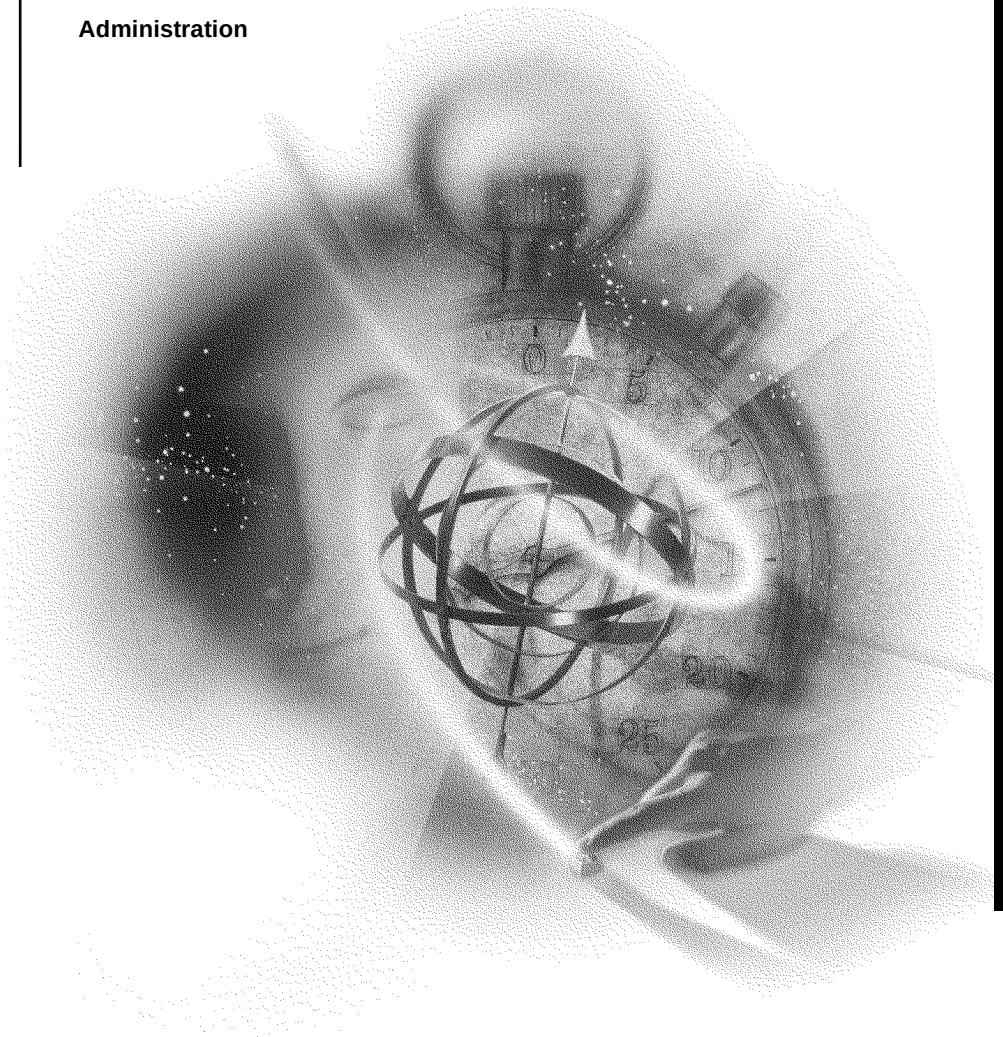
VERSION 5

DNS/DHCP

Administration



NetWare® 5™
NETWORK SOFTWARE

Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

export notice

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

trademarks

Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries.

A complete list of trademarks and their respective owners appears in “Trademarks” on page 143.

U.S. Patent Nos. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,594,863; 5,608,903; 5,633,931; 5,652,854; 5,671,414; 5,677,851; 5,692,129. U.S. and Foreign Patents Pending.

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

DNS/DHCP Administration
July 1998
104-000081-001

Contents

2 Planning

3 Setting Up

6 Troubleshooting

Trademarks

About This Guide

The purpose of this document is to describe the concepts of the Domain Naming System (DNS) and the Dynamic Host Configuration Protocol (DHCP), the setup and configuration of these functions, and how to use Novell DNS/DHCP Services in NetWare 5.

The audience for this document is network administrators. This documentation is not intended for users of the network.

chapter 1

Understanding

This document describes the NDS™ schema extension, the Domain Name System (DNS), and the Dynamic Host Control Protocol (DHCP) server, and it explains their NDS-related functions. This chapter also provides information about the DNS/DHCP Management Console.

Overview of DNS/DHCP Services

Novell® DNS/DHCP Services in NetWare 5 integrates the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) into the NDS™ database. Integrating these services into NDS provides centralized administration and enterprise-wide management of network (IP) addresses, configuration, and hostnames.

The DNS/DHCP Management Console is a Java application that provides a graphical user interface to manage the objects created to support DNS and DHCP. The DNS/DHCP Management Console can function as a standalone utility, or it can be accessed from the Tools menu of the NetWare® Administrator utility.

Note: In this document, the term *host* refers to a network device that requires an IP address and might have a hostname.

For more overview information, refer to:

- "DNS" on page 2
- "DHCP" on page 5
- "DNS/DHCP Management Console" on page 8

DNS

The DNS software in Novell DNS/DHCP Services integrates DNS information into the NDS database. Previously, DNS used Btrieve* as its database for configuration information. Integrating DNS with NDS moves all the information currently held in Btrieve files into NDS.

You can use the DNS/DHCP Management Console to configure DNS from the desktop of a client where it is installed, or DNS can be launched from the NetWare Administrator utility.

Integrating DNS with NDS greatly simplifies the task of network administration by enabling you to enter all configuration information into one distributed database. Furthermore, the DNS configuration information is replicated just like any other data in NDS.

Integrating DNS with NDS also enables an update interaction between DNS and DHCP through the Dynamic DNS (DDNS) feature. When a host is assigned an IP address by DHCP, the DNS information can be automatically updated to associate the hostname with the new address when the DDNS feature is active.

By integrating DNS into NDS, Novell has shifted the concept of a primary or secondary zone away from the server to the zone itself. Once you have used the configuration utility to configure the zone, the data is available to any of the Novell DNS servers you choose to make authoritative for the zone. The Novell DNS server takes advantage of the peer-to-peer nature of NDS by replicating the DNS data.

Novell DNS/DHCP Services interoperates with other DNS servers. The Novell DNS server can act as either a master DNS server or a secondary DNS server in relation to non-Novell DNS servers. The Novell DNS server can act as the master DNS server and transfer data to non-Novell secondary servers. Alternatively, one Novell DNS server can act as a secondary DNS server and transfer data in from a non-Novell master server. All Novell DNS servers can then access the data through NDS replication.

Novell DNS/DHCP Services provides the following DNS features:

- All DNS configuration is done in NDS, facilitating enterprise-wide management.
- A Novell DNS server can be a secondary name server to another zone (DNS data loaded into NDS through a zone transfer), or it can be a primary name server (on which you configure DNS data using the DNS/DHCP Management Console).
- DNS data can be read in from a BIND Master file to populate NDS for convenient upgrades from BIND implementations of DNS.
- DNS data can be exported from NDS into BIND Master file format.
- Root server information is stored in NDS and shared by all NDS-based DNS servers.
- Zone transfers are made to and from NDS through Novell servers and include interoperability with non-NDS-based DNS.
- A Novell DNS server can be authoritative for multiple domains.
- Novell DNS servers maintain a cache of data from NDS so they can respond to queries quickly.
- A Novell DNS server can act as a caching or forwarding server instead of an authoritative server for zones.
- Novell DNS/DHCP Services supports multihoming.
- Novell DNS/DHCP Services software supports round-robin process of responses to queries with multiple Address records (A records) for a domain name.

The DNS software in Novell DNS/DHCP Services conforms to BIND 4.9.5 and supports the standards of the Internet Request For Comments (RFCs) in the following list:

- RFC 819—Domain Naming Convention for Internet User Applications
- RFC 920—Domain Requirements
- RFC 974—Mail Routing and Domain System
- RFC 1032—Domain Administrator's Guide
- RFC 1033—Domain Administrator's Operations Guide
- RFC 1034—Domain Names - Concepts and Facilities
- RFC 1035—Domain Names - Implementation and Specification
- RFC 1036—Standard Interchange of USENET Messages
- RFC 1101—DNS Encoding of Network Names and other Types
- RFC 1122—Requirements for Internet Hosts - Communications Layers
- RFC 1123—Requirements for Internet Hosts - Application and Support
- RFC 1183—New DNS RR Definitions
- RFC 1535—A Security Problem and Proposed Correction with Widely Deployed DNS Software
- RFC 1536—Common DNS Implementation Errors and Suggested Fixes
- RFC 1537—Common DNS Data File Configuration Errors
- RFC 1591—Domain Name System Structure and Delegation
- RFC 1597—Address Allocation for Private Internets

- RFC 1627—Network 10 Considered Harmful (Some Practices Shouldn't Be Codified)
- RFC 1713—Tools for DNS Debugging
- RFC 1884—IP Version 6 Addressing Architecture
- RFC 1886—DNS Extensions to Support IP Version 6
- RFC 1912—Common DNS Operations and Configurations Errors
- RFC 2010—Operations Criteria for Root Name Servers
- RFC 2052—A DNS RR for Specifying the Location of Services (DNS SRV)

DHCP

A NetWare 5 DHCP server automatically assigns IP addresses and other configuration information to clients upon request or when the clients are restarted. Automatic assignment of configuration information reduces the amount of work required to configure and manage a large IP network.

Furthermore, integrating DHCP with NDS enables you to enter all configuration information into one distributed database. This greatly simplifies network administration and provides for the replication of DHCP configuration information.

DHCP provides for both static and dynamic configuration of IP clients. Static configuration enables you to assign a specific IP address and configuration to a client with a specific MAC address. When DHCP assigns IP addresses dynamically, IP clients are assigned an IP address that is chosen from a range of available addresses. You can use dynamic address assignment when you are not concerned about which IP address a particular client uses. Each IP client that requests an address assignment can also use the other DHCP configuration parameters.

DHCP can limit the amount of time a DHCP client can use an IP address. This is known as the *lease time*. You can use the lease time to allow a large number of clients to use a limited number of IP addresses.

DHCP is based on BOOTP and maintains some backward compatibility. Novell DHCP servers can be configured to respond to requests from BOOTP clients.

Novell DNS/DHCP Services provides the following DHCP features:

- All DHCP configuration is done in NDS, facilitating enterprise-wide management.
- DHCP options can be set at three levels:
  - Enterprise level
  - Subnet level
  - Specific client level
- The configuration utility has import/export functions that support
  - Populating NDS from an existing Novell DHCP Server 2.0 DHCPTAB file or from a BOOTPTAB file (for Novell BOOTP)
  - Saving configuration out of NDS
- You can configure the level of SNMP event trap generation using the DNS/DHCP Management Console for all events, major events only, or no events.
- Client assignment policy options (to support mobile clients that move around the network) include
  - Allow Duplicate
  - Delete Duplicate
  - No Duplicate
- You can use the DNS/DHCP Management Console to maintain a hardware exclusion list to deny service to *unwanted* devices by their MAC addresses.
- The DHCP software updates NDS to record all address assignments to LAN clients.

- You can use Dynamic DNS (DDNS) to update DNS with information about addresses assigned and rescinded.
- The DHCP software enables the server to cache addresses and other configuration information from NDS for quick response.
- The DHCP software has one DHCP server NetWare Loadable Module™ (NLM™) file that supports both LAN and remote access clients.
- You can configure the DHCP server to ping an address to verify that no other device is using it before assigning the address to a client.
- Provides fault tolerance as follows:
  - A server can survive a temporary local NDS service outage and recover automatically.
  - DHCP configuration is replicated like other NDS data.
- DHCP auditing can help diagnose problems. Each incidence of address deletion, addition, and rejection is recorded.

Novell DNS / DHCP Services supports the features that were previously provided by Novell DHCP Server 2.0 and supports the standards of the RFCs in the following list:

- RFC 2131—Dynamic Host Configuration Protocol
- RFC 2132—DHCP Options and BOOTP Vendor Extensions
- RFC 2241—DHCP Options and Novell Directory Services
- RFC 2242—NetWare / IP Domain Name and Information

Novell DNS / DHCP Services also supports the BOOTP standards of the RFCs in the following list:

- RFC 1497—BOOTP Vendor Information Extensions
- RFC 1534—Interoperation Between DHCP and BOOTP

- RFC 1542—Clarifications and Extensions for the Bootstrap Protocol

Refer to “DHCP Options” on page 34 for a list of all supported DHCP options.

DNS/DHCP Management Console

The DNS/DHCP Management Console is a Java-based user interface used to configure and manage NDS-based DNS and DHCP. NDS is used as a database to store the administered IP address and name service objects.

The DNS/DHCP Management Console is an independent executable Java application that can be launched from a Windows 95* or Windows NT* client on which Novell Client software delivered with NetWare 5 has been installed. Future plans call for the DNS/DHCP Management Console to be platform-independent, able to run on other non-PC platforms, such as UNIX* and Macintosh.*

For more detailed information about the DNS/DHCP Management Console, refer to “Understanding the DNS/DHCP Management Console” on page 43.

Understanding the NDS Schema Extension

After the Novell® DNS/DHCP Services software has been installed and loaded, the NDS schema must be extended. The NDS schema extension defines additional objects needed for DNS and DHCP.

For more information, refer to:

- “DNS/DHCP Global NDS Objects” on page 9
- “New NDS Objects for DNS” on page 10
- “NDS Objects for DHCP” on page 13

DNS/DHCP Global NDS Objects

When you select Novell DNS/DHCP Services during NetWare 5 installation, the NDS schema is extended to enable the creation of DNS and DHCP objects, and the following objects are created:

- DNS/DHCP Locator object
- DNS/DHCP Group object
- RootSrvrInfo Zone

Only one copy of these objects exist in an NDS tree. The DNS servers, DHCP servers, and DNS/DHCP Management Console must have access to these objects.

The DNS/DHCP Group object is a standard NDS group object. The DNS and DHCP servers gain the rights to DNS and DHCP data within the tree through the Group object. When the DNS/DHCP Management Console is used to create DNS and DHCP servers, the servers have the rights required to access data.

The DNS/DHCP Locator object contains global defaults, DHCP options, and lists of all DNS and DHCP servers, subnets, and zones in the tree. The DNS/DHCP Management Console can display these objects without having to search the tree by using the Locator object. The Locator object is basically hidden by the DNS/DHCP Management Console.

The RootSrvrInfo Zone is a Zone object, an NDS container object, that contains resource record sets for the DNS root servers. The resource record sets contain Address records and Name Server records that provide pointers for DNS queries to the root servers. The RootSrvrInfo Zone object is the equivalent of the BIND *db.root* file.

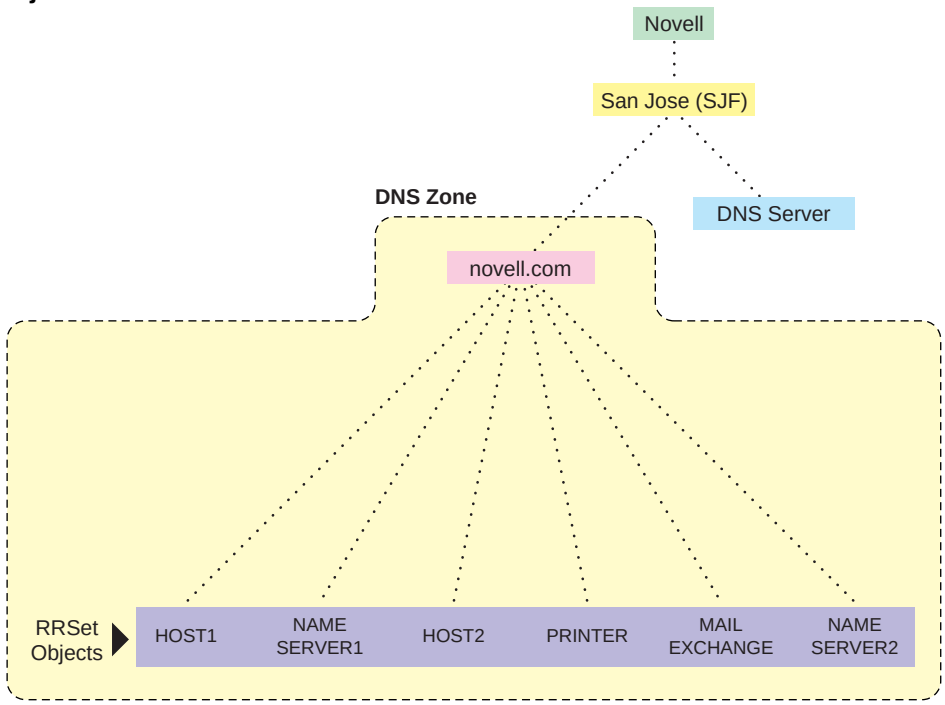
New NDS Objects for DNS

The following new NDS objects support DNS:

- DNS Zone object
- DNS Resource Record Set object
- DNS Name Server object

Figure 1-1 shows an example of a tree of DNS objects.

Figure 1-1
NDS Objects for DNS



DNS Zone Object

The DNS Zone object is a container object that contains all the data for a single DNS zone. A Zone object is the first level of the DNS zone description. A zone object can be contained under an Organization (O), Organizational Unit (OU), a Country (C), or a Locality (L).

Multiple DNS domains can be represented within NDS by using separate, independent DNS Zone objects. A network administrator can support multiple DNS domains on a single NetWare® server by creating multiple DNS Zone objects and assigning the server to serve those zones.

The DNS Zone object contains data that correlates to a DNS Start of Authority (SOA) resource record (RR), a member list of all NDS-based DNS servers that serve the zone, and Dynamic DNS (DDNS) server information.

The DNS name space hierarchy is not represented within the NDS hierarchy. A zone and its child zone might appear as peers within the NDS hierarchy, even though they have a parent-child relationship within the DNS hierarchy.

DNS Resource Record Set Object

The DNS Resource Record Set (RRSet) object is an NDS leaf object contained within a DNS Zone object. An RRSet object represents an individual domain name within a DNS zone. Its required attributes are a DNS domain name, a DNS address class, and a Time-to-Live (TTL) record.

Each domain name within a DNS zone object has an RRSet object. Each RRSet object has one or more resource records beneath it containing additional information about the domain, including a description of the object and version information.

DNS Resource Records

A DNS resource record(RR) is an attribute of an RRSet that contains the resource records type and data of a single RR. RRs are configured beneath their respective RRSet objects. Resource records describe their associated RRset object.

The most common resource records are Address (A) records, which map a domain name to an IP address, and Pointer (PTR) records, which map an IP address to a domain name within an IN-ADDR.ARPA zone.

DNS Server Object

The DNS Server object (or Service object) is different from the NetWare Core Protocol™ (NCP™) Server object. A DNS Server object can be contained in an Organization (O), Organizational Unit (OU), Country (C), or Locality (L). The DNS Server object contains DNS server configuration parameters, including the following:

- Zone List
- DNS Server IP Address
- Domain Name of the DNS Server
- DNS Server Options
- Forwarding List
- No Forwarding List

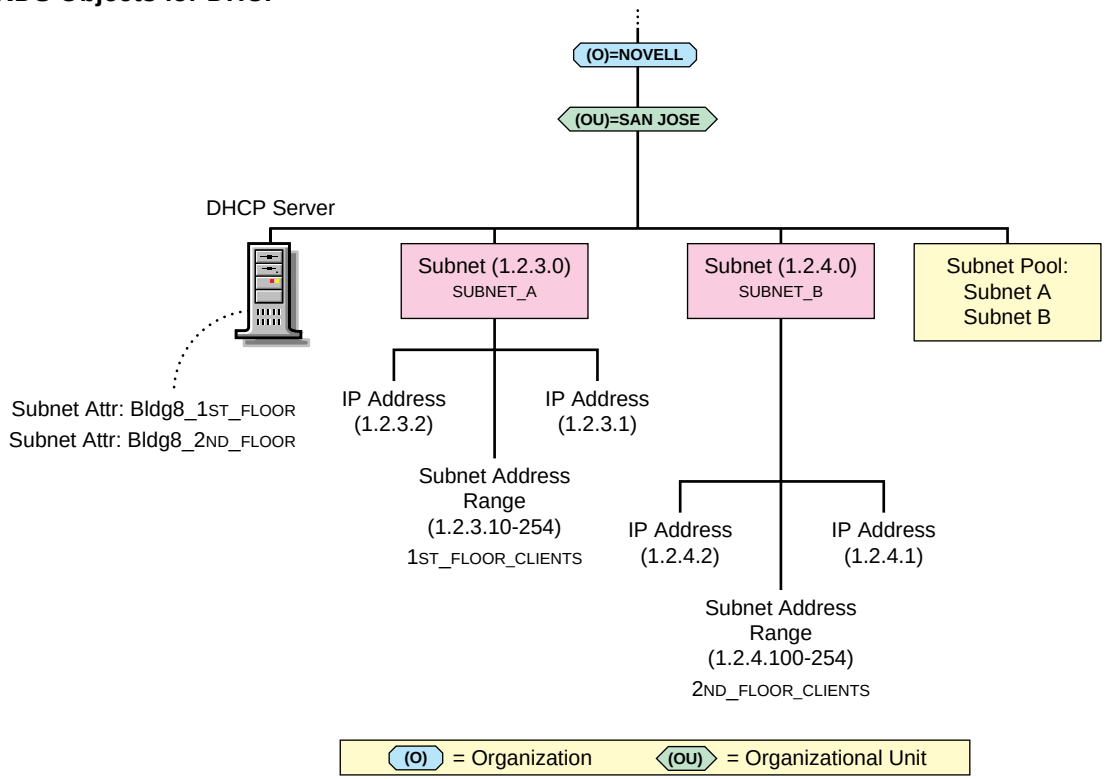
NDS Objects for DHCP

The following new NDS objects support DHCP:

- Subnet object
- Address Range object
- IP Address object
- DHCP Server object
- Subnet Pool object

Figure 1-2 shows a basic configuration of the DHCP objects. This structure might be used for a small to medium size network.

Figure 1-2
NDS Objects for DHCP



Subnet Object

The Subnet object represents a subnet and is the most fundamental DHCP object. The Subnet object can be contained in an Organization (O), an Organizational Unit (OU), a Country (C), or a Locality (L). The Subnet object acts as a container object for the IP Address and Address Range objects. A Subnet object's specific DHCP options and configuration parameters apply to the entire subnet and override global options.

Address Range Object

The Address Range object is primarily used to denote a range of addresses to create a pool of addresses for dynamic address assignment or to identify a range of addresses to be excluded from address assignment. Optionally, the Address Range object stores the start of a hostname that can be assigned to clients when addresses are assigned.

You can use multiple address range objects under a subnet object. You can also specify different range types, such as a range for dynamic address assignment, a range for BOOTP clients, or a range to be excluded from the subnet.

IP Address Object

The IP Address object represents a single IP address. The IP Address object must include an address number and an assignment type. The address can be assigned manually, automatically, or dynamically, or it can be excluded from DHCP address assignment.

You must use the DNS/DHCP Management Console to configure IP Address objects that are manually assigned or excluded from assignment. For dynamically or automatically assigned client addresses, DHCP creates an IP Address object under the subnet where the address is assigned.

An IP address can be assigned to a client based on the client's MAC address. These IP Address objects can also receive specific DHCP options.

When configuring an individual IP Address object, you can provide specific options that override global options or those set at the subnet level. When you create or modify an IP Address object manually, you can also create the necessary DNS resource records.

DHCP Server Object

The DHCP Server object represents the DHCP server and contains a multivalued attribute listing of the subnet ranges the DHCP server is servicing. The DHCP server also contains all server-specific configuration and policy information. A DHCP Server object can be contained in an O, OU, C, or L.

Subnet Pool Object

The Subnet Pool object provides support for multiple subnets through a DHCP or BOOTP forwarder by identifying a pool of subnets for remote LAN address assignments. A Subnet Pool object can be contained in an O, OU, C, or L.

DHCP servers are not required to be on the local subnet to which they assign addresses. If desired, they can be deployed centrally and service remote subnets. Initial DHCP/BOOTP DISCOVER requests, however, are not sent to a DHCP server unless a DHCP/BOOTP forwarder that is local to the client has been configured to forward the addresses.

The Subnet Pool object contains a list of subnet object references and comments.

Understanding DNS

The Domain Name System (DNS) is a distributed database system that provides hostname-to-IP resource mapping (usually the IP address) and other information for computers on an internetwork. Any computer on the Internet can use a DNS server to locate any other computer on the Internet.

DNS is made up of two distinct components, the hierarchy and the name service. 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.

For more information, refer to:

- "DNS Hierarchy" on page 16
- "DNS Name Service" on page 20
- "Traditional DNS" on page 24
- "DNS within NDS" on page 26

DNS Hierarchy

DNS uses a hierarchy to manage its distributed database system. The DNS hierarchy, also called the domain name space, is an inverted tree structure, much like NDS.

The DNS tree has a single domain at the top of the structure called the root domain. A period or dot (.) is the designation for the root domain. Below the root domain are the top-level domains that divide the DNS hierarchy into segments.

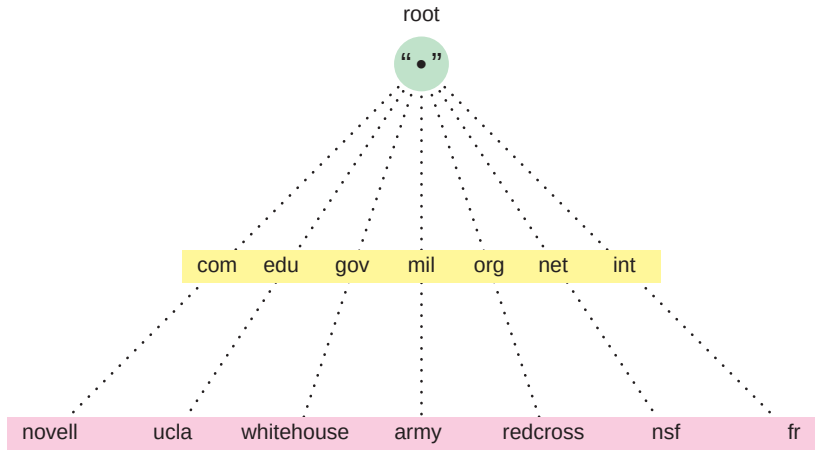
Table 1-1 lists the top-level DNS domains and the types of organizations that use them. Below the top-level domains, the domain name space is further divided into subdomains representing individual organizations.

Table 1-1
Top-Level DNS Domains

Domain	Used by
.com	Commercial organizations, as in novell.com
.edu	Educational organizations, as in ucla.edu
.gov	Governmental agencies, as in whitehouse.gov
.mil	Military organizations, as in army.mil
.org	Nonprofit organizations, as in redcross.org
.net	Networking entities, as in nsf.net
.int	International organizations, as in nato.int

Additional top-level domains organize domain name space geographically. For example, the top-level domain for France is fr. Figure 1-3 illustrates the DNS hierarchy.

Figure 1-3
DNS Hierarchy



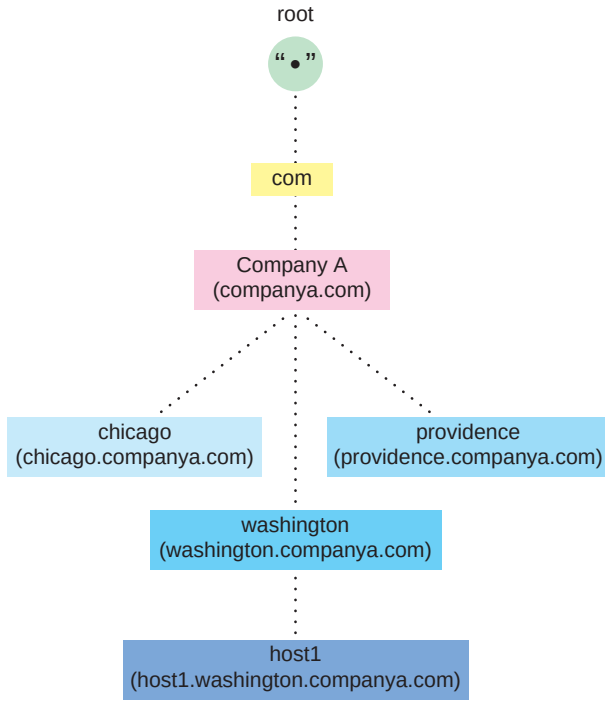
Domains and Subdomains

A domain is a label of the DNS tree. Each node on the DNS tree represents a domain. Domains under the top-level domains represent individual organizations or entities. These domains can be further divided into subdomains to ease administration of an organization's host computers.

For example, Company A creates a domain under the *.com* top-level domain called companya.com. Company A has separate LANs for its locations in Chicago, Washington, and Providence. Therefore, the network administrator for Company A decides to create a separate subdomain for each division, as shown in Figure 1-4.

Any domain in a subtree is considered part of all domains above it. Therefore, chicago.companya.com is part of the companya.com domain, and both are part of the .com domain.

Figure 1-4
Domains and Subdomains



Domain Names

The domain name represents an entity's position within 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. For example, the domain name for the Providence domain within Company A is providence.companya.com, as shown in Figure 1-4 and the list below.

Note that the domain names in the figure end in a period, representing the root domain. Domain names that end in a period for root are called fully qualified domain names (FQDNs).

Each computer that uses DNS is given a DNS hostname that represents the computer's position within the DNS hierarchy. Therefore, the hostname for host1 in Figure 1-4 is host1.washington.companya.com.

Domain Delegation

Domain delegation gives an organization authority for a domain. Having authority for a domain means that the organization's network administrator is responsible for maintaining the DNS database of hostname and address information for that domain.

A group of domains and subdomains for which an organization has authority is called a zone. All host information for a zone is maintained in a single, authoritative database.

For example, the companya.com. domain is delegated to CompanyA, creating the companya.com. zone. There are three subdomains within the companya.com. domain:

- chicago.companya.com.
- washington.companya.com.
- providence.companya.com.

The CompanyA administrator maintains all host information for the zone in a single database and also has authority to create and delegate subdomains.

For example, CompanyA's Chicago location has its own network administrator. The companya.com administrator delegates the chicago.companya.com zone to the Chicago location and no longer has authority over it. CompanyA now has two zones: companya.com and chicago.companya.com.

- companya.com, which has authority over companya.com, washington.companya.com, and providence.companya.com zones
- chicago.companya.com, which has authority over the chicago.companya.com zone

IN-ADDR.ARPA Domain

The IN-ADDR.ARPA domain (or zone) provides mapping of IP addresses to names within a zone, enabling a client (or resolver) to request a hostname by providing an IP address. Some security-based applications require this function, also known as *reverse-lookup* .

The file that stores the IN-ADDR.ARPA data is made up of Pointer records and additional name server records, including Start of Authority (SOA) records, similar to other DNS zone files. Within the IN-ADDR.ARPA zone file, IP addresses are listed in reverse order, and *in-addr.arpa* is appended to the address. A query for a host with an IP address of 1.2.3.4 would require a PTR query with the target address of 4.3.2.1.in-addr.arpa.

DNS Name Service

DNS uses the name service component to provide the actual name-to-IP address mapping that enables computers to locate each other on an internetwork. The name service uses a client-server mechanism in which clients query name servers for host address information.

Name Servers

DNS name servers maintain a database of information about hosts in a specific zone. Each DNS zone must include a name server containing authoritative information about all hosts within the zones it supports. A DNS name server can be either a primary name server or a secondary name server.

In addition to local host information, name servers maintain information about how to contact other name servers. 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, the name server relays the request to other name servers up or down the domain hierarchy until it receives an authoritative answer for the client's query.

Primary Name Servers

One DNS name server in each administrative zone maintains an authoritative database of hostname and address information for an entire domain. This name server is the primary name server, and the domain administrator updates it with hostnames and addresses as changes occur.

All name servers maintain information about how to contact name servers that are at higher or lower levels within the DNS hierarchy. The process of maintaining information about name servers in higher-level domains is called *linking to the existing DNS hierarchy*. The administrator also enters information into the database about name servers in lower-level domains when he or she creates a subdomain.

Secondary Name Servers

Secondary name servers have read-only copies of the primary name server's DNS database. Secondary name servers provide redundancy and load balancing for a domain.

Periodically, and when a secondary name server starts up, it contacts the primary name server and requests a complete copy of the primary name server's DNS database. This process is called a *zone transfer*.

If necessary, a primary name server can also function as a secondary name server for another zone.

Resource Records

Resource records (RRs) contain the host information maintained by the name servers and make up the DNS database. Different types of records contain different types of host information. For example, an Address record provides the name-to-address mapping for a given host, while a Start of Authority (SOA) record specifies the start of authority for a given zone.

A DNS zone must contain several types of resource records for DNS to function properly. Other RRs can be present, but the following records are required for standard DNS:

- Name server (NS)—Binds a domain name with a hostname for a specific name server

  The DNS zone must contain NS records for each primary and secondary name server in the zone. The DNS zone must contain NS records to link the zone to higher- and lower-level zones within the DNS hierarchy.

- 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.

- Canonical name (CNAME)—Specifies the canonical or primary name for the owner. The owner name is an alias.

- Address (A)—Provides the IP address for the zone.

For example, the name server for a zone must contain the following:

- An SOA record identifying its zone of authority
- An NS record for the primary name server within the zone
- An NS record for each secondary name server within the zone

- An A record that maps each name server specified in the NS records to an IP address

Table 1-2 lists the types of resource records and their field differences.

Table 1-2
Resource Record Types and Field Differences

RR Type	Field Differences
A	IP Address, NDS context, comments, and version
AAAA	IPV6 address
AFSDB	Sub-type and hostname fields
CNAME	Domain name of aliased host
HINFO	CPU and OS fields of up to 256 characters each
ISDN	ISDN address and subaddress fields
MB	Mailbox address domain name
MG	Mail group member domain name
MINFO	Responsible mailbox and error message mailbox
MR	Mail rename mailbox
MX	Reference and exchange fields
NS	DNS server domain name
PTR	Domain name
PX	Preference, Map 822 (domain name), and Map x400 fields (domain name in X.400 syntax)
RP	Responsible person's mailbox and TXT RR domain name
RT	Preference and Intermediate fields
SRV	Service, proto, priority, weight, port, and target fields
TXT	Text field for up to 256 characters in multiple strings
WKS	Protocol and bit map fields

RR Type	Field Differences
X25	PSDN address

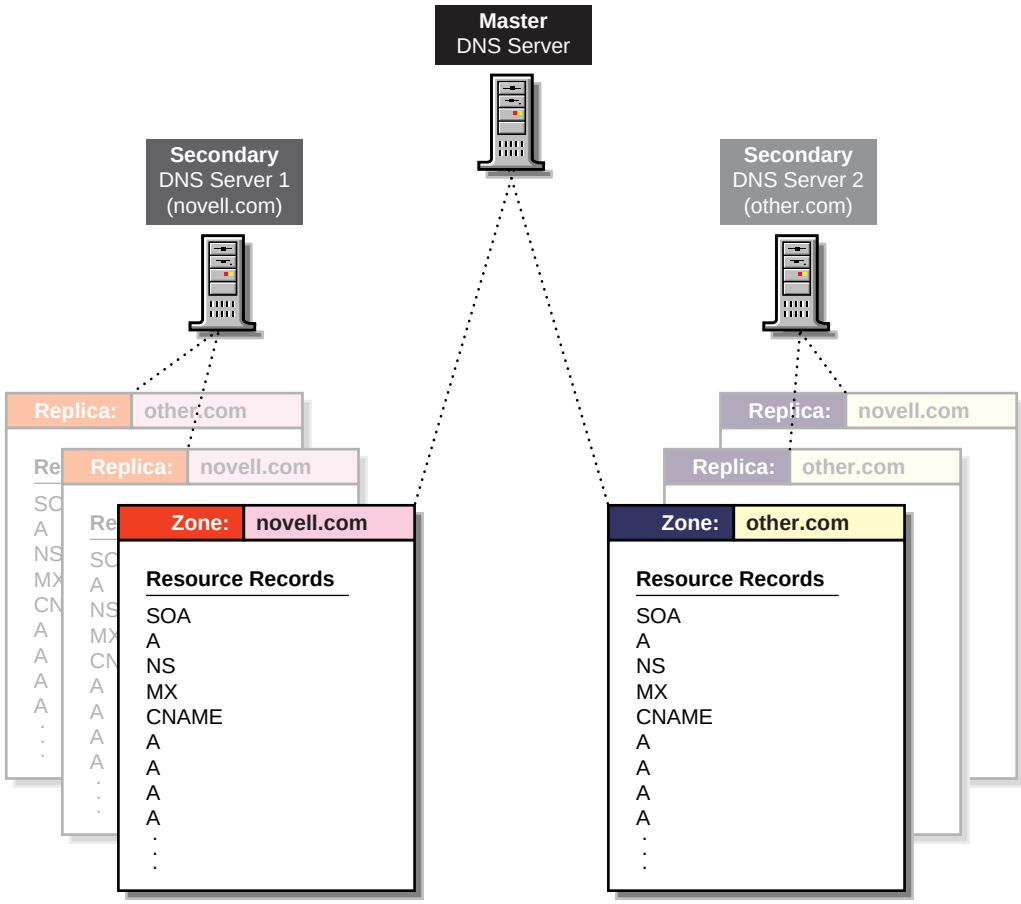
Traditional DNS

In the past, DNS has been administered by building a database of information that includes all of a zone's resource records into a textual file. Novell's earlier support of DNS used Btrieve as its database. Other vendors also use large files to store the information required for a DNS zone. The administration of these files is difficult and cumbersome.

Figure 1-5 represents a traditional DNS strategy. A zone, such as novell.com, would have a master DNS server handling queries about the entities within it. A DNS server might support more than one zone, and it would probably have at least one secondary server for backup (redundancy) or load-sharing purposes. The master DNS server provides DNS name service for two zones: novell.com and other.com. The secondary DNS server provides backup support for the novell.com zone, and the other secondary DNS server provides backup support for the other.com zone.

Additionally, each name server maintains separate copies of the zone data for primary and secondary support. When changes occur, all of these files require updating with zone transfers, which greatly increases network bandwidth use.

Figure 1-5
Traditional DNS Structure



The file storing the RRs for a zone might have hundreds or thousands of entries for different types of resources, such as users' addresses, hosts, name servers, mail servers, and pointers to other resources.

When a client initiates a request to resolve a domain name to an IP address (perhaps by using an Internet browser or by sending e-mail), the client sends a query to the name server specified in the client's configuration. The name server that receives the query will search its authoritative zone information for the desired record. If the record cannot be found, the name server will forward the query up the hierarchy to the name server above it for resolution.

When updates are made to the master name server, the entire contents of the database file must be copied to any secondary name servers.

DNS within NDS

Novell has integrated DNS into NDS by extending the NDS schema and creating new NDS objects to represent zones, RRSets, and DNS name servers. Integrating these new objects into NDS simplifies the administration of DNS, enabling centralized administration and configuration.

A Zone object is an NDS container object that holds RR Set objects, which are leaf objects. A DNS Server object is a leaf object. For detailed information about these objects, refer to “New NDS Objects for DNS” on page 10

By integrating DNS into NDS, Novell has shifted away from the traditional concept of primary or secondary DNS name servers to the concept of a *primary or secondary zone*.

In traditional DNS, all configuration changes are made on a single primary name server. When changes have been made, the secondary name servers request transfers of the changes from the primary name server. This process is called a *zone transfer*. The master-slave approach has several disadvantages, the most significant being that all changes must be made at the primary server.

Using the primary and secondary zone concept, Novell’s approach allows changes from anywhere in the network through NDS, which is not dependent on one server. Zone data is stored within NDS and is replicated just like any other data in the NDS tree.

Novell’s DNS supports the traditional primary-secondary DNS name server approach to moving DNS data in and out of NDS. Although all Novell servers can recognize DNS data after the data is placed in the directory through NDS replication, only one server is required for a zone transfer. The server assigned to perform this function in a secondary zone is called the *Zone In DNS server*.

In a secondary zone, the Zone In server is responsible for requesting a zone transfer of data from the external primary name server. The Zone In server determines which data has changed for a zone and then makes updates to NDS so that other servers are aware of the changes.

The *Designated DNS* (DDNS) server is a server identified by the network administrator to perform certain tasks for a primary zone. The DDNS server for a primary zone is the only server in that zone that receives DNS updates from a NetWare 5 DHCP server to perform Dynamic DNS (DDNS) updates. These updates cause additions and deletions of resource records and updates to the zone's serial number.

Figure 1-6 illustrates a Novell server as the primary DNS name server and primary and secondary zones within NDS. In this example, there are two primary zones. Any of the Novell DNS servers assigned to a zone are able to respond to queries for the zone. For each zone, one server is designated by the administrator to act as the DDNS server. In this example, Server1 is the Designated DNS server for Zone 1 and Server3 is the Zone In server for the secondary zone called Foreign Zone. Server 2 provides DNS services for Zone 1 and Zone 2, but does not perform DDNS updates or zone transfers. Server 3 occasionally requests zone transfers from the foreign server and places the modified zone data into NDS, where any of the Novell servers can respond to queries for it.

Figure 1-6

Novell Server As a Primary DNS Server

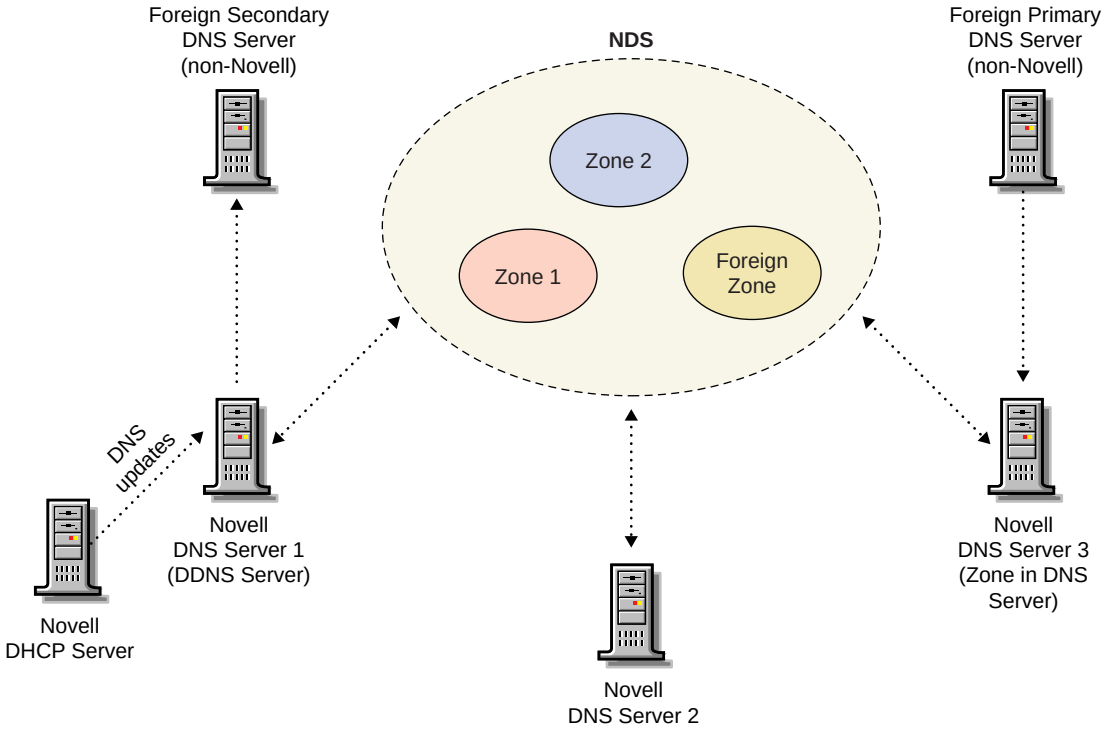
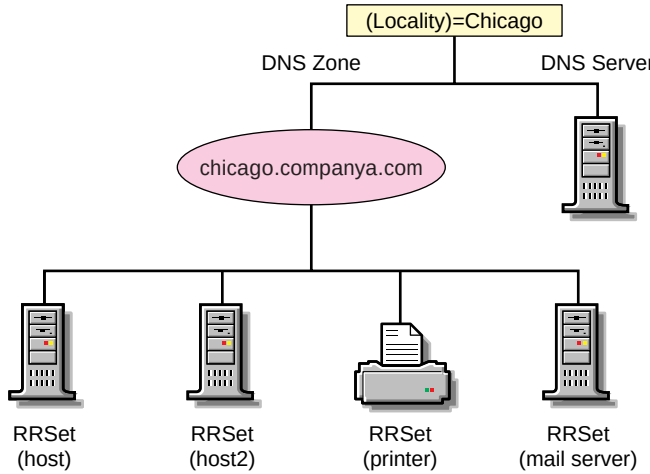


Figure 1-7 shows a representation of NDS objects within a DNS zone.

Figure 1-7

DNS Zone



DNS Master File

A DNS master file contains resource records that describe a zone. When you use the DNS/DHCP Management Console to build a zone, the DNS objects and their attributes translate into resource records for that zone.

You can use the DNS/DHCP Management Console to import a DNS master file if it conforms to IETF RFCs 1035, 1036, and 1183 and is in BIND master file format. A sample DNS master file is shown in the following example.

```
$ORIGIN sjf.novell.com.
@       soa sjfns.sjf.novell.com. Smith.novell.com (
     1996091454 3600 300 604800 86400   )
    ns  sjfns.sjf.novell.com.
    ns  ns.novell.com.
    mx  5 sjf-mx.idz.sjf.novell.com.
$ORIGIN sjf.novell.com.
sjfns   a   123.45.67.89
bsmith  a   123.45.68.103
; End of file
```

Understanding DHCP

The Dynamic Host Configuration Protocol (DHCP) uses a client-server structure to provide configuration parameters to hosts. DHCP consists of a protocol for providing host-specific configuration parameters from a DHCP server (or collection of DHCP servers) to a host and a mechanism to allocate network addresses to a host.

Note: In this document, the term *host* refers to a network device that requires an IP address and might have a hostname.

When the DHCP server is loaded, it reads its configuration information from NDS and stores the information in its cache. As the DHCP server assigns addresses to clients, it updates NDS, adding IP address objects or modifying their NDS status information. The DHCP server can be configured to maintain an audit log of this activity. For information about maintaining an audit log of DHCP server activity, refer to “Configuring DHCP Auditing” on page 107

The network administrator can use the DNS/DHCP Management Console to view objects to see how addresses have been assigned.

For more information, refer to:

IP Address Allocation

Allocation of IP addresses, either temporary or permanent, is one of the two primary services provided by DHCP. Basically, the client requests an IP address, and the DHCP server (or collection of DHCP servers) provides an address and guarantees not to give that address to another client within a specified time. Additionally, the server tries to return the same address to the client each time the client requests an address. The period of time over which an IP address is allocated to a client is called a *lease*.

DHCP supports three methods of IP address allocation:

- Dynamic BOOTP allocation
- Dynamic DHCP allocation
- Manual (or static) allocation

A network can use one or more of these methods. The network administrator decides which methods to use.

Dynamic BOOTP Allocation

Dynamic BOOTP enables a DHCP server to assign permanent addresses to BOOTP clients from a pool of addresses. No manual configuration of the client is required prior to address allocation.

Dynamic DHCP Allocation

Dynamic DHCP allocation is the only method enabling automatic reuse of addresses no longer required by a client. Dynamic DHCP allocation is useful for assigning an address to a client that will be connected temporarily to the network or for sharing a limited number of IP addresses among a group of clients that do not require permanently assigned IP addresses.

Dynamic DHCP allocation is also useful for assigning an IP address to a new client installed on a network on which IP addresses are scarce and must be reclaimed when older hosts are removed. An additional benefit to dynamic DHCP allocation is that when a client's lease is renewed, the DHCP server refreshes the client's configuration.

Manual Allocation

Manual or static allocation enables a network administrator to use the DNS/DHCP Management Console to assign addresses to DHCP or BOOTP clients. A specific IP address is assigned to the client based on an identifier such as the client's hardware or MAC address.

Manual allocation of DHCP eliminates the error-prone method of manually configuring hosts with IP addresses in networks for which IP address management outside a DHCP mechanism is desired. Manual allocation can be permanent or set to expire at a future time. When you perform manual allocation, you can also create corresponding DNS Resource Records, thereby eliminating another error-prone activity.

Lease Options

A client acquires a lease for a fixed period of time. The length of the lease could be a number of hours or days, or it could be for an indefinite period.

After having been granted a lease for an IP address, a client can issue a request to extend its lease. The client can also issue a message to the server to release the address back to the server when the address is no longer required.

If a network has a scarcity of IP addresses and must reassign them, the DHCP server will reassign an address when the lease has expired. The server uses configuration information to choose addresses to reuse. For example, the server might choose the least recently assigned address for reassignment. After receiving an address assignment, the host determines whether the address is in use by another host before accepting the address.

Note: Address duplication sometimes occurs with Windows 95 clients If a Windows 95 client receives a response indicating that the assigned address is in use by another device, a message is displayed indicating the IP address conflict. However, the client does not send a DHCPDECLINE message as required by RFC 1534, section 4.4.1.

To minimize the chance of address duplication, the DHCP server can be configured to ping an address to test its validity prior to assigning it to a host. If the server receives a response from another device (indicating ownership of the address), the current address assignment is withdrawn so that another address can be assigned to the host.

Managing the Database

The Lease Time attribute of the Subnet object enables a dynamic DHCP client to specify a lease time for the entire subnet. Lease expiration time can be modified for each manual IP address allocation.

An IP address can be returned to a DHCP server for one of the following reasons:

- The address is explicitly released by a DHCP client.
- The address is implicitly released because the lease has expired.

- An assigned lease is canceled by the DNS/DHCP Management Console.

If a DHCP client requests an IP address on the same subnet again before the previously assigned address expires, the same address is provided. If the IP address assignment is for a different subnet but the client already has a valid IP address entry in the DHCP server database, three possible actions can occur, depending on the IP Address Assignment Policy attribute of the DHCP server. The three possible actions are listed in Table 1-3.

Table 1-3
IP Address Assignment Policy

IP Assignment Policy	DHCP Server Action
Delete Duplicate	If the client moves to another subnet supported by the same DHCP server, delete any previous IP address assigned to the client, release the original address back to the pool, and assign a new address.
Allow Duplicate	If the client moves to another subnet, assign the new address and leave the old address unchanged in the database.
No Duplicate	If the client moves to another subnet and the old address is still valid, do not assign a new address.

The address deletion might delete a permanent IP object that is dynamically or manually assigned. Therefore, a client with a Delete Duplicate policy can have a *walking* manual IP object, but it cannot walk out of the service scope of a single DHCP server. For a DHCP server to assign an address to a walking manual IP object, the address assignment must be from a DHCP server's reserved Subnet Address Range with Range Type set to Dynamic DHCP, Dynamic BOOTP and DHCP, or Dynamic DHCP with Automatic Hostname Generation.

The DHCPSRVR.NLM software supports local address assignments that obtain IP addresses from multiple local subnets. For example, a DHCP server might have multiple IP addresses bound to one of its network interface cards. Each address is a server address on a separate subnet. No special configuration of the NDS database is required.

The DHCPSRVR.NLM software also supports remote address assignments that obtain IP addresses from multiple remote subnets. This feature requires all such subnets to be identified with a Subnet Pool object.

DHCP Options

Novell DNS/DHCP Services supports vendor options, DHCP options, and BOOTP parameters as defined in Internet RFC 2132 with a few exceptions. Novell DNS/DHCP Services supports new options defined for NetWare over TCP/IP and existing NetWare/IP options.

Note: The following options are not supported in this release of Novell DNS/DHCP Services: 56, 57, 60, 66, and 67. Although options 66 and 67 are not supported, the equivalent BOOTP parameter function is provided.

Assigning Options

DHCP and BOOTP options can be assigned at three levels:

- Globally
- At the Subnet level
- IP Address level

The DHCP server's options inheritance rules specify that options assigned at the lowest level override options set at a higher level. For example, options have been assigned at all three levels for the client on the subnet, as shown in Table 1-4.

Table 1-4
Example of DHCP Options Assignment

Level	Option	Value
Global	1, Subnet Mask	255.255.0.0
	3, Router	132.57.3.8
	4, Time Server	129.23.120.5

Level	Option	Value
Subnet	1, Subnet Mask	255.254.0.0
	5, Name Server	10.73.57.251
	7, Log Server	10.73.58.2
	13, Boot File Size	1024
IP Address	7, Log Server	Null
	13, Boot File Size	256

Table 1-5 lists the effective options for the client with the IP address referred to in the preceding table.

Table 1-5
Client's Effective Options

Option	Value
1, Subnet Mask	255.254.0.0
3, Router	132.57.3.8
4, Time Server	129.23.120.5
5, Name Server	10.73.57.251
7, Log Server	Null
13, Boot File Size	256

DHCP Options for NDS

Novell has defined three DHCP options for NDS. Using these options eliminates the need for users to provide this information each time they log in.

Option 85 provides the IP address of one or more NDS servers for the client to contact for access to the NDS database. Option 86 provides the name of the NDS tree the client will be contacting. Option 87 provides the NDS context the client should use.

Refer to Internet RFC 2241, *DHCP Options for Novell Directory Services,* for more detailed information about using these options in NetWare 5.

NetWare/IP Options

Novell uses option codes 62 and 63 in the DHCP packet for Netware/IP. Option 62 contains the Netware/IP domain name.

Option 63 is the IPX Compatibility option and contains general configuration information such as the primary DSS, preferred DSS, and the nearest servers. Option 63 provides additional information in the form of sub-options, listed in Table 1-6 on page 36.

Table 1-6
IPX Compatibility Sub-Options

Sub-Option Codes	Meaning
5	If the value of this field is 1, the client should perform a NetWare Nearest Server Query to find out its nearest NetWare/IP server.
6	Provides a list of up to five addresses of NetWare Domain SAP/RIP servers.
7	Provides a list of up to five addresses of the Nearest NetWare/IP servers.
8	Indicates the number of times a NetWare/IP client should attempt to communicate with a given DSS server at start-up.
9	Indicates the amount of delay in seconds between each NetWare/IP client attempt to communicate with a given DSS server at start-up.
10	If the value is 1, the NetWare/IP client should support NetWare/IP Version 1.1 compatibility.

Sub-Option Codes	Meaning
11	Identifies the Primary Domain SAP/ RIP Service server (DSS) for this NetWare/IP domain.
12	Identifies network number of the virtual IPX network created by the IPX Compatibility feature.
13	The IPX Stale Time suboption specifies the minimum interval in minutes that must expire before hosts try to refresh their Migration Agent addressing information.
14	Specifies the addresses of one or more Migration Agent servers for the IP nodes to use for communicating with IPX Nodes.

Refer to Internet RFC 2242, NetWare/IP Domain Name and Information, for more detailed information about using these Netware/IP options.

Dynamic DNS

The Dynamic DNS (DDNS) feature of Novell DNS/DHCP Services provides a way to update DNS with accurate A records and Pointer records for address assignments made by a DHCP server. These resource records are required so that both name-to-address and address-to-name DNS resolutions can be made. DDNS eliminates the need for further error-prone configuration of DNS for each host address change.

DDNS is enabled by configuring a subnet address range with Always Update parameter set to on. You must also specify a zone reference in the Subnet object so that the DHCP server can determine which zone to update.

When DDNS is active, the DHCP server updates the DDNS server for the zone, adding or deleting the corresponding Address and Pointer records. The DHCP server also notifies the DDNS server when leases expire, causing the A and PTR records to be deleted. If a lease is renewed, no action occurs because none is necessary.

Only subnet address ranges that are *Dynamic DHCP* or *Dynamic BOOTP and DHCP* can use the Dynamic DNS update feature. For a DDNS update to occur, *Always Update* must be specified for the range's DNS update option and a DNS zone must be specified to link the Zone object to the subnet. When these conditions are met, the DHCP server initiates a dynamic DNS update when an address is assigned to a client.

When a client that is subject to DDNS updates is granted a lease by the DHCP server, the server updates its database and NDS to store the transaction. The DHCP server also contacts the DNS server and submits a request for a DNS update.

For DDNS updates, the DNS server requires the fully qualified domain name (FQDN) and the IP address of the client. The DHCP server knows the IP address, but it must assemble the FQDN from the hostname and the subnet's domain name.

The DNS server usually maintains two resource records for each client. One maps FQDNs to IP addresses using A records. The other maps the IP address to the FQDN using PTR records. When DDNS is enabled and a client receives an address from the DHCP server, the DNS server updates both of these records.

When a client loses or ends its lease and is subject to DDNS updates, the DNS server receives the DDNS update request and deletes the PTR and A records associated with the client.

Compatibility with BOOTP

DHCP is based on the Bootstrap Protocol (BOOTP) and maintains some backward compatibility. BOOTP was designed for manual configuration of the host information in a server database. Novell has extended support for BOOTP to provide Dynamic BOOTP support. A pool of addresses can be set up for BOOTP address assignment so that each BOOTP address does not have to be configured separately.

From the clients' point of view, DHCP is an extension of BOOTP, enabling existing BOOTP clients to interoperate with DHCP servers without requiring any change to the clients' initialization software. Some new, additional options optimize DHCP client-server interaction.

There are two primary differences between DHCP and BOOTP. DHCP defines methods through which clients receive IP addresses for a specified period of time, enabling serial reassignment of addresses to different clients. There is no concept of a lease time in BOOTP; address assignments (even in Dynamic BOOTP) are permanent. Additionally, DHCP provides a method for a client to acquire all the IP configuration parameters it requires to operate.

If multiple servers service a single subnet, only one server, the *principal server*, can be designated as an *automatic* BOOTP server.

Another difference between the two protocols is a change in terminology to clarify the meaning of the *vendor extension* field in BOOTP messages. With DHCP, this field is called the *option* field.

Using a BOOTP Relay Agent

A BOOTP relay agent (also known as a forwarder) is an Internet host that passes DHCP messages between DHCP clients and DHCP servers in a subnetted environment. The forwarder usually resides on an IP router; however, any Novell server on a subnet can run the BOOTPFWD.NLM. The DHCP service in Novell DNS/DHCP Services provides relay agent functions as specified in the BOOTP protocol specification (Internet RFC 951).

When a client starts up, it sends a UDP broadcast message, called a Discover packet, to address 0xFFFFFFFF over port 67 requesting an address.

The forwarder has an IP address on the network and acts like a DHCP server, *listening* for Discover packets from clients on its LAN that are meant for a DHCP server. The forwarder must be configured with the destination address of the actual DHCP server on a different LAN segment that will provide DHCP service.

The DHCP server must be configured to serve the subnet on which the forwarder is located. The DHCP server must have a subnet address range to provide service.

After receiving a Discover packet from a client, the forwarder reformats the packet and sends it to the DHCP server. The DHCP server responds to the forwarder with an Offer packet containing an address for the client.

When the forwarder receives the Offer packet from the DHCP server, the forwarder contacts the client and provides the IP address and lease information.

Virtual LAN Environments

In environments using a *virtual LAN* (VLAN), multiple subnets might be defined on one physical subnet. For example, one physical subnet might contain several Class C addresses to form a larger address range than allowed for a Class C address. To accommodate a VLAN environment, a Subnet Pool object must be configured on the DHCP server to bind the multiple subnets together.

If a forwarder forwards client requests from a physical subnet with multiple subnet bindings and these subnets are bound to a single subnet pool, the collection of addresses available in configured subnet address ranges are available to all clients (DHCP or BOOTP) on that physical subnet. This is the primary use of the subnet pool.

Clients that are on the same subnet as the DHCP server do not have to be configured for the subnet pool if the server is bound to all local subnet addresses, or if the server has an address on each local subnet.

SNMP Event Generation

You can use the DNS/DHCP Management Console to set up SNMP event generation in the case of critical, major, warning, or minor events. The default setting is major and causes the server to log all major and critical events.

Critical events are those that cannot or should not be ignored by the network administrator. Major events denote a significant change in the state of the server processing. Warning and minor events are logged for maintenance and diagnosis only. Warning and minor events should not be turned on unless a problem has developed.

All critical and some major events are logged on the local server console.

The following *warning events* can be logged or trapped for SNMP event generation:

- An NDS update to the subnet failed, causing degraded operation (incomplete transactions are logged to a local file named DHCPLOG.LOG).
- An internal fault recovered and the error code was logged.
- A subnet was not configured and addresses are not available, causing degraded operation.

The following *minor events* are logged and/or trapped for SNMP event generation:

- A Decline was generated against an IP address.
- All logged file transactions have been reprocessed (operational.)

Major events are logged or trapped for SNMP event generation. For example, if when the DHCPSRVR NLM is loaded; the server is operational and ready for LAN-based clients.

The following events are logged or trapped for SNMP event generation:

- The logger cannot open the recovery log file or is having difficulty opening it. (The server is inoperative.)
- The main thread cannot process lease expiration. (The server is inoperative.)

DHCP Auditing

Auditing can be used to perform an analysis of historical data and to help diagnose operational difficulties. Auditing uses a Btrieve database to store and manage data enabling meaningful trend analysis.

When auditing is enabled, every incidence of address deletion, addition, and rejection is recorded in the audit log. The beginning and end of each session is marked to help make sense of the audit log. The beginning session contains records defining the session in terms of addresses already assigned.

Additionally, other major events or alert situations that cause SNMP traps are also audited. Other incoming DHCP requests are also logged, including honored renewal requests and those rejected or dropped.

Console and Debug Logs

The following types of console log entries are generated by both DNS and DHCP:

- Load success or failure
- Unload results normal or abnormal
- Major SNMP events

For each NetWareAlert message generated, an entry is provided in the /SYSTEM/SYS$LOG file.

The DHCP server provides a foreground screen log of every packet received and each reply generated to maintain continuity with the DHCP 2.0 server. The screen provides a useful real-time indication of DHCP 3.0 server operations.

The DHCP server has a debug log feature (primarily used by Novell technical support and engineering groups) that records the exchange of DHCP messages to a screen log or the DHCPSRVR.LOG file (in ASCII text) in the server's \ETC\DHCP directory. When loading the DHCPSRVR, the administrator can use one of three flags to activate the debug log feature. The following table explains the use of the flags.

Flag	Use
-d1	Turns on a background screen log of DHCP packets
-d2	Turns on a background screen log of Debug statements and DHCP packets
-d3	Turns on a background screen log of Debug statements and DHCP packets and writes the log to the server's \ETC\DHCP\DHCPSRVR.LOG file

Understanding the DNS/DHCP Management Console

This section provides information about the DNS/DHCP Management Console, the Java-based user interface used to configure and manage NDS-based DNS and DHCP.

The DNS/DHCP Management Console is an independent executable Java application and can be launched from a Windows 95 or Windows NT client with Novell Client software delivered with NetWare 5 installed. Future plans call for the DNS/DHCP Management Console to be platform-independent, able to run on other non-PC platforms (such as UNIX* and Macintosh*).

A separate Java application provides configuration and management for the two major functions of the DNS/DHCP Management Console: IP address management and name service management. Each application is self-contained and can provide the functions necessary to conduct address or name management.

NDS is used as a database to store the administered IP address and name service objects.

After the software installation is completed, the NDS schema is extended to enable the creation of new NDS objects for DNS and DHCP, including a global DNS/DHCP Locator object. The Locator object serves as the catalog for most of the DNS and DHCP objects; therefore, the DNS/DHCP Management Console is not required to search or scan the entire NDS tree to collect all the DNS and DHCP objects for initial tree display.

The creator of the Locator object should grant Read and Write rights to this object to the network administrators. They will use the DNS/DHCP Management Console to create, update, or delete any DNS or DHCP objects. This allows the contents of the Locator object to be updated when necessary.

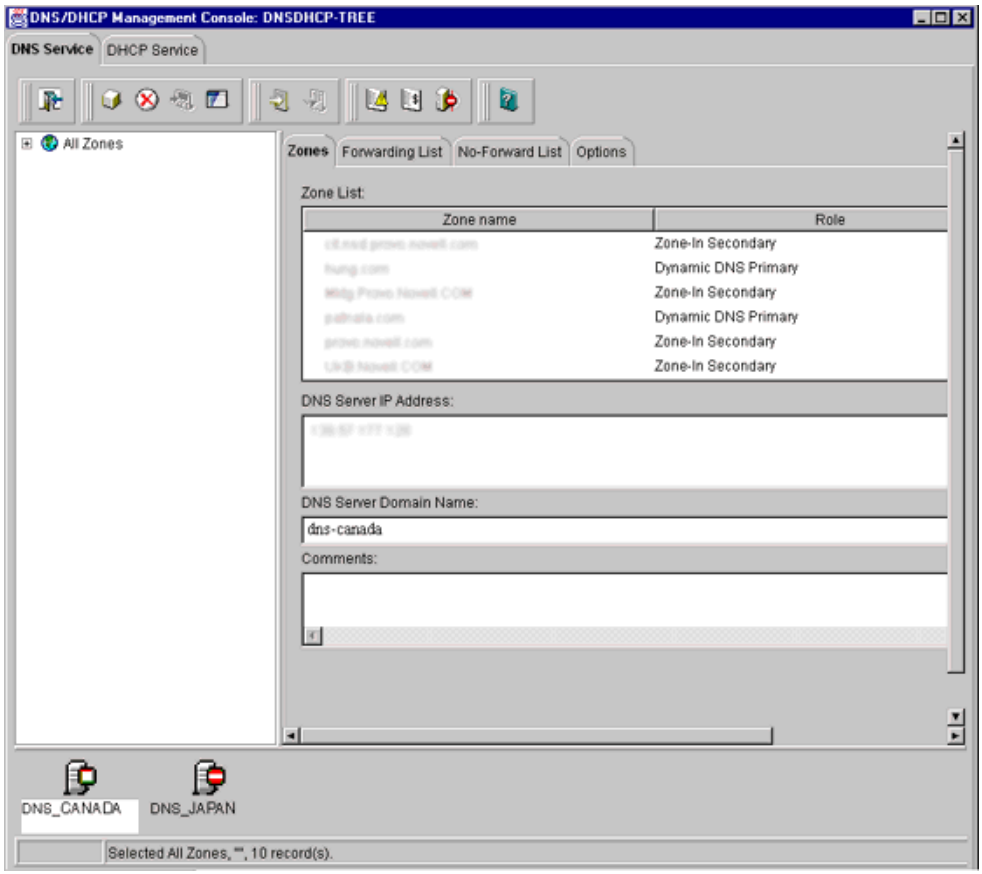
For more information, refer to “Overview of Interface Interaction” on page 44.

Overview of Interface Interaction

The DNS/DHCP Management Console manages one NDS tree at a time. Figure 1-8 shows the main user interface window for DHCP Services.

Figure 1-8

DNS/DHCP Management Console User Interface



If the DNS/DHCP Management Console is launched from the NetWare Administrator utility, the NDS tree the administrator is browsing will be set as the target NDS tree. When the DNS/DHCP Management Console is launched, it will prompt you to select a tree as the target NDS context.

In this release, the administrator must log in to the desired NDS tree prior to launching the DNS/DHCP Management Console. To manage objects in a different NDS tree, the administrator must exit the utility, change context to the other NDS tree, and launch the utility again. The current NDS tree name is displayed in the utility's caption bar.

DNS Service and DHCP Service Tab Pages

There are two main tab pages within the DNS/DHCP Management Console: DNS Service and DHCP Service. There are three pages within each tab page. The left page displays the managed DNS or DHCP objects in tree form. The right page displays the detailed information about the highlighted object in the left or bottom page. The bottom page lists either the DNS or DHCP servers configured to provide necessary services.

The resources are organized according to the object hierarchy and the implicit ordering of objects. For example, all IP addresses displayed within the left page of the DHCP Service page are in ascending numeric order. In the DNS Services page, all zones or resource records within a zone are listed in alphanumeric order.

An administrator can expand the logical container objects, such as Subnet or Subnet Address Range, to see the detailed list of subordinate objects or collapse them to see a concise view of the entire database by double-clicking the logical container object or by selecting the object and clicking the expand/collapse button next to the object.

Subnet and Subnet Pool objects can be created under O, OU, L, or C objects. Subnet Address Range and IP Address objects must be created beneath the Subnet container object. However, because of the IP address of an IP Address object, the subnet address range and IP Address objects can be contained within a subnet address range's address block. The Subnet Address Range and IP Address objects are displayed as subordinate objects below the Subnet Address Range object in the left tree page to show the logical relationship. The DNS Zone object, DNS Server object, and DHCP Server object can be created in the context of an O, OU, L, or C.

All DNS and DHCP objects are created as NDS objects and are subject to NetWare Administrator convention. Therefore, when creating a new object, the administrator should always name the object first in each Create dialog box.

Some objects, such as DHCP server, DNS server, DNS zone, Subnet, and Subnet Pool, can be created in any context. The Create dialog box of these objects has the NDS tree browsing capability; therefore, an administrator with Write or Supervisor rights can select a specific context.

A newly created object's button on the tool bar is context-sensitive in relation to the highlighted item in either service's left tree page. The administrator's right to the DNS or DHCP objects will not be verified until the administrator performs an update, delete, or create against the target objects.

The DNS and DHCP objects available in the new object dialog's creation list box depend on the selected object in the left tree page. Table 1-7 lists the rules for each container object.

Table 1-7
Object Creation Rules

Selected Object	Objects That Can Be Created
Our Network	Subnet, Subnet Pool, and DHCP Server
Subnet	IP Address, Subnet Address Range, Subnet Pool, Subnet, and DHCP Server
DHCP Server	Subnet and Subnet Pool
Subnet Address Range	DHCP Server
All Zones	Zone and DNS Server
DNS Server	Zone and DNS Server
Zone	Resource Record, DNS Server, and Zone
Resource Record Set	Resource Record, DNS Server, and Zone
Resource Record	Resource Record, DNS Server, and Zone

After a new DNS or DHCP object has been created, the DNS/DHCP Management Console grants the objects Read and Write rights to the Locator object.

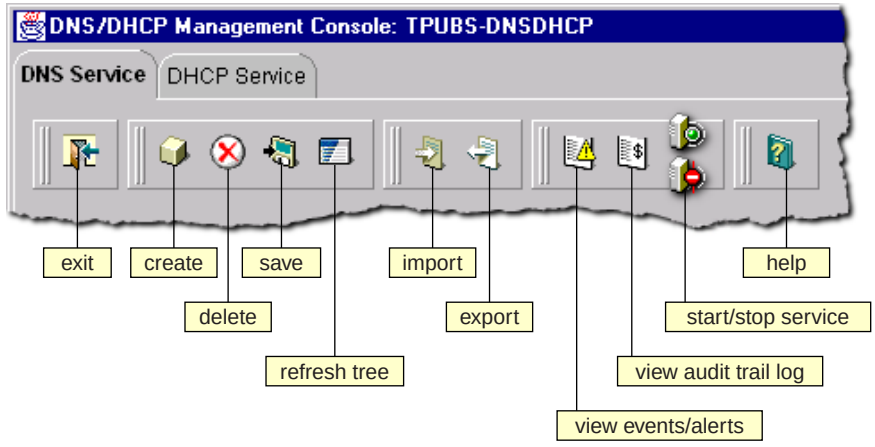
For fast and efficient searching, the distinguished names of newly created zones, DNS servers, subnets, and DHCP servers are added to the corresponding attribute of the Locator object. Renaming or deleting these objects is automatically performed by NDS because of the built-in feature for NDS distinguished names.

After a new DNS or DHCP object has been created, the DNS/DHCP Management Console provides the administrator with the choice of staying in its current focus or setting the focus on the newly created object. The utility also displays its detailed information page in the right page. This feature is provided as a convenience to administrators and can be used by checking the Define Additional Properties check box.

Tool Bar

The DNS/DHCP Management Console offers no menu items. All functions are provided by the tool bar. The functions that are relevant for the item selected in the left tree page or bottom server page are highlighted to show their availability. Figure 1-9 shows the tool bar.

Figure 1-9
Tool Bar



Each button shown on the tool bar has roll-over help associated with it; if you position the cursor over the icon, the icon's name appears. Table 1-8 lists when each tool bar button is enabled in relationship to the selected object.

Table 1-8
Tool Bar Buttons

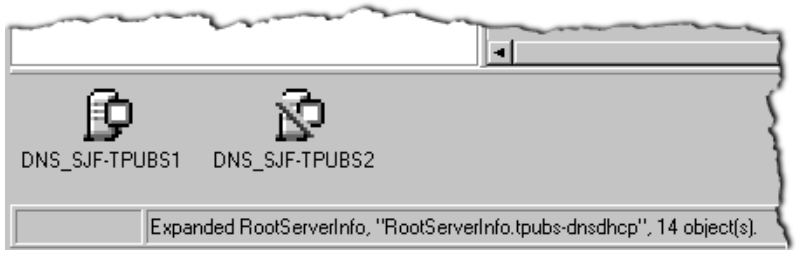
Tool Bar Button	Enabled
Exit	Always
Create	When Our Network, Subnet, Subnet Address Range, IP Address, DHCP Server, Subnet Pool, All Zones, Zone, DNS Server, RRSet, or Resource Record is the selected object
Delete	When Subnet, Subnet Address Range, Subnet Pool, Zone, RRSet, Resource Record, DHCP Server, or DNS Server is selected
Save	When fields have been changed for updates or changes
Tree Refresh	Always enabled
Global Preferences	Enabled for DHCP Service
Import	When Zone is the selected object for DNS or when Our Network is selected for DHCP
Export	When Zone is the selected object for DNS or when Our Network is selected for DHCP
Start/Stop	When DNS Server or DHCP Server is the selected object
View Events/Alerts	When DNS Server or DHCP Server is the selected object
View Audit Log	When DNS Server or DHCP Server is the selected object

Tool Bar Button	Enabled
Help	Always enabled

Status Bar

The status bar displays two fields in the bottom page of the DNS/DHCP Management Console. The first field shows the current database access interface in progress. The second field displays the current selected object or operation status. Figure 1-10 shows the status bar and two DNS server icons. The status bar is at the bottom of the figure.

Figure 1-10
Status Bar



Server Status

Server icons are displayed in the lower portion of the DNS/DHCP Management Console. As shown in Figure 1-11, the DHCP server represented by the icon on the right is operational, but operations have been suspended. The slash through the icon on the left indicates that the server might not be operational.

Figure 1-11
DHCP Server Icons

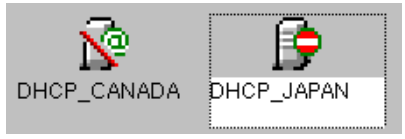
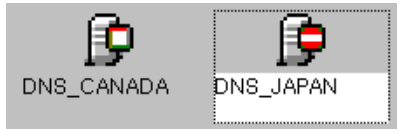


Figure 1-12 shows icons representing two DNS servers. Both servers are operational, NAMED.NLM has been loaded and each can communicate with the DNS/DHCP Management Console, but the operation of the server on the right, DNS_JAPAN, has been suspended.

Figure 1-12
DNS Server Icons



chapter 2

Planning

This chapter provides a summary of issues for you to consider as you plan and design your implementation of and maximize the DNS and DHCP capabilities of the Novell® DNS/DHCP Services software.

NDS Considerations

When installed and configured, the DNS and DHCP servers extend the NDS® schema to create new objects with which to administer and control their services. The DNS/DHCP Group and Locator objects are central to Novell's implementation of DNS and DHCP.

We recommend that you place the DNS/DHCP Group, DNS/DHCP Locator, and the RootServerInfo Zone objects in a separate partition that is accessible from and replicated to all points of the network where NetWare 5 DNS/DHCP servers are located. Although changes to the DNS/DHCP Group and Locator objects occur infrequently (only when you add or delete new servers, zones, or subnets), all NetWare 5 DNS/DHCP servers and the DNS/DHCP Management Console require access to these objects.

Consider the following NDS issues to maintain optimal performance when providing DNS and DHCP services on your NetWare network:

- Where to locate the DNS/DHCP Group and Locator objects
- Where to locate DNS and DHCP servers
- What replication strategy to employ
- How to provide fault tolerance

Plan to create an Organizational Unit (OU) container object near the top of your NDS tree. The location of this container object should be easily and widely accessible. Locate the DNS/DHCP Group and Locator objects and the RootServerInfo Zone object under the container object.

Plan to create an Administrator Group object under this container, also. An Administrator Group should have Read and Write rights to all DNS/DHCP Locator object attributes except the global data and options fields. Members of this group can use the DNS/DHCP Management Console to create and modify DNS and DHCP objects.

Important: A network administrator can access only his or her administrative domain which might not include the DNS/DHCP Locator object. By creating an Administrative Group, you enable administrators who are group members to use the DNS/DHCP Management Console.

Plan to locate your DNS and DHCP servers at locations where they are geographically close to the hosts that require their services. Plan to have one DHCP server in each partition of your network to minimize any WAN communications problems caused by normal load, configuration changes, or replication.

Replicate the partition containing the DNS/DHCP Group and Locator objects to all parts of the network that use DNS and DHCP services to ensure access in the event of system unavailability or hardware problems.

When planning your DNS replication strategy, consider that replication is employed for load balancing when you provide multiple name servers within the DNS zone.

Well-planned replication is the best way to provide fault tolerance for DNS and DHCP services.

Planning a DNS Strategy

Plan to install and operate a primary name server and at least one secondary name server. Secondary name servers provide load balancing and robustness to your DNS implementation.

When you configure your zone, the primary name server is considered authoritative for the zone, meaning that it contains the most up-to-date information about the zone and all the hosts within it.

A secondary name server receives its zone data from the primary name server. When it starts up and at periodic intervals, the secondary name server queries the primary name server to determine whether the information it contains has been changed. If the zone information in the secondary name server is older than the zone information in the primary name server, a *zone transfer* occurs and the secondary name server receives the zone information from the primary name server.

Planning Zones

If you are running a primary name server and providing DNS service for a zone, the size or geography of your network might require creating subzones within the zone.

Keep the zone data as a separate partition, and replicate the partition to all places on your network where you have a name server for the zone. Doing so enables independent replication of the zone data and also provides a degree of fault tolerance in the case of server down time.

Novell DNS Server as a Primary Name Server

You must install the Novell DNS server as a primary name server to have authoritative control over your zone and to take advantage of Dynamic DNS (DDNS), the dynamic updating of DNS by DHCP.

When operating the Novell DNS server as a primary name server, you use the DNS/DHCP Management Console to make configuration changes. When you operate a primary name server, the zone data can receive dynamic updates from DHCP servers. Non-Novell secondary name servers can transfer data in from the Novell primary name server.

Novell DNS Server as a Secondary Name Server (to a Non-Novell Master)

If you plan to operate secondary DNS servers using Novell DNS/DHCP Services software to a non-Novell master name server, one Novell secondary name server must be specified as the Dynamic DNS (DDNS) or *zone in* server. The DDNS server receives zone transfer information from the non-Novell master server and provides updates to NDS. Other Novell secondary name servers can then access the information within NDS.

Reasons for operating a Novell secondary name server to a non-Novell master name server include:

- You are have been using a master DNS server and do not want to designate it as a primary name server because of the responsibility it entails.
- This approach is easy to implement in your existing DNS model.
- You want to install more secondary name servers to provide better load balancing.
- You want to gradually make the transition to operating a primary name server.

Configuring a DNS Server to Forward Requests

If a name server cannot answer a query, it must query a remote server. You can configure primary or secondary name servers to act as forwarders. When you designate a server to be a forwarder, all off-site queries are first sent to the forwarder.

Forwarders that handle the off-site queries develop a robust cache of information. The forwarder probably can answer any given query with information from its cache, eliminating the need to make an outside query to a remote server.

When you decide to make a server a forwarder, configure the other servers in your zone to direct their queries through the forwarder. When a forwarder receives a query, it checks its cache for the information. If the information is unavailable, the forwarder issues a query to the root server.

For more information, refer to:

- "Forwarding Requests for Unknown Addresses" on page 57
- "Restricting Forwarding" on page 57

Forwarding Requests for Unknown Addresses

When you configure your name servers, you provide information about where to forward requests that the servers cannot answer. If you are configuring to use forwarders, you provide the names and IP addresses of servers above your location in your domain. Configure your other name servers to issue queries to the forwarders for queries they cannot answer.

Even if you are using forwarders, a name server that does not receive a timely response from its forwarder eventually attempts to query a root server directly.

Restricting Forwarding

If you have a primary name server with subdomains below it and the primary name server is not aware of the subdomains, the name server sends queries to external name servers.

You can configure your primary name server to not forward queries for specified internal subdomains to external name servers. Instead, the primary name server sends a negative response to any queries for the internal subdomains.

Setting Up the IN-ADDR.ARPA Zone

Just as the data in your name server provides mapping of names to Internet addresses, the IN-ADDR.ARPA zone provides mapping of addresses to names. However, in the structure of the IN-ADDR.ARPA zone, the IP address appears backward. For example, an IP address of 100.20.30.4 in the san-jose. novell.com domain would be *4.30.20.100.in-addr.arpa* in the IN-ADDR.ARPA subdomain.

Registering Your DNS Server with Root Servers

If you plan to operate a primary DNS name server, you must register your name server with your parent domain. Not all your name servers need to be registered, but we recommend registering one-third to one-half of your name servers (up to a maximum of 10) with the parent domain. These servers are queried by servers outside your domain. The remaining name servers are queried only by hosts within your domain that are configured to query them.

If you provide DNS service for other domains and provide an authoritative name server for those domains, you must also register those domains.

To register a domain (and subdomain), you must contact the network administrators of the parent domain (com, for example) and the *in-addr.arpa* domain. Provide the administrators with the name of the domain name server and the name of the domain and any subdomains for which it is authoritative. If you are setting up a new domain, you also need to provide the IP address of any server you want to register.

InterNIC is the organization that registers domain names for the ROOT, com, org, net, edu, and gov domains. To obtain the form for domain registration from InterNIC, contact them at *http://rs.internic.net*. You can also obtain the form for in-addr.arpa domain registration from the same location.

Detailed information about the registration process is available from the InterNIC web site. You can also use the InterNIC web site to research domain names to ensure that the name you want is not already registered and to obtain additional information and help.

Planning a DHCP Strategy

This section provides information to help you plan your DHCP strategy. When planning your implementation of DHCP, consider the following issues:

- Your existing network topology, that is, how you set up your routers and subnets, provides a basic configuration for the distribution of DHCP resources such as Subnet objects, Subnet Address Range objects, and IP Address objects.
- Your existing NDS implementation should be incorporated into your planning. Place the Locator object near the top of your NDS tree where it can be easily accessed by all servers.
- The length of time you set for your leases affects traffic on the network.

Network Topology

Your existing network topology provides a basic configuration for the distribution of DHCP resources. There are two paths, however, depending on whether you are migrating from an existing DHCP solution or you are installing and configuring DHCP for the first time.

For more information, refer to:

- “Migrating from Another DHCP Solution” below
- “Initiating the DHCP Service” below

Migrating from Another DHCP Solution

You can import your existing Novell DHCP 2.0 database or BOOTP-based configuration files using the DNS/DHCP Management Console. The import function enables you to specify the context into which you import the data.

Initiating the DHCP Service

If you are planning to use DHCP for the first time, you must gather a significant amount of information. You need to make a list of all hosts to be served by the DHCP server. You must include all devices that use network addresses in every segment of your network. You must also compile lists of IP address assignments.

Organize your lists of hosts and IP addresses by geographic location. For example, if your network is spread over a WAN, make a list for each location to help you organize the distribution of DHCP resources.

You must have a list of all permanently assigned network addresses. You might also want to make a list of devices that are to be denied IP addresses and those hosts that are to receive strict limitations on leases.

After you gather the necessary information, you need to create the necessary objects to represent this information. This is done by creating subnet address ranges for contiguous network addresses and other, more specific information. You will probably have a separate subnet address range for each LAN segment of your network. You will also create objects of subnets and DHCP servers.

NDS Implementation

Plan to create an Organizational Unit (OU), Country (C), or Locality (L) container object near the top of your NDS tree. Plan to locate the DNS/DHCP Group and Locator objects under the container object.

The DNS/DHCP Locator object must be easily accessible to all DHCP servers on the network. Plan to have multiple routes for DHCP servers to access the DNS/DHCP Group object.

Create Subnet objects to represent each LAN segment. Then create one or more Subnet Address Range objects to represent all your (contiguous strings of) IP addresses.

Place the NetWare Core Protocol™ (NCP™) servers that will provide DCHP service near the data to be updated and close to a writable partition. For fast access and availability, a DHCP server should be on the same LAN as or geographically close to the writable partitions the DHCP server uses.

When a DHCP server makes or modifies address assignments, the database is updated. The partition where this database is stored should have at least two writable replicas. Only one replica might be unsafe because of fault tolerance considerations, but three might be too costly in terms of NDS performance.

Lease Considerations

Many factors must be considered when you decide how long to set your client leases. Issues you must consider include the following:

- Your site's and clients' usage patterns
- Your network's goals
- Availability of servers
- Availability of network (IP) addresses

Another important consideration is that clients attempt to renew their leases half-way through the lease duration. The longer the lease, the longer it takes for client configuration changes to be registered with the DHCP server. It also takes longer for the server to realize that a previously assigned address is no longer in use.

Another issue to consider concerns outages and access to the DHCP server. If a client loses access to its DHCP server before renewing its lease, it must stop using the network after the lease expires. If a client is turned on and connected to the network at the time of the outage, however, the lease does not expire.

The longest lease provided by a DHCP server determines the length of time you might have to wait before configuration changes can be propagated within a network. This length of time could mean manually restarting every client or waiting the time required for all leases to be renewed before the changes take effect. If your site policy is to turn workstation power off at the end of the day, clients could acquire configuration changes at least once per day.

Note: All lease considerations refer to DHCP clients or devices only. For clients or devices that use BOOTP, you must bring down the device and restart it to acquire any new configuration changes.

For more information, refer to:

- "Considering the Length of Leases" below
- "Controlling Client Access to Leases" on page 65

Considering the Length of Leases

When considering the length of leases, ask these questions:

- Will the default of three days work well in your environment?

  The default of three days provides a good balance between a long-lease and a short-lease duration.

- Do you have more users than IP addresses?

  If you have more users than IP addresses, keep leases short to allow access to more users. A short lease could be 15 to 30 minutes, two to four hours, or even a matter of days.

  If your site's usage pattern shows that all clients request an address every day and you have half as many addresses as users, lease times in hours or minutes would provide access to more users.

- Do you provide support for remote access?

  If your site has mobile users or provides remote access to clients, plan to provide service for these clients on a specific subnet. Providing support, including special options the clients might require, makes network administration of the clients easier.

- Do you support a minimum lease time?

  If your site's usage pattern indicates that your users typically use an address for only one or two hours, that should be your minimum lease time.

- How many clients do you plan to support?

  Shorter leases support more clients, but shorter leases also increase the load on the DHCP server and network bandwidth. A lease of two hours is long enough to serve most users, and the network load should be negligible. A lease of one hour or less might increase network load to a point that requires attention.

- How fast are your communications connections between your clients and the DHCP server?

  By locating a DHCP server in close proximity to its users, the network load should be neglible over LAN connections. If a DHCP server must communicate over WAN links to provide service to clients, slowdowns and time-outs might occur.

- How long does your typical server outage last?

  If your typical server outage lasts two hours, a lease of four hours would avoid loss of lease to clients that were active at the time of the server outage.

  We recommend setting your lease times to twice the length of a typical server outage.

  The same recommendation applies to communications line outages. If a communications line is down long enough that leases expire, you might see a significant network load when the service is restored.

- How long can your clients operate without access to the DHCP server?

  If you have users who require a lease for important job functions, consider lease times for them that are twice the length of a maximum server outage. For example, if your DHCP server were to go down on Friday evening and require the entire workday Monday to be restored, that would be an outage of three days. In this case, a six-day lease covers that situation.

- Do you have users who advertise their IP addresses for services they render?

  If you have users setting up web pages or archiving data for others to access, they want addresses that do not change. You might want to assign permanent addresses for these users instead of assigning long lease times (three weeks or two months, for example).

  The relevant length of time is the maximum amount of time you want to allow a client to keep an address, even if the host computer is turned off. For example, if an employee takes a four-week vacation and you want the employee to keep his or her address, a lease of eight weeks or longer is required.

Table 2-1 lists examples of lease times and reasons why these times were chosen.

Table 2-1
Lease Time Examples

Lease Time	Rationale
15 minutes	Keeps the maximum number of addresses free when there are more users than available addresses, but results in significant traffic and frequent updates to NDS
6 hours	Covers a DHCP server outage of 6 hours
12 hours	Ensures that retraction of address assignment takes less than one day
3 days	Used by many sites simply because of software defaults
6 days	Affords a weekend server outage without losing leases
4 months	Enables students to keep their address over a summer vacation, for example

Controlling Client Access to Leases

There usually is a trade-off when an attempt is made to control specific client access to leases. Typically, you would manually configure each client and dedicate an IP address permanently to each client. Novell's DHCP server, however, provides control based on the client's hardware address.

IP Address Availability

This section describes how to identify your IP addresses, how to subnet your addresses, what to do with addresses assigned by other sources, and how to restrict address assignments to clients.

Identifying Your Addresses

If you have been using a previous version of Novell's DHCP, another vendor's product, or another method of tracking your IP address information, information about your addresses should be close at hand. We recommend verifying the accuracy of your IP address records by performing a site audit to prevent communication problems.

If you are unsure of the extent of your IP addresses, we recommend contacting your Internet Service Provider (ISP) or checking other records you have on file.

Subnetting Your Addresses

One of the more difficult configuration tasks concerns configuring your routers if you have multiple subnets. Each might require one or more subnets, depending on your router configuration. Create a Subnet object for each LAN segment that requires dynamic IP address assignment.

Assigning Addresses Manually

Your site might have devices, such as servers and printers, that have addresses assigned by means other than DHCP. Assign addresses to these devices manually.

You also must provide these devices with any specific configuration information they might require. If you want to provide configuration using DHCP, the device must be capable of acting as a DHCP client. You can assign a device a static address and still provide configuration information using DHCP.

To ensure that the assigned addresses are not used by DHCP, use the DNS/DHCP Management Console to exclude the addresses from assignment. You can use the utility to exclude single addresses or entire ranges from address assignment.

Representing Addresses in NDS

IP addresses are represented by IP Address objects under Subnet container objects. Novell DNS/DHCP Services stores address information and attributes of these objects, such as hostnames, hardware addresses, the time when an address lease will expire, and fully qualified domain names (FQDNs), in NDS. You can view this information using the DNS/DHCP Management Console.

Restricting Address Assignment to Clients

By using static address assignment, you can ensure that a device, capable of acting as a BOOTP or DHCP client, receives the same address from the DHCP server each time it is started. You can also explicitly exclude an address assignment to a device based on the device's hardware address. This is done using the DNS/DHCP Management Console Global Preferences button on the tool bar.

Hostnames

Every host on your network that uses the Internet or that can be reached from the Internet should have a name. Each resource record has a hostname field.

Some simple rules are required for hostnames for conformance to accepted Internet standards. Hostnames are called labels and can have alphabetic and numeric characters. A hyphen is allowed if it separates two character strings. Labels might not be all numbers, but they can have a leading digit. Labels must begin and end only with a letter or digit.

chapter 3

Setting Up

This document provides information about configuring DNS and DHCP, and importing and exporting database information.

Configuring DNS

The DNS/DHCP Management Console provides similar interfaces for configuring both DNS and DHCP. The left pane of the DNS Service window displays all DNS resources, the right pane displays detailed information about the object selected in the left pane, and the lower pane displays all DNS servers.

The view in the left pane of the DNS Service window is similar to the DNS hierarchical structure, with the *virtual All Zones* object as the root of the three hierarchical levels shown. The first level contains the Zone objects, the second level contains the Resource Record Set (RRSet) objects, and the third level contains the individual resource records.

The view in the right pane of the DNS Service window provides detailed information about DNS objects selected in the left pane. The detailed information varies, depending on the type of object selected. For example, a Zone object's detailed information includes tab pages for Attributes and Start of Authority, whereas the detailed information for resource records provides only an Attributes page.

The lower pane of the DNS Service window displays all currently existing DNS Server objects in the NDS tree and a description of their operational status.

For DNS configuration instructions, refer to:

- “Importing DNS Configuration Information” on page 70
- “Setting Up DNS” on page 71
- “Detailed DNS Configuration” on page 76
- “Configuring DNS Features” on page 83

Importing DNS Configuration Information

You can use the Novell DNS/DHCP Management Console to import existing DNS configuration information. The DNS information should be in DNS BIND Master file format.

To import existing DNS configuration information using the Management Console, complete the following steps:

1. **Launch the DNS/DHCP Management Console by double-clicking the icon.**
2. **Click the DNS Service tab.**
3. **Click Import DNS Database.**

   The Import-File Input window is displayed, requesting the location of the DNS BIND Master file.
4. **Enter the drive and path to the DNS database file, or click the browse button to navigate your way to the file.**

   After you select the file to import, the path to that file is displayed in the DNS File window.
5. **Click Next.**

   The Import DNS - Zone List window is displayed, listing each zone found in the configuration file.

6. **Select the Zone Context and click Next.**

   The Import window is displayed, indicating the zone context and the zones to import. (The subnet address and name are displayed in the list.)

7. **Click Import.**

   The Server Input window is displayed, prompting you to select a default NetWare Core Protocol® (NCP™) server to manage the newly-imported zone.

8. **Use the browse button to select the target server, then click OK.**

Setting Up DNS

This section provides the following procedures required to accomplish a basic DNS setup:

Note that this section does not describe how to enable all the available features. For detailed configuration information, refer to "Detailed DNS Configuration" on page 76.

DNS Prerequisites

The following steps must be completed before setting up DNS:

1. Install Novell® NetWare 5 on the selected server or servers.

2. Load the Novell Client software delivered with NetWare 5 on client computers that will be used to administer DNS and DHCP.

3. Install the DNS/DHCP Management Console on client computers that will be used to administer DNS and DHCP. For detailed information about installing client software, refer to “Installing the DNS/DHCP Management Console” on page 116.

Logging In to the Tree for DNS Setup

To set up DNS, you must first log in to the tree on which NetWare 5 has been installed.

To log in to the tree, complete the following steps:

1. **Right-click Network Neighborhood and select NetWare Login on a NetWare 5 client workstation on which you have installed the DNS/DHCP Management Console.**

   The NetWare Client login dialog box is displayed.

2. **Under the Login tab, enter your user name and password, then click Connection.**

3. **Under the Connection tab, enter the tree and context names of the server on which you have installed the NetWare 5, then click OK.**

Launching the DNS/DHCP Management Console for DNS Setup

Launch the DNS/DHCP Management Console by double-clicking its icon. The DNS/DHCP Management Console can be installed on a client workstation, or it can be accessed from Tools menu of the NetWare® Administrator utility.

The first time you launch the DNS/DHCP Management Console, you are prompted to enter the name of the NDS™ tree where you want to set up DNS. You can click in the Enter NDS Tree Name field to select an NDS tree that you are logged in to.

Creating a DNS Server Object

Use the DNS/DHCP Management Console to create and set up a DNS Server object for each DNS server you plan to operate.

To create and set up a DNS Server object, complete the following steps:

1. **Click the DNS Service tab of the DNS/DHCP Management Console, if necessary.**

   The All Zones object is the only object displayed on the DNS/DHCP Management Console's left pane.

2. **Click Create on the tool bar.**

   The Create New DNS Object dialog box is displayed, enabling you to create a DNS Server object or a Zone object.

3. **Select DNS Server and click OK.**

   The Create New DNS Server dialog box is displayed, prompting you to select a DNS Server object.

4. **Enter the desired server's name or use the browse button to select the server.**

5. **Enter the server's Domain name, then click Create.**

   The DNS Server object is created and displayed in the lower pane of the DNS/DHCP Management Console.

Creating a Primary DNS Zone Object

After you create a DNS Server object, use the DNS/DHCP Management Console to create and set up a Primary DNS zone. For information about how to create a secondary DNS Zone object refer to “Creating a Secondary DNS Zone Object” on page 78. For information about how to create an IN-ADDR.ARPA Zone object, refer to “Creating an IN-ADDR.ARPA Zone Object” on page 79. For information about how to create an IP6.INT Zone object, refer to “Creating an IP6.INT Zone Object” on page 80.

To create a primary DNS Zone object, complete the following steps:

1. **Click the DNS Service tab of the DNS/DHCP Management Console.**

   The All Zones object and the Root Server Info Zone object are displayed in the DNS/DHCP Management Console’s left pane.

2. **Click Create on the tool bar, select Zone, then click OK**

   The Create Zone dialog box is displayed. The default setting is to create a new, primary zone.

3. **Use the browse button to select the NDS context for the zone.**

4. **Enter a name for the Zone object in the Zone Domain Name field.**

5. **In the Assign Authoritative DNS Server field, select a DNS server.**

   Once you have selected an authoritative DNS server, the Name Server Host Name field is filled with name of the authoritative DNS server.

6. **Click Create.**

   A message is displayed indicating that the new zone has been created, and you are reminded to create the Address record for the host server domain name and corresponding Pointer record in the IN-ADDR.ARPA zone (if you have not already done so).

Starting the DNS Server

After you have created and set up a DNS Server object and a DNS Zone object, enter the following command at the DNS server console:

```
LOAD NAMED
```

After NAMED.NLM is loaded, the DNS server can respond to queries for the zone. For more detailed information about NAMED.NLM command line options, refer to “NAMED Command Line Options” on page 109.

Configuring Clients to Use DNS

Configuring clients to use DNS is performed at the client workstation.

To configure Windows NT or Windows 95 client workstations to use DNS, complete the following steps:

1. **At the client desktop, select Start > Settings > Control Panel, then double-click Network.**

   The Network window is displayed, listing the network components installed on the client workstation.

2. **Select TCP/IP, then click Properties.**

   The TCP / IP Properties window is displayed, usually showing the IP Address tab page.

3. **Click the DNS Configuration tab.**

4. **Provide a hostname and domain name for each client.**

5. **Enter the IP address of DNS servers for this client in the search order of preference, then click OK.**

The client can now send DNS queries to the DNS name server.

Detailed DNS Configuration

This section provides detailed information about configuring DNS objects using the DNS/DHCP Management Console. All the procedures in this section assume that you have already launched the utility and that you have selected the DNS Service tab. The procedures in this section are:

Creating a DNS Name Server Object

The DNS Name Server object is a stand-alone object within the NDS tree, and it can be located in any context you choose.

To create a new DNS Name Server object, complete the following steps:

1. **Click Create on the tool bar.**

   The Create New DNS Object dialog box is displayed, enabling you to create a DNS Server object or a Zone object.

2. **Select DNS Server and click OK.**

   The Create DNS Server dialog box is displayed, prompting you for the name of the server object.

3. **Enter the desired server's name or click the browse button to select the server.**

4. **Enter the server's Domain name, then click Create.**

   The DNS Server object is created and displayed in the bottom pane of the DNS/DHCP Management Console.

Modifying a DNS Name Server Object

After you have created a DNS Name Server object, you can modify it and provide more detailed configuration information.

To modify an existing DNS Name Server object, click the object's icon in the lower pane of the DNS Service window to display detailed information in the right pane. A DNS Name Server object's detailed information window displays four tab pages:

- Zones
- Forwarding List
- No-Forward List
- Options

On the Zones tab page, the Zone List contains a list of all zones and the role each zone serves for the selected DNS Name Server object. To change any of the zone information, you must modify the specific Zone object. Only the zone list is stored in the DNS Name Server object.

The DNS Server IP Address field contains the addresses of any DNS servers assigned to this zone. This field is read-only and is received from the DNS Server.

You can enter up to 256 characters of information about the name server in the Comments field.

The Forwarding List tab page displays a list of all forwarding IP addresses. Click Add to add an address to the list and display the Add Forward IP Address dialog box, which requests an IP address to add to the list. To delete an address from the list, select an IP address and click Delete.

The No-Forward List tab page displays a list of all domain names to which you do not want to send queries. To add a domain name to the No-Forward List, click Add and enter the domain name into the No Forward Name field, then click OK. To delete a domain name from the list, select the domain name from the list and click Delete.

Creating a Zone Object

The DNS Zone object is an NDS container object that comprises Resource Record Set (RRSet) objects and resource records. This section provides information about how to create a Secondary DNS Zone object and an IN-ADDR.ARPA Zone object. For information about how to create a Primary DNS Zone object, refer to “Creating a Primary DNS Zone Object” on page 74.

Creating a Secondary DNS Zone Object

After you create a DNS Server object, you can use the DNS/DHCP Management Console to create and set up Secondary DNS Zone object. To create a Secondary DNS Zone object, you must provide the IP address of the DNS server that will perform zone in transfers for the secondary zone.

1. **Click the DNS Service tab of the DNS/DHCP Management Console.**

2. **Click Create on the tool bar, select Zone, then click OK**

3. **Use the browse button to select the NDS context for the zone.**

4. **Enter a name for the Zone object in the Zone Domain Name field.**

5. **Under Zone Type, select Secondary.**

   When you select a secondary type zone, the Assign Authoritative DNS Server field and the Name Server Host Name field entries are optional.

6. **Enter the IP address of the DNS server that will provide zone out transfers for this secondary zone.**

   You can optionally select to assign an authoritative DNS server.

7. **Click Create.**

   A message is displayed indicating that the new zone has been created, and you are reminded to create the Address record for the host server domain name and corresponding Pointer record in the IN-ADDR.ARPA zone (if you have not already done so).

Creating an IN-ADDR.ARPA Zone Object

After you create a DNS Server object, you can use the DNS/DHCP Management Console to create and set up an IN-ADDR.ARPA Zone object.

To create an IN-ADDR.ARPA Zone object, complete the following steps:

1. **Click the DNS Service tab of the DNS/DHCP Management Console.**

2. **Click Create on the tool bar, select Zone, then click OK**

   The Create Zone dialog box is displayed. The default setting is to create a new, primary zone.

3. **Select Create IN-ADDR.ARPA.**

4. **Use the browse button to select the NDS context for the zone.**

5. **Enter an IP address in the Zone Domain Name field.**

   After you enter the IP address, it is reversed and prepended to .IN-ADDR.ARPA and reflected in the box below the Zone Domain Name field.

6. **Under Zone Type, select Primary or Secondary.**

   If you select Secondary, you must enter the IP address of the DNS Name Server that will provide zone out transfers to this zone.

7. **In the Assign Authoritative DNS Server field, select a DNS server.**

   Once you have selected an authoritative DNS server, the Name Server Host Name field is filled with name of the authoritative DNS server.

8. **Click Create, then click Save.**

Creating an IP6.INT Zone Object

After you create a DNS Server object, you can use the DNS/DHCP Management Console to create and set up an IP6.INT Zone object. Only one IP6.INT DNS Zone object can exist in an NDS tree.

To create an IP6.INT Zone object, complete the following steps:

1. **Click the DNS Service tab of the DNS/DHCP Management Console.**

2. **Click Create on the tool bar, select Zone, then click OK**

   The Create Zone dialog box is displayed. The default setting is to create a new, primary zone.

3. **Select Create IP6.INT.**

4. **Use the browse button to select the NDS context for the zone.**

5. **Under Zone Type, select Primary or Secondary.**

   If you select Secondary, you must enter the IP address of the DNS Name Server that will provide zone out transfers to this zone.

6. **For a Primary zone, click in the Assign Authoritative DNS Server field to select a DNS server to service the zone.**

7. **Click Create, then click Save.**

Modifying a Zone Object

After you have created a Zone object, you can modify it and provide more detailed configuration information.

To modify a new Zone object's attributes, complete the following steps:

1. **Select the Zone object you want to modify.**

2. **To change a Primary zone to a Secondary zone, click the Secondary check box and provide the Primary DNS Server's IP address in the Zone Master IP Address field.**

3. **To designate a DNS name server to be an Authoritative DNS Server, select one or more from the Available DNS Servers list and click Add.**

   The selected DNS name server's name is moved from the list of Available DNS Servers to the list of Authoritative DNS Servers. If only one server is available, that server automatically becomes the designated server.

4. **To select a server from the list of Authoritative DNS Servers to become the designated server, click the Dynamic DNS Server field.**

5. **Type any relevant comments about the zone directly into the Comments field.**

To view or modify a new Zone object's Start of Authority information, click the SOA Information tab. The following information is displayed:

- Zone master
- E-mail address
- Serial number

- Interval values
  - Refresh (default is 180 minutes)
  - Retry (default is 60 minutes)
  - Expire (default is 168 hours)
  - Minimal caching (default is 24 hours)

Creating Resource Records

A resource record is a piece of information about a domain name. Each resource record contains information about a particular piece of data within the domain.

To create a new resource record, complete the following steps:

1. **Select the Zone object under which you want to create a new resource record.**

   The Create New DNS Object window is displayed.

2. **Select Resource Record and click OK.**

   The Create Resource Record dialog box is displayed, prompting you for the domain name of the resource record you want to create. You can select the A record (the default) to create an Address record or the CNAME record to create a canonical name, or you can check the Others box to create a resource record from the displayed list of supported resource record types. The information required for each resource record depends on the resource record type.

3. **Enter the domain name you want to associate with this resource record.**

   The name you select is prepended to the domain name of the zone under which the resource record will be created.

4. **Enter any additional information required for the resource record type, then click Create.**

After you have created a resource record, its type cannot be modified. If changes are required, you must delete the resource record and create a new one.

Note: Start of Authority (SOA) is defined as part of a Zone object's attributes, and a Pointer (PTR) record is created automatically when any new A resource record or IPv6 (AAAA) resource record is created if the IN-ADDR.ARPA zone exists.

If you are creating a new resource record within an existing RRSet object, the Domain Name field is displayed in read-only format in the Create Resource Record dialog box. The domain name was defined for the RRSet object and must be the same for subordinate resource record objects.

Modifying Resource Records

When you select an existing resource record in the left pane of the DNS Service window, the detailed information for the object is displayed in the right pane.

Configuring DNS Features

This section provides procedures to help you configure the DNS features of Novell DNS/DHCP Services. The procedures in this section are:

- "Configuring an NDS Server to Forward Queries to Root Name Servers" on page 83
- "Configuring a Cache-Only Server" on page 84
- "Configuring to Support Child Zones" on page 84

Configuring an NDS Server to Forward Queries to Root Name Servers

When you install NetWare 5, the root server information is automatically loaded into your system. No procedure is required to configure your system to forward queries to the root name servers.

Configuring a Cache-Only Server

A cache-only server should be located between the clients that require address resolution and any DNS name servers that communicate over the Internet. Configure DNS clients to forward their queries to the cache-only server, and configure the cache-only server to forward its queries to a DNS server (or servers) attached directly to the Internet.

To configure a server to function as a cache-only server, follow the instructions to create a DNS server in “Creating a DNS Name Server Object” on page 76. After you have created the DNS Server object, do not assign any zones for it to serve. Configure this server to forward its queries to a DNS server

Configuring to Support Child Zones

If you are supporting child zones, you must configure the *glue logic* or *glue records* to associate the child zones with the parent zone.

The parent zone contains a referral to the child zone, meaning that its zone information contains an Name Server (NS) record that names the zone server for the child zone and an Address record that specifies the IP address for the child zone’s DNS name server.

When configured, queries to the parent zone for names within the child zone are returned with the child zone’s referral records. The requester can then query the child zone’s name server directly.

Configuring DHCP

To manage an organization's IP address database, you must define the global address pool in the form of Class A, B, and C network addresses. The addresses available to a network are managed by the DNS/DHCP Management Console and logically organized into the following types of objects:

- Subnet
- Subnet Address Range
- IP Address
- DHCP Server
- Subnet Pool

The Novell DHCP server views an organization's network as a collection of DHCP objects.

For DHCP configuration instructions, refer to:

- "Importing DHCP Configuration Information" on page 85
- "Setting Up DHCP" on page 87

Importing DHCP Configuration Information

You can use the DNS/DHCP Management Console to import existing DHCP configuration information. The DHCP information should be in DHCP version 2.0 or 3.0 file format.

To import existing DHCP configuration information, complete the following steps:

1. **Launch the Management Console by double-clicking the icon.**
2. **Click the DHCP Service tab.**

3. **Click Import.**

   The Import-File Input window is displayed, requesting the location of the DHCP database file.

4. **Enter the drive and path to the DHCP database file, or use the browse button to navigate your way to the file.**

   After you select the file to import, the path to that file is displayed in the DHCP File window.

5. **Click Next.**

   The Import DHCP - Subnet List window is displayed, listing each subnet found in the configuration file.

6. **Select the desired subnet or subnets and click Add, or click AddAll to import all the subnets on the list.**

7. **Select the Subnet Context and click Next.**

   The Import window is displayed, indicating the subnet context and the subnets to import. (The subnet address and name are displayed on the list.)

8. **Click Import.**

   The Server Input window is displayed, prompting you to select a default NCP server to manage the newly imported subnet.

9. **Use the browse button to select the target server and click OK.**

   If an error occurs during the importing process, an error message will be displayed, and the Details button will be enabled allowing you to display more information.

Setting Up DHCP

This section provides the following procedures required to accomplish a basic DHCP setup:

This section does not describe how to enable all the available features. For more information refer to "Detailed DHCP Configuration" on page 95.

DHCP Prerequisites

The following steps must be completed prior to setting up DHCP:

1. Load NetWare 5 on the selected server or servers.
2. Load the Novell Client software delivered with NetWare 5 on client computers that will be used to administer DNS and DHCP.
3. Install the DNS/DHCP Management Console on client computers that will be used to administer DNS and DHCP.

Logging In to the Tree for DHCP Setup

To complete the steps required to set up DHCP, you must first log in to the tree where NetWare 5 has been installed.

To log in to the server, complete the following steps:

1. **Right-click Network Neighborhood and select NetWare Login on a NetWare 5 client workstation on which you have installed the DNS/DHCP Management Console.**

   The NetWare Client login dialog box is displayed.

2. **Under the Login tab, enter your user name and password, then click Connection.**

3. **Under the Connection tab, enter the Tree, Server, and Context of the server on which you have installed NetWare 5, then click OK.**

Launching the DNS/DHCP Management Console for DHCP Setup

Launch the DNS/DHCP Management Console by double-clicking its icon. The DNS/DHCP Management Console can be installed on a client workstation, or it can be accessed from the Tools menu of the NetWare Administrator utility.

When the DNS/DHCP Management Console loads, you are prompted to enter the NDS Tree Name where you want to set up DHCP.

Setting Global DHCP Options

You use the DNS/DHCP Management Console to set global DHCP options. Setting global DHCP options is not required to set up DHCP, however.

To set global DHCP options, complete the following steps:

1. **Click the DHCP Service tab of the DNS/DHCP Management Console.**

2. **Click Global Preferences on the Tool Bar.**

   The Global Preferences window is displayed listing code, name, and value of any global DHCP options selected. Two other tab pages are available. One shows any global DHCP defaults set for the selected object; the other is the DHCP Options Table.

3. **Click the Global DHCP Defaults tab, then click Add.**

   The Add Exclude Hardware Address dialog box is displayed. Any devices or addresses you configure here will be excluded from any global defaults or global options.

   An asterisk (*) can be used as a wild card character to select a range of addresses to exclude. The asterisk can be used only as a trailing character, however. It cannot be used as a prefix or in the middle of a hardware address.

   The default delimiter for hardware addresses is a colon (:), but a dash (-) or period (.) can also be used. Only one type of delimiter can be used within an address.

4. **Click in the Hardware Type field to select a type of hardware to exclude, and enter an address in the Exclude Hardware Address field.**

   You can use the wild card character (*) and a different delimiter if you choose.

5. **Click the DHCP Options Table tab.**

   A list of DHCP options is displayed, listing all available DHCP options including codes, data syntax, and the option name. For detailed information about DHCP and BOOTP options, refer to “Setting Global DHCP Options” on page 89.

6. **Select a desired option from those listed, then click Add.**

   When you select a DHCP option, if any additional information is required to support the option, you are prompted to provide that information. For example, if you select option 85 for NDS Server, you are prompted to supply the IP address of the NDS Server.

7. **Provide any requested information specific to the selected option, then click OK.**

   The Global Preferences dialog box is displayed, listing the global options that have been set.

8. **When you have completed selecting global DHCP options, click OK.**

Creating a DHCP Server Object

You use the DNS/DHCP Management Console to create and set up a DHCP Server object. A DHCP Server object can be created or located under any of the following objects:

- Organization (O)
- Organization Unit (OU)
- Country (C)
- Locality (L)

To create and set up a DHCP server object, complete the following steps:

1. **Click the DHCP Service tab of the DNS/DHCP Management Console.**

   The Our Network object is the only object displayed on the DNS/DHCP Management Console's left pane.

2. **Click Create on the Tool Bar.**

   The Create New DHCP Object dialog box is displayed, enabling you to create a DHCP Server object, a Subnet object, or a Subnet Pool object.

3. **Select DHCP Server and click OK.**

   The Create DHCP Server dialog box is displayed, prompting you to select a server object.

4. **Use the browse button to select a server within the context, then click Create.**

   The DHCP Server object is created and displayed in the lower pane of the DNS/DHCP Management Console.

Creating a Subnet Object

You use the DNS/DHCP Management Console to create and set up a DHCP Subnet object for each of the subnets to which you will assign addresses.

To create and set up a Subnet object, complete the following steps:

1. **Click the DHCP Service tab of the DNS/DHCP Management Console.**

   The Our Network object is the only object displayed on the DNS/DHCP Management Console's left pane.

2. **Click Create on the Tool Bar.**

   The Create New DHCP Object dialog box is displayed enabling you to create a DHCP Server, a Subnet, or a Subnet Pool object.

3. **Select Subnet and click OK.**

   The Create Subnet dialog box is displayed. For each subnet you create, enter the following information in the fields provided: subnet name, NDS context, subnet address, and subnet mask. If you have setup a default DHCP server, its name is displayed and can be changed.

   You can click the Define Additional Properties check box to provide more detailed configuration, including DHCP options specific to each subnet.

4. **Enter the required information, then click Create.**

   The DHCP Subnet object is created and displayed in the left pane of the DNS/DHCP Management Console.

Creating Subnet Address Ranges

You use the DNS/DHCP Management Console to create and set up Subnet Address Range objects for each pool of addresses you want to be dynamically assigned by DHCP.

To create and set up a Subnet Address Range object, complete the following steps:

1. **Click DHCP Service tab of the DNS/DHCP Management Console.**

2. **Select the Subnet object under which you want to create the Subnet Address Range object, then click Create.**

   The Create New DHCP Record dialog box is displayed.

3. **Select Subnet Address Range and click OK.**

   The Create New Subnet Address Range dialog box is displayed.

4. **Enter a name for the Subnet Address Range, specify the range's starting and ending address, then click Create.**

   If you click the Define Additional Properties check box, the range's detailed information window is displayed, enabling you to provide more detailed configuration information. For more detailed configuration information, refer to "Detailed DHCP Configuration" on page 95.

Creating IP Address Objects

You use the DNS/DHCP Management Console to create and set up any IP Address objects to be assigned to specific devices or to be excluded from dynamic assignment. Create an IP Address object for each such device or address. Assigning a specific address to a client requires you to specify the client's media-access control (MAC) address or Client ID.

If you have set up subnets and subnet address ranges, you are not required to set up individual IP addresses unless you want to perform manual address assignment or exclude addresses from assignment.

To create and set up an IP Address object, complete the following steps:

1. **Click DHCP Service tab of the DNS/DHCP Management Console.**

2. **Select the Subnet object of the target IP address, then click Create on the tool bar.**

   The Create New DHCP Object dialog box is displayed.

3. **Select IP Address and click OK.**

   The Create IP Address dialog box is displayed.

4. **Enter the IP address to be assigned or excluded, select the assignment type, then click Create.**

   If you choose Manual Assignment Type, you must provide information for either the Client Identifier or the MAC Address fields. You can also specify the MAC Type by clicking in the field; the default is FF Any.

Starting the DHCP Server

After you have created and set up a DHCP server and configured the NDS™ objects required for DHCP, enter the following command at the DHCP server console:

```
LOAD DHCPSRVR
```

After you load DHCPSRVR.NLM, the DHCP server can respond to client requests and assign IP addresses. For information about other command line options, refer to “DHCPSRVR Command Line Options” on page 111.

Configuring Clients to Use DHCP

Configuring clients to use DHCP is performed at the client workstation.

To configure Windows 95* and Windows NT* client workstations to use DHCP, complete the following steps:

1. **At the client desktop, select Start > Settings > Control Panel, then double-click Network.**

   The Network window is displayed, listing the network components installed on the client workstation.

2. **Select TCP/IP and click Properties.**

   The TCP / IP Properties window is displayed, usually showing the IP Address tab page.

3. **Select Obtain an IP Address Automatically, then click OK.**

The next time the client starts up, it will send a request to the DHCP server for an IP address.

Important: Any client configuration settings override the configuration received from a DHCP server. The only exception is the hostname parameter set on the DNS Configuration tab of TCP/IP Properties window.

Detailed DHCP Configuration

This section provides detailed information about configuring DHCP objects using the DNS/DHCP Management Console. All the procedures in this section assume that you have already launched the utility and that you have selected the DHCP Service tab.

Refer to “Setting Up DHCP” on page 87 for information about setting up DHCP and creating DHCP objects. The following sections provide detailed information about modifying DHCP objects:

Modifying a DHCP Server Object

Refer to “Creating a DHCP Server Object” on page 90 for information about creating a DHCP Server object. After a DHCP Server object has been created, you can double-click the server icon to display and modify detailed information about the DHCP Server object. The DHCP Server object’s detailed information window displays two tab pages, Server and Options.

On the Server tab page, you can view the Subnet Address Ranges Serviced by this Server and Subnets Serviced by this Server. You can enter comments (up to 256 characters) about the server in the comments field.

On the Options tab page, you can configure policies specific to this DHCP server. You can configure the Set SNMP Traps Option parameter for None (default), Major Events, or All. You can configure the Set Audit Trail and Alerts Option parameter for None (default), Major Events, or All. You can also set the Enable Audit Trail Log on this page (the default is not enabled).

You can also configure the Mobile User Options parameter on the Options tab page to the following:

- No mobile users allowed
- Allow mobile user, but delete a previously assigned address (default)
- Allow mobile user, but do not delete a previously assigned address

Another option available on the DHCP server Options tab page is Ping Enable. Click this check box to have the server ping an address before the address is assigned to a device. Doing so ensures that the address is not already in use; however pinging the address also increases network traffic.

Modifying an Existing Subnet Object

For information about creating a Subnet object, refer to “Creating a Subnet Object” on page 91. After a Subnet object has been created, you can use the DNS/DHCP Management Console to display three tab pages of detailed information about the Subnet object that include Address, Subnet Options, and Other DHCP Options.

The Address tab page displays Subnet Address, Mask, and Type attributes from information entered when the object was created. If changes are required to these attributes, you must delete the Subnet object and re-create it.

If you are going to use Dynamic DNS, this is the page where you configure the DNS zone for dynamic updating (DDNS) and Domain name.

You can modify the subnet pool reference from the default (none) to the subnet pool to which this Subnet object is assigned.

You can also modify the subnet’s default DHCP Server on the Address tab page and enter up to 256 characters of information in the Comments field.

You can configure lease types on the Subnet Options tab page. A lease type can be permanent or timed. If you specify leases to be timed, specify the lease duration in days, hours, and minutes.

You also specify the settings for Set Boot Parameter Options on the Subnet Options tab page.

DHCP options can be configured from the Other DHCP Options tab page. Any options that are set for this subnet are displayed here. You can set additional DHCP options by clicking Modify which displays the Modify DHCP Options window. You a DHCP option from the Available DHCP Options list, then click Add.

Click Default to display the Default DHCP Options window listing all DHCP options and values configured for a subnet.

Modifying a Subnet Address Range Object

Refer to “Creating Subnet Address Ranges” on page 92 for information about creating a Subnet Address Range object. To modify a Subnet Address Range object, you must first select the object, which displays in the left pane of the DHCP Service window. Clicking on the Subnet Address Range object displays the its detailed information in the right pane and enables modifications.

The following range type options are available:

- Dynamic BOOTP
- Dynamic DHCP with Automatic Host Name Generation
- Dynamic DHCP
- Dynamic BOOTP and DHCP (the default)
- Excluded

You can also specify a DHCP server other than the default server for this Subnet Address Range object.

Modifying an Existing IP Address Object

Refer to “Creating IP Address Objects” on page 93 for information about creating IP Address objects. After an IP Address object has been created, its detailed information window displays three tab pages:

- Address
- Usage
- Other DHCP Options

On the Address tab page, the IP Address field of the object is displayed in read-only format. You can set the Assignment Type parameter to Manual or Excluded, and you can specify a client identifier.

You can change the MAC type from the default FF Any to any of the following:

- 15, Frame Relay
- 16, Asynchronous Transfer Mode (ATM)
- 17, HDLC
- 18, Fibre Channel
- 19, Asynchronous Transfer Mode (ATM)
- 20, Serial Line
- 21, Asynchronous Transfer Mode (ATM)

You can enter the IP Address's MAC address, hostname, DNS domain suffix, and identify an NDS object to use a specific IP Address on the address tab page.

The Usage tab page displays the IP Address Lease Expiration option, which can be either Permanent or Timed. If Timed is selected, the year, month, day, hour, and minute that the lease expires is displayed.

DHCP options can be configured from the Other DHCP Options tab page. Any options that are set for this IP Address object are displayed here. You can set additional DHCP options by clicking Modify.

Creating a Subnet Pool Object

A Subnet Pool object is a logical group of related Subnet objects of the same type. A Subnet Pool object can be created or located under any of the following objects:

- Organization (O)
- Organization Unit (OU)
- Country (C)
- Locality (L)

To create a new Subnet Pool object, complete the following steps:

1. **Click Create on the tool bar.**
2. **Select Subnet Pool and click OK.**
3. **Enter a unique name for the Subnet Pool object.**
4. **Use the browse button to select the NDS context in which to create the Subnet Pool object.**

After a Subnet Pool object has been created, you can select it and check the Define Additional Properties check box to display the detailed information window and to add Subnet objects to and remove them from the Subnet Pool object. Only Subnet objects with the same range type can be added to a Subnet Pool object.

Modifying a Subnet Pool Object

Click Add to bring up a dialog box with a list of available Subnet objects (either LAN or WAN) to be added to the list. After a Subnet object has been added to the Subnet Pool object, its NDS distinguished name is updated in the Subnet object's Subnet Pool List attribute.

Configuring Special Features

This section describes how to configure NetWare 5 to use the special features of Novell DNS/DHCP Services. The following configuration tasks are described:

- "Configuring a DNS Server to be Authoritative for Multiple Zones" on page 101
- "Configuring a Multi-Homed Server" on page 101
- "Configuring Dynamic DNS" on page 102
- "Configuring Multiple Logical Networks" on page 103

Configuring a DNS Server to be Authoritative for Multiple Zones

A NetWare 5 DNS server can be authoritative for multiple zones. There is no limit to the number of zones a NetWare 5 server can support other than those mentioned in "Optimizing DNS Performance" on page 113. Those limitations have to do with the total number of objects.

When you configure a zone, the Assign Authoritative DNS Server field in the Create Zone dialog box is the one that specifies the DNS server that will support the zone.

Configuring a Multi-Homed Server

A multi-homed server is a server with more than one IP address. In an Internet environment, a multi-homed server is a single server connected to multiple data links, which may be on different networks.

When using a DNS server with more than one IP address, you must use an address that is bound to the server, and that address must match the address used in the NS and A resource records for the zone.

Configuring Dynamic DNS

Dynamic DNS (DDNS) provides automatic updating of DNS with Address and Pointer records for addresses and hostnames assigned using the DDNS feature. To use DDNS, the following configuration must already exist:

- The DNS Zone object to receive DHCP updates must already be created.
- Subnet Address Range objects that will use DDNS must be set to range type Dynamic BOOTP and DHCP or Dynamic DHCP.

To activate the DDNS feature, complete the following steps:

1. **Select the Subnet object of the Subnet Address Range on which you want to activate DDNS and specify a zone in the DNS Zone for Dynamic Update.**
2. **Select the desired Subnet Address Range and ensure that the range type is set to Dynamic BOOTP and DHCP or Dynamic DHCP.**
3. **Set the DNS update option to Always Update.**
4. **Click Save.**

Configuring Multiple Logical Networks

When you configure multiple logical networks, also known as virtual local area networks (VLANs), you associate each individual LAN or Subnet object with a Subnet Pool object. The Subnet object you associate with the Subnet Pool object can be created prior to creating the subnet Pool object, or an existing Subnet can be modified.

To configure multiple logical networks or VLANs, complete the following steps:

1. **Create a Subnet Pool object.**

   For detailed information about creating a Subnet Pool object, refer to “Creating a Subnet Pool Object” on page 100.

2. **Select a Subnet object or create a new Subnet object.**

   If you create a new Subnet object, click Define Additional Properties.

3. **On the Addressing tab page of a Subnet object’s detailed information window, click the Subnet Pool Reference field, then select a Subnet Pool object with which to associate the Subnet object.**

4. **Click Save.**

5. **Repeat Step 2 through Step 4 for each subnet you want to associate with the Subnet Pool object.**

6. **Select the Subnet Pool object and ensure that each subnet is listed in the Subnet Pool object’s detailed information.**

Configuring for Auditing

You configure DNS and DHCP for auditing and view audit results by using the DNS/DHCP Management Console as described in:

Configuring DNS Auditing

To configure a DNS server to audit activities, complete the following steps:

1. **Log in to the tree containing the service you want to begin auditing, launch the DNS/DHCP Management Console, and click the DNS Service tab.**
2. **Select the desired server to perform the auditing and click the Options tab.**
3. **Under Event Log, select Major Events or All.**
4. **Click the Enable Audit Trail Log check box.**
5. **Click Save on the tool bar.**

Viewing the DNS Event Log

To view a DNS server's event log, complete the following steps:

1. **Log in to the desired tree, launch the DNS/DHCP Management Console, and click the DNS Service tab.**

2. **Select the server that has been configured to perform event logging and click View Events/Alerts on the tool bar.**

   The Events Period-Events Log dialog box displays the starting and ending dates of the current Event Log.

3. **Click OK to view the event log for the period displayed, or modify the dates as desired and click OK.**

   The events log is displayed, showing the entry time, severity, state, and description of each logged event.

4. **Click Display Options to modify the time period to view or to view a specific event's severity and state.**

   The Display Options dialog box is displayed enabling you to change the starting and ending dates, display one or more types of event severity, and to view specific operational states.

Viewing the DNS Audit Trail Log

To view a DNS server's audit trail log, perform the following steps.

1. **Log in to the desired tree, launch the DNS/DHCP Management Console, and click the DNS Service tab.**

2. **Select the server that has been configured to perform auditing and click View Audit Trail on the tool bar.**

   The Events Period-Audit Trail Log dialog box displays the starting and ending dates of the current audit trail log.

3. **Click OK to view the audit trail log for the period displayed, or modify the dates as desired and click OK.**

   The audit trail log is displayed, showing the entry time, type, IP address, and domain name DNS transaction.

4. **Click Display Options to select the time period to view or to view one or more specific transaction types.**

The DNS audit trail logs the following types of transactions:

- Agent Ready—The Simple Network Management Protocol (SNMP) agent is ready to receive or transmit requests.
- Query Received—The DNS server acknowledges receipt of a query by making an entry in the log file.
- Query Forwarded—The DNS server has forwarded a query to a client or another DNS server.
- Response Received—The DNS server has responded to a query from a client or another DNS server.

Configuring DHCP Auditing

You can configure a DHCP server for auditing using the Audit Trail and Alerts Option on the DHCP server Options tab page.

To configure a DHCP server to audit activities, complete the following steps:

1. **Log in to the tree containing the service you want to begin auditing, launch the DNS/DHCP Management Console, and click the DHCP Service tab.**

2. **Select the desired server to perform the auditing and click the Options tab.**

3. **Select the type of auditing desired.**

4. **Click the Enable Audit Trail Log check box.**

5. **Click Save on the tool bar.**

Viewing the DHCP Event Log

To view a DHCP server's event log, complete the following steps.

1. **Log in to the desired tree, launch the DNS/DHCP Management Console, and click the DHCP Service tab.**

2. **Select the server that has been configured to perform event logging and click View Events/Alerts on the tool bar.**

   The Events Period-Events Log dialog box displays the starting and ending dates of the current event log.

3. **Click OK to view the event log for the period displayed, or modify the dates as desired and click OK.**

   The events log is displayed showing the entry time, severity, state and description of each logged event.

4. **Click Display Options to select the time period to view and/or to view specific event's severity and state.**

   The Display Options dialog box is displayed, enabling you to change the starting and ending dates, display one or more types of event severity, and view specific operational states.

Viewing the DHCP Audit Trail Log

To view a DHCP server's audit trail log, complete the following steps.

1. **Log in to the desired tree, launch the DNS/DHCP Management Console, and click the DHCP Service tab.**

2. **Select the server that has been configured to perform auditing and click View Audit Trail on the tool bar.**

   The Events Period-Audit Trail Log dialog box displays the starting and ending dates of the current audit trail Log.

3. **Click OK to view the audit trail log for the period displayed, or modify the dates as desired and click OK.**

   The audit trail log displays the following information for each entry:

   - Entry time
   - IP address
   - Type
   - Status
   - Hostname
   - Hardware address
   - Client ID
   - Lease type

4. **Click Display Options to modify the time period to view or to view one or more specific address lease types.**

   The DHCP audit trail logs transactions based on the following types of address assignment or lease:

   - Manual
   - Dynamic
   - Automatic
   - Exclusion
   - Unauthorized
   - IPCP

NAMED Command Line Options

To start a DNS server, enter the following command at the server console prompt:

```
LOAD NAMED
```

The command line parameters listed in the following table are also supported.

Parameter	Function
-a	Turns on auto-detect of new zones (default setting)
-b	Turns off auto-detect of new zones
-f <scrpt.txt> [context]	Creates multiple zones using a text file in BIND bootfile format; specifying context enables zones to be created anywhere in the NDS tree
-h	Displays help information
-l	Enables a DNS server to login as an administrator to acquire rights required to create and delete zones from the command line

Parameter	Function
-m <file.dat> [context]	Imports file.dat and creates a new primary zone; specifying context enables zones to be created anywhere in the NDS tree
-q	Disables verbose mode for debug messages (default setting)
-r <zone name>	Deletes and removes an existing zone from the zone database
-rp <characters>	Replaces listed characters with a dash (-) in host names for which resource records are dynamically created
-s [zone name]	Prints status information; zone name is optional
-u <file.dat>	Imports file.dat and updates the contents of a previously created zone
-v	Enables verbose mode for debug messages
-zi <zone name>	Forces named zone for zone-in transfer

You can issue the **LOAD NAMED** command repeatedly to invoke different command line options. The NAMED.NLM software is loaded only on the first instance.

DHCPSRVR Command Line Options

To start a DHCP server, enter the following command at the server console prompt:

```
LOAD DHCPSRVR
```

The command line parameters listed in the following table are also supported.

Parameter	Function
-d1	Turns on a background screen log of DHCP packets
-d2	Turns on a background screen log of Debug statements and DHCP packets
-d3	Turns on a background screen log of Debug statements and DHCP packets and writes the log to the server's \ETC\DHCPSRVR.LOG file
-h	Displays command line syntax
-py	Specifies the global polling interval in *y* minutes
-s	Forces server to read from and write to the master replica

chapter 4

Optimizing

You can optimize the performance of Novell DNS/DHCP Services software by using state-of-the-art servers. We highly recommend that you use a server with a 200 MHz (or higher) Pentium* processor with 64 MB of memory. If your network configuration is large, more memory might provide improved performance.

For optimum performance, the designated server should be the most powerful server available. The designated server is the only server in a given tree that performs Dynamic DNS updates and zone transfers of secondary zone information.

The I/O subsystem of the servers can also be an issue for server performance. If you use both DNS and DHCP functions of NetWare 5, you will increase the number of NDS objects and thereby increase the disk space requirements of your SYS: volume.

Because the DNS and DHCP servers cache the required NDS data from disk into system memory, access to this information is not slowed.

Optimizing DNS Performance

Although there is no limit to the size of a zone when you configure DNS, we recommend that you limit the size of any zone to no more than 5,000 objects. If you have a zone with more than 5,000 objects, dividing the objects between two zones will improve performance.

Optimizing DHCP Performance

Although there is no limit to the size or number of subnets when you configure DHCP, we recommend that you limit the number of objects within a single subnet to no more than 2,048. A Novell DHCP server can support several large subnets in a DHCP-only configuration. However, the higher the number of IP Address objects supported, the greater the impact on DHCP server run-time performance.

chapter 5

Managing

This document provides information about installing and using the DNS/DHCP Management Console to perform management tasks.

DNS/DHCP Management Console

The DNS/DHCP Management Console is a Java-based program that enables network administrators to set up and manage DNS (DNS Service) and DHCP (DHCP Service) and the NDS™ objects created for DNS and DHCP.

Important: Before you can use the DNS/DHCP Management Console, the NDS schema must be extended to create the DNS/DHCP Group and Locator objects and to create the RootSrvrInfo zone. The NDS schema is extended when you activate Novell® DNS/DHCP Services from the Customize Server window during the installation of NetWare 5.

The DNS/DHCP Management Console runs on Microsoft* Windows 95* and Windows NT* client workstations on which the Novell Client software delivered with NetWare 5 has been installed.

The DNS/DHCP Management Console provides the following management functions from the client's desktop:

- Importing and exporting configuration to and from NDS
- Creating, updating, reading, or browsing configuration information
- Viewing DNS and DHCP server status, events, and alerts
- Viewing audit trail logs

After the software installation, existing DNS information is converted to master file format and can be imported to the server where NetWare 5 has been installed. You must use the DNS/DHCP Management Console to import any existing DHCP information. If you have no existing configuration information to import, you must use the DNS/DHCP Management Console to create the necessary objects to support your network. If you have imported configuration information, use the DNS/DHCP Management Console to create the DNS and DHCP server objects prior to operation.

Installing the DNS/DHCP Management Console

Installation of the DNS/DHCP Management Console software on a client workstation requires the following:

- 12.5 MB of free disk space
- 64 MB of memory (recommended), 32 MB minimum
- Novell NetWare 5 Client (or higher) software installed

The installation process uses Install Shield to install the DNS/DHCP Management Console on the client's hard disk. Exit all Windows programs before beginning the software installation.

To install the DNS/DHCP Management Console on a client workstation, complete the following steps:

1. **Map a drive to the SYS: volume on a server on which you have installed NetWare 5.**
2. **Click Start, then select Run.**
3. **Use the browse button to select the drive mapped to the SYS: volume on the selected server. Then select the Public and DNSDHCP folders.**
4. **Double-click Setup, then click OK in the Run dialog box.**

You can also begin the installation from the DOS prompt by entering:

```
X:\PUBLIC\DNSDHCP\SETUP.EXE
```

where *x* is the drive mapped to volume SYS on the server on which NetWare 5 has been installed.)

A welcome window is displayed, and you are reminded to exit all Windows programs before running the Setup program. After the installation has completed, you must restart your computer before attempting to use the DNS/DHCP Management Console.

After the DNS/DHCP Management Console has been installed on a workstation, a DNSDHCP icon is added to the client's desktop and the DNSDHCP folder.

Double-click the DNSDHCP icon to launch the DNS/DHCP Management Console. The DNS/DHCP Management Console can also be launched from NetWare Administrator by selecting DNS/DHCP Management Console from the Tools menu.

Using the DNS/DHCP Management Console

You must first log in to the tree you want to administer before launching the DNS/DHCP Management Console.

You must have sufficient rights to use the DNS/DHCP Management Console. All network administrators must have Read and Write rights to the container where the DNS/DHCP Locator and Group objects are located.

Administrators also must have Read and Write rights to the specific containers they manage. For example, if your company has offices in Chicago, Washington, and Providence, all administrators would require Read and Write rights to the container storing the Locator and Group objects. However, the administrator in Chicago would require Read and Write rights only to the Chicago part of the tree for the following objects:

- DNS and DHCP server objects
- DNS Zone object

- Subnet container object
- Subnet Pool object

It might be convenient to create an NDS group object for administrators and grant that object the necessary rights.

Managing DNS

Managing DNS is managing primary and secondary zones. When beginning configuration, it might be better to import the data, especially if you have a large zone. Doing so reduces the chances of error.

If you are using Dynamic DNS (DDNS), when a client receives an address assignment from the DHCP server, a request is made to update NDS. The only way to override DDNS is by using the DNS/DHCP Management Console.

After you have installed and configured your zones, you must still use the DNS/DHCP Management Console to assign a DNS server to service the zones.

Managing DHCP

After configuring your DHCP servers and beginning to provide DHCP services, you can also perform auditing or generate SNMP traps.

Deciding which DHCP options to use depends on your implementation. Refer to “DHCP Options” on page 34 for information about available DHCP and BOOTP options.

Managing DDNS is complicated because each Subnet Address Range type requires a different configuration. Each type’s configuration requirements are described later in this chapter.

It is important to understand the difference between static (or manual) and dynamic address assignment. If you use static address assignment, you must use the DNS/DHCP Management Console to assign permanent IP addresses to the clients in your tree. If you are using dynamic address assignment, the DHCP server assigns the address to a client when it starts.

You can deny address assignment to clients based on hardware address-based exclusion.

Events and Alerts

You can configure the DNS and DHCP servers to maintain a history of server activity in the events log. Events are activities that are considered significant, such as the loading or unloading of the server or problems the server encounters. The events logged depend on parameters set on the server's Options tab page.

You can configure DNS and DHCP servers to log major events, all events, or none (the default).

Event logs can be saved for future reference. When you are logging events, it is important to pay attention to the event log size. Event logs grow rapidly, especially if you are experiencing or researching problems. Event logs should be maintained or purged regularly to control the amount of disk space used. You can launch the CSAUDIT management utility by typing **CSAUDIT** at the server console.

Refer to "Configuring for Auditing" on page 104 for information about configuring event logging and viewing the event logs.

Auditing Server Activity

The audit trail log records a history of activity logged by DNS and DHCP servers. You can use the Audit Trail log to diagnose network trends. A DNS audit trail would include a history of DNS queries and the hosts requesting them. A DHCP audit trail would include a history of address assignments, including which host had an address during a given period of time and a list of addresses that had already been in use when pinged.

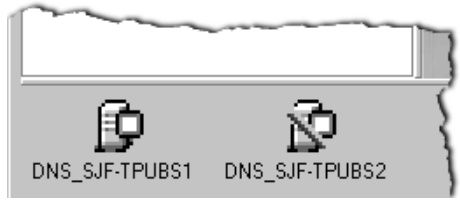
If you have set the Enable Audit Trail Log parameter on a server's Option tab page, you can use the View Audit Trail Log button on the tool bar to view the audit trail log.

Refer to "Configuring DNS Auditing" on page 104 for information about configuring a DNS server for auditing. Refer to "Configuring DHCP Auditing" on page 107 for information about configuring a DHCP server for auditing.

Server Status

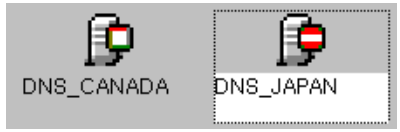
Server status is represented by the server icons displayed in the lower pane of the DNS/DHCP Management Console. Figure 5-1 shows icons representing two DNS servers. The server icon on the left indicates that this server, DNS_SJF-TPUBS1, is operational. The red slash through the server icon on the right indicates that the server might not be operational.

Figure 5-1
Server Status



Even though the server icon has a red slash through it, the server might still be operational. If the DNS/DHCP Management Console is unable to establish communications with the server, perhaps because of telecommunications problems, the utility displays the red slash through the server icon. In Figure 5-2, the operation of the DNS server on the right, DNS_JAPAN, has been suspended.

Figure 5-2
Server Operation Suspended



chapter 6

Troubleshooting

This chapter contains troubleshooting information for DNS and DHCP.

DNS

This section provides the following troubleshooting information for DNS:

Troubleshooting Checkpoints

If you experience problems related to DNS or TCP/IP, you can use the following steps to begin troubleshooting.

1. Run the WINIPCFG utility to determine your IP address, then ping your address from a functioning client.

   If you do not receive a response, your client's TCP/IP stack is not functioning. One of the following problems might be the cause:

   - The client's TCP/IP stack might be incorrectly configured.
   - The client did not receive an IP address from DHCP properly.
   - The IP address is already in use by another client.

2. Ping an IP address on your local network.

   If this approach fails, one of the following conditions might be the cause:

   - The client you pinged is not operational.
   - The LAN is experiencing problems.
   - Your client's TCP/IP stack is experiencing problems.

3. Ping an address on a different network or on the internet.

   If this approach fails but the preceding steps were successful, the problem is probably related to your router or your client's default router. If you are using DHCP, the default router configured for the DHCP server for each client is probably incorrectly configured.

4. Verify name resolution within your network. Ping a domain name within your company's network.

   If this approach fails, the default DNS server configured for your TCP/IP stack is invalid, or the DNS server is not functioning. If you are using DHCP, the DNS server that is configured on the DHCP server is not properly configured.

5. Verify name resolution through the internet. Ping a host on the internet, such as novell.com.

   If this approach fails, your company's DNS server (that forwards DNS requests to the Internet) is not functioning, or the Internet DNS server to which your DNS server forwards requests is not functioning.

Common Configuration Problems

If you experience problems with DNS, check the following configuration problems.

1. Check the consistency of glue records that are shared between parent and child zones. Make sure that Name Server (NS) and Address (A) records within the parent zone match those in the child zone.

2. Keep the IP addresses of the root name servers configured in the RootServerInfo zone updated. Changes to this information are not automatically propagated through a domain; you must enter them manually. The most recent update of root name server information is available through FTP at ftp://rzs.internic.net/domain/named/root.

3. Verify consistency between Pointer records in the IN-ADDR.ARPA domain and other domains.

4. If you change the IP address of a name server, ensure that the parent zone reflects that change.

5. Verify that you have configured a name server to correctly serve every zone.

6. Verify that zone transfers are occurring properly. Ensure that the secondary name server can identify the primary name server.

7. If you cannot access a particular host, verify that PTR records exist. When you create a zone, always select Yes when prompted to create a companion zone. If you created a companion zone, verify that the IP address and hostname are correct.

Common Operational Problems

Internet RFC 1912 provides information about common operational errors found in both the operation of DNS servers and the data the DNS servers contain. The following list describes the most common operational errors that occur.

- Problem—Hosts cannot access a particular system. You changed the IP address for this system recently, but the secondary name server has not yet been updated.

  Cause—The Start of Authority (SOA) record's serial number was not properly incremented. Without the serial number increment, the secondary name server does not recognize when a change has been made. This is usually not a problem with NDS-based DNS because the serial number is incremented automatically. With UNIX systems, failure to increment the serial number is the most common cause of DNS errors. The secondary server does not automatically test for changes in the SOA record. Any changes in the SOA record must be accompanied by a change in the SOA record serial number.

  Solution—Do not change the SOA record serial number manually with NDS-based DNS. If the primary server is not NDS-based, you might need to change the serial number manually for the secondary server to recognize that a change has occurred.

- Problem—You cannot access a particular host.

  Cause 1—When you created a new zone, the PTR records were not created or the PTR records have been deleted or changed.

  Solution 1—When you configure a zone, always select Yes when prompted to create a companion zone. If you created a companion zone, verify that the IP address and hostname are correct. Checkers can easily catch neglected PTRs. For further information, refer to RFCs 1537 and 1713.

  Cause 2—The host is down or is unreachable.

  Solution 2—Use PING to locate the connectivity problem. If the problem exists in your domain, make the necessary repairs to restore connectivity.

  Cause 3—The name server for that domain is not configured with information for the host.

  Solution 3—Configure the name server for that domain with information for the host.

- Problem—You cannot access a host in a different domain using its domain name, but you can access it using its IP address.

  Cause—The IP address or CNAME alias entry of the host's primary or secondary name server was changed, but the parent domain was not informed of the change. The address information in the glue record maintained by the parent domain has become invalid. Another possible cause is that the original address information in the glue record for the local zone is invalid or missing.

  Solution—When you configure a new zone, always enter the IP address when prompted. Verify that all parent zones have the same address information.

- Problem—Nonlocal hosts cannot find the primary domain server for a subdomain and, therefore, cannot access hosts in that subdomain.

  Cause—The IP address of a subdomain's primary server does not match the hostname and IP address configured in the parent domain for the subdomain's primary server.

  Solution—Verify that the hostname and IP address for the subdomain's primary server configured in the parent domain is valid and matches the information configured in the subdomain.

- Problem—A particular host cannot access other hosts.

  Cause—The resolv.cfg file (or equivalent) of the host does not contain the correct domain name or name server address.

  Solution—Enter the correct domain name or name server address in the hosts's resolv.cfg file (or equivalent).

- Problem—Hosts cannot access an entire external domain.

  Cause 1—The root name server information is invalid; therefore, the root servers are unreachable. For non-NDS systems running DNS, changes to this information are not automatically propagated through a domain; you must enter the changes manually.

Solution 1—Verify that the IP addresses of the root name servers configured in the RootServerInfo zone are correct. The most recent update of root name server information is available through FTP at ftp://rzs.internic.net/domain/named/root.

Cause 2—The hostname or IP address was not resolved because the delegation to the zone is incorrect.

Solution 2—Configure the correct hostname or IP address information for the zone in NDS.

Cause 3—The hostname or IP address was resolved to the wrong value.

Solution 3—Change the hostname or IP address information for the zone to the correct value in NDS.

Cause 4—The name server information of the primary name server of the domain is incorrect or missing in the root name servers.

Solution 4—Verify that the domain is properly registered with the INTERNIC, the organization that configures the name server information of the domain.

Cause 5—The name server for the domain is down or is unreachable.

Solution 5—Use PING to locate the connectivity problem. If the problem exists in your domain, make the necessary repairs to restore connectivity.

Cause 6—The root name server for the domain is down or is unreachable.

Solution 6—Use PING to locate the connectivity problem. If the problem exists in your domain, make the necessary repairs to restore connectivity.

Cause 7—You do not have sufficient rights to access the zone.

Solution 7—Contact the network administrator for the zone and obtain sufficient rights to access the zone.

Troubleshooting Windows 95 TCP/IP Problems

This section provides assistance for those troubleshooting TCP/IP problems on Windows 95* clients. You should have a basic understanding of TCP/IP and how it is configured for Windows 95.

Using WINIPCFG

The WINIPCFG utility displays a client's current TCP/IP configuration. To execute this utility, click Start > Run, enter **`winipcfg`**, and click Enter.

If the client's IP address was statically assigned and configured, the information that was entered under TCP/IP Protocols in the control panel's Network settings is displayed.

If the client was configured to obtain an address using DHCP, the information displayed was received from the DHCP server that assigned the IP address.

WINIPCFG provides the following information about the client:

- Network adapter address
- Assigned IP address
- Subnet mask
- Default gateway (default router)
- Hostname
- DNS Server

If the client has obtained an address from a DHCP server, click More Info to identify the DHCP server, when the lease began, and when it expires. Four additional buttons provide the following functions:

- Renew—Sends a DHCPREQUEST to the DHCP server, updates the lease, and updates any assigned values such as a default gateway or DNS server.

- Release—Sends a DHCPRELEASE to the DHCP server indicating that the client is giving up its IP address and that the server is free to assign that address to another client.

- Renew All—Sends a DHCPREQUEST to all network interfaces to which the Windows 95 client is configured.

- Release All—Sends a DHCPRELEASE to all network interfaces to which the Windows 95 client is configured.

If you want another IP address to be assigned to the client, select RELEASE, then select RENEW.

Using PING

PING is the most basic utility available to test, verify, and troubleshoot TCP/IP connectivity within a network. PING sends an ICMP packet to a specific host with a small amount of data and expects that host to respond with the same data packet. If you receive a response, both TCP/IP and connectivity between the two hosts are operational. If you do not receive a response, one of the following conditions exists:

- The host is not up.

- A router between the connections is not up.

- The client's TCP/IP stack is not functioning.

To run PING, from a DOS prompt enter the command followed by a hostname or IP address, such as the following:

```
C:\> ping www.novell.com >
```

If TCP/IP is operational and connectivity exists between the hosts, you will receive the following type of response:

```
Pinging www.novell.com [137.65.2.5] with 32 bytes of
data:
Reply from 137.65.2.5: bytes=32 time=27ms TTL=59
Reply from 137.65.2.5: bytes=32 time=22ms TTL=59
Reply from 137.65.2.5: bytes=32 time=31ms TTL=59
```

If you use the IP address of the host, you will receive the same type of reply.

Using the host's domain name is a good way to determine the host's IP address, and doing so also causes the client to request DNS name resolution before sending the ICMP packet. This approach is an excellent way to determine if DNS name resolution is working. If it is not working, you will receive a message such as the following:

```
Unable to resolve www.novell.com.
```

If DNS name resolution is not working, one of the following conditions might be the cause:

- The DNS server or DNS domain name is not configured properly on the client.
- If using DHCP, the DNS server and / or domain name are not properly configured on the DHCP server.
- The DNS server to which you send DNS name resolution requests is not functioning.

The PING command has the following syntax:

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL]
  [-v TOS] [-r count] [-s count] [[-j host] |
  [-k host-list]] [-w timeout] destination list
```

Table 6-1 explains the use of the PING options.

Table 6-1
PING Options

Option	Meaning
-t	Ping specified host until interrupted
-a	Resolve addresses to hostnames
-n count	Number of echo requests to send
-l size	Send buffer size
-f	Set Don't Fragment flag in packet
-i TTL	Time-To-Live value
-v TOS	Type of service
-r count	Record route for count hops
-s count	Time stamp for count hops
-j host-list	Loose source route along host-list
-k host-list	Strict source route along host-list
-w timeout	Timeout in milliseconds to wait for each reply

Using TRACERT

TRACERT can be very useful when you are resolving network-wide TCP/IP problems. TRACERT traces the route to a specific host and displays all hops that occur to search for the target host.

To run TRACERT, from a DOS prompt enter the command followed by a hostname or IP address, such as the following:

```
C:\> tracert www.novell.com
```

The TRACERT command has the following syntax:

```
tracert [-d] [-h maximum_hops] [-j host-list]
  [-w timeout] target_name
```

Table 6-2 explains the use of the TRACERT options.

Table 6-2
TRACERT Options

Option	Meaning
-d	Do not resolve addresses to host names
-h maximum_hops	Maximum number of hops to search for target
-j host-list	Loose source route along host-list
-w timeout	Timeout in milliseconds to wait for each reply

Using ARP

ARP is an advanced utility that should be used only by those who have a detailed understanding of TCP/IP and must troubleshoot complex problems. The ARP command enables you to display and modify the ARP cache of a client.

Following are three examples of use of the ARP command:

```
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
```

Table 6-3 explains the use of the ARP options.

Table 6-3
ARP Options

Option	Meaning
-a	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and physical addresses for the specified host are displayed.
-g	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and physical addresses for the specified host are displayed.
inet_addr	Specifies an Internet address.

Option	Meaning
-N if_addr	Displays the ARP entries for the network interface specified by if_addr.
-d	Deletes the host specified by inet_addr.
-s	Adds the host and associates the internet address inet_addr with the physical address eth_addr. The physical address is given as six hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr	Specifies a physical address.
if_addr	If present, specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface is used.

Using NETSTAT

NETSTAT is an advanced utility that should be used only by those who have a detailed understanding of TCP/IP and must troubleshoot very complex problems. NETSTAT displays protocol statistics and current TCP/IP network connections.

The NETSTAT command has the following syntax:

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

Table 6-4 explains the use of the NETSTAT options.

Table 6-4
NETSTAT Options

Option	Meaning
-a	Displays all connections and listening ports, but not those of the server side.
-e	Displays Ethernet statistics. This might be combined with the -s option.
-n	Displays addresses and port numbers in numerical form.
-p proto	Shows connections for the protocol specified by proto (either TCP or UDP). If used with the -s option to display per protocol statistics, proto can be TCP, UDP, or IP.
-r	Displays the contents of the routing table.

Option	Meaning
-s	Displays per protocol statistics. By default, statistics are shown for TCP, UDP, and IP. The -p option can be used to specify a subset of the default.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics. If omitted, NETSTAT prints the current configuration information once.

If you suspect that a LAN card is malfunctioning, use the -e option while troubleshooting. The -e option displays Ethernet statistics, including discards and errors.

The -a option provides a detailed display of the active TCP connections of the port number and network host communicating with that port. This information is useful when you are attempting to relate TCP port numbers of the various servers with which the client is communicating.

DHCP

This section provides the following troubleshooting information for DHCP:

- "Troubleshooting Checkpoints" on page 136
- "Common Operational Problems" on page 138
- "Releasing and Renewing DHCP Addresses" on page 141

Troubleshooting Checkpoints

1. Verify that IP hosts with DHCP-assigned parameters operate the same as when you manually configured them.

   If an IP host does not operate the same as when it was manually configured, verify that the parameters assigned by DHCP are the same as those when the host was manually configured.

   If a node is intermittently inoperable, verify that the node is not using the same IP address as another IP host. If a duplicate IP address exists, verify that there is only one DHCP server for the subnet. Also verify that the IP addresses assigned by the DHCP server are not being used by manual nodes.

2. Verify that all DHCP hosts can obtain a DHCP lease when required.

   If DHCP hosts cannot obtain a DHCP lease when required, verify that enough leases exist to accommodate all hosts that use DHCP. If there are too few leases, obtain more IP addresses and configure more leases or reduce the lease time to a few hours. This ensures that more leases are made available to other clients that are waiting to use the IP addresses.

   If a Windows 95 client cannot acquire a lease and responds with the message

   ```
   Unable to obtain an IP network address
   ```

   the client requires a longer timeout. This problem might occur when the client and DHCP server are separated by one or more routers. To increase the timeout for Windows 95 clients, obtain a patch from Microsoft. The patch is dated 2/12/96 and includes a file named VDHCP.386. The patch itself is named DCHCPUPD.EXE.

3. Verify that the number of leases available for clients does not decrease when you are using mobile clients.

   If the number of leases available for clients decreases when you are using mobile clients, verify that the mobile clients' lease is released when the client connects from a remote office or that the mobile client can use the same lease and the same IP address at the new location.

   - If the remote office is on a subnet different from that of the local office and the subnet is serviced by a different DHCP server, verify that the lease is released by the first server within a reasonable amount of time after the mobile client moves to the remote office. If the lease is not released quickly enough, reduce the lease time.
   - If the remote office is on a subnet different from that of the local office and the subnet is serviced by the same DHCP server, verify that the IPAssignmentPolicy attribute of the DHCP server object in NDS is set to DELETE_DUPLICATE. This ensures that only one lease is in use at a time because the original lease is deleted when the mobile client requests a new lease.
   - If the remote office is on the same subnet as that of the local office, the mobile client should use the same IP address. If the mobile client does not use the same IP address, verify that there is only one DHCP server for the subnet.

Common Operational Problems

The following list describes the most common operational errors that occur.

- Problem—A node is intermittently inoperable.

  Cause—An unauthorized DHCP server has been configured by someone attempting to control or disrupt your network. The unauthorized DHCP server is assigning IP addresses and other configuration parameters that have already been assigned to other nodes by an authorized DHCP server. The result is that nodes are assigned duplicate IP addresses or incorrect configuration parameters. Incorrect configuration parameters can interfere with a node's ability to communicate to the network in any number of ways. Incorrect parameters can even be used to cause a node to connect to a server that is controlled by an unauthorized user, thereby allowing the unauthorized user to take control of the client.

  Solution—Find the unauthorized DHCP server and disable it or disconnect it from the network.

- Problem—A Windows 95 client cannot acquire a lease and responds with the message

  ```
  Unable to obtain an IP network address
  ```

  Cause—The Windows 95 DHCP client has a two-second timeout for the time between when it accepts an offer of an IP address in a message sent to the server and the time it expects an acknowledgment of that acceptance in a reply from the server. Other clients, such as Windows NT*, have a four-second timeout.

  Solution—Obtain the DCHCPUPD.EXE patch from Microsoft that changes the timeout on Windows 95 clients from two seconds to four seconds. The patch is dated 2/12/96 and includes a file named VDHCP.386.

- Problem—The use of mobile clients causes fewer leases to be available.

  Cause 1—The mobile clients' lease is not released when the mobile client moves to a remote office. This can occur when the remote office is on a subnet different from that of the local office and the remote subnet is serviced by a different DHCP server.

  Solution 1— Determine the lease time assigned to this client. If the lease is not released quickly enough, reduce the lease time. Otherwise, have the client manually release the old IP address before it leaves the local office.

  Cause 2—The mobile client uses two leases at the same time because it cannot use the same lease and the same IP address at the new location.

  Solution 2—Use one of the following solutions:

  - If the remote office is on a subnet different from that of the local office and the subnet is serviced by the same DHCP server, verify that the IPAssignmentPolicy attribute of the DHCP server object in NDS is set to DELETE_DUPLICATE. This ensures that only one lease is in use at a time because the original lease is deleted when the mobile client requests a new lease.

  - If the remote office is on the same subnet as that of the local office, the client should use the same IP address. If the client does not use the same IP address, verify that there is only one DHCP server for the subnet.

- Problem—Clients work properly when manually configured, but some functions do not work when using DHCP.

  Cause—One or more global client parameters were not configured properly in DHCP.

  Solution—Verify that all parameters assigned by DHCP are properly configured.

- Problem—At a site with a limited number of leases, many clients cannot obtain a lease. The leases are not being efficiently shared by all clients that must use them.

  Cause—Clients are not releasing the leases when they are finished using them because the lease time is too long.

Solution—Reduce the lease time to a few hours so that leases can be made available to other clients that are waiting to use the IP addresses. Otherwise, you might need to purchase more IP addresses and configure more or larger address ranges to make more IP addresses available.

- Problem—It is difficult to identify and manage network resources when using dynamic DHCP assignments.

  Cause—The IP addresses of the clients might change if you use DHCP continually over a period of time and the lease period is set to a reasonably low value.

  Solution—Use static DHCP assignments when you want to use a specific IP address assigned to the client for identification and management.

- Problem—DHCPSRVR.NLM is loaded and the trace screen has been activated with the -d flag, but there is no evidence of interaction between the server and clients, and clients are not receiving IP address assignments.

  Cause—The server is not physically linked to the client's communications media or the server did not bind its IP protocol to the interface card, which shares physical media access with the client.

  Solution—Check the server's physical connections. Load INETCFG to ensure that proper binding exists.

- Problem—DHCPSRVR.NLM is loaded and the trace screen shows client packets being received, but the server is not responding and the REQUEST packets are dropped.

  Cause—The server's configuration for its local interfaces does not match the configuration within the Directory for the same server.

  Solution—Load INETCFG and check to see if the server has a legal IP address on each local subnet it serves. Also check that each local subnet is properly configured using the DNS/DHCP Management Console.

Releasing and Renewing DHCP Addresses

When a host is powered on, it is *leased* an IP address for a period of time, depending on the configuration settings of the subnet from which the address is assigned. If the machine is moved to another network while the original IP address lease is still valid, the user must release the lease. Other situations might also require that a lease be released, such as the use of a laptop computer in different locations of a given network.

Windows 95

To manually release and renew a DHCP-assigned IP address in Windows 95, complete the following steps:

1. **Select Start, then Run.**
2. **Type `winipcfg` and press Enter.**

   The IP Configuration dialog box is displayed.
3. **Click Release All.**

   The IP Address, Subnet Mask, and Default Gateway fields should display no addresses.
4. **Click Renew All.**

   New addresses should appear in the IP Address, Subnet Mask, and Default Gateway fields.
5. **Click OK to close WINIPCFG.**

Windows NT

To manually release and renew a DHCP-assigned IP address in Windows NT, complete the following steps:

1. **Select Start > Programs > MS-DOS Command Prompt.**

2. **From the DOS prompt, execute the command**

   `ipconfig /release`

   A message is displayed indicating that the assigned IP address has been successfully released.

3. **From the DOS prompt, execute the command**

   `ipconfig /renew`

   A message is displayed indicating the new IP address that has been assigned.

   To review DHCP settings,

4. **From the DOS prompt, execute the following command to review DHCP settings:**

   `inconfig /all`

Trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell Trademarks

Access Manager is a registered trademark of Novell, Inc. in the United States and other countries.

Advanced NetWare is a trademark of Novell, Inc.

AlarmPro is a registered trademark of Novell, Inc. in the United States and other countries.

AppNotes is a trademark of Novell, Inc.

AppTester is a trademark of Novell, Inc. in the United States.

BrainShare is a registered service mark of Novell, Inc. in the United States and other countries.

C-Worthy is a trademark of Novell, Inc.

C3PO is a trademark of Novell, Inc.

CBASIC is a registered trademark of Novell, Inc. in the United States and other countries.

Certified NetWare Administrator in Japanese and CNA-J are service marks of Novell, Inc.

Certified NetWare Engineer in Japanese and CNE-J are service marks of Novell, Inc.

Certified NetWare Instructor in Japanese and CNI-J are service marks of Novell, Inc.

Certified Novell Administrator and CNA are service marks of Novell, Inc.

Certified Novell Engineer and CNE are service marks of Novell, Inc.

Certified Novell Salesperson is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

ConnectView is a registered trademark of Novell, Inc. in the United States and other countries.

Connectware is a trademark of Novell, Inc.

Corsair is a registered trademark of Novell, Inc. in the United States and other countries.

Media Support Module and MSM are trademarks of Novell, Inc.

Mirrored Server Link and MSL are trademarks of Novell, Inc.

Mobile IPX is a trademark of Novell, Inc.

Multiple Link Interface and MLI are trademarks of Novell, Inc.

Multiple Link Interface Driver and MLID are trademarks of Novell, Inc.

My World is a registered trademark of Novell, Inc. in the United States and other countries.

N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Natural Language Interface for Help is a trademark of Novell, Inc.

NDS is a trademark of Novell, Inc.

NDS Manager is a trademark of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE/2T is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2000T is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE21500T is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NE32HUB is a trademark of Novell, Inc.

NEST is a trademark of Novell, Inc.

NEST Autoroute is a trademark of Novell, Inc.

NetExplorer is a trademark of Novell, Inc.

NetNotes is a registered trademark of Novell, Inc. in the United States and other countries.

NetSync is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare 3 is a trademark of Novell, Inc.

NetWare 3270 CUT Workstation is a trademark of Novell, Inc.

NetWare 3270 LAN Workstation is a trademark of Novell, Inc.

NetWare 386 is a trademark of Novell, Inc.

NetWare 4 is a trademark of Novell, Inc.

NetWare 5 is a trademark of Novell, Inc.

NetWare Access Server is a trademark of Novell, Inc.

NetWare Access Services is a trademark of Novell, Inc.

NetWare Application Manager is a trademark of Novell, Inc.

NetWare Application Notes is a trademark of Novell, Inc.

NetWare Asynchronous Communication Services and NACS are trademarks of Novell, Inc.

NetWare Asynchronous Services Interface and NASI are trademarks of Novell, Inc.

NetWare Aware is a trademark of Novell, Inc.

NetWare Basic MHS is a trademark of Novell, Inc.

NetWare BranchLink Router is a trademark of Novell, Inc.

NetWare Care is a trademark of Novell, Inc.

NetWare Communication Services Manager is a trademark of Novell, Inc.

NetWare Connect is a registered trademark of Novell, Inc. in the United States.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Distributed Management Services is a trademark of Novell, Inc.

NetWare Document Management Services is a trademark of Novell, Inc.

NetWare DOS Requester and NDR are trademarks of Novell, Inc.

NetWare Enterprise Router is a trademark of Novell, Inc.

NetWare Express is a registered service mark of Novell, Inc. in the United States and other countries.

NetWare Global Messaging and NGM are trademarks of Novell, Inc.

NetWare Global MHS is a trademark of Novell, Inc.

NetWare HostPrint is a registered trademark of Novell, Inc. in the United States.

NetWare IPX Router is a trademark of Novell, Inc.

NetWare LANalyzer Agent is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Link / ATM is a trademark of Novell, Inc.

NetWare Link / Frame Relay is a trademark of Novell, Inc.

NetWare Link / PPP is a trademark of Novell, Inc.

NetWare Link / X.25 is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWare LU6.2 is trademark of Novell, Inc.

NetWare Management Agent is a trademark of Novell, Inc.

NetWare Management System and NMS are trademarks of Novell, Inc.

NetWare Message Handling Service and NetWare MHS are trademarks of Novell, Inc.

NetWare MHS Mailslots is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Mirrored Server Link and NMSL are trademarks of Novell, Inc.

NetWare Mobile is a trademark of Novell, Inc.

NetWare Mobile IPX is a trademark of Novell, Inc.

NetWare MultiProtocol Router and NetWare MPR are trademarks of Novell, Inc.

NetWare MultiProtocol Router Plus is a trademark of Novell, Inc.

NetWare Name Service is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Navigator is a trademark of Novell, Inc.

NetWare Peripheral Architecture is a trademark of Novell, Inc.

NetWare Print Server is a trademark of Novell, Inc.

NetWare Ready is a trademark of Novell, Inc.

NetWare Requester is a trademark of Novell, Inc.

NetWare Runtime is a trademark of Novell, Inc.

NetWare RX-Net is a trademark of Novell, Inc.

NetWare SFT is a trademark of Novell, Inc.

NetWare SFT III is a trademark of Novell, Inc.

NetWare SNA Gateway is a trademark of Novell, Inc.

NetWare SNA Links is a trademark of Novell, Inc.

NetWare SQL is a trademark of Novell, Inc.

NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.

NetWare Telephony Services is a trademark of Novell, Inc.

NetWare Tools is a trademark of Novell, Inc.

NetWare UAM is a trademark of Novell, Inc.

NetWare WAN Links is a trademark of Novell, Inc.

NetWare/IP is a trademark of Novell, Inc.

NetWire is a registered service mark of Novell, Inc. in the United States and other countries.

Network Navigator is a registered trademark of Novell, Inc. in the United States.

Network Navigator - AutoPilot is a registered trademark of Novell, Inc. in the United States and other countries.

Network Navigator - Dispatcher is a registered trademark of Novell, Inc. in the United States.

Network Support Encyclopedia and NSE are trademarks of Novell, Inc.

Network Support Encyclopedia Professional Volume and NSEPro are trademarks of Novell, Inc.

NetWorld is a registered service mark of Novell, Inc. in the United States and other countries.

Novell is a service mark of Novell, Inc. and a registered trademark of Novell, Inc. in the United States and other countries.

Novell Academic Education Partner and NAEP are service marks of Novell, Inc.

Novell Alliance Partners Program is a collective mark of Novell, Inc.

Novell Application Launcher is a trademark of Novell, Inc.

Novell Application Notes is a trademark of Novell, Inc.

Novell Authorized CNE is a trademark and service mark of Novell, Inc.

Novell Authorized Education Center and NAEC are service marks of Novell, Inc.

Novell Authorized Partner is a service mark of Novell, Inc.

Novell Authorized Reseller is a service mark of Novell, Inc.

Novell Authorized Service Center and NASC are service marks of Novell, Inc.

Novell BorderManager is a trademark of Novell, Inc.

Novell BorderManager FastCache is a trademark of Novell, Inc.

Open Look is a registered trademark of Novell, Inc. in the United States and other countries.

Open Networking Platform is a registered trademark of Novell, Inc. in the United States and other countries.

Open Socket is a registered trademark of Novell, Inc. in the United States.

Packet Burst is a trademark of Novell, Inc.

PartnerNet is a trademark and service mark of Novell, Inc.

PC Navigator is a trademark of Novell, Inc.

PCOX is a registered trademark of Novell, Inc. in the United States and other countries.

Perform3 is a trademark of Novell, Inc.

Personal NetWare is a trademark of Novell, Inc.

Pervasive Computing from Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Portable NetWare is a trademark of Novell, Inc.

Presentation Master is a registered trademark of Novell, Inc. in the United States and other countries.

Print Managing Agent is a trademark of Novell, Inc.

Printer Agent is a trademark of Novell, Inc.

QuickFinder is a trademark of Novell, Inc.

Red Box is a trademark of Novell, Inc.

Reference Software is a registered trademark of Novell, Inc. in the United States and other countries.

Remote Console is a trademark of Novell, Inc.

Remote MHS is a trademark of Novell, Inc.

RX-Net is a trademark of Novell, Inc.

RX-Net/2 is a trademark of Novell, Inc.

ScanXpress is a registered trademark of Novell, Inc. in the United States and other countries.

Script Director is a registered trademark of Novell, Inc. in the United States and other countries.

Sequenced Packet Exchange and SPX are trademarks of Novell, Inc.

Service Response System is a trademark of Novell, Inc.

Serving FTP is a trademark of Novell, Inc.

SFT is a trademark of Novell, Inc.

SFT III is a trademark of Novell, Inc.

SoftSolutions is a registered trademark of SoftSolutions Technology Corporation, a wholly owned subsidiary of Novell, Inc.

Software Transformation, Inc. is a registered trademark of Software Transformation, Inc., a wholly owned subsidiary of Novell, Inc.

SPX/IPX is a trademark of Novell, Inc.

StarLink is a registered trademark of Novell, Inc. in the United States and other countries.

Storage Management Services and SMS are trademarks of Novell, Inc.

Technical Support Alliance and TSA are collective marks of Novell, Inc.

Third-Party Trademarks