WAN Overview

Novell.

Legal Notices

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

Novell Trademarks

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

Third-Party Trademarks

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

Contents

About This Guide

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

1 **Planning**

The Novell® Internet Access Server 4.1 routing software enables a NetWare® server to route traffic over wide area networks (WANs) by providing the following three WAN services: the NetWare Link/ATM™ service, the NetWare Link/Frame Relay™ service, and the NetWare Link/X.25™ service.

This section describes how to select which WAN service to use.

All three WAN services are installed when you install the routing software. For information about configuring these services, refer to "Setting Up" in the documentation for the appropriate WAN protocol.

Selecting which Type of WAN to Use

Wide area networks differ from local area networks in that they typically do not have the same distance limitations; however, WANs are limited in the data rates that they can accommodate.

Two basic types of links are used in WANs:

- ◆ Point-to-Point Connections
- ◆ Packet-Switched Networks

Point-to-Point Connections

Point-to-point WAN connections can be permanent or on-demand connections. Novell provides an implementation of the Point-to-Point Protocol (PPP) in the basic Novell Internet Access Server 4.1 package. Refer to Understanding in the *NetWare Link/PPP* documentation for more information.

Packet-Switched Networks

Two common packet-switched networks are currently available: frame relay and X.25.

Frame relay is a relatively new service aimed at reducing network delays, utilizing the available communications bandwidth more efficiently, and lowering equipment costs. The frame relay service might eventually replace the X.25 service, but it does not currently offer the same embedded error protection capabilities that X.25 provides.

X.25 is the predominant packet-switching protocol in use in the United States and most of Europe. X.25 was developed by the ITU-T (International Telecommunications Union, Telecommunications Standardization sector), previously CCITT, in the late 1970s and was later adopted by the International Standards Organization (ISO).

Planning for WAN Connections

Planning is the key to easy installation of WAN connections. Basic planning for WAN connections involves the following:

- Deciding what type of links you want
- Learning what requirements the service provider imposes on the service

Time spent in planning your network, coordinating with service providers, and gathering the information you will need saves time during the installation and configuration procedures.

This topic contains the following sections:

- Contacting Service Providers
- Using NIASCFG

Contacting Service Providers

If you have difficulty in finding a service provider for packet-switched networks, contact your local telephone company for assistance in finding the type of service you want.

Using NIASCFG

The Novell Internet Access Server Configuration utility (NIASCFG) is a menu-driven utility used to configure the Novell Internet Access Server 4.1

WAN protocols. It is installed during the installation of Novell Internet Access Server 4.1.

NIASCFG uses a series of menus to configure related sets of parameters. This configuration interface allows you to define LAN and WAN adapter boards, configure LAN and WAN protocols, and bind the protocols to be used for a specific link or connection to the appropriate adapters. You can enter names for new interfaces, specify parameters, and override defaults without using a command line.

Items in NIASCFG correspond to the steps used to configure Novell Internet Access Server 4.1 protocols and routing software. These items should be configured in the order presented in the procedures provided in this guide.

2 **Optimizing**

Although many optimization techniques can be used on a LAN or WAN, optimization is less an issue for a LAN because bandwidth is inexpensive. On a WAN, performance optimization is critical because WAN media use slower transmission speeds than LAN media.

Because the potential for performance improvement is greater for a WAN than for a LAN, this chapter focuses on techniques that you can use to optimize the performance of your WAN links.

Overview of WAN Optimization

Although LAN performance is measured in packets per second, WAN performance is more accurately measured by the amount of throughput on a link. To optimize performance on a WAN, you must optimize the WAN circuit.

As shown in Figure 1 , WAN circuits are made up of two components:

- ◆ Payload capacity
- ◆ Line overhead

Figure 1   WAN Pipe
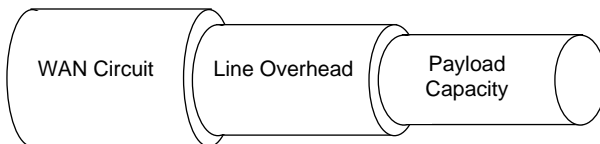
This section discusses the following topics:

- Payload Capacity
- Line Overhead
- Network Optimization Tools

Payload Capacity

Payload capacity is the speed at which data moves through a circuit. If your network is very large (over 4000 network segments and services) and uses only the Internetwork Packet Exchange™ (IPX™) protocol and T1 (1.544-Mbps) connections, maximizing payload capacity can increase network performance significantly.

Because very large networks have minimal line overhead—for example, less than 5 percent of network capacity is associated with in-band maintenance traffic—decreasing line overhead does not significantly increase bandwidth. However, you can overcome transport protocol inefficiencies and increase capacity of a circuit by using data compression.

NOTE: If the link is not already fully using the line speed, adding data compression produces minimal performance improvement.

Line Overhead

Line overhead contains the media's framing, routing protocol, and Network-layer protocol overhead. Line overhead is similar to an envelope in that it restricts the capacity of the system. To increase a circuit's capacity, you must minimize line overhead.

Reducing line overhead in a multiprotocol environment is critical because it increases circuit capacity for all protocols, not only the protocol being optimized. For example, reducing Service Advertising Protocol (SAP) traffic increases the available bandwidth for IPX, IP, and AppleTalk clients.

If your network is large (1000 network segments and services) and consists of small sites and branch offices connected by 64-Kbps or slower circuits, your line overhead can be at 25 percent or more of circuit capacity. In this case, reducing line overhead is critical. Without optimization of line overhead, circuits are saturated and payload optimization produces only minimal improvement.

Network Optimization Tools

By optimizing both the line overhead and the payload capacity, you can dramatically improve network throughput and transmit more user data over

WAN connections. Novell® Internet Access Server 4.1 routing software provides several optimization tools.

For payload optimization, consider using the following:

- PPP data compression
- Packet Burst™ protocol and Large Internet Packet (LIP) protocol

For line optimization, consider using the following:

- Header compression
- RIP and SAP filtering
- Link state routing (NetWare® Link Services Protocol™ [NLSP™] software and OSPF protocol)
- AURP tunneling

Optimizing Permanent WAN Connections

Novell Internet Access Server 4.1 routing software provides not only the optimization tools available for all WAN connection types but also the following tools that can help you further optimize permanent connections:

- Route and Service Information Filters
- Link State Routing
- AppleTalk Update-Based Routing Protocol (AURP)

Route and Service Information Filters

Route and service information filters enable you to more effectively manage the LAN and WAN bandwidth used for routing and service overhead. Filters enable you to connect NetWare services over the WAN and support large NetWare networks. In addition, filters enhance network security by blocking unauthorized access to network segments or individual servers.

IMPORTANT: For IPX networks, the NetWare operating system requires an IPX network number in the routing table before it stores a corresponding service on that network in the bindery. You must carefully plan your implementation of RIP filters to ensure that you do not accidentally filter out services that are needed on your network.

On IPX networks, RIP filters are most useful in providing network security. Because SAP traffic is significantly higher than RIP traffic, filtering SAP

traffic can produce much greater bandwidth improvement than filtering RIP traffic.

On IP networks, filters can reduce traffic. However, because of the default route, route filtering might be ineffective for providing security.

Similarly, on AppleTalk networks, router information filters can provide network security and traffic reduction, whereas device-hiding information filters are most useful for reducing traffic.

The Novell Internet Access Server 4.1 routing software offers inbound route and service filtering on any interface and supports outbound route and service filtering across any interface. These filters can be applied on a global or per-interface basis.

NOTE: By default, the time synchronization component of Novell Directory Services™ (NDS™) software uses SAP to advertise the presence of time servers. Custom configuration turns off this SAP process and replaces it with a time configuration file on each server. Along with turning off the time-related SAP, this also avoids any disruption of time synchronization due to the incorrect configuration of new servers.

For further information about optimizing time synchronization, refer to Time Synchronization in NetWare 4.*x* in the November 1993 *NetWare Application Notes.* For more information about using IPX filters, refer to Effectively Managing RIP and SAP Traffic with Filtering in the September 1994 *NetWare Application Notes.*

Outbound filters are typically used for traffic management. Because route and service information is filtered in the updates produced by the router, different views of the network can be advertised from different interfaces. This capability enables you to give each remote site access only to the resources necessary for communications to that site.

For information about configuring filters, refer to Setting Up in the *Filters* documentation.

Link State Routing

Routing protocols typically use one of two types of routing:

- Distance vector routing
- Link state routing

A traditional distance vector router maintains only enough information to tell it how to reach the next router (hop) on the network. Distance vector routers periodically forward this information to each other, even if it has not changed since the last broadcast. Such periodic updates create unnecessary traffic on the network and consume router CPU time.

A link state router builds and maintains a logical map of the entire internetwork. Instead of sending periodic broadcasts of routing tables, link state routers multicast their link information only when a change occurs in a route or service somewhere in the internetwork.

Link state routing offers several advantages over traditional distance vector routing, the most important advantage being network optimization from reduced network traffic.

Novell Internet Access Server routing software provides link state routing for IPX (NLSP) and TCP/IP (OSPF).

NLSP

NLSP is an IPX routing protocol that reduces service and routing overhead on WANs. (For an in-depth description of NLSP, refer to NLSP Migration.) NLSP provides several advantages over RIP and SAP:

- NLSP reduces SAP overhead on wide-area links.

  NLSP uses variable-length service advertisements (eliminating the need to pad overhead to 48 bytes) and allows more than seven services per advertisement in a single packet.

- NLSP sends updates only when a change occurs somewhere in the internetwork.

  If no changes occur, NLSP sends an update every two hours. (In contrast, RIP and SAP update network routes and services every minute.)

- The IPX RIP hop count is limited to 16, but an NLSP metric can be as large as 127.

  With a larger metric, you can build a larger internetwork.

NLSP routers and servers maintain a complete map of the network built from information in the link state database. Unlike RIP's map, which stores information only about the next hop to the destination, NLSP's map includes the complete end-to-end path for a packet. Because each packet has an origination and sequence number, it can quickly notify the entire network of a change in network topology and service offerings. This capability enables NLSP networks to converge much more quickly than RIP networks.

For information about configuring NLSP, refer to Configuring NLSP in the *IPX* documentation and NLSP Migration.

OSPF

Novell Internet Access Server 4.1 routing software provides OSPF as an alternative TCP/IP routing protocol to RIP. OSPF provides several advantages over RIP:

- The IP RIP hop count is limited to 16, but an OSPF metric can be as large as 65,535, enabling you to build a larger internetwork.

- OSPF allows you to assign a wide range of costs for different types of networks, based on characteristics such as bandwidth.

- OSPF converges on the common routing information faster than RIP does.

   This is partly because OSPF does not have the count-to-infinity problem that RIP does and partly because OSPF link state information is flooded instantaneously rather than processed on each hop, as is done with RIP. Faster convergence prevents loss of connectivity and temporary routing loops.

- OSPF generates less traffic.

   Unlike RIP, which requires periodic updates, OSPF routers update their link state information only when the link state changes. Consequently, more bandwidth is available to the data traffic.

For information about configuring your TCP/IP router to use OSPF, see to Configuring OSPF in the *TCP/IP* documentation.

AppleTalk Update-Based Routing Protocol (AURP)

Novell Internet Access Server 4.1 routing software provides AURP (tunneling AppleTalk packets over IP) as an alternative to Routing Table Maintenance Protocol (RTMP), the routing protocol usually used by AppleTalk. AURP reduces bandwidth utilization by sending updates to peer routers only when network routing information changes, instead of sending periodic broadcasts of the routing table.

On a stable network, AppleTalk routers using RTMP broadcast the same information to each other continuously. Because most networks are stable after initial setup, these frequent broadcasts unnecessarily consume bandwidth that could be used to transport more user data. This consumption is particularly noticeable on slow WAN links. When AURP is used instead of RTMP, AppleTalk routers exchange routing information only when a change occurs in the internetwork.

For information about configuring AURP, refer to Setting Up in the *IP Tunnels for IPX and AppleTalk* documentation.

IMPORTANT: AURP routing is available only over an IP tunnel. If you must use RTMP, you can optimize an AppleTalk WAN connection by increasing the Routing Update Timer. Load NIASCFG and follow this path:

Select Configure NIAS > Protocols and Routing > Bindings

Optimizing On-Demand WAN Connections

In addition to using the optimization tools available for all WAN connection types, you can further optimize on-demand connections by minimizing how frequently the link is demanded by nonuser data.

Many items can demand the on-demand call. Because the primary benefit of an on-demand connection is that the connection is terminated when there is no more data to send to a remote LAN—thereby reducing line costs—it is in your best interest to keep the on-demand connection idle as often as possible. In some network topologies, routers must be configured very carefully to reduce the constant demand for connection, because such demand eliminates the cost benefit of on-demand connectivity.

If an on-demand connection is up too often, you can use PPPTRACE or X25TRACE in conjunction with LANalyzer$^®$ for Windows* software to determine what type of traffic is causing the problem.

An on-demand connection can be kept up by two kinds of potentially undesirable traffic: maintenance traffic and application traffic.

This topic contains the following sections:

- Maintenance Traffic
- Application Traffic
- Time Synchronization and NDS Synchronization for On-Demand Links
- Installing and Configuring NDS Synchronization NLM Files

Maintenance Traffic

An on-demand connection can be kept open constantly by several types of maintenance traffic. Common examples of this kind of traffic are Directory Services Synchronization, Time Synchronization, SPX keep-alive packets, and NCP watchdog packets.

NetWare 4 servers attempt to keep their databases synchronized across the network. The servers attempt to synchronize both the NDS database and the servers' times. This synchronization activity results in packets being exchanged frequently between the various NetWare 4 servers. Although this behavior is desirable on a LAN, it is not advisable when on-demand WAN links are being used. The result is that an on-demand connection will be in use all the time because of this background synchronization traffic.

Updates exist to correct the problems that these synchronizations can cause to on-demand connections.

If you are running applications that use SPX, such as NetWare for SAA*, SPX keep-alive packets can keep your on-demand connections up. If the link is open but idle, SPX sends keep-alive packets periodically.

If you are running applications that use OSPF or ICMP, their redirect packets can also keep your on-demand connections up.

WARNING: Be careful not to bind OSPF over on-demand links. OSPF redirect packets will keep your on-demand connection up, causing significant line costs.

Application Traffic

An on-demand connection can be kept open constantly by several types of application traffic. These include NetBIOS traffic, NetExplorer™ discovery packets, and NetWare Management Agent™ traps.

Applications using NetBIOS send broadcasts that bring up on-demand connections. To eliminate NetBIOS traffic on IPX links, you can also configure NetBIOS filters. For more information, refer to Setting Up in the *IPX* documentation.

IMPORTANT: NetBIOS packets are not forwarded over IPX on-demand connections.

NetExplorer software in ManageWise includes a feature that discovers IPX and IP devices on the network by sending periodic discovery packets. The best way to minimize such traffic is to configure *scoping* —a mechanism (available in ManageWise) that limits how much of the network is visible. You can configure the scoping to keep NetExplorer from sending discovery packets across the on-demand connection.

Traps generated by NetWare Management Agent also activate an on-demand connection if the traps must cross the connection to reach the ManageWise console. By configuring NWTRAP.CFG, the NWTRAP.NLM configuration file provided with NetWare Management Agent software, you can control the frequency and severity of traps reported to the console or prevent the agent

from generating specific traps altogether. If you plan to use ManageWise to manage servers or routers over on-demand connections, refer to the *Setup Guide for ManageWise 2.1 (or 2.0)* for information about configuring NWTRAP.CFG.

The Novell Internet Access Server 4.1 routing software also provides packet filtering that can eliminate the traffic sent by a particular application, network, or node on a network. Packet filtering is available for IPX and IP routers. For information about configuring packet filtering, refer to Setting Up in the *Filters* documentation.

Time Synchronization and NDS Synchronization for On-Demand Links

In a NetWare 4.11 or later environment, NDS is distributed across the network. When users or objects are added to the directory, they are added to the local copy of the database and then propagated throughout the network to other copies (replicas) of the database. If the same object is modified in two different replicas, the order of the modifications must be preserved to correctly propagate the changes. One way to ensure the correct ordering of directory events is to time stamp them. However, without a common time source, each NDS server can have a different reference time. Time synchronization solves this problem by synchronizing the time among NDS servers in the network.

In NetWare 4.11 and later implementations of TIMESYNC, the frequency of Time Synchronization packets is determined by the value of the Timesync Polling Interval parameter. The Timesync implementation in NetWare 4 versions prior to NetWare 4.1 (NetWare 4.0, NetWare 4.01, and NetWare 4.02) contained an error that caused Time Synchronization packets to be sent more frequently than specified by the Timesync Polling Interval parameter.

In NetWare 4.11 and later versions, the NDS synchronization logic checks regularly with each server in its replica list to determine whether any changes have occurred. In addition, NDS generates periodic update traffic, which propagates changes in the directory to each replica.

Frequent maintenance exchanges, such as Time Synchronization polling and NDS updates, can generate enough network traffic to keep Novell Internet Access Server routing software on-demand WAN connections active constantly. This can result in excessive costs for switched circuits supplied by outside service providers such as the local telephone carrier.

To resolve this problem, Time Synchronization and NDS NLM updates have been provided that allow improved user control over, and reduction of,

maintenance traffic exchanges. This section provides information about installing and configuring these updates to minimize maintenance traffic over on-demand WAN connections.

Understanding Time Servers

There are four types of time servers: primary, secondary, reference, and single reference. Because primary, reference, and single reference time servers all provide time to other servers, they are frequently called by the general term time source servers.

Primary Time Servers—Synchronize network time with at least one other primary or reference time server and provide time to secondary time servers and clients. A primary time server gets time from the reference time server, polls other primary time servers on the network, and determines the correct network time.

Secondary Time Servers—Receive time from the time source server (primary or reference timeserver) and provide time to clients. A secondary time server gets time from one time source server and remains synchronized with that time source at all times. You can have multiple secondary time servers on your network.

Reference Time Servers—Provide time to which all other time servers and clients synchronize. The reference time server gets time from its hardware clock and provides time to primary and secondary time servers. It is recommended that you have only one reference time server per network.

Single Reference Time Servers—Provide time to secondary time servers and clients. A single reference time server gets time from its hardware clock and provides time to secondary time servers (if any exist on the network). Single reference time servers are primarily intended to be used on networks that have only one server and cannot coexist on the same network with primary or reference timeservers.

Reducing Time Synchronization Packet Traffic

To reduce the frequency with which time synchronization packets are sent across an on-demand link, configure the network so that a minimum number of servers need to synchronize time across the on-demand link.

Example Network Configuration

You can reduce the amount of time synchronization traffic sent across an on-demand link by configuring the time servers in a manner similar to that shown in Figure 2.

Figure 2   Time Server Configuration for On-Demand Link
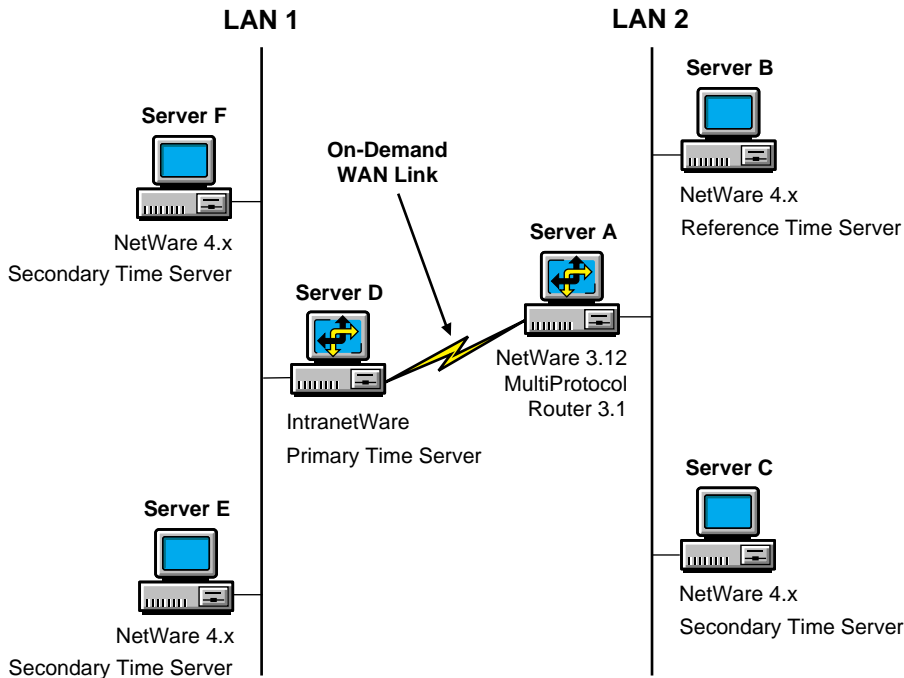
In the network diagrammed in, only Servers B and D exchange time synchronization packets over the on-demand link. Time synchronization occurs as follows:

- Server C, a secondary time server, gets the time from the local Server B (a reference time server).

- Servers E and F, secondary time servers, get the time from local Server D (a primary time server).

- Servers D and B exchange time synchronization packets over the on-demand link. However, the frequency of the packets can be controlled by setting the time synchronization polling interval.

◆ Primary, reference, and secondary time servers have the following line added to their AUTOEXEC.NCF files to set the type of time server:

SET DEFAULT TIME SERVER TYPE = <PRIMARY, SECONDARY, OR REFERENCE>

NOTE: Server A is a NetWare 3.12 server. It has NetWare MultiProtocol Router 3.1 loaded and has been configured with an on-demand link.

The time server type for each server in a Directory tree is assigned by the system administrator at the time you create a Directory tree using the Directory option in INSTALL. Configure the WAN link between servers A and D as permanent and connected before setting up the Directory tree. The WAN link can be reconfigured as an on-demand link after the directory tree is created successfully and the time on all the servers in the tree is synchronized.

For more information about time synchronization, refer to Time Synchronization in Getting Started, Managing Network Time Synchronization in Supervising the Network, and Time Synchronization in NetWare 4 Concepts.

Further Reducing Traffic Using the New TIMESYNC.NLM File

On a NetWare 4.1x server, complete the following steps to update the Timesync Polling Interval:

1 Reset the value of the Timesync Polling Interval using the SERVMAN utility.

   1a Load SERVMAN.

   1b Select Server Parameters, then select Time.

   1c Change the Timesync Polling Interval to a value (in seconds) based on how frequently you want time synchronization information to traverse the on-demand link.

     For example, 86,400 = 1 time every 24 hours.

   1d Press Esc twice to exit SERVMAN.

     The Update Options menu appears.

   1e Select Update TIMESYNC.CFG Now.

     This causes the changes to take effect now and to be in effect when the server is restarted.

   1f Press Esc twice to exit SERVMAN.

2 At the NetWare console prompt, enter

`SET TIMESYNC RESTART FLAG=ON`

This forces TIMESYNC to begin polling for synchronization immediately, and the value of the TIMESYNC POLLING INTERVAL is updated.

IMPORTANT: Do not use the console SET command to change the TIMESYNC POLLING INTERVAL parameter. The console SET command does not write the change to the TIMESYNC.CFG file, and the parameter's old value will be read when TIMESYNC restarts.

Reducing NDS Synchronization Packet Traffic

Two NLM files are used to reduce the number of NDS synchronization packets. DSFILTER.NLM is a configuration utility used to set up the time windows controlling when NDS traffic is allowed to traverse the link. This utility requires that you enter the internal network address of each remote NetWare 4 server that exists in the replica ring. Make sure that each server lists the servers that are on the opposite side of the on-demand WAN link. The PINGFILT.NLM utility uses these addresses to determine what NDS traffic to filter. PINGFILT.NLM should run whenever NDS is running over an on-demand WAN connection. In Figure 3 , PINGFILT.NLM should be run on Servers B, C, D, E, and F.

Figure 3 shows two LANs connected by way of Routers A and D.

Figure 3   NDS Tree Configuration
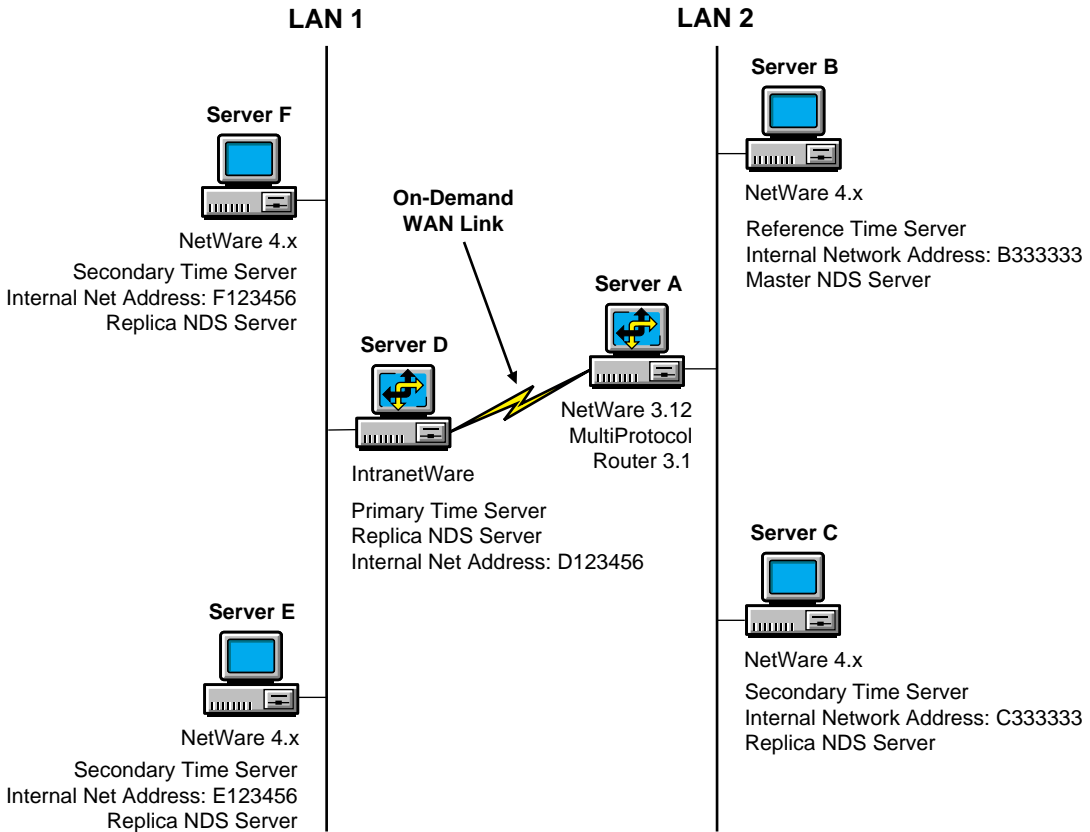
The network is configured as follows:

- ◆ Servers B, C, D, E, and F are in the same Directory tree. Server B contains NDS master replicas, whereas other servers contain read/write replicas.

- ◆ For each server in the Directory tree (B, C, D, E, and F), DSFILTER.NLM was used to configure the time and day of the week when NDS traffic should be allowed to traverse the link.

- ◆ The internal network numbers of Servers D (D123456), F (F123456), and E (E123456) are included in the list of filter addresses of Servers B and C.

- ◆ The internal network numbers of Servers B (B333333) and C (C333333) are included in the list of filter addresses of Servers D, E, and F.

NOTE: In Figure 3 , Server A is a NetWare 3.12 server and is not running NDS.

Installing and Configuring NDS Synchronization NLM Files

Every NetWare 4 server running NDS should be updated with the NDS filter NLM files (DSFILTER.NLM and PINGFILT.NLM) and configured to load the active filter module (PINGFILT.NLM).

Additionally, the DSFILTER.DAT configuration file must be present on each NetWare 4 server that attempts NDS synchronization over an on-demand WAN link. The DSFILTER.NLM utility can be used to create the configuration file on each server within the network.

Alternatively, the DSFILTER.NLM utility can be used to create a single configuration file for each side of the on-demand WAN link, and that file can be copied to all other servers residing on the same side of the WAN link. This reduces the configuration effort on each side of the WAN link.

Installing the NDS Filter NLM Files

Copy the following files to the SYS:SYSTEM directory of all servers in the Directory tree:

 ◆ DSFILTER.NLM

 ◆ PINGFILT.NLM

Configuring the NDS Filters

Configure the NDS filters on at least one server on each side of the on-demand WAN link. To configure the filters, complete the following steps:

1 Load the DSFILTER configuration utility from the NetWare command line.

The DSFilter Utility menu is displayed.

2 Select Filter Pass Through Times.

A screen appears displaying a grid of the days of the week and the hours in a day. The times are displayed and entered in UTC—Universal Time Coordinated (Greenwich mean time). For example, if you are in the Pacific Standard time zone, you are 8 hours behind UTC. Therefore, if you do not want to filter NDS packets at 10:00 p.m. on Tuesday local time, enter an X in the 06:00 a.m. Wednesday field.

To determine the difference between UTC and your time zone, enter the TIME command at the server console prompt. The last two lines of the output show the current time in UTC and local time. Subtract the UTC

time from the local time (for example, 1600 - 2400 = -8 hours). If the result is positive, local time is that many hours ahead of UTC. If the result is negative, local time is that many hours behind UTC.

3 Mark with an X the times of the day you want to allow NDS synchronization packets.

4 Press Esc to save the changes.

5 From the DSFilter Utility menu, select List Filter Addresses.

6 Press Insert to add a server to the list.

The prompt `Enter the Network Address` appears.

7 Press Insert to display a list of servers on the network.

Use the arrow keys to select a server, then press Enter to add it to the list. If the server you want is not on the list, enter it at the `Enter the Network Address` prompt.

NOTE: DSFILTER is a configuration tool and need not be loaded by the AUTOEXEC.NCF file.

8 Press Esc to save your changes.

Copying the NDS Filter Configuration File

Instead of manually configuring the NDS filters for each server, you can copy the files from the first server installed on one side of the WAN link to all other servers on the same side of the WAN link.

Copy the DSFILTER.DAT file from the SYSTEM directory of the originally configured server to all the NetWare 4.x servers located on the same side of the WAN link.

The DSFILTER.DAT file is created in the SYSTEM directory by the DSFILTER utility.

Loading the NDS Filter

Load PINGFILT.NLM on all NetWare servers that are in the same Directory tree.

To ensure that all NDS databases are synchronized, load the PINGFILT.NLM with the *-dnnn* parameter. This option allows PINGFILT to delay its operation *nnn* minutes after loading. The number of minutes to delay depends on the size of the NDS tree.

WARNING: Make sure PINGFILT is loaded after DS is loaded and fully initialized.

The load line (**LOAD PINGFILT -dnnn**) can be added to the AUTOEXEC.NCF file to achieve autoloading of the PINGFILT.NLM utility whenever these servers start up.

Optimization Tools Used for each WAN Media

In Table 1 , an X indicates which types of optimization tools are available for various types of WAN media.

Table 1   Optimization Tools for WAN Media

Optimization Tool	PPP Permanent	PPP On-Demand	X.25 Permanent	X.25 On-Demand	Frame Relay Permanent
Packet Burst	X	X	X	X	X
Data compression	X	X			
IPX header compression	X	X	X	X	X
TCP/IP header compression	X	X			
Data-Link-layer header compression	X	X			
NLSP/OSPF	X		X		X
IPX RIP/SAP filtering	X		X		X
IP Route filtering	X	X	X	X	X
AppleTalk route filtering	X		X		X
AppleTalk service filtering	X	X	X	X	X
Packing forwarding filtering	X	X	X	X	X

3 Troubleshooting

This section contains general troubleshooting information for the Novell®
Internet Access Server 4.1 WAN interfaces software.

Troubleshooting Tips

The following list contains suggestions for solving problems with WAN
interface boards. Check the following areas to ensure that they are not the
source of the problem.

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

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

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

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

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

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

The Synchronous/+ and NW2000 boards use a shared memory interface to the PC. Multiple Synchronous/+ boards can share the same memory address and multiple NW2000 boards can share the same memory address; however, different types of boards cannot be assigned the same address. When assigned an address below 1 MB, a Synchronous/+ board uses 64 KB of shared memory and an NW2000 board uses 16 KB of shared memory. When assigned an address above 1 MB, a Synchronous/+ board uses 512 KB of shared memory and an NW2000 board uses 256 KB of shared memory.

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

Troubleshooting WAN Hardware

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

◆ Network Interface Board Self-Diagnostics

◆ Remote Management of Communication Devices

◆ DSU/CSU Issues

◆ Back-to-Back Testing

Network Interface Board Self-Diagnostics

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

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

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

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

Remote Management of Communication Devices

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

DSU/CSU Issues

Observe the following guidelines when using a DSU/CSU.

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

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

Back-to-Back Testing

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

1 Construct the appropriate crossover cable (as shown in Figure 4 , Figure 5 , or Figure 6) and attach it between the routing systems to be tested.

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

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

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

4 Configure any other needed parameters as described in "Setting Up" in the documentation for the appropriate protocol.

5 Restart both machines.

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

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

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

Figure 4 shows pinouts for constructing an RS-422 crossover cable, which can be used for back-to-back testing on any of the RS-422 ports.

Figure 4   RS-422 Crossover Cable

RS-422 37-Pin Connector Female End   **RS-422 37-Pin Connector Female End**
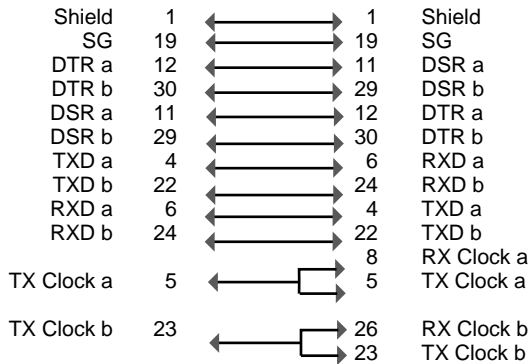
This side
supplies clock.

Shield	1	←→	1	Shield
SG	19	←→	19	SG
DTR a	12	←→	11	DSR a
DTR b	30	←→	29	DSR b
DSR a	11	←→	12	DTR a
DSR b	29	←→	30	DTR b
TXD a	4	←→	6	RXD a
TXD b	22	←→	24	RXD b
RXD a	6	←→	4	TXD a
RXD b	24	←→	22	TXD b
			8	RX Clock a
TX Clock a	5	←─┐	5	TX Clock a
TX Clock b	23	←─┐	26	RX Clock b
			23	TX Clock b

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

Figure 5 shows pinouts for constructing a V.35 crossover cable, which can be used for back-to-back testing on any of the V.35 ports.

Figure 5 **V.35 Crossover Cable**

V.35 34-Pin Connector
Female End

V.35 34-Pin Connector
Female End
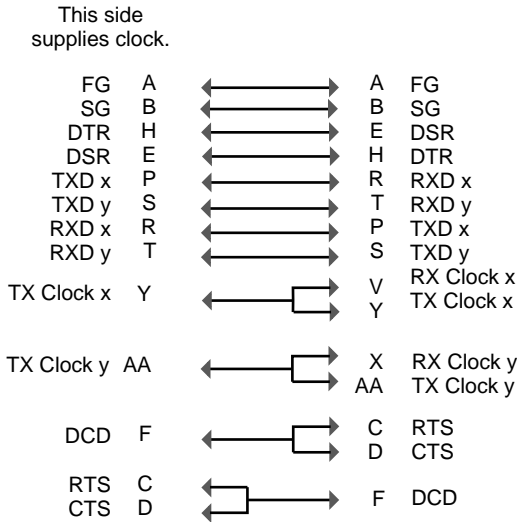
This side
supplies clock.

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

TX Clock x Y ⟵ V RX Clock x
Y TX Clock x

TX Clock y AA ⟵ X RX Clock y
AA TX Clock y

DCD F ⟵ C RTS
D CTS

RTS C
CTS D ⟶ F DCD

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

Figure 6 shows pinouts for constructing an RS-232 crossover cable, which
can be used for back-to-back testing on any of the RS-232 ports.

Figure 6   RS-232 Crossover Cable

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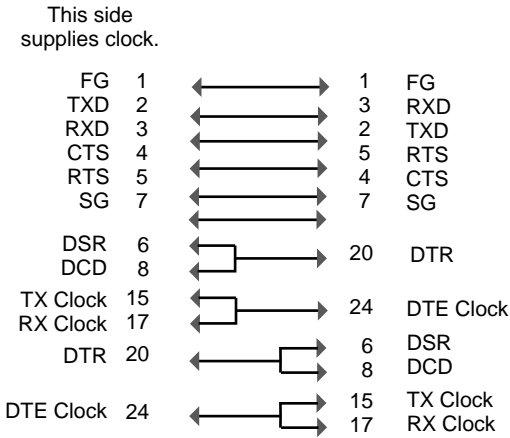
This side
supplies clock.

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

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

WAN Troubleshooting Tools

Table 2 lists the available diagnostic tools for WAN interfaces. For a detailed explanation of each tool, refer to "Managing" in the documentation for the appropriate protocol.

Table 2   Specific Troubleshooting Tools

Protocol or Feature	Troubleshooting Tools
AIO ports	AIO port trace
	Identify Port
	Terminal Mode
	TRACEROUTE

Protocol or Feature	Troubleshooting Tools
Modem script files	WMDMMGR
ISDN	CAPITRCE
PPP	PPPCON
	PPPTRACE
	SPFCON
	Mobile Monitor Icon
ATM	ATMCON
	ATMTRACE
Frame relay	FRCON
	FRTRACE
X.25	X25CON
	X25TRACE

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.