AUGUST 1996

NOVELL® RESEARCH

NetWare/IP 2.2 Implementation and Troubleshooting Guidelines

GARY HEIN
Senior Consultant
Novell Consulting Services

NetWare/IP provides a hassle-free way to integrate IP networks with NetWare. This AppNote summarizes the new features and enhancements made in NetWare/IP version 2.2. It also provides implementation and troubleshooting guidelines to help you design an effective NetWare/IP network and avoid many of the pitfalls that might be encountered along the way.

Introduction
NetWare/IP 2.2 Overview
Domain SAP/RIP Service (DSS)
Domain Name System (DNS)
NetWare/IP-to-IPX Gateway
NetWare/IP Design Guidelines
Migrating from IPX to NetWare/IP
NetWare/IP Implementation and Migration Examples
Troubleshooting NetWare/IP
Conclusion

RELATED APPNOTES
Nov 95 "Guidelines for Implementing NetWare/IP"
Sep 95 "Comparing Novell's IPX-to-IP Connectivity Solutions: IP Tunneling, NetWare/IP, and IP Relay"
Apr 95 "Using NetWare/IP Over Satellite Networks"

ACKNOWLEDGEMENTS
Thanks to Wen Chiu, Ronald Szeto, Alex Salehi, and Paul Reiner of Novell for their help with this AppNote.

TRADEMARKS
NetWare and Novell are registered trademarks and Internetwork Packet Exchange, IPX, NetWare Directory Services, NDS, NetWare Loadable Module, NLM, and NetWare/IP are trademarks of Novell, Inc in the United States and other countries. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Macintosh is a registered trademark of Apple Computers. OS/2 is a registered trademark

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

of International Business Machines Corporation. Microsoft, MS-DOS, and Windows are registered trademarks of Microsoft Corporation. All other product names mentioned are trademarks of their respective companies or distributors.

DISCLAIMER
Novell, Inc. makes no representations or warranties with respect to the contents or use of these Application Notes (AppNotes) or of any of the third-party products discussed in the AppNotes. Novell reserves the right to revise these AppNotes and to make changes in their content at any time, without obligation to notify any person or entity of such revisions or changes. These AppNotes do not constitute an endorsement of the third-party product or products that were tested. Configuration(s) tested or described may or may not be the only available solution. Any test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state, or local requirements. Novell does not warranty products except as stated in applicable Novell product warranties or license agreements.

Copyright © 1996 by Novell, Inc. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Novell, Inc.

Novell, Inc.
1555 N. Technology Way
Orem, Utah 84097 USA

Introduction

NetWare/IP version 2.2 is the latest release of this popular add-on product for the NetWare 4.x operating system. NetWare/IP allows Novell customers to implement NetWare in a mixed IPX-TCP/IP environment, or to migrate to a TCP/IP-only environment. Applications designed to run on NetWare can continue to run, without modification, over TCP/IP instead of IPX.

This AppNote first reviews the new features and enhancements in NetWare/IP 2.2, and then provides some background information on the various components included in the product. It gives some design guidelines and examples for effective implementation of NetWare/IP, followed by troubleshooting tips and tricks.

NetWare/IP 2.2 Overview

NetWare/IP is a collection of components that enable NetWare servers and clients to communicate using TCP/IP instead of IPX as the transport protocol. The components include:

- *Domain Name Service (DNS).* A dynamic database of IP host and IP address information which fully integrate with DNS services running on non-Novell platforms.
- *Dynamic Host Configuration Protocol (DHCP).* Leases IP addresses to clients and provides other necessary information to connect to an IP network.
- *LPR/LPD Gateway*. Permits NetWare servers to print to line printer daemon (LPD) devices, such as embedded IP printers.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

- *NetWare/IP-to-IPX Gateway*. Transparently connects the NetWare/IP and IPX worlds together, provides for a smooth migration from IPX to NetWare/IP.

These components are modular so that customers can selectively choose which components to install based on their network needs.

What's New in NetWare/IP 2.2?

If you are familiar with NetWare/IP 2.1, you'll appreciate the features Novell has added to NetWare/IP 2.2. These include:

- *Automatic NetWare/IP configuration.* During installation, both NetWare/IP and Domain SAP/RIP Service (DSS) servers will attempt to automatically configure NetWare/IP and/or DSS information by querying other NetWare/IP or DHCP servers.
- *Enhanced client initialization.* NetWare/IP 2.2 clients need only to communicate with a NetWare/IP server to initialize, unlike prior versions of NetWare/IP clients that required communication with a DSS server to initialize.
- *Enhanced efficiency of WAN circuits.* Prior to NetWare/IP 2.2, the entire SAP/RIP database was downloaded whenever the NWIP.NLM was loaded. NetWare/IP 2.2 servers now keep a local copy of the SAP/RIP database, downloading only changes from the DSS server when the NWIP.NLM is loaded. This reduces traffic between NetWare/IP and DSS servers.
- *Faster Domain SAP/RIP Service (DSS).* DSS.NLM has been optimized for a 50–100% increase in DSS performance.
- *Domain SAP/RIP Service (DSS) filtering.* Through filtering you can control the types of services advertised between the various secondary DSS servers in your NetWare/IP environment.

NetWare/IP Client Support

NetWare/IP currently supports a wide variety of clients. Here's a summary of client support issues.

DOS and Windows 3.1

- 16-bit client support is available over Novell's TCP/IP stack (provided with NetWare/IP 2.2) or FTP's ONNET client.
- 32-bit client support is available over NetWare Client 32 for DOS/Windows 3.1. This 32-bit client is available from the Novell Web site at `http://support.novell.com/home/client/c32dw/index.htm`.

Windows 95 and Windows NT

NetWare/IP support is available with NetWare Client 32 for Windows 95 or Novell's Windows NT requester, which runs on any TDI-compliant TCP/IP protocol stack, including Microsoft's 32-bit TCP/IP stack provided with Windows 95 and Windows NT.

Macintosh

A Macintosh NetWare/IP client is scheduled for the next release of NetWare 4.x, code named "Green River".

OS/2

Available now in limited beta, this client should be available with "Green River" or shortly thereafter. It runs on both Novell's LAN Workplace for OS/2 and IBM's IP stack included in OS/2 Warp.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

The NetWare/IP client protocol stack presents itself to upper-layer applications as an IPX protocol stack. Thus any client-based application that runs over IPX will be able to run over NetWare/IP. This includes backup and virus scanning software, software distribution packages, host connectivity solutions, even Doom! Although there is a 5 to 8 percent performance loss compared to native IPX, most clients won't notice the difference between IPX and NetWare/IP workstations.

Availability

NetWare/IP 2.2 is available free of charge for NetWare 4.1 customers on Novell's World Wide Web site or ftp site. It can be downloaded from:

```
ftp.novell.com /pub/updates/unixconn/nwip22
```

This area will also include any future updates, enhancements, and patches, so be sure to check back regularly.

NetWare/IP Components

The following sections of this AppNote describe the function and operation of these NetWare/IP components:

- Domain SAP/RIP Service (DSS)
- Domain Name Service (DNS)
- NetWare/IP-to-IPX gateway

Domain SAP/RIP Service (DSS)

In a NetWare/IP environment, the Domain SAP/RIP Service (DSS) provides the same service and route information that exists in the IPX environment. To understand the function of the DSS, it is helpful to review how servers, clients, and routers exchange this information in IPX networks.

Connecting in IPX Networks

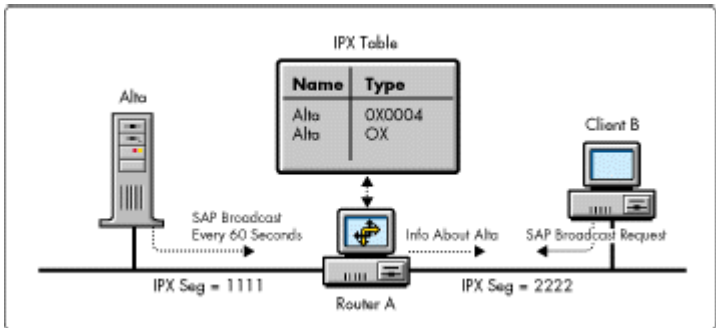
In an IPX network, NetWare servers use the IPX Service Advertising Protocol (SAP) and Routing Information Protocol (RIP) to advertise and locate services and routes, respectively. Every 60 seconds, NetWare servers broadcast SAP packets to advertise their services to the IPX world. NetWare servers also broadcast RIP packets every 60 seconds to tell other IPX routers what routes are available through each NetWare server.

IPX routers, such as NetWare servers and hardware-based routers, listen for all SAP and RIP broadcasts. An IPX router collects this information and organizes it into SAP and RIP tables stored within the router's memory. These tables provide the IPX router a complete view of all services within the network, along with the respective network path to each service.

When an IPX client wants to find a service, such as a NetWare file server or a Novell Directory Services (NDS) server, the client broadcasts an IPX SAP request to the local IPX segment. Since all IPX routers contain a comprehensive list of all services throughout the network, any IPX router on that segment can respond to the client and provide a list of servers with the desired service. This process is illustrated in Figure 1.

Figure 1: In an IPX network, servers, clients, and routers use RIP and SAP to locate services and establish connections.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD



In this example the server, Alta, is on IPX segment 1111. Every 60 seconds, Alta broadcasts SAPs that advertise the services running on Alta, such as NDS, NetWare file services, and print services. The IPX router, Router A, receives Alta's SAPs and stores the SAP information within its SAP table. When the client, B, on segment 2222 wants to connect to the network, it broadcasts a SAP request looking for an NDS server. IPX Router A responds to Client B's request by providing information about the Alta server.

This SAP and RIP broadcast mechanism works well for NetWare in IPX networks because IPX routers store all NetWare service and route information within the router's memory.

Connecting in NetWare/IP Networks

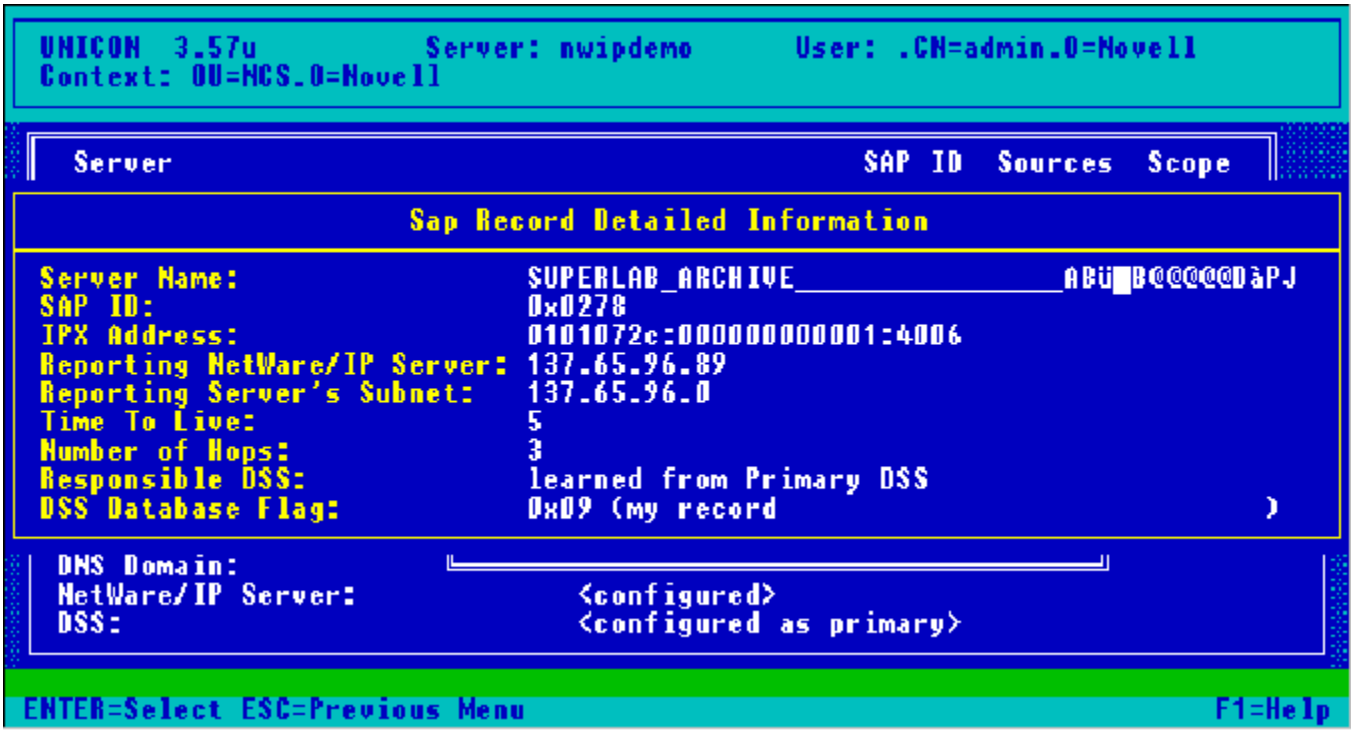
Unlike IPX routers, IP routers do not store any information about NetWare services and routes. IP broadcasts are often not propagated across IP subnets. As a result, it is a bit more challenging for NetWare servers to advertise service and route information in an IP environment. The solution for NetWare/IP was to introduce an alternative name service, known as the *Domain SAP/RIP Service* (DSS), as a repository for storing the same information that SAP and RIP broadcasts provide in an IPX environment.

DSS is a distributed, fault-tolerant database of service and route information, built on the Btrieve engine. In a NetWare/IP environment, the administrator selects a server to provide the DSS service by loading DSS.NLM on that server. NetWare/IP servers are then configured to communicate directly with DSS servers to exchange information that would normally propagate as a SAP or RIP broadcast in an IPX environment. NetWare/IP servers upload all of their service and route information to the DSS, which associates those records with the NetWare/IP servers' IP addresses. NetWare/IP servers also download all of the DSS server's records, thereby enabling the NetWare/IP server to "see" all other services and routes within the NetWare/IP environment.

Figure 2 shows an example of the information held in a typical SAP record in the DSS database, as displayed in the UNICON utility.

Figure 2: An example of a SAP record in the DSS database.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD



Notice the following information in this sample SAP record:

- The service name is "SUPERLAB_ARCHIVE". This identifies an NDS server. The strange characters at the end of the name are present with every NDS Tree service advertisement)they are the hex representation of the server's IPX network, node, and socket.
- The service type is 0x0278, which is for Novell Directory Services. Note that this is identical to the SAP ID or type. A list of all SAPs or service types can be found at `http://www.novell.com/corp/programs/ncs/toolkit/download/ saps.txt`.
- The full IPX address (network:node:socket) of the server's internal IPX "network" is stored in the DSS database. This is very important for IPX processes that only communicate based on an server's internal IPX address.
- The record includes the IP address and subnet of the server that reported this information to the DSS, which in this example are 137.65.96.89 and 137.65.96.0.
- The Number of Hops indicates how many IPX router hops away this service is from the reporting NetWare/IP server. If the Number of Hops is 0, this service is running on a NetWare/IP server. If the Number of Hops is greater than 0, it indicates that the reporting NetWare/IP server is advertising this record on behalf of an IPX-only file server.

  In this example, "SUPERLAB_ARCHIVE" happens to be three IPX router hops away from the NetWare/IP server at 137.65.96.89.

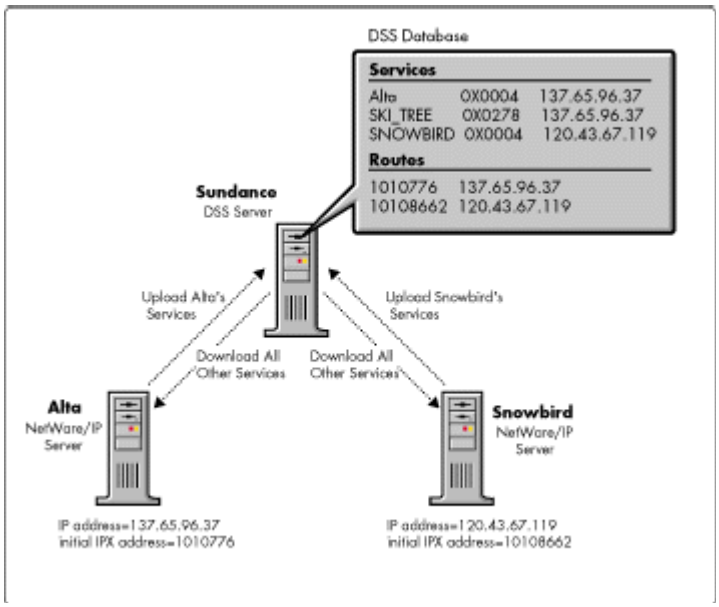
If any remote server or client wants to communicate with this server, packets must be sent to the IP address associated with this DSS entry, which is 137.65.96.89. Thus the DSS database essentially links the IPX resources with IP addresses, allowing any IP client to register or discover NetWare services through the DSS database. It is therefore necessary that the DSS database remain synchronized with changes in the IPX environment.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

DSS Synchronization Basics

The following example illustrates how the DSS database synchronizes information received from multiple NetWare/IP servers. In Figure 3, the NetWare/IP servers Alta and Snowbird are configured to use DSS services on file server Sundance.

Figure 3: With NetWare/IP, the DSS Server synchronizes all service and route information received from NetWare/IP servers.



When server Alta initializes, it contacts Sundance to inform the DSS database about all services available on the Alta server. Records are created within the DSS database for all of these services, such as NDS and NetWare file server. Alta's internal IPX address is stored in the database as well. These DSS database records are associated with Alta's IP address. Upon initialization, Alta also downloads all DSS records for other services and routes within the NetWare/IP environment.

When Snowbird initializes, it too contacts Sundance to inform the DSS database about all of the services it has available, along with its internal IPX address. All of Snowbird's DSS database records are associated to Snowbird's IP address. Snowbird then downloads all DSS records for other services and routes (such as Alta's) available within the NetWare/IP environment.

Once Alta and Snowbird have exchanged this information with the DSS server, they contact Snowbird every five minutes (configurable). If any changes have been made to the DSS database since the last synchronization, the servers exchange only the changed information.

As demonstrated in this example, there are some important rules that NetWare/IP and DSS servers use when exchanging information:

- The first time the NetWare/IP server contacts a DSS, it must download all SAP and RIP records for the entire NetWare/IP domain. NetWare/IP servers hold a copy of the SAP/RIP database in the sys:etc\nwipsap.btr and sys:etc\nwiprip.btr files. During subsequent initializations, the NetWare/IP server downloads only changes to the SAP/RIP database since the last synchronization with a DSS.
- By default, all NetWare/IP servers contact a DSS server every five minutes to exchange SAP and RIP

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

records. (The five-minute time interval is configurable.)

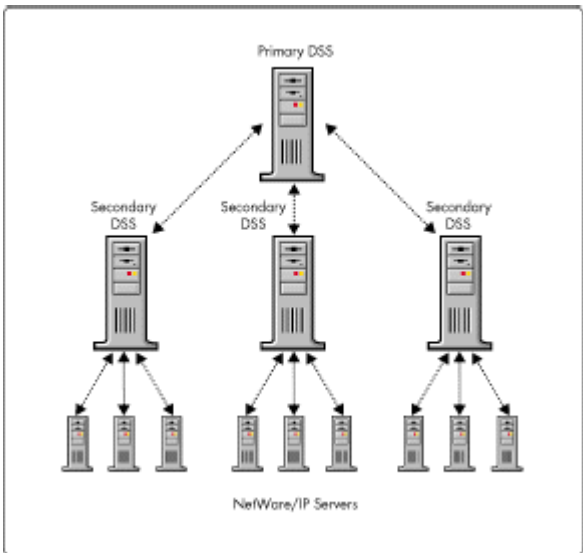
- Only changes made to the DSS database since the last NetWare/IP-DSS synchronization exchange are synchronized.

Building DSS Hierarchy and Fault Tolerance

Because DSS servers are such important components of a NetWare/IP environment, it is important to plan for scalability and fault tolerance. NetWare/IP provides for both of these features by allowing two types of DSS servers: primary and secondary.

Functionally, the primary DSS and secondary DSS are almost identical)in fact, both use the same DSS.NLM. The only difference is that the primary DSS sets NetWare/IP domain parameters, such as DSS-DSS and NWIP-DSS synchronization, DSS SAP filtering, UDP checksums, and a few others. The primary DSS server works with the secondary DSS servers to maintain the consistency of the DSS database. NetWare/IP servers are generally configured to use secondary DSS servers for DSS services, thus reserving the primary DSS to keep the secondary DSS server synchronized (see Figure 4).

Figure 4: NetWare/IP defines a hierarchy in which NetWare/IP servers synchronize with secondary DSS servers, and secondary DSS servers synchronize with the primary DSS server.



As with NetWare/IP-to-DSS server synchronization, the DSS-to-DSS server synchronization also occurs every five minutes (configurable) and only changes to the DSS database are synchronized. Synchronization is always initiated by the lower device. For example, the NetWare/IP server contacts the secondary DSS to exchange information; likewise, the secondary DSS contacts the primary DSS for synchronization.

Domain Name System (DNS)

Domain Name System (DNS) is an optional component of NetWare/IP. If other mechanisms to locate NetWare/IP resources fail, NetWare/IP servers and clients may optionally query DNS during their initialization. The two main uses of DNS within NetWare/IP are:

- To locate DSS servers by querying DNS for name servers of the NetWare/IP domain. Normally

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

NetWare/IP servers and clients use other mechanisms to locate NetWare/IP resources. If these other mechanisms fail, DNS may be consulted to find other DSS servers within the NetWare/IP domain.

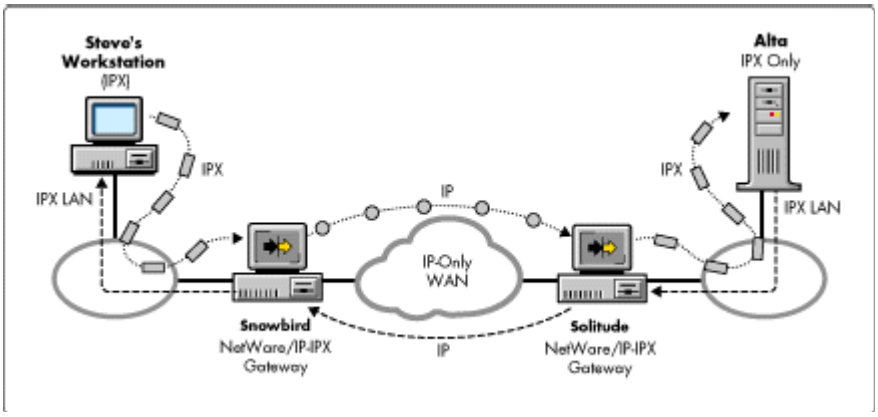
- To resolve DNS names for NetWare/IP resources. For example, it is possible to configure a NetWare/IP server to contact a DSS server by either IP address or by specifying the DNS host name of the DSS server. If the DSS server's host name is used, DNS must be consulted to resolve the DNS host name to an IP address.

If DNS is used, a separate DNS subdomain is created for NetWare/IP. This DNS subdomain does not contain entries for NetWare/IP servers and clients; rather, the NetWare/IP DNS subdomain only contains name server (ns) records for a few selected NetWare servers that provide DSS services.

NetWare/IP-to-IPX Gateway

NetWare/IP includes a "gateway" that converts between IPX and NetWare/IP, allowing network administrators to deploy mixed IPX and NetWare/IP environments. This NetWare/IP-to-IPX gateway transparently connects the IPX and NetWare/IP worlds together. Clients running either IPX or NetWare/IP never need to know whether the remote resource being accessing is located on a NetWare/IP or IPX server. Figure 5 shows an example of how these gateways work.

Figure 5: The NetWare/IP-to-IPX gateway transparently connects NetWare/IP and IPX environments.



In this example, Steve's workstation is using IPX to communicate to IPX server Alta through the NetWare/IP-to-IPX gateways Snowbird and Solitude. Snowbird and Solitude are separated by a WAN link that supports only IP. Steve is able to communicate to Alta by sending IPX packets to Snowbird, where they are converted to NetWare/IP packets and sent across the IP link to Solitude. Solitude converts the packet from IP back to IPX and sends them via IPX to Alta. Steve never knows that his communication to Alta is passing through NetWare/IP-to-IPX gateways.

Effect on Performance

A question is often raised concerning how much performance is affected by using the intermediate NetWare/IP- to-IPX gateways. Technically, NetWare/IP is between 5 and 8 percent slower than native IPX. However, most customers cannot perceive the difference when accessing a resource through NetWare/IP as compared to IPX. In a typical configuration such as the one in Figure 5, the performance bottleneck is the speed of the WAN circuits, not the conversion between IPX and NetWare/IP at the NetWare/IP-to-IPX gateways. In other words, the latency of the NetWare/IP-to-IPX conversion is much smaller than the latency

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

of the WAN circuit. This generally holds true until the WAN speed approaches 8 megabits per second or faster.

Surprisingly, most customers actually notice a net *increase* in performance when implementing NetWare/IP across WAN circuits. This is due to the elimination of IPX SAP and RIP packets from the link, thus freeing up bandwidth for data traffic. Since NetWare/IP uses a five-minute synchronization interval and only changes are transferred, the amount of data sent across the WAN link is significantly reduced.

The following exercise demonstrates the bandwidth savings of NetWare/IP over IPX's SAP and RIP. Consider a customer with 2000 services, such as file servers, directory services, time synchronization, advertising print servers, and so on, in the home office. This customer wants to connect a remote office to the home office via a 56Kbps WAN link, and asks an experienced consultant for assistance. To determine how IPX traffic will impact the WAN, the consultant performs the following calculations:

Each SAP packet is 576 bytes and advertises 7 services every 60 seconds
2000 services / 7 services per SAP packet = 286 SAP packets
*286 SAP packets * 576 bytes/packet = 164,736 bytes per 60-second cycle*

Maximum throughput of the WAN link
56Kbit/sec WAN link = 57,334 bits/sec = 7168 bytes/sec
*7168 bytes/sec * 60 sec/min = 430,080 bytes/minute*

Since SAPs will be sent every minute across the WAN link,
164,736 bytes for SAP / 430,080 bytes available = .383

The bottom line is that in the traditional IPX environment, over a third (38.3%) of the 56Kbps link would be used for SAP updates!

By contrast, in a typical NetWare/IP environment with 2000 or more services, only 20 to 40KB of data is exchanged every five minutes. This equates to *less than 1%* of the 56Kbps WAN bandwidth for NetWare/IP updates.

In general, the quick formula for calculating the SAP load on a WAN circuit can be expressed as follows:

$$\frac{\text{\# of SAPs}}{\text{Speed of WAN in Kbps}} \times 1.07 = \%\text{ of SAP load on WAN circuit}$$

Plugging in the numbers from our above example:

$$\frac{\text{2000 SAPs}}{\text{56Kbps}} \times 1.07 = 38.2\%\text{ of WAN consumed by SAPs}$$

Note: These calculations do not account for RIP information. Generally, RIP doesn't place as great of a load on a WAN link as SAP does, because there are usually fewer RIPs than SAPs, and each 576-byte RIP packet can advertise up to 64 routes. A typical 2000 SAP environment may contain only 500 RIPs, which require about *eight* 576-byte RIP packets. This is considerably less significant when compared to the 286 SAP packets required per minute.

Most customers are looking for some mechanism to reduce the percentage of WAN bandwidth consumed by IPX SAPs. Besides NetWare/IP, other alternatives include:

- Modifying router parameters, such as "SAP On Change"
- Increasing the SAP interval to every 15 minutes
- Using alternative technologies such as NetWare Link Services Protocol (NLSP) or Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

Inside the NetWare/IP-to- IPX Gateway

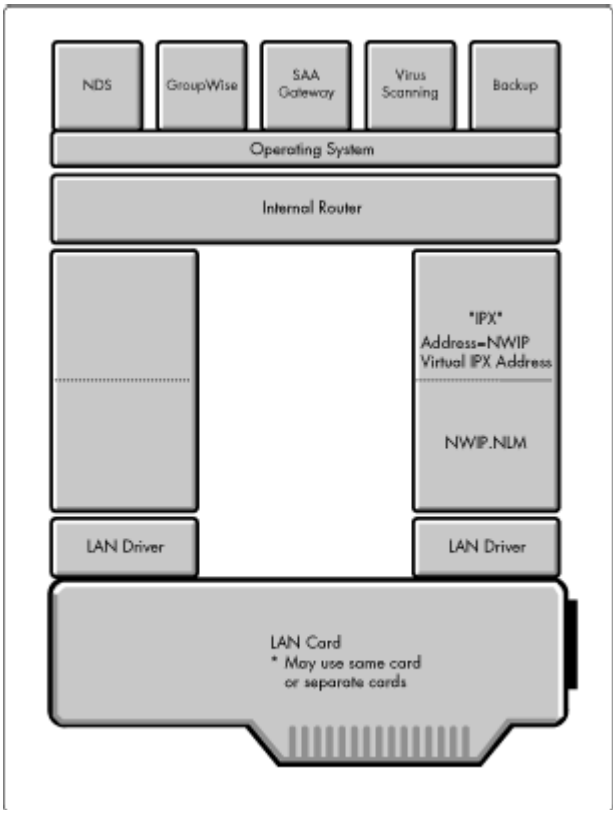
The NetWare/IP-to-IPX gateway is implemented within the NetWare/IP module named NWIP.NLM. Figure 6 shows how NWIP.NLM relates to other components inside the server.

NWIP.NLM presents itself to the server's internal router as an IPX protocol stack. Just like any other IPX protocol stack, it is made available through an IPX binding command such as

```
bind IPX to NE2000 net=1234
```

NetWare/IP uses a *virtual IPX address* for NWIP.NLM. The server "sees" the NetWare/IP segment as an IPX protocol stack with the IPX address of the virtual IPX address (1234 in the above example). This virtual IPX address is assigned once during the configuration of the primary DSS. It is very important that this NetWare/IP virtual IPX address be different from any other real IPX address in the existing network, such as a real IPX segment address or a NetWare server's internal IPX address.

Figure 6: NWIP.NLM is loaded at the server and uses a virtual IPX address.



Since the server believes that NetWare/IP is just another instance of IPX, any server-based application that expects to see IPX will function over NetWare/IP. This includes server-based backup and virus scanning products, SAA gateways, e-mail/messaging solutions, and even NDS.

Configuring a Server to Act as a Gateway

When NWIP.NLM is loaded on an IPX server, it defaults to *not* act as a NetWare/IP-to-IPX gateway. Loading NWIP.NLM on an existing IPX server will allow the NetWare operating system, and all NLMs

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

loaded on the server, to "see" the NetWare/IP network. However, by default, the server will not route packets between the NetWare/IP and IPX segments unless specifically configured to do so.

To enable the server to route between NetWare/IP and IPX, perform the following configuration steps:

1. The NetWare/IP installation adds the following line to the server's AUTOEXEC.NCF file. This disables routing between the NetWare/IP and IPX interfaces.

   ```
   load IPXRTR routing=none
   ```

   To enable the NetWare/IP-to-IPX gateway functionality, remove either this entire statement, or just the "routing=none" portion, from the server's AUTOEXEC.NCF file.

2. By default, the NetWare/IP server will not advertise IPX services in the DSS database. To enable this functionality so that other devices in the NetWare/IP domain will "see" the locally connected IPX devices, load UNICON and set "Forward IPX information to DSS?" to yes.

NetWare/IP Design Guidelines

NetWare/IP is relatively straightforward to implement. This section presents a few guidelines that ensure a highly scalable, fault tolerant design.

DSS Design Guidelines

Any NetWare 4.1 server can be configured to provide DSS services. However, most customers find than only a few DSS servers are actually required within their environment. Listed below are the DSS server placement guidelines:

- Each DSS server can provide DSS services for 50 to 100 NetWare/IP servers. Factors that influence the scalability of DSS servers include size of the SAP/RIP database, frequency of changes, and the DSS-DSS and NWIP-DSS synchronization intervals.
- Not every NetWare/IP server needs to be configured as a secondary DSS server. Generally, secondary DSS servers are located at geographical sites where there are five or more NetWare/IP servers, or at aggregation points within the WAN infrastructure.
- If a DSS server will provide DSS services to fewer than 50 NetWare/IP servers, it may be placed on an existing NetWare 4.x server without much concern. If a DSS server will provide DSS services to more than 50 NetWare/IP servers, consider placing the DSS services on a dedicated NetWare 4.x file server.
- If DSS SAP filtering is used, placement of secondary DSS servers will determine the scope of the DSS database. Most customers who use DSS SAP filtering tend to deploy more DSS servers than necessary to further define SAP boundaries. DSS SAP filtering is described in detail in the Novell Consulting NetWare/IP Advanced Strategy Workbook, found at this URL: `http://www.novell.com/corp/programs/ncs/toolkit/ wl_nwip.html.`
- Consider placing a DSS server at those sites where NetWare/IP clients are located to improve performance of "Nearest Server Queries". By default, NetWare/IP clients will use a UDP broadcast to their local subnet to find services. However, if NSQ_BROADCAST is disabled on the client, or if there is not a NetWare/IP server within UDP broadcast range of the client, the client will query its preferred DSS server to resolve the NetWare service. If the DSS server is across a WAN link, this may cause the client to pause for up to 5 seconds before finding the necessary service from the DSS server.
- For medium and large NetWare/IP implementations, configure the NetWare/IP servers to use secondary DSS servers instead of the primary DSS. Reserve the processing power of the primary DSS

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

server for synchronizing the secondary DSS servers.

- If possible, minimize the number routers between the primary DSS and the secondary DSS servers by placing the primary DSS in the relative center of the WAN.

DNS Guidelines

DNS is not required for NetWare/IP. However, if you choose to use DNS to provide greater fault tolerance during server and client initialization, consider the following guidelines:

- NetWare/IP servers and clients are not placed in the DNS NetWare/IP subdomain. Only a few, select DSS servers should have name server (ns) entries in DNS.
- Don't enter a name server (ns) record for the primary DSS in the DNS NetWare/IP subdomain. This will prevent stray NetWare/IP servers and clients from connecting to the primary DSS.
- NetWare/IP 2.2 provides BIND 4.8.3 DNS. The Novell DNS will interact fully with an existing DNS environment.

NetWare/IP Server Guidelines

These guidelines are helpful when configuring NetWare/IP servers:

- Loading IPXRTR.NLM will improve the efficiency of communication between NWIP.NLM and the server's internal router.
- List several DSS servers in the NetWare/IP "Preferred DSS" list, starting with the closest DSS. Avoid listing the primary DSS if possible.

NetWare/IP-to-IPX Gateway Guidelines

NetWare/IP-to-IPX gateways are found in almost every NetWare/IP environment. The following guidelines should be helpful when configuring these gateways:

- Consider using two NetWare/IP-to-IPX gateways per IPX broadcast domain. Multiple gateways automatically provide load balancing and fault tolerance without any additional configuration.
- Avoid using more than two NetWare/IP-to-IPX gateways per IPX broadcast domain. Each gateway will broadcast SAPs for services found in the DSS database. Multiple NetWare/IP-to-IPX gateways within an IPX broadcast domain may increase IPX broadcasts to an unacceptable level.
- By default, IPX servers that also have NetWare/IP loaded are not NetWare/IP-to-IPX gateways. Enable the NetWare/IP-to-IPX gateway by setting "Forward IPX to DSS" to ON and removing "routing=none" from the "Load IPXRTR routing=none" statement in the AUTOEXEC.NCF file.

Client Guidelines

The following guidelines are useful if the NetWare/IP implemen-tation will include NetWare/IP clients:

- If NetWare/IP clients are within UDP broadcast range of NetWare/IP servers, set "NSQ_BROADCAST" to OFF. If NetWare/IP clients are not within UDP broadcast range of NetWare/IP servers, consider setting "NSQ_BROADCAST" to OFF. If "NSQ_BROADCAST" is set to ON and there are no NetWare/IP servers within UDP broadcast range, clients may pause for up to 5 seconds when searching the network for resources such as file servers and SAA gateways.
- NetWare/IP 2.2 includes a DHCP server. Consider using the DHCP server to provide both IP address and NetWare/IP parameters.
- Set the "Nearest NetWare/IP Server" to local NetWare/IP servers to speed up the initial attachment to

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

the network.

- Set the "Preferred DSS" to the nearest DSS. Don't include the primary DSS in the "Preferred DSS" list.

Migrating from IPX to NetWare/IP

Because NetWare/IP offers the flexibility to run a mixed IPX and NetWare/IP environment, NetWare customers are choosing to implement both IPX and NetWare/IP in different areas of their network. For example, NetWare/IP is often implemented across WAN links while IPX is retained on the LAN. This hybrid solution offers the best of both worlds: a single protocol WAN infrastructure based on TCP/IP with the plug-and-play capability of IPX on local segments. Approximately 90% of customers implementing NetWare/IP are using the hybrid NetWare/IP WAN, IPX LAN solution, either as the final implementation or as a stepping stone towards a complete TCP/IP WAN and LAN.

There are several advantages to replacing IPX with NetWare/IP on the WAN:

- IPX's periodic SAP and RIP broadcasts across WAN segments are inefficient. NetWare/IP eliminates SAP and RIP from the WAN, improving performance as much as 40% or more.
- Most customers are currently routing both TCP/IP and IPX. Removing IPX reduces the router memory requirements and CPU overhead required for routing IPX. NetWare/IP relies on standard IP routing and does not incur any additional overhead on IP routers.
- Most large IPX environments have implemented IPX SAP filtering, which requires additional router memory, CPU cycles, and places a greater burden on the router administrators. NetWare/IP removes the IPX routing burden from the routers. Plus, router administrators won't need IPX training.
- Implementing a NetWare/IP WAN is relatively simple because only one or two NetWare servers per site must be configured with the NetWare/IP server software. It is not necessary to reconfigure every server and every client within the network just to gain the benefits of NetWare/IP over the WAN.

Most customers would like to eventually remove IPX, not just from the WAN but from local segments as well. While technically this is easy, many other issues often arise:

- Most customers are used to IPX's plug-and-play capability, where an IPX client can move to any segment or any site within the corporate network and connect to resources. This is possible with TCP/IP, but requires planning and additional technologies, such as DHCP.
- Many customers are struggling with providing IP addresses and sub-nettting standards for current and anticipated future growth. Allocating and tracking IP addresses requires additional administrative work that is unfamiliar to IPX administrators.
- Migrating IPX clients to NetWare/IP requires between 5 and 15 minutes per workstation, which can be burdensome if there are several thousand workstations on the network.
- It might be very difficult to remove IPX from every segment. Embedded IPX devices, such as printers, may need reconfiguration to provide services over TCP/IP. Other IPX devices, such as CD-ROM servers and fax servers, may not have equivalent TCP/IP functionality.

The hybrid NetWare/IP WAN-IPX LAN solution provides great benefits with minimal work and client interruption. Bringing NetWare/IP to every desktop requires additional work, mostly in establishing IP connectivity to the workstation. Once the work-station has IP connectivity, conversion to NetWare/IP is easy.

There are two phases to create a hybrid NetWare/IP WAN-IPX LAN environment. There are an additional two phases to create a complete NetWare/IP network that eliminates IPX wherever possible. Most customers implement Phase 1 and Phase 2 to provide an NetWare/IP WAN while maintaining IPX on the

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

LAN. You can implement all four phases if a complete NetWare/IP environment is required.

Phase 1: DSS Planning and Installation

Before installing any software, consider the following:

- Decide on the best location for the primary DSS server. Consider placing the primary DSS to minimize WAN hops between the primary DSS server and secondary DSS servers.
- Determine how many secondary DSS servers must be deployed to meet the goals of performance, SAP filtering, and scalability.
- If DNS will be used to allow NetWare/IP servers and client to discover DSS servers by querying DNS, contact the DNS administrator and have the administrator create a NetWare/IP subdomain within DNS.
- Determine the fate of embedded IPX devices. Is it possible to upgrade the device to an equivalent IP service? Is it possible to keep IPX on a few, selected segment to support embedded IPX devices that do not have equivalent IP services.
- Choose a virtual IPX address for the NetWare/IP domain. Ensure that this virtual IPX address isn't filtered within IPX routed network.

Note: Make sure that the NetWare/IP virtual IPX address is not duplicated with a real IPX segment address or NetWare server internal IPX address.

Identify those servers within the environment that are frequently accessed from remote IPX sites. NetWare/IP should be added to these servers early in the migration, thereby permitting the server to respond directly to remote NetWare/IP requests and eliminating a hop through a NetWare/IP-to-IPX gateway. Without NetWare/IP on these server, all remote IPX client traffic must pass through two NetWare/IP-to-IPX gateways)one at the client site and one at the local server site. Adding NetWare/IP to servers that are frequently accessed by remote clients allows an IPX client to send a request to its local NetWare/IP-to-IPX gateway, which then forwards the request directly to the NetWare/IP server, eliminating the transition through the second gateway.

Install the NetWare/IP 2.2 software on a new or existing NetWare 4.x server. Configure the server as the primary DSS and as a NetWare/IP-to-IPX gateway by setting "Forward IPX to DSS" to ON and removing "routing=none" from the "Load IPXRTR routing=none" statement in the AUTOEXEC.NCF file. Consider configuring an additional NetWare/IP-to-IPX gateway to provide fault tolerance and load balancing.

Phase 2: Migrating the WAN from IPX to NetWare/IP

On a site-by-site basis, install NetWare/IP on one or two existing NetWare 4.x servers and configure the servers as NetWare/IP-to-IPX gateways. A single NetWare/IP-to-IPX gateway is sufficient to handle the communication between the remote site and the central office if the WAN speed is less than approximately 6MB/sec. Even though one NetWare/IP-to-IPX gateway is sufficient, consider multiple NetWare/IP-to- IPX gateways per site to take advantage of NetWare/IP's automatic fault tolerance and load balancing.

Once NetWare/IP connectivity has been established to the remote site, disable IPX routing between the remote site and the central office to avoid any routing problems cause by parallel NetWare/IP and IPX routes.

Continue Phase 2 on a site-by-site basis until IPX is removed from all WAN links to remote sites.

Phase 3: Migrating a Site from IPX to NetWare/IP

During the migration from IPX to NetWare/IP, it is very important to provide minimal user interruption. The site migration begins by adding NetWare/IP to all existing IPX servers, thereby permitting equal NetWare server access to both NetWare/IP and IPX clients without an intermediate NetWare/IP-to-IPX gateway. If a

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

secondary DSS server is required at this site (as determined in Phase 1), configure one of the NetWare/IP servers to provide DSS services. Configure all NetWare/IP servers within the site to use the closest secondary DSS server, whether that DSS server is across the WAN or present at the site.

With the exception of the NetWare/IP-to-IPX gateways implemented in phase 2, none of the servers at the site will be configured as NetWare/IP-to-IPX gateways.

After NetWare/IP is added to all existing IPX servers, start migrating IPX clients to NetWare/IP. If possible, migrate embedded IPX devices, such as IPX printers, to an equivalent TCP/IP service.

Phase 4: Removing IPX

After all clients are migrated to NetWare/IP, remove IPX from all NetWare servers and routers wherever possible. If IPX connectivity is required for embedded IPX devices, bind IPX wherever necessary.

NetWare/IP Implementation and Migration Examples

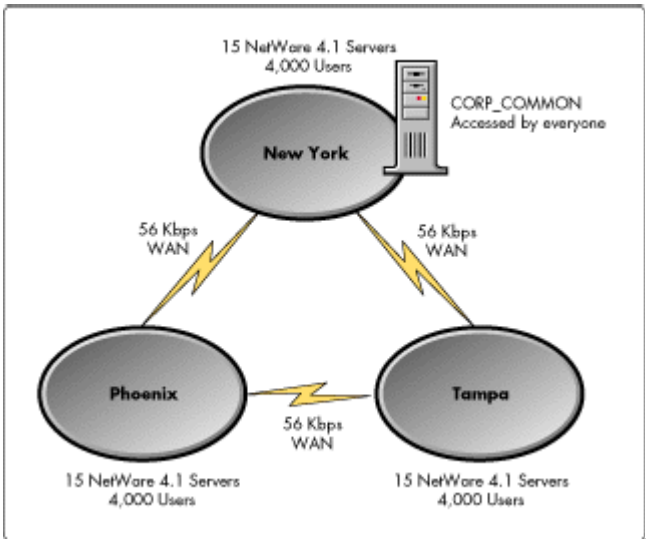
When implementing NetWare/IP, there are two main issues to consider: (1) What is the optimal NetWare/IP WAN design? and (2) What is the optimal NetWare/IP design to completely remove IPX from the WAN and the LAN? This section takes you through three implementation examples, covering the following typical network configurations:

- Three large offices separated by slow IP WAN links
- One large office with 40 small remote sites
- Several small, medium, and large offices

Example 1: Three Large Offices Separated by Slow IP WAN Links

In this first customer example, three sites)in New York, Tampa, and Phoenix)are joined by a 56Kbps WAN that does not support TCP/IP. Each office has 15 NetWare 4.1 servers and 4000 IPX clients. Server CORP_COMMON in New York is accessed frequently by remote clients (see Figure 7).

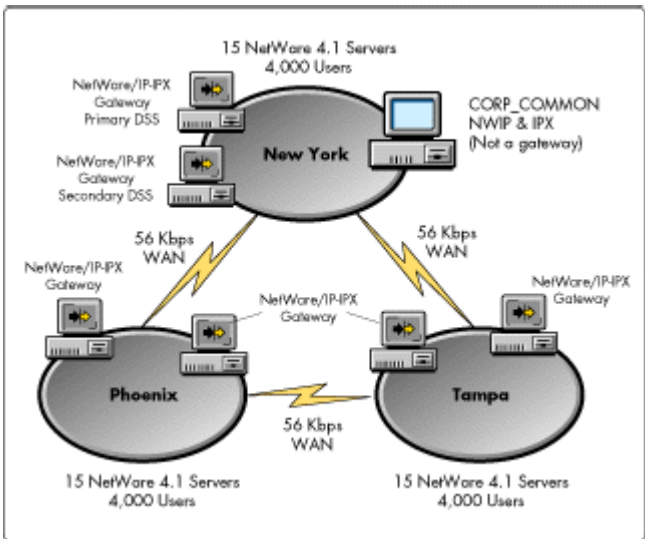
Figure 7: An example network with three large IPX sites joined by an IPX WAN.



Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

Proposed NetWare/IP WAN Design. Place the primary DSS in the New York office. Add NetWare/IP to two existing NetWare/IP servers in each office, configuring these servers as NetWare/IP-to-IPX gateways. While a single NetWare/IP-to-IPX gateway is more than sufficient, multiple gateways are used for fault tolerance. Add NetWare/IP to the CORP_COMMON server in New York, since this server is accessed frequently by remote IPX clients. While the primary DSS could easily handle the synchroni-zation of seven NetWare/IP servers, a secondary DSS server is deployed in New York to provide fault tolerance should the primary DSS become unavailable. This design is illustrated in Figure 8.

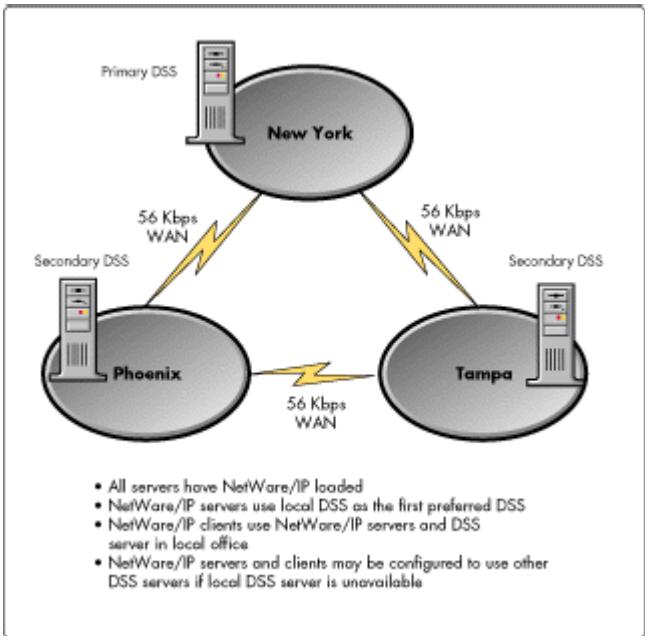
Figure 8: NetWare/IP-to-IPX gateway and DSS server placement. IPX remains on the local segments; only TCP/IP is routed between sites.



Proposed NetWare/IP WAN/LAN Design. Place the primary DSS server in the New York office and one secondary DSS server in each of the Tampa and Phoenix offices. At each office, add NetWare/IP to all of the servers, configuring the servers to use the secondary DSS in their local office as their first preferred DSS, and a DSS server in a remote office as their second preferred DSS. NetWare/IP clients are configured to use local NetWare/IP servers as their "Nearest NWIP Server" and the local secondary DSS server as their "Preferred DSS." IPX is removed from all segments unless required for embedded IPX devices. This design is illustrated in Figure 9.

Figure 9: NetWare/IP is installed on all servers and clients. Servers and clients are configured to use the DSS servers at their local site.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD



Note: To simplify configuration and provide better mobile user support, you can implement Novell's DHCP. Novell's DHCP server provides a single point of management for all client IP addresses, as well as providing the necessary DNS and NetWare/IP configuration information. Details of DHCP implementation will be covered in a follow-up AppNote.

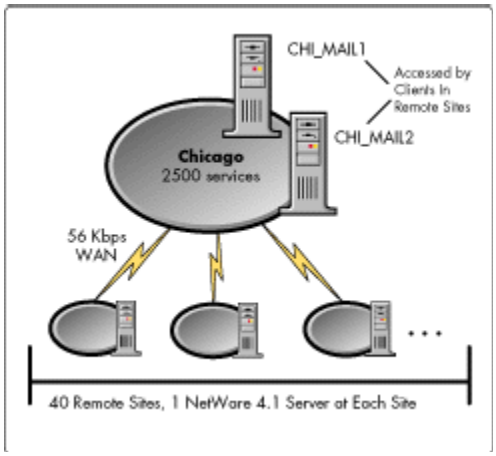
Example 2: One Very Large Office with 40 Small Remote Sites

For our next example, consider a large corporation with over 2500 services (servers, printers, and so on) in the Chicago office. Forty remote sites are connected to the Chicago home office with 56Kbps WAN links. Each remote site has only one NetWare 4.1 server. Chicago servers CHI-MAIL1 and CHI-MAIL2 are mail servers that are frequently accessed by remote clients (see Figure 10).

One other item to note in this example is that WAN performance between the remote sites and the Chicago office is very slow.

Figure 10: Example network with 40 remote sites connected to a home office over 56 Kbps WAN links.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD



Before we determine the best NetWare/IP configuration for this customer, we need to discover why the WAN performance is so slow. To do this, we can use the formula introduced earlier for calculating the percentage of the WAN consumed by IPX SAP broadcasts:

$$\frac{\text{\# of SAPs}}{\text{Speed of WAN in Kbps}} \times 1.07 = \%\text{ of SAP load on WAN circuit}$$

Plugging in the numbers from our example:

$$\frac{2500\text{ SAPs}}{56\text{Kbps}} \times 1.07 = 47.8\%\text{ of WAN consumed by SAPs}$$

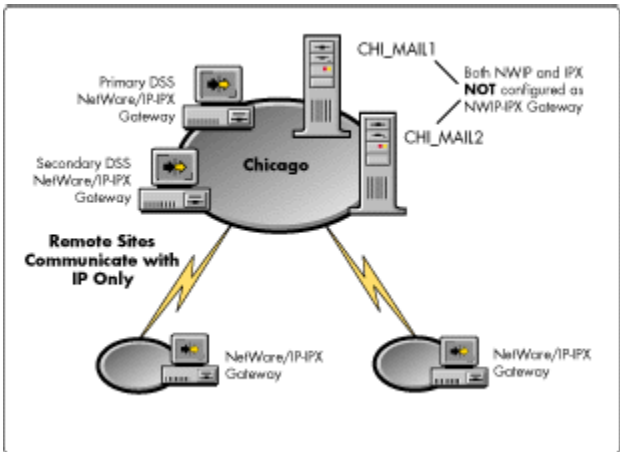
Almost half (47.8%) of the WAN circuit is currently being taken up by service and route advertisements. Switching to NetWare/IP will reduce that consumption to less than 1%. Thus implementing NetWare/IP in this environment will almost double WAN performance.

Proposed NetWare/IP WAN Design. Start by installing NetWare/IP on two new or existing NetWare/IP servers in the Chicago office. Configure one of the servers as the primary DSS, and the second server as a secondary DSS. Make both servers NetWare/IP-to-IPX gateways. Since CHI- MAIL1 and CHI-MAIL2 are accessed frequently from remote sites, add NetWare/IP to these servers, but do not configure the servers as NetWare/IP-to-IPX gateways.

At each site, add NetWare/IP to the existing NetWare 4.1 server and configure the server as a NetWare/IP-to-IPX gateway. At half of the sites, configure the NetWare/IP servers to use the primary DSS and then the secondary DSS in the NetWare/IP server's preferred DSS list. For the other half of the sites, configure the NetWare/IP servers to use the secondary DSS and then the primary DSS in the NetWare/IP server's preferred DSS list. Once NetWare/IP connectivity is established, remove IPX from the WAN router. Continue this process at each site until all WAN links are upgraded from IPX to NetWare/IP (see Figure 11).

Figure 11: NetWare/IP gateways are located in every office. Two DSS servers in Chicago provide DSS services to the entire network.

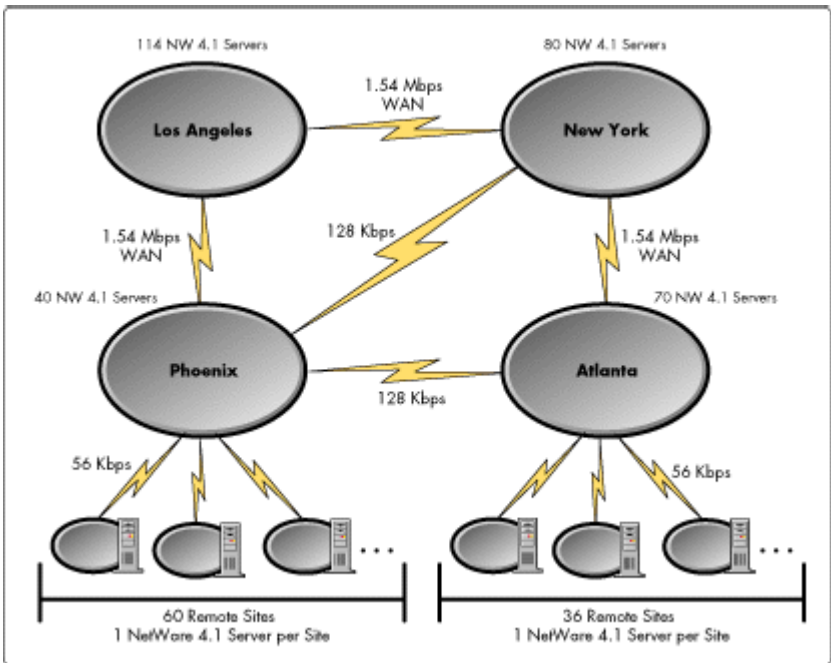
Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD



Example 3: Several Small, Medium, and Large Offices

For our third example, consider a large corporation with the infrastructure shown in Figure 12. This configuration comprises 400 servers in 100 sites, separated by WAN links ranging from 56Kbps up to 1.54Mbps. Some sites have dozens of servers; others, just a single NetWare 4.1 server. Let's go through the migration phases to convert both the WAN and the LAN to a pure NetWare/IP environment.

Figure 12: Example of a large-scale NetWare/IP implementation



Phase 1: DSS Planning and Implementation. DSS servers will be deployed in each major regional site. Here's a site-by-site breakdown of the DSS placement strategy.

- *Los Angeles*. The primary DSS server is in Los Angeles to minimize WAN hops from the secondary

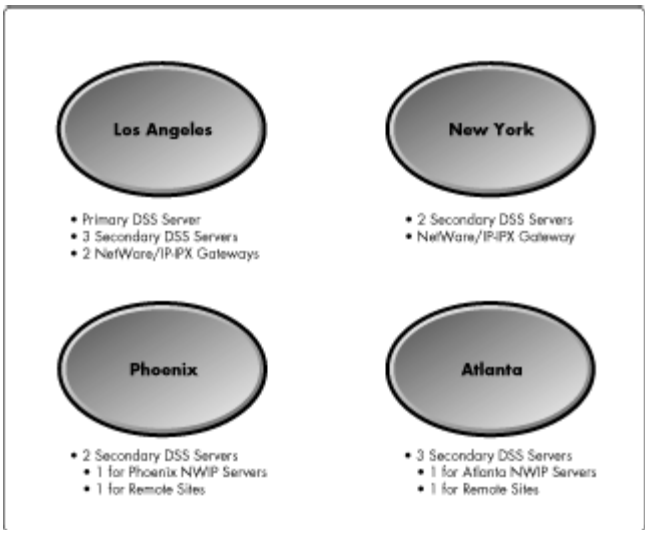
Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

DSS servers, and because most NetWare/IP expertise is concentrated in the Los Angeles office. Three additional Los Angeles servers are configured as secondary DSS servers. All NetWare/IP servers in the Los Angeles office will use local secondary DSS servers. No Los Angeles NetWare/IP servers will be configured to use the primary DSS server; rather, the processing power of the primary DSS server is reserved to keep the secondary DSS servers synchronized.

- *New York*. Two secondary DSS servers are placed in the New York office. NetWare/IP servers in New York will use local secondary DSS servers.
- *Phoenix*. Two secondary DSS servers are placed in the Phoenix office. One of the secondary DSS servers will service the 40 Phoenix NetWare/IP servers. The second Phoenix secondary DSS server will service NetWare/IP servers in the 60 remote sites.
- *Atlanta*. Three secondary DSS servers are placed in the Atlanta office. The Atlanta NetWare/IP servers will be balanced across two of the secondary DSS servers. All the NetWare/IP servers in the 60 remote sites will use the third Atlanta secondary DSS server.

The plan for placing DSS servers in Phase 1 is illustrated in Figure 13.

Figure 13: Summary of DSS server placement.



The highlights of this design are:

- Even though a single DSS server in each of the major sites is sufficient to handle the load of the local NetWare/IP servers, multiple NetWare/IP servers are used. This serves two purposes; first, by keeping the ratios small, the secondary DSS servers may be placed on existing NetWare servers, eliminating the hardware cost of dedicated secondary DSS servers. Second, local NetWare/IP servers are evenly balanced across the local DSS servers, but are configured to use another local DSS server if their first local DSS server is unavailable.
- If DSS SAP filtering is ever required, regional secondary DSS servers simplify DSS SAP filtering. Regional secondary DSS servers are easily configured for SAP filtering, allowing a local site to "see" all of the local SAPs but only those SAPs from remote sites that pass the DSS SAP filter.

Phase 1 indicates that a NetWare/IP-to-IPX gateway should be installed in the home office so that communication between the remote sites and the home office is as direct as possible. However, there isn't

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

really a home office in this design that would provide efficient communication with a single NetWare/IP-to-IPX gateway. For example, what if the a NetWare/IP-to-IPX gateway was installed only in the New York office, and then the remote Atlanta sites were migrated to NetWare/IP? All traffic from the remote office would route through IP to New York, convert to IPX, and then travel to Atlanta.

In this design there is no home office; therefore, two NetWare/IP- to-IPX gateways should be installed on existing NetWare servers in each of the major offices. Once NetWare/IP connectivity is established between the major offices, IPX is removed from the WAN links connecting the major offices. Phase 2 can now begin.

Phase 2: Converting the IPX WAN to NetWare/IP. In this complex design, Phase 1 and Phase 2 blend together. After the major sites are joined by a NetWare/IP WAN, the links to remote sites may be converted to NetWare/IP. Begin by adding a NetWare/IP to an existing NetWare server in each of the remote sites. Configure the server as a NetWare/IP-to-IPX gateway. Once NetWare/IP connectivity is established to the site, remove IPX routing from the WAN link connecting the remote site to the rest of the WAN.

Proceed on a site-by-site basis until IPX is removed from all WAN links. With Phases 1 and 2 complete, a the hybrid NetWare/IP WAN, IPX LAN migration is complete. If NetWare/IP will replace IPX on local LAN segment, proceed with Phases 3 and 4.

Phase 3: Migrating a site from IPX to NetWare/IP. On a site-by-site basis, add NetWare/IP to all existing NetWare servers, but do not configure the servers as NetWare/IP-to-IPX gateways. Configure the NetWare/IP servers within the site to balance the load across the local secondary DSS servers. If possible, install DHCP and configure the DHCP profiles for IP address leasing and to provide NetWare/IP information.

After NetWare/IP is added to all servers, begin the migration of IPX clients to NetWare/IP. Migrate any embedded IPX device to provide equivalent services over TCP/IP, such as reconfiguring embedded IPX printers to use LPR/LPD printing.

Phase 4: Removing IPX. When the client migration to NetWare/IP is complete, remove IPX from those LAN segments where IPX isn't required by reconfiguring routers and removing IPX from NetWare server. On those segments where IPX is required, keep IPX bound. Note that if IPX is required for embedded IPX devices, determine if the device requires access to the NetWare/IP world. If the embedded IPX device most only needs to connect via IPX to a single NetWare server, but does not need to access resources within the NetWare/IP network, the NetWare/IP server should not be configured as a NetWare/IP-to- IPX gateway.

Troubleshooting NetWare/IP

This section provides tips and tricks for troubleshooting NetWare/IP servers, clients, and DSS servers.

General

- When troubleshooting issues at the NetWare server, enable the PKERNEL debugging options. From UNICON, select "Configure Error Reporting", "Configure Error Log in/SNMP Alert Levels", and set both "Product Kernel Screen Error Level" and "Audit Log Error Level" to DEBUG. This enables advanced error messages to the PKERNEL screen. These messages are extremely helpful when troubleshooting DNS, DSS, and NetWare/IP problems at the server console. Use the NetWare/IP 2.2 online documentation to interpret these errors.

- Always ensure that the NetWare/IP virtual IPX address is not duplicated, either as an IPX segment address or an internal IPX address on a NetWare server.

DNS Server

- NetWare/IP includes an nslookup feature in the Unicon utility. From Unicon, select "Manage Services",

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

"DNS", "Administer DNS", "Query Remote Name Server.". This feature is very helpful to determine if DNS is correctly responding to DNS queries generated by NetWare/IP servers and clients.

DSS Server

- Use the "Load DSS /STAT" command to check for DSS-DSS synchronization errors. Use the "Load DSS /SYNC" command to force secondary DSS servers to synchronize with the primary DSS server.

NetWare/IP Server and NetWare/IP-to-IPX Gateway

- Make sure that the NetWare/IP-to-IPX gateway is enabled since the default NetWare/IP install does not enable the NetWare/IP- to-IPX gateway. To enable the NetWare/IP-to-IPX gateway, set "Forward IPX Information to DSS" in the NetWare/IP server configuration, and ensure that IPXRTR is loaded without the "routing = none" statement.
- During the default installation of NetWare/IP, the server's minimum and maximum packet receive buffers are changed to 100 and 500, respectively, overwriting any previous setting.
- Use the "Load NWIP /STAT" command to determine which DSS is providing DSS services, and to check for NetWare/IP-DSS synchronization errors. Use "Load NWIP /SYNC" to force a NetWare/IP-DSS synchronization.
- NetWare/IP reports important information in the Monitor utility's LAN Statistics. These statistics are very useful and are documented in the NetWare/IP 2.2 online documentation.

NetWare/IP Client

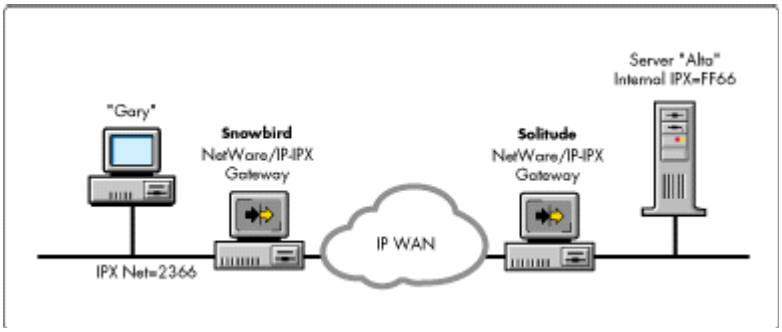
- Use the "NWIP.EXE /V" command during NetWare/IP client initialization to display additional information about DNS, DSS, and NetWare/IP servers consulted during the initial NetWare/IP connection. This function is also provided in the Client 32 error logging function for both DOS/Windows 3.1 and Windows 95 versions of the 32-bit client.

NetWare/IP-to-IPX Gateway Issues

Almost all NetWare/IP-to-IPX gateway issues are due to incorrect configurations. Either routing is disabled with "Load IPXRTR routing=none" or IPX information, such as IPX segment addresses, is not in the DSS database because "Forward IPX Information to DSS" is set to "No".

Consider the example network shown in Figure 14. Gary's IPX workstation is having problems attaching to, or perhaps staying connected to, the IPX server named Alta. Gary is connecting through the NetWare/IP-to-IPX gateways Snowbird and Solitude.

Figure 14: Example configuration to illustrate troubleshooting mixed NetWare/IP - IPX networks.



Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

The following requirements must be met for Gary to log in to Alta:

1. *Alta's SAP and RIP must be in the DSS database*. When Solitude hears Alta broadcast a SAP packet advertising Alta's services, Solitude collects the IPX SAP and creates a SAP record in the DSS database associating Alta's SAP with Solitude's IP address. Likewise, when Alta broadcasts a RIP packet with Alta's internal IPX address, Solitude creates a RIP record in DSS associating Alta's internal IPX address with Solitude's IP address. Solitude is creating these records in the DSS database because "Forward IPX Information to DSS" is set to Yes.

2. *Gary's IPX segment must be in the DSS database*. Snowbird creates a RIP record in the DSS database for Gary's IPX segment. This allows Solitude to see a route to the IPX network 2366 by sending packets to the NetWare/IP-to-IPX gateway, Snowbird, which is connected to IPX network 2366. Snowbird is creating these records in the DSS database because "Forward IPX information to DSS" is set to Yes.

3. *Gary's workstation must see Alta's SAP and RIP*. Solitude learns of Alta from the DSS database. If Solitude is configured as an NetWare/IP-to-IPX gateway, it must broadcast Alta's SAP and RIP to the IPX segment. Solitude won't broadcast Alta's SAP and RIP if IPX routing is disabled with "Load IPXRTR routing=none".

4. *Alta must see Gary's IPX segment*. Once Gary's workstation sees Alta's SAP and RIP, it sends an IPX packet for Alta to Snowbird. Snowbird converts the packet from IPX to NetWare/IP and sends the packet Solitude. Solitude converts the NetWare/IP packet to IPX and sends the packet to Alta. Before Alta can send a response back to Gary's workstation, it must have a route to Gary's IPX segment 2366. Solitude knows that to reach IPX segment 2366, it must send packets to Snowbird's IP address.

For Gary's workstation to send and receive packets from Alta, these conditions must be met:

1. Gary's IPX segment address must be in the DSS database. These DSS records are created because Snowbird has "Forward IPX Information to DSS" set to Yes.

2. Alta's SAP and RIP must be in the DSS database. These DSS records are created because Solitude has "Forward IPX Information to DSS" set to Yes.

3. Gary's workstation must be able to see Alta's SAP and RIP. Gary's workstation sees Alta's SAP and RIP because IPX routing isn't disabled on Snowbird. If Snowbird had IPXRTR loaded with "routing=none," Gary's workstation would not see Alta's SAP and RIP.

All three of these conditions can be checked with the UNICON utility's "Browse DSS Database" feature. Using this feature, a NetWare/IP administrator can check the DSS database to ensure that there is a SAP record for the Alta and that there are two RIP records, once each for Alta's internal IPX address, and one for Gary's IPX segment address. If these three records do not exist in the DSS database, Gary's workstation will not be able to connect to Alta.

Common NetWare/IP Issues

The chart below lists some of the common NetWare/IP issues, symptoms, and possible resolutions.

Symptoms	Possible Problem(s)	Resolution
RCONSOLE fails. NLIST SERVER /B displays remote address services, but IPX clients are unable to connect	NetWare/IP's internal IPX address has been duplicated with another IPX address, either a server's internal IPX address, or an IPX segment address.	NetWare/IP uses a virtual IPX address to advertise the NetWare/IP segment to the internal server operating system. If this is duplicated, packets destined for NetWare/IP links may be rerouted to other

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

to remote services. mis-configured Watchdog disconnects active users.		servers or IPX segments that are with the NetWare/IP virtual IPX address. Check or change the NetWare/IP virtual IPX address by with the UNICON utility and reconfigure the primary DSS, if necessary.
	IPXRTR has been loaded with "routing=none".	By default, NetWare/IP modifies the AUTOEXEC.NCF file to auto-load IPXRTR with routing disabled. This prevents NetWare/IP from forwarding SAP/RIP information learned from the DSS to IPX segments connected to NetWare/IP servers. This also prevents IPX segment information from reaching the DSS. Therefore, remote NetWare/IP servers can't see the IPX segment because the segment information hasn't been propagated to DSS. Check to see if IPXRTR has been loaded with routing disabled on your NetWare/IP–IPX gateways.
	"Forward IPX information to DSS" has been set to No.	By default, NetWare/IP servers that also have IPX bound will not report SAPs and RIPs learned from the IPX segment to the NetWare/IP DSS. This prevents remote NetWare/IP servers from seeing IPX segments connected to the local NetWare/IP server. Check the status "Forward IPX information to DSS" in the UNICON configuration of the NetWare/IP server.
"Undefined Public the Symbol" during UNISTART.NCF execution. DSS or NetWare/IP no longer UNISTART.NCF auto-loads from AUTOEXEC.NCF or UNISTART.NCF file.	Load order in UNISTART.NCF file is incorrect. Load statements missing from UNISTART.NCF.	NetWare/IP uses UNISTART.NCF to load necessary NetWare/IP modules. When the UNICON option "Start/Stop Services" is used to start or stop DNS, DSS, NetWare/IP, LPR_GWY, or XCONSOLE, the file may be updated. For example, if you use "Start/Stop services" to unload Domain SAP/RIP service, the "Load DSS" line is commented out of the UNISTART.NCF file. Restarting DSS from "Start/Stop Services" will un-comment the "Load DSS" statement in the UNISTART file, allowing DSS.NLM to load when UNISTART is executed. Note that UNISTART.NCF may also be used by other products, such as NFS, that may rearrange

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

the		load order of modules used by NetWare/IP.
Excessive UDP receives broadcasts. "UDP Buffer Full" and "Cannot create TCP connection" error messages from PKERNAL.	NetWare/IP-to-IPX gateway is replicating IPX NetBIOS broadcasts to NetWare/IP UDP broadcasts.	If a NetWare/IP-to-IPX gateway server a NetBIOS broadcast any IPX interface, the NetBIOS broadcast is retransmitted to the NetWare/IP interface. This may cause excessive UDP broadcasts. Check the NetWare/IP broadcasts by loading MONITOR, selecting "LAN/WAN Information," selecting the NetWare/IP board, and checking the custom statistic "Packets Transmitted as Broadcasts." If this number is very large relative to the total number of packets sent and received, or if this number continually increments and there are IPX NetBIOS clients (such as Windows for Workgroups, Windows 95, or Windows NT clients using Microsoft Networking), consider disabling IPX NetBIOS replication between IPX and NetWare/IP. To disable IPX NetBIOS replication, load SERVMAN, select "Communication", and change "IPX NetBIOS Replication Option" to 0. **Note:** This may affect NetBIOS communication between IPX and NetWare/IP.
	Insufficient UDP buffers for DSS-NetWare/IP synchronization.	UDP buffers are used during NetWare/IP-to-DSS synchronization. Sometimes a DSS server runs out of UDP buffers if several NetWare/IP servers attempt to synchronize with the DSS server simultaneously. Edit the sys:etc\nwparams file and add "MAX_UDP_PKTS 128" under the DSS heading. See "Modifying DSS Parameters" in the NetWare/IP online documentation.
	Insufficient TCP connections for DSS-to-DSS synchronization.	DSS-to-DSS synchronization requires a TCP connection between DSS servers. If all TCP connections are in use, a secondary DSS server may not be able to communicate the primary DSS. Edit the sys:etc\nwparams file and add "MAX_TCP_CONNS 32" under the DSS heading. See "Modifying DSS Parameters" in the NetWare/IP online documentation.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD

Conclusion

NetWare/IP gives network administrators greater flexibility in their choice of protocols, permitting pure NetWare/IP networks or fully interoperable NetWare/IP and IPX environments. NetWare/IP 2.2 also provides enhancements, such as LPR-LPD printing and DHCP, to further integrate and simplify deploying NetWare in TCP/IP environments.

NetWare/IP 2.2 is a stepping stone in Novell's path towards protocol independence. NetWare/IP 2.2 builds on the strong foundation of NetWare 4 and prior versions of NetWare/IP, delivering a scalable solution for connecting NetWare clients to resources over TCP/IP networks.

For More Information

For further information about NetWare/IP 2.2, consult the following resources:

- Visit the NetWare/IP 2.2 home page and find out more about Novell's Native IP strategy at `http://netware.novell.com/ discover/nwip/index.htm`.
- See the latest NetWare/IP 2.2 Frequently Asked Questions at `http://www.novell.com/corp/programs/ncs/toolkit/ internet.html`. This FAQ provides additional information about design, implementation, and troubleshooting.
- Download the Novell Consulting Services NetWare/IP 2.2 Advanced Strategy Workbook from `http://www.novell.com/corp/programs/ncs/toolkit/wl_nwip.html`. This workbook uses a mixture of graphics and text to describe NetWare/IP in much greater technical detail.

Copyright © 1990-2000, Novell, Inc. All Rights Reserved. Novell Support Connection CD