Front

NetWare/IP Administrator’s Guide

Contents

Managing Host Information 257

Managing the Server Profile 263

Using File Functions 269

TCP/IP and SNMP 279

Error Messages 295

Preface

How to Use This Manual

This manual is for network administrators who are installing or managing the NetWare/IPTM software. NetWare/IP provides access to NetWare® networks using the TCP/IP transport instead of or in addition to the IPXTM protocol used in traditional NetWare environments.

This manual provides an introduction to the NetWare/IP software and includes information about installing, configuring, managing, and troubleshooting a NetWare/IP network.

Note

In Novell® documentation, an asterisk denotes a trademarked name belonging to a third-party company. Novell trademarks are denoted with specific trademark symbols, such as TM.

Contents Overview

This manual includes the following information:

- through Chapter 4, "Understanding the NetWare/IP Server and Client Software," on page 53 explain the components and services that comprise a NetWare/IP network.

- Chapter 5, "Installing the NetWare/IP Software," on page 65 provides information and procedures for installing a NetWare/IP network.

- Chapter 6, "Introducing UNICON and NWIPCFG," on page 83 introduces the utilities you use to manage a NetWare/IP network.

- Chapter 7, "Setting Up DNS Support," on page 89 through Chapter 9, "Configuring NetWare/IP Servers," on page 139 provide procedures for managing the primary components and services that comprise a NetWare/IP network.

- Chapter 10, "Troubleshooting," on page 149 includes tips and procedures for troubleshooting a NetWare/IP network.

- Chapter 11, “Removing the NetWare/IP Software,” on page 185 describes how to remove the NetWare/IP software from servers and workstations.

- Chapter 12, “Configuring a DHCP Server,” on page 195 includes information about installing, configuring, and managing the NetWare DHCP service.

- Chapter 13, “Configuring NetWare-to-UNIX Printing,” on page 211 explains how to set up and use the lpr gateway software that enables IPX-based clients to use network printers attached to UNIX-based hosts.

- Appendix A, “Planning a NetWare/IP Network,” on page 219 contains information to help plan a NetWare/IP network, including an example network configuration and blank planning worksheets.

- Appendix B, “Managing NetWare/IP Remotely,” on page 243 through Appendix F, “TCP/IP and SNMP,” on page 279 provide additional information about using the utilities and protocols included with the NetWare/IP software. The information in these appendices is generally offered as a suggestion, not a requirement.

- Appendix G, “Error Messages,” on page 295 lists the possible error messages that the NetWare/IP software modules may generate, given various conditions. In addition, this appendix includes information about possible remedies for the error-generating condition.

User Comments

We are continually looking for ways to make our products and our documentation as easy to use as possible.

You can help us by sharing your comments and suggestions about how our documentation could be made more useful to you and about inaccuracies or information gaps it might contain.

Submit your comments by using the User Comments form provided or by writing to us directly at the following address:

Novell, Inc.
Documentation Development MS C-231
122 East 1700 South

Provo, UT 84606 USA

e-mail: commentdoc@novell.com

We appreciate your comments.

Chapter

1 *Introducing NetWare/IP*

This chapter provides background information to help you understand how the NetWare/IP™ software fits into your internetworking environment. It introduces the components that make up the Netware/IP service and describes their interrelationships.

Overview of NetWare/IP

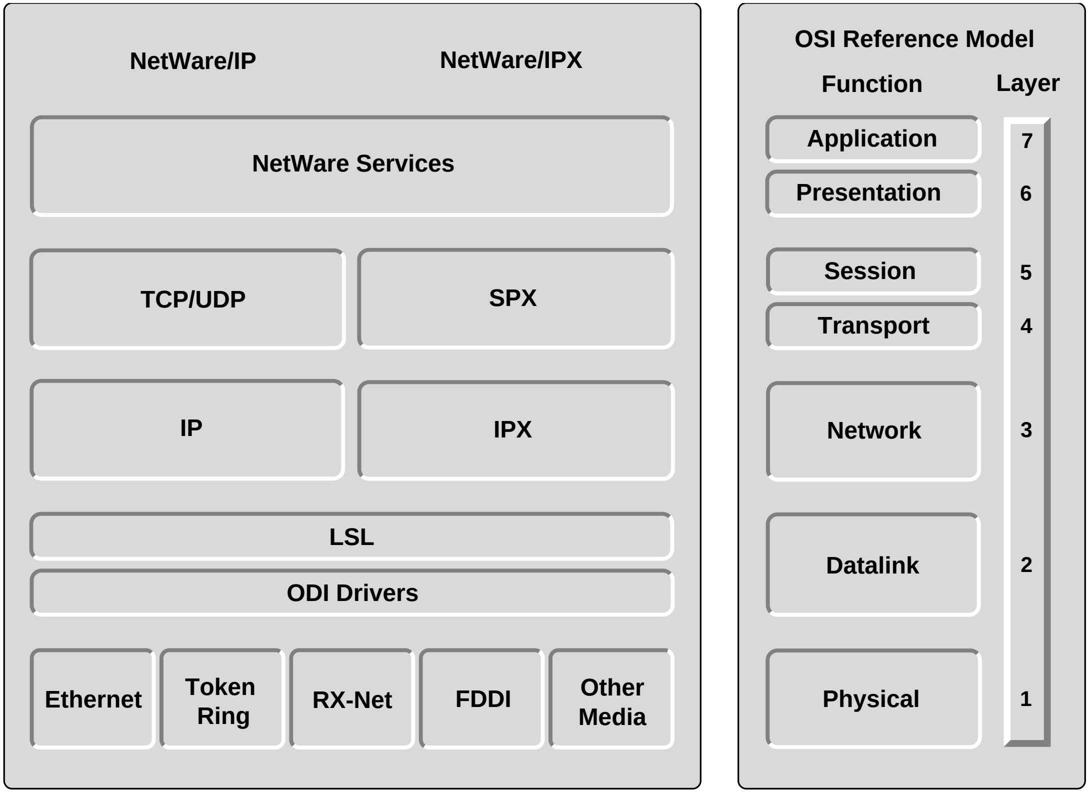
NetWare/IP is a set of server and client software modules that provides access to NetWare® applications using the Transmission Control Protocol/Internet Protocol (TCP/IP) transport instead of or in addition to the Internetwork Packet Exchange™ (IPX™) protocol used in traditional NetWare environments. NetWare/IP enables you to

- Extend NetWare services and applications to nodes on an existing IP network in a manner that is transparent to users
- Migrate your network from IPX to TCP/IP
- Interconnect TCP/IP and IPX networks, enabling users on both networks to access NetWare resources on either network

With NetWare/IP, NetWare applications and services look the same to the user regardless of whether IPX or IP is the transport protocol. In addition, the same datalink-level drivers service both protocols, so both can share the same cabling system.

Figure 1-1 compares the main internal components of NetWare/IP and IPX-based NetWare. These components are presented alongside the Open Systems Interconnection (OSI) reference model, which is widely used to categorize networking protocols.

Figure 1-1
NetWare/IP and NetWare/IPX Comparison



The NetWare/IP server replaces the IPX/SPX protocol stack with the TCP/IP protocol stack while continuing to use the same Link Support Layer™ (LSL™) driver and Open Data-Link Interface™ (ODI™) driver as a traditional NetWare server. The NetWare/IP server NetWare Loadable Module™ (NLM™), NWIP.NLM, provides IPX emulation using the NetWare/IP protocol over the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Thus, NetWare services and applications run identically on the NetWare/IP server to the way they run in the IPX environment.

NetWare/IP Components

Several basic NetWare/IP components must be installed and configured before NetWare/IP can function. This section lists and briefly describes each component and explains the interdependencies and interrelationships of the components.

NetWare/IP Support Services

NetWare/IP requires the following support services, which are included with the NetWare/IP software:

- **Domain Name System (DNS)** —provides a centralized database of host-to-address mapping. The fully functional NetWare DNS server included in this product can be used to manage UNIX® computers as well as NetWare servers.

Note You can also configure NetWare/IP servers and clients to use an existing DNS server.

- **Domain SAP/RIP Service (DSS)** —maintains and distributes service and routing (SAP and RIP) information for the NetWare/IP network.

NetWare/IP support services provide the framework for a NetWare/IP network, supplying information about both the location and availability of services and routes within the network. In an IPX network, NetWare servers broadcast this information every 60 seconds. IP networks, however, do not support this type of internetwork broadcast. Therefore, NetWare/IP requires the following support services to emulate the IPX broadcast mechanism:

- The Domain SAP/RIP Service (DSS) maintains two types of information required by NetWare servers and clients:

    - Service Advertising Protocol (SAP) information about available NetWare services

    - Routing Information Protocol (RIP) information about routes to NetWare nodes

  Once configured, DSS automatically maintains this information and makes it available to all NetWare/IP nodes. For additional information about DSS, see Chapter 3, “Understanding the Domain SAP/RIP Service,” on page 43

- The Domain Name System (DNS) is a distributed database system used to locate computers in TCP/IP internetworks. NetWare/IP servers and clients use DNS to locate the nearest DSS servers. For additional information about DNS, see Chapter 2, “Understanding the Domain Name System,” on page 23

Careful planning and configuration are required to optimize the load DSS and DNS servers place on the network and to ensure that their information is reliably available to all nodes. These services maintain databases that can be replicated for load balancing and reliability. Replication is also useful in servicing portions of the TCP/IP network that are interconnected using slower links, such as leased lines.

NetWare/IP Server

The NetWare/IP server is a NetWare 4™ server that is configured with TCP/IP and NetWare/IP NLMs. The NetWare/IP server provides NetWare services to clients on a TCP/IP network.

To enable IP and IPX to coexist on the same internetwork, NetWare/IP servers can be configured to act as gateways between IP and IPX network segments. NetWare/IP provides the following types of gateways:

- **Forwarding gateways** —interconnect IP and IPX network segments and advertise service and routing information between these dissimilar segments.

- **Non-forwarding gateways** —service both IP and IPX clients.

For additional information about the NetWare/IP server software, see Chapter 4, “Understanding the NetWare/IP Server and Client Software,” on page 53

NetWare/IP Client

The NetWare/IP client is a workstation that is configured with the NetWare/IP client software. The NetWare/IP software enables the client to access NetWare services over a TCP/IP network. For additional information about the NetWare/IP client software, see “Understanding the NetWare/IP Client” on page 58

Interdependencies of Components

The NetWare/IP components build upon each other to provide the NetWare/IP service as follows:

- DNS provides a master database containing information about the location of DSS servers. Until this service is running on the network, NetWare/IP servers and clients, which are configured as DNS clients or resolvers, cannot find the DSS servers.

Important

The NetWare/IP employment of DNS is significantly different from the standard DNS employment. Make sure you understand how NetWare/IP uses DNS before attempting to set up NetWare/IP.

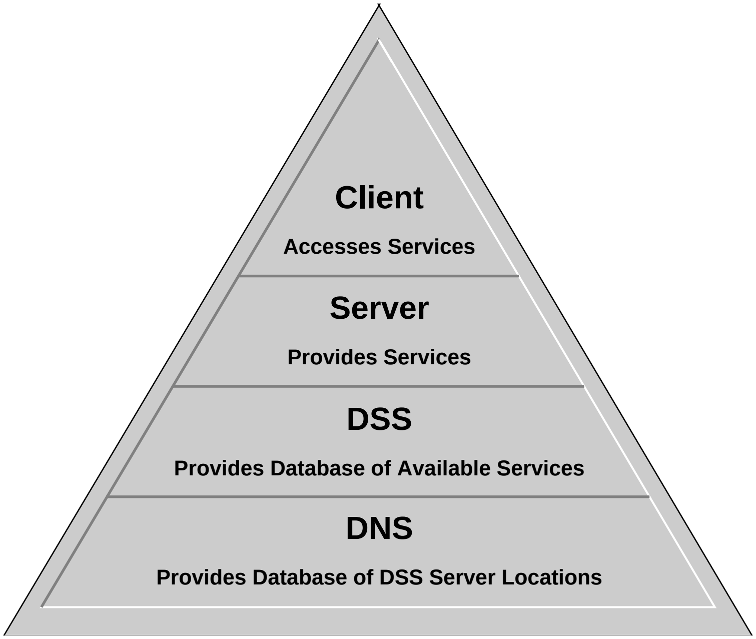
- DSS provides a database of the services and routes available within the network at any given time. Without DSS, servers are not able to register their services, and clients are not able to access network services.

- The NetWare/IP servers provide network services. NetWare/IP servers advertise their services to DSS servers, which in turn distribute the service availability information throughout the NetWare/IP internetwork.

- NetWare/IP clients depend on all the other NetWare/IP components and cannot function until all other NetWare/IP components are up and running.

Because the NetWare/IP components depend on each other, the NetWare/IP software will not allow you to start services in the incorrect order. For example, you cannot start a DSS server until a DNS server is running on the network. "Understanding the NetWare/IP Client" on page 58 illustrates the interdependencies between the NetWare/IP components.

Figure 1-2
Interdependencies of NetWare/IP Components


Client
Accesses Services
Server
Provides Services
DSS
Provides Database of Available Services
DNS
Provides Database of DSS Server Locations

How the Components Work Together

The NetWare/IP components work together as follows to provide NetWare services on a TCP/IP network:

1. When a NetWare/IP server starts up, it queries a DNS server for a list of DSS servers.

2. The NetWare/IP server then queries the nearest DSS server for network-wide configuration information. The NetWare/IP server also registers its services with the DSS server and queries the DSS server about other services that are available within the NetWare/IP network. While the NetWare/IP server is running, it continues to exchange service information with the DSS server at a defined interval.

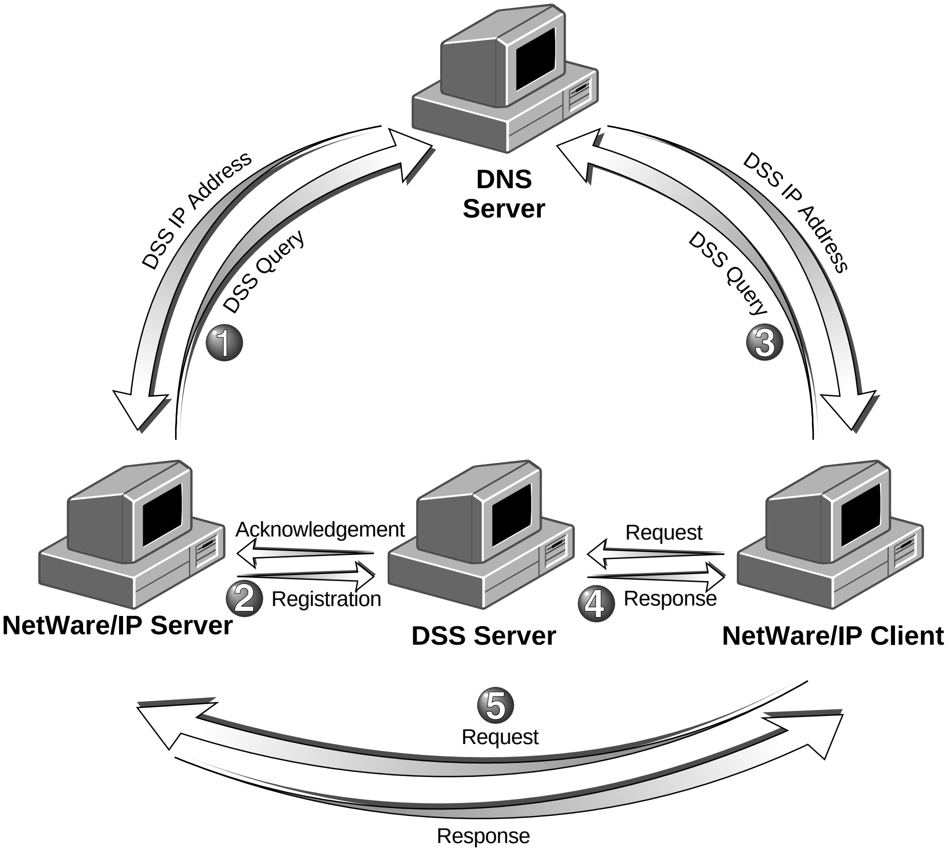
3. When a client system starts up, it must also locate a DSS server to obtain network-wide configuration information and service and routing information for the network. If the client does not know the location of a DSS server, it first queries a DNS server.

4. The client uses a DSS server to locate the nearest NetWare/IP server. The client then directs its NetWare/IP queries to that server.

This process can change somewhat, depending on whether you define Nearest NetWare/IP Server and Preferred DSS Server statements at the server or client and enable NSQ broadcasts at the client.

Figure 1-3 illustrates how the NetWare/IP components work together.

Figure 1-3
Relationship between Components



Administration Utilities

NetWare/IP provides the following utilities to administer this product:

NWIPCFG Administration Utility —enables you to administer the NetWare/IP server component of this product.

UNICON Administration Utility —enables you to administer the DNS and DSS server components of this product.

XConsole —provides remote administration by enabling you to access the NetWare/IP server console from X Window System* terminals and VT100*/VT220 terminals.

NetWare/IP provides the following network management and troubleshooting tools:

SNMP —enables you to monitor the status of NetWare/IP nodes from an SNMP management station.

Note

SNMP service must also be set up on the network.

Error Reporting System —displays or logs error messages when system problems occur on a specific server.

DSS Browser —enables you to view the SAP or RIP records stored in the DSS database.

DSS Viewer —displays information about all DSS servers in a NetWare/IP network.

Chapter

2 *Understanding the Domain Name System*

This chapter provides information to help you understand the NetWare Domain Name System (DNS) and how DNS fits into a NetWare/IP™ network environment.

The Domain Name System is a distributed database system that provides name-to-IP address mapping for computers on an internetwork. Any computer on the Internet can use a DNS server to locate any other computer on the Internet. Instead of using DNS to locate any computer, NetWare/IP servers and clients use DNS to locate a specific type of computer—the DSS server—within the NetWare/IP internetwork.

Conceptually, DNS is made up of two distinct components:

- The DNS hierarchy specifies the structure, naming conventions, and delegation of authority in the DNS service.

- The DNS name service provides the actual name-to-address mapping mechanism.

The following sections describe the standard DNS service. A discussion of how NetWare/IP uses DNS is also included in this chapter.

DNS Hierarchy

DNS uses a hierarchy to manage its distributed database system. The DNS hierarchy, also call the *domain name space* , is an inverted tree structure, much like the Novell Directory Services structure.

The DNS tree has a single node, or domain, at the top, called the root domain (.). Below the root domain are the top-level domains. These domains divide the DNS hierarchy organizationally into the following segments:

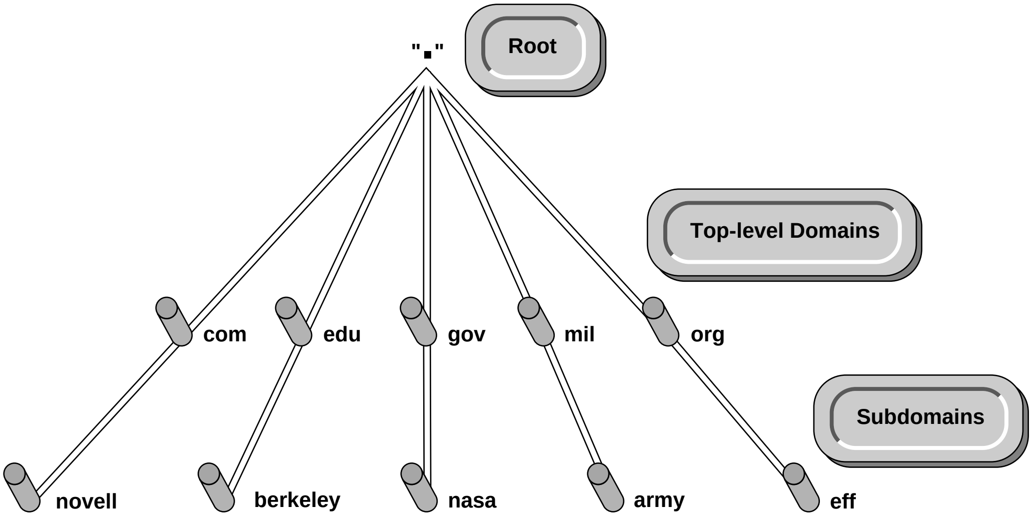
- **COM** —commercial organizations, such as Novell (novell.com)

- **EDU** —educational institutions, such as U.C. Berkeley (berkeley.edu)
- **GOV** —government agencies, such as NASA (nasa.gov)
- **MIL** —military organizations, such as the U.S. Army (army.mil)
- **ORG** —non-profit organizations, such as Electronic Frontier Foundation (eff.org)
- **NET** —networking entities, such as NSFNET (nsf.net)
- **INT** —international organizations, such as NATO (nato.int)

Additional top-level domains organize the domain name space geographically. For example, the top-level domain for France is fr.

Below the top-level domains, the domain name space is further organized into subdomains, which represent individual organizations. Figure 2-1 illustrates the DNS hierarchy.

Figure 2-1
DNS Hierarchy

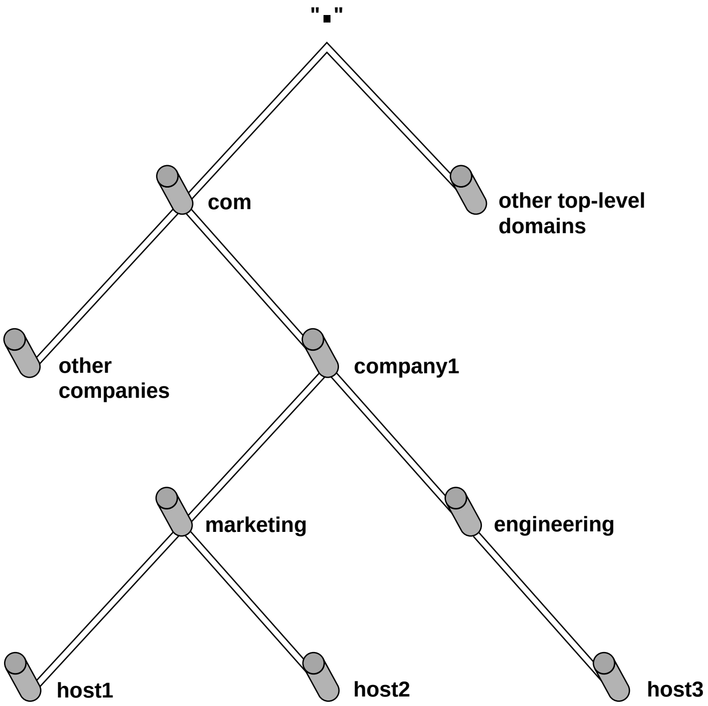


DNS Domains

A domain is a label of the DNS tree. Each node on the DNS tree represents a domain. The domains under the top-level domains represent individual entities. These domains can be further partitioned into subdomains to facilitate the management of information about an entity's host computers. Domains at the leaves of the tree usually represent individual hosts.

For example, suppose a domain is created for company1 under the com. top-level domain. Company1 has separate LANs in its marketing and engineering divisions. Therefore, the Company1 network administrator decides to create two separate subdomains for each division, as illustrated in Figure 2-2 .

Figure 2-2
Domains and Subdomains



Domain Names

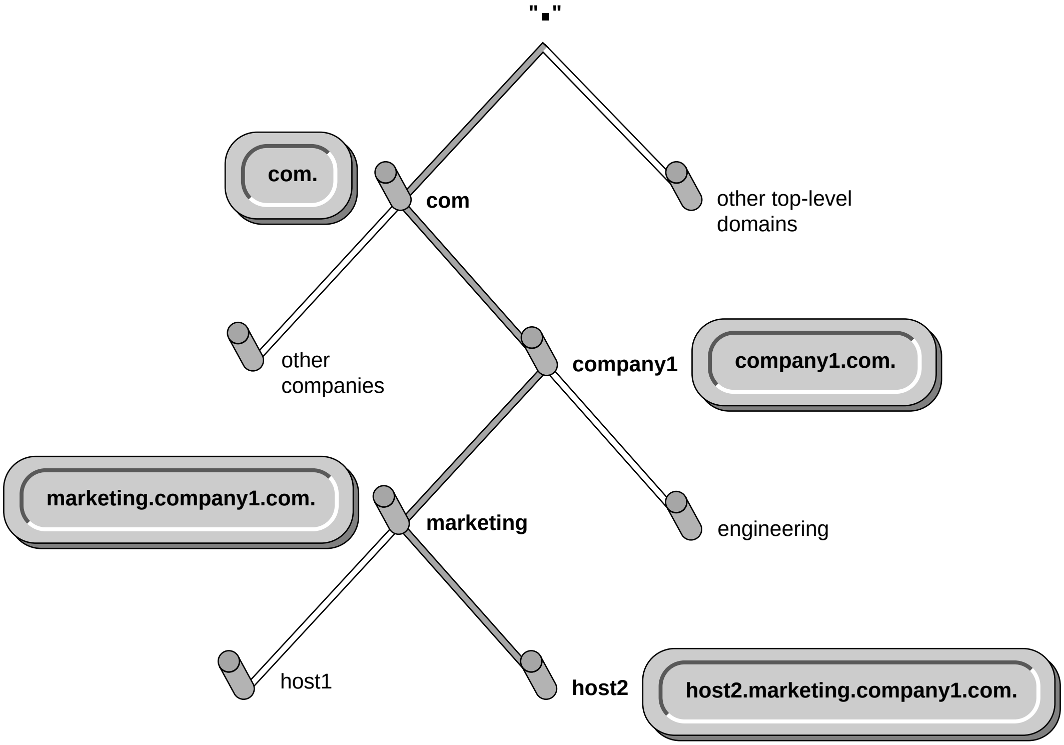
The domain naming scheme reflects the structure of the DNS hierarchy. A domain name is simply a list of all domains in the path from the local domain to the root. Each label in the domain name is delimited by a period or dot (.). For example, marketing.company1.com. is the domain name for the marketing domain in Figure 2-3 . Notice that the domain name in this example ends with a dot, which represents the root domain. Domain names that end with the dot for root are called fully qualified domain names.

Each computer that uses DNS is given a DNS hostname that reflects that computer's position in the DNS hierarchy. Thus, the DNS hostname for host2 in Figure 2-3 is host2.marketing.company1.com.

Any domain in a subtree is considered part of all domains above it. For example, the marketing.company1.com. domain is a part of the company1.com. domain, and also a part of the com. domain.

A full domain name can consist of up to 255 characters, although some systems may impose smaller limits. DNS is case-insensitive; HOST2 is the same as host2.

Figure 2-3
DNS Domain Names and Hostnames



Domain Delegation

Domain delegation gives an organization authority for a domain. Having authority for a domain means that the administrator at the organization is responsible for maintaining the DNS database of host name and address information for that domain. The group of domains and subdomains over which an organization has authority is called a zone. All host information for a zone is maintained in a single, authoritative database.

Note

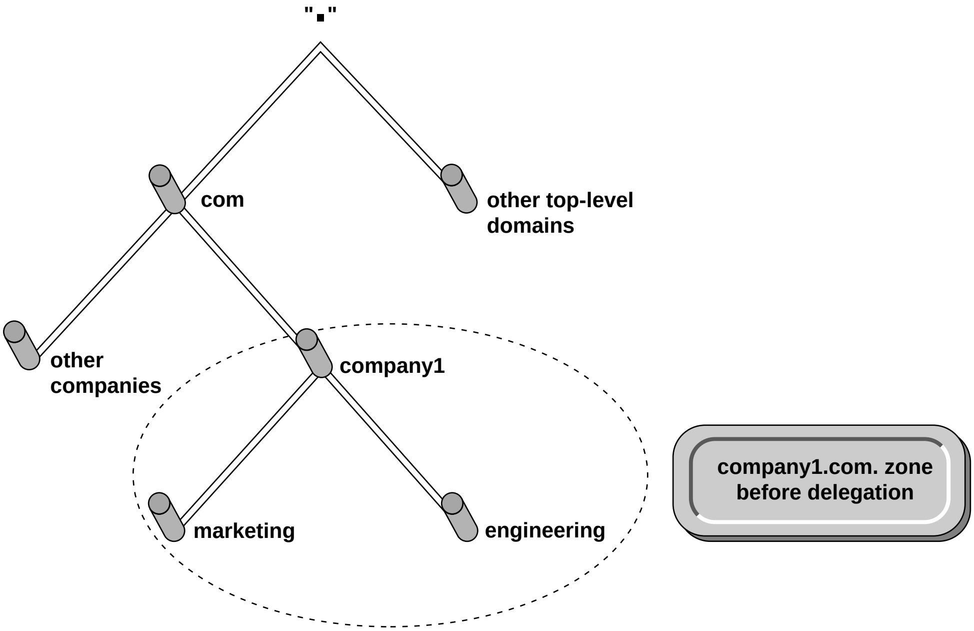
Throughout the industry, the terms zone and domain are used interchangeably.

For example, the company1.com. domain is delegated to company1, creating the company1.com. zone. This zone comprises three domains:

- company1.com.
- marketing.company1.com.
- engineering.company1.com.

The administrator at company1 maintains all host information for the zone in a single database. Figure 2-4 shows the company1.com. zone.

Figure 2-4
DNS Zones

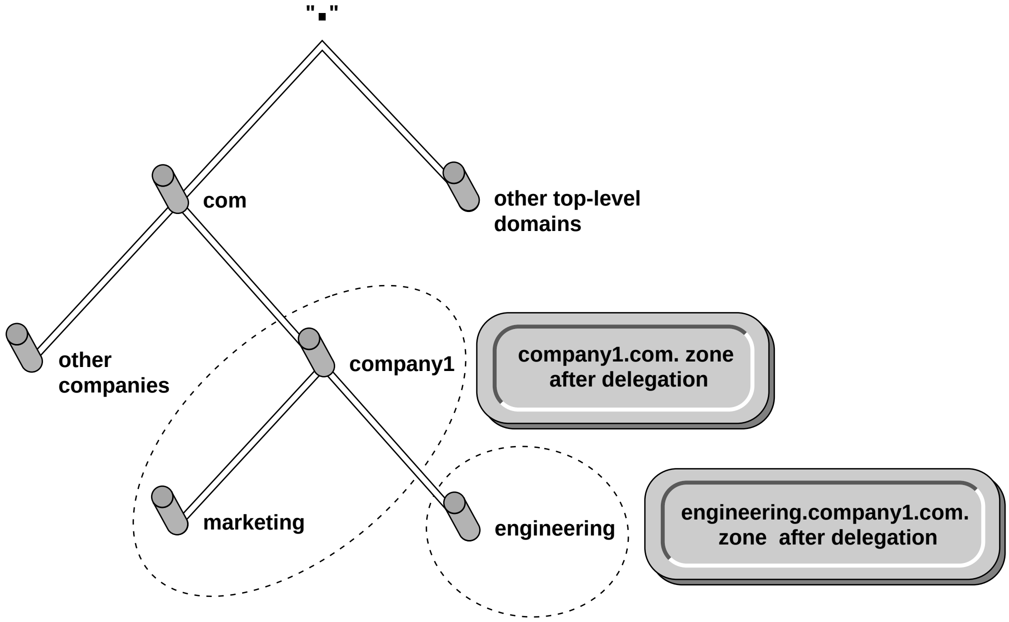


In addition to maintaining host information for a zone, the administrator also has the authority to create and delegate subdomains. For example, suppose the engineering division at company1 has its own administrator. Therefore, company1 delegates the engineering.company1.com. subdomain to the engineering division. The company1.com. zone no longer has authority over the engineering.company1.com. domain. Now the company1.com. domain comprises two zones:

- company1.com., which has authority over the company1.com. domain and the marketing.company1.com. subdomain
- engineering.company1.com., which has authority over the engineering.company1.com. subdomain

Figure 2-5 illustrates this example.

Figure 2-5
Domain Delegation


"."
com
other top-level domains
other companies
company1
company1.com. zone after delegation
marketing
engineering
engineering.company1.com. zone after delegation

DNS Name Service

The name service component of DNS provides the actual name-to-IP address mapping that allows computers to locate each other on an internetwork. The name service uses a client/server mechanism in which clients, called *resolvers* , query servers, called *name servers* , for host information.

Name Servers

DNS name servers are special servers that maintain a database of information about hosts in a specific zone. Each DNS zone must include a name server containing authoritative information for all hosts in the zone.

In addition to local host information, name servers maintain information about how to contact other name servers. As a result, all the name servers in an internetwork are able to contact each other and retrieve host information. If a name server does not have information about a particular domain, it relays the request to other name servers up or down the domain hierarchy until it receives an authoritative answer that it can relay to the client.

There are two types of name servers: master name servers and replica name servers.

Master Name Server

A single DNS name server in each administrative zone maintains an authoritative database of name and address information for that zone. The domain administrator updates this name server, referred to as the *master name server* , as hostnames and addresses within the zone change.

The master name server for each DNS zone in the DNS hierarchy also maintains information about how to contact name servers in higher-and lower-level zones. The administrator enters information into the database about name servers in lower-level domains when creating a new subzone. The administrator must also enter information about the name servers in higher-level domains. This process is called linking to the existing DNS hierarchy.

If a network maintains only one master name server that is linked to the DNS hierarchy, the administrator must configure all other name servers in the zone to *forward* their queries to that master. This process allows all the name servers to link to the DNS hierarchy indirectly.

Replica Name Server

You can create read-only copies of the DNS database for reliability and load balancing. The NetWare DNS service calls these read-only copies *replicas* . When the replica name server starts up, it contacts the master server and requests a complete copy of the DNS database. This process is called a *zone transfer* .

After the replica name server is set up, it is not necessary to manage the zone transfer process manually. The replica name servers query the master periodically and request an update when the replica detects a difference in the database information.

It is important to set up at least one replica name server for each zone. The replica can then function as a backup if the master server goes down. If necessary, a master name server can also function as a replica name server for another zone.

Resource Records

The host information maintained by the name servers is contained in *resource records* . Resource records make up the DNS database. Different types of records contain different types of host information. For example, an A or address record provides the name-to-address mapping for a given host, while an SOA record specifies the start of authority for the zone.

In a standard DNS implementation, the master name server for a zone must contain several types of resource records for DNS to function. Although other resource records may be present, the following records are required for a standard DNS implementation:

- **Start of Authority (SOA)** —indicates the start of authority for the zone. The name server must contain one SOA record specifying its zone of authority.

- **Address (A)** —provides name-to-address mapping for a specific host. The master name server must contain an address record for each host in the zone.

- **Name server (NS)** —binds a domain name with a hostname for a specific name server. The master name server must contain NS records for each master and replica name server in the zone. In addition, to link the zone to the DNS hierarchy, the master name server must contain NS records for the master name servers in higher- and lower-level zones.

For example, suppose the engineering.company1.com. zone contains a server (host1) and a name server (ns2). The master name server for the zone must contain the following:

- An SOA record identifying its zone of authority as engineering.company1.com.

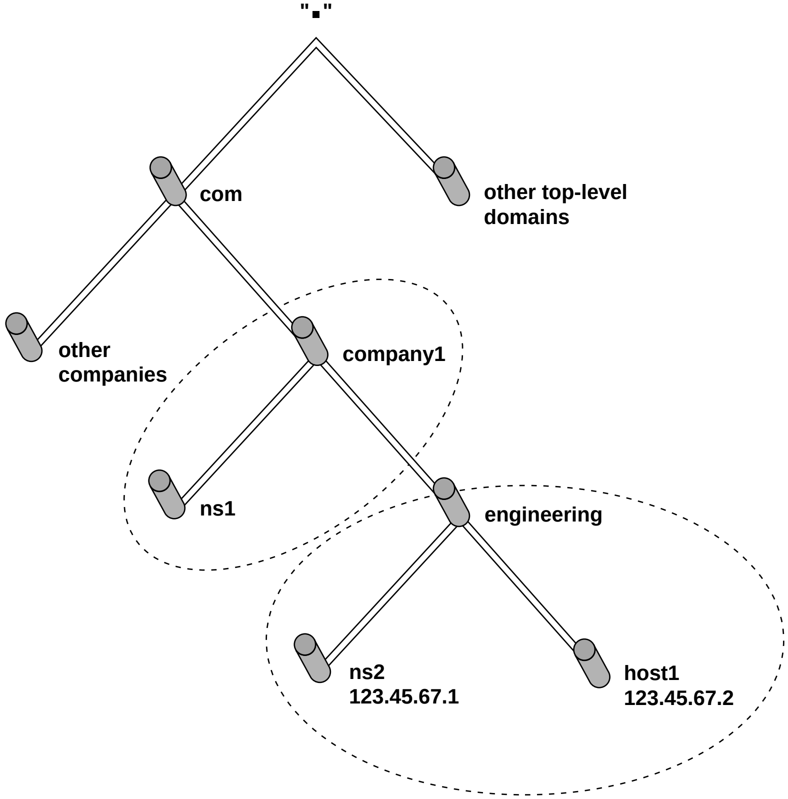
- An NS record for ns2

- Address records for host1 and ns2

- An NS record for the master name server, ns1, in the higher-level zone, company1.com.

Figure 2-6 illustrates this example and shows the resource records required for the engineering.company1.com. zone.

Figure 2-6
Required Resource Records



```
;Resource records for engineering.company1.com. zone

engineering.company1.com.          SOA  ns2.engineering.company1.com.
engineering.company1.com.          NS    ns2.engineering.company1.com.
company1.com.                      NS    ns1.company1.com.
ns2.engineering.company1.com.     A       123.45.67.1
host1.engineering.company1.com.  A       123.45.67.2
```

Resolution Process

Clients, or resolvers, send queries to the name server when trying to locate a host. It is then the responsibility of the name server to determine the answer to the query. This process is called *resolution* .

During the process of resolution, a name server receives a query to locate a host within the network. The name server first searches its own database to find the location of the host. If no record matches the query, the name server next issues a query to the top-level name server for its domain. The top-level domain name servers are called *root name servers* .

The root name server for a domain stores information about all the other top-level root name servers. Each root name server also stores information about the authoritative name servers for its second-level domains. When a query reaches the root name server, the name server can at least provide the name and address of the top-level name server for the domain containing the host for which the query was issued.

Figure 2-7 illustrates the resolution process.

1. The local name server, company1.com, queries the com domain root name server for the address of a host named host1.germany.company2.com.

2. The root name server for the com domain responds with a referral to the authoritative name server for the company2.com domain.

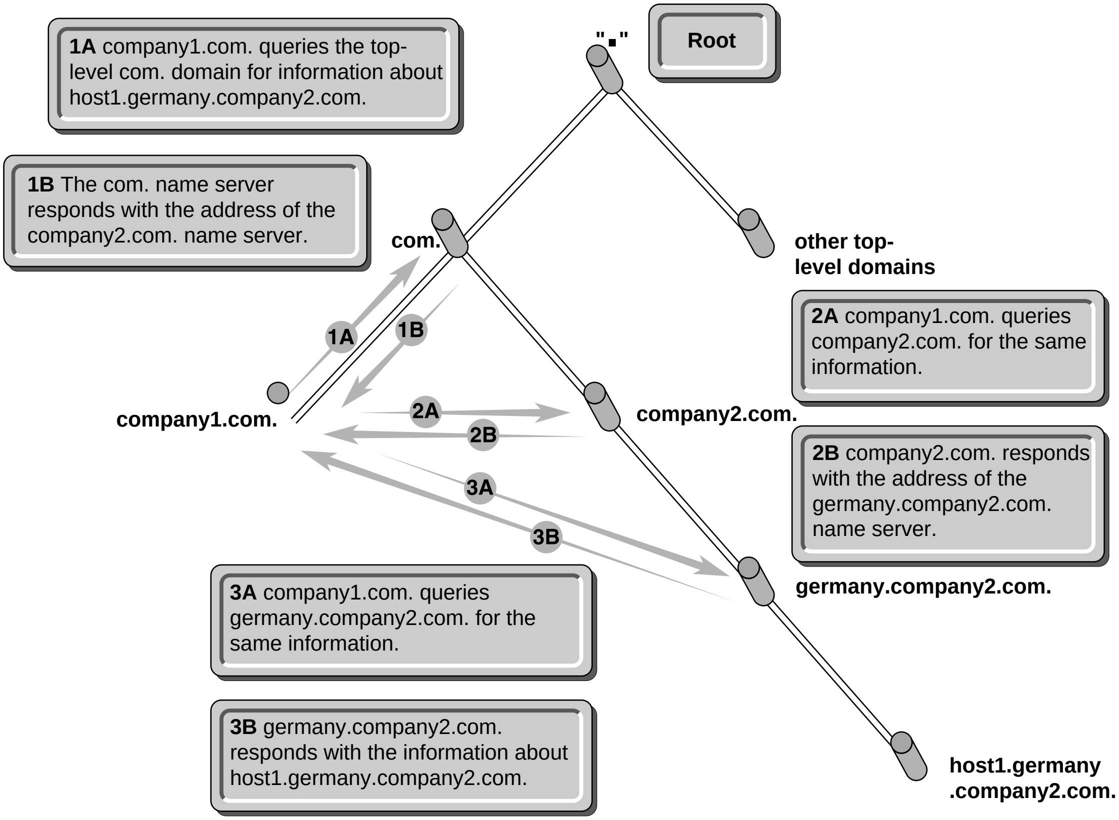
3. The local name server queries the company2.com name server for the same information.

4. The company2.com name server responds with a referral to the name server for the germany.company2.com domain.

5. The local name server queries the germany.company2.com name server.

6. The germany.company2.com name server sends an answer to the query.

Figure 2-7
Resolution Process


1A company1.com. queries the top-level com. domain for information about host1.germany.company2.com.
1B The com. name server responds with the address of the company2.com. name server.
"."
Root
com.
other top-level domains
1A
1B
company1.com.
2A
2B
company2.com.
2A company1.com. queries company2.com. for the same information.
2B company2.com. responds with the address of the germany.company2.com. name server.
3A
3B
germany.company2.com.
3A company1.com. queries germany.company2.com. for the same information.
3B germany.company2.com. responds with the information about host1.germany.company2.com.
host1.germany .company2.com.

Caching

The resolution process of sending out multiple queries can become complex and put an excessive load on the root name servers. To alleviate the load on the root name servers and speed up the resolution process, name servers use *caching* .

Each time a name server sends out a query, it receives multiple responses before receiving the correct response. When the name server receives a response, it caches the response automatically so that it already has the information the next time it receives a query. The amount of time the information stays in the cache is determined by the Time to Live (TTL) parameter. The TTL parameter is configured on the master name server that supplies the information. When the TTL expires, the name server discards the information.

For example, suppose that the local name server receives a query for host1.germany.company2.com. During a previous query, the local name server cached information that provided the address of the authoritative name server for the germany.company2.com domain. Using the cached information, the local name server can send the query directly to the authoritative name server. By using caching, the resolution process can skip two queries.

Caching is an automatic process that requires no configuration. You can also set up other methods to enhance the resolution process. Two of these methods, setting up a cache-only server and setting up a forwarder, are described in the following sections.

Cache-Only Server

In large networks, the resolution process can be enhanced by adding a *cache-only server* . A cache-only server has no database, so it must query other name servers to obtain information. After the cache-only server receives the information, it caches the information and can then respond to requests without querying other name servers.

The first step in balancing the load on a master server is to create replica servers. This practice is useful to a point, but if there are an excessive number of replica servers, the master spends too much time updating the replicas. This is when a cache-only server becomes useful. The cache-only server helps relieve the load without putting an extra burden on the master.

Forwarders

In some networks, a method that will reduce the amount of traffic generated by DNS queries during the resolution process is to set up a *forwarder* . A forwarder is a name server that processes all off-site DNS queries. As the forwarder responds to queries, it builds up a large cache of DNS information. As the cache of information grows, it is more likely that the forwarder can respond to a DNS query from information stored in the cache. This reduces the need to send queries to name servers located off-site.

No special configuration is required to set up a name server as a forwarder. Instead, all other name servers in the network must be configured so that they forward their queries to the name server designated as the forwarder. Using the UNICON utility, the NetWare DNS server can be configured to forward queries to a forwarder.

How NetWare/IP Uses DNS

NetWare/IP uses DNS for two purposes:

- All NetWare/IP nodes are united in a logical DNS domain called the NetWare/IP domain.

- NetWare/IP servers and clients use DNS to locate DSS servers within the NetWare/IP network or internetwork.

NetWare/IP does not require that the DNS service be resident on a NetWare platform. If you are already using DNS on your network, you can continue to use the existing DNS name server. However, the NetWare DNS service provides all the functionality of a standard DNS service without the configuration and management complexities. The NetWare DNS service is fully compatible with Berkeley Internet Name Domain (BIND 4.8.3). Using the DNS administration utility, UNICON, you can accomplish all NetWare DNS tasks by choosing options from a series of menus rather than editing configuration files.

Although the NetWare DNS service offers full DNS support, NetWare/IP uses only a small portion of the DNS capability. The following sections describe how NetWare/IP uses DNS.

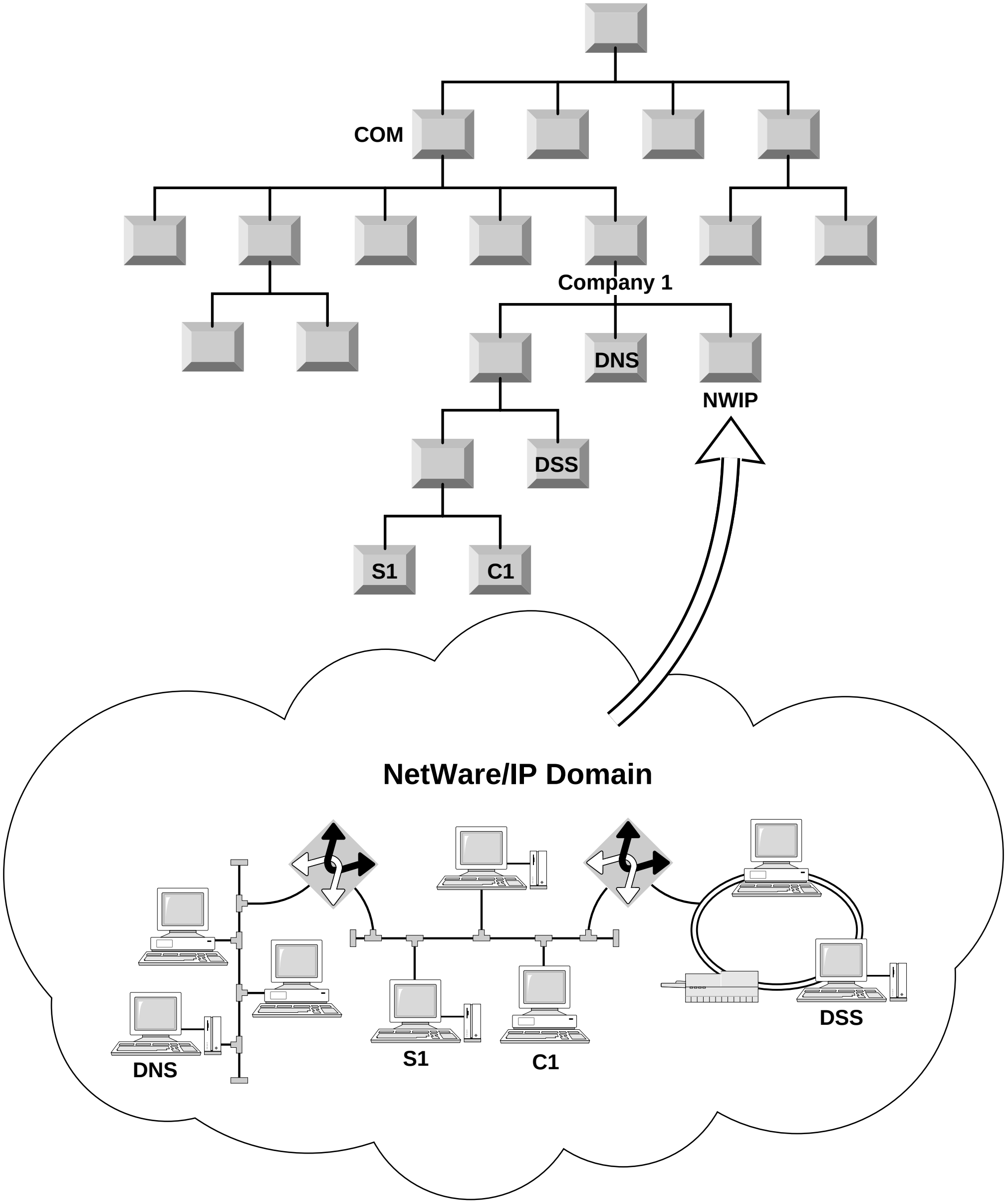
NetWare/IP Domain

To set up a NetWare/IP network, you must create and delegate a special DNS domain called the NetWare/IP domain. This domain is created in the same way as any other domain and, once created, appears in the DNS hierarchy just like any other domain.

However, the NetWare/IP domain is different from a standard DNS domain in that it always resides at the bottom of the DNS hierarchy with no subdomains or hosts. Instead, the hosts that make up the domain are distributed throughout the DNS hierarchy. The function of the NetWare/IP domain is to unite these distributed hosts into a logical network. Thus, even though the hosts are scattered throughout the domain name space, they are administered as a single logical network. All NetWare/IP nodes that belong to the same NetWare/IP domain are serviced by a single primary DSS server. Thus, the NetWare/IP domain also acts as a boundary for SAP and RIP information.

For example, suppose company1 decides to set up a NetWare/IP network. The administrator creates a NetWare/IP domain, nwip.company1.com., below the company1.com. domain. The company1 administrator then installs the NetWare/IP software on servers and clients that are distributed throughout the company1.com. zone and configures them as part of the DNS domain as well as the NetWare/IP domain, as shown in Figure 2-8 .

Figure 2-8
NetWare/IP Domain



NetWare/IP Use of Name Servers

NetWare/IP uses two different types of name servers:

- The DNS name server, which NetWare/IP servers and clients use to locate DSS servers for the NetWare/IP domain

- The DSS name server, which NetWare/IP servers and clients use to locate available services and routes within the NetWare/IP network

How NetWare/IP Uses the DNS Name Server

NetWare/IP uses a standard DNS name server to obtain information about the location of the DSS servers for the NetWare/IP domain. To do this, NetWare/IP requires a standard DNS name server in the parent domain of the NetWare/IP domain. The DNS name server must be modified to recognize the DSS servers as name servers for the NetWare/IP domain.

If DNS is already in use in the network, you can simply add an NS record for each DSS server in the NetWare/IP domain. If DNS is not already in use on the network, you must set up a DNS server and add NS and A records for each DSS server for the NetWare/IP domain and an SOA record for the DNS domain.

Note

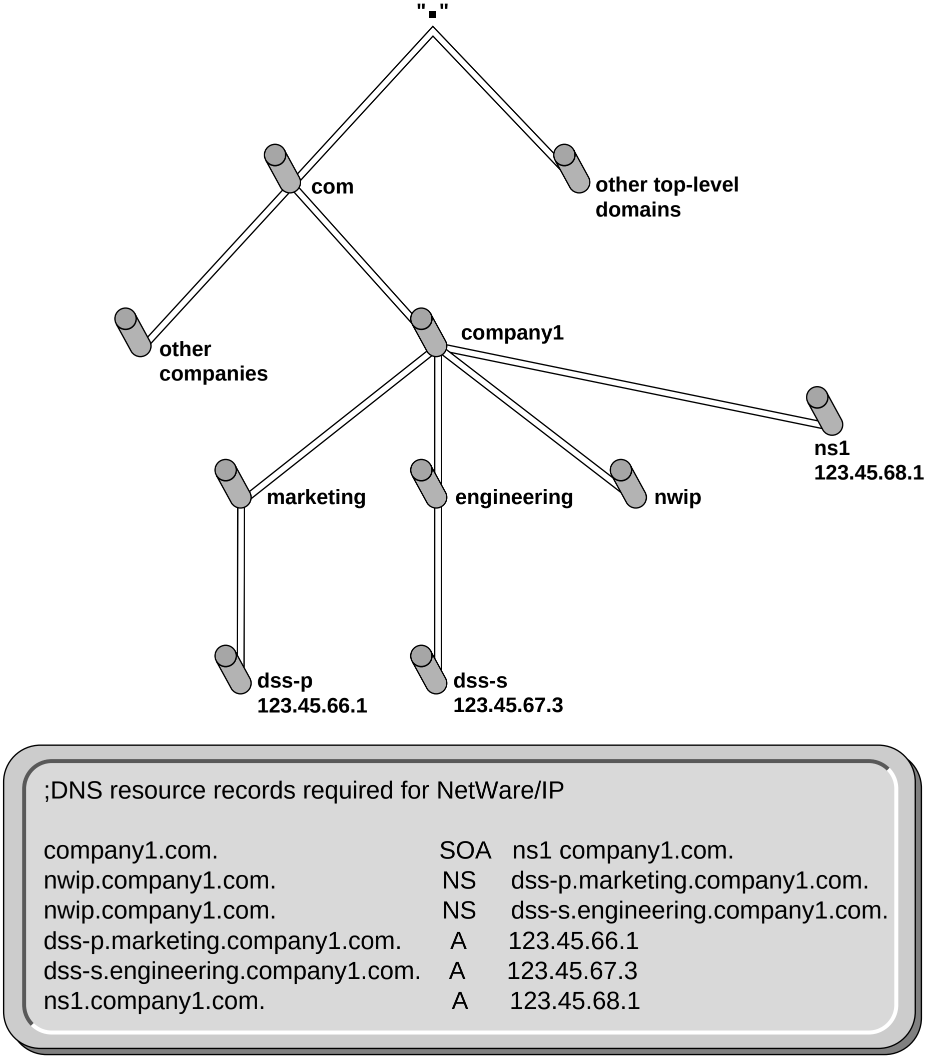
These are the only resource records required for NetWare/IP. NetWare/IP uses only a limited DNS service. Additional resource records would have to be added for the server to function as a standard DNS server within the domain name space.

For example, suppose company1 has two DSS servers, DSS-P and DSS-S, servicing its NetWare/IP domain, nwip.company1.com. The administrator must set up a DNS server in the company1.com. domain. The administrator must also add NS and A records for DSS-P and DSS-S and an SOA record for the company1.com. domain. This example is illustrated in Figure 2-9 .

If company1 wants to connect to the Internet or to other TCP/IP networks, the DNS database must also be populated with appropriate A records for all hosts in the zone and linked to the existing DNS hierarchy.

Figure 2-9

DNS Resource Records Required for NetWare/IP



```
;DNS resource records required for NetWare/IP

company1.com.                       SOA   ns1 company1.com.
nwip.company1.com.                  NS    dss-p.marketing.company1.com.
nwip.company1.com.                  NS    dss-s.engineering.company1.com.
dss-p.marketing.company1.com.       A     123.45.66.1
dss-s.engineering.company1.com.     A     123.45.67.3
ns1.company1.com.                   A     123.45.68.1
```

Each NetWare/IP server and client maintains information about the DNS and NetWare/IP domains in which it is administered and up to three DNS name servers it can contact. Then, when a system starts up, it queries each known DNS name server for the addresses of the available DSS servers for its NetWare/IP domain.

The DSS Server as a Name Server

DSS servers within the NetWare/IP network provide the second level of DNS name services. DSS servers are identified as name servers for the NetWare/IP domain. However, these name servers do not provide the standard name-to-address mapping services. Instead, they maintain information about the availability of services and routes in the network and distribute this information to NetWare/IP hosts as needed.

For more information on the purpose and function of DSS servers, see Chapter 3, “Understanding the Domain SAP/RIP Service,” on page 43

Chapter

3 *Understanding the Domain SAP/RIP Service*

This chapter provides information to help you understand the Domain SAP/RIP Service and how this service fits into a NetWare/IP™ network environment.

Overview

NetWare® servers on IPX™ networks broadcast Service Advertising Protocol (SAP) and Routing Information Protocol (RIP) packets every 60 seconds. These broadcasts circulate current information about available services and routes within the network. IP networks, however, do not support SAP/RIP broadcasts. Instead, the SAP and RIP information for the NetWare/IP internetwork is maintained in a centralized database called the Domain SAP/RIP Service (DSS).

As its name implies, DSS maintains current SAP and RIP information for a domain and distributes it to NetWare/IP servers throughout the domain upon request. DSS maintains information for a single NetWare/IP domain and supplies SAP and RIP information to all hosts that belong to the same NetWare/IP domain.

In the NetWare/IP environment, a DSS server must be set up on a NetWare server. This server does not need to be configured as a NetWare/IP server (it does not have to run NWIP.NLM). Nor does the server need an IPX interface: in a mixed IP–IPX environment, NetWare/IP servers configured as forwarding gateways supply DSS servers with SAP/RIP information for connected IPX segments. The only components required for a DSS server are the DSS NLM, which provides DSS capabilities, and the NAMED NLM, which services DNS SOA queries.

SAP/RIP Exchange

In a NetWare/IP internetwork, DSS servers and NetWare/IP servers and clients exchange SAP and RIP information using User Datagram Protocol (UDP) datagrams and Transmission Control Protocol (TCP) connections.

When a NetWare/IP server starts up, it queries DNS for the location of the DSS servers. It then sends SAP and RIP records to the nearest available DSS server, advertising its services to the NetWare/IP internetwork.

While the NetWare/IP server is running, it continues to resend SAP and RIP information to the DSS server at defined intervals. If a SAP or RIP record has not been updated within a specific time frame, the DSS server deletes the record. This ensures that the data maintained by DSS is accurate and timely.

In addition to sending SAP and RIP information to the DSS server, the NetWare/IP server also downloads a copy of updated DSS database records to a local memory cache at a preconfigured interval. When a NetWare/IP client system starts, it can then directly query the server for available network services.

DSS Server Replication

Any time a NetWare/IP server or client requests a network service, such as DISPLAY SERVERS or NLIST, it relies on information maintained by the DSS servers. Therefore, a DSS server must be available to all NetWare/IP nodes at all times. To provide redundancy and load balancing, NetWare/IP supports DSS server replication in which a single, authoritative DSS server is configured as the primary DSS server and one or more replicas are configured as secondary DSS servers. Each type of DSS server is described in the following sections.

Primary DSS Server

The primary DSS server maintains the master database of SAP and RIP information and is therefore the authoritative DSS server for the NetWare/IP domain. A single primary DSS server supports all servers and clients in a NetWare/IP domain. Because the performance of the NetWare/IP network depends on the performance of the primary DSS server, it is recommended that you designate as the primary DSS server a server that has relatively low use. If heavy NetWare/IP traffic is anticipated, a server may need to be dedicated to providing the primary DSS server capabilities.

In addition to maintaining the master SAP/RIP database, the primary DSS server supplies global configuration parameters used by all NetWare/IP nodes, such as the NetWare/IP domain name, the virtual IPX network number, and the UDP port numbers used for the NetWare/IP service. For more information on the global parameters maintained by the primary DSS server, see “Primary DSS Configuration Form” on page 116

Secondary DSS Server

To provide redundancy and load balancing for DSS on the NetWare/IP internetwork, one or more replica DSS servers, called secondary DSS servers, should be configured. Together, the primary DSS server and its secondaries form a distributed database of SAP/RIP information.

Each DSS server maintains a read-write copy of the global DSS database. This means that the secondary DSS server not only provides SAP/RIP information to its local NetWare/IP hosts, it also accepts SAP/RIP updates.

When a NetWare/IP server starts up, it registers its services with the closest available DSS server. This DSS server is then responsible for maintaining SAP/RIP data for the server and communicating the global communication parameters. Then, at a defined interval, the secondary DSS servers synchronize their databases with the primary DSS server, making the information registered with the secondaries available throughout the entire internetwork. Thus, the secondary DSS servers share the burden of maintaining SAP/RIP information for the internetwork.

When a secondary DSS server comes up for the first time, it must obtain and save global NetWare/IP parameters that come from the primary DSS server. The next time the secondary DSS server comes up, it again looks for the primary DSS server to obtain the current configuration. If it cannot find the primary DSS server, however, it defaults to the configuration it used the last time it was up.

Primary DSS–Secondary DSS Database Synchronization

The primary DSS server and its secondaries automatically synchronize their databases at an interval defined by the primary DSS server. Every DSS database file contains a version number that increments each time the file is updated. Before synchronization, the secondary DSS server compares its database file version number with the primary's version number. If the secondary determines that synchronization is necessary based on the database version number, it initiates a zone transfer.

During the zone transfer, the secondary DSS server uploads all new and changed SAP/RIP records registered at its database to the primary DSS database. Then the secondary DSS server downloads any records that have been changed or added to the primary DSS database since the last synchronization.

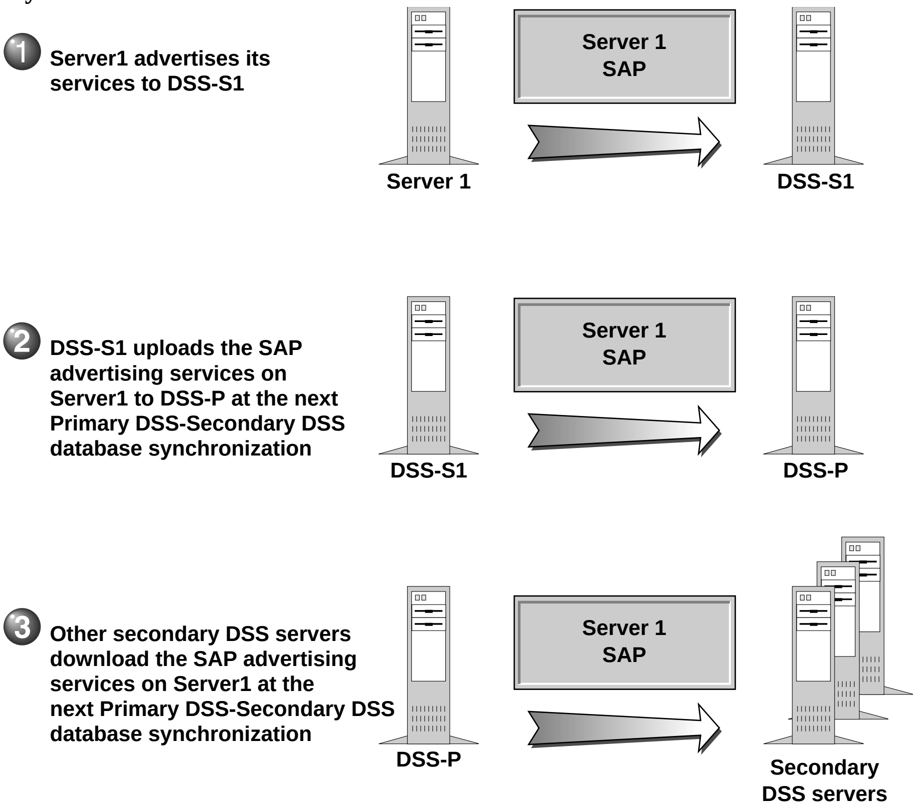
Service and routing information registered with a secondary DSS server is not available throughout the internetwork immediately. This is because SAP and RIP information passes from the secondary DSS server to the primary DSS server at the first database synchronization after a record is updated. The information is not transferred from the primary to the remaining secondaries until the next database synchronization.

Using the default database synchronization interval, which is five minutes, it could be up to 15 minutes (the equivalent of three database synchronization intervals) before newly advertised services are available throughout the entire NetWare/IP internetwork. Figure 3-1 illustrates the primary DSS–secondary DSS database synchronization process.

Note

If the primary DSS server is down, the secondaries cannot learn about any new services registered with other secondaries. They can learn only about new services from local hosts. When the primary DSS server comes back up, database synchronization resumes.

Figure 3-1
Database Synchronization


1
Server1 advertises its services to DSS-S1
Server 1
SAP
Server 1
DSS-S1
2
DSS-S1 uploads the SAP advertising services on Server1 to DSS-P at the next Primary DSS-Secondary DSS database synchronization
Server 1
SAP
DSS-S1
DSS-P
3
Other secondary DSS servers download the SAP advertising services on Server1 at the next Primary DSS-Secondary DSS database synchronization
Server 1
SAP
DSS-P
Secondary DSS servers

Filtering SAP Information

There are two methods you can use to manage the amount of SAP traffic generated on a NetWare/IP network.

IPX-Based Filtering

In an IPX-based NetWare network, an administrator can manage SAP and RIP traffic by implementing IPX filters. In particular, an administrator can implement service information filters to reduce the traffic associated with advertising services and routes throughout the network. In a mixed IP–IPX network, this type of filtering is still possible. And, because the best place to enable and configure filtering is where SAP and RIP traffic are generated, IPX-based filtering is most effective when configured at each NetWare/IP server that is configured as a forwarding gateway. For more information about NetWare/IP gateways, see “Gateway Configuration” on page 54

To enable IPX-based filtering, you use the Internetworking Configuration (INETCFG) utility to enable filtering and the Filter Configuration (FILTCFG) utility to define the filters. For instructions on enabling and configuring IPX-based filtering, see “Configuring Other Filtering Options” on page 135

DSS SAP Filtering

In addition to IPX filtering, an administrator can manage SAP traffic by implementing filters in DSS. DSS SAP filters, when applied, allow only SAP traffic that meets specified criteria to be replicated to other DSS servers. DSS SAP filters are applied globally. Every DSS server uses the same set of filters to determine whether or not SAP information should be shared.

If DSS SAP filtering is enabled, each SAP packet received by a DSS server is checked against the defined filters. If the packet matches a filter, the information is flagged as global and is replicated when the DSS servers synchronize. If the packet does not match a filter, the information is flagged as local and is not replicated.

For more information on DSS SAP filtering, see “DSS SAP Filtering Configuration Form” on page 118

DSS Server Types

There are two types of DSS servers: registered and unregistered. Both primary and secondary DSS servers can be either registered or unregistered.

Registered DSS Server

A registered DSS server is visible to all NetWare/IP nodes through DNS. Each registered DSS server has a corresponding NS record in the DNS database that identifies it as a name server for the NetWare/IP domain. When a NetWare/IP host queries DNS for the location of the nearest DSS server, DNS will return only a list of registered DSS servers, because these are the only DSS servers it knows about.

Unregistered DSS Server

An unregistered DSS server is not registered with DNS. Thus, a NetWare/IP node cannot locate an unregistered DSS server by issuing a DNS query. Instead, the NetWare/IP node must be provided with the name or address of the unregistered DSS server as part of its preferred DSS server list. For example, you might 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 to prevent NetWare/IP servers from redirecting their queries to this DSS server when other, closer DSS servers are busy or down.

DSS Server Selection

The method a host uses to locate and choose a DSS server depends on the host's configuration. The two possible methods are to query DNS or to use a preferred DSS server list.

DNS Query

DNS query is the default method NetWare/IP servers and clients use to locate a DSS server. The DNS database for the parent domain of the NetWare/IP domain maintains information about all registered DSS servers in the NetWare/IP domain. All NetWare/IP servers and clients are configured as DNS clients, or resolvers. A NetWare/IP host uses the following process to query DNS:

1. The NetWare/IP host queries the DNS name server for a list of all DSS servers.

2. DNS replies with a list of all registered DSS servers in the NetWare/IP domain.

3. The host sorts the list based on IP address and/or subnetwork address, placing those DSS servers that it determines as being closest at the top of the list.

4. The host attempts to communicate with each DSS server on the list, beginning with the first DSS server, until it finds an active DSS server.

For more information on DNS, see Chapter 2, "Understanding the Domain Name System," on page 23

Preferred DSS Server List

As an alternative to using DNS to locate a DSS server, NetWare/IP servers and clients can be configured with a list of up to five preferred DSS servers. A NetWare/IP host uses the following process when a preferred DSS server list is configured at the host:

1. When a NetWare/IP server or client starts up, it tries to contact each DSS server on its preferred list to exchange SAP/RIP information, bypassing the DNS name server.

2. If the host cannot communicate with any of the DSS servers on its preferred list, it then queries the DNS name server for an alternate list of DSS servers to try.

Monitoring and Troubleshooting DSS Servers

The performance of the NetWare/IP internetwork hinges on the performance of DSS. Therefore, NetWare/IP includes features to aid in monitoring and troubleshooting DSS performance.

DSS Browser

The DSS Browser is a menu-driven troubleshooting tool included as part of the DSS administration utility, UNICON. This tool allows you to investigate network problems by viewing selected SAP or RIP records stored in a primary or secondary DSS database. Using the DSS Browser, you can view all SAP or RIP records for a given DSS server. Or, you can narrow your search by choosing one of the following display options:

- SAP records of a specific type

- SAP records for a given server name or group of server names

- RIP records for a specific IPX network number

Additionally, you can use the DSS Browser to save all SAP or RIP records for a given DSS server to a text file. For more information on the DSS Browser, see “Troubleshooting DSS Servers” on page 162

SNMP Reporting

DSS servers can be configured to register with Simple Network Management Protocol (SNMP) management stations. The purpose of SNMP is to notify a network manager when system problems occur. When a DSS server is registered with SNMP, it reports information about itself, such as its type, database version number, and database synchronization intervals, to a designated SNMP management station.

For more information on SNMP, see “Managing SNMP Reporting” on page 155

Chapter

4 *Understanding the NetWare/IP Server and Client Software*

This chapter provides information to help you understand the NetWare/IP™ server and client software modules.

Understanding the NetWare/IP Server

A NetWare/IP server is a NetWare 4 server with the following additional NetWare Loadable Modules (NLMs) loaded:

- TCPIP and related NLMs, which provide the TCP/IP transport. These NLMs are included with NetWare 4.
- NWIP.NLM, which provides the NetWare/IP service.

The following sections describe the configuration options available with the NetWare/IP server.

Server Configuration

A NetWare/IP server provides NetWare services to nodes on a TCP/IP network. Unlike an IPX-based NetWare server, the NetWare/IP server accepts TCP and UDP packets. A NetWare/IP server stores the name of its NetWare/IP domain as part of its local configuration. The NetWare/IP server may also store configuration information locally that customizes how it communicates with the DSS servers and with nodes on remote network segments. For more information on NetWare/IP server configuration parameters, see “NetWare/IP Server Configuration Form” on page 141

In addition to its own local configuration information, the NetWare/IP server also obtains global configuration information from a DSS server, such as the virtual IPX network number, UDP port numbers, and DSS–NetWare/IP synchronization interval.

To start the first time, a NetWare/IP server must obtain the network configuration from a DSS server. The NetWare/IP server then saves the parameters to a local file. The next time the NetWare/IP server comes up, it again looks for a DSS server to obtain the current configuration. However, if it cannot find the DSS server, it defaults to the configuration it used the last time it was up.

Gateway Configuration

By default, the NetWare/IP server provides services to TCP/IP nodes only. However, if you have a mixed IP–IPX internetwork, you might want to configure one or more NetWare/IP servers to act as gateways to provide connectivity between IP and IPX networks. A NetWare/IP gateway has both an IP interface and an IPX interface (meaning that TCP/IP and IPX are bound to a network board in the server), which allows it to accept IPX packets in addition to UDP and TCP packets.

There are two types of NetWare/IP gateways: forwarding gateways and non-forwarding gateways.

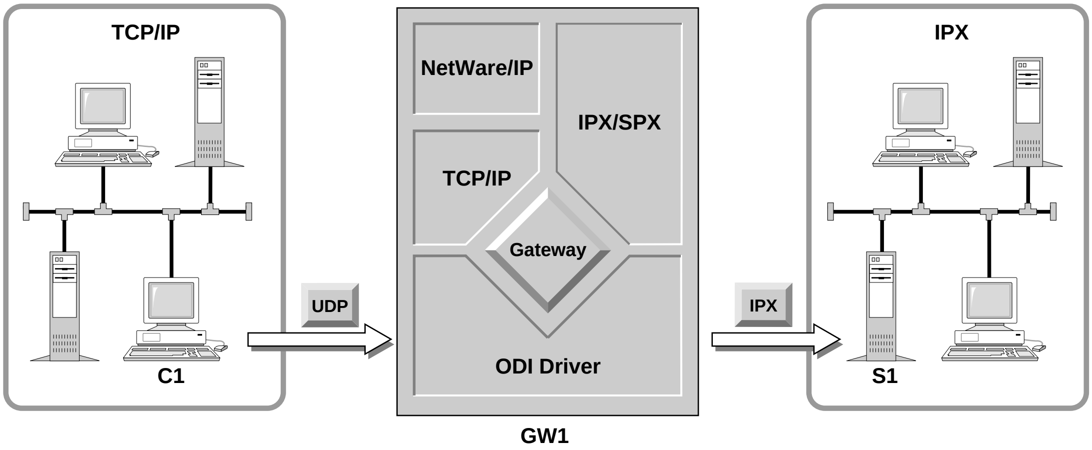
Forwarding Gateways

A forwarding gateway connects separate IP and IPX networks, providing both IP and IPX clients with seamless access to services on either network. This type of gateway forwards packets between the two networks, performing protocol conversion as required.

For example, suppose company1 wants to interconnect a TCP/IP network in its marketing division with an IPX network in its sales division. Company1 sets up a forwarding NetWare/IP gateway, GW1, between the two networks, as shown in Figure 4-1 . Once the gateway is configured, client C1 on the TCP/IP network can access a service provided by server S1 on the IPX network. NetWare/IP automatically routes the service request packet from C1 to the forwarding gateway. The gateway converts the packet from UDP to IPX and then forwards the packet to S1.

Figure 4-1

Forwarding Gateway



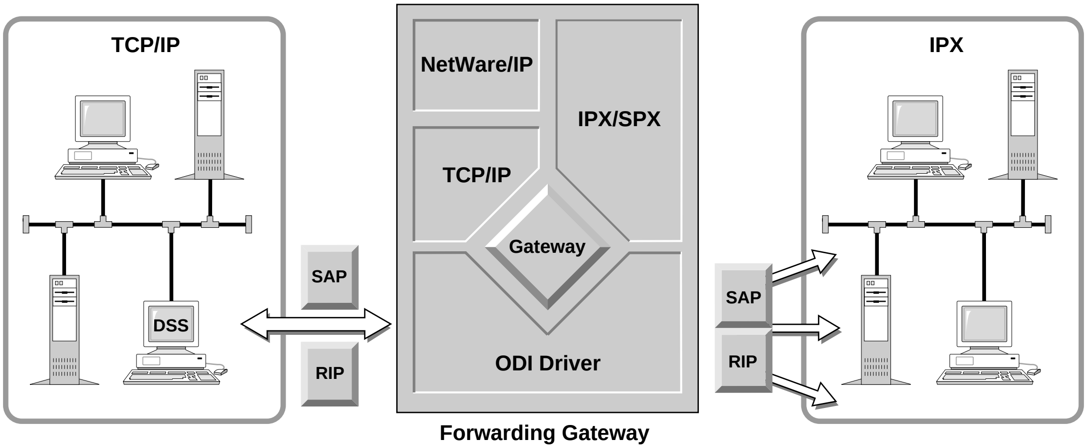
In addition to translating packets and passing them from one network segment to another, the forwarding NetWare/IP gateway is also responsible for communicating service and routing information between the IP and IPX subnetworks.

On an IPX network, services and routes are advertised using SAP and RIP broadcasting. The forwarding gateway accepts the IPX SAP and RIP broadcasts through its IPX interface and uploads them directly to the DSS server. This enables NetWare/IP servers and clients to learn about services and routes on the IPX network.

Similarly, the forwarding NetWare/IP gateway downloads SAP/RIP information for the IP network segment from the DSS server. Then, to advertise the IP services and routes, the gateway broadcasts the SAP and RIP information it downloaded from the DSS server to the IPX network. This enables NetWare servers and clients on the IPX network to learn about services and routes on the IP network. SAP/RIP forwarding is illustrated in Figure 4-2 .

Figure 4-2

SAP/RIP Forwarding



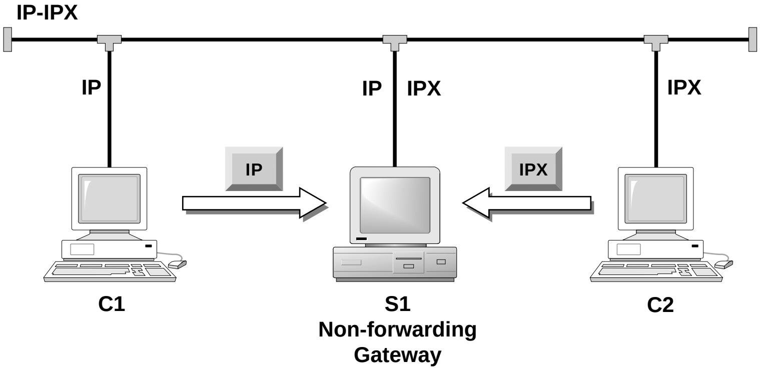
Because forwarding gateways may become heavily loaded with traffic between the two network segments, you should consider dedicating the gateway machine. Additionally, to prevent routing loops, it is recommended that you do not configure more than two forwarding gateways per network pair.

Non-forwarding Gateways

A non-forwarding gateway is simply a NetWare/IP server with both an IP and an IPX interface. The purpose of the non-forwarding gateway is to provide both IP and IPX clients with direct access to its services. If you have a mixed IP–IPX subnetwork, you may want to configure one or more NetWare/IP servers as non-forwarding gateways.

For example, the Engineering subnetwork at company1 has both an IP client, C1, and an IPX client, C2. Therefore, company1 configures server S1 as a non-forwarding gateway, as shown in Figure 4-3 . This allows S1 to accept UDP packets from C1 through its IP interface and IPX packets from C2 through its IPX interface.

Figure 4-3
Non-forwarding Gateway



Non-forwarding Gateways as One-way Gateways

With previous versions of NetWare/IP, the default configuration for a non-forwarding gateway enabled IPX clients to see and access IP services, but it did not enable IP hosts to see or access IPX services. Prior to NetWare/IP 2.2, a non-forwarding gateway actually functioned as a one-way forwarding gateway, providing IPX clients with access to IP services. This occurred because NetWare received information about the IP network from the NetWare/IP service and internally routed it to all existing IPX networks that it knew about.

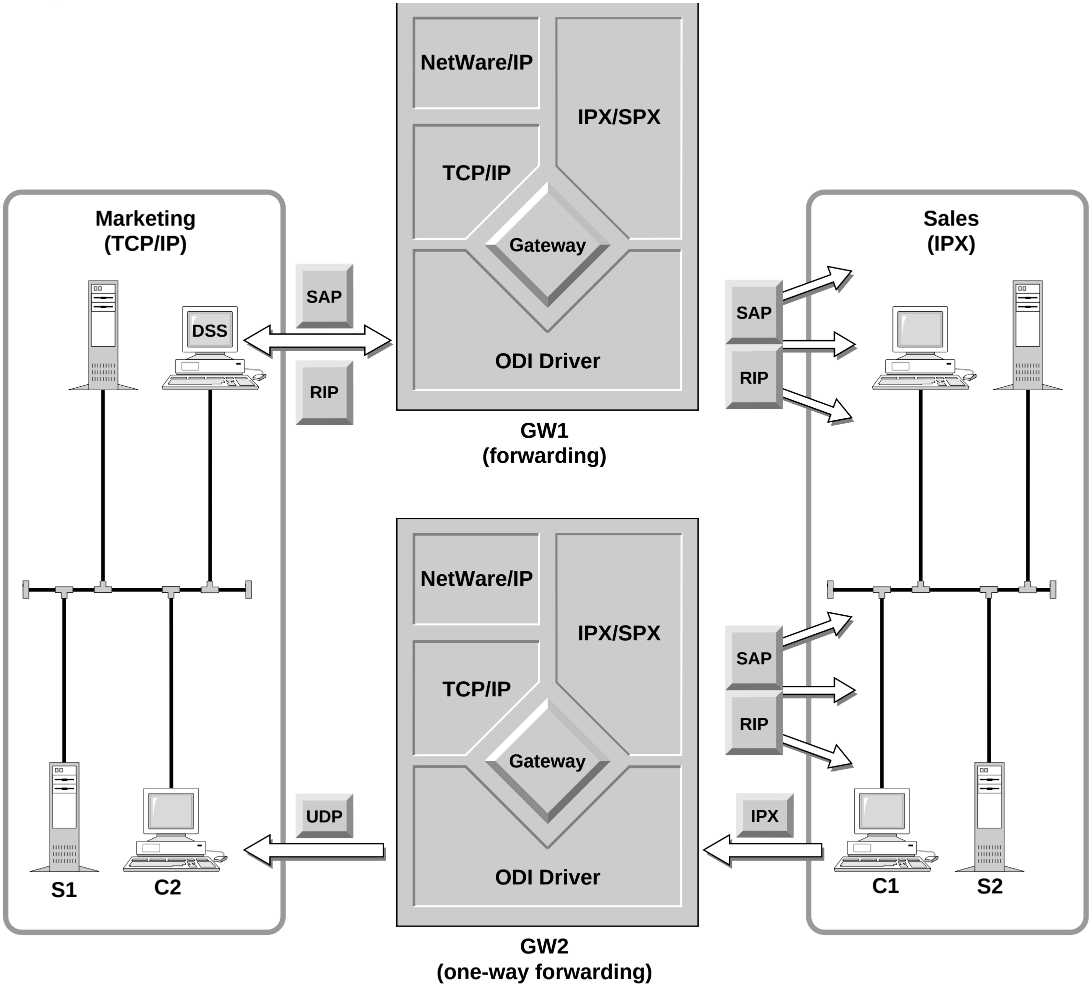
With NetWare/IP 2.2, the server software is configured with the internal routing feature disabled. This means that by default, a non-forwarding gateway does not function as a one-way forwarding gateway. IP network information is not forwarded to the IPX network.

To enable a non-forwarding gateway to function as a one-way forwarding gateway, you need to enable the internal routing feature. You might choose to do this in a few situations to provide one-way load balancing for a heavily used forwarding gateway (balancing the load for IPX to IP communications).

For example, company1 wants to reduce the load on the forwarding gateway between its TCP/IP and IPX subnetworks by configuring a one-way forwarding gateway, GW2, as shown in Figure 4-4 . Client C1 on the IPX segment learns about services provided by S1 on the IP segment through SAP and RIP broadcasts from both GW1 and GW2. Thus, C1 can access services on S1 either through GW1 or GW2. However, C2 can access services only on server S2 through the forwarding gateway, GW1. This is because the forwarding gateway is the only known route from the IP segment to S2 because it is the only server that reported the S2 SAP and RIP information to DSS.

Figure 4-4

Forwarding and One-way Forwarding Gateway Configuration



Understanding the NetWare/IP Client

The NetWare/IP client software extends NetWare capabilities to DOS and Windows workstations on TCP/IP networks. With NetWare/IP, NetWare services and applications run the same as they run in IPX-based NetWare environments.

The NetWare/IP client discussed in the following sections refers to a version of the NetWare DOS Requester client, a 16-bit, VLM-based NetWare client, that has been enhanced to include software modules required to access NetWare/IP networks.

In addition to the 16-bit, VLM-based NetWare/IP client discussed in this section, the following NetWare clients can access a NetWare/IP network when properly configured:

- NetWare Client 32 for Windows 95
- NetWare Client 32 for DOS and Windows
- NetWare Client 32 for Windows NT
- NetWare Client for Mac OS

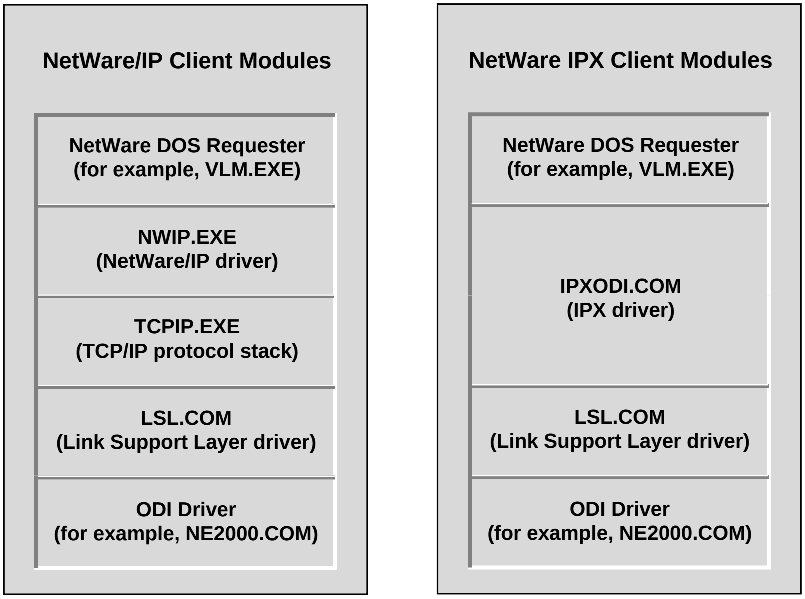
Client Software

To provide seamless connectivity in a TCP/IP environment, the NetWare/IP client uses the same Link Support Layer™ (LSL™) driver, Open Data-Link Interface™ (ODI™) driver, and NetWare DOS Requester™ as an IPX-based NetWare client. However, to provide the TCP/IP transport, the IPX driver is replaced by the following software modules in NetWare/IP:

- TCPIP.EXE, which provides the TCP/IP protocol stack
- NWIP.EXE, which provides the NetWare/IP driver

Figure 4-5 compares the NetWare/IP client with the IPX-based client modules.

Figure 4-5
NetWare/IP Client NetWare Client Comparison



Client Configuration

A NetWare/IP client uses values assigned to both local and global configuration parameters to run.

Local Parameters

Some local configuration parameters are required, and some are optional.

Required Parameters

The NetWare/IP client requires the following local parameter values at startup. All of these required parameters must be configured during installation, unless you are using a Dynamic Host Configuration Protocol (DHCP) server:

- IP address, which specifies the IP address of the client system
- Subnetwork mask, which specifies the subnetwork mask for the TCP/IP network

- Default router, which specifies the IP address of the default router, if any, for this subnetwork
- DNS domain, which specifies the default DNS domain name
- Default DNS name servers, which specifies the IP addresses of up to three DNS name servers for the DNS domain
- NetWare/IP domain, which specifies the NetWare/IP domain to which this client belongs

Optional Parameters

The NetWare/IP client may optionally use values for the following parameters to optimize performance:

- Initial DSS contact retries, which specifies the number of times the client will attempt to communicate with a given DSS server at startup. The default is one retry in a range of 0 to 50.
- Retry interval, which specifies the time interval in seconds between attempts to retry communicating with a given DSS server at startup. The default is 10 seconds in a range of 5 to 100 seconds.
- Preferred DSS servers, which specifies the hostnames, IP addresses, or subnetwork IP addresses of up to five DSS servers that are closest to this client.
- Nearest server, which specifies the hostname, IP address, or subnetwork IP address of the NetWare/IP server closest to this client.
- NSQ broadcast, which specifies whether this client will use Nearest Server Query (NSQ) broadcasts to locate the nearest server. By default, NSQ broadcast is set to on.
- NetWare/IP 1.1 compatibility, which specifies whether this client can access NetWare/IP 1.1 servers. By default, NetWare/IP 1.1 compatibility is set to off.

Obtaining Local Parameter Values

A NetWare/IP client obtains its local configuration from configuration files or from a Dynamic Host Configuration Protocol (DHCP) server.

Configuration Files

The NetWare/IP client configuration is stored in the following two files:

- NET.CFG, which contains TCP/IP and NetWare/IP configuration information

- RESOLV.CFG, which contains DNS client (resolver) configuration information

You can edit the configuration information stored in these files using any text editor.

DHCP Servers

A DHCP server contains a database of client configuration information. If the NetWare/IP client cannot find its local configuration in its NET.CFG file, it queries the DHCP server. The location of the client configuration information is determined at installation. If a DHCP server is not used, you must manually configure the client at installation.

For more information on using a DHCP server, see Chapter 12, “Configuring a DHCP Server,” on page 195

Global Parameters

In addition to the local parameters, the NetWare/IP client also obtains network-wide configuration information from DSS, such as the virtual IPX network number, UDP port numbers for NetWare/IP service, and DSS–NetWare/IP synchronization interval.

To start up the first time, a NetWare/IP client must obtain global configuration parameters from a DSS or NetWare/IP server. The client then saves the parameters to a local file. The next time the client starts up, it again looks for a DSS or NetWare/IP server to obtain the current configuration. However, if it cannot find a server, it defaults to the configuration it used the last time it was running.

Client Startup Process

The NetWare/IP client requires that TCP/IP be loaded and ready before NetWare/IP can run. When TCP/IP is ready, the NetWare/IP client starts up as follows:

1. The client obtains its local configuration parameters using one of the following methods:
   - It reads the local NET.CFG and RESOLV.CFG files.
   - It contacts a DHCP server.
2. The client obtains network-wide parameters from a NetWare/IP or DSS server. The client locates a NetWare/IP or DSS server using one of the following methods:
   - It contacts the nearest NetWare/IP or DSS server listed in its local configuration files.
   - It sends a UDP broadcast to contact the nearest NetWare/IP server. This requires that the NSQ_BROADCAST statement in the NET.CFG file is set to ON (as it is by default).
   - It queries the DNS service.

Limitations on Client Access

Currently, NetWare/IP imposes the following limitations on client access to NetWare services:

- NetWare/IP clients can access NetWare (IPX) printers only if there is a forwarding gateway between the IPX segment on which the printer is located and the IP backbone.
- NetWare/IP supports IPX NetBIOS only on local subnetworks: IPX NetBIOS broadcasts do not carry across IP routers. If you need NetBIOS capability over TCP/IP, you can substitute the RFCNBIOS program provided with the NetWare/IP software.

Chapter

5 *Installing the NetWare/IP Software*

This chapter describes how to install the NetWare/IP™ software. This chapter includes information on the following:

- Preparing to install a NetWare/IP network
- Installing the NetWare/IP server software
- Installing the NetWare/IP client software
- Installing and viewing the online documentation

Note For last-minute information that is not included in this manual, refer to the README.TXT and README.1ST files included in the \NWIP directory on the *NetWare Installation* CD-ROM.

Preparing to Install a NetWare/IP Network

The NetWare/IP software must be installed and configured in a specific manner. The information in this section is provided to help you successfully install and configure a NetWare/IP network. Read this section carefully before installing the NetWare/IP software.

Planning the Network

Planning is an essential step in setting up the NetWare/IP software. You must plan a NetWare/IP internetwork before installing the software. Careful planning enables you to

- Optimize network performance
- Accommodate growth
- Provide redundancy and load balancing

- Minimize traffic

For additional information on planning a NetWare/IP network and using planning worksheets, see Appendix A, “Planning a NetWare/IP Network,” on page 219

Important

Each server on which you install the NetWare/IP software must be configured to use the TCP/IP (TCPIP.NLM) transport protocol.

The following checklist summarizes the considerations behind these decisions:

□ Identify a server to be the master DNS name server for your DNS domain.

- This system can be a NetWare® server or a non-NetWare machine.
- If you choose a NetWare server, you must configure it using the NetWare/IP DNS modules; DNS modules from other NetWare products may not fully support NetWare/IP.
- If you are setting up a new master DNS name server for a new Internet domain, you must configure a higher-level master DNS name server with records identifying the new master DNS name server.

□ Identify the system(s) to be the replica DNS name server(s).

- At least one replica DNS name server is recommended to provide redundancy and load balancing.
- Any network segment that connects to the master DNS name server over slow-speed links or via routers needs a local replica DNS name server.

□ Choose a NetWare server to be the primary DSS server.

- This server's performance can affect the entire NetWare/IP network.
- If there will be a large number of networked systems on the backbone, consider dedicating this server as a DSS server only.
- If the network includes slow-speed links, consider using DSS-based SAP filters.
- Provide at least 4 MB of free disk space on the SYS: volume.

- Use the following formula to determine the memory requirements for the primary DSS server, where *a* equals the number of servers in the network:

  (*a* x 520) + 835,000 = memory in bytes needed on the server

- If the server is not configured as a DNS server, configure it as a DNS client.

□ Choose secondary DSS servers.

- Configure one secondary DSS server at each large site.
- Configure additional DSS servers on backbones where you anticipate heavy traffic.
- Configure an unregistered DSS server on network segments interconnected by WAN links to reduce DNS query traffic.
- Provide at least 4 MB free disk space on the SYS: volume.
- Use the formula provided for the primary DSS server to determine the memory requirements for a secondary DSS server.
- If the server does not have DNS access set up, configure it as a DNS client.

□ Determine which servers to configure as NetWare/IP servers.

- Provide at least 4 MB of free disk space on the SYS: volume.
- Use the following formula to determine the memory requirements for a NetWare/IP server, where *a* equals the number of servers in the network:

  (*a* x 380) + 258,000 = memory in bytes needed on the server

- If the server is not configured as a DNS server, configure it as a DNS client.

□ Determine which NetWare/IP servers to configure as gateways.

- Forwarding gateways are needed between the TCP/IP network and IPX-only network segments. Do not configure more than two forwarding gateways per network segment pair.
- Non-forwarding gateways can be configured on mixed IP–IPX network segments to provide direct service to both IP and IPX clients.

- Each gateway system requires both a TCP/IP interface and an IPX interface.
- Both interfaces can use the same network board; however, separate network boards are recommended for load balancing.

□ Choose a NetWare/IP domain name.

- The domain can be anywhere within the DNS hierarchy.
- The domain cannot have any subdomains.
- Make sure you have permission to administer the master DNS name server for the parent domain.
- The NetWare/IP domain and the NetWare Directory Services™ (NDS™) tree should coincide. Your Directory tree cannot span multiple NetWare/IP domains.

□ Choose an IPX™ network number for the NetWare/IP network (must be unique throughout your IPX internetwork).

Upgrading NetWare/IP

When you run the NetWare/IP installation program, it detects whether or not NetWare/IP is already installed on the server and prompts you to uninstall the existing software. The installation program can uninstall the software for you. You must uninstall an existing version of NetWare/IP before the installation program can proceed.

You do not have to upgrade all NetWare/IP nodes at the same time. All versions of NetWare/IP can coexist. However, to optimize network performance you should upgrade your systems using the following migration sequence:

1. Upgrade NetWare DNS name servers.

   In NetWare/IP 2.1 and later, the NetWare DNS database is stored in Btrieve* files rather than text files. Therefore, if you are upgrading from a version previous to NetWare/IP 2.1, you should back up the NetWare DNS databases before upgrading the software. The DNS database is stored in the server's SYS:ETC\DNS directory.

2. Upgrade the primary DSS server.

3. Upgrade the secondary DSS servers. To optimize DSS performance, you should upgrade all DSS servers in the network.

4. Upgrade forwarding gateways.

   In previous versions of NetWare/IP, all NetWare/IP servers were configured to act as forwarding gateways by default. In NetWare/IP 2.1 and later, you must manually enable the forwarding feature when you configure the server, as described in “Configuring a NetWare/IP Server as a Gateway” on page 143

5. Upgrade NetWare/IP servers.

6. Upgrade NetWare/IP clients.

Migrating from IPX to IP

You can use NetWare/IP to migrate a network from IPX to IP. As you extend NetWare/IP to additional TCP/IP network segments, IPX services and clients can continue to run unchanged. For a sample migration path, see “Sample NetWare/IP Configurations” on page 219

As you migrate, you might identify portions of the network that should remain IPX-based. For example, certain print services and platform-dependent applications cannot be migrated to NetWare/IP. Or, you might have a dedicated-IPX departmental subnetwork that you do not want to convert to TCP/IP.

To interconnect IP and IPX network segments, you can configure a NetWare/IP server to act as a gateway. For more information on NetWare/IP gateways, see “Gateway Configuration” on page 54

Integrating NDS and NetWare/IP

NetWare Directory Services (NDS) is a global, distributed database that contains information about all resources, or objects, in a NetWare network, including users, servers, workstations, printers, and volumes. These objects are organized in a hierarchical tree structure called the Directory tree. The Directory tree is made up of database files that can be partially or wholly replicated on servers throughout the Directory tree. Thus, all servers in the Directory tree must be able to communicate with each other to maintain the Directory database.

Because NDS acts as a boundary for the NetWare network, data cannot be shared across Directory trees. Similarly, the NetWare/IP domain acts as a boundary for the NetWare/IP network; data cannot be shared across NetWare/IP domains. Therefore, when planning a NetWare/IP internetwork, you should plan for the NetWare/IP domain and the Directory tree to coincide.

If you plan to set up multiple NetWare/IP domains, you must also set up a separate Directory tree for each NetWare/IP domain. This is because all servers in a Directory tree must be able to communicate to maintain the Directory database. However, servers in different NetWare/IP domains cannot communicate.

Note

It is possible to have multiple Directory trees in a single NetWare/IP domain; however, you should consider using a single NetWare/IP domain and a single Directory tree within your organization to take advantage of the global features provided by NetWare/IP and NDS.

For more information on NDS, refer to *Guide to NetWare 4 Networks* .

Planning Print Services

When planning a NetWare/IP network, you must consider how to provide print services on the network. The solution depends on whether you plan to use printers that require the TCP/IP transport.

If you plan to use NetWare/IP in an IP-only environment or plan to use a printer that is attached to an IP-based host (a UNIX® server or workstation) you need to configure a gateway that enables the UNIX printing protocol, lpr. For more information on configuring an lpr gateway, see Chapter 13, “Configuring NetWare-to-UNIX Printing,” on page 211

If your network uses both IPX and TCP/IP, you can provide NetWare print services to NetWare/IP clients by locating NetWare print services on mixed IP–IPX or IPX-only network segments. For NetWare/IP clients to access print services, you need to configure a forwarding gateway between any IP-only segments and the IPX segments on which you install NetWare print services.

Specifying Frame Types

Frame types determine how packets of network data are formatted. To communicate, nodes must be configured to use the same frame type.

The default ethernet frame type for NetWare 4 is Ethernet 802.2. However, the NetWare TCP/IP stack used with NetWare/IP requires that you use the Ethernet_II frame type to communicate with other TCP/IP nodes. Therefore, you must specify the Ethernet_II frame type when you load the LAN driver.

For example, to load the NE2000™ LAN driver using Ethernet_II frames and bind IP to the NE2000 interface, enter the following commands at the server console prompt:

```
LOAD NE2000 PORT=320  INT=3  FRAME=ETHERNET_II <Enter>
BIND IP TO NE2000 ADDR=1.2.3.4  <Enter>
```

If the NetWare/IP server is acting as a gateway, the server must have an interface to IPX in addition to IP. To specify multiple frame types and bind IP and IPX to the LAN driver, edit the AUTOEXEC.NCF file as follows:

- For Industry Standard Architecture (ISA) machines (equivalent to IBM-AT* bus type) equipped an NE2000 board, include the following lines in the AUTOEXEC.NCF file:

  ```
  LOAD NE2000 PORT=320  INT=3  FRAME=ETHERNET_802.2
     NAME=IPXLAN
  LOAD NE2000 PORT=320  INT=3  FRAME=ETHERNET_II
     NAME=TCPLAN
  BIND IPX TO IPXLAN  NET=123456
  BIND IP TO TCPLAN  ADDR=1.2.3.4
  ```

- For Micro Channel* machines, include the following lines in the AUTOEXEC.NCF file:

  ```
  LOAD NE232 SLOT=5  FRAME=ETHERNET_II
     NAME=TCPLAN
  LOAD NE232 SLOT=5  FRAME=ETHERNET_802.2
     NAME=IPXLAN
  ```

  Use the same entries for Extended Industry Standard Architecture (EISA) machines, but replace NE/2-32™ with NE3200™ .

Running DOS

If you have used the REMOVE DOS command to remove DOS from a server's memory, you cannot load NLMs from a server's DOS partition. If you have removed DOS, reinstate it by rebooting the server. If the console command

REMOVE DOS has been added to the AUTOEXEC.NCF file, you must remove or disable this line before you reboot.

Note

You need to run DOS only while installing the NetWare/IP software.

Determining the Default Directory Context

When NetWare 4 is installed, the ADMIN user object is placed in the Organization (O) container object of the Directory tree. ADMIN is the default user object used when logging in to a server via UNICON. If you want to log in using a user object other than ADMIN, you can either specify the complete name of the user object or, if the user object is in the server's default context, you can specify the common name of the user object. The default Directory context is determined as follows:

- If a bindery context is set for the server, this context is used.

  When you install NetWare 4 on a server, a corresponding server object is created in a Directory container object. In addition, the bindery context is set for this container object. The bindery context can be reset with the SET command.

  To view a server's current bindery context, type the following command at the server's console prompt:

  SET BINDERY CONTEXT <Enter>

- If a bindery context is not set, the server object's location in the Directory is used.

  For example, if the server has a complete name of .CN=NWserver.OU=mktg.O=acme, the default Directory context is OU=mktg.O=acme.

Using Other TCP/IP Products

NWPARAMS fileThis product maintains its hosts database under DNS. Other TCP/IP products running on the server might rely on a local file called SYS:ETC/HOSTS for host information. If such products are installed on the server, you can set a flag on the parameter WRITELOCALFILES in the SYS:ETC/NWPARAMS file to prevent the local file from being deleted. This condition is called *compatibility mode* .

To set the flag, type the following command at the server's console prompt:

LOAD EDIT SYS:ETC\NWPARAMS <Enter>

Note

If this file does not exist on the server, copy it manually from the *NetWare Installation* CD-ROM to the SYS:ETC directory.

Scroll to the [NETDB] section of the NWPARAMS file. Set the value for the WRITELOCALFILES parameter to 1. If you do not find this parameter in the NWPARAMS file, add the following entry to the [NETDB] section:

```
[NETDB]
WRITELOCALFILES 1
```

Setting Up the Initial DNS and DSS Servers

Before you can configure and launch the first NetWare/IP server in a network, you must have DNS and DSS running on the network. There are two scenarios for setting up an initial NetWare DNS or DSS server:

- If the system you plan to configure as a NetWare DNS or DSS server is already a NetWare server, install the NetWare/IP server software on the server as described in "Installing NetWare/IP on a NetWare 4 Server" on page 78 but do not configure and launch the NetWare/IP server software when prompted. After installation, use UNICON to configure and launch the DSS or DNS service.

- To set up a TCP/IP-only environment or if you do not already have a NetWare Directory Services (NDS) tree, you must install NetWare 4 and NetWare/IP at the same time on a server.

  When you install NetWare 4 and NetWare/IP the first time, you create a Directory tree. However, until you configure and launch a DSS server, this tree is isolated because NDS uses SAP. To install a server in this situation, follow the instructions in "Installing NetWare/IP and NetWare 4 Simultaneously" on page 74

Installing NetWare/IP on a Remote NetWare 4 Server

You can install the NetWare/IP software on a NetWare 4 server from a DOS workstation using the Remote Console™ (RCONSOLE) utility. RCONSOLE enables you to perform server console actions from a DOS workstation using a

LAN, WAN, or modem connection. The NetWare server on which you install the product must be running the REMOTE and RSPX NLMs.

For instructions on setting up an RCONSOLE session, see RCONSOLE in *Utilities Reference* . After you initiate an RCONSOLE session, you can use the procedures in “Installing the NetWare/IP Server Software” on page 76 to install NetWare/IP.

Installing on a Server with Multiple IP Addresses

If a server has more than one IP address, only the first IP address identified by TCP/IP is entered into the SYS:ETC\HOSTS file during a NetWare/IP installation. After installation you must edit the SYS:ETC\HOSTS file and list the remaining IP addresses used by the server.

With BorderManager, the NetWare/IP server software will take advantage of multiple IP boards by default. It is no longer necessary to configure the server as an IP router to take advantage of multiple IP boards.

Installing NetWare/IP and NetWare 4 Simultaneously

If you plan to install NetWare/IP on a NetWare 4 server in a TCP/IP-only environment, you must install NetWare 4 and NetWare/IP at the same time. NetWare/IP provides the TCP/IP transport that the NetWare server needs to communicate with the existing network. During installation, a NetWare 4 server needs to communicate with the network to configure itself as part of the Directory tree.

To enable simultaneous installation, the NetWare 4 and NetWare/IP installations have been integrated. During the integrated installation, you are prompted to install, configure, and load the NetWare/IP server software before NDS is installed. This way, a TCP/IP transport is available so the server can communicate with a TCP/IP-based server and configure itself as part of the existing Directory tree.

Integrated Install Prerequisites

You should have completed the following tasks before you install NetWare/IP using the integrated install:

- Plan the NetWare/IP network as described in “Preparing to Install a NetWare/IP Network” on page 65

- Install, configure, and start a master DNS name server for the DNS domain in which you are installing the server.
- Install, configure, and start a primary DSS server for the NetWare/IP domain in which you are installing the server.

Installing NetWare/IP Using the Integrated Install

To install NetWare/IP during the NetWare 4 installation, use the Custom Installation procedure described in Chapter 3, Custom Installation of the NetWare 4.11 *Installation* manual.

Note

You should install NetWare/IP and NetWare 4 at the same time only on a server that requires the TCP/IP transport to install NDS. In all other cases, you should install NetWare 4 before installing NetWare/IP.

DSS and DNS servers must be installed, configured, and running before you install a NetWare/IP server using the integrated install.

Installing the First Server in a TCP/IP-only Network

If you are installing the first NetWare 4 server in a TCP/IP-only network or if DNS and DSS are not already running on the network, use the following procedure to set up a NetWare DNS or DSS server:

1. **Install NetWare 4 as described in Chapter 3 Custom Installation of the NetWare 4.11 *Installation* manual.**

   When prompted to configure transport protocols, select to use and configure the TCP/IP transport. When prompted to install NetWare/IP, do not configure or start the NetWare/IP service.

   Because you do not start the NetWare/IP service, you can not connect to an existing network, so you can't place an object that represents the server in an existing Directory tree.

2. **After successfully installing NetWare 4, install the NetWare/IP software as described in “Installing NetWare/IP on a NetWare 4 Server” on page 78 but do not configure or start the NetWare/IP service.**

   The software necessary to configure and initialize a DNS name server or DSS server is installed along with the NetWare/IP software.

3. **At the new server, use UNICON to configure and launch the NetWare DNS or DSS server software.**

   For information on configuring a NetWare DNS server, see Chapter 7, “Setting Up DNS Support,” on page 89 For information on configuring a DSS server, see Chapter 8, “Configuring the Domain SAP/RIP Service,” on page 113

4. **At the new server, use NWIPCFG or UNICON to configure and launch the NetWare/IP server.**

   For information on configuring the NetWare/IP server, see Chapter 9, “Configuring NetWare/IP Servers,” on page 139

Installing the NetWare/IP Server Software

This section provides information to help you set up a NetWare/IP server successfully. It includes the following information:

- Getting started
- Prerequisites
- Installation methods
- Installation procedures

Getting Started

To get a NetWare/IP network up and running, you must install, configure, and launch the basic NetWare/IP components. To get the basic NetWare/IP components up and running, you must complete the following tasks:

1. Set up DNS support for NetWare/IP.

   If you already have a DNS name server running on the network, add the resource records required to support NetWare/IP to the DNS database as described in “Adding Resource Records for the DSS Servers” on page 97 or “Setting Up DNS Support on Another Platform” on page 103

   If you are setting up DNS for the first time, you must set up a master DNS name server. See “Setting Up the Initial DNS and DSS Servers” on page 73 or “Setting Up DNS Support on Another Platform” on page 103

2. Set up a primary DSS server.

   To set up a primary DSS server, install the NetWare/IP software on the server, configure the server as a primary DSS server, and start the service. See “Setting Up the Initial DNS and DSS Servers” on page 73 and “Configuring the Primary DSS Server” on page 121

3. Set up a NetWare/IP server.

   To set up a NetWare/IP server, install the NetWare/IP software on the server, configure the server as a NetWare/IP server, and start the NetWare/IP service. See “Installing the NetWare/IP Server Software” on page 76 “Configuring the NetWare/IP Server” on page 142 and “Starting the NetWare/IP Service” on page 146

Installation Prerequisites

A server must meet the following prerequisites before you install the NetWare/IP software:

- Network operating system

  You must install NetWare/IP on a server running NetWare 4, version 4.10 or later unless you are installing NetWare/IP and NetWare 4 at the same time as described in “Installing NetWare/IP and NetWare 4 Simultaneously” on page 74

- TCP/IP

  The TCPIP.NLM, which is included with NetWare, must be loaded and configured.

- Disk Space

  The SYS volume must have 4 MB of free disk space. An additional 16 MB is required if you are installing the online documentation (4 MB for the viewer and12 MB for the documentation).

- Memory

  The memory requirement per server depends on the number of NetWare/IP servers in the network and the specific NetWare/IP NLMs you plan to run. The formulas to determine the memory requirement for each server can be found under the “Planning the Network” on page 65

Important You must restart a server after you install NetWare/IP; therefore, it is important that you install the software during a time when service can be interrupted.

Installation Methods

You can install NetWare/IP using one of the following methods:

- Install from the *NetWare Installation* CD-ROM mounted as a NetWare volume on the server

- Install from the *NetWare Installation* CD-ROM inserted in a CD-ROM drive installed as a DOS drive on the server

- Install across the network from a *NetWare Installation* CD-ROM image copied to a server's disk drive

The method you use to install NetWare/IP determines what you should do for Step 4 of "Installing NetWare/IP on a NetWare 4 Server."

Installing NetWare/IP on a NetWare 4 Server

Use the following procedure to install the NetWare/IP software on a NetWare 4 server:

Note You can get help at any time during the installation procedure by pressing <F1> . You can exit the installation program by pressing <F10> .

1. **At the server's console prompt, stop all services using PKERNEL by typing**

   UNISTOP <Enter>

2. **Start the NetWare installation program by typing**

   LOAD INSTALL <Enter>

3. **Choose the following:**

–>**Product options**

–>**Choose an item or product listed above**

–>**Install NetWare/IP**

4. **When prompted, specify the location of the installation source files.**

- To install from the *NetWare Installation* CD-ROM mounted as a NetWare volume on the server, mount the volume, press <F3> , and enter the following:

  NW411:NWIP

  For information on mounting the *NetWare Installation* CD-ROM as a NetWare volume, see the NetWare 4 *Installation* manual.

- To install from a CD-ROM drive installed as a DOS drive on the server, insert the *NetWare Installation* CD-ROM into the server's CD-ROM drive, press <F3> , and enter the following:

  D:\NWIP

  If necessary, replace *D* with the appropriate drive letter.

- To install from a CD-ROM image copied to a NetWare server, copy the contents of the NWIP directories on the *NetWare Installation* CD-ROM to the server's disk drive. When prompted to enter a path for installation source files, enter the complete path to the source files as follows:

  servername /*vol* :*directory path*

5. **To begin, the installation program checks the server for several conditions. Each of these substeps is conditional, depending on the server's current configuration.**

   5a. **If prompted, choose Yes to remove any existing version of NetWare/IP. When the existing product is uninstalled, press** <Esc> **to continue.**

   5b. **If there is a README.TXT file, press** <Esc> **and choose Yes to stop the installation process and read the README file or No to continue with the installation process.**

   5c. **If you are installing the product for the first time on this server, enter the name of the host on which the product is being installed.**

   5d. **If prompted, configure and load TCP/IP on the server.**

The installation program cannot continue until it detects TCP/IP on the server.

5e. If prompted, unload the DISPATCH NLM.

If the installation program finds a previous version of the NetWare/IP configuration utility NFSCON, you are prompted to unload the DISPATCH NLM. This must be done to enable the new configuration program, UNICON, to be invoked.

6. Enter the location from which you boot the server. This is the location from which you enter the NetWare SERVER command to start the NetWare server.

7. After the program files are copied, the installation program displays a message indicating that NetWare/IP has been successfully installed. Press `<Esc>` to continue.

8. At this point, you have the option to configure and load the NetWare/IP server. Choose Yes to configure the NetWare/IP server or No to bypass the NetWare/IP server configuration process.

To enable network connectivity, you should configure and launch the NetWare/IP server when prompted. After the installation is complete, you can load NWIPCFG and make any desired changes, including stopping the NetWare/IP server. If DNS or DSS are not currently running on the network, should should not configure and launch the NetWare/IP server now.

If you choose to configure the NetWare/IP server at this point, the INSTALL utility invokes the NetWare/IP Configuration utility (NWIPCFG). When invoked, NWIPCFG issues a DHCP request to obtain NetWare/IP configuration parameters. If a DHCP server responds to the request, you are prompted to confirm the parameters.

If you choose not to configure the NetWare/IP server at this point, skip to Step 13 .

9. Configure the server as a DNS client.

9a. From the NetWare/IP Administration menu, choose the Configure DNS Client option.

9b. Enter the name of the DNS domain to which this server belongs.

9c. Enter the IP address(es) of the DNS name server(s) this server should contact to resolve DNS queries.

9d. To exit the DNS Client Access form, press <Esc> **.**

10. Configure the NetWare/IP server.

10a. From the NetWare/IP Administration menu, choose the Configure NetWare/IP Server option.

10b. Enter the name of the NetWare/IP domain.

10c. To configure the NetWare/IP server as a forwarding gateway, choose the Forward IPX Information to DSS field, press <Enter> **, and choose Yes.**

10d. To exit the NetWare/IP Server Configuration form, press <Esc> **and choose Yes.**

11. Start the NetWare/IP server.

11a. From the NetWare/IP Administration menu, choose the Start NetWare/IP Server option.

11b. Press <Esc> **to continue.**

12. Press <Esc> **and choose Yes to exit the NWIPCFG utility.**

13. Press <Esc> **as needed to exit the installation program.**

14. When prompted, choose Yes to exit the installation program or No to choose another installation option.

15. Reboot the computer to activate the NetWare/IP software.

After installing NetWare/IP, make sure the **UNISTART.NCF** command is the last command in the server's AUTOEXEC.NCF file.

Setting Up the NetWare/IP Client

The Novell Client software included with NetWare 4.2 is compatible with NetWare/IP. When installing the Client, click Custom to configure the Client as an IPX-only Client with NetWare/IP support. Refer to the NWIP.TXT file on the Novell Client CD-ROM for detailed configuration instructions.

Chapter

6 *Introducing UNICON and NWIPCFG*

Two utilities enable you to manage NetWare/IP™ : UNICON and NWIPCFG.

The UNICON utility enables you to administer various NetWare® products, including the NetWare Domain Name System (DNS) and the Domain SAP/RIP Service (DSS). The NWIPCFG utility enables you to administer the NetWare/IP server software.

This chapter introduces each utility and describes the configuration and management tasks each can perform.

Using UNICON

You can use UNICON to manage other NetWare products installed on a server. The utility detects the presence of these products and displays the menu options that pertain to them. This manual describes only how to use UNICON to manage NetWare DNS and DSS.

You can perform the following tasks using the UNICON utility:

- Change to another server to configure and manage a different NetWare server running UNICON

- Configure the server's global parameters

- Start, stop, and monitor specific services

- Configure and manage NetWare DNS and DSS servers

- Configure error reporting

- Monitor performance and adjust parameters affecting performance

Authorizing UNICON Access

Anyone with a NetWare account and access to the server console can run UNICON. However, only users with the proper rights to certain files and objects in the Novell Directory Services™ (NDS™) tree can access and use all features.

A NetWare administrator can delegate management tasks by granting individuals rights that allow them wider use of UNICON. When you install a NetWare product that is managed by UNICON, the installation program creates Group objects in the Directory tree. These objects are granted the rights they need to perform management tasks using UNICON. To delegate management tasks to a user, make the user a member of the group that has the rights to perform the tasks you want to delegate.

Table 6-1 shows how management tasks are divided by Group object name. The second column shows the specified group's area of responsibility. The third column shows the menu options that can be accessed to perform the specified tasks. This table lists only groups with management functions applicable to NetWare/IP administration.

Table 6-1 Accounts for NetWare/IP Management Tasks

Group Name	**Area of Responsibility**	**Authorized UNICON Menu Options**
UNICON MANAGER	Full use of the UNICON utility	Access to all menu options
UNICON SERVICES MANAGER	Start, stop, and manage services	Start/Stop Services and Manage Services
UNICON HOST MANAGER	Modify host entries	Manage Global Objects Manage Hosts

If you are unable to log in via UNICON during installation, if you change the server's default context, or if NDS is not installed on the server when NetWare/IP is installed, you must create these groups manually by typing the following command at the server console prompt:

LOAD UNICON /L INITNWIP <Enter>

Starting the UNICON Utility

You use UNICON to complete many of the procedures in this manual. Use the following procedure to start the UNICON utility and log in to a NetWare server.

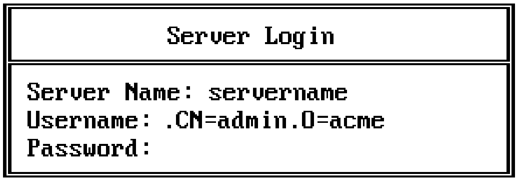
Important

If you did not configure and launch the NetWare/IP server during installation, you may not be able to load UNICON. For information on what to do in this situation, see “Troubleshooting UNICON” on page 183

1. **Start UNICON from the server console prompt by typing**

   LOAD UNICON <Enter>

   The utility displays a login form with the server name filled in.



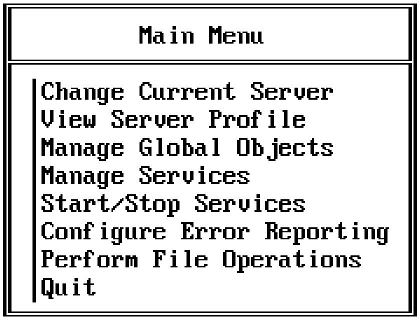
```
Server Login

Server Name: servername
Username: .CN=admin.O=acme
Password:
```

2. **Type an authorized user object name in the Username field, and press** <Enter> **.**

3. **Type the appropriate password in the Password field and press** <Enter> **.**

If the username and password are valid, the utility displays UNICON’s Main Menu.



```
Main Menu

Change Current Server
View Server Profile
Manage Global Objects
Manage Services
Start/Stop Services
Configure Error Reporting
Perform File Operations
Quit
```

The header at the top of the screen shows the hostname or IP address of the NetWare server, the user login name, and the current NDS context.

```
UNICON  3.57u        Server: acme         User: .CN=admin.O=acme
Context: O=acme
```

If the username and password are not valid, you are denied access to the utility.

Changing the Current Server

The Change Current Server option on the Main Menu enables you to manage NetWare/IP modules that are installed on other NetWare servers. When you choose this option, you are prompted to choose a server or log in as follows:

- If you are currently attached to more than one server, the utility displays a list of these servers. You can choose a server from the list and press <Enter> to change to that server, you can log in to a new server by pressing <Insert> , or you can log out from a server by highlighting the server entry and pressing <Delete> .
- If you are currently logged in to only one server, the utility immediately prompts you to log in to another server.

Once you attach to a server, the server is added to the Server Login list. While remaining in the UNICON utility, you can switch control from one server to another by choosing the server name from the list.

For additional information on the Change Current Server option, see Appendix B, “Managing NetWare/IP Remotely,” on page 243

Using UNICON Within a Procedure

Each procedure documented in this manual begins with a step that explains how to access the screen you must use for that procedure.

For example, to access the Configure Error Logging Levels form in UNICON, the first step is presented as in the following example:

1. **From UNICON’s Main Menu, choose the following:**

–>**Configure Error Reporting**
–>**Configure Error Logging/SNMP Alert Levels**

2. **When the Configure Error Logging Levels form is displayed, complete your task.**

Throughout this manual, procedures for configuring the NetWare/IP software require you to use UNICON. These procedures assume that you know how to access the server console and load the UNICON utility.

Using NWIPCFG

The NWIPCFG utility enables you to configure and manage the NetWare/IP server software. With NWIPCFG, you can perform the following tasks:

- Configure a NetWare server as a DNS client
- Configure the NetWare/IP server software
- Start a NetWare/IP server

For more information on any of these tasks, see Chapter 9, “Configuring NetWare/IP Servers,” on page 139

Starting the NWIPCFG Utility

Use the following procedure to start the NWIPCFG utility:

1. **Start NWIPCFG from the server console prompt by typing**

   LOAD NWIPCFG <Enter>

   When the utility successfully loads, it displays the NetWare/IP Administration menu.

2. **From the NetWare/IP Administration menu, select to configure the server as a DNS client, to configure the NetWare/IP server, or to start the NetWare/IP server.**

Using NWIPCFG within a Procedure

Each procedure documented in this manual begins with a step that explains how to access the screen you must use for that procedure. For example, to access the NetWare/IP Server Configuration form in NWIPCFG, the first step is presented as in the following example:

1. **From NWIPCFG's NetWare/IP Administration menu, choose the following:**

   –>**Configure NetWare/IP Server**

2. **When the NetWare/IP Server Configuration form is displayed, complete your task.**

Throughout this manual, procedures for configuring the NetWare/IP software require you to use NWIPCFG. These procedures assume that you know how to access the server console and load the NWIPCFG utility.

Chapter

7 *Setting Up DNS Support*

Before you can run NetWare/IP™ , you must configure a master DNS name server and, optionally, one or more replica DNS name servers. The master DNS name server maintains hostname and address information for the hosts in a DNS domain. NetWare/IP uses DNS name servers to maintain information about the DSS servers that support the NetWare/IP domain. NetWare/IP servers and clients use DNS name servers to locate DSS servers. For a detailed discussion of DNS, see Chapter 2, "Understanding the Domain Name System," on page 23

NetWare/IP does not require you to set up DNS support on a NetWare® server; if you already have a DNS name server running on the network, you can continue to use the existing service. However, the NetWare DNS service provides all the functionality of a standard DNS service without complex configuration and management procedures. Using UNICON, you can accomplish all NetWare DNS administrative tasks by choosing options from a series of menus instead of by editing configuration files. This chapter discusses both of these options.

This chapter includes the following sections:

- Setting Up a NetWare Master DNS Name Server
- Setting Up NetWare Replica DNS Name Servers
- Setting Up DNS Support on Another Platform
- Managing the NetWare DNS Service

Setting Up a NetWare Master DNS Name Server

The following sections provide procedures for setting up a master DNS name server on a NetWare server. To set up and configure a master DNS name server to support NetWare/IP, you must do the following:

- Initialize the DNS database as described in “Initializing the DNS Database” on page 95

- Create the NetWare/IP domain as described in “Initializing the DNS Database” on page 95

- Add resource records to the DNS database as described in “Adding Resource Records for the DSS Servers” on page 97

Master DNS Configuration Forms

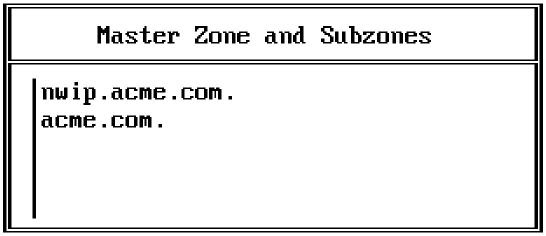
Depending on the configuration of the network, you might use one or more of these UNICON forms to set up DNS support for NetWare/IP.

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

Master Zone and Subzones List

The Master Zone and Subzones list includes all domains over which this master DNS name server has authority. All DNS database configuration procedures begin at this list.

Figure 7-1
Master Zone and Subzones List



```
Master Zone and Subzones

nwip.acme.com.
acme.com.
```

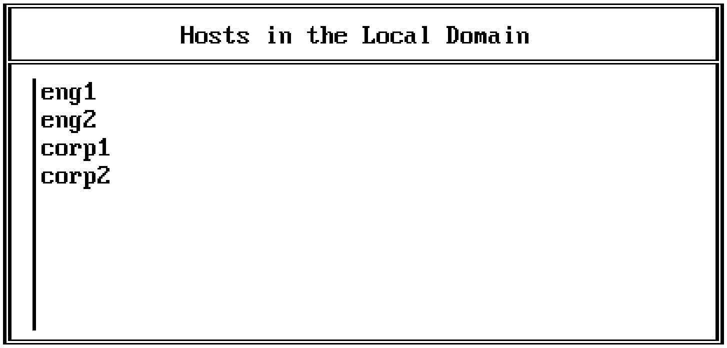
From UNICON's Main Menu, choose the following to display the Master Zone and Subzones list:

–>**Manage Services**
–>**DNS**
–>**Administer DNS**
–>**Manage Master Database**
–>**Delegate Subzone Authority**

Hosts in the Local Domain List

The Hosts in the Local Domain list includes the host entries in the DNS database. All host configuration procedures begin at this list.

Figure 7-2
Hosts in the Local Domain List



```
Hosts in the Local Domain

eng1
eng2
corp1
corp2
```

From UNICON’s Main Menu, choose the following to display the Hosts in the Local Domain list:

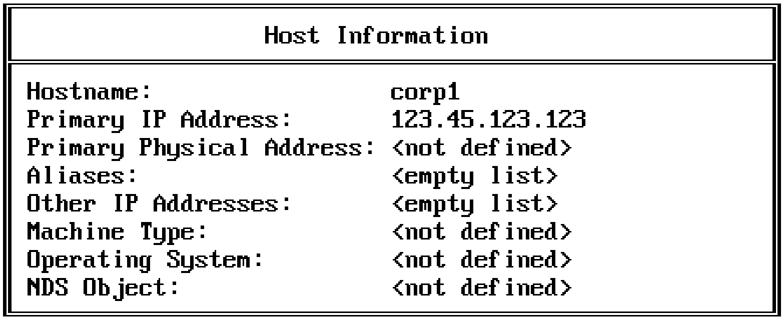
–>**Manage Global Objects**
–>**Manage Hosts**
–>**Hosts**

Host Information Form

The Host Information form displays information about a specific host. Use this form to add or modify a host record.

Figure 7-3

Host Information Form



```
                    Host Information

Hostname:                  corp1
Primary IP Address:        123.45.123.123
Primary Physical Address: <not defined>
Aliases:                   <empty list>
Other IP Addresses:        <empty list>
Machine Type:              <not defined>
Operating System:          <not defined>
NDS Object:                <not defined>
```

From the Hosts in the Local Domain list, choose a host name to display the Host Information form.

On the Host Information form, you use only the following fields when configuring DNS to support NetWare/IP:

Hostname —the name of the specified host.

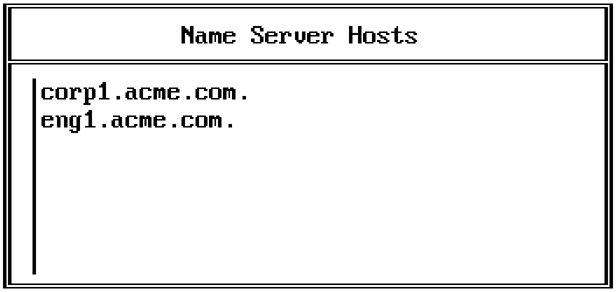
Primary IP Address —the primary Internet address that identifies the host in an IP network. The information you enter into this field must be in standard IP address format, with the parts of the address separated by periods, such as 123.26.9.31.

For information about the other fields on this form, refer to Appendix C, “Managing Host Information,” on page 257

Name Server Hosts List

The Name Server Hosts list includes the hosts that are configured as DNS name servers. Use this list to add name server (NS) resource records to the master DNS database.

Figure 7-4
Name Server Hosts List



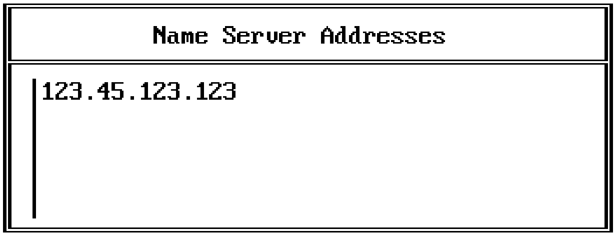
```
corp1.acme.com.
eng1.acme.com.
```

From the Master Zone and Subzones list, choose a DNS domain to display the Name Server Hosts list.

Name Server Addresses List

The Name Server Addresses list displays the IP address for a specific name server. If you choose a name server from the Name Server Hosts list, the Name Server Addresses list appears. If the name server's IP address is not listed, you must add it using the Host Management option.

Figure 7-5
Name Server Addresses List



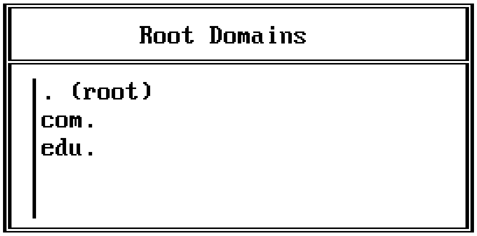
```
123.45.123.123
```

From the Name Server Hosts list, choose a name server to display the Name Server Addresses list.

Root Domains List

The Root Domains list enables you to link a name server to the root name servers in the existing DNS hierarchy.

Figure 7-6
Root Domains List



Root Domains

```
. (root)
com.
edu.
```

From UNICON's Main Menu, choose the following to display the Root Domains list:

–>**Manage Services**
  –>**DNS**
    –>**Administer DNS**
      –>**Link to Existing DNS Hierarchy**
        –>**Link Direct**

The Root Domains list displays all of the root domains to which your name server is linked. From this list you can add a new root domain entry by pressing <Insert>, or delete a root domain entry by highlighting the entry and pressing <Delete> .

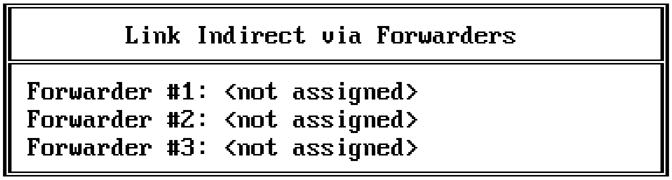
From the Root Domains list, you can also display information about the root name servers servicing each root domain. To display the name of the root name server for a specific root domain, choose the domain and press <Enter> . To display a root name server's IP address, choose a root domain and press <Enter> ; then, choose the name server entry and press <Enter> . You can also modify the root name server name and IP address if changes are made to the root name servers for a domain.

Link Indirect via Forwarders Form

Use the Link Indirect via Forwarders form to designate up to three forwarders that link to the existing DNS hierarchy.

Figure 7-7

Link Indirect via Forwarders Form



```
          Link Indirect via Forwarders

 Forwarder #1: <not assigned>
 Forwarder #2: <not assigned>
 Forwarder #3: <not assigned>
```

From UNICON's Main Menu, choose the following to display the Link Indirect via Forwarders form:

–>**Manage Services**

–>**DNS**

–>**Administer DNS**

–>**Link To Existing DNS Hierarchy**

–>**Link Indirect via Forwarders**

The Link Indirect via Forwarders form contains three fields. You can specify up to three forwarders by typing in the IP address of each forwarder.

Initializing the DNS Database

If you are setting up a new master DNS name server, you must begin by initializing the DNS database. When you initialize the database, the UNICON utility

- Generates the DNS zone and DNS domain
- Creates the DNS database
- Starts the DNS server

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**

   –>**DNS**

   –>**Initialize DNS Master Database**

2. **When prompted for the DNS domain name, enter a fully qualified DNS domain name or choose the default, and press** <Esc> **.**

   By default, the DNS Domain field shows the current hostname in the following syntax: *hostname* .com.

3. **When prompted, specify whether you want DNS to service specific subnetworks.**

   If you choose Yes, you are prompted to specify which subnetworks you want DNS to service.

4. **When prompted, choose Yes to initialize the DNS database.**

   If you choose Yes, the utility displays status messages as the database is created. Upon a successful initialization, the DNS name server is configured.

5. **When the utility displays a message stating that DNS is initialized, press** <Esc> **.**

6. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Now that you have created the master DNS database, you must add the appropriate DNS resource records as described in Appendix C, "Managing Host Information," on page 257 and "Adding Resource Records for the DSS Servers" on page 97

Creating the NetWare/IP Domain

After creating a new master DNS database, you must identify the NetWare/IP domain.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**DNS**
   –>**Administer DNS**
   –>**Manage Master Database**
   –>**Delegate Subzone Authority**

2. **Press** <Insert> **and enter the fully qualified NetWare/IP domain name.**

3. **From the Available Hosts list, choose the server to be the master DNS name server for the new NetWare/IP domain.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Adding Resource Records for the DSS Servers

After you set up the master DNS database, you must add address (A) and name server (NS) resource records to the master database for each of the DSS servers you plan to set up in the NetWare/IP network.

All the information you need to add these resource records is contained in the worksheet described in "NetWare/IP Support Services Planning Worksheet" on page 229

Adding Address Records

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Global Objects**
   –>**Manage Hosts**
   –>**Hosts**

2. **From the Hosts in the Local Domain list, press** <Insert> **to add an address record for the primary DSS server to the database.**

3. **When prompted, enter the hostname of the primary DSS server.**

4. **When prompted, enter the primary DSS server's IP address.**

   The utility displays the Host Information form described in "Host Information Form" on page 91 You can add information about the host, but it is not necessary for NetWare/IP to function.

5. **To return to the Hosts in the Local Domain list, press** <Esc> **.**

6. **Repeat Step 2 through Step 5 to add records for each secondary DSS server in the network.**

7. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Adding Name Server Records

Do not add NS resource records for unregistered DSS servers. For more information on registered and unregistered DSS servers, see "DSS Server Types" on page 48

1. **From UNICON's Main Menu, choose the following:**

–>**Manage Services**
–>**DNS**
–>**Administer DNS**
–>**Manage Master Database**
–>**Delegate Subzone Authority**

2. **From the Master Zone and Subzones list, choose the DNS domain name.**

3. **From the Name Server Hosts list, press** <Insert> **to add a name server (NS) resource record for the primary DSS server to the database.**

4. **From the Available Hosts list, choose the DSS server you want to add as a name server host.**

5. **Repeat Steps 3 and 4 to add name server (NS) records for each secondary DSS server in the network.**

6. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

If this is the first time you are configuring DNS, you must also add the appropriate records to the DNS node above you in the DNS hierarchy (the parent domain of the NetWare/IP domain) as described in "Linking to the Existing DNS Hierarchy" on page 98

Linking to the Existing DNS Hierarchy

To receive queries from outside your domain, you must provide your domain name and the names and IP addresses of your domain name servers to the parent server. For example, if your new domain is acme.com., then you must register your new domain and name server with the master DNS server that services the com. domain. Refer to the appropriate operating system documentation for that server to find out how to add new domain records to the existing DNS database. If the DNS domain above you is administered by someone else, you must register with that administrator and make sure that your records are added to the existing DNS hierarchy.

To send queries outside your domain, you do not need to do anything once your DNS server is running. Your NetWare DNS server automatically links into the DNS hierarchy using the information stored in the SYS:ETC\DNS\ROOT.DB file. This file contains a list of root name servers (current when this product shipped) that are authoritative for the top-level US organizational domains.

You may want to link to another domain so you can query that domain’s name server directly without the overhead of having a root name server resolve your queries. You may also want to improve the effectiveness of sending queries by designating one or more servers as *forwarders* . The following procedures describe how to use UNICON to view the ROOT.DB file, link directly to another name server, and link indirectly via forwarders.

Note

You need to link to the existing DNS hierarchy only the first time you create your master DNS database.

Linking Directly to a Name Server

1. **From UNICON’s Main Menu, choose the following:**

   –>**Manage Services**
     –>**DNS**
       –>**Administer DNS**
         –>**Link to Existing DNS Hierarchy**
           –>**Link Direct**

2. **From the Root Domains list, press** <Insert> **to add the domain to which you want to link.**

3. **Enter the domain name into the entry box.**

4. **To identify the domain’s name server choose the domain name you just added from the Root Domains list and press** <Enter> **.**

5. **To add the name of the server, press** <Insert> **.**

6. **Enter the name of the domain’s name server.**

7. **To indicate the IP address of the name server, choose the server name and press** <Enter> **.**

8. **To add the address of the server, press** <Insert> **.**

9. **Enter the server’s IP address.**

10. **To return to UNICON’s Main Menu, press** <Esc> **as needed.**

The utility links your domain as you specified by adding the information you entered in the SYS:ETC/DNS/ROOT.DB file.

Linking Indirectly via Forwarders

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
       –>**DNS**
           –>**Administer DNS**
               –>**Link to Existing DNS Hierarchy**
                   –>**Link Indirect via Forwarders**

2. **Enter the IP addresses of the servers you want to designate as forwarders.**

3. **When prompted, choose Yes to save your entries.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Setting Up NetWare Replica DNS Name Servers

DNS must be available to NetWare/IP servers and clients at all times. Therefore, after you create a master DNS database, you should configure one or more read-only replicas of the database on other servers to provide redundancy and load-balancing for the network.

You should also consider configuring replica DNS servers on network segments that may become isolated or that are interconnected by slow or heavily used links.

Updates to information maintained by the master name server automatically propagate to the replica systems at a specified interval.

Note

To simplify DNS replication and reduce zone transfer traffic, you can replicate only the portion of the DNS database that pertains to NetWare/IP. This allows you to provide fault tolerance for your NetWare/IP network without replicating the entire DNS database, which can be quite large.

For information on configuring a replica DNS server, see "Creating a Replica DNS Database" on page 102

Replica DNS Configuration Forms

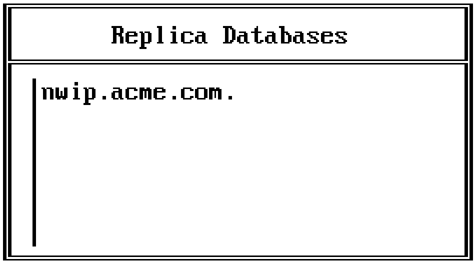
You use the following UNICON screens to set up a replica DNS database on a NetWare server.

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

Replica Databases List

The Replica Databases list provides a list of the DNS master domains for which this server holds a replica database. All replica configuration procedures begin at this list.

Figure 7-8
Replica Databases List



Replica Databases

nwip.acme.com.

From UNICON’s Main Menu, choose the following to display the Replica Databases list:

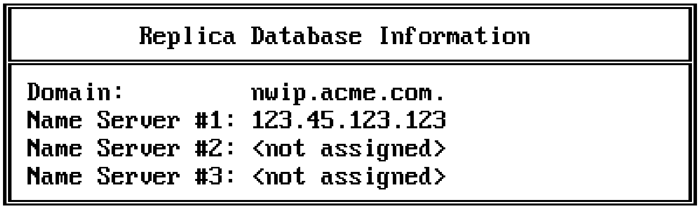
–>**Manage Services**
  –>**DNS**
    –>**Administer DNS**
      –>**Manage Replica Databases**

Replica Database Information Form

The Replica Database Information form displays information about a single replica database. Use this form when adding a replica or when modifying information about an existing replica.

Figure 7-9

Replica Database Information Form



```
        Replica Database Information

Domain:         nwip.acme.com.
Name Server #1: 123.45.123.123
Name Server #2: <not assigned>
Name Server #3: <not assigned>
```

From the Replica Databases list, choose an entry to display the Replica Database Information form.

The Replica Database Information form contains the following fields:

Domain —the name of the DNS domain for which this server contains a replica DNS database.

Name Server —the IP address of the master DNS name server. Use the additional Name Server fields to specify additional DNS name servers.

Creating a Replica DNS Database

1. **From UNICON’s Main Menu, choose the following:**

   –>**Manage Services**

   –>**DNS**

   –>**Administer DNS**

   –>**Manage Replica Databases**

2. **From the Replica Databases list, press** <Insert> **to create a replica of a DNS database on this server.**

3. **On the Replica Database Information form, fill in the Domain field and at least one Name Server field; then press** <Esc> **.**

4. **When prompted, choose Yes to save your changes.**

5. **To return to UNICON’s Main Menu, press** <Esc> **as needed.**

After creating the replica database, you must start the DNS service on this server as described in “Starting DNS” on page 108 After you start the DNS service, the name server can begin responding to queries.

Setting Up DNS Support on Another Platform

If you want to configure an existing master DNS name server on a non-NetWare platform to provide DNS services for a NetWare/IP internetwork, you must add the following DNS resource records to the existing master DNS database:

- Start of Authority (SOA) record for the DNS domain. This DNS domain must be the parent of the NetWare/IP domain. If you are already using DNS on the network, this record will have already been created.
- Address (A) records for the primary DSS server and all secondary DSS servers in the NetWare/IP domain. If you are already using DNS in your network, the master DNS database may already contain address records for these servers.
- Name server (NS) records for the primary DSS server and all secondary DSS servers in the NetWare/IP domain.

Note

Do not add NS resource records for unregistered DSS servers. For more information on registered and unregistered DSS servers, see “DSS Server Types” on page 48

For example, Acme Company wants to configure their existing master DNS name server to support their new NetWare/IP domain, nwip.acme.com. They plan to configure a primary DSS server on server eng2.acme.com. and a secondary DSS server on server corp2.acme.com. The following example shows the resource records that Acme must add to their DNS database to support NetWare/IP:

Table 7-1Resource Records

```
;
acme.com.        IN       SOA   eng2.acme.com.
;
;Name servers
nwip.acme.com.   IN       NS    eng2.acme.com.
nwip.acme.com.   IN       NS    corp2.acme.com.
;
;Host addresses
eng2.acme.com.   IN       A     1.3.0.2
corp2.acme.com.  IN       A     1.1.0.3
```

The SOA record must always point to the parent domain of the NetWare/IP domain. Notice that in this example the SOA record points to acme.com., which is the parent of NetWare/IP domain nwip.acme.com.

For information on how to add resource records to a non-NetWare DNS database, refer to the appropriate operating system documentation. In many non-NetWare DNS implementations, you must edit the file containing the DNS database and enter these records directly using a text editor.

After updating the DNS database, restart the DNS name server software so that the changes take effect.

Managing the NetWare DNS Service

This section provides procedures for performing common DNS management tasks using the UNICON utility. The following sections provide procedures for

- Starting and stopping DNS
- Managing resource records
- Backing up the DNS database
- Disabling the DNS database

DNS Management Screens

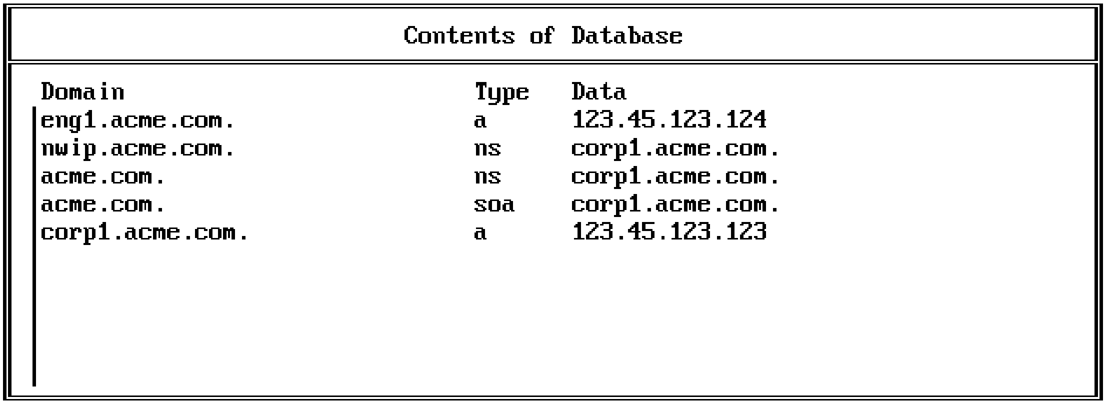
This section describes the forms that you will use when managing the NetWare DNS service.

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

Contents of Database Form

The Contents of Database form lists the resource records currently stored in the master DNS database. The entries are arranged alphabetically by domain name and record type.

Figure 7-10
Contents of Database Form



```
                        Contents of Database

 Domain                          Type   Data
 eng1.acme.com.                  a      123.45.123.124
 nwip.acme.com.                  ns     corp1.acme.com.
 acme.com.                       ns     corp1.acme.com.
 acme.com.                       soa    corp1.acme.com.
 corp1.acme.com.                 a      123.45.123.123
```

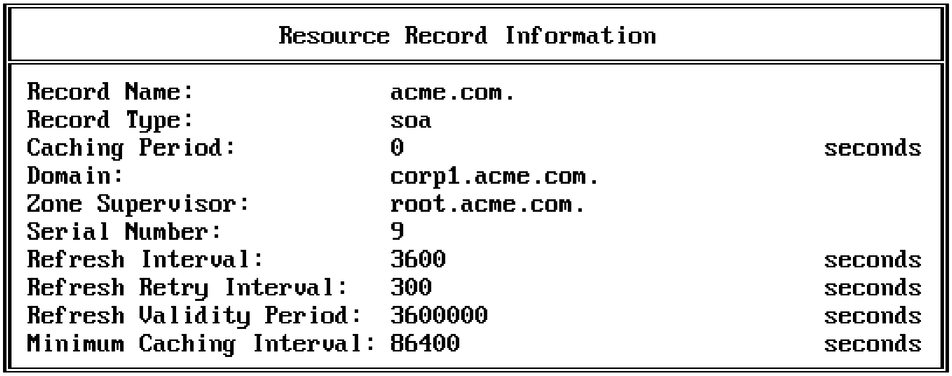
From UNICON’s Main Menu, choose the following to display the Contents of Database form:

–>**Manage Services**
  –>**DNS**
    –>**Administer DNS**
      –>**Manage Master Database**
        –>**Manage Data**

Resource Record Information Form

The Resource Record Information form enables you to view or modify information about a specific resource record or add a new resource record.

Figure 7-11
Resource Record Information Form



```
                    Resource Record Information

Record Name:               acme.com.
Record Type:               soa
Caching Period:            0                                seconds
Domain:                    corp1.acme.com.
Zone Supervisor:           root.acme.com.
Serial Number:             9
Refresh Interval:          3600                             seconds
Refresh Retry Interval:    300                              seconds
Refresh Validity Period:   3600000                          seconds
Minimum Caching Interval:  86400                            seconds
```

From the Contents of Database form

- Choose a record and press <Enter> to see information about a specific record.
- Press <Insert> and choose the type of record from the Record Type list, to enter information for a new record.

The following fields are present for all record types:

Record Name —the name of the resource

Record Type —the record type. The possible record types are

- A—maps names to addresses
- CNAME—specifies an alias for the host's canonical or authoritative name
- MB—identifies a host as a mailbox
- MR—specifies a different domain name to receive mail in place of some previous domain
- MX—identifies a host to deliver or forward mail for a domain
- NS—identifies a name server for a domain
- PTR—maps addresses to names

- SOA—specifies which server is the best source of information for the data within the domain

Caching Period —how many seconds the name server keeps its cached data before it gets updated

Other fields in the form vary depending upon the record type. The following sections describe the fields that are unique to each record type:

Type A Unique Field

Address (A) —the address to which a hostname is mapped.

Type CNAME Unique Field

Canonical Name (CNAME) —the alias for a host's canonical name.

Type NS Unique Field

Name Server (NS) —a name server. There is an NS record for each name server in a domain.

Type PTR Unique Field

Domain Pointer (PTR) —the address-to-name mapping for a host.

Type SOA Unique Fields

Domain —the domain for which the name server is authoritative.

Zone Supervisor —the username responsible for the zone. The default entry is root.*domain_name* .

Serial Number —the serial number for the database. The number is incremented each time the database changes. Secondary servers check this number to determine whether they should download a new copy of the database.

Refresh Interval —how often a secondary server checks the accuracy of its database copy.

Refresh Retry Interval —how long the secondary server waits to re-access the master after a failure to reach the master.

Refresh Validity Period —how long the secondary server waits after a failure to reach the master before the secondary server stops responding to queries. This limit exists to prevent the secondary server from giving out expired data.

Minimum Caching Interval —a global domain parameter that specifies by default the minimum amount of time for which query information is maintained by the master server. The caching period parameter (see “Resource Record Information Form” on page 105) found in all resource records can be set to extend this time.

Note

For more information on DNS resource records, refer to RFC 1034, RFC 1035, or a good source such as DNS and BIND by Paul Albitz and Cricket Liu (O'Reilly & Associates, Inc.).

Starting DNS

1. **From UNICON's Main Menu, choose the following:**

   –>**Start/Stop Services**

2. **From the Running Services list, press** <Insert> **.**

   If DNS appears on the Running Services list, the service is already running.

3. **From the Available Services list, choose the DNS Server option and press** <Enter> **.**

   The DNS Server option is listed if the service is available but not running.

4. **To return to UNICON's Main Menu, press** <Esc>.

Stopping DNS

If this server is configured as a DSS server, you should stop DSS before stopping the DNS service on this server. If you do not, DSS is automatically stopped when you stop DNS. If DSS is automatically stopped because you stopped DNS, it is restarted automatically when you restart DNS.

1. **From UNICON's Main Menu, choose the following:**

–>**Start/Stop Services**

2. **From the Running Services list, choose the DNS Server entry and press** <Delete> **.**

   If DNS Server does not appear in the list, the service is not running.

3. **When prompted, choose Yes to stop the service.**

4. **To return to UNICON's Main Menu, press** <Esc>.

Adding and Deleting Resource Records

The following sections provide procedures for adding and deleting resource records.

Adding a Resource Record

As you add hosts to your network, you must add appropriate resource records to the master DNS database. UNICON automatically adds the information you provide to the appropriate database files.

If you are adding a name server (NS) record for a DSS server, you should use the procedure documented in "Adding Name Server Records" on page 97

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
      –>**DNS**
         –>**Administer DNS**
            –>**Manage Master Database**
               –>**Manage Data**

2. **From the Contents of Database form, press** <Insert> **and choose the type of record from the Record Type list.**

3. **Complete the Resource Record Information form and press** <Esc> **.**

4. **When prompted, choose Yes to save the new resource record.**

5. **Repeat Steps 2 through 4 for each record you want to add to the database.**

6. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Deleting a Resource Record

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**DNS**
   –>**Administer DNS**
   –>**Manage Master Database**
   –>**Manage Data**

2. **From the Contents of Database form, choose the entry you want to delete and press** <Delete> **.**

3. **When prompted, choose Yes to delete the record.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Backing Up the DNS Database

There are at least two reasons for periodically backing up the DNS database:

- You might want to reinitialize the database if, for some reason, the database becomes corrupt.

- You might want to move the database to another server.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**DNS**
   –>**Save DNS Master to Text Files**

2. **When prompted, choose Yes to back up the DNS database to the SYS:ETC/DBSOURCE/DNS/HOSTS file.**

3. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Disabling the Master DNS Database on the NetWare Server

Warning

Exercise extreme caution when using this option. It deletes the entire DNS database. You cannot use the master DNS server after you disable it unless you reconfigure the database.

Use this procedure to disable the NetWare DNS service without unloading the DNS NLMs. If you use the Start/Stop Services option on UNICON's Main Menu to stop DNS, the DNS NLMs are unloaded. This procedure does not unload the NLMs.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
       –>**DNS**
           –>**Administer DNS**
               –>**Disable DNS Service**

2. **When prompted, select Yes to disable the master DNS database.**

3. **To return to UNICON's Main Menu, press** `<Esc>` **as needed.**

Chapter

8 *Configuring the Domain SAP/RIP Service*

The Domain SAP/RIP Service (DSS) maintains a centralized database of SAP and RIP information for a NetWare/IP™ network. For each NetWare/IP domain, there must be one primary DSS server. In addition, you can configure one or more secondary DSS servers to provide redundancy and load balancing for the NetWare/IP network. For a detailed discussion of the Domain SAP/RIP Service, see Chapter 3, "Understanding the Domain SAP/RIP Service," on page 43

Important

You must set up DNS support for your network as described in Chapter 7, "Setting Up DNS Support," on page 89 before configuring the primary DSS server.

This chapter provides procedures for setting up and managing primary and secondary DSS servers, which are included in the following sections:

- Setting Up the Primary DSS Server
- Setting Up a Secondary DSS Server
- Managing DSS Servers

Setting Up the Primary DSS Server

To set up the primary DSS server, you must

1. Configure a NetWare 4™ server as the primary DSS server
2. Add DNS resource records identifying the primary DSS server
3. Start the Domain SAP/RIP Service on the server

Primary DSS Server Prerequisites

Before you can configure a server as the primary DSS server, it must meet the following hardware and software requirements:

- The NetWare/IP server software must be installed as described in Chapter 5, “Installing the NetWare/IP Software,” on page 65

- The master DNS server must be configured and operational as described in Chapter 7, “Setting Up DNS Support,” on page 89

- The SYS: volume must have 1 MB of free disk space.

- The amount of memory required depends on the number of server nodes in the network. Use the following formula to determine the memory requirements for a primary DSS server, where *a* equals the number of servers in the network:

  (a x 520) + 835,000 = memory in bytes needed on the server.

Note If you choose to set up DSS on a server that belongs to a remote DNS domain, you must add resource records to two master DNS databases. You must add a name server record to the master DNS database that is servicing your NetWare/IP domain identifying the DSS server as a name server for the NetWare/IP domain and an address record to the master DNS database of the remote domain specifying the IP address to hostname mapping for the server.

Primary DSS Server Administration Forms

The UNICON forms you use to complete the primary DSS server configuration are shown and described in the following sections.

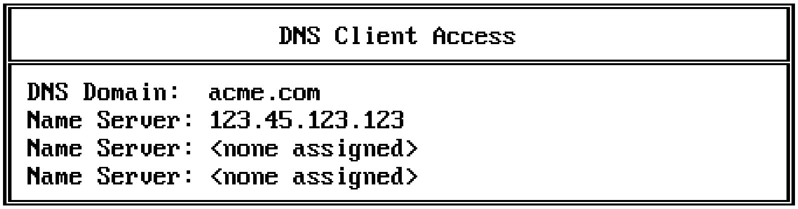
If you need information about a specific field when accessing an online form using UNICON, press <F1> .

DNS Client Access Form

The primary DSS server must be set up as a DNS client or resolver. Use the DNS Client Access form to configure the primary DSS server as a DNS client.

Figure 8-1

DNS Client Access Form



```
                    DNS Client Access

DNS Domain:  acme.com
Name Server: 123.45.123.123
Name Server: <none assigned>
Name Server: <none assigned>
```

The utility displays this form only if you do not have DNS client access set up on this server before you try to configure DSS or NetWare/IP on this server.

You might already have DNS access set up if you configured this machine as a DNS name server, or if you used the Server Profile Configuration form to enable DNS client access, or if the server is running another product that uses DNS.

Note UNICON's Server Profile Configuration form is described in “Server Profile Configuration Form” on page 266

From UNICON’s Main Menu, choose the following to display the DNS Client Access form:

–>**Manage Services**
  –>**NetWare/IP**

The information required to complete this form can be found on a completed NetWare/IP Support Services Planning Worksheet as described in “NetWare/IP Support Services Planning Worksheet” on page 229 A description of each field follows:

DNS Domain —the name of the DNS domain to which the server belongs. The utility checks to make sure that you enter a valid DNS domain name. If you are not sure of the correct syntax, see “Domain Names” on page 25

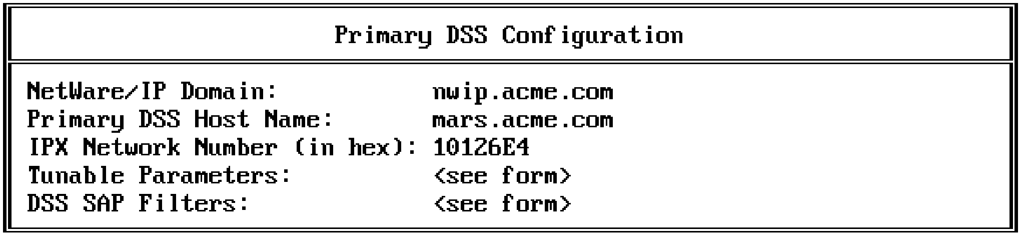
Name Server —the DNS name server this DSS server should contact first to resolve DNS queries. Type the hostname or IP address of the nearest DNS name server.

Name Server —the additional Name Server fields specify additional DNS name servers this DSS server should contact to resolve DNS queries. You do not need to fill in these fields if information about all hosts in your network is available through the first DNS name server.

Primary DSS Configuration Form

Use the Primary DSS Configuration form to set up a NetWare® server as the primary DSS server and to specify the global parameter values for a NetWare/IP domain. You can also use this form to modify the primary DSS server configuration.

Figure 8-2
Primary DSS Configuration Form



```
                      Primary DSS Configuration

 NetWare/IP Domain:             nwip.acme.com
 Primary DSS Host Name:         mars.acme.com
 IPX Network Number (in hex):   10126E4
 Tunable Parameters:            <see form>
 DSS SAP Filters:               <see form>
```

From UNICON's Main Menu, choose the following to display the Primary DSS Configuration form:

–>**Manage Services**
–>**NetWare/IP**
–>**Configure Primary DSS**

The information required to complete the Primary DSS Configuration form can be found on a completed Primary DSS Server Configuration Worksheet as described in "Primary DSS Server Configuration Worksheet" on page 233 A description of each field follows:

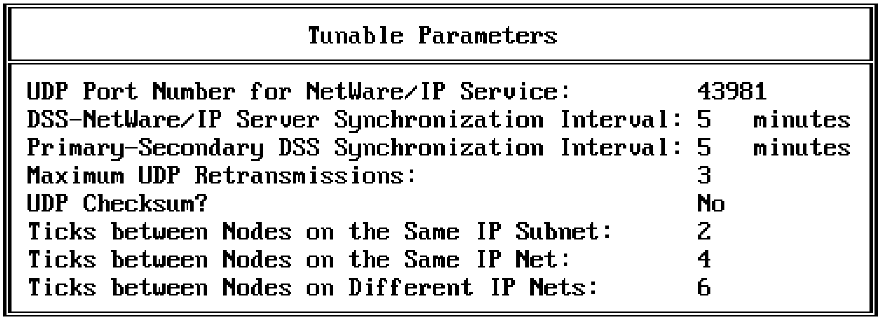
NetWare/IP Domain —the domain for which this DSS server maintains SAP/RIP information. All NetWare/IP servers and clients using this primary DSS server are members of this domain. The NetWare/IP domain conforms to the same naming conventions as the DNS domain. For additional information about NetWare/IP domains, see "NetWare/IP Domain" on page 36

Primary DSS Host Name —the fully qualified hostname of the current server, in the form of *hostname .DNS_domain_name* .

IPX Network Number (in hex) —the IPX™ external network number for your NetWare/IP network. You can assign an arbitrary hexadecimal number of one to eight digits (1 to FFFFFFFF), but the number must be unique throughout your IPX internetwork. If you have a mixed IP–IPX internetwork, make sure that the number you assign is not already being used by another NetWare server on one of your IPX segments. This is the virtual IPX network number used by all NetWare/IP hosts in the NetWare/IP domain.

Tunable Parameters —displays the Tunable Parameters form.

Figure 8-3
Tunable Parameters Form



```
                      Tunable Parameters

UDP Port Number for NetWare/IP Service:         43981
DSS-NetWare/IP Server Synchronization Interval: 5   minutes
Primary-Secondary DSS Synchronization Interval: 5   minutes
Maximum UDP Retransmissions:                    3
UDP Checksum?                                   No
Ticks between Nodes on the Same IP Subnet:      2
Ticks between Nodes on the Same IP Net:         4
Ticks between Nodes on Different IP Nets:       6
```

The Tunable Parameters form enables you to modify the following parameters, which affect all hosts in the NetWare/IP domain:

- **UDP Port Number for NetWare/IP Service** —the first of two consecutive port numbers used by DSS servers and NetWare/IP servers and clients to exchange NetWare/IP packets. This port number identifies the port to which UDP datagrams are directed; the next consecutive port number is the port to which NetWare/IP SAP and RIP queries are directed. The default port numbers are 43981 and 43982. If either of these port numbers is already in use for other services on the network, you must assign a different series of port numbers.

- **DSS–NetWare/IP Server Synchronization Interval** —how often the NetWare/IP servers in the NetWare/IP domain query DSS for updated information. The default interval is 5 minutes. The range is 1 to 60 minutes.

- **Primary–Secondary DSS Synchronization Interval** —how often the secondary DSS servers in this NetWare/IP domain query the primary DSS server for updated information. The default interval is 5 minutes. The range is 1 to 240 minutes.

- **Maximum UDP Retransmissions** —the number of times a NetWare/IP host will retransmit a UDP packet without receiving an acknowledgment. After this number of transmissions, the packet is dropped. The default is 3 times. The range is 1 to 48 times.

- **UDP Checksum?** —specifies whether UDP datagrams will use error detection and correction fields for client to server communications. The default is No, which enables UDP to provide its fastest transmission service because it does not have to check for errors. However, it is possible for data to become corrupt during transit. If you choose Yes, packets marked with checksum errors are rejected and retransmitted.

- **Ticks between Nodes on the Same IP Subnet** —the amount of time in ticks (1/18 of a second) it takes a packet to travel one way between hosts on the same subnetwork. The default is 2 ticks. The range is 1 to 1,000 ticks.

- **Ticks between Nodes on the Same IP Net** —the amount of time in ticks (1/18 of a second) it takes a packet to travel one way between hosts on the same network. The default is 4 ticks. The range is 1 to 1,000 ticks.

- **Ticks between Nodes on Different IP Nets** —the amount of time in ticks (1/18 of a second) it takes a packet to travel one way between two hosts on different TCP/IP networks. The default is 6 ticks. The range is 1 to 1,000 ticks.

DSS SAP Filters —displays the DSS SAP Filtering Configuration form. This form is described in the following section.

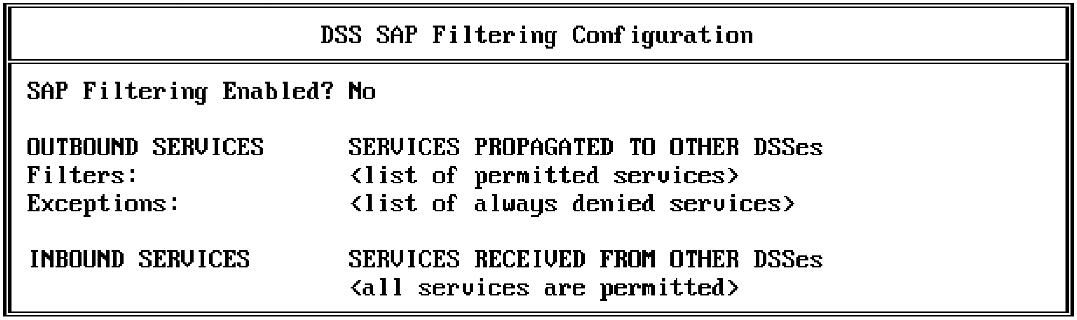
Note

If you change the NetWare/IP domain name, IPX network number, UDP Port Number values, or DSS SAP Filtering after the initial configuration, you must stop and restart the primary DSS server, each secondary DSS server, each NetWare/IP server, and each NetWare/IP client. Changes to the other global parameters are propagated throughout the NetWare/IP network dynamically.

DSS SAP Filtering Configuration Form

Use the DSS SAP Filtering Configuration form to enable and configure DSS SAP filtering.

Figure 8-4
DSS SAP Filtering Configuration Form



```
                    DSS SAP Filtering Configuration

SAP Filtering Enabled? No

OUTBOUND SERVICES      SERVICES PROPAGATED TO OTHER DSSes
Filters:               <list of permitted services>
Exceptions:            <list of always denied services>

INBOUND SERVICES       SERVICES RECEIVED FROM OTHER DSSes
                       <all services are permitted>
```

DSS SAP filters, when applied, allow only SAP traffic that meets specified criteria to be replicated to other DSS servers. DSS SAP filters are applied globally. Every DSS server uses the same set of filters to determine whether or not SAP information should be shared.

If DSS SAP filtering is enabled, each SAP packet received by a DSS server is checked against the defined filters. If the packet matches a filter, the information is flagged as global and is replicated when the DSS servers synchronize. If the packet does not match a filter, the information is flagged as local and is not replicated.

In addition to defining filters, you can define exceptions. Exceptions are defined like filters and enable you to more broadly define a set of filters. Together, filters and exceptions enable you to control the amount of SAP information DSS servers propagate on a NetWare/IP network.

Defining Filters

A DSS SAP filter consists of three elements:

- The IP network or subnetwork address of the host that is advertising a service
- The SAP type, in hexidecimal form
- A server name

When defining filters, you can use *ALL* to specify all IP network and subnetwork addresses or SAP types. Also, you can use the following wildcards as values in the Server Name field:

***** —match any string. SRV* matches all server names which begin with srv, such as srv-mail, srv002, srv-eng, etc.

? —match any single character. MAILSRV? matches all server names with mailsrv as the first seven characters followed by any single character, such as mailsrv1, mailsrv2, etc.

[abc] —match a single character a, b, or c. MAILSRV[158] matches the three server names mailsrv1, mailsrv5, and mailsrv8. Do not separate values with spaces or commas. Only alphanumeric characters are valid.

For example, a filter defined as

Net/Subnet of SAP Reportee: ALL
SAP Type (in hex): 0x0004
Server Name: *

specifies that SAP packets of type 4 from any network address or server name are shared with all DSS servers.

Defining Exceptions

You can define exceptions to filters. For example, suppose you define the filter in the example above, but you don't want SAP packets from a particular server to be distributed globally. You can define an exception to the filter that flags all SAP packets sent by that server as local.

When the DSS server receives a SAP packet from that server, it checks the filter list to see if the information should be distributed globally. The filter indicates that it should. Then, the DSS server checks the exception list. In this case, the exception indicates that it should not, so the SAP information is flagged as local.

When you enable and configure DSS SAP filtering, SAP information that is received by a DSS server but not distributed globally because of filtering is still visible to all NetWare/IP servers and clients that directly use that DSS server. This implies that for each site or geographic region in your network, you should use a standard list of preferred DSS servers. Each NetWare/IP client and server should have the same list of servers in its Preferred DSS Server List.

For instructions on enabling and configuring DSS SAP filtering, see “Enabling and Configuring DSS SAP Filtering” on page 134

Configuring the Primary DSS Server

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**NetWare/IP**

   If the server is not configured for DNS access, the utility displays a message indicating that you must configure this host as a DNS client. If this message does not appear, go to Step 4 .

2. **Press** <Esc> **to continue.**

3. **Fill in the DNS Domain field and at least one Name Server field and press** <Esc> **.**

4. **Choose the Configure Primary DSS option.**

5. **Enter the name of the NetWare/IP domain.**

6. **Enter the fully qualified hostname of the server.**

7. **Enter the IPX network number you have chosen for the NetWare/IP network.**

8. **(Optional) Next to Tunable Parameters, choose <see form> and press** <Enter> **to modify the NetWare/IP tunable parameter settings.**

   For instructions on modifying these parameters, see "Modifying Tunable Parameters" on page 133

9. **(Optional) Next to DSS SAP Filters, choose <see form> and press** <Enter> **to enable and configure DSS SAP filtering.**

   For instructions on enabling and configuring DSS SAP filtering, see "Enabling and Configuring DSS SAP Filtering" on page 134

10. **To exit the Primary DSS Configuration form and save your changes, press** <Esc> **.**

11. **When prompted, choose Yes to save the primary DSS server configuration.**

12. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

After configuring the primary DSS server, you must start the Domain SAP/RIP Service on the server as described in “Starting a DSS Server” on page 127

Important

If you did not already add resource records identifying the primary DSS server to the master DNS database, you must add the records now as described in Chapter 7, “Setting Up DNS Support,” on page 89 If this is a registered DSS server, you must add both NS and A records for the server. If this is an unregistered DSS server, add only an A record for the server.

Setting Up a Secondary DSS Server

After you set up the primary DSS server, you can set up one or more secondary DSS servers. You should configure one DSS server per large network site to provide redundancy and load balancing.

To set up a registered DSS server, you must

1. Configure a NetWare server as a secondary DSS server
2. Add DNS resource records identifying the secondary DSS server
3. Start the Domain SAP/RIP Service on the server

To set up an unregistered secondary DSS server, you must

1. Configure a NetWare server as a secondary DSS server
2. Start the Domain SAP/RIP Service on the server

Secondary DSS Server Guidelines

The impact of the DSS server on network performance is determined by several variables, including the amount and distribution of network traffic, the number of client and server systems, the speed and resources of the DSS servers, and the mix of applications on the network. Therefore, DSS server distribution requirements will vary from site to site. However, there are several guidelines to follow when distributing DSS servers throughout a NetWare/IP internetwork that help optimize network performance:

- Set up at least one DSS server per site or region.

If you have a few large sites in your network, set up a DSS server per site. If you have a lot of small sites, group them by geographic region and set up a DSS server per region.

- Set up multiple DSS servers on subnetworks with heavy traffic. This way, if one DSS server goes down or is too busy to service NetWare/IP hosts, the hosts can contact an alternate DSS server on the same subnet. Otherwise, the hosts would have to be routed to another subnet, which burdens routers and gateways with extra traffic.

- Consider configuring an unregistered DSS server on subnets that are separated from the rest of the NetWare/IP internet by a WAN link, and configure the preferred DSS server list for each node on these subnets to access the unregistered DSS server. This prevents DNS from inadvertently directing NetWare/IP hosts on other subnets to this DSS server for service.

  An unregistered DSS server is a DSS server that is not registered with DNS. The only way for a NetWare/IP host to locate an unregistered DSS server is if the unregistered DSS server is specified in the host's preferred DSS server list. This means that hosts can locate their unregistered DSS server without relying on the DNS server. Thus, you can provide fault tolerance for your network by configuring an unregistered DSS server on isolated network segments.

For information on configuring a secondary DSS server, see “Configuring a Secondary DSS Server” on page 125

Secondary DSS Server Prerequisites

Before you can configure a server as a secondary DSS server (registered or unregistered), the server must meet the following hardware and software requirements:

- The NetWare/IP server software must be installed as described in Chapter 5, “Installing the NetWare/IP Software,” on page 65

- The SYS: volume must have 1 MB of free disk space.

- The memory requirement for a secondary DSS server is the same as for a primary. Use the formula provided in “Primary DSS Server Prerequisites” on page 114 to determine the memory requirement for a secondary DSS server.

- A primary DSS server must be configured and operational.

- The appropriate DNS records must exist for the DSS server.

  If you choose to set up DSS on a server that belongs to a remote DNS domain, you must add DNS resource records to two master DNS databases. You must add a name server record to the master DNS database that is servicing your NetWare/IP domain identifying the DSS server as a name server for the NetWare/IP domain and an address record to the master DNS database of the remote domain specifying the IP address to hostname mapping for the server.

- If the secondary DSS server has multiple IP addresses, you must add the following line to the DSS section of the server's SYS:ETC\NWPARAMS file:

  THIS_DSS_IPADDR *ip_address*

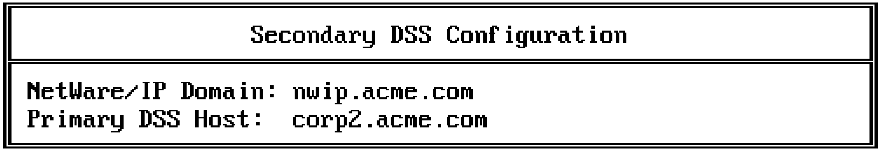
  where *ip_address* is the preferred IP address for use by the DSS server module.

Secondary DSS Configuration Form

Use the Secondary DSS Configuration form to configure a NetWare server as a secondary DSS server.

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

Figure 8-5
Secondary DSS Configuration Form


Secondary DSS Configuration

NetWare/IP Domain: nwip.acme.com
Primary DSS Host: corp2.acme.com

From UNICON's Main Menu, choose the following to display the Secondary DSS Configuration form:

–>**Manage Services**
  –>**NetWare/IP**
    –>**Configure Secondary DSS**

The information required to complete the Secondary DSS Configuration form can be found on a completed NetWare/IP Support Services Planning Worksheet as described in "NetWare/IP Support Services Planning Worksheet" on page 229 A description of each field follows:

- **NetWare/IP Domain** —the name of the NetWare/IP domain. All the NetWare/IP servers and clients using the same primary DSS server are members of this domain. The NetWare/IP domain name conforms to the DNS naming conventions. For additional information about NetWare/IP domains, see "NetWare/IP Domain" on page 36

- **Primary DSS Host** —the name or address of the primary DSS server. Before you can configure a secondary DSS server, you must have a primary DSS server running on the network.

Configuring a Secondary DSS Server

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
     –>**NetWare/IP**

   If the server is not configured for DNS access, the utility displays a message indicating that you must configure this host as a DNS client. If this message does not appear, go to Step 4 .

2. **Press** <Esc> **to continue.**

3. **Fill in the DNS Domain field and at least one Name Server field and then press** <Esc> **.**

4. **Choose the Configure Secondary DSS option.**

   UNICON issues a DHCP request for NetWare/IP information. If a DHCP server responds, you are prompted to confirm the NetWare/IP domain name and primary DSS server name.

5. **When prompted, enter the name of the NetWare/IP domain.**

6. **Enter the name of the primary DSS server for this NetWare/IP domain.**

7. **To exit the form, press** <Esc> **.**

8. **When prompted, choose Yes to save the secondary DSS server configuration.**

9. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Important

If you did not already add resource records identifying the secondary DSS server to the master DNS database, you must add the records now as described in Chapter 7, "Setting Up DNS Support," on page 89 If this is a registered DSS server, you must add both NS and A records for the server. If this is an unregistered DSS server, add only an A record for the server.

After configuring the secondary DSS server, you must start the Domain SAP/RIP Service on the server as described in "Starting a DSS Server" on page 127

Managing the DSS Servers

After you set up primary and secondary DSS servers, DSS requires very little administration. The following sections provide procedures for performing DSS management tasks:

- Starting a DSS Server
- Stopping a DSS Server
- Removing a DSS Server
- Optimizing Performance in WAN Environments
- Modifying Tunable Parameters
- Enabling and Configuring DSS SAP
- Propagating Global Parameter Changes

Starting a DSS Server

Before you can start DSS, you must configure a master DNS server as described in Chapter 7, “Setting Up DNS Support,” on page 89 Before you can start a secondary DSS server, the primary DSS server must be running.

1. **From UNICON’s Main Menu, choose the following:**

   –>**Start/Stop Services**

2. **From the Running Services list, press** <Insert> **.**

   If Domain SAP/RIP Server appears on the Running Services list, the service is already running.

3. **From the Available Services list, choose the Domain SAP/RIP Server option and press** <Enter> **.**

   When you start the DSS server, the DNS server starts automatically if it is not already running. The DSS server uses the DNS server to provide DNS client access.

4. **To return to UNICON’s Main Menu, press** <Esc> **.**

Stopping a DSS Server

1. **From UNICON’s Main Menu, choose the following:**

   –>**Start/Stop Services**

2. **From the Running Services list, choose the Domain SAP/RIP Server option and press** <Delete> **.**

   If Domain SAP/RIP Server is not listed, the DSS server is not running on this server.

3. **When prompted, choose Yes to stop the DSS server.**

4. **To return to UNICON’s Main Menu, press** <Esc> **.**

Removing a DSS Server

The following sections provide procedures for removing each type of DSS server from the network.

Removing the Primary DSS Server

NetWare/IP cannot function without a primary DSS server. Therefore, if you choose to remove the primary DSS server, you must first configure another server as the primary DSS server.

Warning

Do not move the primary DSS server unless absolutely necessary. If you move the primary DSS server, you should use the same IP address to prevent severe service disruption. Designating a new primary DSS server with a different IP address will force you to unload and reload all network nodes.

To remove the primary DSS server, you must

1. Configure another NetWare server as the primary DSS server, as described in “Configuring the Primary DSS Server” on page 121

2. Stop the original primary DSS server, as described in “Stopping a DSS Server” on page 127

3. Stop all NetWare/IP servers and secondary DSS servers.

4. Delete the primary DSS server configuration from the original primary DSS server, as described in “Stopping a DSS Server” on page 127 .

5. Remove or modify any DNS name server (NS) resource records pointing to the original primary DSS server.

6. Reconfigure all secondary DSS servers to use the new primary DSS server, as described in “Stopping a DSS Server” on page 127 .

7. Start the new primary DSS server, as described in “Starting a DSS Server” on page 127

Removing a Secondary DSS Server

To remove a secondary DSS server, you must

1. Stop the secondary DSS server, as described in “Stopping a DSS Server” on page 127

2. Delete the secondary DSS server configuration, as described in “Stopping a DSS Server” on page 127 .

3. Reconfigure any NetWare/IP servers or clients that are configured to use this secondary DSS server as their preferred DSS server.

4. Remove or modify any DNS name server (NS) resource records pointing to the secondary DSS server.

Deleting the DSS Server Configuration

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
       –>**NetWare/IP**
           –>**Delete DSS Configuration**

2. **Press** <Enter> **to continue past the warning.**

3. **When prompted, choose Yes to delete the DSS server configuration.**

4. **Press** <Enter> **to continue.**

5. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Reconfiguring Secondary DSS Servers to Use a New Primary DSS Server

When you set up a different server as the primary DSS server, you must reconfigure all secondary DSS servers in the NetWare/IP domain to use the new primary DSS server. To reconfigure each secondary DSS server, you must

1. Stop the DSS server as described in "Stopping a DSS Server" on page 127

2. Reconfigure the secondary DSS servers to point to the new primary DSS server. To do this, follow the procedure for configuring a secondary DSS server, as described in "Configuring a Secondary DSS Server" on page 125 Enter the hostname of the new primary DSS server in the Primary DSS Host field.

3. Restart the DSS server as described in "Starting a DSS Server" on page 127

Optimizing Performance in WAN Environments

NetWare/IP provides several configuration options to help you optimize network performance in wide area network (WAN) environments, as described in the following sections.

Adjust Tick Values

NetWare/IP maintains information about the length of time in ticks (1/18 second) it takes a packet to travel one way between two hosts. NetWare/IP and IPX-based NetWare clients use tick values to determine how often to retransmit an unacknowledged packet.

If you are running NetWare/IP in a WAN environment, you may find that your IPX client systems time out when trying to communicate with remote hosts. This indicates that the current tick values are inadequate for your slower-speed links. To optimize network performance in these conditions, you can adjust the tick values NetWare/IP assigns. You can customize tick values network-wide or at specific links. For more information on calculating appropriate tick values, see “Calculating Appropriate Tick Values” on page 131

Ticks Between Nodes

WANs:adjusting ticks between nodesYou can set network-wide tick values at the primary DSS server. The tick values you assign here apply to all hosts in the NetWare/IP domain. You can assign tick values between nodes in the

- Same IP subnetwork
- Same IP network
- Different IP networks

For information on configuring the Ticks Between Nodes parameters, see “Configuring the Primary DSS Server” on page 121

Slow Link Customizations

WANs:customizing slow links;WANs Slow Links Customizations parameterYou can customize tick values for specific links at a NetWare/IP server. The tick values you assign here specify the ticks between this server and up to five specific hosts. This parameter overrides the Ticks Between Nodes value specified in the primary DSS server configuration.

You may want to adjust this parameter if you find that modifying the Ticks Between Nodes parameters at the primary DSS server does not completely solve your timeout problems. Specifically, you may need to assign slow link customizations on those NetWare/IP servers that act as IP–IPX gateways and/or send and receive packets over slow WAN links.

If you modify the Slow Links Customizations parameter value, you must unload and reload the NetWare/IP server module for the change to take effect. For information on configuring the Slow Links Customizations parameter, see "Configuring the NetWare/IP Server" on page 142

Calculating Appropriate Tick Values

Use the following procedure to calculate the appropriate tick value to use when configuring the Ticks Between Nodes or the Slow Links Customizations parameters:

1. **Load the NetWare PING utility by typing the following command at the server console prompt:**

   load ping <Enter>

2. **Type the name or IP address of a host on the network you are calculating tick values for and press** <Enter> **.**

3. **Press** <Esc> **to begin pinging the specified host.**

4. **To calculate an appropriate tick value to use to communicate with hosts on this network, divide the value displayed in the average column by 110.**

   The resulting value represents the amount of time in ticks it takes a packet to travel one way between your server and the specified host. Use this value to configure the Ticks Between Nodes or Slow Links Customizations parameters.

5. **Press** <Esc> **to exit the PING utility.**

6. **When prompted, choose Yes to return to the server console prompt.**

Adjust the Database Synchronization Interval

Database synchronization is the process by which the primary DSS server obtains updates from secondary DSS servers and NetWare/IP servers. During a primary DSS–secondary DSS database synchronization, the secondary DSS servers upload any SAP or RIP information they have updated since the last database synchronization to the primary DSS server and download all changed SAP and RIP records and updated configuration information from the primary DSS server. During a DSS–NetWare/IP database synchronization, the NetWare/IP server downloads all new or changed SAP and RIP records from its current DSS server.

By default, the database synchronization intervals are set to five minutes. However, in WAN environments you may want to increase the interval to reduce traffic over WAN links. You can adjust either of the database synchronization interval parameters at the primary DSS server.

For additional information on adjusting the database synchronization intervals, see “Configuring the Primary DSS Server” on page 121

Configure Unregistered DSS Servers on Remote Network Segments

An unregistered DSS server is a DSS server that is not registered with DNS. Thus, a NetWare/IP node cannot locate an unregistered DSS server by issuing a DNS query. Instead, the NetWare/IP node must be specifically configured with the name or address of the unregistered DSS server as part of its preferred DSS server list.

Configuring an unregistered DSS server on network segments separated from the rest of your network by WAN links reduces DNS query traffic. In addition, because the unregistered DSS server is not registered with DNS, other NetWare/IP hosts cannot inadvertently be directed to this DSS server when other, closer DSS servers are busy or down.

For additional information on configuring an unregistered DSS server, see “Setting Up a Secondary DSS Server” on page 122

Configure DSS SAP Filters

DSS SAP filters, when applied, allow only SAP traffic that meets specified criteria to be replicated to other DSS servers. DSS SAP filters are applied globally. Every DSS server uses the same set of filters to determine whether or not SAP information should be shared.

If DSS SAP filtering is enabled, each SAP packet received by a DSS server is checked against the defined filters. If the packet matches a filter, the information is flagged as global and is replicated when the DSS servers synchronize. If the packet does not match a filter, the information is flagged as local and is not replicated.

For instructions on enabling and configuring DSS SAP filtering, see “Enabling and Configuring DSS SAP Filtering” on page 134

Modifying Tunable Parameters

You can optimize DSS server performance by using UNICON to adjust the primary DSS server tunable parameters. These parameters affect the performance of all hosts in the NetWare/IP domain.

1. **From UNICON’s Main Menu, choose the following:**

   –>**Manage Services**
     –>**NetWare/IP**
       –>**Configure Primary DSS**

2. **Choose <see form> in the Tunable Parameters field to display the list of parameters.**

3. **Use the Up- and Down-arrow keys to choose the parameter that you want to change, and enter the new value.**

4. **Press** <Esc> **to return to the Primary DSS Configuration form.**

5. **Press** <Esc> **to exit the form.**

6. **When prompted, choose Yes to save your changes.**

7. **To return to UNICON’s Main Menu, press** <Esc> **as needed.**

Important

If you change the NetWare/IP Domain, IPX Network Number, or UDP Port Number parameter values after your initial configuration, you must stop and restart the primary DSS server, each secondary DSS server, each NetWare/IP server, and each NetWare/IP client. Changes to any of the other global parameters are dynamically propagated throughout the NetWare/IP network.

In addition to modifying DSS tunable parameters at the primary DSS server with UNICON, you can modify the following parameters manually by using any text editor to edit the SYS:ETC\NWPARAMS file:

- DSS Dedicated Mode

By default, the DSS server runs in dedicated mode. If you want to free some system resources for other NLMs, you can edit the DEDICATED_DSS line in the DSS section of the server's SYS:ETC\NWPARAMS file as follows:

DEDICATED_DSS 0 disables dedicated mode.

DEDICATED_DSS 1 enables dedicated mode.

After changing the dedicated mode parameter, you must unload and reload the DSS NLM for the change to take effect.

- Maximum number of UDP datagrams and TCP connections

  You can manually increase the maximum size of the UDP packet queues and the maximum number of simultaneous TCP connections maintained by DSS for storing SAP and RIP information by editing the following lines in the DSS section of the server's SYS:ETC\NWPARAMS file:

  MAX_UDP_PKTS *X (default=64)*

  MAX_TCP_CONNS *Y (default=16)*

  X and *Y* must be decimal integers greater than the default values.

  After changing the maximum number of UDP datagrams and TCP connections parameters, you must unload and reload the DSS NLM for the change to take effect. Changes to these parameters on a DSS server are not propagated to other DSS servers.

Enabling and Configuring DSS SAP Filtering

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**NetWare/IP**
   –>**Configure Primary DSS**

2. **Choose <see form> in the DSS SAP Filters field to display the list of parameters.**

3. **Press** <Enter> **and choose Yes to enable SAP filtering.**

   To add, modify, or delete an exception to an existing filter, skip to Step 9 .

4. **Choose <list of permitted services> and press** <Enter> **to configure SAP filtering.**

5. **To add a filter to the list, press** <Insert> **.**

   5a. **Enter the IP network address or subnetwork address of the host(s) that is advertising a service you want distributed globally.**

   5b. **Enter the SAP type (in hexidecimal format) that you want distributed globally.**

   5c. **Enter the name of the server that is advertising a service you want distributed globally.**

   5d. **Press** <Esc> **and choose Yes to save the defined SAP filter.**

6. **To edit a filter in the list, choose the filter and press** <Enter> **.**

7. **To delete a filter in the list, choose the filter and press** <Delete> **.**

8. **When you are finished, press** <Esc> **to return to the DSS SAP Filtering Configuration form.**

9. **Choose <list of always denied services> and press** <Enter> **to configure filter exceptions.**

   Configure exceptions the same as filters. Complete Steps 5 through 8.

10. **Press** <Esc> **and choose Yes to save your changes.**

Important

If you save changes to the DSS SAP filters, you must stop and restart the primary DSS server to implement the changes. Secondary DSS servers will receive the new filter criteria after the next synchronization interval.

Configuring Other Filtering Options

In addition to DSS SAP filtering, IPX-based filtering is supported via the INETCFG and FILTCFG NLMs. To enable IPX-based filtering, complete the following procedure at the IP–IPX forwarding gateways:

1. **At the server's system console prompt, type the following command:**

   LOAD INETCFG <Enter>

If INETCFG detects changes in the AUTOEXEC.NCF file when it loads, you are prompted to transfer LAN driver, protocol, and remote access commands from the AUTOEXEC.NCF file to configuration files maintained by INETCFG. In almost all cases, you should enter Yes to this prompt.

2. **(Conditional) If you installed NetWare/IP and NetWare 4 at the same time using the integrated install option, configure the NetWare/IP board.**

   2a. **From the Internetworking Configuration menu, choose Boards.**

   2b. **Press** <Insert> **and choose NWIP from the list of Available Drivers.**

   2c. **On the Board Configuration form, enter any unique name in the Board Name field.**

   2d. **Press** <Esc> **, and confirm that you want to save the changes when prompted.**

   2e. **Press** <Esc> **to return to the Internetworking Configuration menu.**

3. **From the Internetworking Configuration menu, choose Protocols.**

4. **Choose the IPX protocol and press** <Enter> **.**

5. **On the IPX Protocol Configuration form, enable Packet Forwarding, choose RIP/SAP Only in the Routing Protocol field, and enable Filtering Support.**

6. **Press** <Esc> **as needed to exit INETCFG.**

7. **At the server's system console prompt, type the following command:**

   REINITIALIZE SYSTEM <Enter>

8. **Use FILTCFG.NLM to define SAP/RIP filters.**

Propagating Global Parameter Changes

Secondary DSS servers and NetWare/IP servers detect changes in the global parameters during database synchronization. The new global parameters are then downloaded along with the updated SAP/RIP records.

Changes to any of the following global parameters take place as soon as they are downloaded:

- DSS–NetWare/IP synchronization interval
- Primary DSS–secondary DSS synchronization interval
- Maximum UDP retransmissions
- UDP checksum
- Ticks between nodes on the same IP subnet
- Ticks between nodes on the same IP net
- Ticks between nodes on different IP nets
- DSS SAP filters or exceptions

Note

You may notice degraded network connectivity while the new parameter values are being propagated throughout the network. This condition is temporary and stops after all DSS servers and NetWare/IP servers have been updated.

Changes to the following parameters cannot be propagated dynamically:

- NetWare/IP domain name
- IPX network number
- UDP port number

If you modify any of these parameters, you must immediately unload and reload all NetWare/IP components in the following sequence:

1. Primary DSS server
2. Secondary DSS servers

3. NetWare/IP servers

4. NetWare/IP clients

Designating a New DNS Name Server

Every DSS server, NetWare/IP server, and NetWare/IP client is configured with the hostname or IP address of the DNS name server to which it should direct its DNS queries. If you move the DNS service to a new server, you must modify the configuration of each NetWare/IP node with the hostname or IP address of the new DNS name server.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Global Objects**
   –>**Configure Server Profile**

2. **On the Server Profile Configuration form, enter the DNS domain name in the (DNS) Domain field.**

3. **Enter the IP address of the new DNS name server.**

4. **Press** <`Esc`> **to exit the screen, save your changes, and return to UNICON's Main Menu.**

Chapter

9 *Configuring NetWare/IP Servers*

The last step in configuring the NetWare/IP service is configuring the NetWare/IP™ servers on your network. Before you configure the NetWare/IP servers, you should be familiar with the concept of the NetWare/IP domain as explained in "NetWare/IP Domain" on page 36

Important You must set up DNS and DSS servers as described in Chapter 7, "Setting Up DNS Support," on page 89 and Chapter 8, "Configuring the Domain SAP/RIP Service," on page 113 before you configure a NetWare/IP server.

Setting Up a NetWare/IP Server

To set up a NetWare/IP server, you must complete the following tasks:

1. Configure a NetWare 4™ server as a NetWare/IP server.

2. Start the NetWare/IP service.

NetWare/IP Server Prerequisites

Before you can configure a NetWare/IP server, the server must meet the following hardware and software requirements:

- The NetWare/IP server software must be installed as described in Chapter 5, "Installing the NetWare/IP Software," on page 65

- The SYS: volume must have 1 MB of free disk space.

- The amount of memory required depends on the number of server nodes in the network. Use the following formula to determine the memory requirements for a NetWare/IP server, where *a* equals the number of servers in the network:

  (*a* x 380) + 258,000 = memory in bytes needed on the server.

Using the NetWare/IP Administration Forms

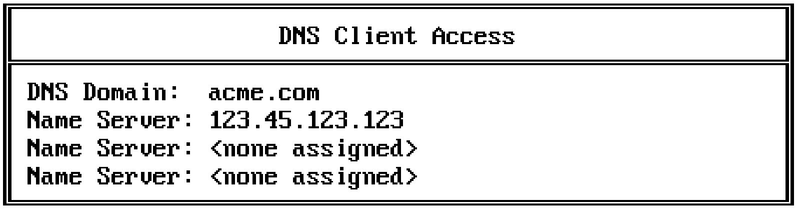
The NWIPCFG forms you use to configure a NetWare/IP server are shown and described in the following sections.

If you need information about a specific field when accessing an online form using NWIPCFG, press <F1> .

DNS Client Access Form

The server must be set up as a DNS client or resolver. Use this form to configure the server as a DNS client.

Figure 9-1
DNS Client Access Form



```
                    DNS Client Access

DNS Domain:  acme.com
Name Server: 123.45.123.123
Name Server: <none assigned>
Name Server: <none assigned>
```

The utility displays this form only if you do not have DNS access set up on this server. You might already have DNS access set up if you configured this machine as a DNS name server, you used the Server Profile Configuration form to enable DNS client access, or the server is running another product that uses DNS.

From NWIPCFG's NetWare/IP Administration menu, choose the following to display the DNS Client Access form:

–>**Configure DNS Client**

The information required to complete the DNS Client Access form can be found on a completed NetWare/IP Support Services Planning Worksheet as described in "NetWare/IP Support Services Planning Worksheet" on page 229 A description of each field follows.

DNS Domain —the name of the DNS domain to which the server belongs. The utility checks to make sure that you enter a valid DNS domain name. If you are not sure of the correct syntax, see "Domain Names" on page 25

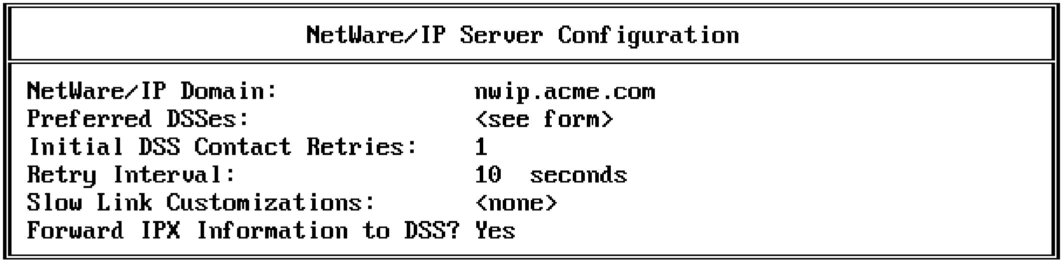
Name Server —the DNS name server this NetWare/IP server should contact first to resolve DNS queries. Type the hostname or IP address of the nearest DNS name server.

Name Server —the additional Name Server fields specify additional DNS name servers this DSS server should contact to resolve DNS queries. You do not need to fill in these fields if information about all hosts in your network is available through the first DNS name server.

NetWare/IP Server Configuration Form

Use the NetWare/IP Server Configuration form to configure a NetWare/IP server.

Figure 9-2
NetWare/IP Server Configuration Form



```
                    NetWare/IP Server Configuration

NetWare/IP Domain:                nwip.acme.com
Preferred DSSes:                  <see form>
Initial DSS Contact Retries:      1
Retry Interval:                   10  seconds
Slow Link Customizations:         <none>
Forward IPX Information to DSS?   Yes
```

From NWIPCFG's NetWare/IP Administration menu, choose the following to display the NetWare/IP Server Configuration form:

–>**Configure NetWare/IP Server**

The information required to complete the NetWare/IP Server Configuration form can be found on a completed NetWare/IP Servers Planning Worksheet as described in “NetWare/IP Servers Planning Worksheet” on page 231 A description of each field follows.

- **NetWare/IP Domain** —the name of the NetWare IP domain. All the NetWare/IP servers and clients using the same primary DSS server are members of this domain. The NetWare/IP domain name conforms to the same naming conventions as the DNS domain names. For additional information about setting up a NetWare/IP domain, see “NetWare/IP Domain” on page 36

- **Preferred DSSes** —the hostnames, IP addresses, or subnetwork IP addresses of up to five DSS servers that are closest to this NetWare/IP server. The NetWare/IP server will attempt to contact the DSS servers on this list sequentially before querying a DNS name server for a list of all available DSS servers. In addition, the only way for a NetWare/IP server to locate an unregistered DSS server is if it is configured as a preferred DSS server for the NetWare/IP server. For more information on using the Preferred DSSes field to optimize network performance, see “Optimizing Performance in WAN Environments” on page 130

- **Initial DSS Contact Retries** —the number of times the NetWare/IP server will retransmit an unacknowledged query to a DSS server at startup. The default is 1 retry. The range is 0 to 50 retries.

- **Retry Interval** —the length of time in seconds the NetWare/IP server will wait before retransmitting a unacknowledged query to a given DSS server at startup. The default is 10 seconds. The range is 5 to 100 seconds.

- **Slow Link Customizations** —the amount of time in ticks (1/18 of a second) it takes a packet to travel one way between this NetWare/IP server and a specified host or subnetwork. The range is 1 to 255 ticks. For more information on customizing slow links, see “Optimizing Performance in WAN Environments” on page 130 .

- **Forward IPX Information to DSS** —specifies whether this NetWare/IP server should act as a forwarding gateway. The default is no. For more information on NetWare/IP gateways, see “Gateway Configuration” on page 54

- **Preferred IP Address** —the IP address chosen for NetWare/IP. The utility displays this field only if the server contains more than one network board. Pressing <Enter> in this field displays a list of available IP addresses for this server.

Configuring the NetWare/IP Server

You use the NWIPCFG utility to configure a NetWare/IP server. The information you need to configure a NetWare/IP server is contained in the NetWare/IP Servers Planning Worksheet as described in “NetWare/IP Servers Planning Worksheet” on page 231

1. **From NWIPCFG’s NetWare/IP Administration menu, choose the following:**

–>**Configure NetWare/IP Server**

NWIPCFG issues a DHCP request for NetWare/IP information. If a DHCP server responds, you are prompted to confirm the NetWare/IP domain name and primary DSS server name.

2. **In the NetWare/IP Domain field, enter the fully qualified NetWare/IP domain name.**

3. **Fill in other configuration fields as appropriate for your network.**

4. **Press** <Esc> **to exit the form.**

5. **When prompted, choose Yes to save the NetWare/IP server configuration.**

After you configure the NetWare/IP server, you must start the NetWare/IP service as described in “Starting the NetWare/IP Service” on page 146

Configuring a NetWare/IP Server as a Gateway

You can configure a NetWare/IP server to function as a forwarding gateway, a one-way forwarding gateway, or a non-forwarding gateway. For a description of each type of gateway, see “Gateway Configuration” on page 54

The following sections provide procedures for completing the gateway configuration tasks.

Configuring a Forwarding Gateway

To configure a server as a bidirectional forwarding gateway, you must complete the following tasks:

1. Bind IPX to a network board in the server.

2. If IPXRTR is loaded with the **route=none** parameter, unload IPXRTR and reload it without the **route=none** parameter. If necessary, remove any command that loads IPXRTR with the **route=none** parameter from the server's AUTOEXEC.NCF file.

3. Configure the server to forward IPX information to DSS.

Configuring a One-Way Forwarding Gateway

To configure a NetWare/IP server as a one-way forwarding gateway, which only enables IPX-based clients to see and access IP services, you must complete the following tasks:

1. Bind IPX to a network board in the server.

2. If IPXRTR is loaded with the **route=none** parameter, unload IPXRTR and reload it without the **route=none** parameter. If necessary, remove any command that loads IPXRTR with the **route=none** parameter from the server's AUTOEXEC.NCF file.

Configuring a Non-Forwarding Gateway

To configure a NetWare/IP server as a non-forwarding gateway, you must bind IPX to a network board in the server.

Binding IPX to the LAN Driver

You must bind the IPX protocol to a server's LAN driver and to a specific network board to configure the server as a non-forwarding or forwarding gateway. You can bind IP and IPX to the same LAN driver and network board, or you can install a separate network board and LAN driver to bind to IPX.

For more information on the BIND command, refer to the *Utilities Reference* manual, which is part of the NetWare 4 documentation set. For instructions on binding a protocol to a network board, see *Supervising the Network* , which is also part of the NetWare 4 documentation set.

Enabling the Forwarding Gateway Function

1. **From NWIPCFG's NetWare/IP Administration menu, choose the following:**

   –>**Configure NetWare/IP Server**

2. **With the cursor in the Forward IPX Information to DSS? field, press** <Enter> **.**

3. **When prompted, choose Yes to enable the forwarding function.**

4. **Press** <Esc> **to exit the form.**

5. **When prompted, choose Yes to save the configuration changes.**

Note

You can also enable SAP/RIP forwarding from the server console prompt by typing **load nwip /forward=yes** <Enter> .

Removing a Gateway

To remove the gateway function from a NetWare/IP server, you must unbind the IPX protocol from the LAN driver. Also, if the server is configured as a forwarding gateway, you must disable the forwarding parameter. The following sections provide procedures for each of these tasks.

Unbinding IPX from the LAN Driver

For instructions on unbinding a protocol from a network board, see *Supervising the Network* , which is part of the NetWare 4 documentation set.

Disabling SAP/RIP Forwarding

To remove a forwarding gateway, you must modify the NetWare/IP server configuration to disable the forwarding of SAP and RIP information from the IPX network to DSS.

1. **From NWIPCFG's NetWare/IP Administration menu, choose the following:**

   –>**Configure NetWare/IP Server**

2. **With the cursor in the Forward IPX Information to DSS? field, press** <Enter> **.**

3. **When prompted, choose No to disable the forwarding function.**

4. **To exit the form, press** <Esc> **.**

5. **When prompted, choose Yes to save the NetWare/IP server configuration.**

Note

You cannot disable SAP/RIP forwarding from the server console prompt with the **load nwip /forward=no** <Enter> command. You must disable forwarding as described above and restart the NetWare/IP service.

Managing the NetWare/IP Server

This section provides procedures for performing common NetWare/IP server management tasks.

Starting the NetWare/IP Service

Before you can start the NetWare/IP service, you must have both DNS and DSS servers running on the network.

1. **From NWIPCFG's NetWare/IP Administration menu, choose the following:**

   –>**Start NetWare/IP Server**

2. **When prompted, press** <Esc> **to return to the NetWare/IP Administration menu.**

Stopping the NetWare/IP Service

1. **From UNICON's Main Menu, choose the following:**

   –>**Start/Stop Services**

2. **From the Running Services list, choose the NetWare/IP Server entry and press** <Delete> **.**

   If the NetWare/IP Server entry does not appear in the list, the service is not running on this server.

3. **When prompted, choose Yes to stop the NetWare/IP service.**

4. **To return to UNICON's Main Menu, press** <Esc> **.**

When you stop a NetWare/IP server, the server reports its status to a DSS server. If the NetWare/IP server and the DSS server are running on the same machine, the NetWare/IP server will most likely report its status to the local DSS server. This results in a problem if you immediately stop the DSS server after stopping the NetWare/IP server, because the rest of the network will not learn about the down status of the NetWare/IP server.

To avoid this situation, type the following command at the server's console prompt after stopping the NetWare/IP server and before stopping the DSS server:

LOAD DSS /SYNC <Enter>

Removing a NetWare/IP Server

To remove a NetWare/IP server, you must delete its NetWare/IP configuration. You do this using the UNICON utility.

Important Before removing a NetWare/IP server, be sure to reconfigure all NetWare/IP client systems that use this server as the nearest NetWare/IP server.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**NetWare/IP**
   –>**Delete NetWare/IP Configuration**

2. **Press** <Enter> **to clear the warning message.**

3. **When prompted, choose Yes to delete the NetWare/IP configuration on this server.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Designating a New DNS Name Server

Every DSS server, NetWare/IP server, and NetWare/IP client is configured with the hostname or IP address of the DNS name server to which it should direct its DNS queries. If you move the DNS service to a new server, you must modify the configuration of each NetWare/IP node with the hostname or IP address of the new DNS name server. For information on configuring the NetWare/IP server to direct its DNS queries to a new name server, see "Gateway Configuration" on page 54 .

Chapter

10 *Troubleshooting*

This chapter describes tools and procedures you can use to monitor the performance of a NetWare/IP™ network and to identify problems with specific NetWare/IP modules. This chapter includes the following sections:

- Managing Error Reporting
- Managing SNMP Reporting
- Using NetWare/IP with ManageWise Autodiscovery
- Troubleshooting DSS Servers
- Troubleshooting Remote Name Servers
- Troubleshooting the NetWare/IP Server
- Troubleshooting NetWare/IP Clients
- Troubleshooting UNICON
- Common Error Messages and Solutions

Managing Error Reporting

The error reporting system maintains a log of system errors. You can use UNICON to configure the type of errors and the destination of the alerts logged by the error reporting system. The following sections provide procedures for managing error reporting.

Error Reporting Management Screens

Manage error reporting using the following screens:

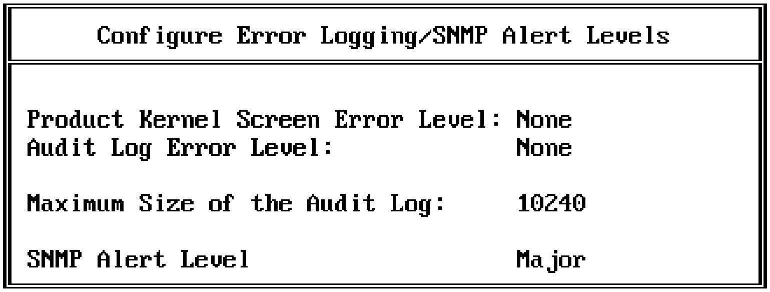
- Configure Error Logging/SNMP Alert Levels form
- AUDIT.LOG file
- Product Kernel Message screen

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

Configure Error Logging/SNMP Alert Levels Form

Use the Configure Error Logging/SNMP Alert Levels form to set up error reporting on a server. You can set reporting levels for the error reporting system and for SNMP. Error messages issued by the error reporting system can be sent to the AUDIT.LOG file or the Product Kernel screen or both. You can also modify the size of the AUDIT.LOG file.

Figure 10-1
Configure Error Logging/SNMP Alert Levels Form



```
      Configure Error Logging/SNMP Alert Levels

Product Kernel Screen Error Level: None
Audit Log Error Level:             None

Maximum Size of the Audit Log:     10240

SNMP Alert Level                   Major
```

From UNICON's Main Menu, choose the following to display the Configure Error Logging/SNMP Alert Levels form:

–>**Configure Error Reporting**
–>**Configure Error Logging/SNMP Alert Levels**

The Configure Error Logging/SNMP Alert Levels form contains the following fields:

Product Kernel Screen Error Level —the level of error messages sent to the product kernel console screen. Pressing <Enter> displays a list of error levels from which you can choose. You can also turn off error reporting from this list.

Audit Log Error Level —the level of error messages written to the AUDIT.LOG file. Pressing <Enter> displays a list of available error levels.

Maximum Size of the Audit Log —the maximum size of the audit file. The default is 10,240 bytes. The maximum size is 262,144 bytes. After the file fills up, the new messages overwrite the oldest messages in the file.

If you increase the maximum size of the AUDIT.LOG file, make sure that the TCP/IP Physical Receive Packet Size parameter is set to a minimum value of 4202. This parameter is reset by the following optional line in the STARTUP.NCF file:

MAXIMUM PHYSICAL RECEIVE PACKET SIZE = *X*

X must be 4202 or larger. You can also remove this line, and the system will set this parameter to the default value of 4202.

SNMP Alert Level —the level of SNMP message reported to SNMP management stations. Pressing <Enter> displays a list of available alert levels. You can also turn off SNMP reporting from this list.

The following error reporting levels are available to the Product Kernel screen or the Audit Log (for SNMP alert levels, see "SNMP Management Screens" on page 156):

- **None** —suppresses error reporting
- **Error** —provides essential notice about a critical problem or likely failure
- **Warning** —provides notice about a potential problem that could lead to failure if nothing is done to remedy the situation
- **Informational** —provides additional descriptive information
- **Debug** —provides detailed information that Novell's technical support staff can use to evaluate a problem

Each level incorporates the information in the levels listed above it. For example, if you choose Informational, you also receive Warnings and Errors.

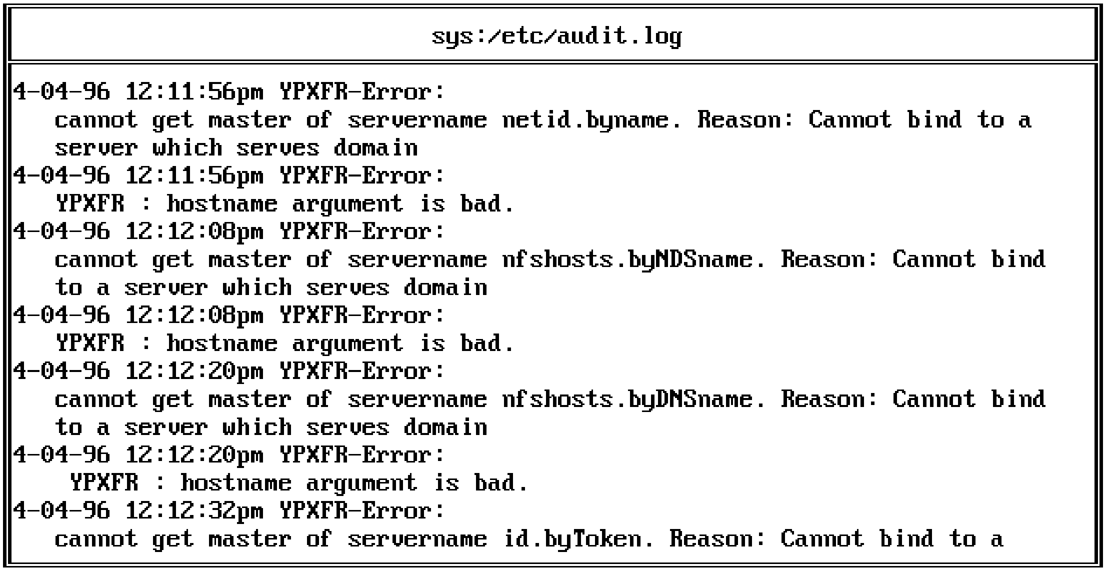
You can choose to have the error reporting messages displayed on the Product Kernel screen, written to the AUDIT.LOG file, or both. The error level settings for the screen are independent of the settings for the log file. The default settings are as follows:

Error level to Product Kernel screen	Error
Error level to audit log	Warning
Maximum size of the audit log	10240 bytes

AUDIT.LOG File

The AUDIT.LOG file records the specified type of error messages. This file is shown in the following screen:

Figure 10-2
AUDIT.LOG File



```
                         sys:/etc/audit.log
4-04-96 12:11:56pm YPXFR-Error:
   cannot get master of servername netid.byname. Reason: Cannot bind to a
   server which serves domain
4-04-96 12:11:56pm YPXFR-Error:
   YPXFR : hostname argument is bad.
4-04-96 12:12:08pm YPXFR-Error:
   cannot get master of servername nfshosts.byNDSname. Reason: Cannot bind
   to a server which serves domain
4-04-96 12:12:08pm YPXFR-Error:
   YPXFR : hostname argument is bad.
4-04-96 12:12:20pm YPXFR-Error:
   cannot get master of servername nfshosts.byDNSname. Reason: Cannot bind
   to a server which serves domain
4-04-96 12:12:20pm YPXFR-Error:
    YPXFR : hostname argument is bad.
4-04-96 12:12:32pm YPXFR-Error:
   cannot get master of servername id.byToken. Reason: Cannot bind to a
```

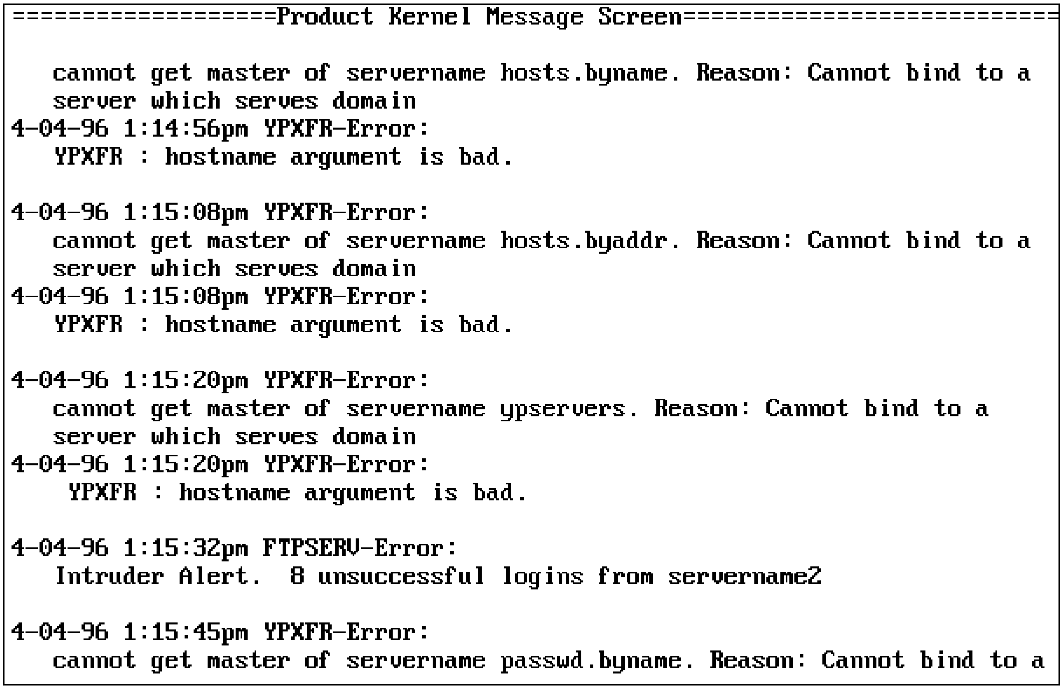
From UNICON’s Main Menu, choose the following to display the AUDIT.LOG file:

–>**Configure Error Reporting**
–>**Display Audit Log**

Product Kernel Screen

The Product Kernel screen displays on the server console. It shows ongoing messages related to the operation of active NetWare® services. This screen also displays those error messages produced by the error reporting system that you designate from within UNICON to display on the Product Kernel screen.

Figure 10-3
Product Kernel Screen



```
==================Product Kernel Message Screen==========================

   cannot get master of servername hosts.byname. Reason: Cannot bind to a
   server which serves domain
4-04-96 1:14:56pm YPXFR-Error:
   YPXFR : hostname argument is bad.

4-04-96 1:15:08pm YPXFR-Error:
   cannot get master of servername hosts.byaddr. Reason: Cannot bind to a
   server which serves domain
4-04-96 1:15:08pm YPXFR-Error:
   YPXFR : hostname argument is bad.

4-04-96 1:15:20pm YPXFR-Error:
   cannot get master of servername ypservers. Reason: Cannot bind to a
   server which serves domain
4-04-96 1:15:20pm YPXFR-Error:
    YPXFR : hostname argument is bad.

4-04-96 1:15:32pm FTPSERV-Error:
   Intruder Alert.  8 unsuccessful logins from servername2

4-04-96 1:15:45pm YPXFR-Error:
   cannot get master of servername passwd.byname. Reason: Cannot bind to a
```

To display the Product Kernel screen, start at any UNICON screen, hold down <Alt> , and press <Esc> until the Product Kernel screen is displayed. To return to UNICON, hold down <Alt> and press <Esc> until the a UNICON screen is displayed.

Viewing the AUDIT.LOG File

1. **From UNICON’s Main Menu, choose the following:**

–>**Configure Error Reporting**
   –>**Display Audit Log**

2. **Press** <Esc> **to exit the AUDIT.LOG file.**

3. **To return to UNICON's Main Menu, press** <Esc> **.**

Saving the AUDIT.LOG File

You cannot save or append the AUDIT.LOG file to an existing file.

1. **From UNICON's Main Menu, choose the following:**

   –>**Configure Error Reporting**
      –>**Save Audit Log**

2. **When prompted, enter the full path and name of the file to which you want to back up the Audit Log.**

3. **To return to UNICON's Main Menu, press** <Esc> **.**

Deleting the Contents of the AUDIT.LOG File

Because this procedure immediately erases the contents of the audit log, you might want to save the audit log before you clear it.

1. **From UNICON's Main Menu, choose the following:**

   –>**Configure Error Reporting**
      –>**Clear Audit Log**

2. **When prompted, choose Yes to erase the AUDIT.LOG file.**

3. **Press** <Enter> **to clear the status message.**

4. **To return to UNICON's Main Menu, press** <Esc> **.**

Clearing the Product Kernel Screen

1. **From UNICON's Main Menu, choose the following:**

–>Configure Error Reporting
  –>Clear Product Kernel Screen

2. **Press** <Enter> **to clear the status message.**

3. **To return to UNICON’s Main Menu, press** <Esc> **.**

Configuring Error Reporting

1. **From UNICON’s Main Menu, choose the following:**

   –>Configure Error Reporting
     –>Configure Error Logging/SNMP Alert Levels

2. **From the Configure Error Logging/SNMP Alert Levels form, choose the level of reporting to be sent to the Product Kernel screen and to the audit log by choosing the appropriate field.**

3. **From the Error Level list, choose None or the level of error message that you want reported.**

4. **Choose the Maximum Size of the Audit Log field. Enter the maximum number of bytes.**

5. **Press** <Esc> **to exit the Configure Error Logging/SNMP Alert Levels form.**

6. **To return to UNICON’s Main Menu, press** <Esc> **.**

Managing SNMP Reporting

SNMP provides a means for you to manage distributed network nodes from a central location called an *SNMP management station* . From the SNMP management station, you can view the following types of information about network nodes:

- Event activity alarms

- Performance statistics

The following sections describe the SNMP services available with NetWare/IP and provide procedures for setting up and managing SNMP reporting.

SNMP Management Screens

Manage SNMP alerts using the following screens:

- SNMP Manager Table
- Configure Error Logging/SNMP Alert Levels form

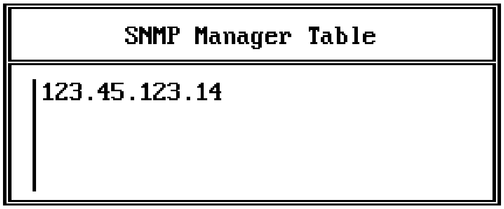
These screens are described in the following sections.

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

SNMP Manager Table

Use the SNMP Manager Table to specify the SNMP management station to which the current server should direct its SNMP trap messages.

Figure 10-4
SNMP Manager Table



SNMP Manager Table

123.45.123.14

To display the SNMP Manager Table, start the INETCFG utility as described in “Specifying an SNMP Management Station” on page 158

From the Internetworking Configuration menu, choose the following:

```
–>Protocols
   –>TCP/IP
```

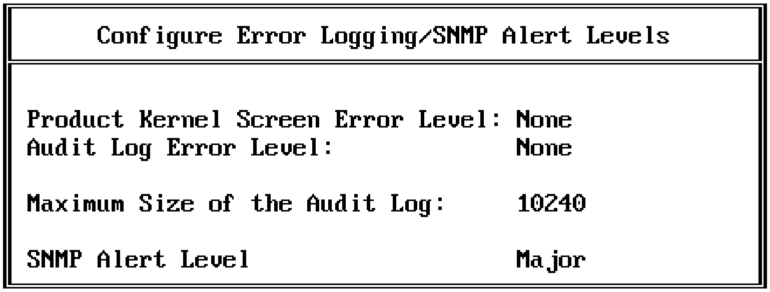
The utility displays the TCP/IP Protocol Configuration form. Choose the SNMP Manager Table field. The utility displays the SNMP Manager Table.

From the SNMP Manager Table, you can specify an SNMP management station for this server by pressing <Insert> and typing the name or address of the SNMP management station. To delete an SNMP management station entry, choose the entry and press <Delete> .

Configure Error Logging/SNMP Alert Levels Form

Use the Configure Error Logging/SNMP Alert Levels form to set reporting levels for SNMP alarms.

Figure 10-5
Configure Error Logging/SNMP Alert Levels Form



```
Configure Error Logging/SNMP Alert Levels

Product Kernel Screen Error Level: None
Audit Log Error Level:             None

Maximum Size of the Audit Log:     10240

SNMP Alert Level                   Major
```

From UNICON's Main Menu, choose the following to display the Configure Error Logging/SNMP Alert Levels form:

–>**Configure Error Reporting**
–>**Configure Error Logging/SNMP Alert Levels**

The Configure Error Logging/SNMP Alert Levels form contains one field pertaining to SNMP:

SNMP Alert Level —the level of SNMP alarm reported to SNMP management stations. Pressing <Enter> displays a list of available levels. You can also turn off SNMP reporting from this list.

You can choose the following SNMP alarm levels:

- **None** —suppresses SNMP alarm reporting
- **Critical** —provides warnings about urgent problems that require immediate action to prevent wide-spread failure
- **Major** —provides warnings about serious problems that require prompt action to prevent failure of the object and possibly some related objects
- **Minor** —provides information about problems that can be addressed as work schedules permit

- **Informational** —provides descriptive information that can be used for such things as trend analysis and planning

Each level incorporates the information in the levels listed above it. For example, if you choose Minor, you also receive Major and Critical messages.

Setting Up SNMP Alarm Reporting

In SNMP, an alarm at an SNMP management station indicates a network event. When an event occurs at a node managed by SNMP, a type of message called a trap is sent to the SNMP management station. For example, SNMP might send a cold start trap to the management station immediately after a node starts up. You can use SNMP to monitor events on your NetWare/IP, DSS, and DNS servers.

If you plan to use SNMP to monitor NetWare/IP events, you must complete the following tasks:

1. Specify the SNMP management station to receive trap messages for each node

2. Copy the DSS.MIB file from the NetWare/IP product diskettes to the SNMP management station

3. Configure the SNMP alert level

The following sections provide procedures for setting up SNMP alarm reporting.

Specifying an SNMP Management Station

To specify an SNMP management station to receive traps for a node, you must add the management station's name or address to the node's SYS:/ETC/TRAPTARG.CFG file. You can edit this file using the Internetworking Configuration (INETCFG) utility.

1. **At the server console, type the following command:**

   load inetcfg <Enter>

2. **From the Internetworking Configuration menu, choose the following:**

–>Protocols
–>TCP/IP

3. **From the TCP/IP Protocol Configuration form, choose the SNMP Manager Table field.**

4. **At the SNMP Manager Table, press** <Insert> **to add the name or address of the destination SNMP management station.**

5. **When prompted, enter the name or address of the SNMP management station.**

6. **To save your entry, press** <Esc> **.**

7. **When prompted, choose Yes to save your changes.**

8. **To exit the INETCFG utility, press** <Esc> **as needed and choose Yes when prompted.**

Configuring the SNMP Alarm Level

The NetWare/IP server sends SNMP alarms (called alerts in this product) to SNMP management stations configured to receive them. The NetWare/IP server also incorporates all SNMP events into its error reporting system to be displayed on the Product Kernel screen and logged to the AUDIT.LOG file along with other system error reporting messages.

The conversion to error reporting levels is done automatically, even if SNMP Reporting Level is set to None. The error reporting system converts each SNMP alert level as follows:

SNMP Reporting Level	Error Reporting System Level
Critical	Error
Major	Error
Minor	Warning
Informational	Informational

Use the following procedure to configure the SNMP alarm level:

1. **From UNICON's Main Menu, choose the following:**

   –>Configure Error Reporting
   –>Configure Error Logging/SNMP Alert Levels

2. **From the Configure Error Logging/SNMP Alert Levels form, choose the SNMP Alert Level field.**

3. **Choose the level that you want reported or None to turn off SNMP reporting.**

4. **Press** <Esc> **to exit the Configure Error Logging/SNMP Alert Levels form.**

5. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Monitoring DSS Server Statistics Using SNMP

For the SNMP management station to display statistics for a node, the node must have a Management Information Base (MIB) set up. A MIB defines and stores the information to be managed for the node. Currently, the DSS server is the only NetWare/IP module with a MIB. Therefore, the DSS server is the only module for which you can monitor performance statistics from an SNMP management station.

Before you can view DSS server statistics from an SNMP management station, you must copy DSS.MIB to the management station. This file is included on the NetWare/IP product diskettes. You must also build a viewer for your network management software. Refer to the documentation that came with your network management product for information on building a viewer.

When the MIB is set up and the DSS server is registered with SNMP, the DSS server can report the following information about itself to the designated SNMP management stations:

- **DSS type** —whether the DSS server is registered or unregistered

- **NetWare/IP domain** —the domain for which this DSS server maintains SAP/RIP information

- **Database version** —the database version number for this DSS server

- **IPX network number** —the virtual IPX network number used by all NetWare/IP nodes in this NetWare/IP internetwork

- **Primary DSS–Secondary DSS Synchronization Interval** —the time interval at which primary and secondary DSS servers synchronize their databases

- **DSS–NetWare/IP Synchronization Interval** —the time interval at which NetWare/IP servers update the DSS servers with current SAP information

- **UDP port number** —the port number used to exchange UDP SAP/RIP queries

- **Maximum UDP retransmissions** —the number of times a NetWare/IP host will retransmit a UDP packet without receiving an acknowledgment

- **UDP checksum** —whether UDP datagrams use error detection and correction fields

- **SAP record count** —the number of SAP records currently stored in this DSS database

- **RIP record count** —the number of RIP records currently stored in this DSS database

- **Primary DSS** —the IP address of the primary DSS server for this NetWare/IP internetwork (secondary DSS servers only)

Using NetWare/IP with ManageWise Autodiscovery

The ManageWise™ autodiscovery feature locates network segments and devices on your internetwork and places representations of these segments and devices on a logical topology map called an Internet Logical Map (ILM). An ILM provides a high-level view of how your internetwork is interconnected and is therefore a valuable network management and troubleshooting tool.

NetWare/IP 2.1 or later nodes are compatible with ManageWise autodiscovery and therefore can be represented on an ILM. However, NetWare/IP 1.1 nodes are not compatible with ManageWise autodiscovery. This means that for a NetWare/IP network to be discovered by ManageWise, all NetWare/IP 1.1 nodes must be upgraded.

Troubleshooting DSS Servers

DSS servers provide NetWare/IP servers and clients with information about available services and routes on the network. DSS maintains this information in a database that stores SAP and RIP records. Because the performance of the network depends on the performance and integrity of the DSS servers, NetWare/IP provides the following tools to help you troubleshoot DSS servers:

- DSS browser
- DSS server listing

The following sections describe when and how to use these troubleshooting tools.

DSS Server Troubleshooting Screens

Troubleshoot DSS servers using the following screens:

- SAP Display screen
- SAP Record Detailed Information screen
- RIP Display screen
- RIP Record Detailed Information screen
- Domain SAP/RIP Servers list

From UNICON's Main Menu, choose the following to access the Browse DSS Database menu:

–>**Manage Services**
–>**NetWare/IP**
–>**Browse DSS Database**

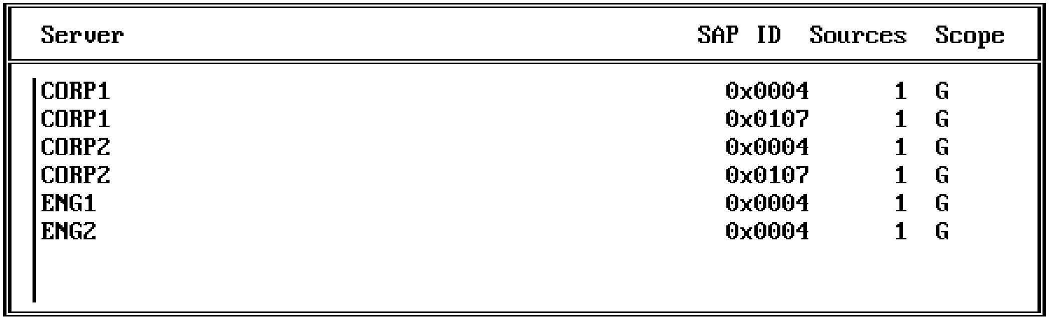
DSS database records are accessed from the Browse DSS Database menu.

If you need information about a specific field when accessing an online form using UNICON, press <F1> .

SAP Display Screen

Use the SAP Display screen to view SAP records stored in the DSS database on the current server.

Figure 10-6
SAP Display Screen



```
Server                                              SAP ID  Sources  Scope

CORP1                                                 0x0004      1   G
CORP1                                                 0x0107      1   G
CORP2                                                 0x0004      1   G
CORP2                                                 0x0107      1   G
ENG1                                                  0x0004      1   G
ENG2                                                  0x0004      1   G
```

When you view SAP records, you can

- Display records of a specific SAP type
- Display records for a specific server
- Display all SAP records stored in the DSS database on this server

From UNICON's Browse DSS Database menu, choose the following to access the SAP Display screen:

–>**Look At SAP Records**
  –>**Display Records for a Given SAP Type**

or

–>**Look At SAP Records**
  –>**Display Records for a Given Server**

The SAP Display screen displays all SAP records in the DSS database that match the display criterion you choose. For each SAP record, this screen displays the following information:

Server —the name of the server that reported the SAP.

SAP ID —a code specifying the type of SAP. For example, a SAP advertising a file server is a type 0x0004 SAP.

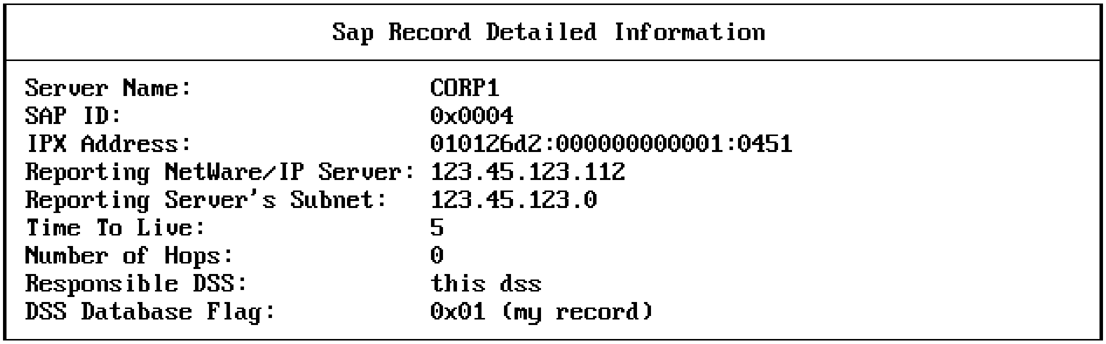
Sources —the number of NetWare/IP servers that reported this service to DSS. If the value in this field is greater than one, the service was reported by a forwarding gateway.

Scope —indicates whether this SAP information is propagated to every DSS server. G indicates a global or replicated SAP, and a blank indicates a local or non-replicated SAP.

SAP Record Detailed Information Screen

Use the SAP Record Detailed Information screen to view detailed information about a specific SAP.

Figure 10-7
SAP Record Detailed Information Screen



```
                        Sap Record Detailed Information

Server Name:                 CORP1
SAP ID:                      0x0004
IPX Address:                 010126d2:000000000001:0451
Reporting NetWare/IP Server: 123.45.123.112
Reporting Server's Subnet:   123.45.123.0
Time To Live:                5
Number of Hops:              0
Responsible DSS:             this dss
DSS Database Flag:           0x01 (my record)
```

From UNICON's Browse DSS Database menu, choose the following to access the SAP Record Detailed Information screen:

–>**Look At SAP Records**
–>**Display Records for a Given SAP Type**

or

–>**Look At SAP Records**
–>**Display Records for a Given Server**

After you specify SAP display criteria, UNICON produces the SAP Display screen. From the SAP Display screen, choose the SAP for which you want to view detailed information. If the value in the Sources field is one, the utility displays the SAP Record Detailed Information screen. If the value in the Sources field is greater than one, the utility displays a list of the IP addresses of all servers reporting the service. You can then choose an IP address from the list to display the SAP Record Detailed Information screen.

The SAP Record Detailed Information screen contains the following fields:

Server Name —the name of the server providing the service.

SAP ID —a code specifying the type of service. For example, a SAP advertising a file server is a type 0x0004 SAP.

IPX Address —a three-part address specifying the IPX address, node number, and socket number of the server providing the service.

Reporting NetWare/IP Server —the IP address of the server that reported the SAP to DSS.

Reporting Server's Subnet —the subnetwork address of the server that reported the SAP to DSS.

Time To Live —the number of database synchronizations after which this SAP will be marked for deletion unless its status is updated.

Number of Hops —the number of hops between the server providing the service and the server advertising the service to DSS. If the server providing the service is a NetWare/IP server, the value in this field is zero. If the server providing the service is a native NetWare (IPX) server, the value in this field is non-zero, which indicates that the SAP was reported to DSS by a NetWare/IP gateway.

Responsible DSS —the DSS server that received the SAP. If the SAP was received by the current DSS server, this value in this field is this dss. If the SAP was received by another DSS server, this field specifies the IP address of the DSS server that received the SAP.

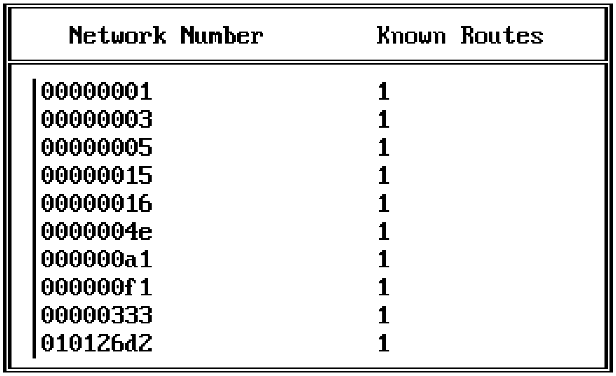
DSS Database Flag —a code specifying any specific information about the record, such as whether it is a SAP or RIP, the responsible DSS server, or whether the record has been marked for deletion.

RIP Display Screen

Use the RIP Display screen to view RIP records stored in the DSS database on the current server.

Figure 10-8

RIP Display Screen



```
   Network Number        Known Routes

00000001                    1
00000003                    1
00000005                    1
00000015                    1
00000016                    1
0000004e                    1
000000a1                    1
000000f1                    1
00000333                    1
010126d2                    1
```

When you view RIP records, you can display

- Records for a specific IPX network
- All RIP records stored in the DSS database on this server

From UNICON's Browse DSS Database menu, choose the following to access the RIP Display screen:

–>**Look At RIP Records**
  –>**Display Records for a Given IPX Network**

or

–>**Look At RIP Records**
  –>**Display All Records**

For each RIP record, the RIP Display screen displays the following information:

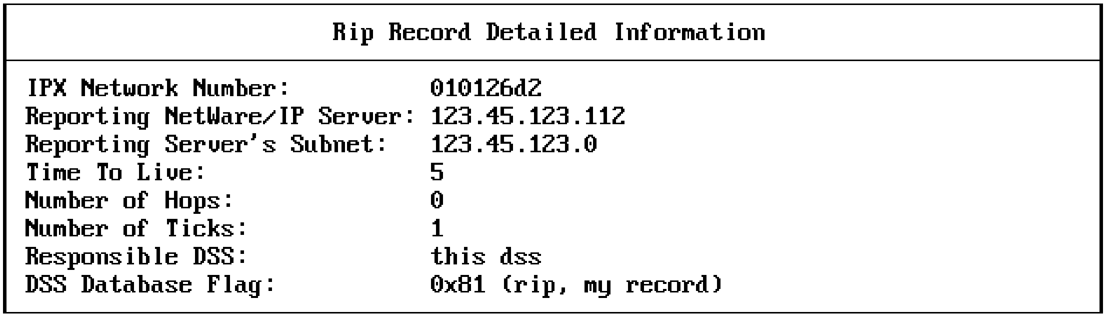
Network Number —the IPX network number of the server that reported the RIP.

Known Routes —the number of NetWare/IP servers that reported the route to DSS. If the value in this field is greater than one, the route was reported by a forwarding gateway.

RIP Record Detailed Information Screen

Use the RIP Record Detailed Information screen to view detailed information about a specific RIP record.

Figure 10-9
RIP Record Detailed Information Screen



```
                     Rip Record Detailed Information

IPX Network Number:          010126d2
Reporting NetWare/IP Server: 123.45.123.112
Reporting Server's Subnet:   123.45.123.0
Time To Live:                5
Number of Hops:              0
Number of Ticks:             1
Responsible DSS:             this dss
DSS Database Flag:           0x81 (rip, my record)
```

From UNICON's Browse DSS Database menu, choose the following to access the 'RIP Record Detailed Information screen:

–>**Look At RIP Records**
–>**Display Records for a Given IPX Network**

or

–>**Look At RIP Records**
–>**Display All Records**

After you specify RIP display criteria, UNICON produces the RIP Display screen. From the RIP Display screen, choose the RIP record for which you want to view detailed information. If the value in the Known Routes field is one, the utility displays the RIP Record Detailed Information screen. If the value in the Known Routes field is greater than one, the utility displays a list of the IP addresses of all servers reporting the route. You can then choose an IP address from the list to display the RIP Record Detailed Information screen.

The RIP Record Detailed Information screen contains the following fields:

IPX Network Number —the IPX network number of the remote network.

Reporting NetWare/IP Server —the IP address of the server that reported the RIP to DSS.

Reporting Server's Subnet —the subnetwork address of the server that reported the RIP to DSS.

Time To Live —the number of database synchronizations after which this RIP will be marked for deletion unless its status is updated.

Number of Hops —the number of hops between a server on the remote network and the server that reported the route to DSS. If the value in this field is zero, the remote network is a TCP/IP network. If the value in this field is non-zero, the remote network is an IPX network.

Number of Ticks —the amount of time in ticks (1/18 of a second) between any server on the remote network and the server that reported the route to DSS.

Responsible DSS —the DSS server that received the RIP. If the RIP was received by the current DSS server, this value in this field is this dss. If the RIP was received by another DSS server, this field specifies the IP address of the DSS server that received the RIP.

DSS Database Flag —a code specifying any specific information about the record, such as whether it is a SAP or RIP, the responsible DSS server, or whether the record has been marked for deletion.

Domain SAP/RIP Servers List

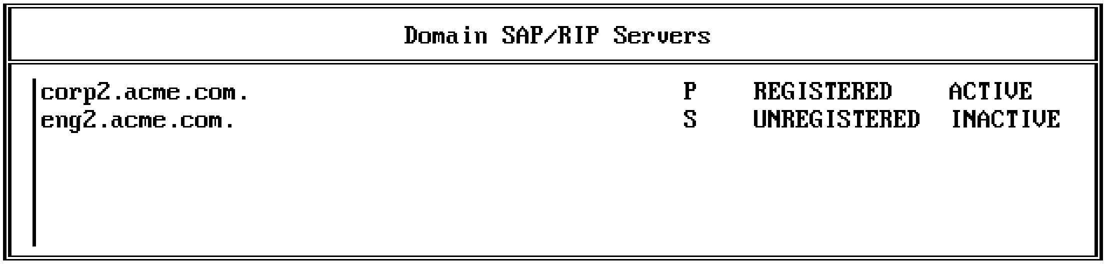
Use the Domain SAP/RIP Servers list to display a list of all DSS servers in a specified NetWare/IP domain.

From UNICON's Main Menu, choose the following to display the Domain SAP/RIP Servers list:

–>**Manage Services**
  –>**NetWare/IP**
    –>**Display All DSSes**

The utility prompts you for a NetWare/IP domain. Enter the name of the NetWare/IP domain for which you want to view DSS servers. The utility displays the Domain SAP/RIP Servers list.

Figure 10-10
Domain SAP/RIP Servers List



```
                         Domain SAP/RIP Servers

corp2.acme.com.                               P    REGISTERED    ACTIVE
eng2.acme.com.                                S    UNREGISTERED  INACTIVE
```

This screen lists all DSS servers in the specified domain. For each DSS server entry, the screen also indicates whether the DSS server is primary or secondary (P or S), registered or unregistered, and active or inactive. A registered DSS server has a resource record in the DNS database specifying it as a name server for the NetWare/IP domain. An unregistered DSS server does not have a name server record in the DNS database.

Note

The information about whether a DSS server is active or inactive is obtained from the primary DSS server. Therefore, if the link between this DSS server and the primary DSS server is down, the information reported may be inaccurate. Also, if the primary DSS server is down, no unregistered DSS servers will be reported.

Displaying SAP Records

When you choose Look At SAP Records from the Browse DSS Database menu, UNICON presents several display options. You can display all SAP records stored in the DSS database on this server or you can display SAP records

- Of a specific type
- For a specific server or selection of servers

The following sections provide procedures for viewing SAP records.

Displaying SAP Records of a Specific Type

1. **From UNICON's Main Menu, choose the following:**

–>**Manage Services**
  –>**NetWare/IP**
    –>**Browse DSS Database**
      –>**Look At SAP Records**
        –>**Display Records for a Given SAP Type**

2. **From the list of SAP types, choose the SAP type for which you want to display records.**

3. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Displaying SAP Records for a Specific Server

1. **From UNICON's Main Menu, choose the following:**

–>**Manage Services**
  –>**NetWare/IP**
    –>**Browse DSS Database**
      –>**Look At SAP Records**
        –>**Display Records for a Given Server**

2. **In the Server Name box, enter the name, IP address, or wildcard name or IP address of the server(s) for which you want to view SAP records and press** <Enter> **.**

3. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Displaying All SAP Records

1. **From UNICON's Main Menu, choose the following:**

–>**Manage Services**
  –>**NetWare/IP**
    –>**Browse DSS Database**
      –>**Look At SAP Records**
        –>**Display All Records**

2. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Displaying RIP Records

When you choose Look At RIP Records from the Browse DSS Database menu, UNICON presents two display options. You can display

- RIP records for a specific IPX network
- All RIP records stored in the DSS database on this server

The following sections provide procedures for viewing RIP records.

Displaying RIP Records for a Specific IPX Network

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
       –>**NetWare/IP**
           –>**Browse DSS Database**
               –>**Look At RIP Records**
                   –>**Display Records for a Given IPX Network**

2. **In the IPX Network Number (in hex) box, enter the IPX network number of the network for which you want to view RIP records and press** <Enter> **.**

3. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Displaying All RIP Records

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
       –>**NetWare/IP**
           –>**Browse DSS Database**
               –>**Look At RIP Records**
                   –>**Display All Records**

2. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Displaying All DSS Servers

With UNICON, you can display a list of all DSS servers in a specific NetWare/IP domain.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**NetWare/IP**
   –>**Display All DSSes**

2. **In the NetWare/IP Domain box, enter the name of the NetWare/IP domain for which you want to view DSS servers and press** <Enter> **.**

3. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Saving SAP Records to a Text File

With UNICON, you can back up all SAP records in the DSS database on the current server.

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**NetWare/IP**
   –>**Browse DSS Database**
   –>**Save SAP Database To Text File**

2. **When prompted, enter the path and name of the file where you want to save the SAP records.**

3. **Press** <Enter> **to clear the status message.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Saving RIP Records to a Text File

With UNICON, you can back up all RIP records in the DSS database on the current server.

1. **From UNICON's Main Menu, choose the following:**

–>**Manage Services**

–>**NetWare/IP**

–>**Browse DSS Database**

–>**Save RIP Database To Text File**

2. **When prompted, enter the path and name of the file where you want to save the RIP records.**

3. **Press** <Enter> **to clear the status message.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

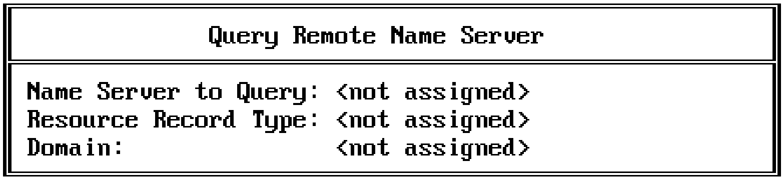
Troubleshooting Remote Name Servers

If you have problems with your network, you might want to check whether or not the remote name servers are responding to queries. You can test a remote name server by using the Query Remote Name Server option described in this section.

Query Remote Name Server Form

Use the Query Remote Name Server form to enter information about the remote name server that you want to query.

Figure 10-11
Query Remote Name Server Form



```
                Query Remote Name Server

Name Server to Query: <not assigned>
Resource Record Type: <not assigned>
Domain:               <not assigned>
```

From UNICON's Main Menu, choose the following to access the Query Remote Name Server form:

–>**Manage Services**

–>**DNS**

–>**Administer DNS**

–>**Query Remote Name Server**

The Query Remote Name Server form contains the following fields:

Name Server to Query —the hostname or IP address of the remote name server you want to query.

Resource Record Type —the type of record you want queried. Pressing <Enter> displays a list of the following record types from which you can choose.

- A—name-to-address mapping
- CNAME—alias for the canonical or authoritative name
- NS—name server in the domain
- PTR—address-to-name mapping
- SOA—server that is the best source of information for the data within the domain

Domain —the name of the domain for which you want information.

Querying a Remote Name Server

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Services**
   –>**DNS**
   –>**Administer DNS**
   –>**Query Remote Nameserver**

2. **On the Query Remote Name Server form, fill in the Name Server to Query field with either the hostname or the IP address of the name server and press** <Enter> **.**

   If the name server responds, the utility highlights the next field. Otherwise, the utility displays a message informing you that the name server is not responding.

3. **If the name server is responding, choose a resource record type by pressing** <Enter> **.**

4. **From the list of record types, choose a record type.**

5. **Enter the name of the domain you want to query.**

The utility displays a response to the query or displays a message stating that no records were found.

If the name server is a master and returns no records, the records do not exist in the database. If the name server is a replica and returns no records, this means that either the records do not exist on the master or that the replica is not able to import a complete copy of the database.

6. **Press** <Enter> **to clear the status message.**

7. **To return to UNICON’s Main Menu, press** <Esc> **as needed.**

Troubleshooting the NetWare/IP Server

You can use the NetWare MONITOR utility to display statistics about the performance of NetWare/IP servers.

NetWare/IP Server Statistics Screen

The NetWare/IP Server Statistics screen displays information about the performance of a NetWare/IP server.

To access the NetWare/IP Server Statistics screen, enter the following command at the server console:

load monitor <Enter>

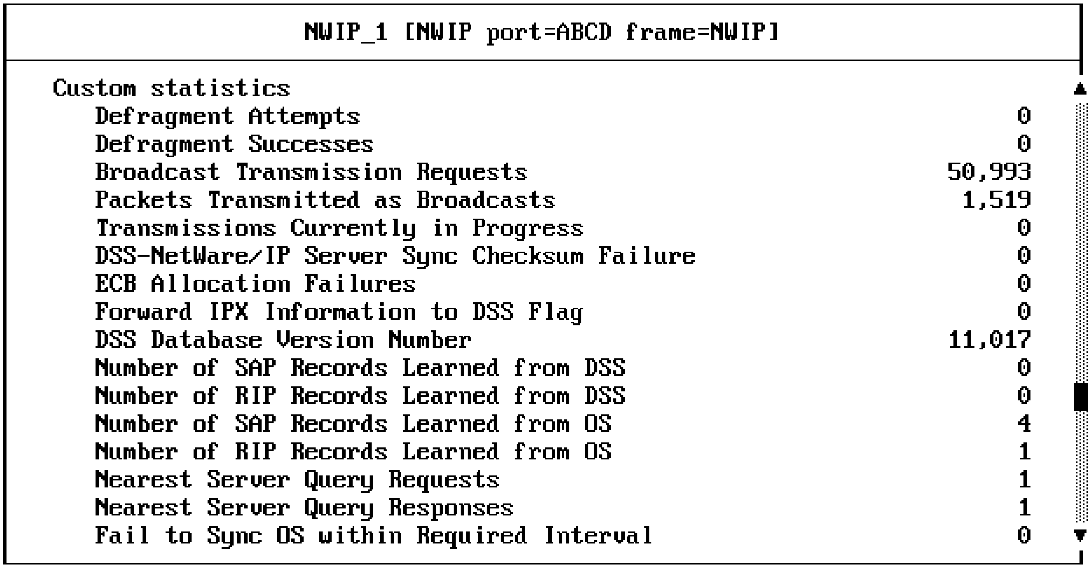
From MONITOR’s Available Options menu, choose the following:

–>**LAN/WAN Information**
  –>**[NWIP port=x frame=NWIP]**

The utility displays statistics about the NetWare/IP server. Press the Down-arrow key until you reach the Custom Statistics section:

Figure 10-12

MONITOR's Custom Statistics for NetWare/IP



```
                    NWIP_1 [NWIP port=ABCD frame=NWIP]

   Custom statistics
      Defragment Attempts                                              0
      Defragment Successes                                             0
      Broadcast Transmission Requests                             50,993
      Packets Transmitted as Broadcasts                            1,519
      Transmissions Currently in Progress                              0
      DSS-NetWare/IP Server Sync Checksum Failure                      0
      ECB Allocation Failures                                          0
      Forward IPX Information to DSS Flag                              0
      DSS Database Version Number                                 11,017
      Number of SAP Records Learned from DSS                           0
      Number of RIP Records Learned from DSS                           0
      Number of SAP Records Learned from OS                            4
      Number of RIP Records Learned from OS                            1
      Nearest Server Query Requests                                    1
      Nearest Server Query Responses                                   1
      Fail to Sync OS within Required Interval                         0
```

NetWare IP server statistics: explainedThis screen includes the following fields, which provide information about the performance of the NetWare/IP server you are currently logged in to:

Defragment Attempts —the number of attempts the server has made to defragment incoming UDP packets to their original state.

Defragment Successes —the number of times the server has successfully defragmented incoming UDP packets to their original state. If the number of defragment attempts is greater than the number of defragment successes, your packet receive buffer may not be large enough to receive the defragmented packets. You can modify the packet receive buffer using the NetWare SET utility. For information on using this utility, refer to the *Utilities Reference* , which is part of the NetWare 4 documentation set.

Broadcast Transmission Requests —the number of packets the server has received from the operating system that are destined for a broadcast address.

Packets Transmitted as Broadcasts —the number of packets this server has sent out as broadcasts. Because NetWare/IP does not support IPX broadcasting, the number of packets transmitted as broadcasts should be significantly fewer than the number of broadcast transmission requests. If this field indicates that the server is transmitting a large number of broadcasts, you may have an IPX broadcast application running on your network.

Transmissions Currently In Progress —the number of packets the server is currently transmitting. While the value in this field varies depending on server activity, this field should periodically return to zero. If the value in this field does not return to zero, your server may have a problem transmitting packets.

DSS–NetWare/IP Server Sync Checksum Failures —the number of times the checksum byte at the end of the NetWare/IP server–DSS zone transfer packet does not match the sum of the records contained in the transfer. If there is a large value in this field, the DSS server may be overloaded. Make sure that the number of forwarding IP–IPX gateways does not exceed two per network segment.

ECB Allocation Failures —a counter that increments when a device sends a packet to your NetWare/IP server but no packet receive buffer is available. The NetWare/IP server allocates more packet receive buffers after each incident until it reaches its maximum limit. You can manually increase the minimum and maximum number of packet receive buffers using the NetWare SET utility. For information on using this utility, refer to *Utilities Reference* .

Forward IPX Information to DSS Flag —a flag that indicates whether this NetWare/IP server is configured as a forwarding gateway. If the value in this field is 0, the server is not configured as a forwarding gateway. If the value in this field is 1, the server is configured as a forwarding gateway.

DSS Data Base Version Number —the version of the DSS database this DSS server is using. After a DSS–NetWare/IP server synchronization, this version number should match the version number of the primary DSS server. You can display the DSS version number by loading the DSS using the /stat switch. For example, at the server console prompt, type **load dss /stat** .

Number of SAP Records Learned from DSS —the number of SAP records stored in the server cache that the server learned from DSS.

Number of RIP Records Learned from DSS —the number of RIP records stored in the server cache that the server learned from DSS.

Number of SAP Records Learned from OS —the number of SAP records reported directly to this server from the operating system. If the server is configured as a forwarding gateway, the total of the number of SAP records learned from DSS plus the number of SAP records learned from OS should equal the total received when you execute the display servers command.

Number of RIP Records Learned from OS —the number of RIP records reported directly to this server from the operating system. If the server is configured as a forwarding gateway, the total of the number of RIP records learned from DSS plus the number of RIP records learned from OS should equal the total received when you execute the display networks command.

Nearest Server Query Requests —the number of nearest server query (NSQ) requests received by this server from NetWare/IP clients.

Nearest Server Query Responses —the number of nearest server query (NSQ) responses sent by this server. Because NSQs are sent point-to-point, the number of NSQ requests should be less than or equal to the number of NSQ responses.

Fail to Sync OS within Required Interval —the number of times the NetWare/IP server has failed to forward SAP/RIP information it learned from DSS to the operating system. If this counter continues to rise, you should increase the minimum and maximum number of packet receive buffers using the NetWare SET utility. For information on using this utility, refer to *Utilities Reference* . In addition to increasing the number of packet receive buffers, you should also check to see if there is an NLM™ hogging the CPU.

Maintenance Packets Dropped on On-Demand Link —the number of NetWare maintenance packets purposely dropped on a TCP/IP interface that is configured to use an on-demand link.

Maintenance Packets Spoofed on On-Demand Link —the number of NetWare maintenance packets purposely spoofed on a TCP/IP interface that is configured to use an on-demand link.

Viewing NetWare/IP Statistics

Use the following procedure to load MONITOR and display the NetWare/IP server statistics:

1. **At the server console, enter the following command:**

   load monitor <Enter>

2. **From the Available Options menu, choose the following:**

   –>LAN/WAN Information

3. **From the Available LAN Drivers list, choose the NetWare/IP option.**

4. **Press the Down-arrow key until you reach the Custom Statistics section.**

5. **Press** <Esc> **as needed to exit the utility.**

6. **When prompted, choose Yes to return to the server console.**

Troubleshooting NetWare/IP Clients

The following sections provide information to help you troubleshoot the NetWare/IP client software.

Running NetWare/IP in Verbose Mode

If you have problems running the NetWare/IP client software on a workstation, you can use the verbose switch (/v) to display information about the status of the network.

To run NetWare/IP using the verbose switch, type the following command at the DOS prompt:

nwip /v <Enter>

The workstation will display diagnostic information. The information displayed depends on whether NetWare/IP has already been loaded into memory.

Starting NetWare/IP Using the Verbose Switch

If NetWare/IP has not yet been loaded into memory, you can use the verbose switch to display information about the NetWare/IP initialization process. As NetWare/IP starts, it displays the following diagnostic information:

- The IP addresses of the DSS and DNS servers this client is attempting to query.

- The IP address of the DSS server from which this client is attempting to obtain global configuration information.

- Error messages specifying any DSS or DNS servers the client is unable to contact.

- Client configuration information, such as the workstation's IP address and the UDP port numbers used for NetWare/IP.

For example, during initialization a workstation might display the following:

```
Retrying contacting unregistered DSSes
Send DNS query to address:1.2.3.4
Trying to get parameters from DSS:1.2.3.5
Successfully received parameters from DSS:1.2.3.5
Configuration: Node address:1.2.3.6
UDP Port: 43981 43982
Checksum: No
```

Using the Verbose Switch While NetWare/IP Is Running

You can also use the verbose switch after NetWare/IP is loaded into memory to display the following diagnostic information:

- The version of NetWare/IP software this client is using.

- The IP addresses of the DSS servers this client knows about. These lines also indicate the number of times the client has attempted to contact each DSS server with no response.

- The IP addresses of the NetWare/IP servers this client is using to obtain network service information. These lines also indicate the number of times the client has attempted to contact each NetWare/IP server with no response.

For example, if NetWare/IP is already loaded into memory, a workstation might display the following:

```
It is a post NWIP v1.1 client TSR
*DSS address: 1.2.3.4 NO_ANS Count: 0
DSS address: 1.2.3.5 NO_ANS Count: 0
DSS address: 1.2.3.9 NO_ANS Count: 0
NWIP Server address: 1.2.3.6 NO_ANS Count: 3
*NWIP Server address: 1.2.3.7 NO_ANS Count: 0
NWIP Server address: 1.2.3.8 NO_ANS Count: 0
```

Note

The * indicates which DSS or NetWare/IP server the client is currently using.

Configuring Other Frame Types

Frame types determine how packets of network data are formatted on different LANs. Ethernet, token ring, ARCnet*, and other LANs use different formats. The TCP/IP and IPX protocols also require different frame types in some instances.

The NetWare/IP installation program automatically configures the following frame types, depending on the network board in the workstation:

- Ethernet board: ETHERNET_II or ETHERNET_SNAP
- Token ring board: TOKEN-RING_SNAP
- ARCnet board: NOVELL_RX-NET
- PCN or PCN II board: IBM_PCN2_SNAP
- FDDI board: FDDI_SNAP

However, network board drivers from other manufacturers may support additional frame types. If your network uses a different frame type, the client software might configure the wrong frame type. In this case, when the NetWare/IP client software is run, the workstation displays the following error message:

```
Error registering protocol IDs
```

If this happens, you must specify a different frame type by modifying the NET.CFG file in the NetWare/IP client directory (C:\NWCLIENT by default).

To enable support for a different frame type, change the FRAME line in the NET.CFG file under the Link Driver heading for the network board driver (*drivername*) and add a PROTOCOL statement including the protocol name, hexadecimal ID number, and frame type.

Consult the documentation accompanying the network board driver for information about changes to the NET.CFG file required for different frame types.

Connecting to Servers in Other NetWare/IP Domains

When you log in to a NetWare/IP server or network, you can access the NetWare/IP servers in your NetWare/IP domain. NetWare/IP also allows you to map drives to servers in other NetWare/IP domains, called *remote domains* . For example, you might want to connect to a NetWare/IP server at another company over the Internet.

To let you connect to remote domains that are accessible from your network, NetWare/IP provides the NWIPMAP utility. You need the following information to use the NWIPMAP utility:

- The fully qualified name of the remote NetWare/IP domain
- The name of the NetWare/IP server in the remote domain
- The volume (and, optionally, a directory) on the remote server

A DSS server in the remote NetWare/IP domain must be accessible through DNS, and you must have permission to attach to the server.

Using the NWIPMAP Utility

The NWIPMAP utility works in a manner similar to the MAP command and has the same format, except that you include the name of the remote NetWare/IP domain:

NWIPMAP *drive* **:=***servername* *\vol* **:***path* **@***domain*

For *domain* , substitute the fully qualified domain name of the remote NetWare/IP domain. For example, the following command maps drive G: to a server named VENUS in NetWare/IP domain nwip.theircorp.com.:

NWIPMAP G:=VENUS\SYS:\PUBLIC@NWIP.THEIRCORP.COM.

After you have connected to a remote server, you can make the mapped drive the current drive and access services provided by that server. You can execute DOS and Windows commands. You can run any NetWare/IP utility that does not require SAP/RIP broadcasting. For example, you can use file services and remote management utilities such as NLIST, but you cannot use print services or the MAP utility. Print services and the MAP utility rely on SAP/RIP broadcasting.

NWIPMAP Limitations

NWIPMAP has the following limitations:

- The NetWare/IP requirement that IPX network numbers must be unique across internetwork connections applies to NWIPMAP connections as well. Furthermore, server names must be unique among all NetWare/IP domains to which you connect.

- All NetWare/IP domains to which you connect must use the same TCP/UDP port numbers.

- NWIPMAP provides file access only. Services in the remote NetWare/IP domain that rely on SAP/RIP broadcasting, such as print services, are not available.

Troubleshooting UNICON

To use UNICON on a server, you must log in. To log in, the server must be able to access the Directory tree containing a valid User object. If the Directory database resides on a server that can be reached only via the IP transport, you must be running TCP/IP to access the Directory on that server.

For example, suppose you are trying to use UNICON and need to log in to a server at your branch office over a TCP/IP link. Unless the NetWare/IP service is configured and running on the branch office server (providing a TCP/IP transport), you cannot log in via UNICON.

If you are unable to log in to a server using UNICON, you must configure and load the NetWare/IP server component using the NetWare/IP Server Configuration (NWIPCFG) utility. This is the same utility invoked by the NetWare/IP installation program. Once the NetWare/IP server is running, you can load UNICON and reconfigure the server as desired.

Note

A DSS server and a DNS name server must be running on the network before you can configure and launch a NetWare/IP server. For information on installing the initial DSS and DNS servers, see “Setting Up the Initial DNS and DSS Servers” on page 73

Use the following procedure to configure and launch a NetWare/IP server using NWIPCFG:

1. **At the server console, type the following command:**

load nwipcfg <Enter>

2. **From the NetWare/IP Server Administration menu, choose the following:**

   –>**Configure DNS Client**

3. **On the DNS Client Access form, fill in the DNS Domain field and at least one Name Server field and press** <Esc> **.**

4. **From the NetWare/IP Server Administration menu, choose the Configure NetWare/IP Server option.**

5. **On the NetWare/IP Server Configuration form, enter your fully qualified NetWare/IP domain name in the NetWare/IP Domain field.**

6. **Fill in other configuration fields as appropriate for your network.**

7. **Press** <Esc> **to exit the NetWare/IP Server Configuration form.**

8. **When prompted, choose Yes to save the NetWare/IP server configuration.**

9. **From the NetWare/IP Server Administration menu, choose the Start NetWare/IP Server option.**

10. **Press** <Esc> **to clear the status message.**

11. **To exit the NWIPCFG utility, press** <Esc> **.**

12. **When prompted, choose Yes to return to the server console.**

Common Error Messages and Solutions

Refer to Appendix G, “Error Messages,” on page 295 for a complete list of error messages and solutions.

Chapter

11 *Removing the NetWare/IP Software*

This chapter explains how to remove the NetWare/IP™ software from a NetWare® server and client workstations.

Removing the NetWare/IP software consists of the following tasks:

- Stopping NetWare/IP services
- Uninstalling the NetWare/IP product
- Deleting the remaining NetWare/IP files
- Removing the NetWare/IP client software

Stopping NetWare/IP Services

Before you can remove the NetWare/IP software, you must stop the services running on the server.

1. **At the server console prompt, stop all services by typing**

   UNISTOP <Enter>

Uninstalling the NetWare/IP Software

Use the INSTALL utility to uninstall the NetWare/IP software from the server.

1. **At the server console prompt, start the NetWare INSTALL utility by typing**

   LOAD INSTALL <Enter>

2. **From the Installation Options menu, choose the following:**

–>**Product options**
  –>**View/Configure/Remove installed products**

3. **Choose the NetWare/IP product entry, and press** <Delete> **.**

4. **When prompted, choose Yes to remove NetWare/IP.**

5. **Press** <Esc> **as needed to exit the installation utility.**

Deleting NetWare/IP Files

Removing the NetWare/IP software does not remove all the NetWare/IP NLMs and configuration files and directories. You must delete these files manually from the SYS: volume after you remove the NetWare/IP software.

Warning

Do not remove these files if another product running on the server is using them.

NLMs

The following NLMs remain after you remove the NetWare/IP software:

SYS:SYSTEM\DLLINFO.NLM
SYS:SYSTEM\NETDB.NLM
SYS:SYSTEM\NWIP.LAN
SYS:SYSTEM\NWIP.LDI
SYS:SYSTEM\NWIP.NLM
SYS:SYSTEM\NWIPCFG.NLM
SYS:SYSTEM\NWIPIO.LAN
SYS:SYSTEM\NWCCSS.NLM
SYS:SYSTEM\PKERNEL.NLM
SYS:SYSTEM\P_UNINST.NLM
SYS:SYSTEM\RPCBSTUB.NLM
SYS:SYSTEM\TELNETD.NLM
SYS:SYSTEM\TUI.NLM
SYS:SYSTEM\UNICRYPT.NLM
SYS:SYSTEM\UNIDLL.NLM
SYS:SYSTEM\XCONSOLE.NLM
SYS:SYSTEM\XCONSSRV.NLM

SYS:SYSTEM\NLS\4\NWIP.MSG
SYS:SYSTEM\NLS\4\NWIPCFG.HLP
SYS:SYSTEM\NLS\4\NWIPCFG.MSG
SYS:SYSTEM\NLS\4\NWIPIO.MSG
SYS:SYSTEM\NLS\4\PKERNEL.MSG
SYS:SYSTEM\NLS\4\TELNETD.MSG
SYS:SYSTEM\NLS\4\XCONSOLE.MSG
SYS:SYSTEM\NLS\4\XCONSSRV.MSG

Configuration Files and Directories

The following configuration files and directories remain after you remove the NetWare/IP software:

SYS:ETC\HOSTS
SYS:ETC\NWPARAMS
SYS:ETC\NAMED.CFG
SYS:ETC\RESOLV.CFG
SYS:ETC\AUDITSAV.LOG
SYS:ETC\AUDITSAV.CTL
SYS:ETC\AUDIT.LOG
SYS:ETC\AUDIT.CTL
SYS:ETC\SAMPLES\*.*
SYS:ETC\INSTALL\*.*
SYS:ETC\NET\*.*
SYS:ETC\NIS\*.*
SYS:ETC\DNS\*.*
SYS:ETC\TMP\*.*
SYS:ETC\DBSOURCE\*.*

Removing the NetWare/IP Client Software

Before you remove the NetWare/IP client software from a workstation, take note of the following warnings:

Warning

Before you delete any files, make sure you have a complete backup copy of the system. If you inadvertently delete files that are needed by another program, you can restore them from the backup.

If the workstation previously ran NetWare IPX™ software and you want to restore that software to operation, do not delete any files from the NetWare IPX client directory or Windows directory. If you deleted the file NWTOOLS.EXE from the Windows directory, restore a backup copy of this file if you want to restore the NetWare Tools™ to operation.

If the workstation runs LAN WorkPlace® or LAN WorkGroup™ , do not delete any files from the NET or Windows directories.

1. **Delete the NetWare/IP client directory, which is C:\NWCLIENT by default.**

2. **Delete the TCP/IP directory, which is C:\NET by default.**

3. **Delete the following files from the Windows directory:**

NOVELL.BMP	NWADMIN.INI
NOVLOGO1.BMP	NWRCON.PIF
NW.GRP	

4. **Delete the following files from the Windows SYSTEM directory:**

NETWARE.DRV	NWUSER.EXE
NETWARE.HLP	PNW.DLL
NWCALLS.DLL	RES_SUPP.DLL
NWGDI.DLL	TASKID.COM
NWIPWIN.EXE	TBMI2.COM
NWIPXSSPX.DLL	TLI_SPX.DLL
NWLOCALE.DLL	TLI_TCP.DLL
NWNET.DLL	TLI_WIN.DLL
NWPOPUP.EXE	VIPX.386
NWPSRV.DLL	VNETWARE.386

5. **Delete the following files from the Windows NLS directory:**

1252_UNI.001	UNI_COL.001
UNI_1252.001	UNI_MON.001

6. **Delete the following files from the Windows NLS\ENGLISH directory:**

NETWARE.HLP	TASKID.MSG
NETWARER.DRV	TBMI2.MSG

For shared Windows installations, the server administrator copies these files to the Windows directory on the server. They do not have to be deleted from a workstation.

7. **If such files exist, restore the backup (.BNW) copies of the following system files:**

AUTOEXEC.BAT	PROGMAN.INI
CONFIG.SYS	SYSTEM.INI
NET.CFG	WIN.INI
STARTNET.BAT	

Backup copies of NET.CFG and STARTNET.BAT exist only if the workstation previously used NetWare IPX client software.

If these system files have been modified in other ways since installing the NetWare/IP client, you can remove the NetWare/IP information from these files manually instead of restoring the backups. The sections that follow provide the information you need to edit these files.

Restoring System Files

If a workstation's system files have changed since the NetWare/IP client software was installed, you might prefer to delete the NetWare/IP changes rather than restoring backup copies. The sections below describe the changes you need to make to the system files when you remove the NetWare/IP client software.

AUTOEXEC.BAT

The NetWare/IP installation program adds the following line to the AUTOEXEC.BAT file:

@CALL C:\NWCLIENT\STARTNET

This line runs a batch file that loads the NetWare/IP client software.

CONFIG.SYS

The NetWare/IP installation program adds the following line to the CONFIG.SYS file:

LASTDRIVE=Z

This line enables the use of drive letters through Z for network drives.

NET.CFG

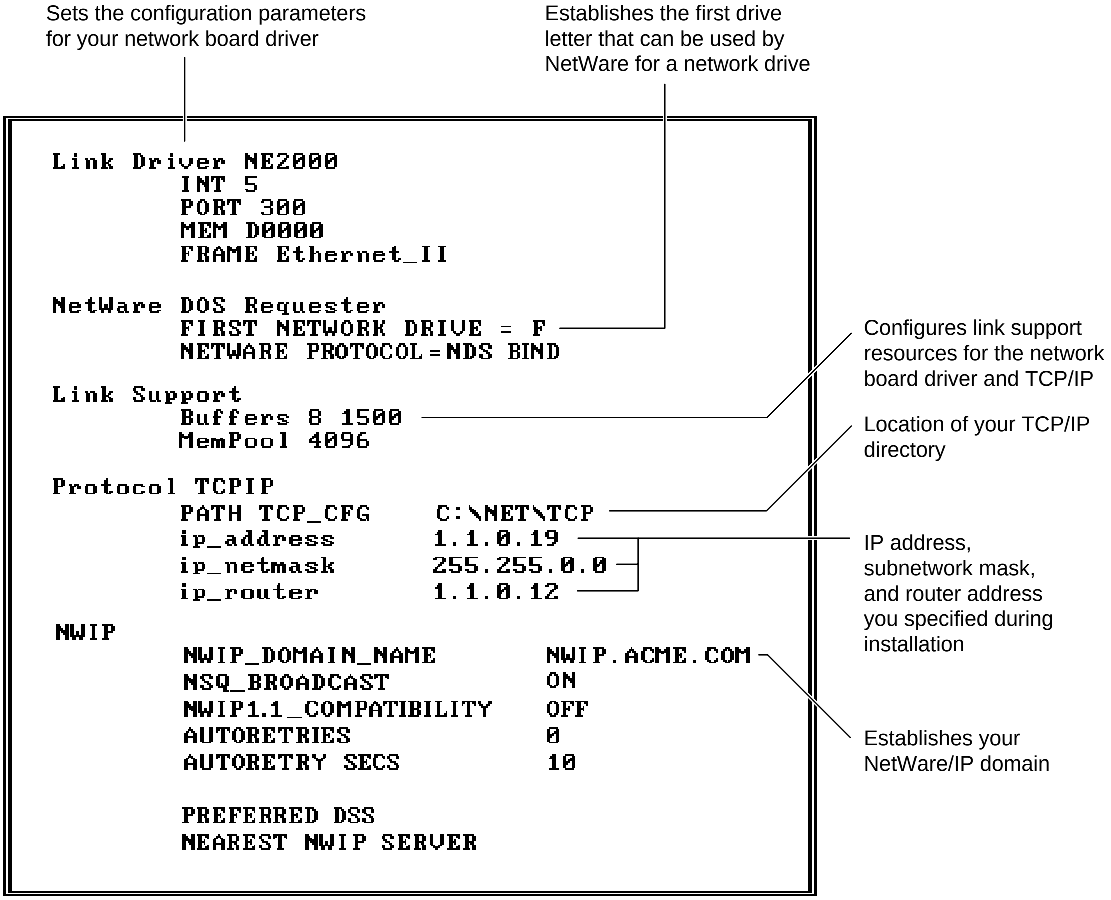
The NET.CFG file is created by the NetWare/IP installation utility unless the workstation previously used NetWare IPX client software.

The NetWare/IP client software requires that a TCP/IP protocol section and an NWIP section exist in the NET.CFG. Figure 11-1 illustrates the changes made to the NET.CFG file.

Other Novell software makes use of the NET.CFG file. If you have customized the NET.CFG file, additional entries might be present.

Figure 11-1

NET.CFG File After NetWare/IP Client Installation



Sets the configuration parameters for your network board driver

Establishes the first drive letter that can be used by NetWare for a network drive

```
Link Driver NE2000
        INT 5
        PORT 300
        MEM D0000
        FRAME Ethernet_II

NetWare DOS Requester
        FIRST NETWORK DRIVE = F
        NETWARE PROTOCOL=NDS BIND

Link Support
        Buffers 8 1500
        MemPool 4096

Protocol TCPIP
        PATH TCP_CFG    C:\NET\TCP
        ip_address      1.1.0.19
        ip_netmask      255.255.0.0
        ip_router       1.1.0.12
NWIP
        NWIP_DOMAIN_NAME        NWIP.ACME.COM
        NSQ_BROADCAST           ON
        NWIP1.1_COMPATIBILITY   OFF
        AUTORETRIES             0
        AUTORETRY SECS          10

        PREFERRED DSS
        NEAREST NWIP SERVER
```

Configures link support resources for the network board driver and TCP/IP

Location of your TCP/IP directory

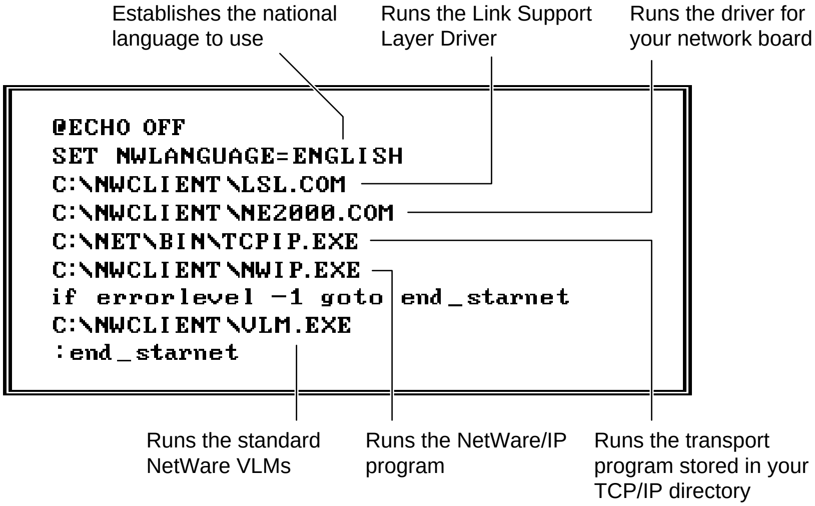
IP address, subnetwork mask, and router address you specified during installation

Establishes your NetWare/IP domain

STARTNET.BAT

Figure 11-2 illustrates changes made to the STARTNET.BAT file.

Figure 11-2
STARTNET.BAT File After NetWare/IP Client Installation



```
@ECHO OFF
SET NWLANGUAGE=ENGLISH
C:\NWCLIENT\LSL.COM
C:\NWCLIENT\NE2000.COM
C:\NET\BIN\TCPIP.EXE
C:\NWCLIENT\NWIP.EXE
if errorlevel -1 goto end_starnet
C:\NWCLIENT\VLM.EXE
:end_starnet
```

Establishes the national language to use

Runs the Link Support Layer Driver

Runs the driver for your network board

Runs the standard NetWare VLMs

Runs the NetWare/IP program

Runs the transport program stored in your TCP/IP directory

Restoring Windows Files

The NetWare/IP installation utility makes several changes to the Windows configuration files in a workstation’s Windows directory, saving the original files in backup copies with a .BNW extension. These files are also used and modified by other Windows applications and by Windows itself.

The sections that follow describe the specific changes made to support NetWare/IP.

WIN.INI

The NetWare/IP installation program adds the following line to the [windows] section of the WIN.INI file:

LOAD=NWPOPUP.EXE

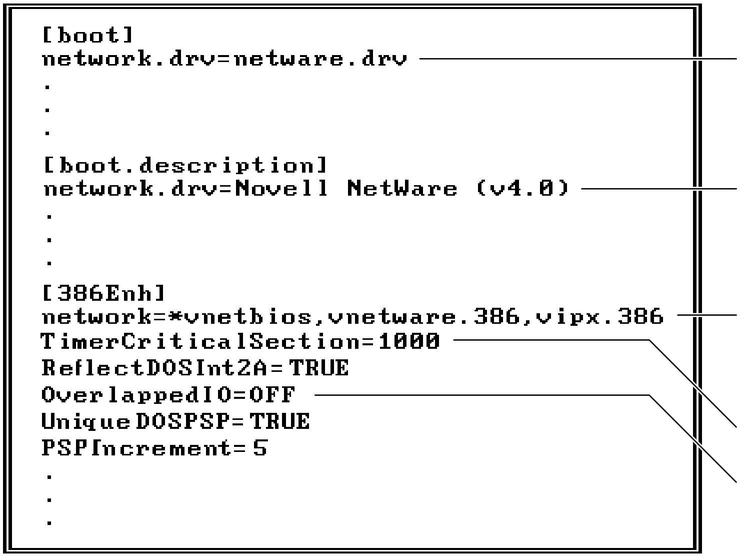
This line loads the program that handles NetWare status line messages in the Windows environment.

SYSTEM.INI

Figure 11-3 illustrates the changes made to the SYSTEM.INI file.

Figure 11-3

Modifications to the SYSTEM.INI File by NetWare/IP Client Installation



```
[boot]
network.drv=netware.drv
.
.
.
[boot.description]
network.drv=Novell NetWare (v4.0)
.
.
.
[386Enh]
network=*vnetbios,vnetware.386,vipx.386
TimerCriticalSection=1000
ReflectDOSInt2A=TRUE
OverlappedIO=OFF
UniqueDOSPSP=TRUE
PSPIncrement=5
.
.
.
```

Loads the general-purpose NetWare driver for MS Windows

Displays this information when MS Windows starts up

Loads drivers required for NetWare support

Adjusts a timer value to ensure smooth handling of network traffic

Ensures proper handling of network traffic

PROGMAN.INI

The NetWare/IP installation program adds the following line to the [Groups] section of the PROGMAN.INI file:

GROUP*x* =C:\WINDOWS\NW.GRP

This line enables the NetWare Tools program group to be displayed in Windows Program Manager. The *x* is replaced by the next available group number.

Chapter

12 *Configuring a DHCP Server*

The Dynamic Host Configuration Protocol (DHCP) enables TCP/IP-based client workstations to receive local and network configuration information automatically when the TCP/IP transport is loaded.

When a DHCP client workstation boots, it broadcasts a DHCP request for its IP address and network configuration. When the DHCP server receives the message, it checks its database to determine which configuration information to return. The DHCP server replies by sending a DHCP reply message that includes all TCP/IP configuration information required by the specific client that sent the request.

This chapter provides procedures for setting up the NetWare DHCP service. To configure the NetWare DHCP service, you must complete the following tasks:

1. Install the NetWare DHCP service, as described in “Installing the NetWare DHCP Service” on page 196

2. Define subnetwork profiles for each subnetwork using DHCP services. Or, if your network does not use subnetting, define a single subnetwork profile. See “Defining Subnetwork Profiles” on page 198 for more information.

3. List IP addresses that are to be assigned statically, as described in “Setting Up IP Address Assignments” on page 207

4. Define a list of nodes that you do not want the DHCP server to reply to, as described in “Defining Excluded Nodes” on page 209

5. Load the DHCP Server NetWare Loadable Module™ (NLM™), as described in “Loading DHCPSRVR” on page 197

The NetWare DHCP service is configured and managed by the DCHP Configuration utility (DHCPCFG). You use DHCPCFG to complete each of the tasks necessary to provide the NetWare DHCP service on a network.

Installing the NetWare DHCP Service

The NetWare DHCP service is installed using the NetWare Installation Utility (INSTALL).

1. **Start the INSTALL utility by typing the following command at the server console prompt:**

   load install <Enter>

2. **From INSTALL's Installation Options menu, choose the following:**

   –>**Product options**
   –>**Install a product not listed**

3. **When prompted, specify the location of the installation source files.**

   - To install from the *NetWare Installation* CD-ROM mounted as a NetWare volume on the server, mount the volume, press <F3> , and enter the following:

     NW411:DHCP

     For information on mounting the *NetWare Installation* CD-ROM as a NetWare volume, see the NetWare 4 *Installation* manual.

   - To install from a CD-ROM drive installed as a DOS drive on the server, insert the *NetWare Installation* CD-ROM into the server's CD-ROM drive, press <F3> , and enter the following:

     D:\DHCP

     If necessary, replace *D* with the appropriate drive letter.

   - To install from a CD-ROM image copied to a NetWare server, copy the contents of the NWIP directories on the *NetWare Installation* CD-ROM to the server's disk drive. When prompted to enter a path for installation source files, enter the complete path to the source files as follows:

     servername /*vol* :*directory path*

4. **Choose the Install Product option and press** <Enter> **.**

5. **From the list of servers, choose the server you want to install the NetWare DHCP service on and press** <Enter> **.**

6. **When prompted, choose Yes to start installing the NetWare DHCP service.**

7. **When the installation utility reports that the installation was successful, press** <Enter> **to clear the status message.**

8. **Press** <Esc> **and choose Yes as needed to exit the installation utility.**

Backward Compatibility with BOOTP

The NetWare DHCP service is backward compatible with Boot Protocol (BOOTP) clients. A DHCP server responds to a BOOTP request as if it is a DHCP request.

All assigned IP addresses for BOOTP clients are treated as Permanent Lease assignments in DHCP, and the addresses are not re-used.

The NetWare DHCP service stores DHCP information in the DHCPTAB file in the SYS:ETC directory. When you install DHCP, the installation program copies the contents of the SYS:ETC/BOOTPTAB file to the SYS:ETC/DHCPTAB file. The DHCPSRVR and DHCPCFG NLMs use only the DHCPTAB file. Any changes to the BOOTPTAB file after installing DHCP are not reflected in the DHCPTAB file.

Loading DHCPSRVR

After you complete each of the tasks necessary to configure the NetWare DHCP service on a network, you need to load the DHCP Server NLM (DHCPSRVR.NLM). To load the DHCP Server NLM, enter the following command at the server console prompt:

load dhcpsrvr [-t *x*] [-a *y*] [-h] <Enter>

where

-t *x* specifies the time interval between checks to see if the DHCPTAB file has changed. The default is 60 seconds.

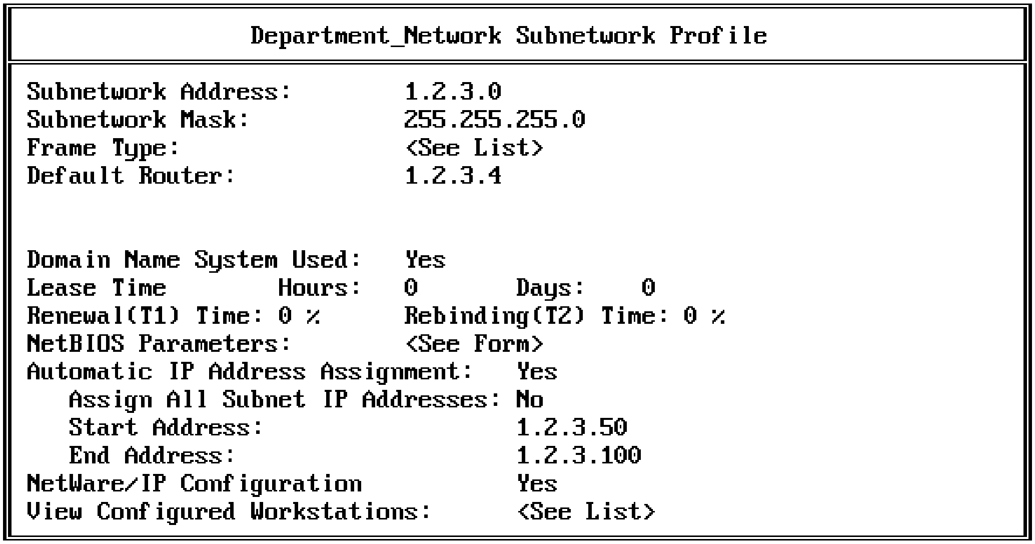
-a *y* specifies the time interval between checks to see if the lease time for an address has expired or not. The default is 10 minutes.

-h displays a help message.

Defining Subnetwork Profiles

A subnetwork profile contains configuration information for a specific network segment. A subnetwork profile is defined using DHCPCFG's Subnetwork Profile form.

Figure 12-1
DHCPCFG's Subnetwork Profile Form



```
                 Department_Network Subnetwork Profile

Subnetwork Address:         1.2.3.0
Subnetwork Mask:            255.255.255.0
Frame Type:                 <See List>
Default Router:             1.2.3.4


Domain Name System Used:    Yes
Lease Time       Hours:     0       Days:    0
Renewal(T1) Time: 0 %       Rebinding(T2) Time: 0 %
NetBIOS Parameters:         <See Form>
Automatic IP Address Assignment:    Yes
   Assign All Subnet IP Addresses: No
   Start Address:                   1.2.3.50
   End Address:                     1.2.3.100
NetWare/IP Configuration            Yes
View Configured Workstations:       <See List>
```

The information required on the subnetwork segment can be divided into the following categories:

- **TCP/IP configuration information** —this identifies general TCP/IP parameter values for the subnetwork, such as the subnetwork mask and subnetwork address.

- **Name service information** —this identifies Domain Name System (DNS) parameter values for the subnetwork.

- **IP address assignment information** —this indicates whether static or automatic IP address assignment is used on the subnetwork. This information also identifies the range of IP addresses to use if automatic assignment is selected.

- **NetWare/IP information** —this defines parameter values to be sent to NetWare/IP clients. This information is required only if there are NetWare/IP clients on the network that use the NetWare DHCP service.

Every network segment that includes DHCP clients must have a subnetwork profile. When a client broadcasts a DHCP request, the DHCP server determines the correct configuration information for that client based on the network segment the client is on.

The following sections

- Describe in detail the information required for each subnetwork profile
- Provide procedures for editing the initial subnetwork profiles created by the NetWare DHCP installation program
- Provide procedures for creating new subnetwork profiles

TCP/IP Configuration Information

The NetWare DHCP service enables you to configure the following TCP/IP-related parameters:

- Subnetwork address
- Subnetwork mask
- IP address of the default router for the subnetwork
- Frame type used for IP transmissions

Name Service Information

The Domain Name System (DNS) provides name-to-IP address mapping services that enable computers to locate each other on a TCP/IP internetwork by name or by IP address. If DNS is not used on your network, you do not need to complete the name service information. If DNS is used on your network, you must know the following information:

- DNS domain name
- IP address of at least one DNS name server

  You can list up to three DNS name servers.

Lease Time Information

DHCP enables clients to be assigned a network address for a fixed time, allowing serial reassignment of network addresses to different clients. The period over which a network address is allocated to a client is referred to as a *lease* .

The Lease Time information tells the DHCP server how long a client wants to lease its assigned IP address. The client can extend its lease with subsequent requests, or the client can issue a message to release the address back to the server when it no longer needs the address. The client can ask for a permanent address assignment by asking for an infinite lease.

You might use DHCP because you have a limited number of IP addresses. If you run out of IP addresses, the DHCP allocation mechanism can re-use addresses that were assigned to clients whose lease has expired. The server uses whatever information is available in the configuration repository to choose an address to re-use.

If the Lease Time parameter is not configured otherwise, the default lease period is three days.

NetBIOS Information

The NetWare DHCP service enables you to configure NetBIOS related information that can be used by NetBIOS over TCP/IP clients. NetBIOS configuration information includes the following:

- NetBIOS over TCP/IP Name Server option

  DHCP enables you to configure a list of IP addresses for NetBIOS name servers. DHCP clients that use NetBIOS over TCP/IP can request a list of NetBIOS name servers from the DHCP server.

- NetBIOS over TCP/IP Node Type option

  DHCP enables you to configure a list of NetBIOS node types. The following 4 node types are supported: B-node (broadcast nodes), P-node (Point-to-Point nodes), M-node (Mixed nodes) and the H-node.

- NetBIOS over TCP/IP scope option

  A NetBIOS scope is the population of computers across which a registered NetBIOS name is known. NetBIOS multicast and broadcast datagram operations must reach the entire extent of the NetBIOS scope. DHCP enables you to define the NetBIOS scope.

Note For more information on NetBIOS related issues, please refer to RFC 1001 and RFC 1002.

IP Address Assignment Information

The NetWare DHCP service enables you to assign IP addresses statically or automatically.

When assigning IP addresses statically, the DHCP server assigns each workstation a specific IP address. Static assignments are based on a defined list of workstation-to-IP address associations.

When assigning IP addresses automatically, the DHCP server assigns a workstation the next available IP address from a pool of IP addresses. The IP address pool may include all IP addresses for a network segment or a subset of IP addresses.

If you choose to have automatic IP address assignment from a subset of IP addresses available for a network segment, you need to define the limits of the IP address pool by designating a start and end IP address for the pool. Addresses that are outside the designated pool limits are still available for static assignment by the DHCP server.

NetWare/IP Information

If NetWare/IP clients on a network segment are using DHCP to obtain an IP address and network configuration information, the subnetwork profile for that segment must include the following NetWare/IP configuration information:

- The name of the NetWare/IP domain to which the clients belong
- Whether or not NetWare/IP clients use Nearest Server Query (NSQ) broadcasts to locate NetWare/IP servers

  An NSQ broadcast is a UDP broadcast that a NetWare/IP client sends out at startup in the following cases:

  - A nearest NetWare/IP server is not specified in the DHCP reply

  - The NetWare/IP servers specified in the DHCP reply are busy or unavailable

- Whether or not clients are using NetWare/IP 1.1 software

- The IP address of the primary DSS server for the NetWare/IP domain to which this NetWare/IP server belongs

- The hostnames, IP addresses, or subnetwork IP addresses of up to five DSS servers that are closest to the NetWare/IP clients on this subnetwork

- The hostnames, IP addresses, or subnetwork IP addresses of up to five NetWare/IP servers that are closest to the NetWare/IP clients on this subnetwork

  NetWare/IP clients must locate a NetWare/IP server at startup. If a nearest NetWare/IP server is not provided by DHCP, NetWare/IP clients will send an NSQ broadcast or query a DSS server to locate a NetWare/ IP server.

- The number of times NetWare/IP clients will attempt to communicate with a given DSS server at startup

- The number of seconds NetWare/IP clients will wait between attempts to communicate with a given DSS server at startup

Important You need to specify NetWare/IP configuration information only if NetWare/IP clients on the subnetwork are using DHCP or BOOTP to obtain their TCP/IP and NetWare/IP configurations. If TCP/IP and NetWare/IP are configured locally, you do not need to complete the NetWare/IP Configuration form.

Editing an Initial Subnetwork Profile

When you install the NetWare DHCP service, DHCPCFG automatically detects all subnetworks to which the DHCP server is directly connected and creates a subnetwork profile for each one. For example, if the DHCP server has three network cards, each attached to a different subnetwork, DHCPCFG automatically creates an initial subnetwork profile for each of the three subnetworks. However, the information on these initial subnetwork profiles may be incomplete. Therefore, you should edit the initial subnetwork profiles to reflect the configuration information you want the DHCP server to return to the workstations on each subnetwork.

Use the following procedure to customize a subnetwork profile that was automatically created by DHCPCFG during installation:

1. **Start the DHCPCFG utility by typing the following command at the server console prompt:**

   load dhcpcfg <Enter>

2. **From DHCPCFG's Configuration Menu, choose the following:**

   –>**Subnetwork Profile**

3. **To change the name of a subnetwork profile, choose the profile you want to modify from the list of subnetwork profiles and press** <F3> **.**

4. **When prompted, enter a new name for the subnetwork profile.**

5. **To display the Subnetwork Profile form, choose the profile you want to modify from the list of subnetwork profiles and press** <Enter> **.**

6. **Edit the subnetwork profile configuration as necessary.**

7. **When you finish editing a subnetwork profile, press** <Esc> **.**

8. **When prompted, choose Yes to save your changes.**

9. **To return to DHCPCFG's Configuration Menu, press** <Esc> **.**

Creating a New Subnetwork Profile

You must manually create new subnetwork profiles for any subnetworks that contain DHCP clients and to which the DHCP server is not directly connected.

1. **Start the DHCPCFG utility by typing the following command at the server console prompt:**

   load dhcpcfg <Enter>

2. **From DHCPCFG's Configuration Menu, choose the following:**

   –>**Subnetwork Profile**

3. **At the list of subnetwork profiles, press** <Insert> **.**

4. **When prompted, enter a name for the new subnetwork profile.**

5. **When prompted, enter the subnetwork address.**

6. **On the Subnetwork Profile form, choose the subnetwork mask used on this network segment.**

   6a. **Press** <Enter> **in the Subnetwork Mask field.**

   6b. **From the Available Subnet Masks list, choose the appropriate subnetwork mask and press** <Enter> **.**

7. **Choose the TCP/IP frame type used on this subnetwork.**

   7a. **Press** <Enter> **in the Frame Type field.**

   7b. **From the Frame Type list, press** <Insert> **.**

   7c. **From the Available Frame Types list, choose a frame type or choose Specify Other and enter the name of another frame type.**

   7d. **To save the entry and return to the Subnetwork Profile form, press** <Esc> **.**

8. **Enter the IP address of the default router for this subnetwork.**

9. **Indicate whether the network uses DNS.**

   If you enter No, skip to Step 11 .

10. **Set up DNS support.**

    10a. **In the Domain Name field, enter the fully qualified name of the DNS domain for the DNS clients, or resolvers, on this subnetwork.**

    10b. **In the Primary Name Server field, enter the IP address of the first DNS name server the hosts on this subnetwork should contact to resolve DNS queries.**

    10c. **In the Secondary Name Server and Tertiary Name Server fields, enter the IP addresses of the second and third DNS name servers the hosts on this subnetwork should contact to resolve DNS queries.**

    10d. **To return to the Subnetwork Profile form, press** <Esc> **.**

11. **In the Lease Time Hours or Days field, enter the amount of time an IP address assignment lease is valid.**

12. **In the Renewal Time (T1) field, enter the percentage of lease time remaining when the client should attempt to contact the DHCP server that originally issued it an IP address.**

13. **In the Rebinding Time (T2) field, enter the percentage of lease time remaining when the client should attempt to contact any DHCP server.**

14. **To configure NetBIOS parameters, choose <See Form> in the NetBIOS Parameters field and press** <Enter> **.**

    14a. **In the Primary Name Server field, enter the IP address of the first NetBIOS name server the hosts on this subnetwork should contact.**

    14b. **In the Secondary Name Server and Tertiary Name Server fields, enter the IP addresses of the second and third NetBIOS name servers the hosts on this subnetwork should contact.**

    14c. **In the Node Type field, press** <Enter> **to choose a node type from the list of node types.**

    14d. **In the Scope field, enter the alphanumeric value the indicates the NetBIOS scope.**

    14e. **To return to the Subnetwork Profile form, press** <Esc> **.**

15. **In the Automatic IP Address Assignment field, indicate whether the DHCP server should assign IP addresses on this subnetwork automatically.**

    If you enter No, skip to Step 18 .

    If you enter Yes, the Assign All Subnet IP Addresses field appears on the Subnetwork Profile form.

16. **In the Assign All Subnet IP Addresses field, indicate whether the DHCP server should assign all IP addresses on this subnetwork automatically.**

    If you enter No, the Start Address and End Address fields appear on the Subnetwork Profile form.

If you enter Yes, DHCPCFG automatically fills in the Start Address and End Address fields on the Subnetwork Profile form. Skip to Step 18 .

17. **In the Start Address and End Address fields, enter the limits of the IP address pool from which the DHCP server should assign addresses.**

18. **Indicate whether this DHCP server will support NetWare/IP clients on this subnetwork.**

    If you enter No, skip to Step 20 .

19. **Set up NetWare/IP support.**

    19a. In the NetWare/IP Domain Name field, enter the fully qualified name of the NetWare/IP domain to which the nodes on this subnetwork belong.

    19b. Indicate whether the NetWare/IP clients on this subnetwork should use NSQ broadcasts to locate the nearest server.

    19c. Indicate whether the NetWare/IP clients are using NetWare/IP version 1.1 software.

    19d. Enter the IP address of the primary DSS server for the NetWare/IP domain to which the NetWare/IP clients on this subnetwork belong.

    19e. Enter the IP addresses or subnetwork addresses of up to five DSS servers that are closest to the NetWare/IP clients on this subnetwork.

    19f. Enter the IP addresses or subnetwork addresses of up to five NetWare/IP servers that are closest to the NetWare/IP clients on this subnetwork.

    19g. Enter the number of times the NetWare/ IP clients on this subnetwork will attempt to communicate with a given DSS server at startup.

    19h. Enter the amount of time in seconds the NetWare/[P clients on this subnetwork will wait before retrying a given DSS server at startup.

    19i. To return to the Subnetwork Profile form, press <Esc> **.**

20. **To exit the Subnetwork Profile form and save your changes, press** <Esc> **.**

21. **When prompted, choose Yes to save the new subnetwork profile.**

22. **To return to DHCPCFG's Configuration Menu, press** <Esc> **.**

Setting Up IP Address Assignments

An IP address assignment is an entry in the DHCP server database that associates an IP address with a specific network node. When you use automatic IP address assignment, the DHCP server creates an IP address assignment entry for each workstation to which it automatically assigns an IP address. When you use static IP address assignment, you must manually enter an IP address assignment for each workstation to which you want the DHCP server to assign a specific address.

There are two situations in which you should set up an IP address assignment:

- Set up an IP address assignment for any DHCP or BOOTP client that has an established IP address. This can be a NetWare DHCP client, a BOOTP client, or a NetWare/IP client.

- Set up an IP address assignment for any node, such as a NetWare server or a UNIX host, that has an IP address within the range of IP addresses that you designated for automatic assignment.

Gathering Necessary Information

You use the IP Address Assignment option from DHCPCFG's Configuration Menu to set up an IP address assignment. To set up an IP address assignment, you need the following information about the workstation:

- The workstation name

  This can be an arbitrary label of up to 48 uppercase or lowercase letters. However, for simplicity, it is best to use the username of the workstation user.

- The IP address that you want the DHCP server to assign to the workstation or the established IP address of the NetWare server or UNIX host

When you fill in the IP address, the DHCPCFG utility automatically displays the name of the subnetwork to which the node belongs.

- The physical, or MAC, address of the workstation

  The physical address for Ethernet and token ring network boards is six hexadecimal bytes separated by colons—for example, 00:00:lc:36:06:cf. For ARCnet* network boards, the address is one hexadecimal byte—for example, 4a.

  If you do not know the client's MAC address, you can get it by executing one of the following commands at the DOS prompt:

  - **nlist user /a** (NetWare 4)
  - **userlist /a** (NetWare 3.12)

  If you are adding an IP address entry for a NetWare server or UNIX host, you do not need to enter a physical address.

Note

NetWare DHCP does not allow duplicate MAC addresses in IP address assignments. If you add an IP address assignment entry with a MAC address that is used in another entry, DHCPCFG will delete the first entry. For example, if you create a new IP address assignment for a workstation that has been moved to a new subnetwork, DHCPCFG will automatically delete the previous IP address assignment entry.

Creating a New IP Address Assignment

1. **Start the DHCPCFG utility by typing the following command at the server console prompt:**

   load dhcpcfg <Enter>

2. **From DHCPCFG's Configuration Menu, choose the following:**

   –>IP Address Assignment

3. **From the list of IP Address Assignments, press** <Insert> **.**

4. **When prompted, enter the workstation name, usually the username of the workstation user.**

5. **In the Internet Address field of the Workstation IP Address Assignment form, enter the workstation's IP address.**

The utility automatically displays the name of the subnetwork profile that will be used for the workstation.

6. **Enter the workstation's physical address.**

   For Ethernet and token ring networks, enter the physical address as six hexadecimal bytes separated by colons. For ARCnet networks, enter the physical address as one hexadecimal byte.

7. **To exit the Workstation IP Address form, press** `<Esc>` **.**

8. **When prompted, choose Yes to save the new assignment.**

9. **To return to DHCPCFG's Configuration Menu, press** `<Esc>` **.**

Note For static entries, the Lease Time field will show 0 days, 0 hours and cannot be edited.

Defining Excluded Nodes

The DHCP server assigns IP addresses to all workstations that broadcast a DHCP request unless directed otherwise. If there are nodes on your network that you do not want to receive IP address assignments, you must add the nodes to the excluded nodes list. The DHCP server will not send a DHCP reply to any workstation that is listed on the excluded nodes list.

Gathering Necessary Information

You use the Excluded Nodes option from DHCPCFG's Configuration Menu to set up a list of workstations that you do not want the DHCP server to respond to.

To exclude a node, you need to know the physical (MAC) address of the workstation. You can also exclude a group of nodes by using the wildcard character in place of the node portion of the MAC address. NetWare DHCP accepts the asterisk (*) as a wildcard character.

For example, to exclude all nodes using a particular type of network board, you would enter the manufacturer ID portion of the MAC address and replace the node portion of the address with an asterisk (*).

Creating an Excluded Node Entry

1. **Start the DHCPCFG utility by typing the following command at the server console prompt:**

   load dhcpcfg <Enter>

2. **From DHCPCFG's Configuration Menu, choose the following:**

   –>**Excluded Nodes**

3. **From the list of excluded nodes, press** <Insert> **.**

4. **When prompted, enter the physical address of the excluded workstation or a wildcard version of the physical address for a group of workstations.**

   For Ethernet and token ring networks, enter the physical address as six hexadecimal bytes separated by colons. For ARCnet networks, enter the physical address as one hexadecimal byte.

5. **Enter a comment indicating why the workstation is excluded.**

6. **To return to DHCPCFG's Configuration Menu, press** <Esc> **.**

Chapter

13 *Configuring NetWare-to-UNIX Printing*

To provide print services on a NetWare/IP™ network that uses only the TCP/IP protocol suite or to print to a UNIX* printer on a mixed IP–IPX network, you need to configure the UNIX printing protocol, lpr.

To use the lpr protocol, you need to

- Make sure that network printers are using printer cards that support the line printer daemon (lpd) protocol.
- Configure the UNIX host to which the printer is attached, as described in "Configuring the UNIX Host" on page 211
- Configure an lpr gateway, as described in "Configuring the lpr Gateway" on page 212 The lpr gateway software is installed with NetWare/IP.
- Load the NetWare® print server software and the lpr gateway, as described in "Starting the lpr Gateway" on page 217

This chapter provides procedures for configuring NetWare-to-UNIX printing. Specific steps for configuring the UNIX host to which the printer is attached depend on the type of UNIX operating system installed on the host, so this chapter includes only general guidelines for configuring the host machine.

For detailed procedures on configuring various UNIX operating systems, see NetWare NFS Bidirectional Printing in *Novell Application Notes* (December 1992).

Configuring the UNIX Host

The NetWare-to-UNIX print service uses the lpr protocol to transmit and receive printing related commands and data from UNIX hosts. Before you configure the NetWare-to-UNIX print service, determine whether or not the UNIX host to which the network printer is attached supports the lpr protocol.

A remote UNIX host cannot accept print jobs from the lpr gateway software until you

- Identify the NetWare/IP server running the lpr gateway to the UNIX host.
- Authorize the NetWare/IP server to access the UNIX host.

Each of these tasks is briefly described in the following sections.

Identifying the NetWare/IP Server to the UNIX Host

To identify the NetWare/IP server running the lpr gateway to the UNIX host, add the name and IP address of the NetWare server to the /etc/hosts file on the UNIX host.

Authorizing Access

When a UNIX host receives a print request from a client, it searches for the client name in an authorization file. Only clients listed in the file are authorized to send print jobs. If the NetWare/IP server is not identified in this file, you cannot use the NetWare-to-UNIX print service.

Some implementations of UNIX use the /etc/hosts.lpd file as the authorization file, but other implementations of UNIX might use a different file. See your UNIX system documentation for information about authorizing NetWare access.

Configuring the lpr Gateway

To configure the lpr gateway software, you need to complete the following tasks:

- Install and configure the NetWare/IP software on the server that will function as an lpr gateway, as described in Chapter 5, “Installing the NetWare/IP Software,” on page 65
- Create Novell Directory Services™ (NDS™) objects that represent the network printer, the print server, and a print queue.
- Make the appropriate associations among the Directory objects you create.

Each of these tasks is described in the following sections.

Prerequisites

Before trying to configure NDS and the lpr gateway software, make sure that the following prerequisites are completed on the NetWare/IP server:

- The TCPIP NetWare Loadable Module™ (NLM™) is loaded and configured properly.
- The NetWare/IP server has an entry in its SYS:ETC\HOSTS file for the UNIX host.

Creating Printing-Related Objects

Before you can use the NetWare-to-UNIX print service, you need to create three objects in the Directory database: a Print Queue object, a Printer object, and a Print Server object. Each of these objects represents a physical entity on the network.

All three of these objects should be created in the same Directory context. The Directory context should be determined by who will most often use the NetWare-to-UNIX print service and where the Server object is that represents the NetWare/IP server on which the lpr gateway and print server software are loaded.

The following sections describe procedures for creating Directory objects that will enable you to use the NetWare-to-UNIX print service on your network.

Creating a Print Queue Object

Use NetWare Administrator to create a Print Queue object:

1. **From NetWare Administrator's browse window, choose the container into which you want to place the Print Queue object.**
2. **From the Object menu, choose Create.**
3. **From the list of objects, choose Print Queue and choose OK.**
4. **In the Print Queue Name field, enter a name for the Print Queue object.**

The name should be descriptive of who should use the queue or where it is located and should follow standard object naming conventions.

5. **In the Print Queue Volume field, enter or browse for the name of a volume that can support a print queue.**

   The volume should have enough disk space free to support the largest print job load the queue may hold.

6. **Choose the Create button.**

Creating a Printer Object

Use NetWare Administrator to create a Printer object:

1. **From NetWare Administrator's browse window, choose the container into which you want to place the Printer object.**

2. **From the Object menu, choose Create.**

3. **From the list of objects, choose Printer and choose OK.**

4. **In the Printer Name field, enter a name for the Printer object.**

   The name should be descriptive of the type of printer this object represents or where it is located, and should follow standard object naming conventions.

5. **Choose the Define Additional Properties box, and choose the Create button.**

6. **On the right side of the Printer object dialog, choose the Assignments button.**

7. **Choose the Add button to assign a print queue to this Printer object.**

8. **Choose the Print Queue object you created to service the NetWare-to-UNIX print service, and choose OK.**

9. **On the right side of the Object dialog, choose the Configuration button.**

10. **From the Printer Type drop-down list, choose UNIX.**

11. **When prompted, enter the host name of the UNIX host to which the network printer is attached in the Host Name field.**

12. **In the Printer Name field, enter the name by which the printer is known to remote hosts, and choose OK.**

13. **Choose OK to exit the Printer object dialog.**

Creating a Print Server Object

Use NetWare Administrator to create a Print Server object:

1. **From NetWare Administrator's browse window, choose the container into which you want to place the Print Server object.**

2. **From the Object menu, choose Create.**

3. **From the list of objects, choose Print Server and choose OK.**

4. **In the Print Server Name field, enter a name for the Print Server object.**

   The name should be descriptive of the type of print server this object represents or where it is located, and should follow standard object naming conventions.

5. **Choose the Define Additional Properties box, and choose the Create button.**

6. **On the right side of the Print Server object dialog, choose the Assignments button.**

7. **Choose the Add button to assign a printer to this Print Server object.**

8. **Choose the Printer object you created to represent the network printer attached to a UNIX host on the network, and choose OK.**

9. **Choose OK to exit the Print Server object dialog.**

Associating Printers, Queues, and Print Servers

If you created Directory objects as described in the previous sections, you have already associated a Print Server with a Printer and a Printer with a Print

Queue. If you are using existing Directory objects to enable NetWare-to-UNIX printing, you might need to assign a Printer object to a Print Server object and a Print Queue object to a Printer object.

Assigning a Queue to a Printer

Use NetWare Administrator to assign a print queue to a printer:

1. **From NetWare Administrator's browse window, choose the Printer object to which you want to assign a print queue.**

   The Printer object should be configured to represent the network printer attached to a UNIX host.

2. **From the Object menu, choose Details.**

3. **On the right side of the Printer object dialog, choose the Assignments button.**

4. **Choose the Add button to assign a print queue to this Printer object.**

5. **Choose the Print Queue object you want to service the NetWare-to-UNIX print service, and choose OK.**

6. **Choose OK to exit the Printer object dialog.**

Assigning a Printer to a Print Server

Use NetWare Administrator to assign a printer to a print server:

1. **From NetWare Administrator's browse window, choose the Print Server object to which you want to assign a printer.**

2. **From the Object menu, choose Details.**

3. **On the right side of the Print Server object dialog, choose the Assignments button.**

4. **Choose the Add button to assign a printer to this Print Server object.**

5. **Choose the Printer object you created to represent the network printer attached to a UNIX host on the network, and choose OK.**

6. **Choose OK to exit the Print Server object dialog.**

Starting the lpr Gateway

With the UNIX host to which a network printer is attached, and the NetWare/IP server that is to function as an lpr gateway properly configured, and the necessary Directory objects created, you are ready to initialize the lpr gateway software. To start the lpr gateway and enable NetWare-to-UNIX printing, you need to

- Load the NetWare print server software (PSERVER.NLM) on the NetWare/IP server that is to function as an lpr gateway

- Load the LPR_GWY NLM on the NetWare/IP server that is to function as an lpr gateway.

Loading the Print Server

Use the following procedure to load the NetWare print server software on the NetWare/IP server that is to function as an lpr gateway:

1. **At the server console prompt, load the print server software by typing the following command:**

   load pserver

2. **When prompted, enter the complete name of the Print Server object you created using "Creating a Print Server Object" on page 215**

3. **Press** <Alt–Esc> **as needed to return to the server's system console prompt.**

Loading the lpr Gateway Software

Use the following procedure to load the lpr gateway software on the NetWare/IP server that is to function as an lpr gateway:

1. **At the server console prompt, load the lpr gateway software by typing the following command:**

   load lpr_gwy

With the print server and lpr gateway software loaded, you are ready to print from a NetWare/IP client to a network printer attached to a UNIX host.

To test the NetWare-to-UNIX printing configuration:

1. At a NetWare client, capture the print queue assigned to the network printer attached to the UNIX host.

2. Send a print job.

Use the Job List page of the Print Queue object dialog in NetWare Administrator and the Printer Status screen in PSERVER to check the status of the print job.

Appendix

A *Planning a NetWare/IP Network*

This appendix provides information and exercises to help you plan and implement a NetWare/IP™ network. There are two parts to this appendix.

- The first part describes NetWare/IP networks with varying degrees of complexity. The sample configurations can help you plan a NetWare/IP internetwork.
- The second part of this appendix provides the NetWare/IP planning worksheets.

Sample NetWare/IP Configurations

This section provides sample NetWare/IP configurations to help you plan a NetWare/IP internetwork. These sample configurations use the fictitious Acme Company to illustrate how to deploy NetWare/IP using the planning guidelines presented in this appendix.

These examples build on each other, from a simple initial installation to a complex WAN configuration. Use the sample that most closely matches your network environment. Or, read through all the examples for an illustration of a typical IPX™ to IP migration.

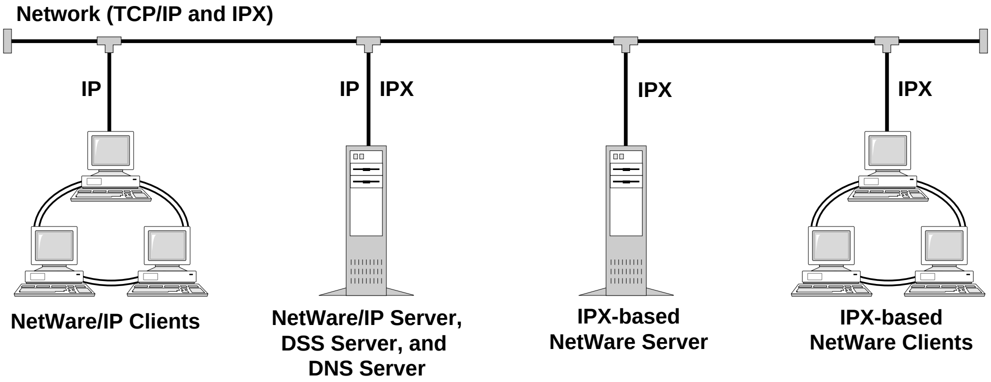
For a sample . . .	**See . . .**
Single-server configuration	"Single-Server Configuration" on page 220
Forwarding gateway configuration	"Forwarding Gateway Configuration" on page 221
Internetwork configuration	"Internetwork Configuration" on page 223
WAN configuration	"WAN Configuration" on page 225
IPX to IP migration	"WAN Configuration" on page 225

Single-Server Configuration

When you first introduce NetWare/IP into your site, you may want to configure a single server with all of the required NetWare/IP services. Figure 1-1 illustrates a single server NetWare/IP configuration.

Figure 1-1

Single-Server Configuration



In this example, Acme installs the NetWare/IP software on a single NetWare server and on several NetWare clients on its corporate LAN. To support the mixed IP–IPX environment, Acme does the following:

1. Configures the NetWare/IP server as the master DNS name server.

   Acme has never used DNS in their network; therefore, the administrator creates the acme.com. DNS domain and configures the NetWare/IP server as the master DNS name server for this domain. Then, to support NetWare/IP, the administrator creates the nwip.acme.com. NetWare/IP domain and adds the following resource records to the master DNS database:

   - An SOA record for acme.com.
   - An NS record linking the primary DSS server to the nwip.acme.com. NetWare/IP domain
   - An A record for the primary DSS server

2. Configures the NetWare/IP server as the primary DSS server.

3. Configures the NetWare/IP server as a non-forwarding gateway.

Because the non-forwarding gateway has both IP and IPX interfaces, it can service NetWare/IP clients as well as IPX-based NetWare clients.

This configuration is valuable for initial setup and testing. However, using a single server to run NetWare/IP and both support services (DSS and DNS) is not recommended in the long run for the following reasons:

- Performance may be impacted: the increased traffic on a server running NetWare/IP, DSS, and DNS may create a bottleneck.

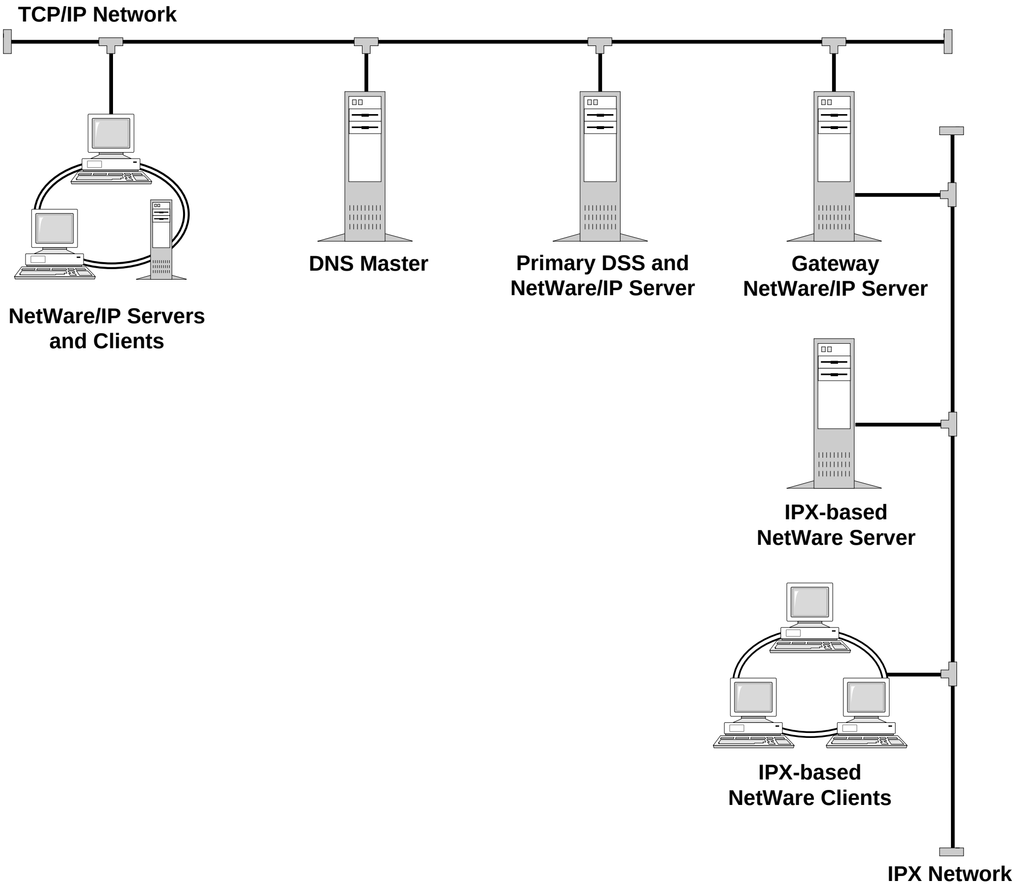
- Reliability may be diminished: if the single server is off-line, no NetWare/IP clients anywhere on the network can access NetWare services.

Forwarding Gateway Configuration

As you migrate from IPX to IP, you might identify network segments that must remain IPX-based. To accommodate any remaining IPX-based network segments, you can configure a NetWare/IP server to act as a forwarding gateway. Figure 1-2 illustrates a simple forwarding gateway configuration.

Figure 1-2

Forwarding Gateway Configuration


TCP/IP Network
NetWare/IP Servers and Clients
DNS Master
Primary DSS and NetWare/IP Server
Gateway NetWare/IP Server
IPX-based NetWare Server
IPX-based NetWare Clients
IPX Network

In this example, Acme continues to migrate its network from IPX to IP by completing the IPX to IP conversion on its corporate LAN. However, the network in Acme's marketing department remains IPX-based. To connect the two network segments, Acme does the following:

1. Configures a NetWare/IP server as a forwarding gateway.

   The forwarding gateway has an interface to the TCP/IP network and a second interface to the IPX network. It transfers packets between the TCP/IP backbone and the IPX backbone, translating between the two protocols. As a result, clients on either backbone can access NetWare services on both backbones.

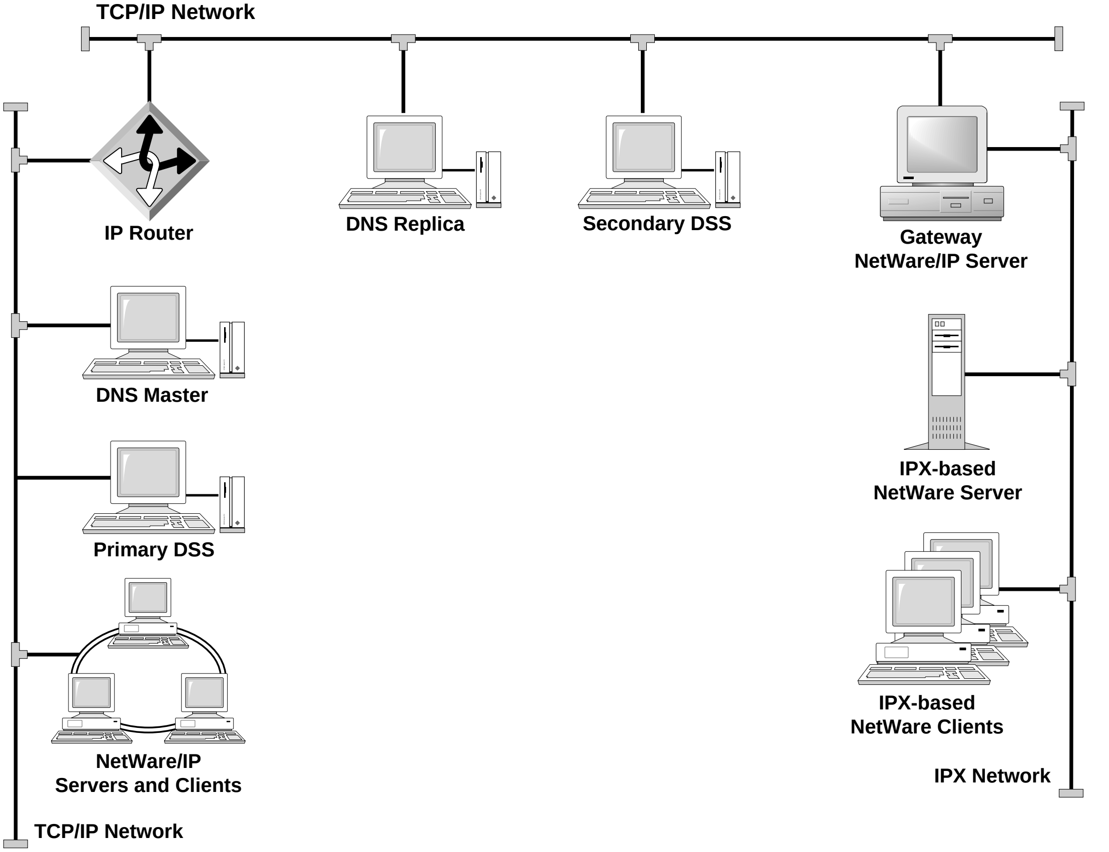
2. Distributes the NetWare/IP support services to balance the network load.

   Because the NetWare/IP gateway machine is heavily loaded with traffic between the two backbones, Acme decides not to configure it as a DSS or DNS server. Instead, a second server is configured as the master DNS name server, and a third server is configured as the primary DSS server.

Internetwork Configuration

When NetWare/IP is used on separate TCP/IP LANs interconnected by IP routers, locating and replicating support services to preserve performance and reliability becomes essential. Figure 1-3 illustrates a simple internetwork configuration.

Figure 1-3
Internetwork Configuration



In this example, Acme installs NetWare/IP on its engineering backbone and interconnects the engineering and corporate network segments with an IP router. Now, NetWare/IP clients on the corporate and engineering backbones can access NetWare servers on both TCP/IP network segments and on the IPX segment. The IPX clients gain access to services on both TCP/IP networks through the forwarding gateway. As a result, the system administrator must allow for the effects of this traffic on the IP router that connects the two TCP/IP network segments and the forwarding gateway that connects the IPX segment with the other segments. Therefore, Acme does the following:

1. Configures a replica DNS name server on the engineering backbone.

2. Configures a secondary DSS server on the engineering backbone.

3. Adds Address (A) and Name Server (NS) resource records for the secondary DSS server to the master DNS name server for the NetWare/IP domain.

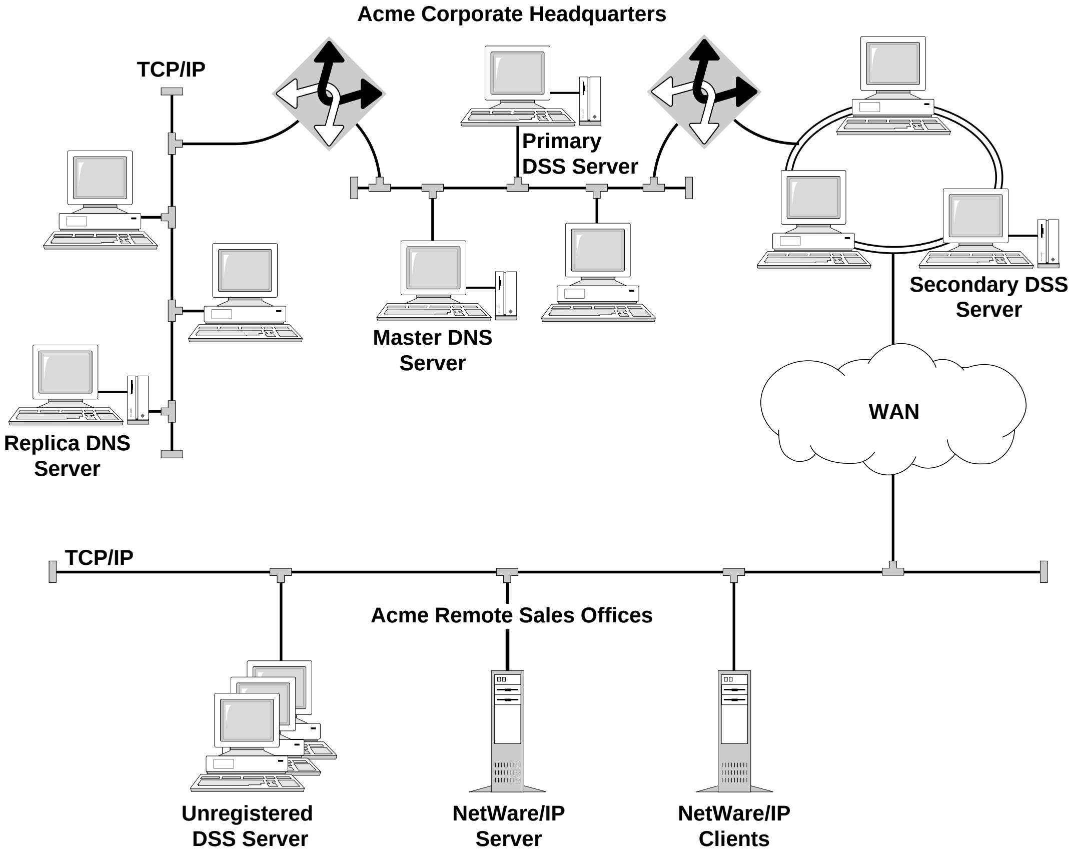
As a result, traffic across the heavily used IP router link between the engineering and corporate network segments is reduced, so performance is impacted less. Should the router be taken offline for any reason, the NetWare/IP clients on both TCP/IP networks can continue to access local services, because the DNS and DSS support services are present on both segments.

WAN Configuration

When NetWare/IP is used in a wide area network (WAN) environment, NetWare/IP and its support services must be configured to minimize traffic over the slow speed WAN link. Figure 1-4 illustrates a simple WAN configuration.

Figure 1-4

WAN Configuration



In this example, Acme completes its IPX to IP migration by installing NetWare/IP on the remaining clients and servers throughout the company, including its remote sales office. The remote sales network is connected to the rest of the NetWare/IP network by a WAN link. To optimize performance across this slow speed link, Acme does the following:

1. Configures an unregistered DSS server on the sales network.
2. Configures each NetWare/IP client and server on the sales network to use the unregistered DSS server as the preferred DSS server.
3. Increases the DSS–NetWare/IP Synchronization Interval and Primary DSS–Secondary DSS Synchronization Interval parameter values at the primary DSS server from the default five minutes to 15 minutes.

4. Calculates the amount of time in ticks it takes a packet to travel from a node on the corporate network to a node on the sales network. Acme then configures Ticks Between Nodes on Different IP Networks parameter at the primary DSS server with the average tick value calculated.

As a result, the DNS query and database synchronization traffic across the WAN link is minimized. In addition, should the WAN link go down, the NetWare/IP clients on the sales network can continue to access local services via the unregistered DSS server.

Using the Planning Worksheets

Before you begin the installation or configuration procedures in this manual, complete the following worksheets:

- NetWare/IP Support Services Planning Worksheet
- NetWare/IP Servers Planning Worksheet
- Primary DSS Configuration Worksheet
- NetWare/IP Client Configuration Worksheets

You might not need to fill in every worksheet, but it is recommended that you fill in as many as apply to ensure a smooth installation and configuration. After you complete the worksheets, you have all the information you need to configure a NetWare/IP network. The completed worksheets also provide a valuable written record of your network's configuration.

This section includes the following:

- Examples of completed planning worksheets

Note The worksheets in this section are examples only. You must fill in the applicable blank worksheets with information that applies to your specific network configuration.

- Blank planning worksheets

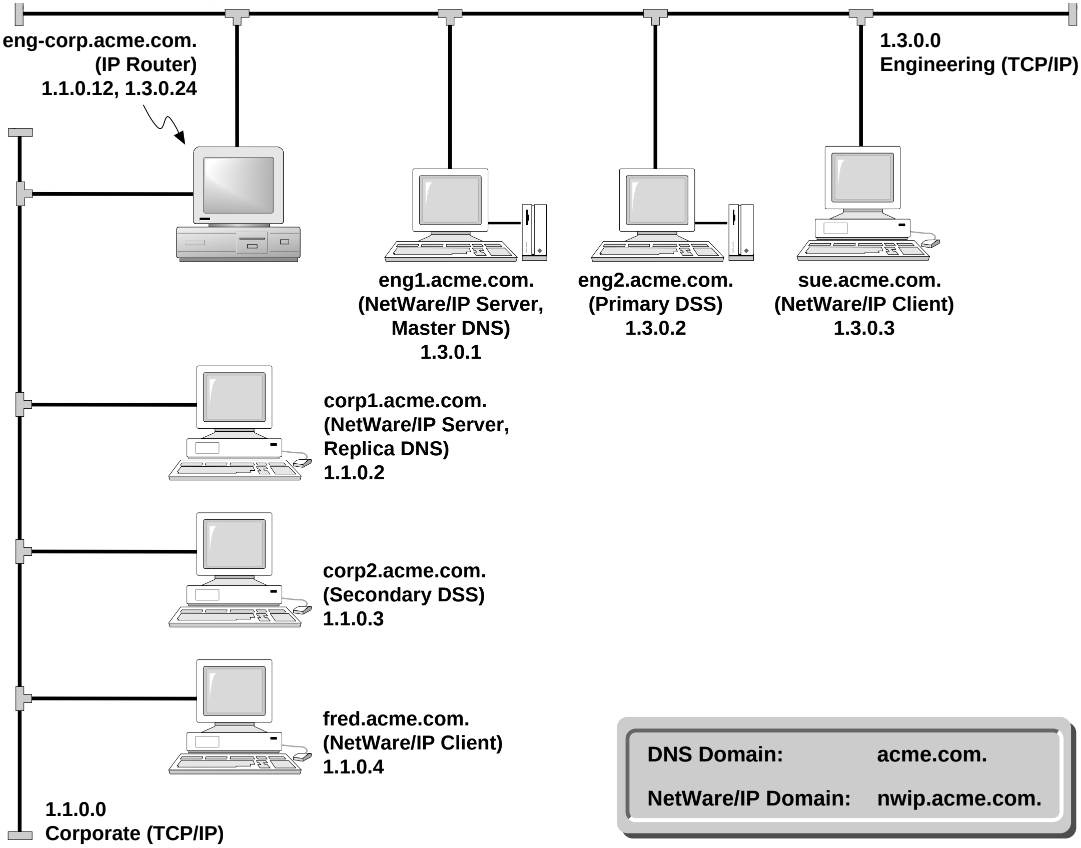
Planning Worksheet Examples

The sample worksheets in this section illustrate an IP-only NetWare/IP network. In this configuration, the internetwork consists of two TCP/IP backbones connected by an IP router. Because NetWare/IP clients reside on both backbones, NetWare/IP support services are replicated for load balancing and redundancy.

Figure 1-5 illustrates the NetWare/IP configuration Acme Company uses to connect the TCP/IP network in its engineering department with its corporate TCP/IP backbone. These separate network segments are connected by an IP router, eng-corp.acme.com.

Acme has configured a replica DNS and a secondary DSS server on the corporate backbone. If the IP router should become unavailable, NetWare/IP clients on the corporate backbone can still access their local servers because DNS and DSS support services are provided on their subnetwork.

Figure 1-5
TCP/IP-Only Configuration



NetWare/IP Support Services Planning Worksheet

Section 1 of the NetWare/IP Support Services Planning Worksheet specifies the DNS and NetWare/IP domain names. The DNS domain you specify must be the parent domain of the NetWare/IP domain. This section also lists the names and IP addresses of the master and replica DNS name servers you plan to configure.

Section 2 lists the hostnames and IP addresses of the primary DSS server and the secondary DSS servers you plan to configure to support your NetWare/IP domain.

Because Acme's NetWare/IP internetwork includes multiple TCP/IP segments connected by an IP router, Acme has replicated the DNS and DSS support services on the corporate network by configuring corp1.acme.com. as a replica DNS name server and corp2.acme.com. as a secondary DSS server. Eng1.acme.com. is the master DNS name server and eng2.acme.com. is configured as the primary DSS server.

NetWare/IP Support Services Planning Worksheet

Date ***November 11, 1996***

Prepared by ***Henry Lodge***

	Use this form to plan your NetWare/IP domain and identify your DNS and DSS servers	Name *Fill in the fully qualified name of the domain or system*	Address *Give IP addresses in dotted notation*
1	**Domain Name System (DNS)**		
	NetWare/IP Domain	***nwip.acme.com.***	
	DNS Domain *Must be the parent domain of the NetWare/IP domain*	***acme.com.***	
	Master DNS Name Server	***eng1.acme.com.***	***1.3.0.1***
	Replica DNS Name Server(s)	***corp1.acme.com.***	***1.1.0.2***
2	**Domain SAP/RIP Service (DSS)**		
	Primary DSS Server	***eng2.acme.com.***	***1.3.0.2***
	Secondary DSS Server(s) *Configure at least one per subnetwork*	***corp2.acme.com.***	***1.1.0.3***

NetWare/IP Servers Planning Worksheet

This worksheet lists the hostnames and IP addresses of all NetWare/IP servers you plan to configure for a given NetWare/IP domain.

Acme Company has four servers configured as NetWare/IP servers: eng1.acme.com., eng2.acme.com., corp1.acme.com., and eng-corp.acme.com., which is configured as an IP router. Note that only one of the IP interfaces on the IP router is designated as its primary interface for NetWare/IP traffic.

NetWare/IP Servers Planning Worksheet

Date ***November 11, 1996***

Prepared by ***Henry Lodge***

Use this form to plan your NetWare/IP servers	Name *Fill in the fully qualified name of the domain or system*	Address *Give IP addresses in dotted notation*
NetWare/IP Domain	***nwip.acme.com.***	
NetWare/IP Servers	***eng1.acme.com.***	***1.3.0.1***
	eng2.acme.com.	***1.3.0.2***
	eng-corp.acme.com.	***1.1.0.12***
	corp1.acme.com.	***1.1.0.2***

Primary DSS Server Configuration Worksheet

Section 1 of the Primary DSS Server Configuration Worksheet identifies the primary DSS server for your NetWare/IP domain and specifies the IPX network number you have assigned to your NetWare/IP internetwork. The IPX network number enables the NetWare/IP internetwork to function as a virtual IPX network; the IPX network number you choose must be unique throughout your internetwork.

Section 2 specifies the tunable parameter settings you wish to use on your NetWare/IP internetwork. The tunable parameters are configured at the primary DSS server. These parameter values are then downloaded to all secondary DSS servers, NetWare/IP servers, and NetWare/IP clients. Thus, these parameters determine performance network-wide. As their name implies, you can adjust the tunable parameters as needed to optimize network performance. For a description of each tunable parameter, see “Primary DSS Configuration Form” on page 116

Performance monitoring has indicated that Acme can benefit from increasing the DSS–NetWare/IP server and primary–secondary DSS database synchronization intervals. Their overall configuration is sufficiently stable that less frequent updates will not impact availability of services, and the decreased traffic will benefit throughput. Acme Company decides to use the default values for all other tunable parameters.

Section 3 provides tables for indicating DSS SAP filters. Acme has not decided to implement DSS SAP filtering at this time.

Primary DSS Server Configuration Worksheet

Date *November 11, 1996*

Prepared by *Henry Lodge*

1

Required Information

NetWare/IP Domain *nwip.com.*

Primary DSS Server Name *eng2.acme.com.*

IPX Network Number *0100fb23*
Hexadecimal address, unique for your internetwork

2

Tunable Parameters

UDP Port Number *43981*
First of two consecutive port numbers assigned for DSS use (default: 43981)

DSS-NetWare/IP Server Synchronization Interval *20*
Frequency in minutes with which the NetWare/IP servers and the Primary DSS server synchronize their databases (range: 1 through 60; default: 5)

Primary-Secondary DSS Synchronization Interval *20*
Frequency in minutes with which the secondary DSS servers and the Primary DSS server synchronize their databases (range: 1 through 60; default: 5)

Maximum UDP Retransmissions *3*
Number of times unacknowledged packets are re-sent (range: 1 through 48; default: 3)

Use UDP Checksum *no*
Specifies whether transmissions are checked for errors (default: no)

Ticks Between Nodes on the Same IP Subnet *2*
Specifies the amount of time in ticks (1/18 second) it takes a packet to reach a host on the same subnetwork

Ticks Between Nodes on the Same IP Net *4*
Specifies the amount of time in ticks (1/18 second) it takes a packet to reach a host on the same network

Ticks Between Nodes on the Different IP Nets *6*
Specifies the amount of time in ticks (1/18 second) it takes a packet to reach a host on a different network

Primary DSS Server Configuration Worksheet

Date *November 11, 1996*

Prepared by *Henry Lodge*

3

DSS SAP Filters

Enable Filtering (default: no) *no*

Outbound Services

Filters		
IP Subnet/Net	SAP Type	Server Name

Exceptions		
IP Subnet/Net	SAP Type	Server Name

Blank Planning Worksheets

This section includes the following planning worksheets:

- NetWare/IP Support Services Planning Worksheet

  Make one copy of this worksheet to identify the DNS and DSS servers for your NetWare/IP network.

- NetWare/IP Servers Planning Worksheet

  Make as many copies of this worksheet as you need to list all of your NetWare/IP servers.

- Primary DSS Server Configuration Worksheet

Make one copy of this worksheet, which provides the information you need to configure the global parameters.

- NetWare/IP Client Worksheet

  Make as many copies of this worksheet as you need before installing the NetWare/IP client software on the workstations in your network.

Short descriptions of some parameters are included on the worksheets. If you need more information about a specific parameter, you can access the configuration forms using the UNICON utility as described in Chapter 6, “Introducing UNICON and NWIPCFG,” on page 83 After you access an online form, you can press the `<F1>` key for detailed information.

NetWare/IP Support Services Planning Worksheet

Date ____________________

Prepared by ____________________

Use this form to plan your NetWare/IP domain and identify your DNS and DSS servers	Name *Fill in the fully qualified name of the domain or system*	Address *Give IP addresses in dotted notation*
1 **Domain Name System (DNS)** NetWare/IP Domain		
DNS Domain		
Must be the parent domain of the NetWare/IP domain Master DNS Name Server		
Replica DNS Name Server(s)		
2 **Domain SAP/RIP Service (DSS)** Primary DSS Server		
Secondary DSS Server(s)		
Configure at least one per subnetwork		

NetWare/IP Servers Planning Worksheet

Date ____________________

Prepared by ____________________

Use this form to plan your NetWare/IP servers	Name *Fill in the fully qualified name of the domain or system*	Address *Give IP addresses in dotted notation*
NetWare/IP Domain		
NetWare/IP Servers		

Primary DSS Server Configuration Worksheet

Date ____________________

Prepared by ____________________

1

Required Information

NetWare/IP Domain ____________________

Primary DSS Server Name ____________________

IPX Network Number ____________________
Hexadecimal address, unique for your internetwork

2

Tunable Parameters

UDP Port Number ____________________
First of two consecutive port numbers assigned for DSS use (default: 43981)

DSS-NetWare/IP Server Synchronization Interval ____________________
Frequency in minutes with which the NetWare/IP servers and the Primary DSS server synchronize their databases (range: 1 through 60; default: 5)

Primary-Secondary DSS Synchronization Interval ____________________
Frequency in minutes with which the secondary DSS servers and the Primary DSS server synchronize their databases (range: 1 through 60; default: 5)

Maximum UDP Retransmissions ____________________
Number of times unacknowledged packets are re-sent (range: 1 through 48; default: 3)

Use UDP Checksum ____________________
Specifies whether transmissions are checked for errors (default: no)

Ticks Between Nodes on the Same IP Subnet ____________________
Specifies the amount of time in ticks (1/18 second) it takes a packet to reach a host on the same subnetwork

Ticks Between Nodes on the Same IP Net ____________________
Specifies the amount of time in ticks (1/18 second) it takes a packet to reach a host on the same network

Ticks Between Nodes on the Different IP Nets ____________________
Specifies the amount of time in ticks (1/18 second) it takes a packet to reach a host on a different network

Primary DSS Server Configuration Worksheet

Date ____________________

Prepared by ____________________

3

DSS SAP Filters

Enable Filtering (default: no) ____________________

Outbound Services

Filters		
IP Subnet/Net	SAP Type	Server Name

Exceptions		
IP Subnet/Net	SAP Type	Server Name

NetWare/IP Client Worksheet – *Page 1*

Date ____________________

Prepared by ____________________

1

▼ Installation Information ▼

Target Drive and Directory for NetWare/IP Client Software: ____________________

Allow Changes to AUTOEXEC.BAT and CONFIG.SYS? □ Yes □ No

Do you want to install MS* Windows support? □ Yes □ No

MS Windows Drive and Directory: ____________________

Do you want to install SMS™ support? □ Yes □ No

SMS Server Name: ____________________

Client System Name: ____________________

SMS Password: ____________________

Number of Buffers: ____________________

Drives to Back Up: ____________________

Network Board Driver: ____________________

2

▼ TCP/IP Configuration Information ▼

Target Drive and Directory for TCP/IP Software: ____________________

Is this client using a BOOTP server? □ Yes □ No

Client System's IP Address: ____________________

Subnetwork Mask: ____________________

IP Router: ____________________

DNS Domain Name (from Support Services Worksheet): ____________________

IP Address of First DNS Name Server to Contact: ____________________

IP Address of Second DNS Name Server to Contact: ____________________

IP Address of Third DNS Name Server to Contact: ____________________

NetWare/IP Client Worksheet – *Page 2*

Date ____________________

Prepared by ____________________

3

▼ NetWare/IP Configuration Information ▼

Is this client using a DHCP server? □ Yes □ No

NetWare/IP Domain Name: ____________________

Preferred DSS Servers: ____________________

____

____

____

____

Nearest NetWare/IP Servers: ____________________

____

____

____

____

Appendix

B *Managing NetWare/IP Remotely*

You can manage a NetWare® server remotely from a DOS workstation, another NetWare server, a machine running an X Window System* client or a UNIXWare™ client, or a VT100*/VT220 terminal.

This appendix discusses the following topics:

- Managing a NetWare server using RCONSOLE
- Managing a different NetWare server using UNICON
- Managing a NetWare server using XConsole

Managing a NetWare Server Using RCONSOLE

Use the RCONSOLE utility to manage a NetWare server from a DOS workstation. After accessing the NetWare console via RCONSOLE, you can use UNICON to log in to another server and manage multiple servers from one console. The following section describes how to use UNICON to log in to another server.

RCONSOLE is included with NetWare. For more information on the RCONSOLE utility, see the NetWare 4 *Utilities Reference* .

Managing a Different NetWare Server Using UNICON

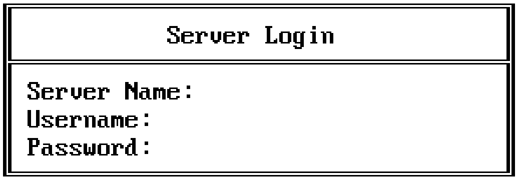
You can use UNICON to log in to any server that is running NetWare NFS Services software or any other software that is UNICON compatible. This allows you to administer multiple servers from one console.

Use the Server Login form to log in to another server.

Using the Server Login Form

The Server Login form provides a way to enter information the first time you log in to a server.

Figure 2-1
Server Login Form



Server Login

Server Name:
Username:
Password:

From UNICON's Main Menu, choose the following to display the Server Login form:

–>**Change Current Server**

The first time you use this option, the utility displays the Server Login form.

If you have used the utility to access other servers, it displays a list of the servers you are currently logged in to. To log in to a server not included on the list, press <Insert> . The utility displays the Server Login form.

This form contains the following fields:

Server Name —the name or IP address of the server you want to log in to.

User Name —your user name. If you are logging in from a different context, use your complete name, such as .CN=RBROWN.OU=SALES.O=ARGOS. UNICON displays the context of the server in a box below the Server Login form.

Password —the password assigned to the user name you entered.

After you log in to a server, you stay logged in until you either use <Delete> to log out or quit UNICON.

Note

Before you can log in to a server using the server name, you must use UNICON to enter the server's IP address in the host table. For further instructions, see Appendix C, "Managing Host Information," on page 257

Logging In to Another Server

1. **From UNICON's Main Menu, choose the following:**

   –>**Change Current Server**

   The first time you use this option, the utility displays the form described in "Using the Server Login Form" on page 244

   If you have used the utility to access other servers, UNICON displays a list of servers that you are logged in to.

2. **Choose the server to access.**

   2a. If the server you want to access is listed, highlight it and press <Enter> **.**

   The utility connects you to the selected server and displays the list of servers. The process continues with Step 4 .

   2b. If the server you want to access is not listed, press <Insert> **.**

   The utility displays the form described in "Using the Server Login Form" on page 244

3. **Fill in the Server Login form.**

   The utility connects you to the selected server and displays the list of servers. The new server appears in the list.

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Managing a NetWare Server Using XConsole

XConsole allows you to administer the NetWare server from an X terminal, a workstation that provides X terminal functionality (runs an X server), a VT100/VT220 terminal, or a terminal that provides exact VT100/VT220 terminal emulation.

XConsole runs on a NetWare file server. You can open a console session on the remote workstation and view the NetWare console display. You can perform any operation during the session that you could perform at the server console, except for restarting the server or XConsole module.

You can open multiple XConsole sessions to a single NetWare server and have each session show a different console screen. You can also open sessions to multiple NetWare servers simultaneously.

Using XConsole

To run XConsole, you must have the following NetWare Loadable Modules™ (NLMs) installed and running on your NetWare server:

- The REMOTE NLM, which handles various NetWare screen drivers, including RSPX/RCONSOLE. The REMOTE NLM is part of the NetWare 3.x and NetWare 4.x software packages.

- The XCONSOLE NLM, which contains a simplified version of the TELNET server and the means to display the NetWare console screen as an X Window System screen or a VT100/VT220 screen. The XCONSOLE NLM is part of the NetWare NFS Gateway product.

Loading the XConsole Software

Load the REMOTE NLM from the NetWare console, if it is not already running, by typing

LOAD REMOTE <Enter>

Next, load the XCONSOLE NLM from the NetWare console, if it is not already running, by typing

LOAD XCONSOLE [s=*sessions* **] [/24]** <Enter>

Replace *sessions* with the number of XConsole sessions that the server can run concurrently (up to 64). The default value is 6.

If you load XConsole using the /24 option, the screen displays lines 2 through 25 of the NetWare server console on a 24-line terminal. Therefore, the first line is not displayed.

You can also start XConsole using the Start/Stop Services option of UNICON.

The following error message may appear in the audit log or on the Product Kernel Message screen when you try to establish a connection through XConsole:

```
XCONSOLE-Error: Fatal IO error (60), Connection timed out,
on: hostname: 0.0(1)
```

If you receive this message, check the version of the LAN driver you are using for your NetWare server. For example, if you are using a Western Digital LAN driver, you must have version 3.00 or later.

Providing Your Display and Screen Number

When you start an XConsole session, you are prompted to enter your display and screen numbers.

The X Window System defines a display as a monitor with its own separate keyboard or mouse. For example, if you have two monitors attached to a single computer, and each monitor has its own separate keyboard or mouse, you have two displays.

You can also have two monitors linked together with only one mouse, as shown in Figure 2-2 (Display 0 Screen 0 and Display 0 Screen 1 are controlled by the same mouse). In this case, you have one display but two screens. Or, one display can have more than one screen, such as a monitor that is switchable between monochrome and color (see Figure 2-3).

Each workstation display is numbered consecutively beginning with zero. Each screen is also numbered consecutively.

Figure 2-2

Two X Window System Displays

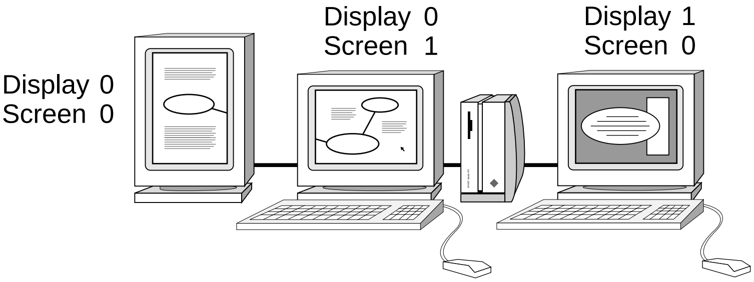
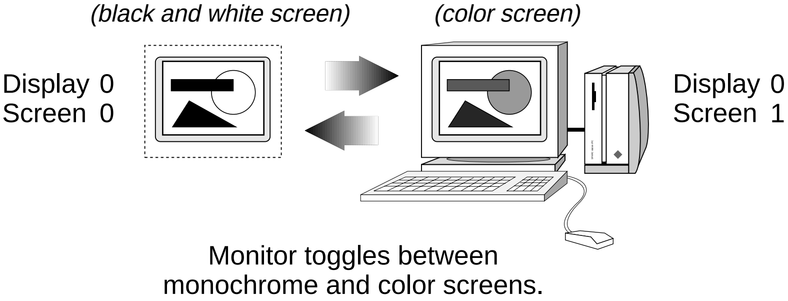


Figure 2-3

One X Window System Display with Two Screens



Starting and Ending an XConsole Session Using X Windows

1. **Start the window manager on your workstation.**

   You can run XConsole without a window manager, if you prefer. The session is displayed in a window, but you will not be able to manipulate the window.

2. **Give the NetWare file server rights to send data to the workstation display by typing**

   xhost *servername* <Enter>

   The xhost command adds the NetWare file server *servername* to the workstation's X-server access control list. To allow all hosts to write to the display, type a plus sign (+) in place of *servername* .

Note

Before you disable access control and allow all hosts, evaluate the potential security risk.

3. **Connect to the NetWare server running XConsole by typing**

   telnet *servername* <Enter>

   Depending on your terminal type, there may be several terminal services available. If there is more than one available service, telnet prompts you to choose the service type.

   For example, if your terminal type is set to VT100/220, there are two services available and the following prompt appears:

   ```
   [Select one of the following Telnet Services]
   1- X11 Console Session to the NetWare Server
   2- VT220 Console Session to the NetWare Server
   ```

   ```
   Help is Ctrl-? or Ctrl-w
   Exit is Ctrl-x
   ```

4. **If there is more than one terminal service available, TELNET prompts you to choose the appropriate service. Enter the appropriate number to choose an X Window terminal type.**

   The TELNET connection prompts you for a password.

5. **Enter either the remote console password or the password for the server's SUPERVISOR account.**

   When you enter the correct password, the following prompt appears:

   ```
   Do you want the X-session displayed on
   a display other than the default
   [localhost IP address :0.0] (y/n)? [n]
   ```

6. **Respond to the display prompt.**

   6a. If you want to display the session on the default display, accept the default response (No) by pressing <Enter> **.**

   The process continues with the response to Step 8 .

   6b. If your computer has more than one display or screen, and you want to display the session on a display other then the default, enter Y for Yes.

   NetWare prompts for the host name:

```
Enter the name of the host where XConsole
should start the X-session [host :0.0]:
```

7. **Press <Enter> to accept the default (local) host or type the appropriate host name or IP address and press <Enter> .**

   NetWare prompts for your display and screen number:

   ```
   Enter display number [0]:
   Enter screen number [0]:
   ```

8. **Enter the appropriate display and screen number.**

   A window displaying the server console opens on your display, and the following message is displayed before the TELNET connection closes:

   ```
   XConsole session created successfully on host :x .x
   ```

9. **Activate the window and interact with the console from your keyboard as if you were at the server's console.**

10. **To open additional windows, repeat Step 3 through Step 8.**

11. **End the XConsole session as required by your window manager.**

    Some window managers allow you to close the window to end the console session. If your window manager does not allow you to close the window, choose the window and press <Ctrl–X> to end the session.

Troubleshooting an X Session

If an X server cannot establish a session with XConsole, the following error message may appear on your screen:

```
Cannot open X display, possible cause:
1. NetWare host is not authorized to use this X display, or
2. X server is not installed properly, or
3. This is not an X display
```

If you receive this message, make sure your workstation is running a true X terminal remote client. Then repeat Step 3 on page 249 .

Starting and Ending a VT100/VT220 XConsole Session

XConsole provides remote console operations from VT100/VT220 terminals and terminals that provide exact VT100/VT220 terminal emulation.

To use VT100 /VT220 emulation on a Sun Workstation, run the xterm program instead of running the command or shell tools.

Use this procedure to start and end a VT100/VT200 XConsole session:

1. **Connect to the NetWare server running XConsole by typing**

   telnet *servername* <Enter>

   Depending on your terminal type, there may be several terminal services available. If there is more than one available service, telnet prompts you to choose the service type.

   For example, if your terminal type is set to VT100/220, there are two services available and the following prompt appears:

   ```
   [Select one of the following Telnet Services]
   1- X11 Console Session to the NetWare Server
   2- VT220 Console Session to the NetWare Server
   ________________________________
   Help is Ctrl-? or Ctrl-w
   Exit is Ctrl-x
   ________________________________
   ```

2. **If there is more than one terminal service available, TELNET prompts you to choose the appropriate service. Enter the appropriate number to choose a VT100/220 terminal type.**

3. **When prompted, enter the remote console password or the password for the server's SUPERVISOR account.**

   After you enter the correct password, you can interact with the console using your keyboard as if you were at the server's console.

4. **To end the session, press** <Ctrl–X> **.**

Note

When using VT100/VT220 emulation mode, you may need to use the control key functions listed in Table 2-1 .

Using Keyboard Functions

Certain keys can be used in an X Window or VT100/220 session to control the screen. For example, you can apply the keypad – (minus) key to display the previous screen. This section provides instructions for substituting other keys and for modifying your keyboard mapping in case your keyboard does not have the appropriate function keys.

Using the Control Key for Special Key Substitution

NetWare maps keyboard functions to the IBM PC Enhanced 101-key keyboard. However, XConsole supports an additional set of key functions based on use of the left <Ctrl> key.

Table 2-1 shows the functions mapped to various <Ctrl> key combinations. The key combinations are not case sensitive.

Table 2-1 **Control Key Functions Supported by XConsole**

Key Combination	Specialty key or function
<Ctrl–?>	Print XConsole control key help page for X-Windows or VT100/VT220 mode
<Ctrl–w>	Print XConsole control key help page for VT100/ VT220 mode
<Ctrl–a>	<Alt>
<Ctrl–a> <1>	<F1>
<Ctrl–a> <2>	<F2>
<Ctrl–a> <3>	<F3>
<Ctrl–a> <4>	<F4>
<Ctrl–a> <5>	<F5>
<Ctrl–a> <6>	<F6>
<Ctrl–a> <7>	<F7>
<Ctrl–a> <8>	<F8>
<Ctrl–a> <9>	<F9>
<Ctrl–a> <a>	<F10>
<Ctrl–a> <b>	<F11>
<Ctrl–a> <c>	<F12>
<Ctrl–a> <d>	<F13>
<Ctrl–a> <e>	<F14>
<Ctrl–a> <f>	<F15>
<Ctrl–b>	<Begin> (<Home>)
<Ctrl–d>	<Down-arrow>
<Ctrl–e>	<End>
<Ctrl–f>	Switch screen forward

Key Combination	Specialty key or function
<Ctrl–g>	<Delete>
<Ctrl–h>	<Backspace>
<Ctrl–l>	<Left-arrow>
<Ctrl–n>	<PageDown> (Next)
<Ctrl–o>	<Insert>
<Ctrl–p>	<PageUp> (Prior)
<Ctrl–r>	<Right-arrow>
<Ctrl–u>	<Up-arrow>
<Ctrl–x>	<Exit> (Quit session)
<Ctrl–z>	Select a screen
<Ctrl–[>	<Esc>
plus (+ on numeric keypad)	Next screen
minus (– on numeric keypad)	Previous screen

Using the Modifier Keys to Substitute for Function Keys

XConsole recognizes the following modifier keys:

- Left <Shift>
- Left <Ctrl>
- Left <Alt>
- Right <Shift>
- Right <Ctrl>
- Right <Alt>

Left <Shift> , Left <Ctrl> , and Right <Shift> are X Window System defaults and are preset in the keyboard modifier map. You can add the other three keys

(Left <Alt> , Right <Ctrl> , and Right <Alt>) to the modifier map using the X utility *xmodmap* .

Adding the Modifier Keys

Add Right <Ctrl> to xmodmap as modifiername Control. Add Left <Alt> or Right <Alt> as modifiernames Mod 1, Mod 2, Mod 3, Mod 4, or Mod 5.

For example, to add Left <Alt> as Mod 1, type

xmodmap -e add Mod1 = Alt_L <Enter>

Refer to your X Window System documentation for additional information.

Using the Modifier Keys

You can use <Alt> in combination with hexadecimal equivalent keys 1 through 9 and a through f to substitute for function keys. Use <Alt > as modified by xmodmap (as described above) or use the substitute Alt key (<Ctrl–a> combination). Table 2-2 shows the possible combinations. The combinations are not case sensitive.

To use the <Ctrl–a> key combination, press and hold <Ctrl> , press <a> , release both keys, and then press the hexadecimal equivalent key. To use the <Alt> combinations, press <Alt> and the hexadecimal equivalent key simultaneously.

Table 2-2Alt Key Combinations Supported by XConsole

Function key	**Ctrl Key (VT100/220, X-terminal)**	**Modified Alt Key (X terminal only)**
<F1>	<Ctrl–a><1>	<Alt–1>
<F2>	<Ctrl–a><2>	<Alt–2>
<F3>	<Ctrl–a><3>	<Alt–3>
<F4>	<Ctrl–a><4>	<Alt–4>
<F5>	<Ctrl–a><5>	<Alt–5>
<F6>	<Ctrl–a><6>	<Alt–6>

Function key	Ctrl Key (VT100/220, X-terminal)	Modified Alt Key (X terminal only)
<F7>	<Ctrl–a><7>	<Alt–7>
<F8>	<Ctrl–a><8>	<Alt–8>
<F9>	<Ctrl–a><9>	<Alt–9>
<F10>	<Ctrl–a><a>	<Alt–a>
<F11>	<Ctrl–a><b>	<Alt–b>
<F12>	<Ctrl–a><c>	<Alt–c>
<F13>	<Ctrl–a><d>	<Alt–d>
<F14>	<Ctrl–a><e>	<Alt–e>
<F15>	<Ctrl–a><f>	<Alt–f>

Appendix

C *Managing Host Information*

This appendix contains information about host management that is not essential to setting up and configuring NetWare/IP™ .

Note

If you are using the host management option to manage another product, refer to that product's documentation for specifics about managing host information for that product.

This appendix discusses the following topics:

- Creating host entries on the NetWare/IP server
- Displaying the host status window
- Using the host management screens
- Creating and deleting host entries on the NetWare/IP server
- Displaying or modifying host information

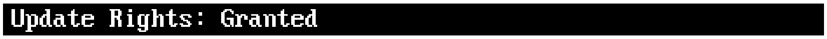
Creating Host Entries on the NetWare/IP Server

Host information consists of a hostname and an IP address which NetWare/IP uses in conjunction with DNS to locate machines on the network. You can enter new host information or modify current host information using the UNICON utility. The NetWare/IP host database must contain an entry for each DSS server in the NetWare/IP network.

Displaying the Update Rights Status Window

You use the Update Rights Status window to view whether you have the right to update the current host information.

The UNICON utility displays the Update Rights Status window at the bottom of the screen during host administration.



Update Rights: Granted

From UNICON’s Main Menu, choose the following to display the Update Rights Status window:

–>**Manage Global Objects**
–>**Manage Hosts**
–>**Hosts**

The status window contains the following field:

Update Rights —this field reads either Granted or Denied. If this field reads Granted, then you have the right to update host information. If this field reads Denied, you do not have the right to update host information.

You could be denied the right to update host information for the following reasons:

- You do not have supervisory rights on this server.
- Your NetWare/IP server is set up to use the DNS database on another server to store host information. In this case, all host administration must be performed on the master DNS server.
- You did not set up DNS as described in Chapter 7, “Setting Up DNS Support,” on page 89

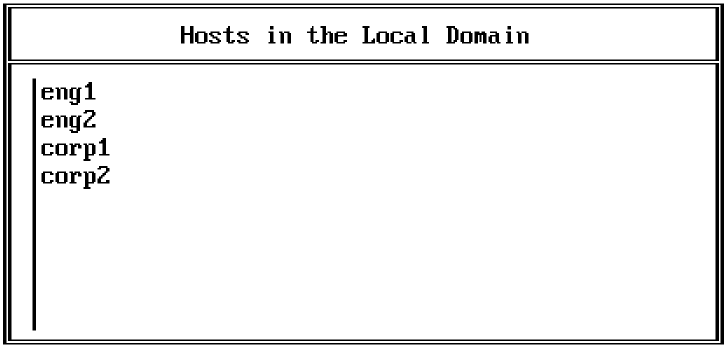
Using the Host Management Screens

You use two screens to manage host information: the Hosts in the Local Domain list and the Host Information form. These screens are shown and described in the following sections.

Hosts in the Local Domain List

The Hosts in the Local Domain list provides a list of the hosts in the DNS database. You begin all your host configuration procedures from this list.

Figure 3-1
Hosts in the Local Domain List



```
Hosts in the Local Domain

eng1
eng2
corp1
corp2
```

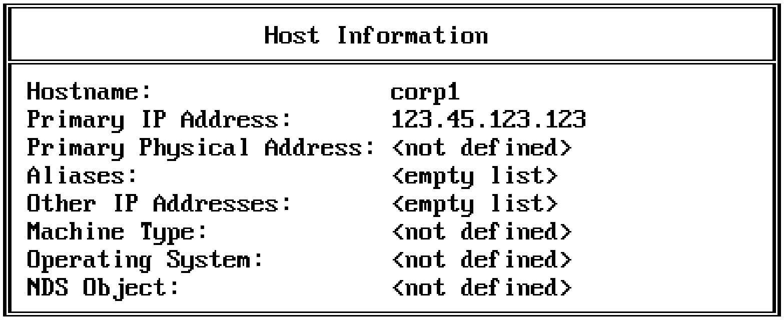
From UNICON’s Main Menu, choose the following to display the Hosts in the Local Domain list:

–>**Manage Global Objects**
  –>**Manage Hosts**
    –>**Hosts**

Host Information Form

The Host Information form displays information about a specific host. Use this form to add or modify a host record.

Figure 3-2
Host Information Form



```
Host Information

Hostname:                  corp1
Primary IP Address:        123.45.123.123
Primary Physical Address:  <not defined>
Aliases:                   <empty list>
Other IP Addresses:        <empty list>
Machine Type:              <not defined>
Operating System:          <not defined>
NDS Object:                <not defined>
```

From UNICON’s Hosts in the Local Domain list, choose a specific host entry, and press <Enter> to display the Host Information form.

This form contains the following fields:

Hostname —the name of the host. The hostname can contain up to 46 characters.

Primary IP Address —the IP address that identifies the host in an IP network. The information in this field must be in standard IP address format (for example, 123.26.9.31).

Primary Physical Address —the unique address assigned to each machine by the vendor who produces the machine. This address is a 6-byte hexadecimal number, such as 0x08 0x00 0x14 0x57 0x69 0x69.

Aliases —other names for the host. If the host has any aliases, these names are listed in the /etc/hosts file or in the DNS database. Choose this field to display a list of known aliases for a specified host. You can add and delete known aliases using <Insert> and <Delete> .

Other IP Addresses —other Internet addresses. Choose this field to display a list of alternate IP addresses for a specified host. You can add and delete other IP addresses using <Insert> and <Delete> .

Machine Type —the type of machine (for example, Sun workstation).

Operating System —the operating system running on the machine (for example, SunOS*).

NDS Object —the name of the Novell Directory Services™ (NDS) object mapped to this host entry. The UNICON utility allows you to map a host entry to a corresponding NDS object so that you can manage all host entries using the NETADMIN or NWADMIN utility.

Adding a Host

Host information consists of a hostname and an IP address that the server uses to locate other machines on the network.

Use the following procedure to add a host entry:

1. **From UNICON’s Main Menu, choose the following:**

–>**Manage Global Objects**
  –>**Manage Hosts**
    –>**Hosts**

The utility displays the list described in "Hosts in the Local Domain List" on page 258

2. **Press** <Insert> **.**

3. **When prompted, enter the new host's name.**

4. **When prompted, enter the host's IP address.**

5. **Complete the Host Information form with the appropriate information and press** <Esc> **.**

6. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Deleting a Host

Warning

The local hostname is the name assigned to the NetWare/IP server. This name is used by DNS and therefore you should not delete or modify the local host entry.

Use the following procedure to delete a host entry:

1. **From UNICON's Main Menu, choose the following:**

–>**Manage Global Objects**
  –>**Manage Hosts**
    –>**Hosts**

The utility displays the list described in "Hosts in the Local Domain List" on page 258

2. **Highlight the host to be removed and press** <Delete> **.**

3. **When prompted, choose Yes to delete the host.**

4. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Displaying and Modifying Host Information

Warning

The local hostname is the name assigned to the NetWare/IP server. This name is used by DNS and therefore you should not delete or modify the local host entry.

Use the following procedure to display or modify host information:

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Global Objects**
   –>**Manage Hosts**

   The utility displays the list described in "Hosts in the Local Domain List" on page 258

2. **Highlight a specific host on the list and press the** <Enter> **key.**

   The utility displays the form described in "Host Information Form" on page 259

3. **Choose and modify the appropriate fields.**

   You can add or delete an alias or other IP address by choosing the corresponding field, and then using the <Insert> or <Delete> key.

4. **Press the** <Esc> **key to exit the Host Information form.**

5. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Appendix

D *Managing the Server Profile*

The Server Profile provides a way to modify global parameters, including pointing to an existing DNS master server.

This appendix describes how to manage server profile information and global parameter settings. This form is only for viewing. Those field entries that can be modified can be changed from the Server Profile Configuration form, which is a subset of the Server Profile form. Changes to the configuration form appear in the Server Profile form.

Note

If you are using the Server Profile option to manage another product, refer to that product's documentation for specifics about managing host information for that product.

The following topics are discussed in this appendix:

- Configuring the Server Profile
- Modifying the synchronization interval
- Designating a new NetWare® master DNS server

Using the Server Profile Screens

Display and manage server information and global parameters using the following screens:

- Server Profile form
- Server Profile Configuration form

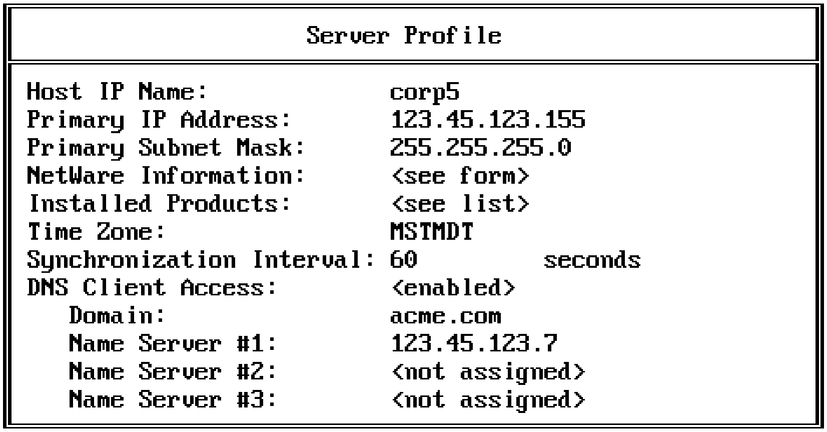
These screens are shown and described in the following sections.

If you need information about a specific field when accessing an online form using the UNICON utility, press <F1>

Server Profile Form

Use the Server Profile form to display global information about the server. A description is given for all the fields.

Figure 4-1
Server Profile Form



```
                      Server Profile

Host IP Name:             corp5
Primary IP Address:       123.45.123.155
Primary Subnet Mask:      255.255.255.0
NetWare Information:      <see form>
Installed Products:       <see list>
Time Zone:                MSTMDT
Synchronization Interval: 60         seconds
DNS Client Access:        <enabled>
   Domain:                acme.com
   Name Server #1:        123.45.123.7
   Name Server #2:        <not assigned>
   Name Server #3:        <not assigned>
```

From UNICON’s Main Menu, choose the following to display the Server Profile form:

–>**View Server Profile**

The Server Profile form contains the following fields:

Host IP Name —the IP name of the NetWare host. This field is display only.

Primary IP Address —the IP address of the NetWare Server. This field is display only.

Primary Subnet Mask —the subnet mask which, when added to the IP address, provides the IP network number. This field is display only.

NetWare Information —form displays the following information:

- **Operating System Version** —the operating system of the specified host. This field is display only.

- **Current NDS Context** —the context or logical position of the server within the Directory tree.

- **Current NDS Tree** —the current Directory tree

Installed Products —list identifies all NetWare installed products by name, version, stratification, and serial number.

Time Zone —the world time reference for your area. The time zone is used to set time synchronization. The correct time is important for time stamps, such as file modification time. The time zone reference is set during installation of NetWare.

Synchronization Interval —the interval (in seconds) after which the NetWare server checks the following files in the ETC directory for changes: NFSUSERS, NFSGROUP, and NWPARAMS. When a change is detected, the file is reread into memory. You can modify this field by typing a new value. Valid parameter values are integers from 1 to 1000. The default value is 60 seconds.

DNS Client Access —this field allows you to enable or disable DNS access. The fields that follow configure access to DNS services.

Note

Do NOT disable DNS access at any time.

(DNS) Domain —this field displays the DNS Domain name entered during installation. You can change the DNS Domain by typing a new Domain name. When you exit the Server Profile form, the utility checks to see that you have entered a valid DNS domain name. If you have not, the utility provides you with the option of returning to the Server Profile form to either change the DNS domain or to disable DNS access.

(DNS) Name Server #1 —this field displays the primary DNS server you entered during installation. The primary server serves as the primary DNS host database. You can change the primary server by typing a new DNS server name or IP address.

When you exit the Server Profile form, the utility checks to see that you have entered at least one (primary) valid DNS server. If you have not, the utility provides you with the option of returning to the Server Profile form to either change the DNS server or to disable DNS access.

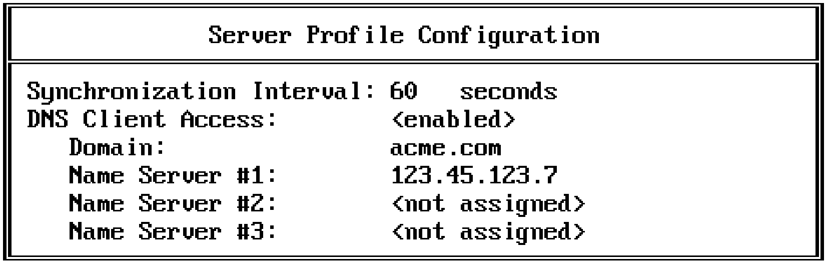
(DNS) Name Server #2 —the secondary DNS server provides an additional host database if your host request cannot be located in your primary server or if your primary server is down. You do not need to specify a secondary server if all your host entries are available through your primary server. You can enter or modify the secondary server by typing a new DNS server name or IP address.

(DNS) Name Server #3 —the tertiary DNS server provides an additional host database if your host request cannot be located in your primary or secondary server or if both servers are down. You do not need to specify a tertiary DNS server if all your host entries are available through your primary and secondary servers. You can enter or modify the tertiary server by typing a new DNS server name or IP address.

Server Profile Configuration Form

Use the Server Profile Configuration form to change configurable global parameters.

Figure 4-2
Server Profile Configuration Form



```
                Server Profile Configuration

 Synchronization Interval: 60   seconds
 DNS Client Access:        <enabled>
    Domain:                acme.com
    Name Server #1:        123.45.123.7
    Name Server #2:        <not assigned>
    Name Server #3:        <not assigned>
```

From UNICON's Main Menu, choose the following to display the Server Profile Configuration form:

–>**Manage Global Objects**
–>**Configure Server Profile**

The Server Profile Configuration form includes a subset of the fields on the Server Profile form containing only those fields that can be changed. The previous section provides a description of these fields as part of the overall description of fields in the Server Profile form.

The next section describes how to modify the synchronization interval.

Modifying the Synchronization Interval

Use this procedure to change the synchronization interval. For a description of this parameter, see “Server Profile Form” on page 264

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Global Objects**
   –>**Configure Server Profile**

   The utility displays the Server Profile Configuration form.

2. **On the Server Profile Configuration form, choose the Synchronization Interval field and enter a new interval.**

3. **Press** `<Esc>` **as needed to return to UNICON's Main Menu.**

4. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
   –>**Edit File**

5. **Enter SYS:ETC\TIMEZN at the file name prompt.**

6. **Add an entry to the end of the file in the following format:**

   ```
   +8     00    Pacific Standard Time
   ```

   where the first entry is the number of hours away from Greenwich Mean time (time zones in the western hemisphere have positive (+) offsets, while time zones in the Eastern hemisphere have negative (–) offsets), the second is the number of minutes away from Greenwich Mean time, and the third is the name of the time zone.

7. **Press** `<Esc>` **to exit the file.**

8. **When prompted, choose Yes to save the changes and exit the screen.**

9. **To return to UNICON's Main Menu, press** `<Esc>` **as needed.**

   You can now go view the new time zone in the list of available time zones on the Server Profile form.

Designating a New Master DNS Server

If you create an environment that has more than one NetWare/IP™ server, you must configure the NetWare/IP servers and DSS servers to use the existing master DNS server. You can configure your NetWare/IP or DSS server to use an existing master DNS database by modifying the server profile as described in the following procedure.

Use the following procedure to choose an existing DNS server:

1. **From UNICON's Main Menu, choose the following:**

   –>**Manage Global Objects**
   –>**Configure Server Profile**

   The utility displays the form described in "Server Profile Configuration Form" on page 266

2. **Choose the DNS Domain field.**

3. **If the default DNS domain name is valid for your new DNS server, press** <Enter> **. Otherwise if the name is not valid, enter the new DNS domain name, and then press** <Enter> **.**

   The cursor moves to the DNS Server field. If the utility can determine the address of the new domain's name server, it automatically displays it in the DNS Server field. If the utility displays the new address in the field, skip to Step 5. Otherwise, to enter the IP address for the new server, continue with Step 4.

4. **Type the IP address of the new master DNS and then press** <Enter> **.**

5. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Appendix

E Using File Functions

This appendix contains information about using the UNICON file functions that are not essential to setting up and configuring NetWare/IP™ .

Note If you are using the file function options to manage another product, refer to that product's documentation for specifics about using file functions for that product.

This appendix includes the following sections:

- Copying Files Using FTP
- Editing Files
- Backing Up and Restoring files

Copying Files Using FTP

You can use the Copy Files Using FTP option to transfer files to and from computers that support FTP server functions. The remote server you log in to must be running an FTP (File Transfer Protocol) server program (know as a *daemon* on some systems) for you to use the file copy function.

Using the FTP Management Screens

Copy files with FTP using the following screens:

- Status inset
- FTP Server Login form
- FTP Server list
- Get File form

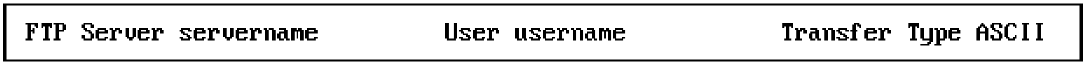
- Put File form

If you need information about a specific field when accessing an online form using the UNICON utility, press <F1> .

Status Inset

After you connect to a specific FTP server, a status inset like the following appears at the bottom of the UNICON screen:

Figure 5-1
Status Inset



```
FTP Server servername        User username          Transfer Type ASCII
```

The FTP Status Inset contains the following fields:

FTP Server —the name of the host or the IP address of the host you logged in to.

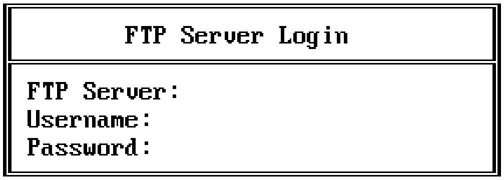
User —the user name that you used when you logged in.

Transfer Type —the type of file transfer (ASCII or Binary) that is currently specified.

FTP Server Login Form

Use the FTP Server Login form to log in for the first time and to log in to additional remote servers.

Figure 5-2
Server Login Form



```
FTP Server Login

FTP Server:
Username:
Password:
```

From UNICON's Main Menu, choose the following to display the FTP Server Login form:

–>**Perform File Operations**
–>**Copy Files Using FTP**

The first time you choose the Copy Files Using FTP option, the utility displays the FTP Server Login form. The next time you choose the Copy Files Using FTP option, the utility displays a list of active FTP sessions. Each time you press <Insert> to log in to a new server, the utility displays the FTP Server Login form.

The FTP Server Login form contains the following fields:

FTP Server —the name of the remote host, which must be running the FTP server (known as a daemon on some systems).

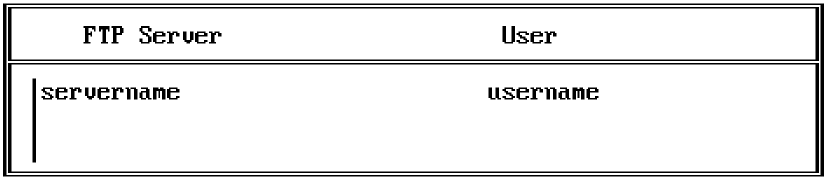
Username —your remote host username.

Password —your password (if necessary).

FTP Server List

The FTP Server list displays the names or IP addresses of the FTP hosts that have been logged in to and the names of the logged-in users.

Figure 5-3
FTP Server List



FTP Server	User
servername	username

From UNICON's Main Menu, choose the following to display the FTP Server list:

–>**Perform File Operations**
–>**Copy Files Using FTP**

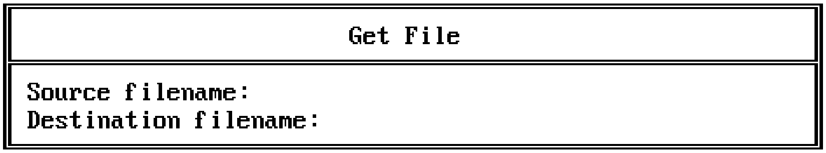
If you are logged in to one or more FTP servers, the utility displays the FTP Server list.

Get File Form

Use the Get File form to transfer a file from a remote server.

Figure 5-4

Get File Form



```
                    Get File
Source filename:
Destination filename:
```

From UNICON’s Main Menu, choose the following to display the Get File form:

–>**Perform File Operations**
  –>**Copy Files Using FTP**

After you choose a session from the FTP Server list or log in to an FTP server, the utility displays the File Operations menu. Choose the following from the File Operations menu:

–>**Get File**

The Get File form contains the following fields:

Source filename —the full path of the file you want to copy from the remote host.

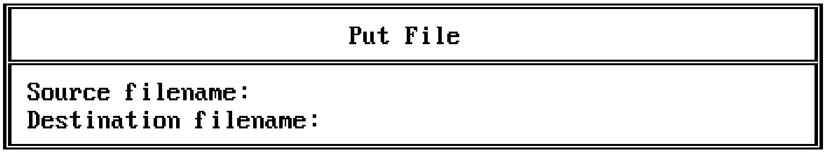
Destination filename —the full path of the file destination on the NetWare server.

Put File Form

Use the Put File form to transfer a file from your server to a remote server.

Figure 5-5

Put File Form



```
                    Put File
Source filename:
Destination filename:
```

From UNICON's Main Menu, choose the following to display the Put File form:

–>**Perform File Operations**
–>**Copy Files Using FTP**

After you choose a session from the FTP Server list or log in to an FTP server, the utility displays the File Operations menu. Choose the following from the File Operations menu:

–>**Put File**

The Put File form contains the following fields:

Source filename —the full path of the file you want to copy from the NetWare server to the remote host.

Destination filename —the full path of the file destination on the remote server.

Entering Directory Paths and Filenames

Enter path and filename information in the correct syntax known by the remote FTP server. For example, if you are logged in to a UNIX® host, you must enter pathnames in UNIX format (for example, /sys/etc/hosts).

If you enter a destination path for a NetWare® server, use NetWare format (for example, SYS:ETC/HOSTS).

Connecting to One or More FTP Servers

Use this procedure to connect to FTP Servers:

1. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
   –>**Copy Files Using FTP**

   The first time you use the Copy Files Using FTP option, the utility displays the FTP Server Login form described in "FTP Server Login Form" on page 270 If you are logged in to an FTP server, the utility displays the FTP Server list described in "FTP Server List" on page 271

2. **If the FTP Server Login form appears, enter the remote server name, username, and password (if necessary) and press** <Enter> **. If**

the FTP Server list appears, either choose an FTP server from the list or use <Insert> **to log in to an additional server.**

The utility lists the logged-in FTP servers in the FTP Server list. Upon logging in to an FTP server, the utility displays the FTP Operations menu. The status window at the bottom of the screen lists the FTP server you are currently logged in to, your username, and the FTP file transfer type.

Listing Remote Directories

Use the following procedure to list directories that are on a remote host:

1. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
   –>**Copy Files Using FTP**

   After you choose a session from the FTP Server list or log in to an FTP server, the utility displays the File Operations menu.

2. **From the File Operations menu, choose the following:**

   –>**List Directory**

3. **When prompted, enter the path name of the directory that you want listed.**

4. **Press** <Esc> **to exit the list.**

5. **Choose another FTP operation from the menu or press** <Esc> **as needed to return to UNICON's Main Menu.**

Selecting the Transfer Type

Use the following procedure to change the transfer type to ASCII or binary:

1. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
   –>**Copy Files Using FTP**

   After you choose a session from the FTP Server list or log in to an FTP server, the utility displays the File Operations menu.

2. **From the File Operations menu, choose the following:**

   –>**Select Transfer Type**

3. **Choose the appropriate transfer type (ASCII or Binary).**

4. **Press** <Esc> **to exit the Select Transfer Type screen.**

5. **Choose another FTP operation from the menu or press** <Esc> **as needed to return to UNICON's Main Menu.**

Copying a File from a Remote Host

Use the following procedure to copy a file from a remote host:

1. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
     –>**Copy Files Using FTP**

   After you choose a session from the FTP Server list or log in to an FTP server, the utility displays the File Operations menu.

2. **From the File Operations menu, choose the following:**

   –>**Get File**

3. **Complete the Get File form and press <Enter>.**

   If the remote file does not exist, the utility displays an error message. Otherwise, the utility transfers the file and redisplays the Get File form.

4. **Repeat Step 3 for each file that you want to transfer.**

5. **Press** <Esc> **to exit the form.**

6. **Choose another FTP operation from the menu or press** <Esc> **as needed to return to UNICON's Main Menu.**

Copying a File to a Remote Host

Use the following procedure to copy a file to a remote host:

1. **From UNICON's Main Menu, choose the following:**

–>**Perform File Operations**
–>**Copy Files Using FTP**

After you choose a session from the FTP Server list or log in to an FTP server, the utility displays the File Operations menu.

2. **From the File Operations menu, choose the following:**

   –>**Put File**

3. **Complete the Put File form and press** <Esc> **.**

   If the local file does not exist, the utility displays an error message. Otherwise, the utility transfers the file and redisplays the FTP Operations menu.

4. **Choose another FTP operation from the menu or press** <Esc> **as needed to return to UNICON's Main Menu.**

Logging Out from an FTP Server

Use the following procedure to log out from an FTP server:

1. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
   –>**Copy Files Using FTP**

   The utility displays the FTP Server list described in "FTP Server List" on page 271

2. **Highlight the FTP Server from which you want to log out and press** <Delete> **.**

3. **Press** <Esc> **to return to the File Operations menu.**

4. **Choose one of the file operations from the menu or press** <Esc> **as needed to return to UNICON's Main Menu.**

Editing Files

The UNICON edit function enables you to edit files located on the NetWare server. You can use this utility to edit files containing up to 64,000 bytes.

1. **From UNICON's Main Menu, choose the following:**

   –>**Perform File Operations**
   –>**Edit File**

2. **When prompted, enter the pathname of the file you want to edit.**

   If the file does not exist, the utility asks if you want to create the file. If you answer Yes or if the file already exists, the file appears in an editing screen.

3. **Edit the file as necessary.**

4. **Press** <Esc> **to end the edit session.**

5. **When prompted, choose Yes to save any changes.**

6. **To return to UNICON's Main Menu, press** <Esc> **as needed.**

Backing Up and Restoring Files Using NetWare Utilities

This section explains how to back up and restore files using NetWare utilities.

You can use the following NetWare utilities to ensure that data is not lost or corrupted:

- SBACKUP utility
- FILER utility salvage option

For specific information about these utilities, refer to the NetWare 4 *Utilities Reference* .

Using the SBACKUP Utility

Use the SBACKUP utility to back up NetWare files that support multiple name spaces, such as NFS and Apple Macintosh files.

Using the FILER Utility Salvage Deleted Files Option

Use the FILER salvage option to recover files that have been erased. When users erase a file from NetWare, NetWare keeps a backup copy of the file hidden on the server. Backup copies are not removed until the server needs additional disk space or they are purged by the owner or the NetWare supervisor. You can use the salvage option to restore backup files that have not yet been purged.

Appendix

F *TCP/IP and SNMP*

This appendix describes the Novell® TCP/IP Transport for DOS, which is included with the NetWare/IP™ product software.

About the TCP/IP Transport Software

The following programs provide the TCP/IP transport for NetWare/IP:

- TCP/IP Transport driver: TCPIP.EXE
- RFC-1001/1002 compliant NetBIOS driver: RFCNBIOS.EXE
- Reverse ARP server: RARPD.EXE
- SNMP MIB-2 agent program (TSR): SNMP.EXE
- MS Windows Sockets API support: WINSOCK.DLL, WLIBSOCK.DLL, and NOVASYNC.EXE

The Novell TCP/IP Transport for DOS provides the following standard protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- BOOTP and DHCP

- Simple Network Management Protocol (SNMP)
- Management Information Base (MIB)
- NetBIOS Service Interface using the RFC-1001/1002 compliant B-node (broadcast) type of the NetBIOS Protocol (RFC NetBIOS)

Note A workstation running NetBIOS software must also be running the TCP/IP Transport software.

The TCP/IP transport software also includes support for MS Windows Enhanced Mode operation.

Using the TCP/IP Utilities

The TCP/IP transport software includes the following utilities:

- LWPCON, which displays local and remote configuration information, network statistics, and TCP/IP service status
- PING, which checks for network connectivity to a specific host

Using the LWPCON Utility

The LAN WorkPlace Console (LWPCON) utility is a DOS menu-based application that lets you display TCP/IP configuration, statistical, and service information for your workstation and remote hosts on your network. With LWPCON you can

- Check the configuration parameters for your workstation and remote hosts on your network
- Forcibly close TCP connections
- Check whether remote hosts are available
- Check the network route used to connect you to a remote host
- List the services available on a remote host
- Determine which remote host services are currently available

- Determine what remote host information is available from your network's DNS name servers

- Set an entry in the routing table

In addition to these capabilities, LWPCON provides several statistical displays that network administrators can use to monitor network traffic and isolate problems.

Starting LWPCON

1. **To start LWPCON from the DOS prompt, type the following command:**

   lwpcon <Enter>

The utility displays the Available Options menu. You begin all LWPCON activities from this menu.

Checking Workstation and Remote Host Configuration

Use the following procedure to check the TCP/IP configuration settings for your workstation or for a remote host on your network:

1. **From LWPCON's Available Options menu, choose Local Workstation or Remote Host.**

   If you choose Local Workstation, the utility displays the Local Workstation Options menu.

   If you choose Remote Host, the utility prompts for the remote hostname.

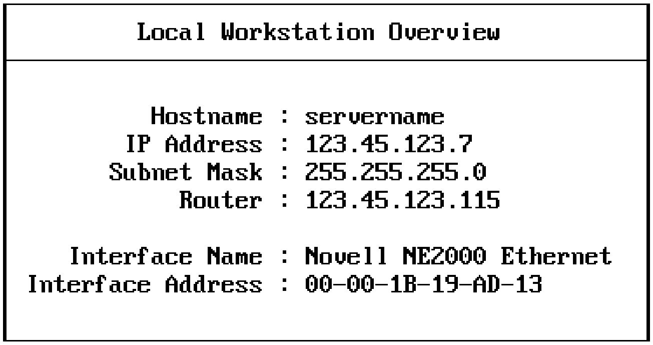
2. **If prompted for a hostname, enter the hostname or IP address (in dotted notation) of the host for which you want to view configuration information.**

   The remote host must be running an SNMP agent program. For example, a remote server must be running a program such as TCPIP.NLM, which automatically loads SNMP.NLM. A remote PC workstation must be running programs such as TCPIP.EXE and SNMP.EXE.

   After you enter a valid remote hostname or IP address, the utility displays the Remote Host Options menu.

3. **Choose Overview to display configuration information.**

The utility displays a host overview screen.



```
         Local Workstation Overview

          Hostname : servername
        IP Address : 123.45.123.7
       Subnet Mask : 255.255.255.0
            Router : 123.45.123.115

    Interface Name : Novell NE2000 Ethernet
 Interface Address : 00-00-1B-19-AD-13
```

The host overview screen displays the following TCP/IP configuration information:

- **Hostname** —the fully qualified name of the remote host or local workstation
- **IP address** —the address configured for this host or workstation
- **Subnet mask** —the subnetwork mask configured for this host or workstation, if your network has subnetworks
- **Router** —the address of the IP router, if your network has one
- **Interface name** —usually displays the name of the device driver providing network connection support
- **Interface address** —the hardware or MAC address of the local workstation or remote host

4. **To return to the Available Options menu, press** `<Esc>` **as needed.**

The other choices on the Available Options menus (Interfaces, Protocols, Tables, and SNMP) provide statistical information that is of interest to the network administrator.

Listing and Closing TCP Connections

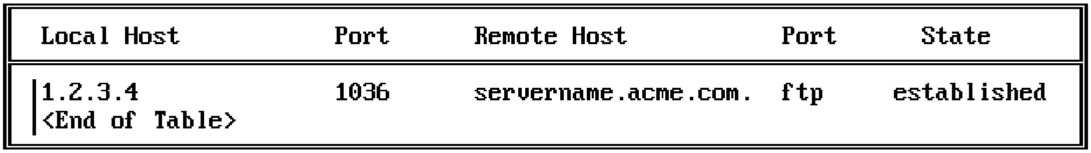
Occasionally a TCP connection might not be closed properly (for example, when a remote connection is severed unexpectedly). This can result in a shortage of TCP resources (sockets) on your workstation.

Use the following procedure to list and close TCP connections:

1. **From LWPCON's Available Options menu, choose the following:**

   –>**Local Workstation**
   –>**Tables**
   –>**TCP Connection Table**

   The utility displays the TCP Connection Table.



```
 Local Host           Port      Remote Host          Port      State

 1.2.3.4              1036      servername.acme.com.  ftp     established
 <End of Table>
```

   For each workstation connection, the utility displays the workstation (Local Host) address and port and the remote host address, port, and status.

2. **Choose the connection you want to close and press** <Delete> **.**

   Use caution in deleting established connections. When you delete a connection that is in use, you lose any unsaved data.

3. **When prompted, press** <Enter> **to close the connection.**

4. **To return to the Available Options menu, press** <Esc> **as needed.**

Determining Remote Host Status

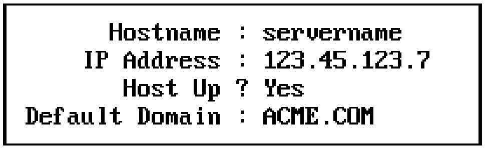
Use the following procedure to determine the status of a remote host:

1. **From LWPCON's Available Options menu, choose the following:**

   –>**Services**

2. **When prompted, enter the name or IP address (in dotted notation) of a host on the network.**

   The utility displays a status table for the remote host. If the remote host is running and available on your network, the value in the Host Up field is Yes.



```
     Hostname : servername
   IP Address : 123.45.123.7
      Host Up ? Yes
Default Domain : ACME.COM
```

3. **To return to the Available Options menu, press <Esc> as needed.**

Checking the Network Route to a Host

If you are having difficulty connecting to a host or the response from the host is slow, you may want to verify the connection between your workstation and the remote host.

Use the following procedure to check the route between your workstation and a remote host:

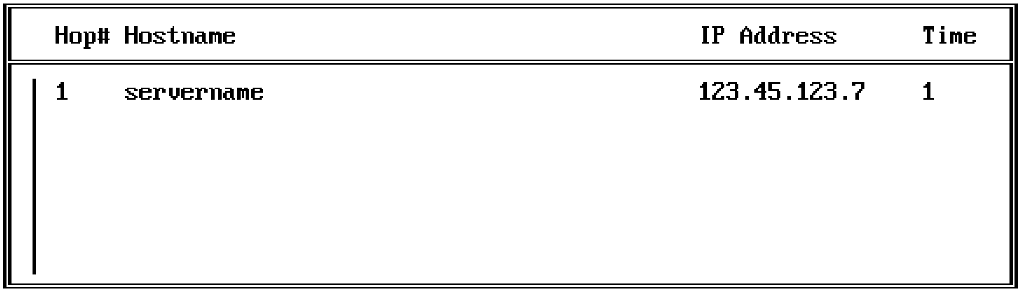
1. **From LWPCON's Available Options menu, choose the following:**

   –>Services

2. **When prompted, enter the name or IP address (in dotted notation) of a host on the network.**

3. **From the Services Options menu, choose Trace Route.**

   The utility displays a route table.



```
Hop# Hostname                                  IP Address      Time
1    servername                                123.45.123.7    1
```

The route table lists the name and IP address of each intermediate host through which your connection is routed, starting with your router (hop 1) and ending with the remote host you specified. The route table also lists the amount of time in milliseconds required to make each intermediate connection. A time of 0 indicates that fewer than 55 milliseconds were required to connect, as is often the case for a LAN connection.

If a host in the route does not respond to LWPCON within its time limit, the table displays the message Not Available. You can use these messages to determine where a problem is occurring in reaching a remote host. For example, if both hop 6 and hop 7 are part of the same network and both are not available, you might suspect that their network is down.

4. **To return to the Available Options menu, press** `<Esc>` **as needed.**

Checking Remote Host Services

Use the following procedure to display information about the availability of remote host services:

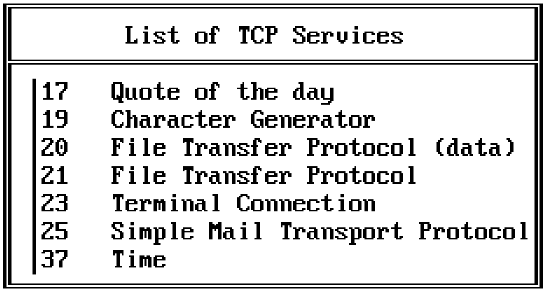
1. **From LWPCON's Available Options menu, choose the following:**

   –>**Services**

2. **When prompted, enter the name or IP address (in dotted notation) of a host on the network.**

3. **From the Services Options menu, choose Check Active TCP Services.**

   The utility displays a list of TCP services.



```
        List of TCP Services

 17   Quote of the day
 19   Character Generator
 20   File Transfer Protocol (data)
 21   File Transfer Protocol
 23   Terminal Connection
 25   Simple Mail Transport Protocol
 37   Time
```

This list includes a service number with each well-known TCP port number. For example, the File Transfer Protocol service, usually service (port) 21, provides services used by FTP.

4. **To check the availability of a service for which you do not know the port number, choose the service you want to check.**

If a service is available, LWPCON replies with the following message:

servicename is active.

If the service is inactive, a problem exists on the remote host. The server program that supports this service might not be running on the remote host. The remote host administrator can check and activate the service.

5. **To check the availability of a service for which you know the port number, choose Other.**

6. **When prompted, enter a TCP port number.**

7. **To return to the Available Options menu, press** <Esc> **as needed.**

Displaying Host Information

Domain Name System (DNS) name servers maintain information about hosts on a network. You can use LWPCON to display information the DNS name server stores for the hosts on your network. Use the following procedure to display DNS information for a remote host:

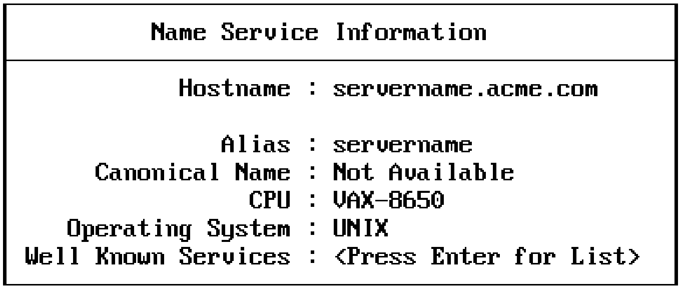
1. **From LWPCON's Available Options menu, choose the following:**

   –>Services

2. **When prompted, enter the name or IP address (in dotted notation) of a host on the network.**

3. **From the Services Options menu, choose Query Name Service.**

   The utility displays the Name Service Information screen, which lists the available DNS information for the remote host.



```
          Name Service Information

            Hostname : servername.acme.com

               Alias : servername
      Canonical Name : Not Available
                 CPU : VAX-8650
    Operating System : UNIX
 Well Known Services : <Press Enter for List>
```

4. **To return to the Available Options menu, press** <Esc> **as needed.**

Using the PING Utility

The PING utility tests a workstation's network connections. This utility sends ICMP echo packets (ICMP ECHO_REQUEST) to the remote host you specify and records the time it takes the host to respond to the packets. The utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram to get an echo response from the specified host or network router.

This utility lets you specify the number of packets that PING sends to the remote host as well as the size of the packets and the time interval between packet transmissions. You can specify one size for all packets or vary the size incrementally. You can also specify that the utility display the IP addresses and hostnames of the IP routers along the path of the packet between your workstation and the destination host.

Command Syntax

PING *hostname [option . . .]*

Command Parameters

Replace *hostname* with the name of the host you want to ping.

Replace *option* with one or more options from the following table.

Option	Description	Default Value
/R[N]	Enables the trace route function so that PING displays the IP addresses and hostnames of the IP routers in the path taken by the ICMP echo packets. Include N to display the IP addresses without displaying the hostnames.	–
/T*n*	Modifies the destination response timeout value. Type the time in seconds.	2
/N*n*	Modifies the number of packets you send to the destination host.	1

Option	Description	Default Value
/P*n*	Modifies the amount of time (seconds) that PING waits before sending a packet to the destination host. PING begins waiting once it receives a response from the destination host for the previous packet. You can type a 0 for a continuous stream of packets.	0
/L*n*	Modifies the fixed size of ICMP echo packets. The minimum size of a packet is 12 bytes; the maximum size is 8192 bytes.	12
/S*n*	Specifies the starting packet size for variable-sized ICMP echo packets. The minimum size of a packet is 12 bytes; the maximum size is 8192 bytes.	12
/I*n*	Modifies the number of bytes that PING uses as an increment between variable-sized ICMP echo packets.	1

Errors

If you type a hostname that PING cannot resolve with DNS or with the host file, PING displays the following message:

```
PING: hostname  could not be resolved
```

If an error occurs in any of the socket functions used by PING, the utility displays the error and exits.

Examples

Some of the options have default values. When you do not specify these options when entering the PING command, the utility uses these default values. For example, when you type the following PING command

PING JUPITER.ACME.COM <Enter>

the utility uses the default options as though you typed the following command:

PING JUPITER.ACME.COM /T2 /N1 /P0 /L12 <Enter>

When you send one packet with the PING utility, the utility displays response statistics for the one packet. For example, after you send a packet to the

JUPITER.ACME.COM host, the utility displays transmission statistics in the following format:

```
Packet: 1 Length: 12  Response: 54 ms.

JUPITER.ACME.COM (1.2.3.4) responded in 54 milliseconds
```

You can use the /N and /P options to send multiple packets to a remote host and specify the amount of time the utility waits between packet transmissions.

For example, the following command sends nine packets to JUPITER.ACME.COM with a pause of five seconds between packet transmissions:

PING JUPITER.ACME.COM /N9 /P5 <Enter>

When you send multiple packets, the utility displays information about the status of each packet, including information about the number of packets you sent and received as well as the minimum, average, and maximum response times for the packets as follows:

```
Packet: 9 Length: 12  Response: 54 ms.

JUPITER.ACME.COM (1.2.3.4) response statistics:

9 packets sent, 9 responses received

Minimum response time: 54 milliseconds

Average response time: 54 milliseconds

Maximum response time: 54 milliseconds
```

You can use the /L option to test your network to see how it performs with a packet of a specific size. For example, you can send a 100-byte packet to host JUPITER.ACME.COM by typing the following command:

PING JUPITER.ACME.COM /L100 <Enter>

You can use the /L and /N options to send multiple packets of a specific size to the remote host. For example, you can send nine 100-byte packets to host JUPITER.ACME.COM by typing the following command:

PING JUPITER.ACME.COM /L100 /N9 <Enter>

You can determine the maximum size of packets transported by your network by varying the size of the packets. You vary the size of the packets using the /N, /S, and /I options together. For example, to send 10 packets, the first containing 100 bytes and each following packet being 10 bytes longer than the previous packet, type the following command:

PING JUPITER.ACME.COM /N10 /S100 /I10 <Enter>

You can use the /R option to trace the route or network path between your workstation and the remote host. For example, the following command traces the route to the JUPITER.ACME.COM host:

PING JUPITER.ACME.COM /R <Enter>

The utility displays the route from the workstation to the specified host as follows:

```
Packet: 1  Length: 12  Response: 109 ms.

JUPITER.ACME.COM (1.2.3.4) responded in 109 milliseconds

HOP  IP Address     Host Name                Time

1    1.2.3.6        ROUTER1.ACME.COM           0

2    1.2.3.7        ROUTER2.ACME.COM           0

3    1.2.3.8        ROUTER3.ACME.COM           0

4    1.2.3.4        JUPITER.ACME.COM         109
```

Setting Up the SNMP Agent

SNMP is a Simple Network Management Protocol (SNMP) agent TSR program. It lets a remote SNMP Management Station monitor the TCP/IP protocol stack running on the workstation. SNMP allows remote and local SNMP clients complete access to the TCP/IP portion of the Management Information Base (MIB). SNMP supports the MIB-II variables.

To use the LWPCON utility to access SNMP, see “Using the LWPCON Utility” on page 280 LWPCON does not require the SNMP agent to be running on the workstation to return local statistics. The SNMP TSR is required if you want remote SNMP client programs to be able to gather statistics from your workstation.

The SNMP protocol is fully described in RFC 1157, *Simple Network Management Protocol (SNMP)* .The MIB-II standard is described in RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II* .

To use the SNMP agent on a workstation, you must first load and bind TCP/IP to the interface it will be using. The typical loading sequence is as follows:

LSL
NE2000 (or appropriate driver)
TCPIP
SNMP

The agent is a terminate and stay resident (TSR) program that can be loaded by typing the following command:

SNMP <Enter>

To remove the agent from memory, type the following command:

SNMP U <Enter>

You configure the SNMP agent by adjusting settings in the NET.CFG file. If the NET.CFG file is not configured for SNMP, it runs with the *MonitorCommunity* variable set to public (all clients can read the MIB values) and *ControlCommunity* set to disabled (client write access to the MIB values is not allowed).

SNMP NET.CFG Summary

There are five SNMP settings under the Protocol SNMP section of the NET.CFG configuration file. Table 6-1 summarizes the valid and default values of these settings.

Table 6-1NET.CFG Settings for SNMP

Parameter	Explanation
SYSCONTACT	This parameter specifies the name of the person who is responsible for this machine. Normally, this will be the name of the person using the machine.
SYSNAME	This parameter specifies the full domain name.
SYSLOCATION	This parameter specifies the physical location of the machine.
MONITORCOMMUNITY	This parameter sets the community name for read-only access. By default, this community is public.
CONTROLCOMMUNITY	This parameter sets the community name for read and write access. By default, this community is disabled.

Community Names

Community names are used to authenticate SNMP request messages received at the agent. The community name in a message requesting a given access type must match the name defined for that access type by one of the SNMP community options.

Community names are arbitrary 32-character text strings. You can use the string noAccess to disable the appropriate community. This name is reserved and is not case sensitive.

SNMP Operations

The SNMP protocol allows four operations:

- Retrieve specific management information
- Retrieve general management information

- Manipulate management information
- Report extraordinary events

The Trap operation has not been implemented in this release.

Authentication

SNMP defines a community as a relationship between an SNMP agent and one or more SNMP managers. At the present, only trivial authentication mechanisms are available with SNMP. This means that the community name is placed, in clear text, in an SNMP message. If the community name corresponds to a community known to the receiving SNMP entity, the sending SNMP entity is considered to be authenticated as a member of that community.

The SNMP agent lets you specify any community names you require. Two different communities are used by the agent. The monitor community is used for read-only access; the control community is used for read-write access. If the community name is not known to the agent, the request from the SNMP manager station is ignored.

By default, the monitor community is set to public and the control community is disabled. To override these default settings, you must edit the NET.CFG file.

MsgAppendix

G *Error Messages*

This appendix lists the error messages you could encounter when using the NetWare/IP™ product.

Error messages are categorized by the module that initiates the message. These modules are arranged alphabetically, and the messages within each module are arranged numerically by error identification number or alphabetically if there is no error identification number.

Following each message is the name of the module, the severity of the problem, an explanation of the cause, and a recommended action for correcting the problem. The severity of the error messages is defined as follows:

- **ERROR** —an essential notice about a critical problem or likely failure.
- **WARNING** —a notice about a potential problem that could lead to failure if no action is taken.
- **INFORMATIONAL** —information about the status of NetWare/IP modules.

For information about managing the error reporting system, see “Configuring Error Reporting” on page 155

DNSAGENT Module

5: <host filename>: Entry on line number <number> cannot be included in the DNS database.

Source: DNSAGENT

Severity: ERROR

Explanation: The specified host file contains an incomplete entry at the indicated line number.

Action: Ensure that the entry for the specified host is correct.

35: <host filename>: Record number <number> is badly formatted.

Source: DNSAGENT

Severity: ERROR

Explanation: The specified host file contains a bad record form at the indicated line number.

Action: Check the host file.

155: Unable to free arguments.

Source: DNSAGENT

Severity: ERROR

Explanation: The NLM fails to free RPC arguments from the stack.

Action: Contact your authorized Novell reseller for assistance.

9005006: Unable to free arguments.

Source: DNSAGENT

Severity: ERROR

Explanation: The NLM fails to free RPC arguments from the stack.

Action: Contact your authorized Novell reseller for assistance.

9005007: <NLM name>: Failed to register with the dispatcher.

Source: DNSAGENT

Severity: ERROR

Explanation: The specified NLM failed to register with the dispatcher.

Action: Contact your authorized Novell reseller for assistance.

DSS Module

Aborting database delta transfer. Error receiving data of len=<n> from Primary DSS.

Source: DSS

Severity: WARNING

Explanation: A secondary DSS server is not receiving information from the primary.

Action: Ensure physical connectivity between DSS servers, and then check the status of the primary DSS server.

Aborting database transfer type=<type> to DSS=<ipaddress>; retval=<n> errno=<number>.

Source: DSS

Severity: WARNING

Explanation: Communication with the specified secondary DSS was aborted due to an error.

Action: Ensure physical connectivity between DSS servers, and then check the status of the secondary DSS server.

Aborting database transfer type=<type> to server=<ipaddress>; retval=<n> errno=<number>.

Source: DSS

Severity: WARNING

Explanation: Communication with a NetWare/IP server, identified by its IP address, was aborted due to an error.

Action: Ensure physical connectivity between the DSS server and the NetWare/IP server. Then check the status of the NetWare/IP server.

Aborting filter transfer. Error receiving data of len=%d from Primary DSS

Source: DSS

Severity: WARNING

Explanation: A secondary DSS server is not receiving information from the primary DSS server.

Action: Ensure physical connectivity between the DSS servers and check the status of the primary DSS server.

Aborting transfer of filters to DSS=%s

Source: DSS

Severity: WARNING

Explanation: Communication with the specified secondary DSS server was aborted due to an error.

Action: Ensure physical connectivity between the DSS servers and check the status of the secondary DSS server.

Cannot accept new TCP connections. Check TCP/IP status.

Source: DSS

Severity: ERROR

Explanation: TCP may be unbound from the network interface card. This error message sets off an alarm at the SNMP management station.

Action: Bind TCP/IP to the network interface card.

Cannot allocate resource tag for Event Notification.

Source: DSS

Severity: ERROR

Explanation: The system cannot provide memory to load DSS.NLM.

Action: Add more RAM or unload other NLMs.

Cannot bind to TCP socket using IP Address <ipaddress>.

Source: DSS

Severity: WARNING

Action: Ensure that the IP address is bound to a network interface card.

Cannot connect to the primary DSS. Database cannot be synchronized.

Source: DSS

Severity: ERROR

Action: Ensure that there is physical connectivity to the primary DSS server.

Cannot open a TCP socket.

Source: DSS

Severity: WARNING

Action: Free up some system resources.

Cannot receive follow-on packet from Primary DSS. Aborting database transfer.

Source: DSS

Severity: ERROR

Explanation: The system was unable to communicate with the DSS server and is aborting the transfer of information.

Action: If you see this message infrequently, no action is required. If you see this message frequently, check the status of the DSS server.

Cannot start a thread to do SOA Updates.

Source: DSS

Severity: ERROR

Explanation: The system was unable to create a new process to maintain the database.

Action: Unload some NLMs to free some resources.

Cannot synchronize database. Need to unload and reload DSS.

Source: DSS

Severity: ERROR

Explanation: A protocol error occurred during database synchronization. This error sets off an alarm at the SNMP management station.

Action: None required.

Configured NetWare/IP domain (<domain name>) is different from the domain name in the SOA file (<domain name>).

Source: DSS

Severity: WARNING

Explanation: The NetWare/IP domain name currently configured for this DSS server is different from the NetWare/IP domain name used the last time this DSS server was loaded.

Action: If this DSS server is a secondary DSS server, it must be able to contact the primary DSS server in order to run. If this is a primary DSS server, no action is required.

<NLM> – Corrupted or missing configuration information.

Source: DSS

Severity: ERROR

Action: Configure the NetWare/IP software and reload the NLM.

CreateBtrvFile: BTRV_CREATE failed. File=<filename>, status=<status code returned by btrieve).

Source: DSS

Severity: ERROR

Explanation: An error occurred when creating a btrieve file. This error probably occurred because there is insufficient disk space on the SYS: volume.

Action: Check the disk space on the SYS: volume.

DSS domain name has changed in file <filename>. DSS must be reloaded for the change to take effect.

Source: DSS

Severity: ERROR

Explanation: DSS cannot operate safely because a basic configuration parameter has changed while DSS was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

DSS Filtering status has changed. Primary DSS server will be dysfunctional till it is reloaded.

Source: DSS

Severity: CRITICAL

Explanation: The SAP filtering status or criteria has changed. To prevent incorrect information from being replicated to the rest of the NetWare/IP network, DSS will be non-functional until it is re-loaded.

Action: Unload and re-load the primary DSS server.

DSS_Malloc: 8K Buf: <buffer pointer> missing signature. Possible memory overwrite.

Source: DSS

Severity: ERROR

Explanation: Another NLM is overwriting the DSS buffers on this server.

Action: Identify the offending NLM.

DSS on server <server name> is going down. May lead to degraded NetWare/IP service.

Source: DSS

Severity: WARNING

Explanation: The DSS NLM has been unloaded. This error message sets off an alarm at the SNMP management station.

Action: Reload the DSS NLM as soon as possible.

DSS will be dysfunctional till it is reloaded.

Source: DSS

Severity: CRITICAL

Explanation: Some important NetWare/IP parameters have changed or some critical problem has been detected.

Action: Unload and reload DSS to clear this problem.

Error in primary DSS’s database transfer RIP packet (%x).

Source: DSS

Severity: WARNING

Explanation: A protocol error occurred during database synchronization.

Action: None required.

DSS Type in file <filename> has changed. DSS must be reloaded for the change to take effect.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter has changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

Error in primary DSS's database transfer SAP packet (%x).

Source: DSS

Severity: WARNING

Explanation: A protocol error occurred during database synchronization.

Action: None required.

Error in secondary DSS's upload packet (<n>).

Source: DSS

Severity: WARNING

Explanation: A protocol error was found in a packet received from a secondary DSS server.

Action: None required.

Error in secondary DSS's upload SAP packet (<n>).

Source: DSS

Severity: WARNING

Explanation: A protocol error was found in a packet received from a secondary DSS server.

Action: None required.

Error while receiving data of len=<n> from Primary DSS.

Source: DSS

Severity: WARNING

Explanation: The system was unable to communicate with the primary DSS server and is aborting the data transfer.

Action: If you see this message infrequently, no action is required. If you see this message frequently, check the status of the DSS server.

FATAL ERROR – Cannot open SOA file. errno=<number>.

Source: DSS

Severity: ERROR

Explanation: The NWIP_DSS.SOA file in the SYS:\ETC directory is corrupt. This error sets off an alarm at the SNMP management station.

Action: Unload the NLM, delete the file, and then reload the NLM.

Full database transfer aborted due to error.

Source: DSS

Severity: ERROR

Explanation: DSS could not perform a full zone transfer.

Action: Follow the action specified in the preceding messages.

HndlSecDSSUpld: Error in receiving upload information.

Source: DSS

Severity: WARNING

Explanation: The secondary-to-primary DSS server communication was aborted due to an error.

Action: Ensure physical connectivity between the DSS servers.

Illegal TCP Packet Type=<type> received at secondary DSS. Check DNS & DSS configuration.

Source: DSS

Severity: WARNING

Explanation: The secondary DSS server received an illegal packet type.

Action: Check the DSS server configuration.

Illegal TCP Pkt received of type=<type>.

Source: DSS

Severity: WARNING

Action: If you see this message infrequently, no action is required.

Illegal UDP Packet Type=<type> received from host at <ipaddress>.

Source: DSS

Severity: WARNING

Explanation: The host, identified by its IP address, is sending packets of unknown type.

Action: If you see this message infrequently, no action is required.

InitHashTbls – Btrieve error = <btrieve error code>.

Source: DSS

Severity: WARNING

Explanation: The DSS hash tables cannot be initialized due to an error in btrieve file operation.

Action: Check disk space on the SYS: volume.

InitHashTbls – Out of memory.

Source: DSS

Severity: WARNING

Explanation: The DSS hash tables cannot be initialized due to lack of memory.

Action: Add more RAM or unload other NLMs.

IPX Net Number in file <filename> has changed. DSS must be reloaded for the change to take effect.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

<NLM> – Missing or wrongly configured information about the NWIP domain.

Source: DSS

Severity: ERROR

Action: Configure the NetWare/IP domain and reload the NLM.

<NLM> – Missing or wrongly configured information about the Primary DSS address.

Source: DSS

Severity: ERROR

Explanation: The secondary DSS does not have the correct primary DSS information.

Action: Reconfigure the secondary DSS with the correct primary DSS information.

New TCP connections cannot be granted at this time.

Source: DSS

Severity: WARNING

Explanation: The DSS server is congested with zone transfer request traffic.

Action: If the system displays this message frequently and the DSS server is running on a dedicated machine, you should consider increasing the maximum number of TCP connections allowed by the DSS server in the SYS:ETC\NWPARAMS file. Otherwise, you should consider reducing the load on the DSS server by making it an unregistered DSS server or by reducing the number of NetWare/IP servers and clients that use this DSS server as their preferred DSS server.

NSQ – UDP Pkt queuing error. Unload and reload DSS NLM.

Source: DSS

Severity: ERROR

Explanation: A software error occurred.

Action: Unload and reload the DSS NLM.

Parameter: <parameter> not found in configuration file: <filename>.

Source: DSS

Severity: ERROR

Explanation: An expected DSS configuration parameter was not found. If the parameter is deleted while the DSS server is running, this error message sets off an alarm at the SNMP management station.

Action: Check the DSS server configuration.

Parameter: <parameter> not found in configuration file. Using defaults.

Source: DSS

Severity: WARNING

Action: If the defaults are not acceptable, reconfigure the parameter stated in the message and reload the NLM.

<n> – Primary DSS is not responding or is down.

Source: DSS

Severity: ERROR

Explanation: The secondary DSS server cannot communicate with the primary DSS server.

Action: Ensure connectivity to the primary DSS server, check the DSS server configuration, and then reload the DSS NLM.

Reached Maximum TCP connections limit. Postpone creating new connections.

Source: DSS

Severity: WARNING

Action: If you see this message infrequently, no action is required. If you see this message frequently, set up a new DSS server to balance the load.

RIP RO Database access error=<error number>.

Source: DSS

Severity: WARNING

Explanation: An error occurred in accessing the RIP btrieve database. This may indicate that the btrieve database is corrupt.

Action: If this message is displayed frequently, unload and reload the DSS NLM using the /RESETDB switch.

RIP – UDP Pkt queuing error. Unload and reload DSS NLM.

Source: DSS

Severity: ERROR

Explanation: A software error occurred.

Action: Unload and reload the DSS NLM.

SAP – UDP Pkt queuing error. Unload and reload DSS NLM.

Source: DSS

Severity: ERROR

Explanation: A software error occurred.

Action: Unload and reload the DSS NLM.

SDB_ReplaceDBRec: Btrieve Error=<btrieve error code>. Get_Drct from pos=<position in the btrieve file>.

Source: DSS

Severity: WARNING

Explanation: An error occurred in accessing the btrieve SAP/RIP database (possibly due to btrieve file corruption).

Action: If this error occurs frequently, unload and reload the DSS NLM using the /RESETDB switch.

SDB_ReplaceDBRec: Btrieve Error=<error number> during Delete Operation.

Source: DSS

Severity: WARNING

Explanation: An error occurred in deleting a record from the btrieve SAP/RIP database (possibly due to btrieve file corruption).

Action: Check disk space. If this error occurs frequently, unload and reload the DSS NLM using the /RESETDB switch.

SDB_ReplaceDBRec: Btrieve Error=<error number> during Update Operation.

Source: DSS

Severity: WARNING

Explanation: An error occurred in updating the btrieve SAP/RIP database (possibly due to btrieve file corruption).

Action: Check disk space. If this error occurs frequently, unload and reload the DSS NLM using the /RESETDB switch.

SecDSSUpld: Unable to receive follow-on upload packet from secondary.

Source: DSS

Severity: WARNING

Explanation: The secondary-to-primary DSS server communication was aborted due to an error.

Action: Ensure physical connectivity between the DSS servers.

Secondary DSS cannot operate safely because a basic configuration parameter has changed on the primary DSS.

Source: DSS

Severity: ERROR

Explanation: The secondary DSS server cannot operate safely because a basic configuration parameter has changed on the primary DSS server. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

Secondary DSS has discovered that domain name has changed on the primary DSS.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

Secondary DSS has discovered that UDP port number for NetWare/IP service has changed on the primary DSS.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

Secondary DSS has discovered that virtual IPX net number has changed on the primary DSS.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

Secondary DSS will be dysfunctional till configuration inconsistency between the primary DSS and this DSS is corrected.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

Secondary DSS will be dysfunctional till it is reloaded.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

SOA File seems to be corrupted.

Source: DSS

Severity: ERROR

Explanation: The NWIP_DSS.SOA file in SYS:\ETC directory is corrupt. This error message sets off an alarm at the SNMP management station.

Action: Delete the file and then reload the NLM.

UDP NSQ Packet queue is full. Consider setting up more DSSes.

Source: DSS

Severity: WARNING

Action: If you see this message infrequently, no action is required. If you see this message frequently, set up a new DSS server to balance the load.

UDP Port Number in file <filename> has changed. DSS must be reloaded for the change to take effect.

Source: DSS

Severity: ERROR

Explanation: The DSS server cannot operate safely because a basic configuration parameter changed while the DSS server was running. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload the DSS NLM.

UDP RIP Packet queue is full. Consider setting up more DSSes.

Source: DSS

Severity: WARNING

Action: If you see this message infrequently, no action is required. If you see this message frequently, set up a new DSS server to balance the load.

UDP SAP Packet queue is full. Consider setting up more DSSes.

Source: DSS

Severity: WARNING

Action: If you see this message infrequently, no action is required. If you see this message frequently, set up a new DSS server to balance the load.

Unable to add more routes for network=<n>.

Source: DSS

Severity: WARNING

Explanation: The RIP entry for the IPX™ network has the maximum number (16) of routes to the network registered with the DSS server.

Action: None required.

Unable to add more routes for server=<string>.

Source: DSS

Severity: WARNING

Explanation: The SAP entry for the server has the maximum number of routes (16) to the server registered with the DSS server.

Action: None required.

<NLM> – Unable to allocate/initialize system resources.

Source: DSS

Severity: ERROR

Explanation: The system cannot provide sufficient memory to load DSS.NLM.

Action: Add more RAM or unload other NLMs, and then reload the NLM.

<NLM> – Unable to determine DSS type (primary or secondary).

Source: DSS

Severity: ERROR

Explanation: Configuration files are not synchronized with respect to the configuration of the DSS.

Action: Reconfigure the DSS software and then reload the NLM.

<NLM> – Unable to down-load database from primary DSS.

Source: DSS

Severity: WARNING

Explanation: An error occurred while communicating with the primary DSS server.

Action: Ensure connectivity to the primary DSS server, check the primary DSS server configuration, and then reload the NLM.

<NLM> – Unable to establish a process to listen for TCP packets.

Source: DSS

Severity: ERROR

Action: Ensure that no other NLM is using the DSS's registered port number (43981 by default).

<NLM> – Unable to establish a process to listen for UDP packets.

Source: DSS

Severity: ERROR

Action: Ensure no other NLM is using the DSS's registered port number (43981 by default).

Unable to get system resources. Cannot provide effective service.

Source: DSS

Severity: ERROR

Explanation: The system is unable to create a new process to handle a TCP connection. This error message sets off an alarm at the SNMP management station.

Action: Unload unnecessary NLMs to free some resources.

<NLM> – Unable to initialize data base due to low memory or low disk space.

Source: DSS

Severity: WARNING

Action: Add more RAM, unload other NLMs, or free up about 500K of disk space on the SYS: volume, and then reload the NLM.

Unable to load.

Source: DSS

Severity: ERROR

Explanation: The previous messages should indicate the problem.

Action: Follow the action specified for the preceding messages.

<NLM> – Unable to read or write a file to SYS:/ETC.

Source: DSS

Severity: ERROR

Action: Free about 500K of disk space in the SYS: volume and then reload the NLM.

Unable to send data on UDP (retval=<n>). Verify TCPIP is operational.

Source: DSS

Severity: WARNING

Action: Check TCP/IP status.

NAMED Module

10: \'<filename>\' in <string> is an invalid zone type.

Source: NAMED

Severity: ERROR

Explanation: The specified configuration file has a bad keyword.

Action: Check the configuration file and correct the keyword.

15: Too many zones.

Source: NAMED

Severity: WARNING

Explanation: Too many zones are specified in the configuration file.

Action: Check the configuration file and specify the correct number of zones.

20: Ignoring input after line <number> in <string>.

Source: NAMED

Severity: WARNING

Explanation: After sending error message No. 15, the named server stopped reading the configuration file.

Action: Check the configuration file that caused the problem and correct it.

25: <filename>: line <number>: missing zone origin.

Source: NAMED

Severity: WARNING

Explanation: The specified configuration file has an incomplete zone configuration at the indicated line number.

Action: Check the configuration file and correct it.

30: <filename>: no database source for zone <name>.

Source: NAMED

Severity: WARNING

Explanation: The specified configuration file has an incomplete zone configuration for the indicated zone.

Action: Check the configuration file and correct it.

35: Zone <name> empty.

Source: NAMED

Severity: WARNING

Explanation: The specified zone is empty.

Action: None.

40: <filename>: No such file.

Source: NAMED

Severity: WARNING

Explanation: The specified database file does not exist.

Action: Check the database file.

45: Zone <name> information incomplete.

Source: NAMED

Severity: WARNING

Explanation: The specified zone contains incomplete information.

Action: Check the database file.

50: No IP address for secondary zone <name> master.

Source: NAMED

Severity: WARNING

Explanation: No IP address is assigned for the specified zone.

Action: Check the configuration file.

55: Cannot provide information on zone <name>.

Source:	NAMED
Severity:	WARNING
Explanation:	The module cannot provide the service (information) for the specified zone.
Action:	Check the configuration file.

60: More than one cache zone specified in <filename>.

Source:	NAMED
Severity:	WARNING
Explanation:	More than one cache zone is specified in the configuration file.
Action:	Check the configuration file.

75: <filename>: No valid cache, primary or secondary zone.

Source:	NAMED
Severity:	ERROR
Explanation:	The configuration file does not contain enough zone information.
Action:	Check the configuration file.

90: <filename>: line <line number>: database format error.

Source:	NAMED
Severity:	WARNING
Explanation:	The specified database file contains an illegal string at the indicated line number.
Action:	Correct illegal string.

95: Failure in save data for domain <name>.

Source:	NAMED
Severity:	WARNING
Explanation:	There was a failure to allocate memory for storing the domain information.
Action:	Add more system memory.

100: <filename>: Unknown $ option: <option found>\n.

Source: NAMED

Severity: WARNING

Explanation: The specified database file contains an unknown option.

Action: Correct the option.

105: <filename>: line <number>: expected a number.

Source: NAMED

Severity: ERROR

Explanation: The specified database file expects a number at the indicated line number.

Action: Assign a number.

110: <filename>: line <number>: expected a number.

Source: NAMED

Severity: ERROR

Explanation: The specified database file expects a number at the indicated line number.

Action: Assign a number.

115: <filename>: line <number>: unexpected EOF.

Source: NAMED

Severity: ERROR

Explanation: The specified database file detects an unexpected end-of-file (EOF) marker at the indicated line number.

Action: Remove the EOF marker.

120: <filename>: <name of service> port no. <number> too big.

Source: NAMED

Severity: WARNING

Explanation: The specified database file has a service with an illegal port number.

Action: Correct the port number.

150: Out of memory in getspmem.

Source: NAMED

Severity: ERROR

Explanation: The system needs more memory.

Action: Add more memory.

155: Unable to free arguments.

Source: NAMED

Severity: ERROR

Explanation: The NLM fails to free RPC arguments from the stack.

Action: Contact your authorized Novell reseller for assistance.

180: Maximum Cache Size should be <number>–<number>K.

Source: NAMED

Severity: WARNING

Explanation: The specified command line parameter is out of range.

Action: Check the command line parameter.

185: Proceeding with Maximum Cache Size of <number>K.

Source: NAMED

Severity: WARNING

Explanation: The specified command line parameter is out of range. Therefore, the server proceeds with the maximum cache size.

Action: Check the command line parameter.

9005001: Out of memory.

Source: NAMED

Severity: ERROR

Explanation: The system needs more memory.

Action: Add more memory.

9005001: Cannot allocate memory resourcetag.

Source: NAMED

Severity: ERROR

Explanation: The name server cannot allocate memory resource tag.

Action: Contact your authorized Novell reseller for assistance.

9005001: Out of memory.

Source: NAMED

Severity: ERROR

Explanation: The system needs more memory.

Action: Add more memory.

9005002: <filename>: No such file.

Source: NAMED

Severity: ERROR

Explanation: The specified configuration file does not exist.

Action: Check the configuration file and correct it.

9005002: Cannot open file <filename> for dumping NAMED cache.

Source: NAMED

Severity: ERROR

Explanation: The storage device is out of space.

Action: Check the available space on the storage device.

9005006: Unable to free arguments.

Source: NAMED

Severity: ERROR

Explanation: The NLM fails to free RPC arguments from the stack.

Action: Contact your authorized Novell reseller for assistance.

9005007: Failure to Register with the dispatcher.

Source: NAMED

Severity: ERROR

Explanation: The name server failed to register with the dispatcher.

Action: Contact your authorized Novell reseller for assistance.

NWIP Module

Aborting IPX Cache upload to DSS <IP address>.

Source: NWIP

Severity: ERROR

Explanation: Either the server is busy or a software error occurred.

Action: None required.

AddRipTrack – Cannot allocate <amount> bytes of memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

AddSapTrack – Cannot allocate <amount> bytes of memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

All 4 components of an ip address must be provided in PREFERRED DSS entries.

Source: NWIP

Severity: WARNING

Explanation: The string used to specify a preferred DSS server is not valid.

Action: Specify an acceptable value in the server's Preferred DSS server listing.

Bad RIP record found in DB Xfer Pointer=<pointer location>, Count=<record number>.

Source: NWIP

Severity: ERROR

Explanation: An unexpected record type was found in the data received from the DSS server. Either the DSS server is returning bad data or some NLM is corrupting the memory locally.

Action: Check the current DSS server for NWIP.NLM. You may also want to trace locally which NLM is corrupting the system or other NLMs.

Bad SAP record found in DB Xfer Pointer=<pointer location>, Count=<record number>.

Source: NWIP

Severity: ERROR

Explanation: An unexpected record type was found in the data received from the DSS server. Either the DSS server is returning bad data or some NLM is corrupting the memory locally.

Action: Check the current DSS server for NWIP.NLM. You may also want to trace locally which NLM is corrupting the system or other NLMs.

Cannot allocate memory for building DSS list.

Source: NWIP

Severity: ERROR

Explanation: The server is trying to recontact the DSS servers it learned about from the DNS server.

Action: Check the status of your DSS servers. Check the IP connectivity between this server and the DSS servers.

Cannot allocate resource tag for Alloc. Check system's health.

Source: NWIP

Severity: ERROR

Explanation: The system cannot provide memory to load NWIP.NLM.

Action: Add more RAM or unload other NLMs.

Cannot bind a TCP socket. Aborting synchronization with DSS.

Source: NWIP

Severity: WARNING

Explanation: The DSS database cannot be synchronized because the system is low on resources.

Action: None required.

Cannot connect to DSS at <ipaddress>. Check its status.

Source: NWIP

Severity: WARNING

Explanation: The DSS server, identified by its IP address, is not accepting new TCP connections.

Action: Ensure that there is physical connectivity to the DSS server.

Cannot determine a local IP address. Check if TCPIP is bound.

Source: NWIP

Severity: ERROR

Explanation: The system cannot provide information about local TCP/IP configuration.

Action: Configure TCP/IP and reload TCPIP.NLM.

Cannot determine DSSes servicing the NetWare/IP domain <domain name> by looking at the Preferred DSS list and by sending DNS queries.

Source: NWIP

Severity: ERROR

Explanation: The NetWare/IP server cannot locate a DSS server in the specified NetWare/IP domain.

Action: Use the UNICON Query Remote Name Server function to make sure that DNS Name Server (NS) records have been added for the DSS servers in the NetWare/IP domain.

Cannot obtain global DSSes by sending DNS queries. Check your DNS client (resolver) configuration.

Source: NWIP

Severity: ERROR

Explanation: The server cannot locate DSS servers for its NetWare/IP domain by sending DNS queries.

Action: Check the DNS client (resolver) configuration for the server using the UNICON View Server Profile function.

Cannot open a TCP socket. Aborting synchronization with DSS (errno=<number>).

Source: NWIP

Severity: WARNING

Explanation: The DSS database cannot be synchronized because the system is low on resources.

Action: None required.

Cannot open local parameters file <filename> for reading.

Source: NWIP

Severity: ERROR

Explanation: The NetWare/IP server cannot read from the file containing its local copy of the global NetWare/IP parameters.

Action: Make sure that the file exists. Check the file attributes for the file.

Cannot open local parameters file <filename> for writing.

Source: NWIP

Severity: ERROR

Explanation: The NetWare/IP server cannot open the file containing its local copy of the global NetWare/IP permeates.

Action: Check the file attributes for the file. Check disk space on the SYS: volume.

Cannot receive database data from DSS. Expected length=<n>.

Source: NWIP

Severity: WARNING

Explanation: The system was unable to communicate with the DSS server and is aborting the transfer of information.

Action: If you see this message infrequently, no action is required.If you see this message frequently, check the status of the DSS servers.

Cannot reply to RIP query because cannot get lock.

Source: NWIP

Severity: ERROR

Explanation: The server cannot respond to an RIP query because it is unable to lock the particular RIP hash table entry.

Action: Follow the action specified in the preceding messages.

Cannot reply to SAP query because of failure to get lock.

Source: NWIP

Severity: ERROR

Explanation: The server cannot respond to a SAP query because it is unable to lock the particular SAP hash table entry.

Action: Follow the action specified in the preceding messages.

Cannot set socket to non-blocking mode.

Source: NWIP

Severity: ERROR

Explanation: There is an error in making a call to the TCP/IP socket library.

Action: Make sure that TCP/IP is properly bound to the network interface.

Cannot synchronize database. Unload and reload NWIP.NLM.

Source: NWIP

Severity: ERROR

Explanation: A software error occurred while trying to synchronize databases with the DSS.

Action: Unload and reload NWIP.NLM.

Cannot write to local parameters file <filename>.

Source: NWIP

Severity: ERROR

Explanation: The NetWare/IP server cannot write to the file containing its local copy of the global NetWare/IP parameters.

Action: Check the file attributes for the file. Check disk space on the SYS: volume.

Configuration parameter specified by <parameter> has invalid IP Address=<ipaddress>.

Source: NWIP

Severity: WARNING

Explanation: Invalid information is present in the NetWare/IP configuration files. The software uses the default value until the error is corrected.

Action: If the default value is not acceptable, reconfigure NetWare/IP.

Configuration parameter <parameter> with value=<ipaddress> is not bound.

Source: NWIP

Severity: WARNING

Explanation: The IP address specified in the NetWare/IP configuration files as the Preferred IP Address is not being used. The software uses the default value until the error is corrected.

Action: If the default value is not acceptable, bind TCPIP using the preferred IP address.

Consider increasing the maximum number of packet receive buffers on this machine.

Source: NWIP

Severity: WARNING

Explanation: The system does not have a large enough pool of packet receive buffers.

Action: Increase the maximum number of packet receive buffers.

Could not fully synchronize the OS with NetWare/IP cache because of packet receive buffer allocation failures.

Source: NWIP

Severity: WARNING

Explanation: The system does not have a large enough pool of packet receive buffers for NWIP.NLM to work effectively.

Action: If the system displays this message frequently, consider increasing the maximum number of packet receive buffers.

Failed to get NetWare/IP global parameters from DSS at <IP address>.

Source: NWIP

Severity: WARNING

Explanation: The NetWare/IP server did not receive a response to a parameter query sent to the specified DSS server.

Action: Make sure that the current DSS server is up and running and reachable via IP from this server.

Failed to receive GET OPTIONAL PARAMS response from DSS at <IP address>.

Source: NWIP

Severity: WARNING

Explanation: The NetWare/IP server did not receive a response to a parameter query sent to the DSS server.

Action: Make sure that the current DSS server is up and running and reachable via IP from this server.

Failed to register a dynamic port with UDP.

Source: NWIP

Severity: ERROR

Explanation: UDP service is unavailable.

Action: Unload and reload the TCPIP.NLM.

Failed to register configured port <portnumber> with UDP.

Source: NWIP

Severity: ERROR

Explanation: The UDP port numbers, configured on the primary DSS server, are in use on the local machine.

Action: Either unload the NLM using the configured port numbers, or reconfigure the primary DSS server with new port numbers and then restart the DSS server(s), NetWare/IP servers, and NetWare/IP clients.

FATAL: Unable to get NWIP global parameters from any DSS.

Source: NWIP

Severity: ERROR

Explanation: The server cannot get a response from any of the DSS servers. If the server is loading for the first time after configuration, it will be unable to operate.

Action: Check the status of the DSS servers. Check the IP connectivity between this server and the DSS servers.

FATAL: Unable to get NWIP parameters from all available DSSes.

Source: NWIP

Severity: ERROR

Action: Check the status of the DSS servers.

Ignoring the local copy of parameters because it does not correspond to the NetWare/IP domain name <domain name>.

Source: NWIP

Severity: WARNING

Explanation: The server has been reconfigured for a new NetWare/IP domain. Therefore, the server cannot use the file containing its local copy of the global NetWare/IP parameters.

Action: None required.

IpxcacheTimeOut – Cannot allocate 8K of memory.

Source: NWIP

Severity: WARNING

Explanation: The machine does not have enough memory to run the NWIP.NLM.

Action: Add some more RAM or unload some other NLMs.

<Server name>: IPX Network number has changed for the NetWare/IP network. NWIP NLM must be reloaded for the change to take effect.

Source: NWIP

Severity: ERROR

Explanation: The server has detected a change in a basic configuration parameter at the primary DSS server. The server cannot operate safely until it is unloaded and reloaded. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload NWIP.NLM.

<String> is not an acceptable specification of a PREFERRED DSS.

Source: NWIP

Severity: WARNING

Explanation: The string used to specify a preferred DSS server is not valid.

Action: Specify an acceptable value in the server’s Preferred DSS server listing.

MaintainNWIPRip – Cannot allocate <amount> bytes of memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

MaintNWIPSap – Cannot allocate <amount> bytes of memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

MakeIPXECB – Failed to allocate SAP/RIP Packet for the OS.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

<Server name> NetWare/IP domain name on DSS <IP address> does not match the locally configured domain. Check DSS and NetWare/IP domain configuration.

Source: NWIP

Severity: ERROR

Explanation: The server has detected a change in a basic configuration parameter at the primary DSS server. The server cannot operate safely until it is unloaded and reloaded. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload NWIP.NLM.

NetWare/IP parameters received from DSS <IP address> are different from the local ones.

Source: NWIP

Severity: WARNING

Explanation: The server has detected a change in a global configuration parameter at the primary DSS server.

Action: Check the NetWare/IP domain name configured at the DSS server. Unload and reload NWIP.NLM.

<Server name>: NetWare/IP server (an IP/IPX gateway) is going down. May lead to degraded service.

Source: NWIP

Severity: WARNING

Explanation: A NetWare/IP gateway is being unloaded. This may prevent some clients from communicating with some servers in the mixed IP/IPX network. This error message sets off an alarm at the SNMP management station.

Action: Reload the NetWare/IP server as soon as possible.

<Server name>: NetWare/IP server cannot operate safely because a basic configuration parameter has changed on the current DSS (<DSS IP Address>).

Source: NWIP

Severity: ERROR

Explanation: The server has detected a change in one or more of the following parameter values: NetWare/IP domain name, UDP port number, or IPX network number. This error sets off an alarm at the SNMP management station.

Action: If the NetWare/IP domain name has changed, obtain the new domain name from your network administrator and reconfigure the server. Reload NWIP.NLM.

<Server name>: NetWare/IP server cannot synchronize database with DSS. Unload and reload the NWIP NLM.

Source: NWIP

Severity: ERROR

Explanation: A software error occurred during the database synchronization with the current DSS server.

Action: Unload and reload NWIP.NLM.

<Server name>: NetWare/IP server could not lock the IPX RIP Hash Entry <entry number> in <number> minutes.

Source: NWIP

Severity: WARNING

Explanation: This error should not occur unless something is fundamentally wrong with the server (such as an NWIP.NLM thread being stuck waiting for some event to happen). This error sets off an alarm at the SNMP management station.

Action: Collect as much data as you can about your configuration and call technical support. You can reload NWIP.NLM to get out of this state.

<Server name>: NetWare/IP server could not lock the IPX SAP Hash Entry <entry number> in <number> minutes.

Source: NWIP

Severity: WARNING

Explanation: This error should not occur unless something is fundamentally wrong with the server (such as an NWIP.NLM thread being stuck waiting for some event to happen). This error sets off an alarm at the SNMP management station.

Action: Collect as much data as you can about your configuration and call technical support. You can reload NWIP.NLM to get out of this state.

<Server name>: NetWare/IP server will be dysfunctional till it is reloaded.

Source: NWIP

Severity: ERROR

Explanation: The server has detected a change in one or more of the following parameter values: NetWare/IP domain name, UDP port number, or IPX network number. This error sets off an alarm at the SNMP management station.

Action: If the NetWare/IP domain name has changed, obtain the new domain name from your network administrator and reconfigure the server. Reload NWIP.NLM.

NWIP.NLM cannot load.

Source: NWIP

Severity: ERROR

Explanation: The previous message should indicate the problem.

Action: Follow the action specified in the preceding messages.

NWIP NLM could not synchronize with the OS in <number> secs for <number> consecutive times. Could be due to too much load and/or too few ECBs.

Source: NWIP

Severity: WARNING

Explanation: The thread used to synchronize information received from the DSS server is starving (not getting enough time) because some other thread is hogging the processor.

Action: Check the CPU utilization of different threads on the system to identify the offending thread and NLM. You may also want to consider increasing the number of maximum packet receive buffers.

NWIPRipExit – Cannot allocate 8K memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: None required.

NWIPSapExit – Cannot allocate 8K memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: None required.

NWIP.NLM cannot load.

Source: NWIP

Severity: ERROR

Explanation: The previous messages should indicate the problem.

Action: Follow the action specified for the preceding messages.

OutboundRipFilter – Cannot allocate <amount> bytes of memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

OutboundSapFilter – Cannot allocate <n> bytes of memory.

Source: NWIP

Severity: WARNING

Explanation: The system cannot provide enough memory to NWIP.NLM for communication purposes.

Action: If you see this message infrequently, no action is required. If you see this message frequently, add more RAM or unload other NLMs.

Received an unexpected response from DSS. Packet Type=<type>.

Source: NWIP

Severity: WARNING

Explanation: The erroneous packet received is being dropped.

Action: If you see this message infrequently, no action is required.

Retrying contacting Global DSSes.

Source: NWIP

Severity: WARNING

Explanation: The server is retrying the DSS servers it learned about from the DNS server.

Action: Check the status of the DSS servers. Check the IP connectivity between the server and the DSS servers.

Retrying contacting Local DSSes.

Source: NWIP

Severity: WARNING

Explanation: The server is retrying the DSS servers specified in its preferred DSS listing.

Action: Check the status of the DSS servers. Check the IP connectivity between the server and the DSS servers.

Skipping current RIP Track because cannot lock RIP Hash Table entry <entry number>.

Source: NWIP

Severity: ERROR

Explanation: Some IPX RIP cache entries cannot be correctly maintained at this time because either the server or the current DSS server is very busy.

Action: Follow the action specified in the preceding messages.

Skipping current SAP Track because cannot lock SAP Hash Table entry <entry number>.

Source: NWIP

Severity: ERROR

Explanation: Some IPX SAP cache entries cannot be correctly maintained at this time because either the server or the current DSS server is very busy.

Action: Follow the action specified in the preceding messages.

Skipping RIP Hash Table Entry <entry number> in IpxCacheTimeout.

Source: NWIP

Severity: WARNING

Explanation: Some IPX RIP cache entries cannot be correctly maintained at this time because the server is very busy.

Action: Follow the action specified in the preceding messages.

Skipping SAP Hash Table Entry <entry number> in IpxCacheTimeout.

Source: NWIP

Severity: WARNING

Explanation: Some IPX SAP cache entries cannot be correctly maintained at this time because the server is very busy.

Action: Follow the action specified in the preceding messages.

System out of resources. NWIP.NLM cannot load.

Source: NWIP

Severity: ERROR

Explanation: The system cannot provide sufficient memory for NWIP.NLM.

Action: Add more RAM or unload other NLMs.

<Server name>: UDP port number has changed for NetWare/IP network. NWIP NLM must be reloaded for the change to take effect.

Source: NWIP

Severity: ERROR

Explanation: The server has detected a change in a basic configuration parameter at the primary DSS server. The server cannot operate safely until it is unloaded and reloaded. This error message sets off an alarm at the SNMP management station.

Action: Unload and reload NWIP.NLM.

Unable to communicate with any of the known DSSes.

Source: NWIP

Severity: ERROR

Explanation: The server cannot contact any of the DSS servers at startup time. The server may continue to operate in a degraded state. This error message sets off an alarm at the SNMP management station.

Action: Check the status of the DSS servers. Make sure there is IP connectivity between the server and the DSS servers.

Unable to communicate with preferred DSS at <ipaddress>. Check DSS status.

Source: NWIP

Severity: WARNING

Explanation: The DSS server identified by this IP address is not responding.

Action: Ensure that the DSS server is running and that it can be reached from the server via the IP protocol.

Unable to create a new process. Check system resources.

Source: NWIP

Severity: ERROR

Explanation: The system is low on memory.

Action: Unload a few NLMs.

Unable to send request to DSS <ipaddress>. Aborting synchronization with DSS.

Source: NWIP

Severity: WARNING

Explanation: The specified DSS server is not responding.

Action: None required.

Using alternate DSS at <ipaddress>.

Source: NWIP

Severity: WARNING

Explanation: The DSS server closest to this server is not responding. Therefore, the server is trying to contact a less than optimal DSS server.

Action: Ensure that the current DSS server is running and can be reached from this server via the IP protocol.

PKERNEL Module

35: trap_free() found an invalid memory block.

Source: PKERNEL

Severity: ERROR

Explanation: PKERNEL.NLM detected memory corruption. The system is unstable and may crash when this message is displayed.

Action: Ask users to log out of the system, and then restart NetWare. If this is not possible, you must stop the NFS Services software. After unloading the software, unload PKERNEL.NLM, reload PKERNEL.NLM, and then restart NFS 2.0.

40: trap_free() found an invalid memory block (line <number> in <string>).

Source: PKERNEL

Severity: ERROR

Explanation: PKERNEL.NLM detected memory corruption. The system is unstable and may crash when this message is displayed.

Action: Ask users to log out of the system, and then restart NetWare. If this is not possible, you must stop the NFS Services software. After unloading the software, unload PKERNEL.NLM, reload PKERNEL.NLM, and then restart NFS 2.0.

50: Trap memory header corrupted.

Source: PKERNEL

Severity: ERROR

Explanation: Memory corruption is detected by PKERNEL.NLM. System is unstable and may crash when this message is displayed.

Action: Ask users to log out of the system, and then restart NetWare. If this is not possible, you must stop the NFS Services software. After unloading the software, unload PKERNEL.NLM, reload PKERNEL.NLM, and then restart NFS 2.0.

55: Trap memory link list corrupted.

Source: PKERNEL

Severity: ERROR

Explanation: Memory corruption is detected by PKERNEL.NLM. System is unstable and may crash when this message is displayed.

Action: Ask users to log out of the system, and then restart NetWare. If this is not possible, you must stop the NFS Services software. After unloading the software, unload PKERNEL.NLM, reload PKERNEL.NLM, and then restart NFS 2.0.

60: Cannot allocate resource tag.

Source: PKERNEL

Severity: ERROR

Explanation: PKERNEL failed in allocating a server resource tag. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

65: Out of memory, cannot allocate non-movable cache memory.

Source: PKERNEL

Severity: WARNING

Explanation: PKERNEL failed while allocating nonmovable cache memory from the server. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

70: Cannot allocate a task number for Product Kernel Synchronization.

Source: PKERNEL

Severity: ERROR

Explanation: PKERNEL failed while allocating a task number from the server. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

90: Cannot open LocalSemaphore.

Source: PKERNEL

Severity: WARNING

Explanation: PKERNEL failed while acquiring required semaphore from the server. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

170: Cannot create the client handle in the portmapper module.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot create the client handle for future RPC operations. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

175: Out of memory, cannot create UDP client handle.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot allocate memory for the UDP client handle for future RPC operations. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

340: Out of memory, cannot allocate dynamic memory.

Source: PKERNEL

Severity: WARNING

Explanation: The NetWare server may be overloaded. The PKERNEL failed while allocating the required memory from server. This problem is usually due to insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

440: RPC/UDP receive queues are full, packet dropped.

Source: PKERNEL

Severity: WARNING

Explanation: Too many UDP packets have been received and have exceeded the UDP receive queues capacity in the RPC module. Some UDP packets may be lost. The server performance is degrading.

Action: This symptom could be caused by a spurt of network activities such as an RPC broadcast storm. In most cases, no action is required. If this symptom persists, monitor the network traffic using a packet trace analyzer (for example, Novell LANalyzer®).

445: Cannot find the local IP addr for Local Host (error=<errno_number>).

Source: PKERNEL

Severity: WARNING

Explanation: The IP address for the local host cannot be found.

Action: Check if the SYS:/ETC/HOSTS table is properly set up. Check NIS setup (if NIS is running).

455: RPC: svc_register failed for prog=<number>, vers=<number>.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot register the RPC service program.

Action: Ensure that the program and version number are already registered.

465: RPC: svcudp_create failed for prog=<number>, vers=<number>.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot initiate the RPC service program. In most cases, this problem is due to insufficient server memory.

Action: Free up server memory. For example, unload unneeded NLMs to release RPC connection ports.

505: Failed to register with UDP (error=<errno_number>).

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot register the RPC/UDP client program. Future RPC operations are not possible.

Action: Ensure that TCPIP.NLM is loaded.

515: Failed to deregister with UDP (error=<errno_number>).

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot deregister the RPC/UDP client program.

Action: The system may be unstable. If possible, restart NetWare or stop NFS Services, unload TCPIP.NLM, reload TCPIP.NLM, and then restart NFS Services.

530: Cannot send out the UDP Packet to <hostname>. (error=<errno_number>).

Source: PKERNEL

Severity: ERROR

Explanation: PKERNEL failed while sending out UDP packets to the remote host.

Action: There are numerous possibilities for action. For example, the TCPIP.NLM may not be correctly configured on the local host, the network traffic may be too high, or the remote host may not be running.

535: Cannot create the authentication handle.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot create the authentication handle for the authentication process. In most cases, this problem is caused by insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

540: Out of memory, cannot allocate dynamic memory for the authentication handle.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module cannot allocate memory for the authentication handle for the RPC authentication process. In most cases, this problem is caused by insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

560: xdrrec_create:out of memory.

Source: PKERNEL

Severity: ERROR

Explanation: The XDR module cannot allocate memory for the future XDR operations. In most cases, this problem is caused by insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

595: TCP: rendezvous request accept failed.

Source: PKERNEL

Severity: ERROR

Explanation: RPC module cannot initiate the RPC/TCP service program. In most cases, this problem is caused by insufficient server memory.

Action: Free up server memory (for example, unload unneeded NLMs).

615: TCP: svcsock_run return unexpected.

Source: PKERNEL

Severity: ERROR

Explanation: The RPC module ran into an unexpected state. The server is no longer stable.

Action: The system may be unstable. If possible, restart the NetWare server or stop all NetWare/IP modules, unload TCPIP.NLM, reload TCPIP.NLM, and then restart the NetWare/IP modules.

SRVAGT Module

5: SRVAGT.NLM: Failed to register with the NDS.

Source: SRVAGT

Severity: ERROR

Explanation: The specified NLM failed to register with Directory Services.

Action: Reload the NLM. If it fails again, contact Novell Customer Support.

10: SRVAGT.NLM: Failed to register with the dispatcher.

Source: SRVAGT

Severity: ERROR

Explanation: The specified NLM failed to register with the dispatcher.

Action: Reload the NLM. If it fails again, contact Novell Customer Support.

15: Unable to free arguments.

Source: SRVAGT

Severity: ERROR

Explanation: SRVAGT failed to free memory.

Action: Contact Novell Customer Support.

USRAGT Module

5: USRAGT.NLM: Failed to register with the dispatcher.

Source: USRAGT

Severity: ERROR

Explanation: The specified NLM failed to register with the dispatcher.

Action: Reload the NLM. If it fails again, contact Novell Customer Support.

10: USRAGT.NLM: unable to free arguments.

Source: USRAGT

Severity: ERROR

Explanation: The specified NLM failed to free memory.

Action: Call Novell Customer Support.

XConsole Module

5: XConsole failed to start the select screen.

Source: XCONSOLE

Severity: ERROR

Explanation: The selected screen is used to jump to an active NetWare screen.

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

10: XConsole failed to start the help screen.

Source: XCONSOLE

Severity: ERROR

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

15: The XConsole telnet daemon is unable to send data to the remote client, reason: <reason>.

Source: XCONSOLE

Severity: ERROR

Action: Close your XConsole session and establish a new session.

20: The XConsole telnet daemon is unable to start a new NetWare thread for a new session. <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to start a new session.

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

21: The XConsole telnet daemon is unable to allocate space for a new session. <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: The server is out of memory.

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

40: XConsole is unable to obtain the server's name. XConsole is unable to receive UnixWare requests.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to obtain the current server's name from NDS.

Action: Unload and reload XConsole.

45: Unable to open an SPX listen port. XConsole is unable to receive UnixWare requests.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to listen for a connection request on SPX.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

50: Unable to open an SPX listen port. XConsole is unable to receive UnixWare requests.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to listen for a connection request on SPX.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

55: Unable to allocate SPX buffers. XConsole is unable to receive UnixWare requests.

Source: XCONSOLE

Severity: ERROR

Explanation: The server is out of memory.

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

60: Unable to bind to rexecd port. XConsole is unable to receive UnixWare requests.

Source: XCONSOLE

Severity: ERROR

Explanation: UnixWare uses REXECD to connect to XConsole.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

65: The rexecd port (<port_num>) is already in use. XConsole is unable to receive UnixWare requests.

Source: XCONSOLE

Severity: ERROR

Action: Another NLM is using the given port number. Unload the NLM using this port, and then unload and reload XConsole.

70: The XConsole server on (<server_name>) is not able to advertise itself to UnixWare clients.

Source: XCONSOLE

Severity: ERROR

Explanation: The XConsole server will not show up in the UnixWare Remote_Aps application.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

80: XConsole is unable to listen for UnixWare clients requests. Reason: <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: An error occurred while XConsole was listening for UnixWare requests.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

85: Unable to open a new SPX connection to the UnixWare client. Reason: <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to accept a UnixWare Remote_Apps request.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

90: Unable to bind the new UnixWare client to the SPX connection. Reason <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to accept a UnixWare Remote_Apps request.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

95: Unable to accept the new UnixWare client connection. Reason <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to accept a UnixWare Remote_Apps request.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

100: A remote user was unable to connect to XConsole because the session limit (<max_session>) was reached.

Source: XCONSOLE

Severity: ERROR

Explanation: Login failed because the maximum number of sessions was reached.

Action: Close all inactive sessions. Reload the XConsole NLM and increase the number of maximum allowable sessions from the command line.

105: XConsole is unable to process new UnixWare Connection requests.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to start a new process to handle a Remote_Apps request.

Action: Unload any unnecessary NLMs to free up memory for XConsole. Unload and reload the XConsole NLM.

115: Unable to get the rexecd error port number from the client.

Source: XCONSOLE

Severity: ERROR

Explanation: An error occurred in the communication between XConsole and Remote_Apps.

Action: Establish a new XConsole session from UnixWare.

130: Unable to open the rexecd error port.

Source: XCONSOLE

Severity: ERROR

Action: Establish a new XConsole session from UnixWare.

135: Unable to bind to the error port.

Source: XCONSOLE

Severity: ERROR

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

140: Unable to allocate memory for accepting a UnixWare client.

Source: XCONSOLE

Severity: ERROR

Explanation: The server is out of memory.

Action: Unload any unnecessary NLMs to free up memory for XConsole. Unload and reload the XConsole NLM.

155: Unable to connect to UnixWare client. Reason: <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: An error occurred in the communication between XConsole and Remote_Apps.

Action: Ensure that IPX is properly bound to your network card. Unload and reload XConsole.

170: XConsole is unable to send data to the remote client. Reason <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is unable to respond to UnixWare’s Remote_Apps.

Action: Reauthenticate to XConsole through the UnixWare program remote applications.

175: XConsole is unable to respond to the UnixWare client after receiving a request to list available services. TLOOK returned: <return_val>.

Source: XCONSOLE

Severity: ERROR

Action: Close your XConsole session and reestablish a new session.

185: Unable to send the list of services provided by this server to UnixWare. TLOOK returned: <return_val>.

Source: XCONSOLE

Severity: ERROR

Action: Reauthenticate to NetWare through the UnixWare program remote applications.

235: XConsole is unable to read data from the remote client. Reason <reason>.

Source: XCONSOLE

Severity: ERROR

Explanation: The authentication to XConsole from remote applications failed.

Action: Reauthenticate to XConsole from the UnixWare program remote applications.

240: The username from rexec is too long. The size limit is <max_namelength>.

Source: XCONSOLE

Severity: ERROR

Explanation: This message only occurs during the LOGIN procedure from UnixWare.

Action: Reauthenticate using a shorter username.

241: The password from rexec is too long. The size limit is <max_passlength>.

Source: XCONSOLE

Severity: ERROR

Explanation: The UnixWare authentication from Remote_Apps failed.

Action: Reauthenticate using a shorter password.

242: The command from rexec is too long. The size limit is <max_cmdsize>.

Source: XCONSOLE

Severity: ERROR

Explanation: This error only displays during the login from UnixWare.

Action: Reauthenticate to XConsole from remote applications.

250: While XConsole was polling for data from the remote client, an error occurred on the connection.

Source: XCONSOLE

Severity: ERROR

Action: Close your current XConsole session and start a new session.

255: While XConsole was polling for data from the remote client, XConsole timed out because the remote client failed to respond.

Source: XCONSOLE

Severity: ERROR

Action: Try to continue your XConsole session. You might need to open a new XConsole session.

260: While XConsole was polling for data from the remote client, the remote host terminated the connection.

Source: XCONSOLE

Severity: ERROR

Action: Establish a new XConsole session.

265: While XConsole was polling for data from the remote client, the connection became invalid.

Source: XCONSOLE

Severity: ERROR

Action: Establish a new XConsole session.

270: Unable to receive data from the remote host; TLOOK returned: <err_val>.

Source: XCONSOLE

Severity: ERROR

Explanation: An unexpected event occurred on the XConsole connection while XConsole was trying to read data.

Action: Establish a new XConsole session.

275: Unable to receive data from the remote host. Reason: <reason>.

Source: XCONSOLE

Severity: ERROR

Action: Establish a new XConsole session.

290: An XConsole session login failed because an error occurred while XConsole was trying to read data from the remote client.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole is trying to read data from the remote client.

Action: Restart the remote XConsole session.

295: The XConsole login was not completed because the remote client closed the connection to XConsole or a connection error occurred.

Source: XCONSOLE

Severity: ERROR

Action: Restart the remote XConsole session. The remote client may need to be restarted.

300: Remote XConsole session failed to login, possible cause: invalid password.

Source: XCONSOLE

Severity: ERROR

Explanation: An invalid password was entered.

Action: Establish a new connection to XConsole and enter the correct password.

310: Unable to allocate memory for a VT100/220 session.

Source: XCONSOLE

Severity: ERROR

Explanation: The server is out of memory.

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

315: XConsole failed to receive a complete escape sequence from the remote client.

Source: XCONSOLE

Severity: ERROR

Explanation: Part of an escape sequence was received from the remote VT100/220 client, but the rest of the sequence is missing.

Action: You may need to reload XConsole using the ESCTIMEOUT command line option set to more than the default of 500 msec.

320: XConsole failed to receive a complete escape sequence from the remote client. The remote client may have disconnected from XConsole.

Source: XCONSOLE

Severity: ERROR

Explanation: A complete escape sequence was not received but XConsole received a hangup signal from the remote host.

Action: Reestablish a new XConsole session.

335: XConsole failed to register with PKERNEL.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole cannot be loaded unless it successfully registers with PKERNEL.

Action: Unload and reload the XConsole NLM.

340: XConsole failed to allocate a resource tag for the screen activate callback. Error #<err_num>.

Source: XCONSOLE

Severity: ERROR

Explanation: NetWare was unable to allocate a resource for XConsole. The server may be out of memory.

Action: Unload and reload the XConsole NLM.

345: Failed to register for screen activation notification. Error #<err_num>.

Source: XCONSOLE

Severity: ERROR

Explanation: NetWare was unable to allocate a resource for XConsole. The server may be out of memory.

Action: Unload and reload the XConsole NLM.

350: XConsole is unable to start accepting SPX connections.

Source: XCONSOLE

Severity: ERROR

Explanation: XConsole was unable to start the process that handles UnixWare requests.

Action: Unload any unnecessary NLMs to make more memory available to XConsole. Unload and reload XConsole.

385: The NetWare server has insufficient memory to create an X window on <hostname>.

Source: XCONSOLE

Severity: ERROR

Explanation: The server is out of memory.

Action: Unload any unnecessary NLMS to make more memory available to XConsole. Unload and reload XConsole.

390: The screen driver failed to start.

Source: XCONSOLE

Severity: ERROR

Explanation: The screen driver is a function that updates the remote screen.

Action: Unload any unnecessary NLMS to make more memory available to XConsole. Unload and reload XConsole.

400: XConsole failed to find a valid font in the font tables and internal tables on the remote X-server <hostname>.

Source: XCONSOLE

Severity: ERROR

Action: Add the font names available to your X Window System* server to the appropriate font file on the NetWare server.

405: XConsole failed to create an X window on <hostname>.

Source: XCONSOLE

Severity: ERROR

Action: Use the xhost command to ensure that the NetWare server can access your X Window System server.

410: XConsole is unable to create the remote X Window name on <hostname>.

Source: XCONSOLE

Severity: ERROR

Action: Use the xhost command to ensure that the NetWare server can access your X Window System server.

415: XConsole cannot create an icon name for the remote XConsole session on <hostname>.

Source: XCONSOLE

Severity: ERROR

Action: Use the xhost command to ensure that the NetWare server can access your X Window System server.

430: XConsole received the error event (<err_num>) from <hostname> session <sess_num>. <err_msg>.

Source: XCONSOLE

Severity: ERROR

Action: Reestablish the XConsole session.

445: Fatal IO error (<err_num>) <err_msg>, occurred on <hostname> session <sess_num>.

Source: XCONSOLE

Severity: ERROR

Explanation: The <err_msg> describes the unexpected error which occurred.

Action: Reestablish the XConsole session.

NetWare/IP Client Modules

An invalid entry was found on line n of the configuration file. Entry <entry name> ignored.

Source: NWIP.EXE

Severity: WARNING

Explanation: An invalid entry was found in the IPX™ section of your NET.CFG file.

Action: Enter a valid value for the parameter on the specified line of your NET.CFG file.

Cannot allocate memory for building DSS list.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: Memory allocation failure.

Action: Unload any unused TSRs to free up some memory.

Cannot contact any of the DSSes to get the SOA record.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: The client was able to locate a DSS server using a DNS query but was unable to obtain an SOA record from the DSS server.

Action: Have your NetWare/IP administrator check that DNS and DSS are properly configured and loaded.

Cannot find a NetWare/IP client to unload.

Source: NWIP.EXE

Severity: WARNING

Explanation: You tried to unload the NetWare/IP client software, but it is not loaded.

Action: None required.

Cannot get NWIP parameters from DSS.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: The client located a DSS server but was unable to obtain the global NetWare/IP configuration parameters.

Action: Have your NetWare/IP administrator check the primary DSS server configuration.

Cannot obtain global DSSes by sending DNS queries. Check DNS client (resolver) configuration.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: The client cannot locate any DSS servers in the DNS hierarchy by querying DNS.

Action: Have your NetWare/IP administrator add name server (NS) resource records to the DNS database for all DSS servers in your NetWare/IP domain.

Cannot open local parameters file NWIPPARM.NOV for writing.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: NetWare/IP cannot open or create the local NWIPPARM.NOV parameter file for writing.

Action: Make sure your workstation is not out of disk space. Check to make sure that the permissions are set properly for your files and directories.

Cannot pass NWIP Initialization, NWIP.EXE is not loaded!

Source: NWIP.EXE

Severity: ERROR

Explanation: NetWare/IP is unable to initialize. This may be due to errors encountered in NWIPINIT.EXE.

Action: Fix any problems reported by NWIPINIT.EXE.

Cannot read from local parameters file NWIPPARM.NOV.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: NetWare/IP cannot read from the local NWIPPARM.NOV parameter file.

Action: Check the file attributes for NWIPPARM.NOV.

Cannot unload NetWare/IP because another program has been loaded above it. Unload the other program or programs and try again.

Source: NWIP.EXE

Severity: ERROR

Explanation: Other applications or TSRs are using NetWare/IP.

Action: Unload the other applications or TSRs before unloading NetWare/IP.

Cannot use local NetWare/IP parameters because the NWIP Domain has changed.

Source: NWIPINIT.EXE

Severity: WARNING

Explanation: The client was unable to obtain the global NetWare/IP parameters from the NetWare/IP server or DSS server and attempted to start up using its local copy of the global parameters. However, the NetWare/IP domain name has changed since the last time the client was running.

Action: Have your NetWare/IP administrator verify that the NetWare/IP domain name has changed. If the NetWare/IP domain name has changed, the administrator must restart the primary DSS server, all secondary DSS servers, and all NetWare/IP servers. You must then reboot your client system.

Cannot write to local parameters file NWIPPARM.NOV.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: NetWare/IP cannot open or create the local NWIPPARM.NOV parameter file for writing.

Explanation: Make sure your workstation is not out of disk space.

Could not contact any DSS. Using local copy of NetWare/IP parameters.

Source: NWIPINIT.EXE

Severity: WARNING

Explanation: The client cannot locate a DSS server and is therefore using its local copy of the NetWare/IP parameters to boot.

Action: Have your NetWare/IP administrator check the DSS and DNS server configurations. Check that your RESOLV.CFG file is configured properly.

DNS name defined in net.cfg cannot be resolved.

Source: NWIPINIT.EXE

Severity: WARNING

Explanation: The DNS hostname specified for the PREFERRED_DSS or NEAREST_NWIP_SERVER parameter in the [NWIP] section of your NET.CFG file cannot be resolved. As a result, the entry will be ignored.

Action: Make sure that the DNS hostname specified in the NET.CFG file is spelled correctly.

Error in getting NWIP parameters, *n* bytes received.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: The client erroneously received NetWare/IP parameters from the DSS.

Action: Call Novell Technical Support.

Failed to invoke nwipinit.exe, NWIP aborted.

Source: NWIP.EXE

Severity: ERROR

Explanation: NetWare/IP cannot find NWIPINIT.EXE in the directory where NWIP.EXE is loaded.

Action: Make sure NWIPINIT.EXE is in the same directory as NWIP.EXE.

FATAL: Cannot get NWIP Domain Name, check net.cfg file!

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: The NWIP_DOMAIN_NAME parameter is not defined in your NET.CFG file.

Action: Configure the NWIP_DOMAIN_NAME parameter in the [NWIP] section of your NET.CFG file with the name of your NetWare/IP domain.

FATAL: TCP/IP is not loaded.

Source: NWIP.EXE

Severity: ERROR

Explanation: There is no TCP/IP stack loaded on this machine.

Action: Load the TCP/IP stack before loading NWIP.EXE.

FATAL: Unknown error resulting from get local IP address.

Source: NWIP.EXE

Severity: ERROR

Explanation: NetWare/IP cannot obtain your system's IP address from the TCP/IP stack.

Action: Call Novell Technical Support.

Invalid BIND statement on line n of the configuration file. Bind is not applicable to NWIP. Entry was ignored.

Source: NWIP.EXE

Severity: WARNING

Explanation: A BIND statement was found in the IPX section of your NET.CFG file.

Action: Remove the BIND statement from your NET.CFG file.

Invalid command line option was specified: <option>

Source: NWIP.EXE

Severity: WARNING

Explanation: An invalid command line option was specified while loading NWIP.EXE.

Action: Check the commands that execute while loading NetWare/IP.

Local DSS at this IP address is not responding. Its entry is dropped.

Source: NWIPINIT.EXE

Severity: WARNING

Explanation: A local DSS server specified as a preferred DSS server for your workstation is not responding.

Action: Check the PREFERRED_DSS parameter entry to ensure that the IP address entered is correct. Have your NetWare/IP administrator check that the DSS is properly configured and loaded.

Maximum number of stacks already loaded. Either unload an existing stack or increase the maximum by adding a MAX STACKS entry to the LINK SUPPORT section of the NET.CFG file.

Source: NWIP.EXE

Severity: ERROR

Explanation: The maximum number of stacks specified for the MAX_STACKS parameter in the Link Support section of your NET.CFG file has been reached.

Action: Increase the MAX STACKS parameter value in the Link Support section of your NET.CFG file.

Message file is invalid. Program load aborted.

Source: NWIP.EXE

Severity: ERROR

Explanation: The specified message file is invalid.

Action: Examine the reported path and name of the message file and then fix it.

Missing or invalid IPATCH values were specified on line *n* of the configuration file. Entry was ignored.

Source: NWIP.EXE

Severity: WARNING

Explanation: The IPATCH value specified in your NET.CFG file is invalid.

Action: Correct the IPATCH value specified in your NET.CFG file.

Missing or invalid value for *x* parameter was specified on line *n* of the configuration file.

Source: NWIP.EXE

Severity: WARNING

Explanation: A parameter value in your NET.CFG file is missing or incorrect.

Action: Examine the parameter on line *n* of the NET.CFG file. Add a value or correct the existing value.

NetWare/IP cannot be unloaded because interrupt *n* is owned by another program. Unload the other program and then unload NetWare/IP.

Source: NWIP.EXE

Severity: ERROR

Explanation: NetWare/IP cannot be unloaded because it cannot unhook the specified interrupt, which is currently hooked by another program.

Action: Unload the program that hooks the specified interrupt and then try to unload NetWare/IP again.

NetWare/IP cannot be unloaded because the installed NetWare/IP or IPXODI is a different version than this NetWare/IP module.

Source: NWIP.EXE

Severity: ERROR

Explanation: The memory resident NWIP or IPX is different than the NWIP.EXE in the load path.

Action: Find the NWIP.EXE that matches the memory-resident NWIP and then try unloading again.

NetWare/IP client is loaded but NOT ready since TCP/IP is NOT available.

Source: NWIP.EXE

Severity: INFORMATIONAL

Explanation: NetWare/IP is running in a deferred TCP/IP environment, which could be mobile or VxD/DLL-based TCP/IP.

Action: None required.

NWIPINIT cannot be executed by itself! Execute NWIP.EXE now.

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: NWIPINIT.EXE cannot be loaded and executed alone. It is implicitly loaded and executed by NWIP.EXE.

Action: Run NWIP.EXE.

The LSL is not loaded. Please load the LSL then NetWare/IP.

Source: NWIP.EXE

Severity: ERROR

Explanation: Your system attempted to load NWIP.EXE before loading LSL™ .

Action: Load LSL.COM now.

The loaded LSL is too old. LSL.COM must be v1.20 or higher.

Source: NWIP.EXE

Severity: ERROR

Explanation: Your system is using a version of LSL.COM prior to version 1.20.

Action: Load version 1.20 or higher of LSL.COM.

There is no local copy of the NetWare/IP parameters.

Source: NWIPINIT.EXE

Severity: WARNING

Explanation: The client was unable to obtain the global NetWare/IP parameters from the NetWare/IP server or DSS server and attempted to start up using its local copy of the global parameters. However, the client was unable to find the configuration information locally.

Action: Have your NetWare/IP administrator check that DNS, DSS, and NetWare/IP are running and are configured properly.

WARNING: Cannot resolve NWIP Domain <domain name>, check DNS/DSS configuration!

Source: NWIPINIT.EXE

Severity: ERROR

Explanation: The specified NetWare/IP domain is not resolvable using DNS queries.

Action: Make sure the NetWare/IP domain name is specified correctly in the [NWIP] section of your NET.CFG file. Have your system administrator check the configuration of the DSS and DNS servers.

Glossary

Bootstrap Protocol (BOOTP)

A standard means of supplying a computer on an IP network with address and other configuration information when the computer is booted. BOOTP servers enable the network administrator to manage IP address assignment from a single location.

Buffer

An area in workstation memory set aside to hold data temporarily.

DNS Client

Software that enables a workstation to query a DNS name server about the location of a host on the network.

DNS Domain

A group of networked computers under common DNS management. Domains can be determined by logical grouping rather than physical location.

DNS Name Server

A server that contains a database of information about hosts in one or more DNS domains and makes this information available to DNS clients, or resolvers, throughout the network.

Domain

A group of networked computers under common DNS management. Domains can be determined by logical grouping rather than physical location.

Domain Name System (DNS)

A standardized system that provides information about hostname and IP address mapping throughout an internetwork. DNS maintains this information in a decentralized distributed database.

Domain SAP/RIP Service (DSS)

A service on a NetWare/IP™ network that replaces IPX™ broadcast services. DSS servers maintain a database that provides NetWare/IP servers and clients with SAP/RIP information (service availability and routing) required by NetWare® applications.

Driver

A software module that manages the operation of a specific device or protocol and provides services to modules running above it. Drivers allow higher-level modules, such as applications, to be device- and protocol-independent (able to run on any device or protocol for which a driver is available).

Frame Type

Frame types determine how packets of network data are formatted on different LANs. Ethernet, token ring, ARCnet, and other LANs use different formats. The TCP/IP and IPX protocols also require different frame types in some instances.

Gateway

A system that transfers network data between different network types, translating the data between the two types as needed. For example, a NetWare/IP forwarding gateway passes NetWare traffic between IP and IPX segments, translating as needed between the two protocols.

Host

A networked computer.

Internet Protocol (IP)

An industry-standard suite of networking protocols that enables dissimilar nodes in a heterogeneous environment to communicate with one another.

Internetwork Packet Exchange™ (IPX)

A Novell communication protocol that sends data packets to requested destinations, such as servers and workstations. IPX addresses and routes outgoing data packets across a network. It reads the assigned addresses of incoming data and directs the data to the proper area of the workstation or server operating system.

IP Address

A 4-byte numeric value that specifies a particular network and node on that network. The standard format is dotted decimal, for example 1.2.3.4.

IP Router

A system that manages the exchange of information between TCP/IP networks. IP routers run special protocols that maintain information about the best way to transfer information among different networks, including hops across multiple networks.

IPX Network Number

A hexadecimal number used by IPX to uniquely identify a network cable segment or a NetWare server. Each NetWare/IP domain, consisting of many servers and clients, is assigned a single IPX network number for communication with IPX resources.

Link Support Layer™ (LSL™)

An intermediary between the system’s LAN drivers and communication protocols.

Master DNS

The name server that maintains the read/write database of name-to-address mappings for an administrative zone (domain). Each zone has a single DNS master.

Name Server

A system that maintains a DNS database of hostname and IP address mappings. Name servers respond to queries from servers and client workstations for host addresses.

NetBIOS (Network Basic Input/Output System)

A layer of software that links the network operating system with specific hardware using a generic networking Application Programming Interface (API) that can run over multiple transports or media.

NetWare DOS Requester™

The client software portion of NetWare 4. It replaces, and is compatible with, the NetWare shells used in previous NetWare versions.

NetWare/IP

A set of software modules that allows servers and workstations on TCP/IP networks to run NetWare. NetWare/IP replaces the traditional IPX transport with industry-standard TCP/IP, extends NetWare to TCP/IP networks, and can coexist with IPX NetWare.

NetWare/IP Domain

A DNS domain used to administer NetWare/IP servers and clients. The NetWare/IP domain is always a subdomain that has no lower-level domains in the DNS hierarchy.

NetWare/IP Driver

The interface between the TCP/IP protocol stack and the NetWare DOS Requester.

NetWare Tools™

Utilities that enable users to perform a variety of network tasks such as accessing network resources, mapping drives, setting up printing, and sending messages.

Network Board

A circuit board installed in workstations and servers to allow them to communicate on a network.

Node

Any networked computer. Nodes include both server and client systems.

Open Data-Link Interface™ (ODI™)

A set of specifications that defines the relationship between one or more protocol stacks, the Link Support Layer (LSL), and one or more Multiple Link Interface Drivers (MLIDs). These specifications allow multiple communication protocols, such as IPX/SPX and TCP/IP, to share the same driver and adapter.

Parent Domain

The next higher level domain in the DNS hierarchy. For example, the parent domain of nwip.acme.com. is acme.com. Parent domains delegate administrative authority and responsibility to lower-level domains.

Port

In TCP/IP, a well-known point of access to a service on a host computer. Certain ranges of port numbers are usually assigned to the same services by convention; other ranges are available for use as needed by applications.

Primary DSS Server

The DSS server that maintains the global configuration information for a NetWare/IP network. One primary DSS server is configured for each NetWare/IP domain.

Protocol

A formal description of message formats and the rules two or more machines must follow to exchange messages in those formats.

Protocol Stack

The software modules that take data from an application and transform or encapsulate it for transmission across a network. The stack may have several layers of modules. Each layer provides services to the layer above; each layer requests services from the layer below. Examples of protocol stacks are TCP/IP and IPX.

Replica DNS

A name server that maintains a read-only copy of the DNS master's database for a domain. DNS replicas are configured to off-load network traffic from the master and to ensure service if the master becomes unavailable.

Resolver

See DNS Client.

Router

A software and hardware connection between two or more networks, usually of similar design, that permits traffic to be routed from one network to another.

Routing Information Protocol (RIP)

An IPX protocol that propagates information about routes between nodes throughout an IPX internetwork.

Secondary DSS Server

An additional DSS server that supplements the primary DSS server and off-loads NetWare/IP traffic from it. Secondary DSS servers are configured on remote subnetworks to provide service locally in case the primary DSS server becomes unavailable.

Server

A node that provides services to other nodes on the network.

Service Advertising Protocol (SAP)

An IPX protocol that propagates service availability information on a NetWare internetwork.

Storage Management Services™ (SMS™)

A NetWare service that allows data to be backed up and retrieved from servers and workstations attached to the network. SMS is independent of both the backup and restore hardware and file systems (such as DOS, OS/2*, Windows, Macintosh*, or UNIX*).

Subnetwork Mask

The filter that separates subnetted IP addresses into network and local portions. Local systems will have a subnetwork mask in order to restrict broadcasts to the local network only.

TCP/IP Protocol Stack

An industry-standard suite of networking protocols that enables dissimilar nodes in a heterogenous environment to communicate with one another.

Transmission Control Protocol (TCP)

An industry-standard protocol that provides for reliable delivery of data over IP networks.

Unicode

An industry-standard 16-bit character representation scheme. Unicode allows you to represent the characters in multiple national languages using a single representation.

User Datagram Protocol (UDP)

An industry-standard protocol that provides for unverified delivery of data over IP networks.

Virtual Loadable Module™ (VLM™)

A modular executable program that runs at each NetWare workstation and enables communication with NetWare servers. These VLMs replace, and are compatible with, the NetWare shells used in previous NetWare versions.

Workstation

A node that requests services from other nodes on the network, but does not provide services to other nodes.