up...> Define Remote Access Port Usage). You can select outbound ports by group name or individual name. If you select a port by group name, the remote access software will select an available port within the port group.

Home Server

If you have configured a Home Server for a PPRNS user or container, ensure that the specified Home Server is running IPXRTR.NLM and is reachable by the remote access server.

Configuring IP

In NIASCFG, select Configure NIAS > Remote Access > Set Up... > Select Remote Access Services. Select PPRNS and press Enter. Select IP. Enter a valid IP address. This address serves as the IP address for the virtual interface that is set up by remote access. This address *must* be on a separate network (subnet) from the LAN. TCPIP.NLM version 3.01 or later must be loaded with IP forwarding enabled. This version allows the option of variable subnetting

and stub-subnetting. It also contains code that distributes IP addresses to dial-in clients. The remote access server allows for the configuration of a client address range. If addresses will be assigned from the server, enter the addresses at this point. If addressees will not be assigned, ensure that clients are entering IP addresses that belong to the unique PPPRNS subnet into their dialers.

ISDN

If you are using ISDN Synchronous Bus Adapters for remote access, make sure that you configure the ISDN interfaces using the NIASCFG Remote Access configuration menu. If you configure the ISDN interfaces using the NIASCFG Protocols and Routing menu, the interface functions only for routing.

If the server is using only ISDN, reduce the dialback parameter in NIASCFG so that the dialback takes place sooner (parameter path: Select configure NIAS > Remote Access > Configure Security > Set Global Parameters). The default dialback timer values are for analog modems. Values of 1 or 2 seconds are more appropriate for ISDN.

If the server is supporting both ISDN and analog modems, try using a value that is lower than the default. Make sure both analog and ISDN users are successfully called back. For example, try a value of 10 or 15 seconds. The limiting factors are how quickly the server's modem can hang up and reinitialize an outgoing call and how quickly the clients can hang up and reinitialize to listen for incoming calls.

ISDN Terminal Adapter

If you are using ISDN Terminal Adapters (TA) for remote access, make sure you use the configuration program provided by the manufacturer to configure the TA with the necessary information as specified by your ISDN provider. For example, the ISDN provider might require following settings, the Service Profile Identifier D-channel Protocol, (SPID) and Terminal Endpoint Identifier (TEI).

Port Modem Type

If a port name appears in the port configuration list but is not displayed in the port status listing, verify that the port modem type is not set to Unknown. Ensure that the port is configured for remote access use by selecting Configure NIAS > Remote Access > Set Up... > Select Remote Access Ports. If the port

in question is not listed, press Ins, highlight the correct port modem type in the list, and press Enter. If you have ports to which no modems are connected (direct connect ports), you must select Modem Type None for each port.

Common Problems

This section discusses various symptoms of common problems related to ports and modems and the potential solutions.

The port does not initialize.

Before a port can receive a call, the port must be in the WAITING state. Use NIASCFG (parameter path: Select View Status for NIAS > Remote Access > Display Port Status) to examine the port status. If the state of your port is any of the following, it is not capable of receiving any incoming calls for the remote access server.

- ◆ IDLE—Indicates that either the port is a dial-out-only port or that no remote access service (PPPRNS, ARAS, or NCS) is running that is configured to use this port for a dial-in connection. Determine whether the services you configured are running. Check the Restrict Service by Port configuration to verify that the service is allowed to use the port. If you modify the configuration so that this port is now used for a dial-in connection by a running service, the port status should change from IDLE to INITIALIZING to WAITING.
- ◆ WAITING—Indicates that you have configured remote access for Dial-In only or Dial-In and Dial-Out. If, after a successful dial has been completed, the port status changes to DISCONNECTED and remains there, try resetting the port to see if the status returns to WAITING.
- ◆ START UP—Indicates that the Service Selector is not running. Run NWCSTART.NCF from the server console prompt.
- ◆ BROKEN—Indicates that remote access has failed to initialize the modem attached to this port. This can be caused by a defective modem, a modem type mismatch in the configuration, or a cabling problem. Use NWCTERM.NLM to send characters to the modem so you can observe the modem's responses. A port status of BROKEN can also indicate that the AIO driver is not loaded.
- ◆ UNAVAILABLE—Indicates that the AIO driver that is providing this port is not loaded or is not registering this port to AIO.
- ◆ ACQUIREDOTHER—Indicates that the port is already acquired by other non-remote access server modules. For example, the port might have

been acquired by a routing component. Use NIASCFG to verify the remote access port usage configuration and the usage of ports by other components of the system.

- ◆ CONNECTING—Indicates that an incoming call has been received. The status changes from CONNECTING to CONNECTED as soon as the Service Selector determines to which service the call is destined. The call is then sent to the appropriate remote access server module. Use NIASCFG (parameter path: View Status for NIAS > Remote Access > Display Port Status) to view the call's destination.

You have added a new communications adapter to the server, but the ports on the adapter do not appear in the Port Configuration or Port Information window on the server console.

If you have multiple communications adapters in the server, ensure that they use I/O port addresses in the proper sequence. Refer to the adapter manufacturer's documentation for the proper sequence of I/O port addresses.

Also, complete the following checks:

- ◆ Use NIASCFG (parameter path: Select Configure NIAS > Remote Access > Set Up... > Select Remote Access Ports) to verify that the ports are selected for use with remote access.
- ◆ Ensure that the server's communications adapters are configured correctly and do not use I/O port addresses or memory addresses that conflict with other hardware.
- ◆ Verify that the AIO.NLM driver and the correct drivers for the adapters are loaded.
- ◆ Ensure that the LOAD parameters for the I/O drivers specified in the NETINFO.CFG file (in SYS: ETC\NETINFO.CFG) for each communications adapter match the switch setting on the adapters.
- ◆ Ensure that you have the latest drivers for the adapter.
- ◆ If the ports appear in the port configuration but not in the Display Port Status portion of the menus, use Config Port (parameter path: Select Configure NIAS > Remote Access > Configure Port) to verify that a modem type has been set for the port to a value other than Unknown.

Data transfer errors or a PC lockup occurs.

Interrupt settings for LAN boards or other devices conflict with PC COM port settings, causing data transfer errors or a PC lockup.

By default, many LAN boards, such as the NE2000™ board, use interrupt level 3. This conflicts with the default interrupt used by the second communications port, COM2. PC COM ports use interrupt level 3 or 4.

If you do not require more than one COM port, remove or disable the second COM port. If the second port is on an add-in board, remove the add-in board or change the jumpers on the board to disable the COM port. If you need to use the second COM port, change the LAN board to use an available interrupt level.

Modem or communications adapter takes too long to initialize.

Ensure that you are using Novell-certified communications adapters and that the drivers are up-to-date. Contact the manufacturer for information about updated drivers. Also verify that the modem type is specified correctly and that the latest modem scripts are being used.

The remote access software uses all available AIO ports, causing other NLM files on the server to generate error messages.

You might need to dedicate ports for server applications that are not part of remote access. To reserve a port for another application, use the NIASCFG utility (parameter path: Select Configure NIAS > Remote Access > Set Up... > Select Remote Access Ports). Select the desired port and press Del.

You want to determine which port a modem is using.

To determine which port a modem is using, display the port status for the desired port (parameter path: Select View Status for NIAS > Remote Access > Display Port Status) and select the desired port. Use the Identify Port menu option to toggle the port's DTR signal. This causes the modem's TR or DTR light to blink.

Modem or port initialization problems occur.

If the port status for a modem is displayed as Broken, perform the following procedures:

- ◆ Ensure that the modem type defined for the port matches the modem attached to the port. For information on certified modem scripts, refer to the WWW location <http://support.novell.com>. Choose the search feature and enter NWCMOD.EXE for access to scripts.

- ◆ Verify cable connections. Use Terminal Mode in NIASCFG (parameter path: Select View Status for NIAS > Remote Access > Display Port Status > Select a Port > Terminal Mode) to verify that modem cable connections are functional. Use the modem **ATI** commands and try to establish a dial-out connection using the **ATDT** command. You might need to issue an **ATE1** command to enable echoing back to the screen.
- ◆ If you are using a communications adapter, try placing the modem on the server's COM port. If you are not using a communications adapter, try switching the modem to another COM port.
- ◆ Try a different modem.

No users or only some users can access communications ports.

Use NIASCFG to generate a configuration report and verify that users have access to the ports (parameter path: Select Configure NIAS > Remote Access > Generate Configuration Report). Also, if the server is on a network that is connected to the workstation by a bridge or router, ensure that the bridge or router is operating correctly and that the user has access to the server. In addition, ensure that all hardware is installed correctly, including all add-on boards and cable connections. Consider resetting ports to reactivate them.

Verify that the container TEST has access to CONNECT object by completing the following steps:

- 1** Right click on container TEST.
- 2** Check TRUSTEES OF THIS OBJECT.
The CONNECT object should be displayed.
- 3** Select the CONNECT object to display the rights.
- 4** Correct the rights if required.

The port you are trying to dial in to in order to access PPRNS shows a status of connecting; however, the incorrect service is displayed (ARAS).

Make sure that you are using the correct modem configured for that port, that the modem is compatible with the modem on the server, and that the speeds are the same. Sometimes the modem forwards the V.42bis negotiation to the remote access software, thereby making the software process this call as an ARAS call.

Remote Access Server Configuration Problems

This section discusses various symptoms of common problems related to the server configuration and the potential solutions.

AppleTalk zones do not appear on the network.

Ensure that the network range you specify when you bind AppleTalk to ARAS is unique for each server on the LAN. The network range is specified when you load ARAS using NIASCFG. Keep in mind that each group of ports on the server running ARAS is considered to be a network.

Data transfer errors or a PC lockup occurs.

Interrupt settings for LAN boards or other devices conflict with PC COM port settings, causing data transfer errors or a PC lockup.

By default, many LAN boards, such as the NE2000, use interrupt level 3. This conflicts with the default interrupt used by the second communications port, COM2. PC COM ports use interrupt level 3 or 4.

If you do not require more than one COM port, remove or disable the second COM port. If the second port is on an add-in board, remove the add-in board or change the jumpers on the board to disable the COM port. If you need to use the second COM port, change the LAN board to use an available interrupt level.

More than one server is running Novell Internet Access Server 4.1, and one server does not show up on the network.

Ensure that all server names and IPX network addresses are unique and have not been assigned to other servers. Use NLIST to display the names of the servers on which Novell Internet Access Server 4.1 is running. Use IPXPING to verify if the server is reachable.

A remote access server halts unexpectedly.

If you have loaded the AIOCOMX driver, ensure that the interrupt specified by the int= parameter does not conflict with interrupts used by other hardware devices in the PC. If you do not specify an interrupt when AIOCOMX is loaded, the driver assigns default interrupts to the COM ports as follows:

- ◆ For one or two ports, AIOCOMX assigns IRQ4 to the first COM port found and IRQ3 to the second COM port found.

- ♦ For three or more ports, AIOCOMX assigns IRQ4 to the first COM port found and IRQ3 to the second COM port found. You are then asked for the IRQ value for any additional ports.

If you are using COM2 and COM2 is assigned IRQ3, ensure that your LAN adapter is not set to use IRQ3. Note that NE2000 uses a default IRQ3 setting.

You have restarted a server after loading the remote access software, and the server cannot find the license data, the server has corrupted the audit trail database, or the Remote Access Supervisor (NWCSU.NLM) reports problems logging in to the network.

Unload NIASCFG by exiting the utility. Enter **NWCSTOP** and verify that all NLM files were unloaded successfully. Unload all AIO drivers, including AIO.NLM. Enter **NWCRPAIR** at the system console prompt. Two unrecoverable errors, Butil-610-18 and Butil-610-9, might occur during the access of the sequential file. These errors are normal. If any other unrecoverable errors appear, corruption in the Btrieve Database has occurred.

Rename or delete the NWC*.BTR files in the system directory. If a backup copy of these files is available, restore the files.

If you do not have a backup copy from which to restore the NWC*.BTR configuration files, you must start from a blank configuration. To start from a blank configuration, complete the following steps:

- 1** Delete NWC*.BTR from SYS: SYSTEM.
- 2** Load SVCDEF SYS:\SYSTEM\CONNECT\SVCS.DEF at the system console prompt.
- 3** Enter port configuration and access control configuration information from the configuration report.
- 4** Restart the server and restart Novell Internet Access Server 4.1.

When you start the remote access software, error messages appear that indicate your server has insufficient memory.

The server might be using only the first 16 MB of memory. Use the MEMORY command at the NetWare console prompt to verify the amount of available memory. If the amount of displayed memory is less memory than you actually have, enter the REGISTER MEMORY command to make the additional memory available. Novell Internet Access Server 4.1 requires a minimum of 32 MB of RAM.

AIOPPTP Problems

Use the following information to isolate and resolve problems with AIOPPTP.

- ◆ Use PING to verify that a path exists between the PPTP Access Concentrator (PAC) and the Novell Internet Access Server 4.1.
- ◆ Verify that the PAC port has been configured with a PPTP Network Server (PNS) IP address that matches the Novell Internet Access Server 4.1 IP address.

Remote Node (PPPRNS and ARAS) Connections

This section contains remote node (PPPRNS) and AppleTalk* Remote Access Server (ARAS) connection troubleshooting information that is divided into four categories:

- ◆ Troubleshooting Tools
- ◆ Configuration Tips
- ◆ Troubleshooting Checkpoints
- ◆ Common Problems

If a problem that is general in nature occurs, the procedure described in *Troubleshooting Checkpoints* will help you isolate and resolve the problem. If a problem with a specific symptom occurs, refer to *Common Problems*.

Troubleshooting Tools

The following troubleshooting tools can be used to troubleshoot remote node connections:

- ◆ **PPPTRACE.** Refer to *Using the PPPTRACE Utility in the PPP* documentation.
- ◆ **AIO Port Trace.** Refer to *Activating Remote Access Port Traces*.
- ◆ **PING.** Refer to *Determining Whether a Remote TCP/IP Node Is Reachable in the TCP/IP* documentation.
- ◆ **IPXPING.** Refer to *Using the IPXPING Utility on the Server and Using the IPXPING Utility on the Workstation in the IPX* documentation.

Configuration Tips

We recommend the following guidelines for configuring remote access dial-in connections:

- ◆ By default, only Novell proprietary NWCAP authentication is enabled for Windows 95* and Windows NT* connections. Load NIASCFG to enable PAPRemote configuration and CHAP for PPPRNS (parameter path: Select Configure NIAS > Remote Access > Configure Services > PPPRNS > Configure Security).
- ◆ Assign remote client passwords to users who will be dialing in from Windows 95 or Windows NT dialers.
- ◆ For Windows 95 or Windows NT dial-in users who want to use PAP and CHAP authentication, they must use Remote Client passwords, not their NetWare[®] passwords. PAP and CHAP passwords are case-sensitive. For more information on Remote Client passwords, refer to Setting Remote Client Passwords.
- ◆ Novell's Remote Access Dialer for Windows 3.x (as well as older Novell Dialers) use NWCAP authentication. This enables remote users to use their NetWare passwords when dialing in.
- ◆ Windows 95 dialers can also use NWCAP authentication by using the latest Novell Client[™].
- ◆ Windows NT users establishing dialback connections should verify that Enable PPP LCP Extensions is enabled in Dial-Up Networking.
- ◆ Dialback failures are often caused by configuration errors. If you cannot find any errors in the configuration, use Audit Trail and PPPTRACE.
- ◆ The Novell dialback feature requires the NWCAP authentication method.
- ◆ For the dialback feature to work with the Windows 95 dialer, the server must be configured for Allow User to Request Dialback to Any Number or Force Dialback to a Caller Specified-Number.
- ◆ Dialback fails when the server is configured to Force Dialback to a Specific Number if the caller still provides a dialback number, even if the caller puts in the same number as the number specified on the server.

Troubleshooting Checkpoints

To isolate and resolve problems with remote node (PPPRNS) connections, complete the following tasks:

- ◆ Verify that PPPRNS is configured to support all the Authentication Protocols (NWCAP, PAP, or CHAP) that dial-in clients will use.
- ◆ Verify that users who will be using PAP or CHAP have remote client passwords defined.
- ◆ Verify that the PPPRNS Internetwork Packet Exchange™ (IPX™) network number is a unique IPX network number among all IPX servers on the network.
- ◆ Verify the following on Home Servers configured for users or containers.
 - ◆ They are reachable by all remote access servers that users (or users in containers) will be attempting to access. Load NIASCFG to verify (parameter path: Select Configure NIAS > Remote Access > Configure Services > PPPRNS > Set IPX Parameters > select any user > Home Server). Press Ins to display a list of servers visible to the remote access server.
 - ◆ They are running IPXRTR.NLM.
- ◆ If the remote access server is configured to use third-party security, make sure of the following:
 - ◆ The third-party security software is installed and configured properly.
 - ◆ PPP clients (dialers) are configured to open a terminal window (after the modem connection is made) in order to execute the third-party security processing.
 - ◆ Users are aware of the third-party security steps that are necessary and have the appropriate hardware or software to successfully pass the third-party security authentication.
 - ◆ The PPP dialers must use the same name that was used in the third-party security authentication to perform any subsequent PPP authentication. That is, the NetWare username that the third-party software associates with this connection is the same name that PPP authentication must use.
 - ◆ Verify in NIASCFG that the modem and cabling is configured correctly to send and receive AT commands and responses to the modem (parameter path: Select View Status for NIAS > Remote Access > Display Port Status > select a port > Terminal Mode).

- ◆ Verify in NIASCFG that all dial-in ports are in the Waiting State (parameter path: Select View Status for NIAS > Remote Access > Display Port Status).
- ◆ Check the port usage security restrictions to make sure that PPPRNS and the user are allowed to use the port in question.

If the users are unable to access any network resources, use the following checkpoints to help isolate the problem:

- ◆ In the CONFIG.SYS file, verify the following:
 - Files = 75 (minimum)
 - Buffers = 40 (minimum)
- ◆ Install the Novell Client for Windows 95 or the Novell Client for Windows NT on the workstation before you install Dial-Up Networking or Remote Access Server (RAS).
- ◆ In the NIASCFG utility on the server, verify the following:
 - ◆ Specified Home Server is running IPXRTR.NLM.
 - ◆ PPPRNS IPX network address is unique.
 - ◆ Specify IPX Address for users is set to No.
- ◆ Set the data rate to 19,200 when you use AIOCOMX.
- ◆ On the file server, perform the following:
 - ◆ Apply the current driver for the communications adapter.
 - ◆ Try connecting the modem to a COM port to bypass the communications adapter.
 - ◆ Set Reply to Get Nearest Server = ON.
 - ◆ Apply all current OS, CLIB, and Sequenced Packet Exchange™ (SPX™) patches.
 - ◆ Set Maximum Packet Receive Buffers = 2000.
 - ◆ Set Minimum Packet Receive Buffers = 500.
 - ◆ Apply all current Novell Directory Services™ (NDS™) patches for NetWare.
 - ◆ Decrease the DCE-to-DTE data rate to 57,600. Use the modem script editing tool, WMDMMGR.EXE, in SYS:SYSTEM\UTILS to change this value. This modem script editor is also available from the WWW location <http://support.novell.com>. For more information,

refer to *Using the WMDMMGR Utility in the documentation for Modems*.

If ARAS users are able to make a connection but cannot log in to a server, complete the following steps:

- 1** Open the Control Panel folder and double-click the MacIPX icon.
- 2** Select the AppleTalk icon.
- 3** Select an IPX gateway.
- 4** Exit MacIPX and close the folder.

If you cannot find an IPX gateway, make sure the software is loaded on your remote access server.

Common Problems

This section discusses various symptoms of common problems related to PPPRNS connections and AppleTalk Remote Access Server (ARAS) connections and the potential solutions.

PPPRNS client does not receive configured IP domain information.

Ensure that DHCPD.NLM is loaded on the server running the remote access software. DHCPD.NLM must be loaded in order to pass the domain information to the client.

Also, load NIASCFG and select Configure NIAS > Remote Access to verify that the PPPRNS IP parameters for the user's container includes domain information, such as domain name and address.

NOTE: Windows 95 uses a proprietary protocol that does not request (or receive) Domain Name System (DNS) information provided by the DHCP services on a Novell Internet Access Server 4.1 server. This prevents Windows 95 Dial-Up Networking from receiving IP DNS information from the Novell Internet Access Server 4.1 server.

Users report a timeout error while waiting for a modem response.

This condition might be caused by heavy traffic or delays in response. Access the Port Settings dialog box for the desired PhoneBook entry. Increase the Seconds to Wait After Dialing setting. By default, this value is set to 60 seconds.

This condition might also be caused by a faulty RS-232 cable or the cable not being secured at both the serial port and modem connections.

Remote PPP users cannot establish a NetWare Core Protocol™ (NCP™) connection. After entering F:, users are returned to the C: prompt. If users attempt to log in from the C:\NWCLIENT or C:\NOVELLCLIENT32 directory, an NCP connection error message appears.

Cause 1— Users are configured for a Home Server that is not visible from the server running the remote access software.

NOTE: You must first unload NWCCON.

From NIASCFG, select Configure NIAS > Remote Access > Services > PPPRNS > Set IPX Parameters. Select the desired username and press Enter. Select Home Server and press Enter. In the Home Server field, either specify a home server that the current server can route to or leave the field blank. Make sure that the Home Server is running IPXRTR.NLM.

Cause 2— The Maximum Packet Receive Buffers value is too low.

Make sure the remote access server has been configured with a sufficient value for Packet Receive Buffers. Typical values are 500 minimum and 1000 to 2000 maximum depending on LAN/WAN traffic.

During an attempt to establish a PPPRNS connection, an error occurs indicating DCD carrier detect is off.

This condition could be due to a modem script problem or defective modem. If your modem uses the standard Hayes command set, use one of the Hayes Compatible modem scripts or try a different modem. You can also try a null-modem connection.

This condition could also be due to the server expecting third-party security on the PPP client but the client is not properly configured to go through the authentication process before sending PPP frames. Configure the client to open a terminal window after modem connection is established to execute the authentication process.

PPPRNS Windows 95 client reports that authentication failed.

Ensure that the client is specifying the complete NDS username and the correct remote client password. PAP and CHAP remote client passwords are case-sensitive. Ensure that CHAP is enabled in PPP security on the client. Ensure that PAP and CHAP security options are enabled on the server.

When the Windows dialer is executed, the following message is displayed: Dialer tried to open a communication port, but none was available.

Ensure that the port is enabled and not in use by another application. Also, ensure that the correct port is specified in the configuration.

Calling card bong tone not supported by modem.

If your modem is not waiting for the correct bong tone from the ISP before sending calling card details, refer to the modem documentation to determine the character that the modem supports. Usually, the ampersand (&) is used by the modem to instruct it to wait for the bong. If your modem does not support the use of the ampersand, edit the dialing string to use a different character, such as dollar sign (\$). If your modem does not support a different character, use commas to specify a time interval. Start with two commas.

Dialback fails.

Dialback failures are most often caused by configuration errors. If you cannot find any errors in the configuration, use Audit Trail and PPPTRACE.

The following are additional configuration guidelines:

- ◆ Windows NT users should verify that the Enable PPP LCP Extensions is enabled in Dial-Up Networking.
- ◆ When the Novell dialer is used, the dialback feature is effective only if the NWCAP authentication method is used.
- ◆ When the Windows 95 dialer is used, the dialback feature will work if the server is configured for Allow User to Request Dialback to Any Number or Force Dialback to a Caller-Specific Number. In the latter case, the caller must provide a dialback number.
- ◆ When the server is configured for Force Dialback to a Caller-Specific Number, dialback fails if the caller provides a dialback number, even if the number is identical to the one entered on the client.

ARA 1.0 clients can log in, but PPP clients cannot.

When both the ARAS and PPRNS services are in use, a workstation dialing in using a modem with V.42bis compression will try to connect using ARAS (as seen at the server console). The reason is that ARA 1.0 packets have the same headers as V.42bis packets. ARA 2.0 packets do not present this problem.

Use the following checkpoints to resolve the problem:

- ◆ Change Support Apple Remote Access Client Version to 2.0 only. Only ARA 2.0 clients can connect, but this allows PPP clients to use the same ports as ARA clients.
- ◆ Assign separate ports for ARAS and PPRNS.
- ◆ Disable V.42bis on the modems.

ARA clients are unable to establish a connection to Novell Internet Access Server 4.1 remote access, but PPP clients can.

Most ARA dial-in problems are related to modem scripts. Use the latest ARA-specific modem script for your modem from the modem manufacturer. The Novell Labs™ group does not create modem scripts for ARA.

Remote Control (NCS) Connections

This section discusses various symptoms of common problems related to remote control (NASI™ Connection Services [NCS]) connections.

You cannot see ports under Win2NCS.

Not being able to see a list of NCS ports displayed in Win2NCS often indicates a security problem. If you enter an incorrect username or context in the Set Security window of the Win2NCS Mapping Utility, you are prevented from seeing NCS resources in the Map Communication Ports window. Verify that you have the proper context entered and that you have the proper rights to use the CONNECT Object.

Users dialing in with a remote control application have trouble connecting.

Use usernames and passwords that contain only alphanumeric characters without spaces. Enter the complete NDS name and remote client password when prompted. Also, consider reducing the baud rate.

Another troubleshooting tool is a null modem cable. Use a null modem cable for a direct connection to the remote access software to eliminate modem incompatibilities.

No NCS service names are displayed when a user dials in to remote access.

If the remote control software has just been started, wait a few minutes and retry the request. Service names might not have been broadcast to the network. Also, a user can only access sessions owned by the user or general sessions. Verify that such sessions have been brought up on the network.

Windows 95 Connections

This section contains troubleshooting information for using Windows 95 with the remote access software. This information is divided into two categories:

- ◆ Configuration Tips
- ◆ Troubleshooting Checkpoints

Configuration Tips

The Windows 95 tool, DEVICE MGR, can also be used to troubleshoot. For information on DEVICE MGR, refer to your Windows 95 documentation.

Follow the procedure under Preparing the Server to prepare a Novell Internet Access Server 4.1 server for use with the Microsoft Windows 95 Dial-Up Adapter client. Explanations of different client configurations and the protocols they allow are also included.

Preparing the Server

To connect to PPRNS from Windows 95, PAP or CHAP must be turned on through NIASCFG (parameter path: Select Configure NIAS > Remote Access > Configure Services > PPRNS > Configure Security).

NOTE: PAP and CHAP use the remote client password, which must be set through NIASCFG > Configure NIAS > Remote Access > PPRNS > Configure Security or, if you applied the latest Novell Client update, through the Check/Set Remote Password utility under Novell Dial-Up services.

Preparing the Workstation

To use the Windows 95 Dial-Up Adapter to access a Novell Internet Access Server 4.1 remote access server, either the Novell Client for Windows 95 or the Microsoft Client for NetWare Networks should be installed. If the

Microsoft client is used, the Protocol Service for NDS and the latest Service Pack should be installed on the client. Both are available from Microsoft.

If the Dial-Up Adapter software is not installed, complete the following steps to install it:

- 1** From the Control Panel, double-click Add/Remove Programs.
- 2** Click Windows Setup.
- 3** Double-click Communications.
- 4** Check the box for Dial-Up Networking, then click OK.
- 5** Click Apply and insert the Windows 95 media as requested.
- 6** Click OK to exit.

After the Dial-Up Adapter is installed, the client must be installed.

For an IPX connection that uses the Novell client, verify that at least the following network components are installed:

- ◆ Novell Client for Windows 95
- ◆ Dial-Up Adapter
- ◆ IPX 32-bit protocol
- ◆ IPX/SPX-compatible protocol

Alternatively, for an IPX connection that uses the Microsoft client, verify that at least the following network components are installed:

- ◆ Microsoft Client for NetWare Networks
- ◆ Dial-Up Adapter
- ◆ IPX/SPX-compatible Protocol Service for NDS, as required

For an IP connection using the Novell client, verify that at least the following network components are installed:

- ◆ Novell Client for Windows 95
- ◆ Dial-Up Adapter
- ◆ TCP/IP

Alternatively, for an IP connection that uses the Microsoft client, verify that at least the following network components are installed:

- ◆ Microsoft Client for NetWare Networks

- ◆ Dial-Up Adapter
- ◆ TCP/IP

To configure the Dial-Up Adapter, complete the following steps:

- 1** Double-click Dial-Up Networking.
- 2** Double-click Make New Connection.
- 3** Follow the prompts to create the icon.
- 4** Right click the new icon, then click Properties.
- 5** Click Server Type.
- 6** Set Type of Dial-Up Server to PPP: Windows 95, Windows NT 3.5, Internet.
- 7** Uncheck NETBEUI.
- 8** If you will be using only IPX, uncheck TCP/IP. If you will be using only IP, uncheck IPX/SPX.
- 9** If desired, click TCP/IP Settings to configure the TCP/IP protocol parameters. (Consult your network administrator for details on TCP/IP configuration.)
- 10** Click OK to exit.
- 11** Double-click the icon just created to dial in and connect to the server running the remote access software.
- 12** Ensure that the username (with context, for example username.orgunit.organization) is correct.
- 13** Provide the password. Use the remote client password instead of the NetWare password.
- 14** Click CONNECT to dial in and connect to the server.

Troubleshooting Checkpoints

To isolate and resolve Windows 95 connection problems, complete the following tasks:

- ◆ If Require Encrypted Password is checked in the Properties of the Dial-Up Networking folder, make sure that CHAP is enabled on the server.
- ◆ Ensure that Frame Type is set to AUTO.
- ◆ Ensure that SPX connections are set between 60 and 90.

- ◆ Make sure that NETBEUI is not bound to the Dial-Up Adapter.

If you have Novell Client for Windows 95 installed and the remote client is dialing in using IPX, Intranetware Client should make the connection. If it does not, complete the following steps on the server:

- 1 Load NIASCFG.
- 2 Select Configure NIAS > Remote Access.
- 3 Select PPRNS (it should be set to Yes) and press Enter.

Make sure that the IPX number for the PPRNS service is unique and is not being used by the server or any other device on the network.

NCS Dial-Out Connections

This section contains configuration tips for dial-out problems related to Dial-out connections: NCS NASITM Connection Services (NCS) connections.

Configuration Tips

Use NIASCFG to configure NCS on the Novell Internet Access Server 4.1 server (parameter path: Select Configure NIAS > Remote Access > Configure Services > NCS). Use the following information to determine your use of the Modem-Independent Group option.

The NCS Configuration Options menu contains the Modem-Independent Group option. This option is used to configure a group of ports to be modem-independent so that modems from different vendors can be added to a single modem-independent group. The advantages are that third-party applications can use the dial-out modem pool more easily and that you can restrict dial-out numbers.

Unfortunately, improper use or misunderstanding of this option's limited capabilities can cause problems. If you do use this option, use the following guidelines:

- ◆ When configuring NCS, do *not* select ANY_PORT in the Modem-Independent field.

The default value is None. Selecting ANY_PORT means that all the modems are limited to a small set of industry-standard AT commands. For a list of the commands, refer to Modem Commands in the *Commands for Modem Independent Ports Reference*.

- ◆ If you create and configure a port group name using the Configure Port Group option, and then select the name in the Modem-Independent Group field, modems will still be limited to a small set of industry-standard AT commands.

Symptoms you might encounter when you configure and use a port group name in the Modem-Independent Group field are as follows:

- ◆ Applications are unable to dial out.
- ◆ Applications can communicate at only 300 bps.
- ◆ Applications are unable to connect to an NCS port.
- ◆ Applications are unable to identify the modem correctly.
- ◆ Applications (such as pcANYWHERE*) might encounter a General Network Error.
- ◆ Applications receive errors when initializing the modem.
- ◆ Applications are unable to dial out using 7,E,1.

Win2NCS Connections

This section contains Win2NCS software troubleshooting information that is divided into two categories:

- ◆ Configuration Tips
- ◆ Common Problems

NOTE: Online help for Win2NCS provides you with an overview of its functionality, installation instructions, and information about using Win2NCS. Additional troubleshooting issues and tips are also included.

Configuration Tips

You can change the way configuration files are handled at any time by changing the networked entry in the configuration section of the USER.INI file as follows:

- 0 = Config files in installed directory
- 1 = Config files based on Logged-In name (includes context).
- 2 = Config files always on drive C.
- 3 = Config files in Windows directory.
- 4 = Config files based on User name (ignores context).

These changes will take place the next time you start Win2NCS.

You can use the Win2NCS Mapping Utility to change the mapping of a COM port, even if the port is presently redirected and active. However, the mapping only applies to the next time the COM port is used; it will not cause the present connection to be redirected.

Common Problems

This section discusses various symptoms of common problems related to Win2NCS connections and the potential solutions.

Dynamic Port Redirection Is Not Working

You do not see Win2NCS messages when using the Win2NCS Mapping Utility or an application that communicates with the COM port through Win2NCS.

- ◆ Check with your system administrator to make sure that the username and password that you are using have been assigned services by your NASI Connection Services (NCS) server. Your network login name and password might not be assigned any services, and you might be required to use another username and password to acquire services. You can also test the security to determine whether this information is active.
- ◆ If you are using Prompt For 4x Context, make sure that your context is correct.
- ◆ If you are using Windows for Workgroups, you must disable the Microsoft-compatible Internetwork Packet Exchange™ /Sequenced Packet Exchange™ (IPX™ /SPX™) driver so that the Novell IPX/SPX driver is used instead. For more information, refer to Windows for Workgroups 3.11 Driver Issues

Focus Might Not Be Restored Correctly after a Win2NCS Redirection Message Is Displayed

When you are using Windows NT, the cursor might not be restored correctly to the Communications Application window after a Win2NCS redirection message is displayed. In most cases, Windows NT ignores the System Modal capability of the Win2NCS redirection message. This response causes the communications application to run at the same time as the redirection message. If the communications application changes the window while the redirection message is displayed, the focus is restored to the incorrect window.

Although this can be a benefit, it can also be a disadvantage because the user must manually restore the focus to the Communications Application window.

It Takes a Long Time to Find Available Modems

At large sites that have many NetWare[®] servers, it might take a long time to find available modems (acquire a service) when using Win2NCS Redirection. For example, there are four available services on two NCS servers from a network containing 20 NCS servers. Because the Redirector does not know on which server the services you require reside, it must contact each server to request services information. If the servers you require are some of the last to be contacted, the wait can be quite long, especially if some of the servers are on routers. Two possible solutions are as follows:

- ◆ Use the Define Server Restrictions option to select only the servers from which you would want to acquire services. Then, only the servers that you defined would be used for the query.
- ◆ Use Manual Mapping with wildcards (asterisk and question mark) to restrict the servers searched.

No Communication Ports Assigned to Windows 95

Communication ports are not assigned to Win2NCS if all COM ports (1 through 8) are already assigned to hardware. If you have an eight-port COM board in your system, COM1 through COM8 have probably been assigned to that board. To assign a COM port to Win2NCS, complete the following steps:

- 1** Manually remove some of the COM port assignments using the Windows 95 Control Panel (system icon).
- 2** Run Win2NCS Setup again.
- 3** Map the chosen COM ports to Win2NCS.

Problems with Win2NCS after Reinstalling Windows 95

If you experience a problem with Windows 95 that is unrelated to Win2NCS and decide to reinstall, port assignments might be changed. The reason is that when Windows 95 is reinstalled, the device manager searches for all available hardware. Because Win2NCS does not use any hardware, the device manager assumes that the ports were configured incorrectly and reassigns them as standard COM ports. To reassign the COM ports, complete the following steps:

- 1** Run Win2NCS Setup.

Win2NCS recognizes the reassigned ports as not attached to hardware and prompts you to unassign the ports so that they can be reassigned.

2 Click Yes.

The ports are reassigned.

Modems Frequently Disconnect

Modem disconnects are most often caused by either bad lines or incorrect modem selections. Make sure that you select the correct modem type. If you are using a pool of modems and if you used a wildcard selection (asterisk and question mark) with the Win2NCS Mapping Utility, make sure that all possible ports in the wildcard selection have modems that are identical.

To determine whether the modem is the source of the problem, complete the following steps:

- 1** Map a unique service to a COM port using the Win2NCS Mapping Utility.
- 2** In Windows 95, select the correct modem type (parameter path: Select Settings > Control Panel > Modems).
- 3** Run the application to determine whether its performance is improved.

Time to Redirect Is Slow

If your Map Communications Ports option is usually fast, but it has recently become slower and is displaying a Searching Server message, your network might have an NCS server that is broadcasting into the network but will not allow Win2NCS to contact it. Ask your system administrator to put a filter on the router to stop the broadcasts into the network. You can also set the Query Service Timeout in Global Options to a lower value to terminate the search earlier.

Cannot Switch to Another Application

While Win2NCS is initializing (for example, acquiring ports), you cannot switch to another application.

Wait until initialization is completed before switching applications. While Win2NCS is acquiring ports, it runs exclusively. Other processes cannot be started during the few seconds that the Win2NCS is taking place.

COM Port Is Not Redirected

If the Win2NCS Redirector does not direct the COM port to NCS and you do not see any information messages from the Win2NCS Redirector when you start the application, first make sure that Win2NCS Redirection is enabled. If Win2NCS Redirection is enabled, make sure that the COM port is mapped correctly and that Redirector Informational Messages is enabled in Global Mapping Options of the Win2NCS utility.

Windows for Workgroups 3.11 Cannot Find Any Services

Remove support for Microsoft Networking by removing the IPX/SPX compatible driver selection in Windows for Workgroups 3.11.

To remove support for Microsoft Networking permanently, complete all the following steps. If you plan to use Microsoft Networking later, complete only Step 1 through Step 5.

- 1** Double-click the Network icon in the Program Manager or Control Panel in Windows 95.
- 2** Double-click Network Setup.
- 3** Click Drivers.
- 4** In the Drivers box, select IPX/SPX Compatible Transport with NetBIOS.
- 5** Click Remove and follow the instructions.

Stop here and restart windows if you do not want to remove support for Microsoft Networking permanently.
- 6** In the Network Setup window, select Networks.
- 7** At the bottom of the window, select the radio button labeled Install Windows Support for the Following Network Only.
- 8** Use the scroll bar to locate Novell NetWare (Workstation shell 4.0 and later).
- 9** Click OK on both windows.
- 10** Restart Windows for the changes to take effect.

Windows for Workgroups 3.11 Driver Issues

Windows for Workgroups should support the same applications as Windows 3.1 Enhanced Mode if the Microsoft IPX/SPX Compatible Transport Driver

is *not* installed. When the Microsoft driver is not installed, the Novell IPX/SPX driver is used. With the Novell driver, NetBIOS packets are not routed.

If the Microsoft driver is used, the Mapping Utility and Redirector might not operate properly. This is due to incompatibilities in the SPX implementation in the Microsoft driver.

Services Are Displayed in the Win2NCS Mapping Utility but Not in Dynamic Redirection

The Win2NCS Mapping Utility displays all services associated with the user, whether or not the services are busy. This allows the user to map any service for possible future use. However, the Win2NCS Redirector only displays services that are presently not being used by someone else. In this case, probably all the services are in use by others.

Mac2NCS Connections

This section contains Mac2NCS software troubleshooting information that is divided into three categories:

- ◆ Configuration Tips
- ◆ Troubleshooting Checkpoints
- ◆ Common Problems

If a problem that is general in nature occurs, the procedure described in *Troubleshooting Checkpoints* will help you isolate and resolve the problem. If a problem with a specific symptom occurs, refer to *Common Problems*.

Additional troubleshooting information is provided in the Mac2NCS README file.

Configuration Tips

We recommend the following guidelines for troubleshooting Mac2NCS connections:

- ◆ This product supports the stop bit settings of 1 and 2. It does not support a setting of 1.5.
- ◆ To ensure proper modem initialization, make sure that the modem script and the modem used on the server match. A mismatch might result in disconnection problems.

- ◆ If you anticipate using Mac2NCS for repeated transfers of extremely large files over a fast link, consider performing the following procedures:
 - ◆ Open the Control Panel within the System Folder, double-click the MACIPX icon, and select Advanced Options. Set the value of Default Retry Count in the SPX parameters box to 100 or another high value.
 - ◆ Ensure that the Ethernet driver is an Apple* built-in Ethernet driver that is version 1.01 or higher.
 - ◆ If the receiving device appears to fail between file transfers, insert a delay between the file transfers.

Troubleshooting Checkpoints

To isolate and resolve Mac2NCS connection problems, complete the following tasks:

- ◆ Make sure that your modem type is correctly identified in the Specific Name and General Name fields in the Chooser menu.
- ◆ Use the modem script supplied by your modem's vendor.
- ◆ Avoid setting software flow control if possible.
- ◆ If you must modify a vendor-supplied modem script, use the following guidelines:
 - ◆ Use the modem command AT&D0 to configure your modem to ignore the DTR lines.
 - ◆ Make sure the line rate (modem transmission speed over the phone wire) and the port rate (modem communication speed with a host computer) are not synchronized. Refer to Common Problems for examples of this issue.
 - ◆ If your modem stops responding when you try different speeds, check the availability of the port selection on the Chooser menu. If the port is not available, ask your system administrator to reset the port and restart your Macintosh.

Common Problems

This section discusses various symptoms of common problems related to Mac2NCS connections and the potential solutions.

You cannot use the Mac2NCS Chooser because of a Type 1 error.

There is a conflict between the Mac2NCS drivers and the drivers in your system. To use Mac2NCS, you must identify and remove the conflicting drivers. First, identify a basic set of drivers that allow Mac2NCS to function without the Type 1 error. All system drivers are located within the Extension or Control Panel folders of the System Folder. Move all nonessential Extension folder and Control Panel objects to different folders (Unused Extension and Unused Control Panel, for example). Restart your Macintosh system.

After you have established a basic set of functioning drivers, you can identify the conflicting driver by moving the unused objects back to their original folders until the Type 1 error reoccurs.

After you click Chooser Setup, a message states that no server was found or another error message appears.

Ensure that all modules are installed correctly and that the desired servers are accessible to your Macintosh. Open the remote access Mac Client folder (or diskette), open the Mac2NCS folder, drag the IPXNetStat application into the System Folder, and answer yes to the prompt. This adds IPXNetStat to the Apple menu. From the Apple menu, select IPXNetStat and enter **394** in the Query type field. A report of all the Novell Internet Access Server 4.1 servers accessible to your Macintosh appears. If IPXNetStat does not function properly, check the physical connection to the LAN and reinstall Mac2NCS.

If the desired server is accessible, reinstall Mac2NCS by clicking the Installer icon within the remote access Mac Client folder (diskette).

When you use a modem application, a message states that the attempt to use a remote access port has failed.

Verify port access by first clicking SetUp in the Mac2NCS Chooser. In the remote access Login window, enter your password and click Continue. The remote access Port Selection window appears. Ensure that the desired remote access port can be selected. Also, ensure that there are no other configuration errors. Exit the Chooser and try the modem application again. If the message appears, contact your system administrator.

Mac2NCS cannot detect a modem even though it is configured to use the modem.

Verify that the Redirect to LAN buttons in the Mac2NCS Chooser are set to On. Also, ensure that the serial port selected by the modem application matches the serial port selected by the Mac2NCS configuration.

You cannot dial out with Mac2NCS.

From the Chooser menu, select Mac2NCS. In AppleTalk Zones, select a zone. Click Setup and enter the User ID, Context, and password of a valid Novell Directory Services™ (NDS™) user. Click Options and then select Server, General Name, and Specific Name. Click OK to return to the Chooser main menu. If the only option that appears is Any Available, there is a communication problem between the server and the workstation. Use NIASCFG on the server to troubleshoot the server configuration (parameter path: Select Configure NIAS > Protocols and Routing > Protocols > AppleTalk).

If the application you are using is Mac2NCS aware, set Redirect to LAN to Off in the Chooser. Within the application you are using, change Modem Port to Mac2NCS. If the application is not Mac2NCS aware, set Redirect to LAN to On. Within the application, change Mac2NCS to Modem Port.

Your modem application uses a stop bit setting of 1.5.

Most AIO drivers on the server do not use a 1.5 stop bit setting. Instead, use a stop bit setting of 1 or 2.

Your modem application uses a bps rate of 12,000, 14,400, 28,800, or 33,600.

Set the bps rate to the next highest rate. Supported bps rates above 9,600 are 19,200, 38,400, 57,600, and 115,200. For example, if you want to use a bps rate of 12,000, instead, use the next higher supported rate of 19,200.

Using a 14,400-bps V.32bis modem, you cannot establish a connection to Novell Internet Access Server 4.1.

Remove the AT-extended commands &Q0 and &M0 from the initialization script string. These commands instruct the modem to use Direct Asynchronous mode, which eliminates buffering and requires the line speed to match the port speed. Because remote access ports do not support 14,400 bps, a mismatch of port and line speed causes the connection attempts to fail. These problems do not occur on modems with 9,600-bps or lower ratings.

Clicking the Redirection On and Redirection Off buttons in the Mac2NCS Chooser interface does not change the Redirection setting. In addition, the diagnostic claims another application is still using the serial driver, but you cannot find this application in the Finder.

Restart your system. The serial driver was not closed properly by the last application using it.

As you attempt to establish a connection while using a client program from an online service or from a bulletin board software package, a message states that the modem does not respond properly.

This can be caused by mismatched modem types between the application and the remote access port. Ensure that the modem type used by the application matches the modem type configured for the remote access port. Also, ensure that the remote access port is not configured as a modem-independent port.

You do not want to use hardware flow control with a Bocamodem* 14,4000-bps V.32bis modem.

The remote access software initializes a Bocamodem 14,400-bps V.32 modem to use hardware flow control. If you do not want to use hardware flow control, send the modem the AT&K0 command to cancel the hardware flow control mechanism for the modem.

You have problems downloading large files from online services.

Make sure you have the latest version of the online service installed on your Macintosh.

You cannot see your Novell Internet Access Server 4.1 server on the Login window, but other servers are visible.

Your preferred server is not responding to the SAP query generated by Mac2NCS. Contact your network administrator.

You have selected 115,200 bps or 230,400 bps, but data transfer seems to be using a much lower rate.

Sometimes an application simply does not support these rates, even though the selection is available on the application's user interface. Contact your network administrator.

You cannot establish a connection to an online service or bulletin board using 14,400 bps or 28,800 bps.

The reason might be that the application does not support these rates, even though they appear on the application's user interface. Contact your network administrator. The solution is usually specific to a particular modem type.

One possible solution is to configure your online service software to use only a 9,600-bps or lower rate and then dial in to an online service that supports 9,600-bps or lower rates.

Login Problems

This section discusses various symptoms of common problems related to the login process and the potential solutions. If, after connecting, users are unable to access any network resources, use the following list of troubleshooting guidelines to isolate the problem:

- ◆ In the NET.CFG file, verify the following for a Windows 3.x workstation:

```
SPX Connection = 60
```

```
For NetWare 4.x (or later): Preferred Tree = <tree name>
```

```
For NetWare 4.x (or later): NetWare Protocol = NDS, Bind
```

The NetWare Protocol statement might also specify one protocol if the server environment is homogenous (all NetWare servers of the same version).

- ◆ In the CONFIG.SYS file, verify the following:

```
Files = 75 (minimum)
```

```
Buffers = 40 (minimum)
```

- ◆ Install the latest Novell Client™ software or Virtual Loadable Module™ (VLM™) client software on the workstation before you install the dialers.
- ◆ In the NIASCFG utility on the server, verify the following:
 - ◆ Any specified Home Server is running IPXRTR.NLM.
 - ◆ Any user-specified IPX address is not duplicated in the network. To verify duplication, remove the address from the user's configuration. If the user can access the network, the IPX address must be a duplicate. Make sure that all user-specified IPX addresses are unique.

- ◆ PPPRNS IPX network address is unique.
- ◆ On the file server, perform the following:
 - ◆ Set Reply to Get Nearest Server to ON.
 - ◆ Apply all current OS, CLIB, LAN, and Sequenced Packet Exchange™ (SPX™) patches.
 - ◆ Apply all current Novell Directory Services™ (NDS™) patches for NetWare.
 - ◆ Set Maximum Packet Receive Buffers to 2000.
 - ◆ Set Minimum Packet Receive Buffers to 500.

If the user is unable to establish a PPP connection at all, use the following list of troubleshooting tips to help isolate the problem:

- ◆ In the NIASCFG utility, verify that security for NWCAP is enabled. If the user is using the Novell Mobile Dialer, verify that CHAP or PAP is enabled. If the user is using Windows 95 dial-up networking, verify that the user has a remote client password configured.
- ◆ Connect the modem on a COM port to bypass the communications adapter.
- ◆ Set the data rate to 19,200 when you use AIOCOMX.
- ◆ Apply the current driver for the communications adapter.
- ◆ For NetWare 4.x or later, make sure that the Connect Rights Level is set correctly to allow the user to be authenticated by this server.

The Container context (Connect Rights Level) is defined when you create the CONNECT object in the NDS tree during Novell Internet Access Server 4.1 installation. All users in the Connect container and below can access remote access, except those users in containers that are blocked with the Inheritance Rights Filter. A user not belonging to the Container context might fail to establish a connection.

Use NIASCFG (parameter path: Select Configure NIAS > Remote Access > Generate Configuration Report > Screen) to determine whether Connect Rights are set correctly.

Use NWADMIN to verify or grant additional rights of the CONNECT object for the server. The CONNECT object requires Browse rights to all properties of the user object to authenticate the user.

- ♦ Decrease the DCE-to-DTE data rate to 57,600. Use the modem script editor, WMDMMGR.EXE (in SYS:SYSTEM\UTILS), to change this value for the modem.

A

Novell Trademarks

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

Advanced NetWare is a trademark of Novell, Inc.

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

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppTester is a registered service mark of Novell, Inc. in the United States and other countries.

BrainShare is a registered service mark of Novell, Inc. in the United States and other countries.

C-Worthy is a trademark of Novell, Inc.

C3PO is a trademark of Novell, Inc.

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

Certified NetWare Administrator in Japanese and CNA-J are service marks of Novell, Inc.

Certified NetWare Engineer in Japanese and CNE-J are service marks of Novell, Inc.

Certified NetWare Instructor in Japanese and CNI-J are service marks of Novell, Inc.

Certified Novell Administrator and CNA are service marks of Novell, Inc.

Certified Novell Engineer is a trademark and CNE is a registered service mark of Novell, Inc. in the United States and other countries.

Certified Novell Salesperson is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

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

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

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

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

Custom 3rd-Party Object and C3PO are trademarks of Novell, Inc.

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

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

ElectroText is a trademark of Novell, Inc.

Enterprise Certified Novell Engineer and ECNE are service marks of Novell, Inc.

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

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

EXOS is a trademark of Novell, Inc.

Global MHS is a trademark of Novell, Inc.

Global Network Operations Center and GNOC are service marks of Novell, Inc.

Graphics Environment Manager and GEM are registered trademarks of Novell, Inc. in the United States and other countries.

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

GroupWise XTD is a trademark of Novell, Inc.

Hardware Specific Module is a trademark of Novell, Inc.

Hot Fix is a trademark of Novell, Inc.

InForms is a trademark of Novell, Inc.

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

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

IPX/SPX is a trademark of Novell, Inc.

IPXODI is a trademark of Novell, Inc.

IPXWAN is a trademark of Novell, Inc.

LAN WorkGroup is a trademark of Novell, Inc.

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

LAN WorkShop is a trademark of Novell, Inc.

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

LANalyzer Agent is a trademark of Novell, Inc.

Link Support Layer and LSL are trademarks of Novell, Inc.

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

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

Media Support Module and MSM are trademarks of Novell, Inc.

Mirrored Server Link and MSL are trademarks of Novell, Inc.

Mobile IPX is a trademark of Novell, Inc.

Multiple Link Interface and MLI are trademarks of Novell, Inc.

Multiple Link Interface Driver and MLID are trademarks of Novell, Inc.

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

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

Natural Language Interface for Help is a trademark of Novell, Inc.

NDS Manager is a trademark of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE/2T is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2000T is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NE32HUB is a trademark of Novell, Inc.

NEST Autoroute is a trademark of Novell, Inc.

NetExplorer is a trademark of Novell, Inc.

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

NetSync is a trademark of Novell, Inc.

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

NetWare 3270 CUT Workstation is a trademark of Novell, Inc.

NetWare 3270 LAN Workstation is a trademark of Novell, Inc.

NetWare 386 is a trademark of Novell, Inc.

NetWare Access Server is a trademark of Novell, Inc.

NetWare Access Services is a trademark of Novell, Inc.

NetWare Application Manager is a trademark of Novell, Inc.

NetWare Application Notes is a trademark of Novell, Inc.

NetWare Asynchronous Communication Services and NACS are trademarks of Novell, Inc.

NetWare Asynchronous Services Interface and NASI are trademarks of Novell, Inc.

NetWare Aware is a trademark of Novell, Inc.

NetWare Basic MHS is a trademark of Novell, Inc.

NetWare BranchLink Router is a trademark of Novell, Inc.

NetWare Care is a trademark of Novell, Inc.

NetWare Communication Services Manager is a trademark of Novell, Inc.

NetWare Connect is a registered trademark of Novell, Inc. in the United States.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Distributed Management Services is a trademark of Novell, Inc.

NetWare Document Management Services is a trademark of Novell, Inc.

NetWare DOS Requester and NDR are trademarks of Novell, Inc.

NetWare Enterprise Router is a trademark of Novell, Inc.

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

NetWare Global Messaging and NGM are trademarks of Novell, Inc.

NetWare Global MHS is a trademark of Novell, Inc.

NetWare HostPrint is a registered trademark of Novell, Inc. in the United States.

NetWare IPX Router is a trademark of Novell, Inc.

NetWare LANalyzer Agent is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Link/ATM is a trademark of Novell, Inc.

NetWare Link/Frame Relay is a trademark of Novell, Inc.

NetWare Link/PPP is a trademark of Novell, Inc.
NetWare Link/X.25 is a trademark of Novell, Inc.
NetWare Loadable Module and NLM are trademarks of Novell, Inc.
NetWare LU6.2 is trademark of Novell, Inc.
NetWare Management Agent is a trademark of Novell, Inc.
NetWare Management System and NMS are trademarks of Novell, Inc.
NetWare Message Handling Service and NetWare MHS are trademarks of Novell, Inc.
NetWare MHS Mailslots is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare Mirrored Server Link and NMSL are trademarks of Novell, Inc.
NetWare Mobile is a trademark of Novell, Inc.
NetWare Mobile IPX is a trademark of Novell, Inc.
NetWare MultiProtocol Router and NetWare MPR are trademarks of Novell, Inc.
NetWare MultiProtocol Router Plus is a trademark of Novell, Inc.
NetWare Name Service is trademark of Novell, Inc.
NetWare Navigator is a trademark of Novell, Inc.
NetWare Peripheral Architecture is a trademark of Novell, Inc.
NetWare Print Server is a trademark of Novell, Inc.
NetWare Ready is a trademark of Novell, Inc.
NetWare Requester is a trademark of Novell, Inc.
NetWare Runtime is a trademark of Novell, Inc.
NetWare RX-Net is a trademark of Novell, Inc.
NetWare SFT is a trademark of Novell, Inc.
NetWare SFT III is a trademark of Novell, Inc.
NetWare SNA Gateway is a trademark of Novell, Inc.
NetWare SNA Links is a trademark of Novell, Inc.
NetWare SQL is a trademark of Novell, Inc.
NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.
NetWare Telephony Services is a trademark of Novell, Inc.
NetWare Tools is a trademark of Novell, Inc.
NetWare UAM is a trademark of Novell, Inc.
NetWare WAN Links is a trademark of Novell, Inc.
NetWare/IP is a trademark of Novell, Inc.

NetWire is a registered service mark of Novell, Inc. in the United States and other countries.

Network Navigator is a registered trademark of Novell, Inc. in the United States.

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

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

Network Support Encyclopedia and NSE are trademarks of Novell, Inc.

Network Support Encyclopedia Professional Volume and NSEPro are trademarks of Novell, Inc.

NetWorld is a registered service mark of Novell, Inc. in the United States and other countries.

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

Novell Alliance Partners Program is a collective mark of Novell, Inc.

Novell Application Launcher is a trademark of Novell, Inc.

Novell Authorized CNE is a trademark and service mark of Novell, Inc.

Novell Authorized Education Center and NAEC are service marks of Novell, Inc.

Novell Authorized Partner is a service mark of Novell, Inc.

Novell Authorized Reseller is a service mark of Novell, Inc.

Novell Authorized Service Center and NASC are service marks of Novell, Inc.

Novell BorderManager is a trademark of Novell, Inc.

Novell BorderManager FastCache is a trademark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

Novell Corporate Symbol is a trademark of Novell, Inc.

Novell Customer Connections is a registered trademark of Novell, Inc. in the United States.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

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

Novell ElectroText is a trademark of Novell, Inc.

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

Novell Gold Authorized Reseller is a service mark of Novell, Inc.

Novell Gold Partner is a service mark of Novell, Inc.

Novell Labs is a trademark of Novell, Inc.

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

Novell NE/2 is a trademark of Novell, Inc.

Novell NE/2-32 is a trademark of Novell, Inc.

Novell NE3200 is a trademark of Novell, Inc.

Novell Network Registry is a service mark of Novell, Inc.

Novell Platinum Partner is a service mark of Novell, Inc.

Novell Press is a trademark of Novell, Inc.

Novell Press Logo (teeth logo) is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Replication Services is a trademark of Novell, Inc.

Novell Research Reports is a trademark of Novell, Inc.

Novell RX-Net/2 is a trademark of Novell, Inc.

Novell Service Partner is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

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

Novell Technical Services and NTS are service marks of Novell, Inc.

Novell Technology Institute and NTI are registered service marks of Novell, Inc. in the United States and other countries.

Novell Virtual Terminal and NVT are trademarks of Novell, Inc.

Novell Web Server is a trademark of Novell, Inc.

Novell World Wide is a trademark of Novell, Inc.

NSE Online is a service mark of Novell, Inc.

NTR2000 is a trademark of Novell, Inc.

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

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

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

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

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

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

Open Socket is a registered trademark of Novell, Inc. in the United States.

Packet Burst is a trademark of Novell, Inc.

PartnerNet is a registered service mark of Novell, Inc. in the United States and other countries.

PC Navigator is a trademark of Novell, Inc.

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

Perform3 is a trademark of Novell, Inc.

Personal NetWare is a trademark of Novell, Inc.

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

Portable NetWare is a trademark of Novell, Inc.

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

Print Managing Agent is a trademark of Novell, Inc.

Printer Agent is a trademark of Novell, Inc.

QuickFinder is a trademark of Novell, Inc.

Red Box is a trademark of Novell, Inc.

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

Remote Console is a trademark of Novell, Inc.

Remote MHS is a trademark of Novell, Inc.

RX-Net is a trademark of Novell, Inc.

RX-Net/2 is a trademark of Novell, Inc.

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

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

Sequenced Packet Exchange and SPX are trademarks of Novell, Inc.

Service Response System is a trademark of Novell, Inc.

Serving FTP is a trademark of Novell, Inc.

SFT is a trademark of Novell, Inc.

SFT III is a trademark of Novell, Inc.

SoftSolutions is a registered trademark of SoftSolutions Technology Corporation, a wholly owned subsidiary of Novell, Inc.

Software Transformation, Inc. is a registered trademark of Software Transformation, Inc., a wholly owned subsidiary of Novell, Inc.

SPX/IPX is a trademark of Novell, Inc.

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

Storage Management Services and SMS are trademarks of Novell, Inc.

Technical Support Alliance and TSA are collective marks of Novell, Inc.

The Fastest Way to Find the Right Word is a registered trademark of Novell, Inc. in the United States and other countries.

The Novell Network Symbol is a trademark of Novell, Inc.

Topology Specific Module and TSM are trademarks of Novell, Inc.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

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

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

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

Yes, It Runs with NetWare (logo) is a trademark of Novell, Inc.

Yes, NetWare Tested and Approved (logo) is a trademark of Novell, Inc.

ZENworks is a trademark of Novell, Inc.

