NOVEMBER 1995

NOVELL® RESEARCH

Guidelines for Implementing NetWare/IP

GARY HEIN
Senior Consultant
Novell Consulting Services

The popularity of TCP/IP as a transport protocol has been steadily increasing in corporate business networks. NetWare/IP is an add-on product that allows Novell customers to implement NetWare in a mixed IPX-IP environment or to migrate to an IP-only environment. NetWare applications can continue to run, without modification, over TCP/IP instead of IPX . This AppNote examines various NetWare/IP implementation scenarios and give guidelines and recommendations for each one.

Introduction . . . . . .
Background on NetWare/IP . . . . . .
Implementation Methodology. . . . . .
Case Studies. . . . . .
Tips, Tricks, and Suggestions . . . . . .
Sample Traces . . . . . .

RELATED APPNOTES

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, Faiq Ghatala, Myron Mosbarger, and Ronald Szeto of Novell for their help with this AppNote.

TRADEMARKS

NetWare, the N-Design, and Novell are registered trademarks and the NetWare Logotype (teeth logo), 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. UnixWare is a registered trademark of Novell, Inc. in the United States and other countries.

OS/2 is a registered trademark 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

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

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 (c) 1995 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.
122 East 1700 South
Provo, Utah 84606 USA

Introduction

NetWare/IP is a set of NetWare Loadable Modules (NLM s) and client software that enables existing NetWare 3 and NetWare 4 servers to use TCP/IP or Novell's IPX (or both) as their transport protocol. This flexibility allows customers to deploy a total IP solution or a mixed IPX-IP solution in their NetWare environment.

This AppNote provides a brief background of NetWare/IP, and gives some design options and strategies for effective implementation. It presents three case-study scenarios to help you see the advantages and disadvantages of various configurations. These are followed by tips, tricks, and suggestions for implementing NetWare/IP. Finally, two packet traces are analyzed to illustrate the underlying processes that occur when a NetWare/IP client connects to a NetWare/IP server, and when a NetWare/IP server initializes.

Background on NetWare/IP

This section gives some background information on NetWare/IP. After a brief overview of the benefits and latest updates of NetWare/IP, it introduces the various components that comprise the NetWare/IP software.

Benefits of NetWare/IP

NetWare/IP delivers a variety of benefits to organizations that want to use TCP/IP. It uses standard TCP/IP components and systems (domains, DNS, and so on), and provides the option of running NetWare on an IP-only infrastructure.

NetWare/IP eases migration of IPX-based networks to TCP/IP networks and eliminates dual administration of IP and IPX on routers. With NetWare/IP, existing client- and server-based NetWare applications can run seamlessly over TCP/IP. NetWare/IP also gives users the ability to log in to the NetWare resources from the Internet.

NetWare/IP eliminates the periodic SAP and RIP broadcasts associated with native IPX by providing a well known repository for SAP and RIP information. Many customers have implemented NetWare/IP simply as a means to eliminate periodic SAP and RIP broadcast traffic from slower WAN links.

NetWare/IP's performance compares very favorably to that of native IPX. Testing has shown NetWare/IP's

average throughput to be about 8 percent less than native IPX, due to the processing overhead associated with the additional NetWare/IP software running at the client and the server. However, this performance degradation is not noticeable to users. In fact, NetWare/IP can outperform IPX on slower WAN links, thanks to a user-configurable parameter to reduce the frequency of SAP and RIP traffic.

Latest Updates

The current release of tested patches for NetWare/IP version 1.1 is found in the file NIP318.EXE, which can be downloaded from CompuServe from the NetWare General Files Forum (go nwgenfiles), Library 02. This file may also be downloaded from Novell's Internet FTP server (ftp.novell.com or 137.65.1.3). The username is `anonymous`, and the password is `YourName@org`. NIP318.EXE is located in the `/pub/updates/unxiconn/nwip11` directory. Watch these online areas for future NetWare/IP updates.

Note: All recommendations given in this AppNote assume that patches from NIP318.EXE have been applied. Be sure to read all documentation provided with the patch. NIP318.EXE is required for NetWare/IP version 1.1 only.

NetWare/IP version 2.1 is currently available free with NetWare 4.1 until December 1995. The server and client software are also available for download as files NIPS21.EXE and NIPW21.EXE, respectively. These files are located in the /pub/updates/ unxiconn/nwip21 directory on Novell's FTP server. NIPS21.EXE contains the NetWare 4.1 NetWare/IP server software and online documentation. NIPW21.EXE contains the NetWare/IP 2.1 client software, and is only required if NetWare/IP connectivity is desired between NetWare/IP servers and DOS/Windows 3.1 workstations.

Novell will soon release NIP197.EXE, a patch to NetWare/IP 2.1 that fixes minor issues and enhances the product functionality. This patch will be available on NetWire and the /pub/updates/ unxiconn/nwip21 area on Novell's Internet FTP server.

NetWare/IP 2.1 includes enhancements that greatly improve scaling to thousands of servers. Some of the new NetWare/IP 2.1 features include:

- Full DNS support (BIND 4.8.3)
- Ability to "push" NetWare/IP parameters to the client via Novell's BOOTP
- More robust client (doesn't require DNS or DSS access to initialize)
- Third-party TCP/IP stack support
- Full NetWare Directory Services support
- Improved NLM performance through better CPU utilization
- Better WAN support and improved WAN performance tuning
- Support for registered and unregistered DSS
- SNMP instrumentation for the DSS and NWIP.NLM
- No stratification of server license, no serialization broadcasts
- Installation integrated with NetWare 4.1 INSTALL
- Support for Flex/IP and Unix print servers (allow printing to TCP/IP printers)
- Support for Windows NT, Windows 95, and DOS/Windows 3.1 machines running Novell's 32-bit client software (no OS/2 client support)
- Support for SLIP/PPP Dialer for remote clients through LAN WorkPlace for DOS

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

In general NetWare/IP 2.1 is very similar to NetWare/IP 1.1. The NetWare/IP 2.1 client will work with a NetWare/IP 1.1 server, but the NetWare/IP 1.1 client will not work with 2.1 servers. Because of the improvements to the NetWare/IP 2.1 client software, Novell strongly recommends the NWIP 2.1 client upgrade for all NetWare/IP 1.1 clients.

NetWare/IP 2.1 is designed and optimized for new features of the NetWare 4.1 operating system; therefore, NetWare/IP 2.1 is incompatible with NetWare 3.x servers. NetWare/IP 1.1 must be used if NetWare/IP is required on NetWare 3.x servers. NetWare/IP 2.1 and NetWare/IP 1.1 are fully interoperable.

Most of the guidelines in this AppNote apply to NetWare/IP 1.1 and 2.1 equally. Where there are differences, they will be noted.

Domain Name System (DNS)

The Domain Name System (DNS) is a hierarchical, distributed lookup service used primarily to link a host name to its associated IP address in a TCP/IP environment. DNS provides a flexible way for NetWare/IP clients and servers to locate NetWare Domain SAP/RIP Servers (DSSes). (DSS is explained under the next subheading.)

DNS is essentially a central database that maps mnemonic host names (such as `host1.novell.com`) to IP addresses (such as 137.25.17.1). This database can be queried by other TCP/IP nodes on the network. With a DNS server in place, users can contact a given host by name rather than by its four-octet integer IP address.

DNS uses administrative zones called *domains* to simplify and organize the management of portions of a very large network. Each domain is administered separately, eliminating the need for centralized allocation of IP addresses and host names. DNS domains can be divided into multiple subdomains. When configuring NetWare/IP, you create a single domain referred to as the *NetWare/IP Domain*. This domain contains DNS name server entries for a selected few NetWare DSSes that service the NetWare/IP domain. The NetWare/IP domain *does not* contain the host names of NetWare/IP servers or clients.

NetWare/IP servers and clients may query the DNS for authorized DSSes of their NetWare/IP domain. The DNS returns a list of hosts authorized to supply DSS information for that NetWare/IP domain.

NetWare/IP uses standard DNS services (BIND 4.8.3 compatible). These services may be provided by NetWare, UnixWare, or any other standard Unix DNS. Novell's DNS is able to fully integrate with third-party vendors' DNS servers in both primary and secondary configurations. NetWare/IP 1.1 provides limited DNS services through a set of server-based NLMs. NetWare/IP 2.1 provides a full DNS services. Both versions may act as a standalone DNS server, or as a subdomain of a larger DNS structure.

For more information about DNS and the role of DNS in NetWare/IP, see the *NetWare/IP Administrator's Guide*.

Domain SAP/RIP Server (DSS)

The DSS is a distributed, replicated Btrieve database of all services and routes within a particular NetWare/IP domain. In a NetWare/IP environment, DSS acts as a replacement for IPX broadcast-based SAP and RIP updates by providing a well-known repository for registering these services. Instead of broadcasting SAP and RIP service advertisements and requests, NetWare/IP servers and clients use point-to-point communication with a DSS for such information.

The DSS creates records of any learned services or routes that are reported to DSS by a NetWare/IP server. NetWare/IP servers (and sometimes clients) query the DSS for information about the NetWare resources available in a NetWare/IP DSS domain.

For example, suppose a server named FS1 is running DSS.NLM (the NetWare/IP DSS software). FS2 is a

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

NetWare/IP server that has an IPX interface to a network segment to which another server, FS3, is connected. When FS2 initializes and loads NWIP.NLM, it does the following:

1. Reports to FS1 (the DSS) any other SAP or RIP information that FS2 has learned about (namely itself and any services from the IPX segment).

2. At the same time, FS2 creates a TCP connection to FS1 (where the DSS resides) and downloads all SAP and RIP records from the DSS.

3. Broadcasts IPX SAP and RIP information from DSS onto the locally connected IPX segment, thereby allowing FS3 to "see" all of the services and routes available in the DSS domain.

Primary and Secondary DSS. NetWare/IP designates DSSes as either primary or secondary. Each NetWare/IP domain contains only one primary DSS, and may contain one or more secondary DSSes. Every DSS holds a database of all SAP and RIP information for the NetWare/IP domain. NetWare/IP servers communicate regularly with a DSS to obtain and register SAP and RIP updates.

Periodically, all DSSes synchronize with the primary DSS to update the services information within the NetWare/IP domain. The periodic synchronization between the primary DSS and secondary DSS, and from DSS to NetWare/IP server, occurs every five minutes by default. Each synchronization interval can be adjusted independently.

Every time a SAP or RIP entry is added or deleted, the "Version Number" of the DSS database changes. During synchronization, each version number is compared. If one is found to be different (either side has added, deleted, or changed a SAP/RIP record), only the changes between the versions are sent. By periodically comparing version numbers and sending only changes between versions, NetWare/IP uses very little network bandwidth to maintain advertisement of services and routes.

For larger NetWare/IP implementations (100 or more NetWare/IP servers), it is advisable to create a DSS hierarchy wherein NetWare/IP servers and clients synchronize with secondary DSSes. This reserves the full processing power of the primary DSS to maintain DSS synchronization.

Registered and Unregistered DSS. NetWare/IP uses DNS only as a "placeholder" for the NetWare/IP DNS subdomain, delegating name server authority to NetWare/IP servers running DSS.NLM. Therefore, "NS" (name server) and "A" (address) records are added to DNS for the host names and IP addresses of selected (not all) NetWare file servers running DSS.NLM.

DSS servers can be either registered or unregistered with DNS. A registered DSS server is visible to all NetWare/IP nodes through DNS query. Each registered DSS server has corresponding NS records in the DNS database, which identify it as a name server for the NetWare/IP domain. When a NetWare/IP client queries DNS for the location of the nearest DSS server, DNS will only return a listing of registered DSS servers, because they are the only ones it knows about.

If a DSS server is unregistered with DNS, a NetWare/IP node cannot locate it by issuing a DNS query. Instead, the NetWare/IP node must be provided the name or address of the unregistered DSS server as part of its preferred DSS server listing.

For example, you may want to designate a DSS server that is isolated from the rest of the NetWare/IP internetwork by a WAN link as an unregistered DSS server. This prevents NetWare/IP servers from redirecting their queries to this DSS server when other, closer DSS servers are busy or down. Yet other DSS servers should be registered in DNS, guaranteeing that a client may locate a DSS by querying DNS.

NetWare/IP Servers

Any existing server running NetWare 3 or 4 can be easily configured as a NetWare/IP server by loading NWIP.NLM. NetWare 3 servers can run only NetWare/IP 1.1. NetWare 4.1 servers must run NetWare/IP 2.1.

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

Additionally, a NetWare/IP server that has IPX bound to any interface can be configured as NetWare/IP gateway, which provides IPX clients access to IPX or NetWare/IP services via TCP/IP. NetWare/IP gateways are used primarily in the following circumstances:

- During the migration from IPX to NetWare/IP
- To provide remote IPX sites access to other sites via an IP-only link
- To provide IPX compatibility for embedded IPX devices (such as IPX print servers)

Every server that has IPX and NetWare/IP loaded will act as a NetWare/IP gateway, servicing requests between IPX segments and NetWare/IP services and routes. When NetWare/IP and IPX are both loaded on a NetWare file server, SAP/RIP information from NetWare/IP can be sent to any attached IPX segment, allowing other IPX servers and clients on the IPX segment to access all services and routes known to the DSS.

By default, a NetWare/IP server will *not* forward local IPX SAPs and RIPS to the DSS. If you want to pass SAPs and RIPs discovered on the IPX segment to the DSS, NetWare/IP must be configured within UNICON as "Forward IPX to DSS", or alternatively, the NWIP.NLM may be loaded with the optional forward parameter set to YES, as shown here:

```
LOAD NWIP ... /FORWARD=YES
```

NetWare/IP Clients

With minor changes, any current DOS IPX node using ODI drivers can be easily converted to a NetWare/IP node. This is done by loading TCPIP.EXE and NWIP.EXE in place of IPXODI.COM. TCPIP.EXE provides the IP protocol suite. NWIP.EXE is an IP application, similar to IPXODI.COM, that acts as an IPX Far Call emulator. NWIP.EXE generates UDP datagrams that completely eliminate the need for IPX packets. Applications that require IPX fully believe that IPXODI is present, thus assuring compatibility with any legacy IPX applications.

Note: The NetWare/IP product does not provide other TCP/IP applications such as FTP, TELNET, and so forth. These TCP/IP applications are available in LAN WorkPlace for DOS, NetWare Connect Services, and other Novell products.

NetWare/IP clients are very similar to their IPX counterparts, requiring only a few optional NET.CFG parameters that specify the client's preferred DSS server(s) and possibly NetWare/IP servers. NetWare/IP clients also maintain a NWIPPARM.NOV file located in the NWCLIENT directory that may be used for initialization when other mechanisms fail (more on this later).

Putting It All Together

A review of the steps necessary for a NetWare/IP 2.1 client to initialize will provide a basis for understanding how all of these pieces fit together to provide network access.

Step 1: The client locates a DSS server.

1a. When NWIP.EXE loads, the NetWare/IP client checks its NET.CFG file for the PREFERRED_DSS parameter. If any of the PREFERRED_DSS parameters reference a DSS host name instead of the DSS IP address, the client will query DNS to resolve the DSS host name to an IP address. The client then creates a list of all DSS IP addresses and proceeds to step 2.

1b. If the PREFERRED_DSS parameter has not been set in the client's NET.CFG, the client will generate a list of DSSes by querying the DNS servers listed in the client's RESOLV.CFG file, starting with the first

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

entry and proceeding until a DNS is found. Each DNS is queried for NS records of the NetWare/IP domain, as specified in the client's NET.CFG file via the NWIP_DOMAIN parameter. DNS will respond with all NS records of the NetWare/IP domain, which in effect is a list of all registered DSSes. Once the DSS list has been created, the client proceeds to step 2.

1c. If DNS does not respond, or DNS does not have NS records for the NetWare/IP domain, the client will check for the existence of the NWIPPARM.NOV file, which contains vital NetWare/IP information (such as the IP address of a valid DSS) from a successful client initialization. If the file exists, the client will search this file to locate a DSS by IP address. If the file does not exist, the client initialization fails.

Step 2: The client contacts DSS for NetWare/IP domain parameters.

The client next contacts a DSS and requests information about the NetWare/IP domain, such as UDP port, whether or not UDP checksums are used, timeout parameters, and so on.

Step 3: The client contacts and connects with a NetWare/IP server.

3a. If NSQ_BROADCAST is set to ON in the client's NET.CFG, the NetWare/IP client will send an IP UDP Get Nearest Server broadcast. Any NetWare/IP servers on the client's local segment will respond, unless the NetWare/IP server has been configured with "Reply to Get Nearest Server" set to OFF.

3b. If NSQ_BROADCAST is set OFF but the NEAREST NWIP SERVER is configured, the NetWare/IP client will attempt to connect to one of the servers listed under NEAREST NWIP SERVER in the client's NET.CFG.

3c. If NSQ_BROADCAST is set OFF and the NEAREST NWIP SERVER is not configured in the NetWare/IP client's NET.CFG, the NetWare/IP client will query DSS for a file server.

Once the client has located a valid NetWare/IP server, the VLM.EXE software creates a connection to the server, negotiating parameters for Large Internet Packets (LIP) and Packet Burst. From now on, instead of sending IPX broadcast requests for SAP or RIP advertisements or information, the NetWare/IP client will contact the NetWare/IP server directly for SAP/RIP information.

Note: During initialization and normal communication, the NetWare/IP client *always* communicates via TCP/IP.

At the end of this AppNote is a packet trace that shows packet-by-packet how the NetWare/IP client initialization process takes place. Also included is a packet trace of a NetWare/IP server with DSS initializing. Refer to these packet traces for more information about NetWare/IP client and server initialization.

Implementation Methodology

This section gives some NetWare/IP design options and strategies for effective implementation. Generally, NetWare/IP is implemented in four phases:

- Phase 1: Installing NetWare/IP and creating the Primary DSS
- Phase 2: Creating NetWare/IP gateways to connect remote sites
- Phase 3. Adding NetWare/IP to existing IPX NetWare file servers
- Phase 4: Creating an *all* NetWare/IP network (no IPX)

Each phase can be completely transparent to the end-users. Customers can choose to implement all four phases, or they may stop after any phase, depending on their particular IP requirements.

Note: NetWare/IP clients can be added any time after Phase 1. However, it is recommended that IPX

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

clients *not* be migrated to NetWare/IP until all local NetWare servers are migrated to NetWare/IP (completion of Phase 3).

Phase 1: Installing NetWare/IP and creating the Primary DSS. DNS allows partitioning of the DNS tree into DNS subdomains. Before installing NetWare/IP, you should determine a suitable location within the DNS hierarchy for the NetWare/IP DSS domain so that it is most accessible to your NetWare/IP users.

During the configuration of the primary DSS, an IPX Network number is assigned to the NetWare/IP configuration. This creates a "virtual" IPX segment of all NetWare/IP services and routes. This IPX address *must be* unique within your network.

Since NetWare/IP collects all services and routes and places these routes into a single DSS database, NetWare/IP is more sensitive to IPX address conflicts than are pure IPX networks. Address conflicts can cause service and route visibility problems. To prevent routing conflicts, it is strongly recommended that an IPX naming standard be adopted to ensure unique internal IPX and segment addresses.

Phase 2: Creating NetWare/IP gateways. NetWare/IP is often used to connect IPX sites via an IP WAN link. In this configuration, one (or occasionally more than one) NetWare/IP gateway is located at each IPX site and is connected to the IP WAN segment.

All IPX traffic destined for a location connected via IP must be routed through the NetWare/IP gateway. When communicating across the IP WAN, IPX clients send packets to the local NetWare/IP gateway. The gateway converts the IPX packets to IP packets. The IP packets are then routed to the other NetWare/IP gateway via IP routers. The NetWare/IP gateway at the receiving end converts the packets back to IPX and they are sent, via IPX, to the destination node.

The NetWare/IP gateway will place an additional load on the server. Therefore, it is recommended that a lightly loaded server function as the NetWare/IP gateway. If the IPX site is large (100 or more clients, 10 or more servers) and WAN traffic is expected to be moderate to heavy, consider dedicating multiple gateways per site. Each site should have no more than two NetWare/IP-IPX forwarding gateways, which will provide load balancing as well as fault tolerance.

Phase 3: Adding NetWare/IP to existing IPX NetWare file servers. When communicating between remote sites, installing NetWare/IP on all servers will improve overall network efficiency and reduce the processing load on NetWare/IP gateways.

For example, on an IPX network where one or two servers are designated as NetWare/IP gateways, IPX clients or NetWare servers using only IPX must send IPX packets to a local gateway. The gateway converts the IPX packets to IP and then routes them directly to the destination NetWare/IP server. However, when NetWare/IP is installed on the destination server, the server can accept the incoming IP packet. No packet conversion is required, and the need for an additional gateway is eliminated.

Note: NetWare Directory Services synchronization between NetWare/IP servers occurs without any assistance whatsoever from the gateway.

By adding NetWare/IP to all existing IPX file servers, communication via IP becomes more efficient than passing all traffic through the gateway. However, NetWare/IP servers that also have IPX configured will broadcast SAP/RIP information to the IPX segments. Large customer sites (those with more than 500 NetWare file servers) need to plan accordingly for additional local-segment SAP and RIP traffic.

Phase 4: Creating an all NetWare/IP network (no IPX). NetWare/IP is designed to support an IP-only configuration in which an entire NetWare environment can be deployed without using IPX at all. In this configuration, all servers and clients are migrated to NetWare/IP. IPX may be removed from those segments where IPX is no longer needed.

Some corporations have implemented an "IP only" policy for all or portions of their networks. In some cases, people are under the mistaken impression that TCP/IP is a "savior" that will resolve all bandwidth

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

and routing problems. IP address management and proper IP subnetting of the segments are complex issues, and corporations usually have personnel dedicated solely to these tasks.

Conversely, IPX is often cited as a poor WAN protocol due to SAP/RIP broadcast storms and the "chatty" nature of the NetWare Core Protocol (NCP). A new routing protocol called NetWare Link Services Protocol (NLSP) is now available to eliminate SAP and RIP from IPX networks, providing a much more scalable IPX WAN solution. (NLSP is very similar to Open Shortest Path First for IP). Packet Burst and Large Internet Packets (LIP) eliminate the chattiness of NCP and provide extremely efficient use of available network bandwidth. These solutions should be considered before choosing TCP/IP as a replacement to IPX in the corporate environment.

In Novell's experience, most customers choose not to eliminate IPX from their network because the additional burden of administering IP addresses on clients far exceeds any gains of using IP on the local LAN segments. Also, most vendors of IPX embedded devices (IPX printers, modem sharing devices, and so on) have not released NetWare/IP-compatible firmware upgrades. This precludes the elimination of IPX from LAN segments.

Implementation Case Studies

How are Novell customers implementing NetWare/IP? Most customers implement a Phase 3 configuration because it eliminates SAP and RIP broadcasts and creates an IP-only WAN without changing client configuration. Typically, customers choose to place NetWare/IP on SAA gateways, e-mail servers, database servers, or the like. In addition to creating gateways, they also install NetWare/IP on critical NetWare servers throughout the company, providing more efficient IPX-to-IP communication for IPX clients.

This section presents some typical NetWare/IP integration scenarios based on "real world" projects completed by the Novell Consulting Services team. The first case study provides great detail of the NetWare/IP configuration of a typical customer. The other two case studies give a more general overview of the suggested implementation.

Case 1: Three Main Offices

Consider the network of ABC Inc. Employees are located at three main geographical locations in Los Angeles, California; Provo, Utah; and Tampa, Florida. Each site communicates to the two other sites across 56 Kbps WAN links. IPX and IP are currently routed across the WAN, but the company wants to convert the entire network to a single protocol, namely TCP/IP.

At each site there are approximately 500 users sharing four file servers. The four servers at each site share a common high-speed backbone with two routers. One router connects the high-speed server backbone to the other remote sites. A second router connects the high- speed server backbone to several Ethernet segments where the client workstations are located. For simplicity, the servers are named to reflect their geographical location (for instance, PRV_1, PRV_2, LA_3, TAMPA_2, and so on).

This project has two milestones first, migrating from an IPX WAN to an IP WAN; and second, migrating all IPX clients to NetWare/IP. Following are the steps necessary to successfully implement NetWare/IP in this environment.

Phase 1: Installing the Primary DSS and configuring the NetWare/IP domain

Since IS expertise resides in Provo, the NetWare/IP primary DSS will be located on one of the four existing servers at the Provo site. With only four file servers and perhaps ten IPX printers at each site, the number of SAP/RIP entries in the DSS database is relatively small. Therefore, the DSS.NLM can be located on an existing server in Provo without impacting the server's response time to local clients. Server PRV_1 is chosen for the role of the Primary DSS.

A DNS structure is already in place reflecting the geographical locations of the company

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

(provo.abc.com, tampa.abc.com, la.abc.com). A NetWare/IP DNS subdomain is chosen as nwip.abc.com.

DSS Configuration for PRV_1. The NetWare/IP 2.1 product is installed on server PRV_1. During the installation, the following parameters are chosen during the DSS configuration:

```
NetWare/IP Domain      ³nwip.abc.com
Name                   ³
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Primary DSS host       ³prv_1.provo.abc.com
name                   ³
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
IPX network number     ³13131313
```

NWIP Configuration for PRV_1. In addition to providing DSS services, this server will also load NWIP.NLM. The following parameters are chosen during the NWIP.NLM configuration:

```
NetWare/IP Domain      ³nwip.abc.com
Name                   ³
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Preferred DSS          ³prv_1.provo.abc.com (or its IP
                       ³address)
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Forward IPX to DSS?    ³Yes
```

Since only one DSS exists, the preferred DSS list is pretty simple. However, as more NetWare servers are configured as secondary DSSes, additional Preferred DSS entries could be entered to provide additional fault tolerance for when the first preferred DSS is unavailable.

DNS Information. DNS already exists on a non-NetWare platform and it won't be duplicated on a NetWare server. However, the existing DNS structure must be modified to include information about the NetWare/IP domain. The DNS administrator is contacted and a new name server ("NS" record) is entered in DNS:

```
nwip.abc.com      in     ns    prv_1.provo.abc.com
```

This NS record registers the DSS with DNS, permitting any NetWare/IP server or client to query DNS and locate PRV_1 as the DSS of the NetWare/IP domain. If it doesn't already exist in DNS, the DNS administrator must add an address entry ("A" record) in DNS for prv_1.provo.abc.com. The A record permits any server or client to resolve the host name "prv_1.provo.abc.com" to the corresponding IP address.

Phase 1 is now complete. IPX clients could be converted to NetWare/IP at this time, but it is recommended that customers wait until after Phase 3 is completed.

Phase 2: Installing NetWare/IP in the Tampa and Los Angeles sites

The ultimate goal of this NetWare/IP implementation is to extend NetWare/IP to every server and client at every geographical site. Since there will eventually be many "consumers" of DSS information at every geographical site, at least one additional secondary DSS will be placed at every site. Servers TAMPA_1 and LA_1 are arbitrarily chosen as secondary DSSes.

DSS Configuration for TAMPA_1. On TAMPA_1, NetWare/IP 2.1 is installed and configured as a

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

NetWare/IP server and a secondary DSS. The following parameters are chosen during the configuration of DSS:

```
NetWare/IP Domain Name ³nwip.abc.com
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Primary DSS            ³prv_1.provo.abc.com (or its IP
                       ³address)
```

NWIP Configuration for TAMPA_1. The following parameters are chosen during the configuration of NWIP.NLM:

```
NetWare/IP Domain Name ³nwip.abc.com
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Preferred DSS          ³tampa_1.tampa.abc.com  (or its IP
                       ³address)
                       ³prv_1.provo.abc.com  (or its IP
                       ³address)
                       ³la_1.la.abc.com  (or its IP
                       ³address)
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Forward IPX to DSS?    ³Yes
```

Note that the first preferred DSS is the server's local DSS. If this DSS is unavailable, TAMPA_1 will attempt to contact PRV_1 and then LA_1 for DSS information.

DSS Configuration for LA_1. On LA_1, NetWare/IP 2.1 is installed and configured as a NetWare/IP server and a secondary DSS. The following parameters are chosen during the configuration of DSS:

```
NetWare/IP Domain Name ³nwip.abc.com
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Primary DSS            ³prv_1.provo.abc.com (or its IP
                       ³address)
```

```
NetWare/IP Domain Name        ³nwip.abc.com
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Preferred DSS                 ³la_1.la.abc.com  (or its IP address)
                              ³tampa_1.tampa.abc.com  (or its IP
                              ³address)
                              ³prv_1.provo.abc.com  (or its IP
                              ³address)
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Forward IPX to DSS?           ³Yes
```

NWIP Configuration for LA_1. The following parameters are chosen during the configuration of NWIP.NLM:

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

Phase 2 is now complete. At this point IPX can be removed from the WAN. Servers PRV_1, TAMPA_1, and LA_1 are NetWare/IP-to-IPX gateways, joining the local IPX segments together across an IP-only WAN. The resulting implementation is illustrated in Figure 1.

Figure 1: Implementing NetWare/IP in a scenario with three main offices.

<Graphic Not Available>

With IPX eliminated from the WAN, all communication between sites must be routed through the NetWare/IP gateways (PRV_1, TAMPA_1, and LA_1). For example, if server TAMPA_3 needs to synchronize DNS information with server LA_4, TAMPA_3 first sends an IPX packet to TAMPA_1 where it is converted to an IP UDP packet. TAMPA_1 sends this UDP packet to LA_1, which converts the packet back to IPX and sends it to LA_4. Likewise, if an IPX client in Provo wants to log in to the LA_4 file server, PRV_1 and LA_1 must act as intermediate IP-to-IPX gateways.

One obvious question arises in this scenario: If all IPX traffic between sites must be routed through the NetWare/IP-IPX gateways, will performance between sites suffer? Generally, performance will not suffer because overall performance is limited to the slowest link namely, the speed of the WAN itself. From real-world experience, there isn't a noticeable performance decrease for WAN speeds from 56 Kbps up to 1.54 Mbps. In fact, many customers actually experience a performance *increase* over the WAN after eliminating IPX's periodic SAP/RIP updates with NetWare/IP.

Phase 3: Implementing NetWare/IP on all NetWare servers

Phase 3 improves the performance and efficiency of communication between sites by configuring every server with NetWare/IP. This reduces the dependency on the NetWare/IP - IPX gateways.

At each geographical location, NetWare/IP is installed on the remaining servers. The remaining servers are configured to use their local DSS first, and DSSes at remote sites if their local DSS is unavailable. For example, consider the NWIP configuration of LA_3:

```
NetWare/IP Domain Name          ³nwip.abc.com
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Preferred DSS                   ³la_1.la.abc.com  (or its IP
                                ³address)
                                ³tampa_1.tampa.abc.com  (or its IP
                                ³address)
                                ³prv_1.provo.abc.com  (or its IP
                                ³address)
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Forward IPX to DSS?             ³No
```

Successful completion of Phase 3 provides more efficient communication between sites. Consider the prior example: If TAMPA_3 needs to synchronize DNS information with LA_4, TAMPA_3 sends a UDP packet directly to LA_4. Neither IPX-IP gateway in Tampa or Los Angeles is required. Likewise, if an IPX client in Provo wants to log in to the LA_4 file server, only PRV_1 must act as an intermediate IP-IPX gateway.

Many customers stop their NetWare/IP implementation after the completion of Phase 3. Implementing NetWare/IP through Phase 3 provides the benefits of an extremely efficient IP-only WAN backbone, while retaining the simplicity of IPX on the local segments.

Phase 4: Removing IPX from local segments

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

Before IPX can be removed from local segments, all devices on the segment should be converted from IPX to an IP-based solution. For those segments with only IPX workstations, simply upgrade the IPX client to the corresponding NetWare/IP requester. Novell provides NetWare/IP requesters for DOS/Windows 3.1, Windows NT, and Windows 95. OS/2 Warp and Macintosh support is forthcoming.

Segments that include embedded IPX devices, such as fax servers and printers that have built-in IPX LAN cards, need special consideration. Some embedded IPX devices support IP natively, while others do not. Many customers find that due to embedded IPX devices, it is not possible to completely eliminate IPX from all network segments. However, if feasible, these embedded IPX devices may be consolidated onto a single IPX segment.

Most common of all embedded IPX devices are IPX printers. Many of these printers can be converted from IPX to LPR-LPD, an IP-only printing solution. However, this requires additional software and configuration above and beyond traditional NetWare printing. Other embedded IPX printers may be connected to an NPRINTER workstation, which would communicate to the NetWare server via NetWare/IP.

Once all IPX devices are removed from local segments, you can simply remove IPX from the corresponding servers and routers.

Case 2: Single Office with Many Remote Sites

Consider another typical NetWare/IP customer that has one large central office with 60 remote offices. The central office is a terminating point for leased-lines, or a fast entry point into a frame relay circuit that connects the remote offices to the central office. Several hundred users at the central office share a few NetWare 4.1 servers, connecting via IPX.

Each of the 60 remote offices is connected to the main office by either a 56 Kbps or 256 Kbps WAN circuit. Within each remote office is a single NetWare 4.1 server, which is shared among the remote office's 50 users. Remote users occasionally transfer files and send E-mail to the central office.

NetWare/IP has been selected to join these remote offices to the central office by converting their existing IPX WAN to NetWare/IP. However, NetWare/IP will not be implemented at the clients' desktops.

To achieve an IP-only WAN, NetWare/IP will be implemented on all of the central office's servers and each of the 60 servers in the remote offices. Because none of the clients will be migrated to NetWare/IP, there is no need to provide DSSes at each of the remote sites. Therefore, there are 70 consumers of DSS information 60 remote servers and 10 servers in the central office.

One existing, lightly loaded file server in the central office is designated as the primary DSS. Two other existing central office servers are configured as secondary DSSes to provide load balancing and fault tolerance of DSS services.

In DNS, create name server (NS) records for the two secondary DSSes. Registering these secondary DSSes in DNS permits clients to query DNS to locate a secondary DSS.

NetWare/IP is installed on every NetWare server in the central office and at each remote site (see Figure 2).

Figure 2: Implementing NetWare/IP in a scenario with a single central office and many remote sites.

<Graphic Not Available>

The Preferred DSS list of the NetWare/IP server is configured such that the load is equally distributed across the two secondary DSSes, and the primary DSS is used only if neither secondary DSS is available.

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

For example, assume that the Primary DSS was FS1_PDSS and the two secondary DSSes were FS2_SDSS and FS3_SDSS. For half of the NetWare/IP servers, the Preferred DSS NetWare/IP configuration list would look similar to this:

Preferred DSS	fs2_sdss.central_office.abc.com fs3_sdss.central_office.abc.com fs1_pdss.central_office.abc.com

The other half of the NetWare/IP servers would have a Preferred DSS NetWare/IP configuration list similar to this:

Preferred DSS	fs3_sdss.central_office.abc.com fs2_sdss.central_office.abc.com fs1_pdss.central_office.abc.com

Case 3: Medium-sized Remote Site of IPX Users with IP WAN Link

This scenario is very similar to the previous example where many remote sites are connected to a central office by an IP-only WAN. However, in this scenario, consider the needs of a remote office that has ten NetWare 4.1 file servers. IPX clients in this office attach to the local NetWare file servers for all applications and data, and only occasionally log in to a server in the main office to access data. The NetWare file servers also contact other servers in the main office for occasional e-mail transfer. The speed of the WAN link from this site to the main office is T1 (1.54 Mbps).

The solution for this case is to load NetWare/IP on one or more file servers in the remote office, depending on the anticipated need of the remote office to contact the central office. Loading NetWare/IP on all of the servers in this remote office permits server-to-server communication without the need for intermediary NetWare/IP-IPX gateways. Bind IPX on every file server to allow local IPX clients direct access to the server via IPX, without passing through a gateway (see Figure 3).

Figure 3: Implementing NetWare/IP in a medium- sized remote site scenario.

<Graphic Not Available>

Since every server at the remote site uses DSS services, it is important to provide DSS services locally. Configure one server as a secondary DSS, and configure all NetWare/IP servers to use their local secondary DSS as the preferred DSS and other secondary DSSes in the central office if their local preferred DSS is unavailable. Don't register this DSS with DNS, as it may be undesirable for NetWare/IP clients to connect across the WAN to this DSS.

Tips, Tricks, and Suggestions

Many factors influence the design of a NetWare/IP migration and roll-out. Listed below are some considerations and tips that will help in the design of your NetWare/IP environment. These tips, suggestions, considerations, and "gotchas" are based on experiences of Novell Consulting Services.

DNS

Create a single NetWare/IP domain.

Although it is possible to create many NetWare/IP domains, NetWare servers and clients can only belong to a one NetWare/IP domain at any one time. The information supplied by SAP and RIP is contained within a single NetWare/IP domain. Services located outside of this NetWare/IP domain are not available to servers

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

and clients within the domain.

Use existing DNS services.

While NetWare/IP can supply both master and replica DNS services through the NAMED.NLM supplied with the product, we recommend that you use existing DNS services. (For more information regarding DNS configuration on non-NetWare servers, see "Creating DNS Database Records on a Non-NetWare Master DNS Server" in the *NetWare/IP Administrator's Guide*.)

Provide reliable DNS services.

To establish a connection, NetWare/IP 1.1 servers and clients require access to DNS. Ensure that timely DNS access is available throughout the network. Since DNS is a single point of failure within NetWare/IP, you'll need to plan accordingly. Create read-only replicas of the DNS database on other servers to provide load balancing and redundancy.

Note: NetWare/IP 2.1 servers and clients do not require full-time access to DNS to initialize. NetWare/IP 2.1 servers and client only use DNS when other mechanisms to locate DSS fail.

Limit the number of registered DSS servers in a NetWare/IP domain.

Because of a deficiency in most DNS implementations, a reply to a DNS query cannot exceed 1.5KB in size. This limits the number of registered DSSes to under 20. If there are more name servers than a DNS packet can accommodate, all name server entries may not be returned in response to an NS query. You can bypass this deficiency by using unregistered DSS servers. When you use unregistered DSSes, there should still be at least one registered DSS in each major region. This will provide fault tolerance for the NetWare/IP node if the link to the unregistered DSS is down.

DSS

Provide reliable DSS services.

NetWare/IP servers and clients require access to the DSS to initialize. Ensure that DSS access is available to all NetWare/IP servers and clients. If IP router service is unreliable, place a secondary DSS on each separate subnetwork cabling system where NetWare/IP servers or clients reside.

Always have a reliable primary DSS.

The primary DSS plays a special role within the NetWare/IP domain namely, keeping the secondary DSSes synchronized. Ensure that the primary DSS is located on a very reliable and highly accessible NetWare server. If the primary DSS becomes unavailable, each secondary DSS will "freeze" its image of the DSS domain. Secondary DSSes will continue to add and delete records as reported by NetWare/IP servers, but one secondary DSS will not learn of changes occurring within the DSS domain if the changes are reported to another secondary DSS.

Consider dedicating a NetWare server as the primary DSS.

As the number of secondary DSSes increases within the NetWare/IP domain, the load on the primary DSS also increases. It may be necessary or advantageous to dedicate a NetWare server to function as the primary DSS. Use a server with a NetWare speed rating of at least 900 (486/33 CPU or better) and at least 16 MB of memory.

Configure NetWare/IP servers and clients to communicate with secondary DSSes only.

To provide the best possible scalability in a NetWare/IP network, reserve the processing power of the primary DSS for synchronizing secondary DSSes. To do this, configure NetWare/IP servers and clients to communicate with secondary DSSes only. Only secondary DSSes should communicate with the primary DSS.

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

Provide sufficient memory and disk space for the DSS.

You should allocate at least 1 MB of free disk space on the SYS volume of the DSS server. Use the following formulas to determine the memory requirements for the DSS server, where *n* is the number of NetWare/IP servers in the network:

NetWare v3.11 or v3.12
(*n* 440) + 450,000 = memory needed on the server, in bytes

NetWare 4.x
(*n* 440) + 750,000 = memory needed on the server, in bytes

Provide a unique IPX segment address for the NetWare/IP domain.

During the configuration of the primary DSS, an IPX segment address is assigned to the NetWare/IP domain. Ensure that this segment address is unique to the NetWare/IP domain only, and that it is not duplicated as a server's internal IPX address or an IPX cabling segment address.

Configure NetWare/IP nodes to use unregistered DSS.

An administrator can use unregistered DSSes to designate exactly which DSS servers a NetWare/IP node should use. This gives the administrator better control over DSS server utilization and load balancing.

Don't enable UDP checksums for the NetWare/IP domain.

Enabling UDP checksums in the Primary DSS configuration will decrease performance for all clients in the NetWare/IP domain. Ethernet and Token Ring adapters in the client are already checking for corruption, so UDP checksums are redundant.

Load DSS.NLM with the "/STAT" option to gather information about DSS.

Loading DSS.NLM with the "/STAT" option will display additional information about the local DSS services, including the DSS version (of the DSS domain information), the type of DSS (either Primary or Secondary), and the number of SAP and RIP records in the DSS database.

Use MONITOR.NLM to determine the load of DSS on the file server.

MONITOR can display the processor load of each process or task executing on the file server. Highlight the "Processor Utilization" option under MONITOR (in NetWare 3.x, enable this by loading MONITOR with the undocumented "-P" option), press <Enter>, and then press <F3>. This builds a list of all processes and tasks currently executing on the file server. Locate processes by the name "DSS". The "% LOAD" measurement should give a good indication of the load that DSS is placing on the server.

Configure lightly loaded DSSes as non-dedicated DSSes.

By default, DSS.NLM will consume as much CPU time as necessary to ensure DSS processing. If a secondary DSS is lightly loaded (meaning that fewer than 20 NetWare/IP servers use the DSS), consider configuring the DSS as a non-dedicated DSS, thereby ensuring that DSS.NLM will not "hog" CPU cycles. To configure the DSS as non-dedicated, edit the SYS:ETC\ NWPARAMS file, and set DEDICATED_DSS to 0 in the DSS configuration section.

Increase UDP buffers and TCP connections for large DSS servers.

If a DSS provides services to more than 60 DSS "clients," consider increasing the UDP buffers and TCP connections to ensure that all DSS clients are properly serviced. For example, if a large NetWare/IP environment contains 100 secondary DSSes that must communicate to a single primary DSS, or if a single secondary DSS services 100 or more NetWare/IP servers, it may be necessary to increase the maximum UDP buffers and TCP connections. Edit the SYS:ETC\NWPARAMS file and increase the MAX_UDP_PKTS

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

and MAX_TCP_CONNS parameters in the DSS configuration section. (See the README.TXT file on the NetWare/IP 2.1 installation disk #1 for more details.)

NetWare/IP Server

Here's a troubleshooting tip for NetWare/IP server installation. During the installation of the first NetWare/IP server, you will receive the message "FATAL -- Unable to get NetWare/IP global parameters from any DSS. NWIP.NLM cannot load." This message is returned whenever NWIP.NLM cannot locate a DSS for the NetWare/IP domain parameters. This message will always appear during the first NetWare/IP server install since a DSS is not yet configured. Use UNICON to configure the primary DSS and reload the NWIP.NLM.

Avoid placing DNS, DSS, and NetWare/IP on a single server if high NetWare/IP utilization is expected.

DNS, DSS, and NetWare/IP each require CPU cycles, and therefore reduce the processing power available for other services (file, print, and so on). If possible, distribute the workload of DNS, DSS, and NetWare/IP across multiple servers. If a single server will provide all three services for a network segment, consider moving critical file and print services to another NetWare server.

Allocate sufficient resources for NetWare/IP servers.

NetWare/IP requires at least 2MB of disk space on volume SYS, and sufficient server memory. Memory requirements for a NetWare/IP server can be calculated from the following formula, where *n* is the number of NetWare/IP servers in the NetWare/IP domain:

(*n* 380) + 75,000 = memory needed on the server, in bytes

Configure NetWare/IP servers to choose the best DSS.

NetWare/IP servers should be configured to attempt communication to at least two DSSes during initialization. Use UNICON to enter the closest DSS's host name or IP address in the "Preferred DSS #1" field, and select up to four additional DSSes to contact during initialization if Preferred DSS #1 is unavailable. Valid entries include the host name, IP address, or a network address (for example, any DSS on network 137.65.43.0).

Consider dedicating a NIC for IP traffic on NetWare/IP gateways.

If a NetWare/IP gateway provides IP access to many IPX clients, consider dedicating a NIC (network adapter) for IP traffic. Distributing the gateway's load across multiple NICs will increase the performance of IP services to IPX clients.

Minimize the number of NetWare/IP gateways per IPX segment.

IPX segments may use multiple NetWare/IP gateways to provide load balancing and fault tolerance. Each NetWare/IP gateway will broadcast all SAP and RIP information known to the NetWare/IP domain to all locally connected IPX segments. As NetWare/IP gateways are added to an IPX segment, the SAP and RIP traffic on the IPX segment increases. Minimize the number of NetWare/IP gateways per IPX segment to reduce SAP/RIP broadcasts on the IPX segments. The NetWare/IP gateway functionality also adds processing overhead to the file server. Therefore, choose file servers with sufficient hardware resources that can handle the additional load of the NetWare/IP gateway.

To minimize the number of broadcast SAPs and RIPs placed on local IPX segment by NetWare/IP-IPX gateways, disable the server's internal routing by loading "IPXRTR routing=none" on the NetWare/IP-IPX gateway. This will prevent the NetWare/IP server from advertising SAPs and RIPs from the DSS database to the local IPX segment, reducing the overall number of SAP and RIP broadcasts on the local IPX segment. Note that at least one NetWare/IP - IPX gateway must have routing enabled to propagate the SAP and RIP information from DSS.

Use NetWare/IP gateways to provide IPX services to IPX-embedded devices (as needed).

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

Since NetWare/IP is a relatively new product, many vendors haven't included native support for NetWare/IP. Common examples include IPX-embedded printers, FAX servers, and so on. If you have devices that do not yet support NetWare/IP on your network, use a NetWare/IP gateway to provide IPX services to those devices.

Load IPXRTR on NetWare/IP servers that also have IPX loaded.

Loading IPXRTR on NetWare/IP servers that also have IPX loaded will result in more efficient synchronization between NetWare/IP servers and DSS, reducing the frequency and number of packets required to report local IPX SAP/RIP information to the DSS.

Use MONITOR.NLM's LAN/WAN statistics or load NWIP.NLM with the /STAT option to gather information about the current NetWare/IP configuration.

MONITOR displays numerous LAN/WAN statistics that are helpful in gathering configuration information. Also, loading NWIP.NLM with the "/STAT" option will display information about the current version of SAP/RIP information, the DSS that the NetWare/IP server is exchanging SAP/RIP information with, whether or not the server is a NetWare/IP gateway, and the number of errors experienced when sending or receiving changes from the DSS.

Use MONITOR.NLM to determine the load of NWIP on the file server.

MONITOR can display the processor load of each process or task executing on the file server. Highlight the "Processor Utilization" option under MONITOR (enable this in NetWare 3.x by loading MONITOR with the undocumented "-P" option), press <Enter>, and then <F3>. This will build a list of all processes and tasks currently executing on the file server. Locate processes by the name "NWIP". The "% LOAD" measurement should give a good indication of the load that NWIP is placing on the server.

NetWare/IP Client

Use the VLM client software to connect to NetWare servers.

NetWare/IP servers and clients are compatible with Packet Burst, Large Internet Packets (LIP), and the enhanced security features of NetWare 3.12 and 4.x. Use the NetWare DOS Requester (VLM) for DOS/Windows clients to gain the performance and security advantages of these features.

Use TCPIP.EXE dated 10-10-94 or later.

In very isolated circumstances, versions of TCPIP.EXE dated prior to 10-10-94 could result in data corruption on NetWare/IP clients using parallel tasking Ethernet cards in a Windows environment with Packet Burst. As of this writing, TCPIP.EXE can be found in the LWP42T.EXE file located in NWGENFILES Library 02 on NetWire.

Use a memory manager to load TCPIP.EXE and NWIP.EXE into upper memory blocks.

TCPIP.EXE and NWIP.EXE require approximately 28 KB more workstation memory that IPXODI alone. Both modules can be loaded into upper memory blocks to conserve conventional memory.

Configure NetWare/IP clients to use the PREFERRED DSS and NEAREST_NWIP_SERVER parameters.

To prevent possible delays during client initialization, use the PREFERRED DSS and NEAREST_NWIP_SERVER parameters in the NWIP configuration section of the client's NET.CFG file. The PREFERRED DSS statement directs the client to particular DSS, while the NEAREST_NWIP_SERVER directs the client to a preferred NetWare/IP server. You may specify a host name, a host IP address, or a subnetwork address. For example, assume that the following parameters were set in the client's NET.CFG file:

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

```
NWIP
      PREFERRED DSS nwiptemp.ipdemo.com 137.65.43.0
      NEAREST_NWIP_SERVER nwiptemp.ipdemo.com
       137.65.43.91 137.65.43.0
```

This client configuration would use `nwiptemp.ipdemo.com` as the first choice for a DSS; otherwise, any DSS on the subnetwork 137.65.43.0 will be used. Requests for the nearest NetWare/IP server are handled in a similar fashion. This client would choose `nwiptemp.ipdemo.com` first, 137.65.43.91 second, and then any NetWare/IP server on the subnetwork of 137.65.43.0. (See the example traces at the end of this AppNote for more information.)

Use RFCNBIOS to provide NetBIOS emulation to NetWare/IP clients.

NetWare/IP supports IPX NetBIOS only on local subnetworks: IPX NetBIOS broadcasts are not routed across IP routers. If NetBIOS capability is required over NetWare/IP, replace the NetWare NetBIOS emulator (NETBIOS.EXE) with RFCNBIOS.EXE provided with the NetWare/IP software.

Load NWIP.EXE with the "/V" option for verbose information about NetWare/IP.

Loading NWIP.EXE with the "/V" option will display IP address information while the NetWare/IP client contacts DNS, DSS, and a NetWare/IP server. This information may be helpful when troubleshooting a client connection problem.

Sample Traces

The following pages contain LANalyzer for Windows traces and packet-by-packet explanations of the data transfers.

Note: Novell Consulting Services recommends that NetWare/IP customers use LANalyzer for Windows in NetWare/IP environments because it will correctly decode the NCP information in the NetWare/IP packet. Other protocol analyzers can use "protocol forcing" to decode UDP packets as NCP, but often the fields are decoded incorrectly.

NetWare/IP Client Connecting to a NetWare/IP Server

The first trace illustrates the exchange of packets when a NetWare/IP client connects to a NetWare/IP server. Following is a list of IP addresses and other background information to help you understand the trace.

DNS: 137.65.96.89
DNS Domain: ipdemo.com
NetWare/IP Domain: nwip.ipdemo.com
NetWare/IP IPX Network Number: 13131313
Primary DSS: 137.65.96.89 (nwipdemo.ipdemo.com)
Preferred DSS: 137.65.96.89 (nwipdemo.ipdemo.com)
NEAREST_NWIP_SERVER: 137.65.96.89 (nwipdemo.ipdemo.com)
Client's address: 137.65.96.92

The first packet is generated when TCPIP.EXE loads at the client.

Packet Number 1: The client ARPs for its IP address to ensure that it is unique and not used by another node on the network.

```
Length : 64 bytes
ether: ==================== Ethernet Datalink Layer ====================
      Station: 00-00-1B-1E-74-BA ----> Broadcast
```

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

```
      Type: 0x0806 (ARP)
arp: ================== Address Resolution Protocol ==================
      Hardware: Ethernet
      Protocol: 0x0800 (IP)
      Operation: ARP Request
      Hardware adress length: 6
      Protocol address length: 4
      Sender Hardware Address: 00-00-1B-1E-74-BA
      Sender Protocol Address: 0.0.0.0
      Target Hardware Address: 00-00-00-00-00-00
      Target Protocol Address: 137.65.96.92
```

Packet Number 2: NWIP.EXE loads. The client reads its NET.CFG, locates the PREFERRED DSS (137.65.96.89), and ARPs to resolve the IP address.

```
Length : 64 bytes
ether: ==================== Ethernet Datalink Layer ====================
      Station: 00-00-1B-1E-74-BA ----> Broadcast
      Type: 0x0806 (ARP)
arp: ================== Address Resolution Protocol ==================
      Hardware: Ethernet
      Protocol: 0x0800 (IP)
      Operation: ARP Request
      Hardware adress length: 6
      Protocol address length: 4
      Sender Hardware Address: 00-00-1B-1E-74-BA
      Sender Protocol Address: 137.65.96.92
      Target Hardware Address: 00-00-00-00-00-00
      Target Protocol Address: 137.65.96.89
```

Packet Number 3: The ARP is successful. The client now has the MAC address of the DSS.

```
Length : 64 bytes
  arp: ================== Address Resolution Protocol ==================
      Hardware: Ethernet
      Protocol: 0x0800 (IP)
      Operation: ARP Reply
      Hardware adress length: 6
      Protocol address length: 4
      Sender Hardware Address: 00-20-AF-51-6C-3C
      Sender Protocol Address: 137.65.96.89
      Target Hardware Address: 00-00-1B-1E-74-BA
      Target Protocol Address: 137.65.96.92
```

Packet Number 4: The client verifies that the DSS is valid by requesting a Start Of Authority (SOA) record for the NWIP DNS domain. This ensures that DSS.NLM is loaded and functioning.

```
Length : 80 bytes
   ip: ======================== Internet Protocol ========================
      Station:137.65.96.92 ---->137.65.96.89
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 61
```

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

```
      Identification:     1
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 60  seconds
      Checksum: 0xAB77(Valid)
  udp: ===================== User Datagram Protocol ====================
      Source Port: 1025
      Destination Port: DOMAIN
      Length = 41
      Checksum: 0x4719(Valid)
  dns: ====================== Domain Name Service ======================
      Header:
            ID: 1
            Op Code: 0 (Standard Query)
            Flags: 0x0100 (Recursion Desired)
            Question Count: 1
            Answer Count: 0
            Authority Record Count: 0
            Additional Count: 0
      Questions:
            Domain Name: NWIP.IPDEMO.COM
            Type: 6 (Start of a Zone of Authority)
            Class: 1 (Internet)
```

Packet Number 5: DSS responds to the client's SOA request, indicating that the DSS is available and functioning.

```
Length : 142 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.92
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 123
      Identification: 25191
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 128 seconds
      Checksum: 0x04D3(Valid)
  udp: ===================== User Datagram Protocol ====================
      Source Port: DOMAIN
      Destination Port: 1025
      Length = 103
      Checksum: 0x7FCA(Valid)
  dns: ====================== Domain Name Service ======================
      Header:
             ID: 1
            Op Code: 0 (Standard Query)
            Response Code: 0 (No Error)
            Flags: 0x8580 (Response, Authoritative Answer,
                  Recursion Desired, Recursion Available)
            Question Count: 0
            Answer Count: 1
            Authority Record Count: 0
            Additional Count: 0
       Answers:
```

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

```
            Domain Name: NWIP.IPDEMO.COM
            Type: 6 (Start of a Zone of Authority)
            Class: 1 (Internet)
            Time to Live: 0
            Data Length: 56
            Name Server: nwipdemo.ipdemo.com
            Mailbox of Responsible Person: THE-NWIP-GURU
            Serial Number of Zone Info: 14654
            Refresh Interval: 300
            Failed Refresh Retry Interval: 300
            Max Expiration Interval: 1499480457
            Minimum Time to Live: 1
```

Packet Number 6: The client requests the NetWare/IP domain parameters from DSS.

```
Length : 64 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.92 ---->137.65.96.89
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 32
      Identification:     2
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 60  seconds
      Checksum: 0xAB93(Valid)
  udp: ===================== User Datagram Protocol ====================
      Source Port: 1026
      Destination Port: 396
      Length = 12
      Checksum: 0x2604(Valid)
nwipu: ========================== NetWare/IP ==========================
      Packet Type: 12 (Request NWIP Parameters)
      Sequence Number: 256
```

Packet Number 7: DSS responds with the current NetWare/IP parameters.

```
Length : 70 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.89 ---->137.65.96.92
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 52
      Identification: 25192
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 128 seconds
      Checksum: 0x0519(Valid)
   udp: ===================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 1026
```

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

```
      Length = 32
      Checksum: 0x0000(checksum not used)
nwipu: ============================ NetWare/IP ============================
      Packet Type: 13 (Response NWIP Parameters)
      Sequence Number: 256
      IPX Network Number String: 0101030c
      IPX Network Number: 0x101030C
      NetWare/IP Port Number: 43981
      Checksum Usage Flag: 0 (No)
      DB Sync. Interval (secs): 300
      Max. UDP Retransmissions: 3
```

Packet Number 8: VLM.EXE loads. Since NSQ_BROADCAST is set ON in the client's NET.CFG, the client broadcasts an IP UDP Nearest Server query to the local IP subnet. Any NWIP server on this subnet should respond, unless it server has "Reply to Get Nearest Server" set to OFF. The VLM client is looking for SAP type 0x0278 (632 decimal), which corresponds to NetWare Directory Services.

```
Length : 70 bytes
ether: ==================== Ethernet Datalink Layer ====================
      Station: 00-00-1B-1E-74-BA ----> Broadcast
      Type: 0x0800 (IP)
   ip: ======================== Internet Protocol ========================
      Station:137.65.96.92 ---->255.255.255.255
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 52
      Identification:     3
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 60  seconds
      Checksum: 0x9519(Valid)
  udp: ====================== User Datagram Protocol ======================
      Source Port: 43982
      Destination Port: 43982
      Length = 32
      Checksum: 0x0000(checksum not used)
 nwipn: ============================ NetWare/IP ============================
      Packet Type: 2 (Request NWIP Nearest Server)
      Source IPX Socket: 0x4008
      Server Type: 632
      NWIP Domain Length: 16
      NWIP Domain Name: NWIP.IPDEMO.COM.
```

Packet Number 9: A NetWare/IP server responds to the client's Nearest Server query UDP broadcast.

```
Length : 72 bytes
   ip: ======================== Internet Protocol ========================
      Station:137.65.96.92 ---->137.65.96.89
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 54
```

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

```
      Identification:     4
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 60  seconds
      Checksum: 0xAB7B(Valid)
  udp: ====================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 396
      Length = 34
      Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
      Packet Type: 2 (Request NWIP Extended Nearest Server)
      Source IP Socket: 16392
      Server Type: 632
      Source IP Subnet Mask: 0xFFFFFF00
      Extended Signature: 0x4E574950
      Number Extra Fields: 1
      Extra Field #1:
      ID: 1
      Length: 6
      Number of Bytes: 4
      IP Address Pattern: 137.65.96.89
```

Packet Number 10: The NWIP server then sends five valid responses to the NWIP client's Nearest Server query. Since this is an isolated test environment, all five servers in the response are identical. The NWIP server responds with the first five SAP entries that match the client's request.

```
Length : 402 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.92
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 384
      Identification: 25214
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 128 seconds
      Checksum: 0x03B7(Valid)
  udp: ====================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 396
      Length = 364
      Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
      Packet Type: 3 (Response NWIP Nearest Server)
      Source IPX Socket: 0x4008
      Record Count: 5
      Server #5 IP Address: 137.65.96.89
      Server #5 Ticks: 2
      Server #5 IP Address: 137.65.96.89
      Server #5 Ticks: 2
      Server #5 IP Address: 137.65.96.89
      Server #5 Ticks: 2
      Server #5 IP Address: 137.65.96.89
      Server #5 Ticks: 2
```

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

```
      Server #5 IP Address: 137.65.96.89
      Server #5 Ticks: 2
      Server Record #1:
            Server Type: 632
            Server Name: NOVELL_INC_____________________ABTHK@@@@@DàPJ
            IPX Network Number: 0x10105B1
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Intermediate Networks: 0
      Server Record #2:
            Server Type: 632
            Server Name: IL-TREE________________________ABP J@@@@@DàPJ
            IPX Network Number: 0x10104A9
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Intermediate Networks: 0
      Server Record #3:
            Server Type: 632
            Server Name: NOVELL_INC_____________________AB@H@@@@@@DàPJ
            IPX Network Number: 0x1010001
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Intermediate Networks: 0
      Server Record #4:
            Server Type: 632
            Server Name: NOVELL_INC_____________________AB¥ B@@@@@DàPJ
            IPX Network Number: 0x101AE28
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Intermediate Networks: 0
      Server Record #5:
            Server Type: 632
            Server Name: NOVELL_INC_____________________AB £M@@@@@DàPJ
            IPX Network Number: 0x101F3D6
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Intermediate Networks: 0
```

Packet Number 11: The VLM client chooses the first server in the list returned by the NWIP server. Next, the VLM client must resolve a route to the internal IPX address (10105B1 see packet #10). To resolve this IPX internal network address, the NetWare/IP client will send a NWIP RIP request to the NetWare/IP server.

```
Length : 64 bytes
   ip: ====================== Internet Protocol ======================
      Station:137.65.96.92 ---->137.65.96.89
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 36
      Identification:     5
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 60  seconds
      Checksum: 0xAB8C(Valid)
  udp: ==================== User Datagram Protocol ====================
      Source Port: 43982
```

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

```
      Destination Port: 43982
      Length = 16
      Checksum: 0x0000(checksum not used)
nwipn: ============================ NetWare/IP ============================
      Packet Type: 16 (Request NWIP RIP)
      Source IPX Socket: 0x453 (RIP)
      IPX Network Number: 0x10105B1
```

Packet Number 12: The NetWare/IP server responds with its IP address, since it will act as the intermediate gateway between the NetWare/IP client and the IPX segment.

```
Length : 66 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.92
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 48
      Identification: 25215
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 128 seconds
      Checksum: 0x0506(Valid)
  udp: ===================== User Datagram Protocol ====================
      Source Port: 43982
      Destination Port: 43982
      Length = 28
      Checksum: 0x0000(checksum not used)
nwipn: ============================ NetWare/IP ============================
      Packet Type: 17 (Response NWIP RIP)
      Source IPX Socket: 0x453 (RIP)
      IP Address: 137.65.96.89
      IPX Network Number: 0x10105B1
      Intermediate Networks: 3
      Ticks: 4
      Data:
            0: 68 A7 A9 01                                          |h...
```

Packet Number 13: The NetWare/IP client verifies that the NetWare/IP gateway can actually reach the IPX segment in question (10105B1) by attempting to echo a packet to the segment.

```
Length : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.92 ---->137.65.96.89
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 42
      Identification:     6
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 60  seconds
      Checksum: 0xAB85(Valid)
```

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

```
  udp: ===================== User Datagram Protocol ====================
       Source Port: 43982
       Destination Port: 43982
       Length = 22
       Checksum: 0x0000(checksum not used)
 nwipn: ========================== NetWare/IP ==========================
       Packet Type: 14 (Request NWIP Echo)
       IPX Socket: 0x453 (RIP)
       Ticks: 9103
       IPX Network Number: 0x10105B1
       Intermediate Networks: 3
       Ticks: 4
```

Packet Number 14: The NetWare/IP server (also a NetWare/IP - IPX gateway) responds successfully to the RIP echo.

```
Length : 64 bytes
    ip: ======================= Internet Protocol =======================
       Station:137.65.96.89 ---->137.65.96.92
       Protocol: UDP
       Version: 4
       Header Length (32 bit words): 5
       Precedence: Routine
             Normal Delay, Normal Throughput, Normal Reliability
       Total length: 42
       Identification: 25218
       Fragmentation allowed, Last fragment
       Fragment Offset: 0
       Time to Live: 128 seconds
       Checksum: 0x0509(Valid)
  udp: ===================== User Datagram Protocol ====================
       Source Port: 43982
       Destination Port: 43982
       Length = 22
       Checksum: 0x0000(checksum not used)
nwipn: ========================== NetWare/IP ==========================
       Packet Type: 15 (Response NWIP Echo)
       IPX Socket: 0x453 (RIP)
       Ticks: 9103
       IPX Network Number: 0x10105B1
       Intermediate Networks: 3
       Ticks: 4
```

From this point forward, the client attaches as a normal VLM workstation, negotiating a Packet Burst connection and Large Internet Packets. Note that during the entire initialization process not a single IPX packet was placed on the network.

NetWare/IP Server with DSS Initializing

This is a trace of server ATL1 loading NWIP.NLM, demonstrating how a NetWare/IP server initializes. This server is also configured as a secondary DSS, so it must create a TCP connection to the primary DSS and download version changes to the DSS database. DSS is loaded at approximately packet #25.

Here is the appropriate background information:

Server name: atl1.ipdemo.com
Server's IP address: 137.65.96.91

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

NWIP Domain Name: nwip.ipdemo.com
NWIP Virtual IPX address: 13131313
Primary DSS: 137.65.96.89 (nwipdemo.ipdemo.com)
Secondary DSS: 137.65.96.91 (atl1.ipdemo.com)
First preferred DSS: 137.65.96.89 (nwipdemo.ipdemo.com)
Second preferred DSS: 137.65.96.91 (atl1.ipdemo.com)

Note that the first preferred DSS for `atl1.ipdemo.com` is `nwipdemo.ipdemo.com`. Since `atl1.ipdemo.com` is also a secondary DSS, it should be configured to use itself as the first preferred DSS, and then to use `nwipdemo.ipdemo.com` only as an alternate. The configuration used in this test is less than optimal, but this was necessary to demonstrate how NWIP.NLM initializes.

Packet Number 1: This is the first packet generated by NWIP.NLM as it loads. Since the preferred DSS was configured to 137.65.96.89, NWIP.NLM sends an SOA query for the NWIP domain (nwip.ipdemo.com) to verify that DSS.NLM is loaded.

```
Length : 80 bytes           Slice : 80 bytes
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.91 ---->137.65.96.89
       Protocol: UDP
       Version: 4
       Header Length (32 bit words): 5
       Precedence: Routine
             Normal Delay, Normal Throughput, Normal Reliability
       Total length: 61
       Identification: 34417
       Fragmentation allowed, Last fragment
       Fragment Offset: 0
       Time to Live: 128 seconds
       Checksum: 0xE107(Valid)
  udp: ===================== User Datagram Protocol ====================
       Source Port: 2850
       Destination Port: DOMAIN
       Length = 41
       Checksum: 0x3FF9(Valid)
  dns: ======================= Domain Name Service =====================
       Header:
             ID: 1
             Op Code: 0 (Standard Query)
             Flags: 0x0100 (Recursion Desired)
             Question Count: 1
             Answer Count: 0
             Authority Record Count: 0
             Additional Count: 0
       Questions:
             Domain Name: NWIP.IPDEMO.COM
             Type: 6 (Start of a Zone of Authority)
             Class: 1 (Internet)
```

Packet Number 2: DSS responds to the SOA query for the NWIP domain.

```
Length : 142 bytes          Slice : 142 bytes
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: UDP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
```

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

```
      Total length: 123
      Identification:  4689
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 128 seconds
      Checksum: 0x54EA(Valid)
  udp: ===================== User Datagram Protocol ====================
      Source Port: DOMAIN
      Destination Port: 2850
      Length = 103
      Checksum: 0x6A0C(Valid)
  dns: ====================== Domain Name Service ======================
      Header:
            ID: 1
            Op Code: 0 (Standard Query)
            Response Code: 0 (No Error)
            Flags: 0x8580 (Response, Authoritative Answer,
                        Recursion Desired, Recursion Available)
            Question Count: 0
            Answer Count: 1
            Authority Record Count: 0
            Additional Count: 0
      Answers:
            Domain Name: NWIP.IPDEMO.COM
            Type: 6 (Start of a Zone of Authority)
            Class: 1 (Internet)
            Time to Live: 0
            Data Length: 56
            Name Server: nwipdemo.ipdemo.com
            Mailbox of Responsible Person: THE-NWIP-GURU
            Serial Number of Zone Info: 55116
            Refresh Interval: 300
            Failed Refresh Retry Interval: 300
            Max Expiration Interval: 1499480457
            Minimum Time to Live: 1
```

Packet Number 3: NWIP.NLM requests the NWIP domain parameters.

```
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 2851
      Destination Port: 396
      Length = 12
      Checksum: 0x0000(checksum not used)
nwipu: ============================ NetWare/IP ========================
      Packet Type: 12 (Request NWIP Parameters)
      Sequence Number: 256
```

Packet Number 4: DSS responds with the NWIP domain parameters.

```
Length : 70 bytes           Slice : 70 bytes
     ip: ======================= Internet Protocol ======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: UDP
```

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

```
  udp: ===================== User Datagram Protocol ====================
       Source Port: 396
       Destination Port: 2851
       Length = 32
       Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
       Packet Type: 13 (Response NWIP Parameters)
       Sequence Number: 256
       IPX Network Number String: 0101030c
       IPX Network Number: 0x101030C
       NetWare/IP Port Number: 43981
       Checksum Usage Flag: 0 (No)
       DB Sync. Interval (secs): 300
       Max. UDP Retransmissions: 3
```

Packet Number 5: NWIP requests additional parameters that are required for NWIP servers. Note that clients generally don't need this information, only NWIP servers.

```
Length : 64 bytes           Slice : 64 bytes
   ip: ======================== Internet Protocol =======================
       Station:137.65.96.91 ---->137.65.96.89
       Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
       Source Port: 2851
       Destination Port: 396
       Length = 12
       Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
       Packet Type: 18 (Request NWIP Optional Parameters)
       Sequence Number: 256
```

Packet Number 6: DSS responds. The NWIP optional parameters are used to estimate IPX packet transmit times between subnets. These parameters are set in the Primary DSS configuration in UNICON.

```
Length : 78 bytes           Slice : 78 bytes
    ip: ======================== Internet Protocol =======================
       Station:137.65.96.89 ---->137.65.96.91
       Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
       Source Port: 396
       Destination Port: 2851
       Length = 40
       Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
       Packet Type: 19 (Response NWIP Optional Parameters)
       Sequence Number: 256
       Response Length: 32
       Number Parameters: 4
       Parameter Number #1:
             ID: 2
             Length: 2
             Same Subnet Ticks: 2
       Parameter Number #2:
             ID: 3
             Length: 2
             Same Net Ticks: 4
       Parameter Number #3:
```

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

```
            ID: 4
            Length: 2
            Other Net Ticks: 6
      Parameter Number #4:
            ID: 1
            Length: 2
            DSS/DSS Transfer Interval: 300
```

Packet Number 7: NWIP requests the version of the DSS database for use in a later request.

```
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 2851
      Destination Port: 396
      Length = 12
      Checksum: 0x0000(checksum not used)
 nwipu: ============================ NetWare/IP ==========================
      Packet Type: 8 (Request Database Version Number)
Data:
      0: 1D F1                                                 |..
```

Packet Number 8: DSS responds with the DSS database version number.

```
Length : 64 bytes           Slice : 64 bytes
    ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 2851
      Length = 12
      Checksum: 0x0000(checksum not used)
nwipu: ============================ NetWare/IP ==========================
      Packet Type: 9 (Response Database Version Number)
      Version Number: 55116
```

Packet Number 9: The NWIP server reports its internal IPX address to DSS so that other servers may contact DSS and locate a route to the server.

```
Length : 74 bytes           Slice : 74 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: UDP
   udp: ===================== User Datagram Protocol ====================
      Source Port: 2851
      Destination Port: 396
      Length = 36
      Checksum: 0x0000(checksum not used)
 nwipu: ============================ NetWare/IP ==========================
      Packet Type: 5 (RIP Information Update)
      Reserved: 0x6963
      Sequence Number: 1
      Record Count: 1
```

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

```
      Source IP Address: 137.65.96.91
      Source IP Subnet Mask: 0xFFFFFF00
      RIP Record #1:
            IPX Network Number: 0x301016A5
            Intermediate Networks: 1
            Ticks: 2
            Record Flag: 0x2 (New record)
            Reserved: 0x6F20
```

Packet Number 10: DSS acknowledges that the RIP information was successfully added to the DSS database.

```
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 2851
      Length = 12
      Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
      Packet Type: 6 (RIP Information Update Acknowledgment)
      Sequence Number: 1
```

Packet Number 11: ATL1 sends its SAP information to the DSS for inclusion in the DSS database.

```
Length : 128 bytes          Slice : 128 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 2851
      Destination Port: 396
      Length = 90
      Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
      Packet Type: 1 (SAP Information Update)
      Reserved: 0x6E64
      Sequence Number: 1
      Record Count: 1
      Source IP Address: 137.65.96.91
      Source IP Subnet Mask: 0xFFFFFF00
      SAP Record #1:
            Server Type: 263
            Server Name: ATL1
            IPX Network Number: 0x301016A5
            IPX Node: 000000000001
            IPX Socket: 0x8104
            Intermediate Networks: 1
            Record Flag: 0x2 (New record)
```

Packet Number 12: DSS acknowledges that the SAP information was successfully added to the DSS database.

```
Length : 64 bytes           Slice : 64 bytes
```

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

```
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: UDP
   udp: ===================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 2851
      Length = 12
      Checksum: 0x0000(checksum not used)
nwipu: ============================ NetWare/IP ==========================
      Packet Type: 7 (SAP Information Update Acknowledgment)
      Sequence Number: 1
```

Packet Number 13: ATL1 sends additional SAP information to DSS.

```
Length : 194 bytes          Slice : 194 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 2851
      Destination Port: 396
      Length = 156
      Checksum: 0x0000(checksum not used)
nwipu: ============================ NetWare/IP ==========================
      Packet Type: 1 (SAP Information Update)
      Reserved: 0x6572
      Sequence Number: 2
      Record Count: 2
      Source IP Address: 137.65.96.91
      Source IP Subnet Mask: 0xFFFFFF00
      SAP Record #1:
            Server Type: 632
            Server Name: FOB_TREE_______________________òà ìJ@@@@@DàPJ
            IPX Network Number: 0x301016A5
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Intermediate Networks: 1
            Record Flag: 0x2 (New record)
      SAP Record #2:
            Server Type: 4
            Server Name: ATL1
            IPX Network Number: 0x301016A5
            IPX Node: 000000000001
            IPX Socket: 0x451 (NCP)
            Intermediate Networks: 1
            Record Flag: 0x2 (New record)
```

Packet Number 14: DSS acknowledges that the records were added to the DSS database.

```
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol ======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 2851
      Length = 12
```

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

```
      Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
      Packet Type: 7 (SAP Information Update Acknowledgment)
      Sequence Number: 2
```

Packets 15 through 18 show ATL1 opening a TCP connection to DSS for database synchronization. In effect, ATL1 is "receiving" the DSS database.

```
Packet Number : 15          4:24:19 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 1050
      Destination Port: 396
      Sequence Number: 519876966
      Acknowledgement Number: 0
      Data Offset (32-bit words): 6
      Window: 0
      Control Bits:
            Synchronize Sequence Numbers (SYN)
      Checksum: 0xEEE6(Valid)
      Urgent Pointer: 0
      Option:MAXIMUM SEGMENT SIZE
            Option Length: 4
            Maximum Segment Size : 1460


Packet Number : 16          4:24:19 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 396
      Destination Port: 1050
      Sequence Number: 2707072157
      Acknowledgement Number: 519876967
      Data Offset (32-bit words): 6
      Window: 16060
      Control Bits: Acknowledgement Field is Valid (ACK)
                  Synchronize Sequence Numbers (SYN)
      Checksum: 0x6A21(Valid)
      Urgent Pointer: 0
      Option:MAXIMUM SEGMENT SIZE
            Option Length: 4
            Maximum Segment Size : 1460


Packet Number : 17          4:24:19 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 1050
      Destination Port: 396
```

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

```
      Sequence Number: 519876967
      Acknowledgement Number: 2707072158
      Data Offset (32-bit words): 5
      Window: 16060
      Control Bits: Acknowledgement Field is Valid (ACK)
      Checksum: 0x81DE(Valid)
      Urgent Pointer: 0
```

In Packet Number 18, NWIP is pulling the SAP/RIP records from DSS.

```
Packet Number : 18          4:24:19 PM
Length : 70 bytes           Slice : 70 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: TCP
  tcp: ================== Transmission Control Protocol ==================
      Source Port: 1050
      Destination Port: 396
      Sequence Number: 519876967
      Acknowledgement Number: 2707072158
      Data Offset (32-bit words): 5
      Window: 16060
      Control Bits: Acknowledgement Field is Valid (ACK)
            Push Function Requested (PSH)
      Checksum: 0x81C8(Valid)
      Urgent Pointer: 0
nwipt: ============================ NetWare/IP ============================
      Packet Type: 257 (Request DSS to NWIP Database Full Transfer)
      Local DB Version Number: 0
      Local IP Address: 0.0.0.0 (Not Applicable)
      Local IP Subnet Mask: 0xFFFFFF00
```

Packet Number 19: DSS is sending SAP and RIP records. Note that the "TRUNCATED PACKET -- ABORTING DECODE" message results from using a small packet slice in LANalyzer for Windows. This was chosen because we are interested in the NetWare/IP mechanisms, not the data.

```
Length : 74 bytes           Slice : 74 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: TCP
  tcp: ================== Transmission Control Protocol ==================
      Source Port: 396
      Destination Port: 1050
      Sequence Number: 2707072158
      Acknowledgement Number: 519876979
      Data Offset (32-bit words): 5
      Window: 16048
      Control Bits: Acknowledgement Field is Valid (ACK)
            Push Function Requested (PSH)
            Checksum: 0xA963(Valid)
            Urgent Pointer: 0
nwipt: ============================ NetWare/IP ============================
      Packet Type: 258 (Response DSS to NWIP Database Full Transfer)
      DSS DB Version Number: 55120
      Total Entries in DB (checksum): 0
      Packet Flag: 0x0
      Total Packet Length: 16
```

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

```
      Number of SAP records: 0
      Number of RIP Records: 0
      RIP Record #1:
            Record Type: 12844
            Record Flag: 0x300D (Changed record, Changed record by retarget)
            IPX Network Number:
            TRUNCATED PACKET - ABORTING DECODE


Packet Number : 20          4:24:19 PM
Length : 64 bytes           Slice : 64 bytes
ether: ==================== Ethernet Datalink Layer ====================
      Station: NWIPDEMO ----> 00-00-1B-1E-74-BA
      Type: 0x0800 (IP)
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: TCP
      Version: 4
      Header Length (32 bit words): 5
      Precedence: Routine
            Normal Delay, Normal Throughput, Normal Reliability
      Total length: 40
      Identification:  4698
      Fragmentation allowed, Last fragment
      Fragment Offset: 0
      Time to Live: 128 seconds
      Checksum: 0x553F(Valid)
  tcp: ================= Transmission Control Protocol =================
      Source Port: 396
      Destination Port: 1050
      Sequence Number: 2707072174
      Acknowledgement Number: 519876979
      Data Offset (32-bit words): 5
      Window: 16048
      Control Bits: Acknowledgement Field is Valid (ACK)
            No More Data from Sender (FIN)
      Checksum: 0x81CD(Valid)
      Urgent Pointer: 0
```

The remainder of this trace is DSS loading on ATL1 and synchronizating to the primary DSS. Like the NWIP server, the secondary DSS checks to ensure that the primary DSS is functional, receives the NWIP parameters, gets the DSS database version number, and then starts to receive the DSS database.

```
Packet Number : 26          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
    ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
      Source Port: 396
      Destination Port: 396
      Length = 12
      Checksum: 0x0000(checksum not used)
  rpc: ===================== Remote Procedure Call =====================
      Transaction ID: 0xCDEAD
      Message Type: 0 (Call)
      FRAGMENTED PACKET - DISPLAYING REMAINDER OF FIRST FRAGMENT
```

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

```
Packet Number : 27          4:24:32 PM
Length : 70 bytes           Slice : 70 bytes
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.89 ---->137.65.96.91
       Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
       Source Port: 396
       Destination Port: 396
       Length = 32
       Checksum: 0x0000(checksum not used)
nwipu: ============================ NetWare/IP ==========================
       Packet Type: 13 (Response NWIP Parameters)
       Sequence Number: 57005
       IPX Network Number String: 0101030c
       IPX Network Number: 0x101030C
       NetWare/IP Port Number: 43981
       Checksum Usage Flag: 0 (No)
       DB Sync. Interval (secs): 300
       Max. UDP Retransmissions: 3


Packet Number : 28          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.91 ---->137.65.96.89
       Protocol: UDP
udp: ===================== User Datagram Protocol ====================
       Source Port: 396
       Destination Port: 396
       Length = 12
       Checksum: 0x0000(checksum not used)
  rpc: ===================== Remote Procedure Call =====================
       Transaction ID: 0xEBDAB
       Message Type: 0 (Call)
       FRAGMENTED PACKET - DISPLAYING REMAINDER OF FIRST FRAGMENT


Packet Number : 29          4:24:32 PM
Length : 846 bytes          Slice : 846 bytes
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.89 ---->137.65.96.91
       Protocol: UDP
  udp: ===================== User Datagram Protocol ====================
       Source Port: 396
       Destination Port: 396
       Length = 808
       Checksum: 0x0000(checksum not used)
 nwipu: ============================ NetWare/IP ==========================
       Packet Type: 15 (UNKNOWN PACKET TYPE)
       Data:
             0: BD AB 6E 77 69 70 2E 69 70 64 65 6D 6F 2E 63 6F
|..nwip.ipdemo.co
            10: 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|m...............


Packet Number : 30          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
```

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

```
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.91 ---->137.65.96.89
       Protocol: UDP
  udp: ===================== User Datagram Protocol =====================
       Source Port: 396
       Destination Port: 396
       Length = 12
       Checksum: 0x0000(checksum not used)
  rpc: ===================== Remote Procedure Call =====================
       Transaction ID: 0x12BAAB
       Message Type: 0 (Call)
       FRAGMENTED PACKET - DISPLAYING REMAINDER OF FIRST FRAGMENT


Packet Number : 31          4:24:32 PM
Length : 78 bytes           Slice : 78 bytes
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.89 ---->137.65.96.91
       Protocol: UDP
  udp: ===================== User Datagram Protocol =====================
       Source Port: 396
       Destination Port: 396
       Length = 40
       Checksum: 0x0000(checksum not used)
nwipu: ========================== NetWare/IP ==========================
       Packet Type: 19 (Response NWIP Optional Parameters)
       Sequence Number: 47787
       Response Length: 32
       Number Parameters: 4
       Parameter Number #1:
             ID: 2
             Length: 2
             Same Subnet Ticks: 2
       Parameter Number #2:
             ID: 3
             Length: 2
             Same Net Ticks: 4
       Parameter Number #3:
             ID: 4
             Length: 2
             Other Net Ticks: 6
       Parameter Number #4:
             ID: 1
             Length: 2
             DSS/DSS Transfer Interval: 300


Packet Number : 32          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
       Station:137.65.96.91 ---->137.65.96.89
       Protocol: TCP
  tcp: ================ Transmission Control Protocol ================
       Source Port: 1051
       Destination Port: 396
       Sequence Number: 523158675
       Acknowledgement Number: 0
             Data Offset (32-bit words): 6
       Window: 0
```

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

```
      Control Bits: Synchronize Sequence Numbers (SYN)
      Checksum: 0xDB86(Valid)
      Urgent Pointer: 0
      Option:MAXIMUM SEGMENT SIZE
      Option Length: 4
      Maximum Segment Size : 1460


Packet Number : 33          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 396
      Destination Port: 1051
      Sequence Number: 2710353866
      Acknowledgement Number: 523158676
      Data Offset (32-bit words): 6
      Window: 16060
      Control Bits: Acknowledgement Field is Valid (ACK)
            Synchronize Sequence Numbers (SYN)
      Checksum: 0x4362(Valid)
      Urgent Pointer: 0
      Option:MAXIMUM SEGMENT SIZE
      Option Length: 4
      Maximum Segment Size : 1460


Packet Number : 34          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: TCP
   tcp: ================= Transmission Control Protocol =================
      Source Port: 1051
      Destination Port: 396
      Sequence Number: 523158676
      Acknowledgement Number: 2710353867
      Data Offset (32-bit words): 5
      Window: 16060
      Control Bits: Acknowledgement Field is Valid (ACK)
      Checksum: 0x5B1F(Valid)
      Urgent Pointer: 0


Packet Number : 35          4:24:32 PM
Length : 70 bytes           Slice : 70 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.91 ---->137.65.96.89
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 1051
      Destination Port: 396
      Sequence Number: 523158676
      Acknowledgement Number: 2710353867
      Data Offset (32-bit words): 5
      Window: 16060
      Control Bits: Acknowledgement Field is Valid (ACK)
```

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

```
            Push Function Requested (PSH)
      Checksum: 0x9918(Valid)
      Urgent Pointer: 0
nwipt: ========================== NetWare/IP ==========================
      Packet Type: 273 (Request DSS to DSS Database Full Transfer)
      Local DB Version Number: 55108
      Local IP Address: 137.65.96.91
      Local IP Subnet Mask: 0x00000000


Packet Number : 36          4:24:32 PM
Length : 64 bytes           Slice : 64 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 396
      Destination Port: 1051
      Sequence Number: 2710353867
      Acknowledgement Number: 523158688
      Data Offset (32-bit words): 5
      Window: 16048
      Control Bits: Acknowledgement Field is Valid (ACK)
      Checksum: 0x5B1F(Valid)
      Urgent Pointer: 0


Packet Number : 37          4:24:32 PM
Length : 344 bytes          Slice : 344 bytes
   ip: ======================= Internet Protocol =======================
      Station:137.65.96.89 ---->137.65.96.91
      Protocol: TCP
  tcp: ================= Transmission Control Protocol =================
      Source Port: 396
      Destination Port: 1051
      Sequence Number: 2710353867
      Acknowledgement Number: 523158688
      Data Offset (32-bit words): 5
      Window: 16048
      Control Bits: Acknowledgement Field is Valid (ACK)
            Push Function Requested (PSH)
      Checksum: 0x9967(Valid)
      Urgent Pointer: 0
nwipt: ========================== NetWare/IP ==========================
      Packet Type: 274 (Response DSS to DSS Database Full Transfer)
      DSS DB Version Number: 55120
      Total Entries in DB (checksum): 4
      Packet Flag: 0x0
      Total Packet Length: 286
      Number of SAP records: 3
      Number of RIP Records: 1
      SAP Record #1:
      Record Type: 1
            Server Name: ATL1
      IPX Network Number: 0x301016A5
      IPX Node: 000000000001
      IPX Socket: 0x8104
      Server Type: 263
      IP Address Count: 1
```

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

```
      IP Address Record #1:
            IP Address: 137.65.96.91
            IP Subnet: 137.65.96.0
            Time to Live: 5
            Intermediate Networks: 0
            Reserved: 0x0000
            Authoritative DSS's IP Address: 0.0.0.0 (Primary DSS)
            Record Flag: 0x1 (DSS is authoritative)
      SAP Record #2:
            Record Type: 1
            Server Name: FOB_TREE_____________________òà ìJ@@@@@DàPJ
            IPX Network Number: 0x301016A5
            IPX Node: 000000000001
            IPX Socket: 0x4006
            Server Type: 632
            IP Address Count: 1
                  IP Address Record #1:
                  IP Address: 137.65.96.91
                  IP Subnet: 137.65.96.0
                  Time to Live: 5
                  Intermediate Networks: 0
                  Reserved: 0x0000
                  Authoritative DSS's IP Address: 0.0.0.0 (Primary DSS)
                  Record Flag: 0x1 (DSS is authoritative)
      SAP Record #3:
            Record Type: 1
            Server Name: ATL1
            IPX Network Number: 0x301016A5
            IPX Node: 000000000001
            IPX Socket: 0x451 (NCP)
            Server Type: 4
            IP Address Count: 1
            IP Address Record #1:
                  IP Address: 137.65.96.91
                  IP Subnet: 137.65.96.0
                  Time to Live: 5
                  Intermediate Networks: 0
                  Reserved: 0x0000
                  Authoritative DSS's IP Address: 0.0.0.0 (Primary DSS)
                  Record Flag: 0x1 (DSS is authoritative)
RIP Record #1:
      Record Type: 2
            IPX Network Number: 0x301016A5
            IP Address Count: 1
            IP Address Record #1:
                  IP Address: 137.65.96.91
                  IP Subnet: 137.65.96.0
                  Time to Live: 5
                  Intermediate Networks: 0
                  Ticks: 1
                  Authoritative DSS's IP Address: 0.0.0.0 (Primary DSS)
                  Record Flag: 0x81 (DSS is authoritative, RIP record)
```

This process continues until DSS has all of the SAP and RIP records from the Primary DSS.

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