

Novell NetWare 6.5

#.#

February 28, 2005

NOVELL DNS/DHCP SERVICES
ADMINISTRATION GUIDE

www.novell.com

N

Novell®

Legal Notices

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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Novell DNS/DHCP Services for NetWare Administration Guide for NetWare 6.5

February 28, 2005

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

Novell Trademarks

Novell is a registered trademark of Novell, Inc. in the United States and other countries.
SUSE is a registered trademark of SUSE LINUX AG, a Novell business.

Third-Party Materials

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

Contents

- Contents** **5**
- About This Guide** **9**
- 1 Understanding DNS/DHCP Services** **11**
 - DNS 11
 - DNS Hierarchy 12
 - DNS Name Service 15
 - Resource Records 18
 - DNS Structure. 19
 - Novell DNS Services 22
 - Novell eDirectory Objects for DNS 23
 - eDirectory Schema Extensions for DNS 25
 - DNS SNMP Events 27
 - Dynamic DNS 27
 - Zone Transfer 28
 - ICE Zone Handlers 29
 - Dynamic Reconfiguration 30
 - Fault Tolerance 30
 - Cluster Support 31
 - Notify 31
 - Load Balancing 32
 - Forwarding 32
 - No-forwarding 32
 - Benefits of Integrating DNS Server with eDirectory. 33
 - DHCP 33
 - DHCP and BOOTP 36
 - IP Address Allocation 37
 - Virtual LAN Environments. 38
 - DHCP Auditing 38
 - DHCP Options 38
 - eDirectory Objects for DHCP 40
 - DNS/DHCP Management Utility and Management Console 42
 - Management Utility 43
 - Management Console. 45
- 2 Planning Your DNS/DHCP Implementation** **51**
 - Resource Requirements 51
 - eDirectory Considerations 51
 - Planning a DNS Strategy 52
 - Planning Zones 52
 - Using the Novell DNS Server as a Primary Name Server 53
 - Using the Novell DNS Server as a Secondary Name Server 53
 - Configuring a DNS Server to Forward Requests 53
 - Setting Up the IN-ADDR.ARPA Zone 54
 - Registering Your DNS Server with Root Servers 54

| | |
|--|------------|
| Planning a DHCP Strategy | 55 |
| Network Topology | 55 |
| eDirectory Implementation | 56 |
| Lease Considerations | 56 |
| IP Address Availability | 58 |
| Hostnames | 59 |
| 3 Installing DNS/DHCP Services | 61 |
| Installation | 61 |
| Management Utilities | 62 |
| DNS/DHCP iManager Utility | 62 |
| DNS/DHCP Java-Based Management Console | 64 |
| eDirectory Rights Required to Manage DNS/DHCP Configuration | 65 |
| Upgrade | 65 |
| Validating the DNS/DHCP Services Installation | 66 |
| Repair Utility | 66 |
| Uninstallation | 67 |
| DNS/DHCP Services | 67 |
| Uninstalling the iManager Utility | 67 |
| Uninstalling the Java-Based Management Console | 67 |
| 4 Configuring DNS | 69 |
| Configuring Clients to Use DNS | 69 |
| DNS Server Configuration Parameters | 69 |
| NetWare 6.5 DNS Server Options | 70 |
| Zone Configuration Parameters | 73 |
| Using the iManager Utility to Configure DNS | 75 |
| Scope Settings | 75 |
| DNS Prerequisites | 76 |
| DNS Server Management | 76 |
| Zone Management | 83 |
| Resource Record Management | 87 |
| Using the Java-Based Management Console to Configure DNS | 89 |
| DNS Prerequisites | 89 |
| Logging In to the Tree for DNS Setup | 90 |
| DNS Server Management | 90 |
| Zone Management | 94 |
| Resource Record Management | 97 |
| Command Line Options | 99 |
| Configuring DNS Features | 99 |
| Configuring Roles for Novell DNS Server | 100 |
| Configuring a DNS Server to Forward Queries to Root Name Servers | 100 |
| Configuring a DNS Server as a Cache-Only Server | 100 |
| Configuring Child (Sub) Zone Support | 101 |
| Configuring a Multi-Homed Server | 101 |
| Configuring Dynamic DNS | 101 |
| Loading the DNS Server | 102 |
| NAMED Command Line Options | 102 |
| Description of Command Line Options | 103 |
| 5 Configuring DHCP | 107 |
| Configuring Clients to Use DHCP | 107 |
| Logging In to the Tree for DHCP Setup | 107 |
| Using the iManager Utility to Configure DHCP | 108 |
| Scope Settings | 108 |
| DHCP Prerequisites | 109 |
| 6 Novell DNS/DHCP Services for NetWare Administration Guide for NetWare 6.5 | |

| | |
|---|------------|
| Global DHCP Configuration | 109 |
| DHCP Server Management | 112 |
| Subnet Pool Management | 116 |
| Subnet Management | 117 |
| Address Range Management | 119 |
| IP Address Management | 121 |
| Using the Java-Based Management Console to Configure DHCP | 123 |
| DHCP Prerequisites | 123 |
| Global DHCP Configuration | 123 |
| DHCP Server Management | 127 |
| Subnet Pool Management | 130 |
| Subnet Management | 131 |
| Address Range Management | 132 |
| IP Address Management | 133 |
| Command Line Options | 135 |
| Configuring Multiple Logical Networks | 135 |
| Loading the DHCP Server | 135 |
| DHCP SRVR Command Line Options | 136 |
| Monitoring DHCP | 136 |
| Events and Alerts | 136 |
| Auditing Server Activity | 137 |
| DHCP SNMP Events | 137 |
| 6 Troubleshooting | 139 |
| DNS | 139 |
| Troubleshooting Checkpoints | 139 |
| Common Installation and Upgrade Problems | 140 |
| Common Configuration Problems | 141 |
| Common Operational Problems | 145 |
| Troubleshooting Windows 95 TCP/IP Problems | 149 |
| Using the -F Command Line Option for Dninst.nlm | 153 |
| Server Access to DNS/DHCP Locator Object Not Required | 153 |
| DHCP | 154 |
| Troubleshooting Checkpoints | 154 |
| Common Operational Problems | 155 |
| Releasing and Renewing DHCP Addresses | 157 |
| Console and Debug Logs | 157 |
| 7 DNS/DHCP Advanced Features | 159 |
| Configuring the ICE Zone Handler | 159 |
| Modifying the ice.cfg File | 159 |
| Importing Configuration and Script Files | 160 |
| Exporting Configuration and Script Information | 162 |
| Cluster Support | 163 |
| Clustering in NetWare 6.0 | 163 |
| Clustering in NetWare 6.5 | 163 |
| Creating a Cluster-Enabled DNS Server | 163 |
| Configuring a DNS Server in a Clustered Environment | 164 |
| Deleting Empty Resource Records | 166 |
| 8 OES Coexistence and Migration Issues | 169 |
| Coexistence | 169 |
| Compatibility | 169 |
| Coexistence Issues | 169 |
| Migration | 170 |
| Pre-requisites | 170 |

| | |
|-------------------------------------|------------|
| Recommended Procedure | 170 |
| Migration Issues | 171 |
| A Appendix | 173 |
| Supported RFCs | 173 |
| Types of Resource Records | 174 |
| DHCP Option Descriptions | 176 |
| Assigning Options | 183 |
| DNS-DHCP SNMP Events | 184 |
| DNS Root Servers | 185 |
| B Glossary | 187 |

About This Guide

This document describes 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[®] 6.5.

The audience for this document is network administrators. This documentation is not intended for users of the network. This guide is divided into the following sections:

- ◆ Chapter 1, “Understanding DNS/DHCP Services,” on page 11
- ◆ Chapter 2, “Planning Your DNS/DHCP Implementation,” on page 51
- ◆ Chapter 3, “Installing DNS/DHCP Services,” on page 61
- ◆ Chapter 4, “Configuring DNS,” on page 69
- ◆ Chapter 5, “Configuring DHCP,” on page 107
- ◆ Chapter 7, “DNS/DHCP Advanced Features,” on page 159
- ◆ Chapter 6, “Troubleshooting,” on page 139
- ◆ Appendix A, “Appendix,” on page 173
- ◆ Appendix B, “Glossary,” on page 187

Documentation Updates

For the most recent version of the *Novell DNS/DHCP Services Administration Guide*, see the *NetWare* (<http://www.novell.com/documentation>) documentation.

Documentation Conventions

In this document, the term *iManager utility* is used to refer to the DNS/DHCP iManager Utility, and the term *Management Console* is used to refer to the DNS/DHCP Java-Based Management Console.

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

In this documentation, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX*, should use forward slashes as required by your software.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with NetWare 6.5. To contact us, use the User Comments feature at the bottom of any page in the online documentation.

1

Understanding DNS/DHCP Services

This section describes the Domain Name System (DNS), the Dynamic Host Configuration Protocol (DHCP), and the Novell® eDirectory™ schema extension; it also explains their eDirectory-related functions. This section also provides information about the zone handler, the iManager utility and the Management Console.

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

The iManager utility provides a Web interface to manage the objects created to support DNS and DHCP and runs in a browser window. It does not require a Novell Client™ or any installed component as a prerequisite. It shares a common interface with other utilities that are based on the iManager framework, and is thus tightly integrated with NetWare.

The Management Console is a Java* application that provides a graphical user interface to manage the objects created to support DNS and DHCP. The 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 detailed overview information, see the following:

- ◆ [“DNS” on page 11](#)
- ◆ [“Novell DNS Services” on page 22](#)
- ◆ [“DHCP” on page 33](#)
- ◆ [“DNS/DHCP Management Utility and Management Console” on page 42](#)

DNS

DNS is a distributed database system that provides hostname-to-IP resource mapping (usually the IP address) and other information for computers on a network. 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, see:

- ◆ [“DNS Hierarchy” on page 12](#)
- ◆ [“DNS Name Service” on page 15](#)
- ◆ [“DNS Resolver” on page 16](#)

- ◆ “Resource Records” on page 18
- ◆ “DNS Structure” on page 19

DNS/DHCP supports the standards of the Internet Request For Comments (RFCs). For more information, see [Appendix A, “Appendix,” on page 173](#).

DNS Hierarchy

DNS uses a hierarchy to manage its distributed database system. The DNS hierarchy, also called the domain namespace, is an inverted tree structure, much like eDirectory. Each node in the tree has a text label, which is zero to 63 characters long. The label (zero length) is reserved and is used for the root.

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.

There are three types of Top Level Domains (TLD):

- ◆ “Generic TLD” on page 12
- ◆ “Country Code TLD” on page 13
- ◆ “Infrastructure TLD” on page 13

Below the top-level domains, the domain namespace is further divided into subdomains representing individual organizations.

A list of TLDs is available at the [Internet Assigned Numbers Authority Web site \(http://www.iana.org\)](http://www.iana.org).

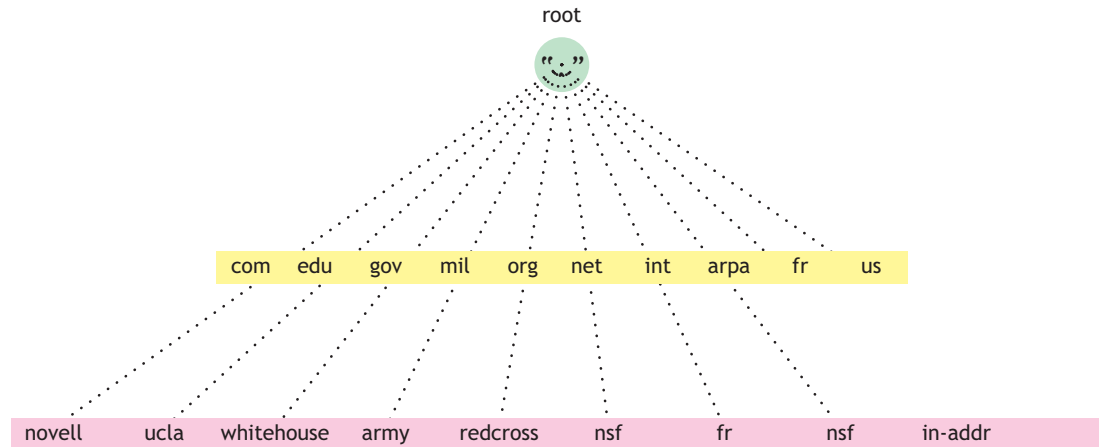
Generic TLD

The following table shows the top-level DNS domains and the organization types that use them:

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

The DNS hierarchy is shown in [Figure 1 on page 13](#).

Figure 1 DNS Hierarchy



Country Code TLD

Top-level domains organize domain namespace geographically.

| Domain | Used by |
|--------|---------------|
| .fr | France |
| .in | India |
| .jp | Japan |
| .us | United States |

Infrastructure TLD

The .arpa (Address and Routing Parameter Area) TLD is used extensively for Internet-infrastructure. It contains the in-addr.arpa, ipv6.arpa, etc., subdomains.

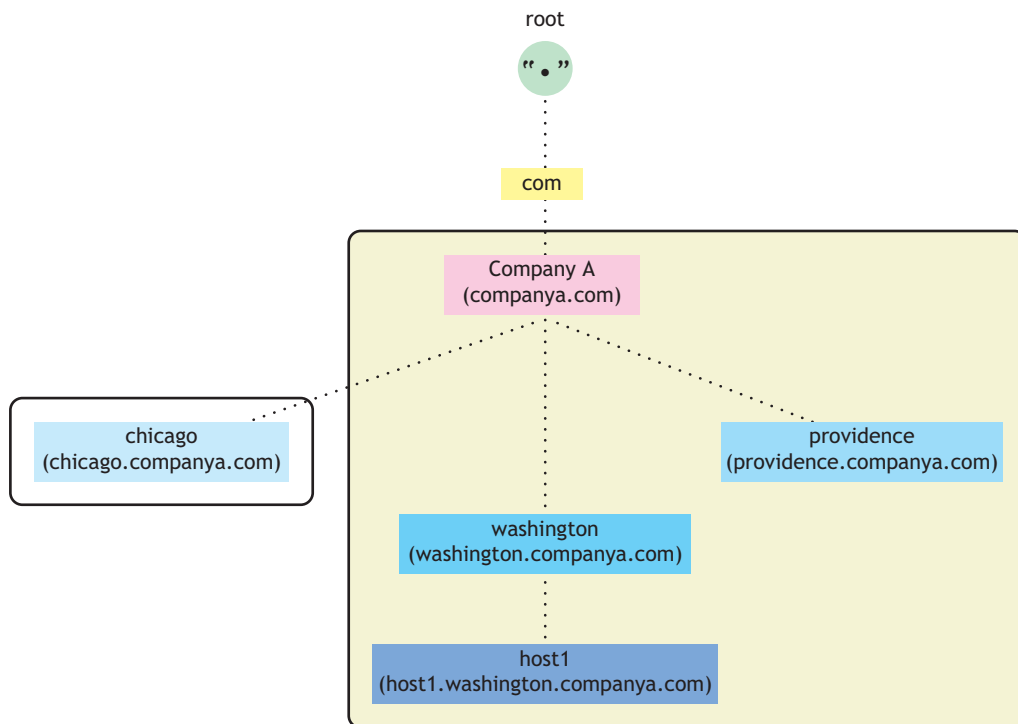
Domains and Subdomains

A domain is a subtree 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 called `companya.com` under the `com` top-level domain. 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 2 on page 14](#).

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 2 Domains and Subdomains



Domain Names

The domain name represents the position of an entity within the structure of the DNS hierarchy. The domain name of a node is the list of the labels on the path from the node to the root of the tree. Domain names are not case sensitive and their length is limited to 255 characters. Valid characters for the domain names are a-z, A-Z, 0-9, hyphens, and underscores. 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 2](#).

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 2](#) is host1.washington.companya.com.

NOTE: The domain names in the figure end with a period, representing the root domain. Domain names that end with a period are called Fully Qualified Domain Names (FQDNs).

IN-ADDR.ARPA Domain

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

The file that stores the IN-ADDR.ARPA data contains pointer (PTR) records and additional name server records, including the Start of Authority (SOA) records, which are similar to the 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 10.10.11.1 requires a PTR query with the target address of 1.11.10.10.in-addr.arpa.

Domain Delegation

Domain delegation gives authority to an organization 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. Domain delegation helps in distributing the DNS namespace.

Cuts can be made between any two adjacent nodes in the namespace. After all cuts are made, each group of connected namespace is considered as a separate zone. The zone is authoritative for all names in the connected region, and these cuts are managed by domain delegation. All the host information for a zone is maintained in a single authoritative database.

For example, in [Figure 2 on page 14](#), companya.com. domain is delegated to company A, creating the companya.com. zone. There are three subdomains within the companya.com. domain:

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

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

For example, if company A's Chicago location has its own network administrator, they could make a cut between the chicago.companya.com domain and the companya.com domain and then delegate the chicago.companya.com zone. Then companya.com would have no authority over chicago.companya.com. Company A would have two domains:

- ◆ companya.com zone, which has authority over the companya.com, washington.companya.com, and providence.companya.com domains
- ◆ chicago.companya.com zone, which has authority over the chicago.companya.com domain

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

Name servers are information repositories that make up the domain database. The database is divided into sections called zones, which are distributed among the name servers. The name servers answer queries using data in their zones or cache. 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.

All name servers maintain information about contacting name servers that are available in other parts of the DNS namespace. This process of maintaining information is called linking to the existing DNS hierarchy. This is done by providing information about the root name servers. The administrator also enters information into the database about name servers in the lower-level

domains. For example, when creating a subdomain, the administrator would provide the name server information of the subzone.

Primary Name Servers

One DNS name server in each administrative zone maintains the read-write copies of hostname database 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.

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, the secondary name server contacts the primary name server and requests a full or incremental copy of the primary name server's DNS database. This process is called zone transfer.

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

Root Name Servers

Root name servers contain information for the name servers in all top-label domains. The root server plays a very significant role in resolving DNS query. Currently, there are 13 name servers available, which contain information of the name servers for all TLDs.

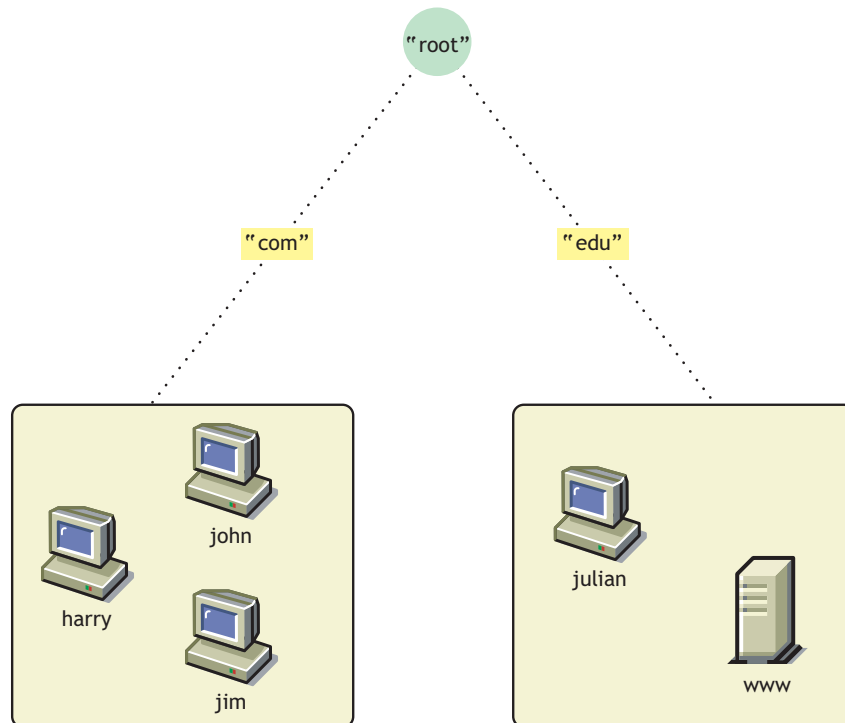
DNS Resolver

Resolvers are programs. They interface user programs to domain name servers. A resolver receives a request from a user program and returns the desired information. It basically does a name-to-address, address-to-name, and general lookup.

Name Resolution

DNS is a distributed database with multiple servers that maintain different parts of the same tree. The links between the servers are through root server and domain delegation as shown in [Figure 3 on page 17](#).

Figure 3 DNS Namespace



DNS queries can be resolved in two ways:

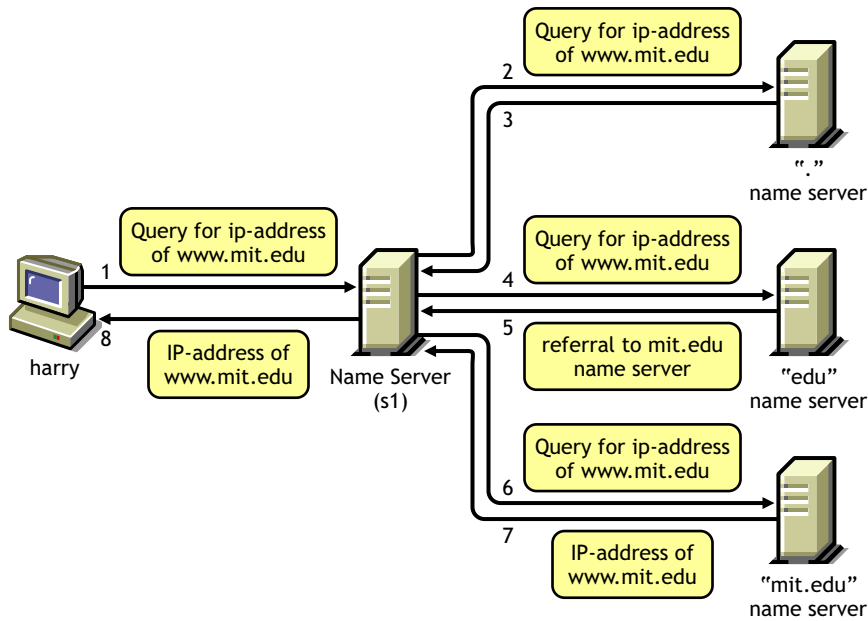
- ♦ **Iterative query:** An iterative request from a client expects the best actual answer or referral that the DNS server can immediately provide, without contacting other DNS servers.

For example, in [Figure 4 on page 18](#), Harry initiates an iterative query for A record of `www.mit.edu`. After receiving this query, the name server (s1) might return the answer, if the answer is available in the cache. If the answer is not available, the server will return a referral [NS and A rrs] to the other DNS servers that are closer to the names queried by the client.

- ♦ **Recursive query:** A recursive request from a client expects the actual answer that the DNS server can provide either from its own cache or by contacting other DNS servers.

For example, in [Figure 3](#) and in [Figure 4 on page 18](#), Harry initiates a recursive query for A record of `www.mit.edu`. After receiving this query, the name server (s1) will contact the root server to resolve this query and get the referrals (name server info) for `edu. zone`. Now, s1 will again initiate a query for A record of `www.mit.edu` to the name server (using the referrals received) of `edu.zone` and will get the referrals for `mit.edu.zone`. Server s1 will again initiate a query for A record of `www.mit.edu` to the name server (using the referrals received) of `mit.edu. zone` and will get the A record. This A record will be returned to Harry.

Figure 4 Name Resolution



Caching

Caching is a mechanism to improve the performance of query resolution. The cache memory will be empty when a server first starts. This cache is built as it starts resolving queries. It will cache all the answers and referrals during recursive queries, and the cached data will remain in the cache memory until the Time-To-Live (TTL) expires. The TTL specifies the time interval that the entries can be cached before they are discarded.

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 in order 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 itself) for each primary and secondary name server of the zone. It must also contain NS records of the lower-level zones (if any) to provide links within the DNS hierarchy.

- ◆ Start of Authority (SOA)—Indicates the start of authority for the zone.

The name server must contain only one SOA record, specifying its zone of authority.

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

- ◆ NS records for delegated zones, if any
- ◆ A records for the NS record (if applicable)

For more information about Resource Record types and their RDATA (Resource Record data), see “Types of Resource Records” on page 174.

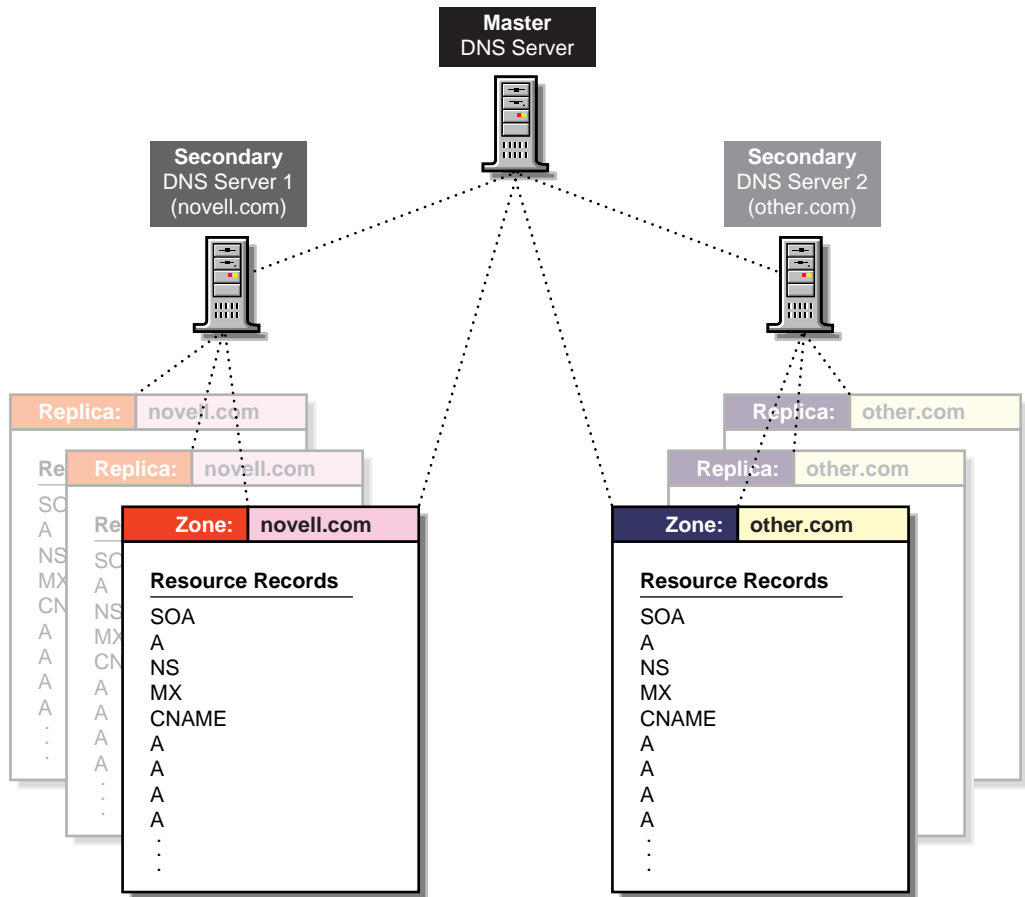
DNS Structure

DNS is administered by building a database of information that includes all the resource records of a zone into a text file called a master file. The administration of these files is difficult and cumbersome. Initial versions of the Novell DNS server used Btrieve as its database. Other vendors also use large files to store information required for a DNS zone.

Figure 5 on page 20 represents a traditional DNS strategy. A zone, such as novell.com, uses a primary DNS server to handle queries about the entities within it. A DNS server supports more than one zone, and it has at least one secondary server for backup (redundancy) or load-sharing purposes. The primary DNS server provides DNS name service for two zones: novell.com and other.com. The secondary DNS server 1 provides backup support for novell.com zone, and the secondary DNS server 2 provides backup support for other.com zone. When changes occur to the DNS database, the master files corresponding to that zone at the secondary server are updated by zone transfers.

The file storing the resource records 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.

Figure 5 DNS Structure



DNS Master File

A DNS master file is a text file that contains resource records that describe a zone. When you build a zone, the DNS objects and their attributes translate into resource records for that zone.

You can import a DNS master file if it conforms to IETF RFCs 1034, 1035, and 1183 and is in BIND master file format. A sample DNS master file is shown in the following example.

```
$ORIGIN companya.com.

@      soa      ns.companya.com.  admin.novell.com (
                                1996091454 /* SOA sr no */
                                3600 /* Zone Refresh interval*/
                                300 /* Zone retry interval */
                                604800 /* Zone Expire interval */
                                86400) /* Zone Minimum TTL */

      ns      ns1.companya.com.
      ns      ns2.companya.com.
      mx      5      companya.com.

$ORIGIN companya.com.
ns1   a      123.45.67.89
ns2   a      123.45.68.103; End of file
```

Master File Directives

The master file directives include \$GENERATE, \$ORIGIN, \$INCLUDE, and \$TTL.

- ◆ **\$GENERATE:** Enables you to create a series of resource records that differ from each other only by an iterator.

The syntax is:

```
$GENERATE range lhs type rhs [comment]
```

Range can be set to start–stop or start–stop/step. All values for start, stop, and step must be positive.

lhs is the owner name of the records to be created. The \$ symbols in the lhs will be replaced by the iterator value. Using \ \$ allows a \$ symbol in the output. A \$ can be optionally followed by a modifier as $\$[\{\text{offset}[\text{width}[\text{base}]]\}]$.

A modifier can have an offset, a width, and a base. The offset is used to change the value of the iterator, base specifies the output format in which the values are printed, and width is used for padding. The available base values are decimal (d), octal (o), and hexadecimal (x or X). The default modifier is $\$\{0, 0, d\}$. If the lhs is not absolute, the current value of \$ORIGIN is appended to the name.

Type is the resource record type. The supported types are PTR, CNAME, DNAME, A, AAAA, and NS.

rhs is the domain name and processed similarly to lhs.

For example,

```
$ORIGIN 0.0.192.IN-ADDR.ARPA
```

```
$GENERATE 1-2 0 NS SERVER$.EXAMPLE.com
```

is equivalent to

```
0.0.0.192.IN-ADDR.ARPA NS server1.example.com
```

```
0.0.0.192.IN-ADDR.ARPA NS server2.example.com
```

- ◆ **\$ORIGIN:** Enables you to set the domain name as the origin. The origin is appended to all domain names in the zone data file that do not end with a dot.

The syntax is:

```
$ORIGIN domain-name [comment]
```

For example,

```
$ORIGIN example.com.
```

```
WWW CNAME Web server
```

is equivalent to

```
WWW.EXAMPLE.COM. CNAME webserver.example.com.
```

- ◆ **\$INCLUDE:** Enables you to include another file in the current file. The included file can be read and processed as if it were present in the current file at that point. The domain name can also be specified with the \$INCLUDE directive, to process the file included with \$ORIGIN set to that value. If the origin is not specified, the current \$ORIGIN is used.

After the included file is processed, the origin and the domain name values are reset to their previous values before processing the included file.

The syntax is:

```
$INCLUDE filename [origin] [comment]
```

NOTE: This directive is not supported in the Management utilities. Use the ICE utility to use this directive.

- ◆ **\$TTL:** Enables you to set the default time to live for the subsequent resource records without any TTL values. The time range for TTL is from 0 to 214748367 seconds. If the \$TTL value is not present in the master file, SOA minimum TTL is used as the default.

The syntax is:

```
$TTL default-ttl [comment]
```

Novell DNS Services

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

Integrating DNS with eDirectory greatly simplifies network administration by enabling you to enter all configuration information into one distributed database. The DNS configuration information is replicated just like any other data in eDirectory.

By integrating DNS into eDirectory, Novell has shifted the concept of a primary or secondary away from the server to the zone itself. After you have configured the zone, the data is available to any of the Novell DNS servers you select to make authoritative for the zone. The Novell DNS server takes advantage of the peer-to-peer nature of eDirectory 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 get transferred data from a non-Novell master server. All Novell DNS servers can then access the data through eDirectory replication.

Novell DNS/DHCP Services provides the following DNS features:

- ◆ All DNS configuration is stored in eDirectory, facilitating enterprise-wide management.
- ◆ A Novell DNS server can be a secondary name server to a zone (DNS data loaded into eDirectory through a zone transfer), or it can be a primary name server.
- ◆ DNS data can be imported using a BIND Master file to populate eDirectory for convenient upgrades from BIND implementations of DNS.
- ◆ DNS data can be exported from eDirectory into BIND Master file format.
- ◆ Root server information is stored in eDirectory and shared by all eDirectory-based DNS servers.
- ◆ Zone transfers are made to and from Novell servers. Full Zone Transfer-In (AXFR) and Incremental Zone Transfer-In (IXFR) are supported when the server is a designated secondary. Any type of server can perform a zone-out transfer.
- ◆ A Novell DNS server can be authoritative for multiple domains.
- ◆ Novell DNS servers maintain a cache of data from eDirectory so they can quickly respond to queries.

- ◆ A Novell DNS server can act as a caching or forwarding server.
- ◆ A Novell DNS server supports fault tolerance when there is an eDirectory service outage.
- ◆ Novell DNS servers support multihoming.
- ◆ DNS auditing can help diagnose problems. Each incident of zone transfer or server up and down is recorded.
- ◆ Novell DNS server software supports shuffling responses to queries that have multiple resource records.
- ◆ Novell DNS server is multi-threaded and MP-safe.
- ◆ Novell DNS server supports dynamic reconfiguration (automatic detection of the configuration and data changes).

Novell eDirectory Objects for DNS

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

A Zone object is an eDirectory container object that holds RRSet objects, which are leaf objects. A DNS server object is a leaf object. For detailed information about these objects, see [“eDirectory Objects and Attributes for DNS” on page 25](#).

By integrating DNS into eDirectory, 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 data changes are made on a single primary name server. When changes are 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, the Novell approach allows changes from anywhere in the network through eDirectory, which is not dependent on one server. Zone data is stored within eDirectory and is replicated just like any other data in the eDirectory tree.

The Novell implementation of DNS supports the traditional primary-secondary DNS name server approach to moving DNS data in and out of eDirectory. Although all Novell servers can recognize DNS data after the data is placed in the directory through eDirectory 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 (Designated Secondary) 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 eDirectory 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 dynamic updates from a 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 6 on page 24](#) illustrates a Novell server as the primary and secondary DNS name server and also illustrates primary and secondary zones within eDirectory. In this example, there are two zones. Any of the Novell DNS servers assigned to a zone is able to respond authoritatively to

queries for the zone. For each zone, one server is designated by the administrator to act as the DDNS server. S1 is the Designated Primary DNS server for Zone 1 and S3 is a Passive Primary server. S1 accepts the Dynamic updates from the DHCP server. S2 is the Zone In (Designated Secondary) server and S4 is the Passive Secondary server for the secondary zone zone2, called the Foreign Zone. S2 occasionally requests zone transfers from the foreign server and places the modified zone data into eDirectory, where any of the Novell servers can respond to queries for it. S3 and S4 will get the latest data through eDirectory.

Figure 6 Novell Server As a Primary/Secondary DNS Server

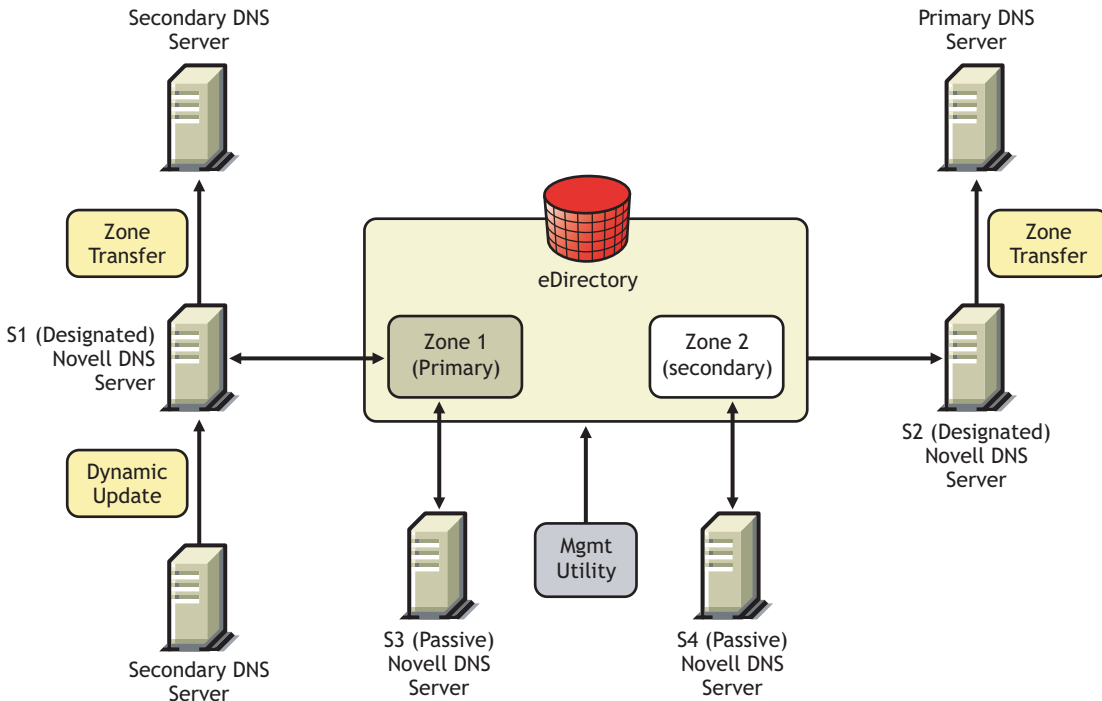
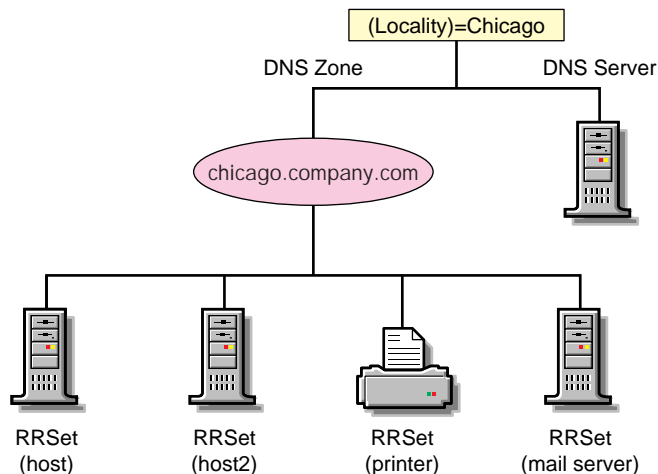


Figure 7 shows a representation of eDirectory objects within a DNS zone.

Figure 7 DNS Zone



eDirectory Schema Extensions for DNS

The eDirectory schema extension defines additional objects needed for DNS and DHCP.

DNS/DHCP Global eDirectory Objects

When you select Novell DNS/DHCP Services during the NetWare 6.5 installation, the eDirectory 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 exists in an eDirectory tree. The DNS servers, DHCP servers, iManager, and Management Console must have access to these objects.

The DNS/DHCP Group object is a standard eDirectory group object. The DNS and DHCP servers gain rights to DNS and DHCP data within the tree through the Group object.

The DNS/DHCP Locator object is created during the NetWare 6.5 installation, if the DNS/DHCP option is chosen. The creator of the Locator object will grant Read and Write rights to this object to the network administrators.

The DNS/DHCP Locator object contains global defaults, DHCP options, and a list of all DNS and DHCP servers, subnets, and zones in the tree. The iManager utility and Management Console use the Locator object contents instead of searching the entire tree to display these objects. The Locator object is basically hidden by the iManager utility and Management Console.

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

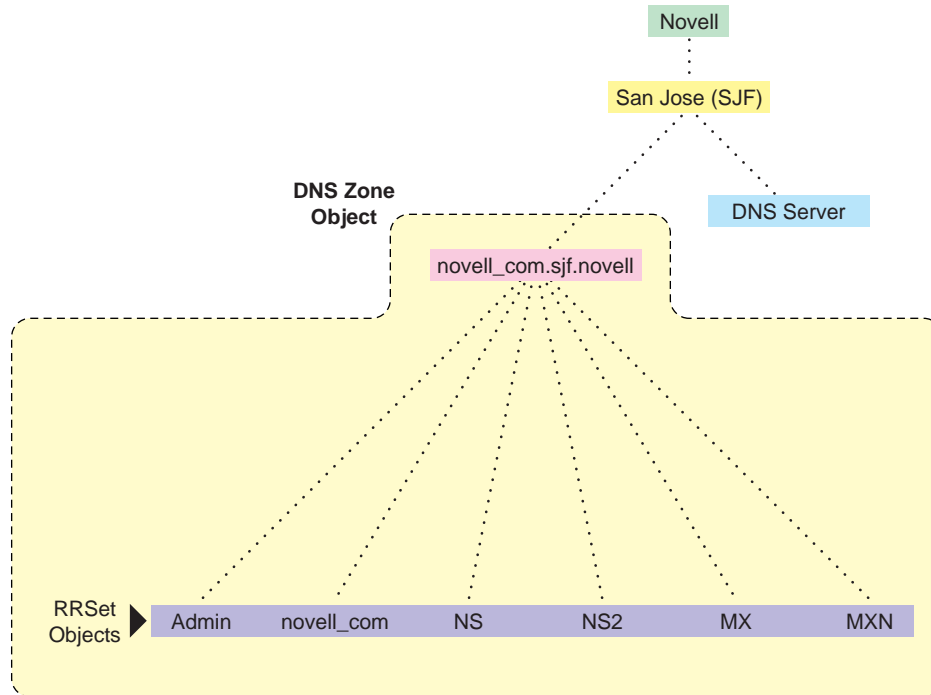
eDirectory Objects and Attributes for DNS

The following new eDirectory objects are required for DNS:

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

[Figure 8 on page 26](#) shows an example of a tree with DNS objects.

Figure 8 eDirectory Objects for DNS



DNS Server Object

The DNS server object (or Service object) is created by extending the NetWare Core Protocol™ (NCP) server object. The DNS server reference is stored in the NCP server during the creation of the 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
- ◆ Access Control List for zone transfer, query, recursion, notify, etc.
- ◆ Other additional advanced options to fine-tune the DNS server

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 zones can be represented within eDirectory by using separate, independent DNS Zone objects. A network administrator can support multiple DNS zones 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 eDirectory-based DNS servers that serve the zone, and Dynamic DNS (DDNS) server information.

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

DNS object names are created using the DNS Zone names as follows:

All “.” will be replaced by “_” and all “_” will be replaced by “#”. The only supported characters for domain names are a-z, A-Z, 0-9, hyphens, and underscores. For example, the name of the Zone object for new.york.companya.com zone, which exists in an eDirectory context sjf.us., would be new#york.companya_com.sjf.us.

DNS Resource Record Set Object

The DNS Resource Record Set (RRSet) object is an eDirectory 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 and Resource Records (RRs).

Each domain name within a DNS zone object has an RRSet object. Each RRSet object has one or more resource records beneath it that contain additional information about the zone data.

DNS Resource Records

A DNS resource record (RR) is an attribute of an RRSet that contains the resource record 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 SNMP Events

SNMP event generation can be set up in a Novell DNS server for all, major, or no events. The default setting is none, which causes the server not to log any event.

SNMP trap flag is a single-valued attribute in eDirectory, which is an optional attribute in the DNS server objects. SNMP trap flag can be set using the management utilities.

SNMP event generation can be set up either for trapping major events or all events. This can also be disabled for not generating any traps.

Dynamic DNS

Dynamic DNS (DDNS) provides a way to dynamically update DNS with resource records from applications such as DHCP servers, DNS clients, etc. DDNS eliminates the need for any additional configuration of DNS for each host address change. Novell DNS server supports the following DDNS mechanisms:

- ◆ Novell DDNS, a mechanism by which Novell DHCP servers update Novell DNS servers
- ◆ RFC 2136-based dynamic updates

All changes made to a zone using dynamic updates are stored in the zone's journal file. This file is automatically created by the server in a binary format when the first dynamic update takes place. The journal file name has the .jnl extension. This file is also used for IXFR.

NOTE: Do not edit the contents of the journal file.

Novell DDNS

The Dynamic DNS (DDNS) feature of Novell DNS/DHCP Services provides a way to update DNS with accurate Address (A) records and Pointer (PTR) records for address assignments made by a DHCP server. Address (A) records map a domain name to an IP address. A Pointer (PTR) record specifies a domain name that points to some location in the domain namespace. These resource records are required for both name-to-address and address-to-name resolutions.

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.

When the DHCP server grants a lease to a client that is subject to DDNS updates, the DHCP server updates its IP address database and eDirectory 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.

NOTE: While using the Novell DHCP server, both the forward and reverse zones must be designated primary on a single server.

2136 Dynamic Update

Novell DNS server supports dynamic updates complying the RFC 2136 standards. This support provides the ability to update various types of resource records into DNS under certain specified conditions. Dynamic update is fully described in RFC 2136.

2136 dynamic update can be enabled or disabled on a zone-by-zone basis, by specifying the allow-update filter for the zone. It grants permission to the clients to update any record or name in the zone.

Zone Transfer

Zone transfer is essential for maintaining up-to-date zone data in the server. When a Novell server is designated as primary, all the changes made by the designated primary to eDirectory are reflected in the eDirectory replicas, using the eDirectory sync property. When a Novell server is designated secondary, zone transfer is needed for receiving the most up-to-date zone data from any primary servers.

The designated secondary server sends a zone-in request after the refresh time interval or after receiving a notification from the primary server. The zone transfer-in requests are not triggered if the eDirectory services are not available.

The final step in a successful zone transfer-in is to update the SOA serial number. The passive secondary servers compare the eDirectory SOA serial number with their own copy to determine whether there is a need to synchronize the data from eDirectory.

The following types of zone transfers are supported:

- ◆ **Full-Zone Transfer-In**
- ◆ **Incremental Zone Transfer-In**

NOTE: No zone transfers-in will be initiated if it fails while the zone transfer is taking place. The changed data will be overwritten during the next zone transfer.

Full-Zone Transfer-In

The secondary server receives a full zone transfer-in (AXFR) into a different zone database. After the complete zone data is received, the server will replace the old database with the new one, and will try to identify the difference between the existing zone database and the new database that is received. This difference is then applied to eDirectory for better performance.

For more information on DNS AXFR, refer to RFC 1034.

Incremental Zone Transfer-In

Incremental zone transfer-in (IXFR) is considered to be a more efficient zone transfer mechanism than AXFR because it transfers only the changed data of the zone. IXFR transfers only the modified data using the journal file maintained by the DNS server. When a server gets an IXFR request (which has the current SOA serial number of the requester), the server looks into the JNL file to get the modified data from that SOA serial number to the latest SOA serial number and returns the data to the requester.

For more information on DNS IXFR, refer to RFC 1995.

ICE Zone Handlers

ICE zone handler is a utility to import or export the DNS server, zone configuration information, and data to or from the eDirectory database.

The Import-Convert-Export (ICE) utility is a framework provided by Novell that contains the ICE engine, the source handler, and the destination handler. This provides a command line interface to access its functionality and to read the required data. It expects the data processed by the handlers in LDAP format.

The ICE zone handler is plugged into the ICE framework. The required data and the handler information must be provided using the command line interface, which will be processed by the zone handler and passed to the ICE engine. The ICE engine migrates this data. ICE has the option of using LDAP Bulk Update/Replication Protocol (LBURP) to increase the speed of data migration.

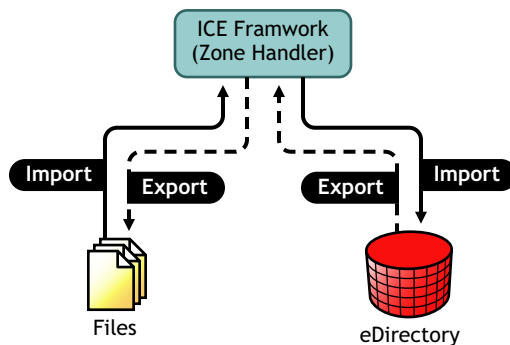
The zone module handlers consist of a zone source handler and a zone destination handler. Using these handlers, data can be migrated from files to eDirectory (import operation) or from eDirectory to the files (export operation).

A zone source handler that forms the data to be imported and the LDAP destination handler that does the eDirectory update operation are used to import a zone. A zone destination handler that reads the required data from eDirectory and the zone source handler that formats the data and writes into the files are used to export a zone.

The table below describes the source and destination handlers for zone import and export.

| Operation | Source Handler | Destination Handler |
|-------------------------------|----------------|---------------------|
| Import (read from file) | Zone | LDAP |
| Export (read from eDirectory) | Zone | Zone |

Figure 9 ICE Framework



For more information, see [“DNS/DHCP Advanced Features” on page 159](#).

Dynamic Reconfiguration

The Novell DNS server supports dynamic reconfiguration. The DNS server will automatically detect and update any change in the server’s or zone’s configuration data. This enables the server to configure itself with these changes without having the administrator intervene to stop and restart the server. Also, out-of-band data changes (creating, modifying, deleting RRs through management utility) are addressed.

The Dynamic reconfiguration is also used to monitor the availability of eDirectory with respect to the individual zones, and to detect and log changes that can be used for fault tolerance.

Fault Tolerance

A Novell DNS server supports fault tolerance during an eDirectory service outage. The DNS server loads the configuration and zone data from eDirectory during startup. Also, the dynamic updates received for zone data are updated to eDirectory. It is essential for the DNS server to maintain backup copies of eDirectory to get to the zone database during eDirectory unavailability.

The DNS server supports standard DNS queries during fault tolerance mode. However, dynamic updates and zone-in transfers are not supported during this mode because eDirectory cannot be updated.

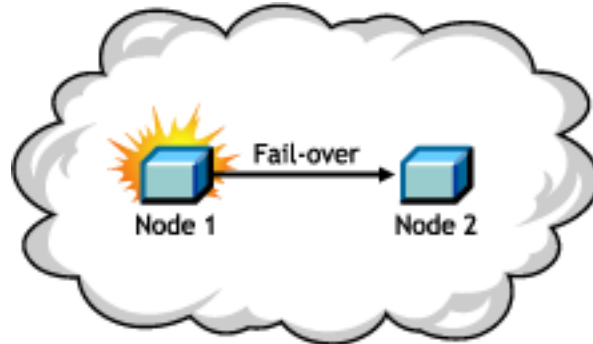
NOTE: During fault tolerance mode operation, eDirectory might not be available for all zones. Operations other than dynamic update and zone-in are supported for zones that are unavailable.

Cluster Support

The Novell DNS server supports cluster service with active-passive and cluster-safe modes. When a DNS server is run on any node, it uses a DNS server object in eDirectory. The cluster-enabled DNS service uses the same DNS server object for the other nodes during a node outage.

When there is a node (node1) outage, clustering enables a DNS server to automatically bring up any other node (node2) using the same server object that was used before the outage. The DNS server object contains a reference to the virtual NCP server, which is used to locate the DNS server object. For more information, see [“Cluster Support” on page 163](#).

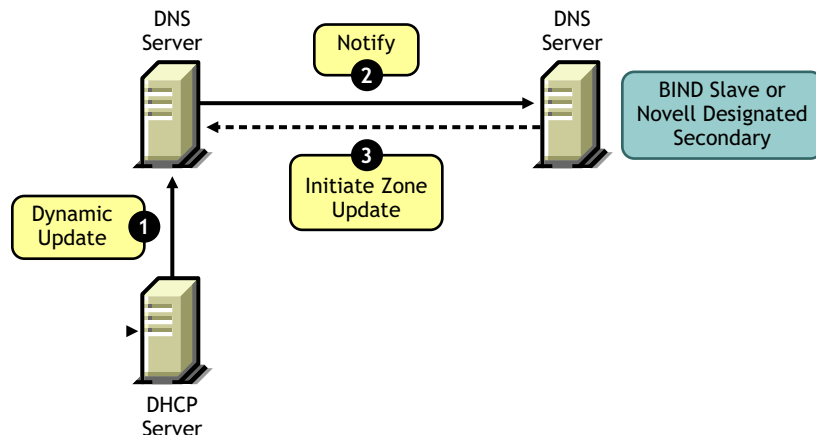
Figure 10 Cluster Support



Notify

DNS Notify is a mechanism that allows master name servers to notify their slave servers of changes to a zone's data. In response to a notification from a master server, the slave verifies the (version) SOA serial number of the zone (sent through the notify mechanism) is the newer compared to the current (version) SOA serial number. If the serial number is newer, a zone transfer is initiated. For Novell DNS servers, receiving Notify is valid only for designated secondary servers. Passive servers receive the latest data through eDirectory replication.

Figure 11 Notify



For more information on DNS notify, refer to RFC 1996.

Load Balancing

If all resolvers querying for a name get the same response, and if all of them contact the same host, then that host becomes overloaded. Primitive load balancing can be achieved in DNS using multiple records for one name. When a resolver queries for these records, the DNS server shuffles them and responds to the query with the records in a different order. See the description of the [RRset-ordering](#).

For example, suppose you have three Web servers with these three different IP addresses:

```
www 3600 IN A 10.10.0.1
    3600 IN A 10.10.0.2
    3600 IN A 10.10.0.3
```

DNS server will randomly shuffle the RRs so that clients randomly receive records in the order 1, 2,3; 2, 3, 1; and 3, 1, 2. Most clients use the first record returned and discard the rest.

Forwarding

The name server can forward some or all of the queries that it cannot satisfy from its authoritative data or cache to another name server; and this is commonly referred to as a forwarder.

Forwarders are typically used when all servers at a given site should not be allowed to interact directly with the rest of the Internet servers. A typical scenario involves a number of internal DNS servers and an Internet firewall. Servers unable to pass packets through the firewall will forward to the server that can do it, and that server will query the Internet DNS servers on the internal server's behalf. An added benefit of using the forwarding feature is that the central machine develops a much more complete cache of information that all of the clients can take advantage of. Forwarding occurs only on those queries for which the server is not authoritative and does not have the answer in its cache.

The forwarding list is a list of IP addresses for the DNS servers to forward the queries to. So if a name server is configured to forward queries to 10.10.10.2, all queries that do not have resolutions to the name server will be forwarded to 10.10.10.2. See [“DNS Namespace” on page 17](#).

NOTE: The forwarding list syntax is different from the Bind 9.2 syntax for forwarders.

No-forwarding

No-forwarding is blocking queries to the list of DNS domains. The No-forward list is the list of domain names whose unresolved queries is not forwarded to other DNS servers.

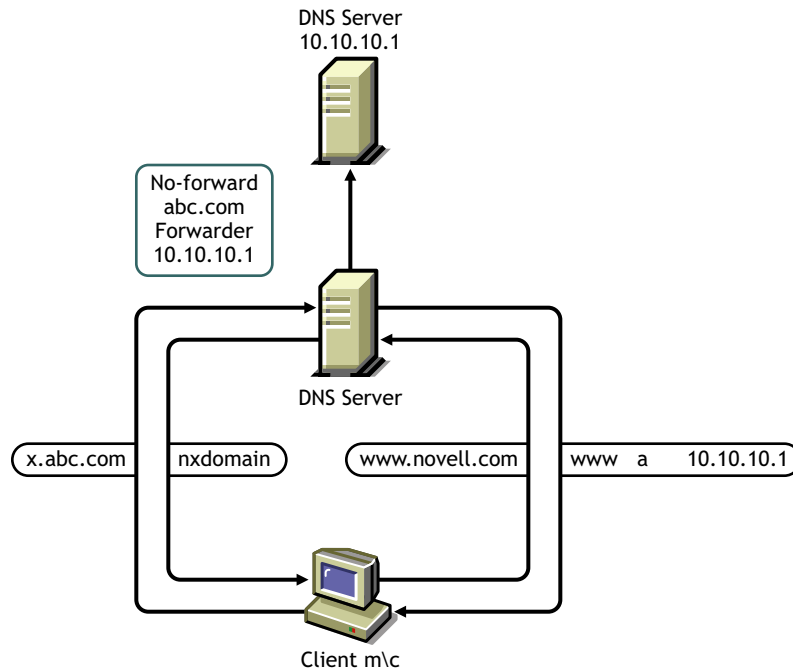
On a query from the client, the authoritative database is first checked. If the domain name is not found, no-forward list is checked. If the no-forward list contains the entry, the query is not answered and the response `domain does not exist (NXDOMAIN)` is sent to the client. See [“Name Resolution” on page 18](#).

For example, having the domain name “abc.com” in the no-forward list will block the queries to “abc.com”, “support.abc.com”, or any other subdomain of abc.com.

Wildcard characters are not supported in the no-forward list. An asterisk or a root domain in the no-forward list cannot be used to block queries to all domain names.

For example, `developer.*.com` cannot be used to block the queries to `developer.novell.com` or `developer.xyz.com`, etc.

Figure 12 No-Forwarding



Benefits of Integrating DNS Server with eDirectory

The primary benefits of integrating DNS server with eDirectory include:

- ◆ Centralized eDirectory-based DNS configuration and management. Configuration must typically be done on a per-server basis with non-Novell DNS servers.
- ◆ DNS data is centrally managed in eDirectory. So, all servers associated with a zone become primary or secondary. That is, you get the benefit of all zones being primary, as opposed to a single zone being primary.
- ◆ DNS zone data is replicated using eDirectory replication, which eliminates the need for explicit DNS replication.

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 eDirectory and stores the information in its cache. As the DHCP server assigns addresses to clients, it updates eDirectory, adding IP address objects or modifying their eDirectory 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, see [“Configuring DHCP Auditing” on page 114](#).

The network administrator can view objects to see how addresses have been assigned.

For more information:

- ◆ “DHCP and BOOTP” on page 36
- ◆ “IP Address Allocation” on page 37
- ◆ “Virtual LAN Environments” on page 38
- ◆ “DHCP Auditing” on page 38
- ◆ “DHCP Options” on page 38
- ◆ “eDirectory Objects for DHCP” on page 40

A Novell 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.

In addition, integrating DHCP with eDirectory 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 machine or 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 assignments 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.

NOTE: In order to use the Novell DHCP server, the Novell DNS server must be a DNS designated primary server for both the forward and reverse zones.

Novell DNS/DHCP Services provides the following DHCP features:

- ◆ All DHCP configuration is managed in eDirectory, 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 the following:
 - ◆ Populating eDirectory from an existing Novell DHCP server 2.0 DHCPTAB file or from a BOOTPTAB file (for Novell BOOTP)
 - ◆ Saving configuration information out of eDirectory
- ◆ You can configure the level of SNMP event trap generation 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 maintain a hardware exclusion list to deny service to unwanted devices by their MAC addresses.
- ◆ The DHCP software updates eDirectory 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 eDirectory 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 eDirectory service outage and recover automatically.
 - ◆ DHCP configuration is replicated like other eDirectory data.
- ◆ DHCP auditing can help diagnose problems. Each incident of address deletion, addition, and rejection is recorded.
- ◆ The DHCP software can work with any DNS server.

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

- ◆ 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 following RFCs:

- ◆ RFC 1497—BOOTP Vendor Information Extensions
- ◆ RFC 1534—Interoperation Between BOOTP and DHCP
- ◆ RFC 1542—Clarifications and Extensions for the Bootstrap Protocol

For more information:

- ◆ [“DHCP Options” on page 38](#)
- ◆ [“eDirectory Objects for DHCP” on page 40](#)

DHCP and 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 need 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 client initialization software. Some new, additional options optimize DHCP client-server interaction.

There are two primary differences between BOOTP and DHCP. 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. In addition, DHCP provides a method for a client to acquire all of the IP configuration parameters it requires to operate.

If multiple servers service a single subnet, only 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 subnet 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.

NOTE: The BOOTP protocol, unlike DHCP, does not provide a mechanism for a client to accept only a single offer of an IP address; therefore, the iManager utility and the Management Console allow only the server that is specified as the default server in a Subnet object to be assigned to any address ranges that include BOOTP addresses. If you want to assign other servers to the address ranges, you should change the address range type so that it doesn't include BOOTP. If the range type includes BOOTP, you will not be allowed to change the DHCP server assigned to the range.

IP Address Allocation

Allocation of IP addresses, either temporary or permanent, is one of the two primary services provided by DHCP. 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 is used 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 without DHCP is desired. Manual allocation can be permanent or set to expire at a future time. When you manually allocate addresses, 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 can be a number of hours or days, or it can be for an indefinite period.

After a lease for an IP address has been granted, 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 limited number 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.

IMPORTANT: 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 indicates 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 before 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.

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 need 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.

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 providing 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 aid in reviewing the audit log. The beginning session contains records defining the session in terms of addresses already assigned.

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.

DHCP Options

Novell DNS/DHCP Services supports vendor options, DHCP options, and BOOTP parameters as defined in Internet RFC 2132 with a few exceptions. A table listing the option codes and names is found in [“DHCP Option Descriptions” on page 176](#).

Novell DNS/DHCP Services also supports new options defined for NetWare over TCP/IP and existing NetWare/IP options.

DHCP Options for eDirectory

Novell has defined three DHCP options for eDirectory. These options eliminate the need to provide this information each time users log in.

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

For detailed information about using these options in NetWare 6.5, refer to Internet RFC 2241, *DHCP Options for Novell Directory Services*.

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, the IPX Compatibility option, contains general configuration information such as the primary DSS, the preferred DSS, and the nearest servers. Option 63 also provides additional information in the form of suboptions, listed in the table below.

| Suboption 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 startup. |
| 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. |
| 11 | Identifies the Primary Domain SAP/RIP Service server (DSS) for this NetWare/IP domain. |
| 12 | Identifies the 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 to communicate with IPX Nodes. |

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

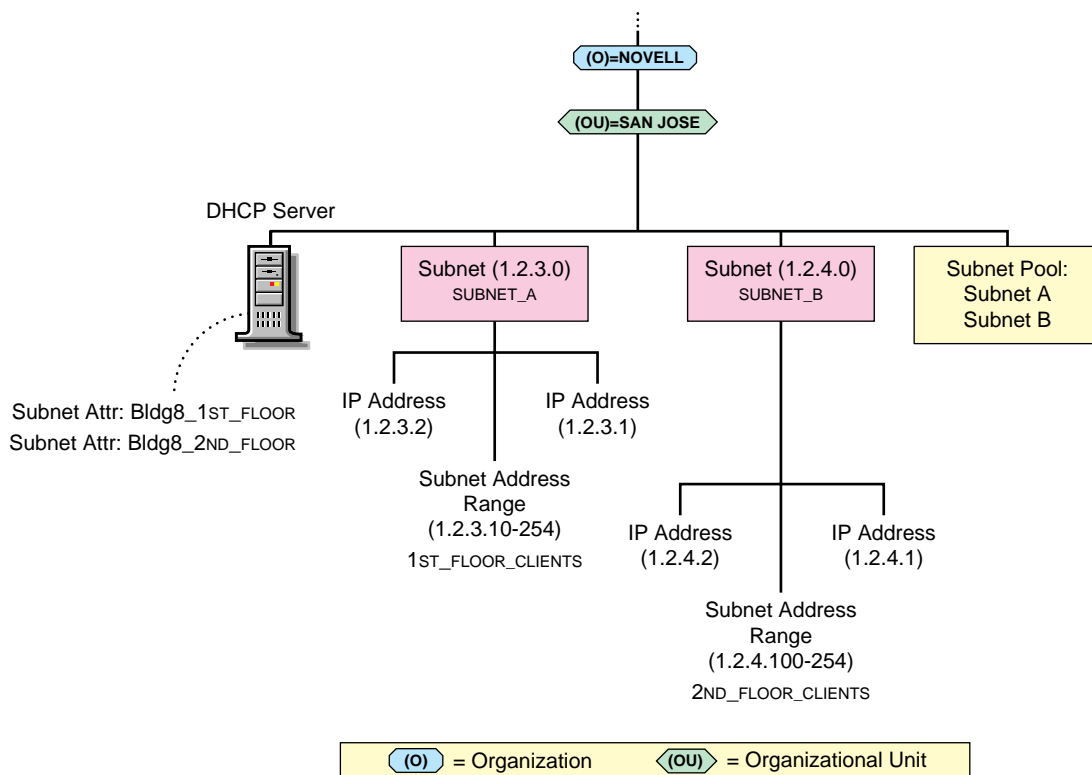
eDirectory Objects for DHCP

The following new eDirectory objects support DHCP:

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

Figure 13 shows a basic configuration of the DHCP objects. This structure might be used for a small to medium-size network.

Figure 13 eDirectory Objects for DHCP



DHCP Server Object

The DHCP server object (or service object) is created by extending the NetWare Core Protocol™ (NCP) server object. During the server object creation, the DHCP server reference is set in the NCP server.

The DHCP server object represents the DHCP server and contains a multivalued attribute listing 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 Organization (O), Organizational Unit (OU), Country (C), or Locality (L).

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.

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 Organization (O), Organizational Unit (OU), Country (C), or Locality (L).

DHCP servers are not required to be on the local subnet to which they assign addresses. If you want, they can be deployed centrally to service remote subnets. However, the initial DHCP/BOOTP discover requests are not sent to a DHCP server unless a DHCP/BOOTP forwarder that is on the same computer as the client has been configured to forward the addresses.

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

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 the global options.

Using the Subnet Object to Manage IP Addresses

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.

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 actions are listed in the table below.

| 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. In order 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 the Range Type set to Dynamic DHCP, Dynamic BOOTP and DHCP, or Dynamic DHCP with Automatic Hostname Generation.

The `dhcprsvr.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 eDirectory database is required.

The `dhcprsvr.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.

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 can 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.

DNS/DHCP Management Utility and Management Console

This section provides information about the iManager utility and the Management Console.

- ◆ [“Management Utility” on page 43](#)
- ◆ [“Management Console” on page 45](#)

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

The Locator object is created at the time of the NetWare 6.5 installation, if you choose the DNS/DHCP option. The Locator object serves as the catalog for most of the DNS and DHCP objects; therefore, the iManager utility or the Management Console is not required to search or scan the entire eDirectory 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 network administrators. They will use the iManager utility or the 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.

Management Utility

The iManager utility can be used to configure and manage eDirectory-based DNS and DHCP can run on any browser workstation and does not require the Novell Client or any installed component as a prerequisite. It operates within the common iManager framework and is thus tightly integrated with NetWare 6.5.

For more information, see:

- ◆ [“Management Utility Interface” on page 43](#)
- ◆ [“Taskbar” on page 44](#)
- ◆ [“Managing Roles and Tasks” on page 45](#)

Management Utility Interface

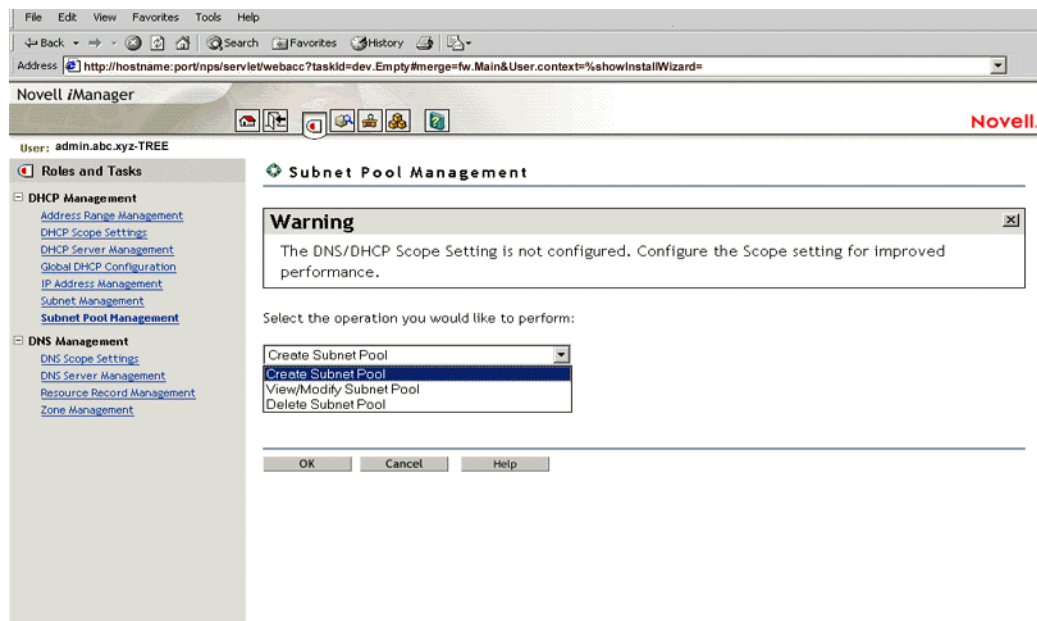
iManager manages one eDirectory tree at a time.

When iManager is started in the browser, the first screen you see is the login screen. You are prompted to provide your username, password, eDirectory context, and the eDirectory tree whose objects you want to manage.

Administration authentication in iManager is based on the common authentication mechanism.

To manage objects in a different eDirectory tree, you must log in to the utility again, specifying the eDirectory tree you want to access. Your login identity is displayed at the top of the screen.

Figure 14 The DNS/DHCP iManager Interface



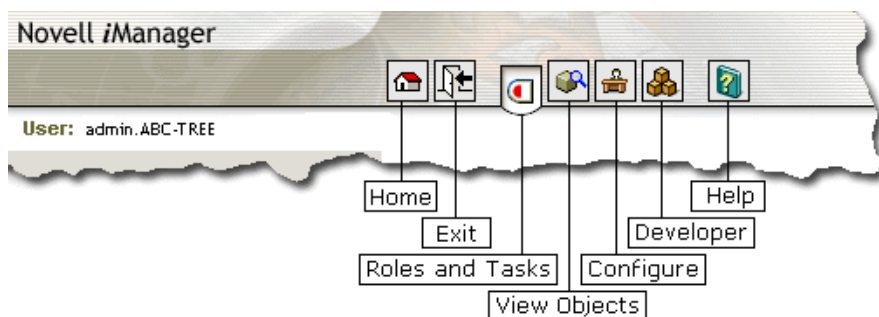
The main screen has three parts: a taskbar at the top of the screen that displays icons for top-level management functions; a left panel that displays roles, tasks, and other administrative functions; and a main panel that allows you to manage role-based and administrative tasks. For more information on the taskbar, see the following section, [Taskbar](#). For more information on roles and tasks, see [“Managing Roles and Tasks” on page 45](#).

Taskbar

The iManager utility shares a common taskbar with other NetWare 6.5 products that use the Novell iManager. The taskbar displays the following icons:

- ◆ Home: Takes you to the home page of the utility.
- ◆ Exit: Allows you to logout of the utility.
- ◆ Roles and Tasks: Displays the roles and tasks on the left panel.
- ◆ Administration: Enables you to carry out role installation and role management.
- ◆ Help: Launches global help for the utility.

Figure 15 The eDirectory Management Framework



If you position the cursor over the icon, the icon's name appears on the taskbar.

Managing Roles and Tasks

The DNS and DHCP services have been logically organized into roles and tasks in a way that is intuitive to network administrators. Each role consists of a set of tasks arranged in a manner that is hierarchical, top-down, and easy to administer.

To view the roles, click the Roles and Tasks icon on the taskbar.

At the top level, there are two roles that you can install and manage: DNS and DHCP. The tasks under each of these roles are logically arranged in a top-down manner with the option to configure DNS or DHCP scope settings at the head of each role. A role, depending on its current state, is preceded by a plus or a minus sign. An administrator can expand a role such as DNS to see the tasks it contains or collapse it for a more concise view. This can be done by clicking the plus/minus sign next to the role.

The organization of roles and tasks follows the containership rules of object creation and manipulation in DNS and DHCP. For example, if you expand the DNS role on the left pane, the logical tasks this role contains appear under it. At the top is the task DNS/DHCP Scope Settings. This is followed by DNS Server Management, which allows you to specify the location of the Locator object and the administrative scope for the session. At the next level is Zone Management, that manages zones handled by DNS servers. Finally Resource Record Management allows you to manage resource records contained within a zone.

Each task is associated with a set of operations that appear in a drop-down menu on the main panel when you click on the task.

For example, to create a new DNS zone, click DNS > Zone Management. This launches the Zone Management window in the main panel of the screen. Select Create Zone from the drop-down menu and click OK to open the Create New Zone window, where you can proceed with the task of creating a new zone.

You can select one object, more than one object, or all objects for deletion with the multi-select delete feature.

IMPORTANT: For improved performance, configure the DNS/DHCP scope settings before you start using the iManager utility.

Management Console

The Management Console can be used to configure and manage eDirectory-based DNS and DHCP. It is an independent executable Java application. It can be launched through Windows* using the Programs menu. Click Start > Programs > DNS-DHCP Management Console > DNSDHCP. It can also be launched by double-clicking the DNSDHCP shortcut icon created on the desktop or through the NetWare Administrator utility.

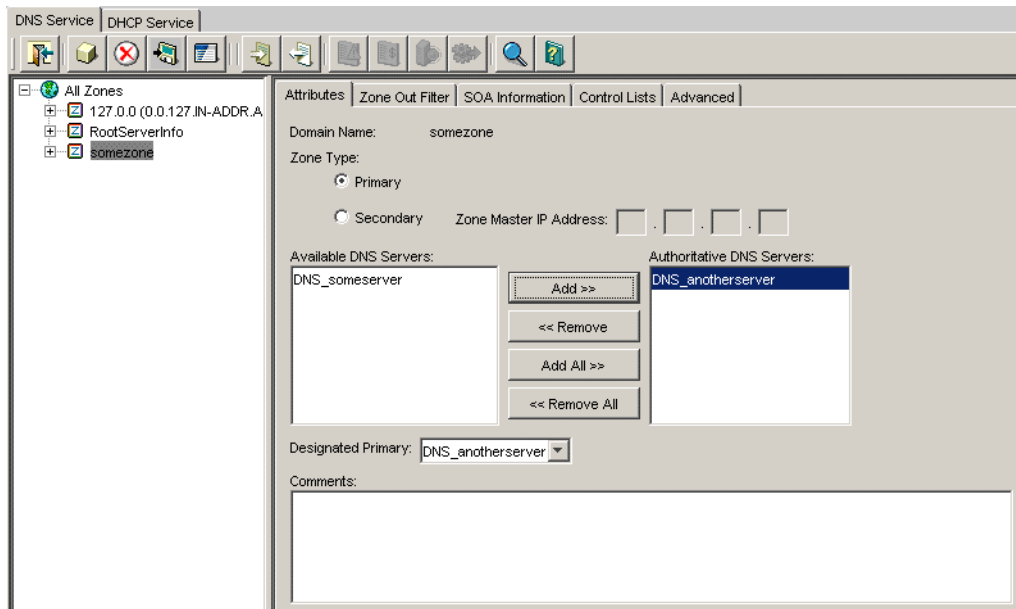
If the Management Console is launched through the NetWare Administrator utility, the eDirectory tree you are browsing will be set as the target eDirectory tree. When the Management Console is launched, it will prompt you to select a tree as the target eDirectory context.

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

The Management Console provides configuration and management for the two major functions of the Management Console: DHCP service management and name service management. Each application is self-contained and can provide the functions necessary to conduct DHCP or name management.

The Management Console manages one tree at a time. [Figure 16](#) shows the main user interface window for DHCP Services.

Figure 16 DNS/DHCP Java-based Management Console User Interface



For more information:

- ◆ [“DNS Service and DHCP Service Tab Pages” on page 46](#)
- ◆ [“Toolbar” on page 47](#)
- ◆ [“Status Bar” on page 49](#)
- ◆ [“Server Status” on page 49](#)
- ◆ [“Object Creation Rules” on page 49](#)

DNS Service and DHCP Service Tab Pages

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

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

All DNS and DHCP objects are created as eDirectory objects and are subject to NetWare Administrator conventions. Therefore, when creating a new object, you 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 browsing capability in the eDirectory tree, so an administrator with Write or Supervisor rights can select a specific context.

A newly created object's button on the toolbar is context-sensitive in relation to the highlighted item in either service's left tree pane. Your rights to the DNS or DHCP objects will not be verified until you perform 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 pane. The following table lists the rules for each container object.

| Selected Object | Objects that can be created |
|------------------------|--|
| All Zones | DNS Server, Zone |
| DNS Server | DNS Server, Zone |
| Zone | DNS Server, Zone, and Resource Record |
| RRSet | DNS Server, Zone, and Resource Record |
| Resource Record | DNS Server, Zone, and Resource Record |
| Our Network | DHCP Server, Subnet, Subnet Pool |
| DHCP Server | DHCP Server, Subnet, Subnet Pool |
| Subnet | Subnet Address Range, DHCP Server, IP Address, Subnet, Subnet Pool |
| Subnet Address Range | DHCP Server, Subnet, Subnet Pool |
| IP Address | DHCP Server, Subnet, Subnet Pool |
| Subnet Pool | DHCP Server, Subnet, Subnet Pool |

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

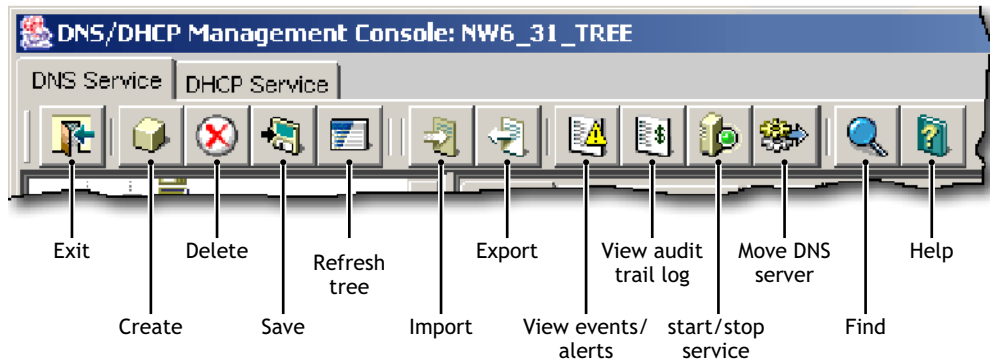
For fast and efficient searching, the distinguished names of newly created zones, DNS servers, subnets, and DHCP servers are added to the corresponding attribute of the Locator object. Renaming or deleting these objects is automatically performed by eDirectory because of the built-in feature for eDirectory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

After a new DNS or DHCP object has been created, the Management Console gives you 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.














Toolbar

The Management Console offers no menu items. All functions are provided by the toolbar. The functions that are relevant for the item selected in the left tree pane or bottom server pane are highlighted to show their availability.

Figure 17 Toolbar



If you position the cursor over the icon, the icon's name appears. The following table lists when each toolbar button is enabled in relationship to the selected object.

| Toolbar Button | Enabled |
|--|---|
| Exit  | Always enabled |
| 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 Log  | When DNS Server or DHCP Server is the selected object |
| View Audit Log  | When DNS Server or DHCP Server is the selected object |
| Move DNS Server  | When a NetWare 6.5 or later DNS Server is the selected object |
| Help  | Always enabled |

Status Bar

The status bar displays two fields in the bottom pane of the 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 18](#) shows the status bar and two DNS server icons. The status bar is at the bottom of the figure.

Figure 18 Status Bar



Server Status

Server icons are displayed in the lower portion of the Management Console. As shown in [Figure 19](#), 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 19 DHCP Server Icons



[Figure 20](#) shows icons representing two DNS servers. Both servers are operational, named.nlm has been loaded and each can communicate with the Management Console, but the operation of the server on the right, DNS_JAPAN, has been suspended.

Figure 20 DNS Server Icons



Object Creation Rules

These are certain rules that govern the creation and manipulation of objects in the DNS/DHCP object hierarchy.

Subnet and Subnet Pool objects can be created under an Organization (O), Organizational Unit (OU), Locality (L), or Country (C) objects. Subnet Address Range and IP Address objects must be created beneath the Subnet container object. However, because of the IP address, 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 pane to show the logical relationship. The

DNS Zone object, DNS server object, and DHCP server object can be created in the context of an Organization (O), Organizational Unit (OU), Locality (L), or Country (C).

All DNS and DHCP objects are created as eDirectory objects and are subject to NetWare Administrator conventions.

Some objects such as DHCP server, DNS server, DNS zone, subnet, and subnet pool can be created in any context.

After a new DNS or DHCP object has been created, the iManager utility grants the Read and Write rights to the Locator object. For fast and efficient search operations, the distinguished names of the 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 eDirectory because of the built-in feature for eDirectory distinguished names.

2

Planning Your DNS/DHCP Implementation

This section provides information to plan and design your implementation of DNS and DHCP in order to maximize capabilities of the Novell® DNS/DHCP Services software.

- ◆ “Resource Requirements” on page 51
- ◆ “eDirectory Considerations” on page 51
- ◆ “Planning a DNS Strategy” on page 52
- ◆ “Planning a DHCP Strategy” on page 55

Resource Requirements

The CPU requirements for NetWare 6.5 DNS server will vary depending on whether you are serving few static zones without caching to serving an enterprise type DNS.

The memory of the server must be large enough to accommodate the cache and zones loaded off disk. NetWare 6.5 requires at least 512 MB RAM. The max-cache-size option can be used to limit the amount of memory used by the cache, at the expense of reducing cache hit rates and creating more DNS traffic. It is still a good practice to have enough memory to load all zones and cache data into the memory. However, the best way to determine this for a given installation is to watch the name server in operation. After a few weeks the server process should reach a relatively stable size where entries are expiring from the cache as fast as they are being inserted. Ideally, the resource limits should be set higher than this stable size.

eDirectory Considerations

Consider the following Novell eDirectory™ 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

We recommend the following:

- ◆ Place the DNS/DHCP Group, the 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 6.5 DNS/DHCP servers are located. This is because all NetWare 6.5 DNS/DHCP servers, iManager, and Management Console require access to these objects.
- ◆ Plan to also create an Organizational Unit (OU) container object near the top of your eDirectory 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 the container object near the top of the eDirectory tree 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 iManager utility or 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 iManager utility or 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/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/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, fault tolerance, and robustness to your DNS implementation.

When you configure your zone, the primary name server 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.

For more information, see the following:

- ◆ [“Planning Zones” on page 52](#)
- ◆ [“Using the Novell DNS Server as a Primary Name Server” on page 53](#)
- ◆ [“Using the Novell DNS Server as a Secondary Name Server” on page 53](#)
- ◆ [“Configuring a DNS Server to Forward Requests” on page 53](#)
- ◆ [“Setting Up the IN-ADDR.ARPA Zone” on page 54](#)
- ◆ [“Registering Your DNS Server with Root Servers” on page 54](#)

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 that you create subzones within the zone. Although there is no limitation on the size of a zone when you configure DNS, we recommend that you do not create very large zones. Novell DNS server can support very large zones, but the higher the number

of resource records in a zone, the greater the impact on DNS query resolving for that zone. Managing small zones is simpler and more efficient. So, you could divide your zones into smaller subzones based on the geographic locations or organizational structures.

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 case of server down time.

Using the 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 iManager utility or 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 obtain data from the Novell primary name server.

Using the Novell DNS Server as a Secondary Name Server

If you plan to operate secondary DNS servers that use Novell DNS/DHCP Services software and that connect to a non-Novell master name server, one Novell secondary name server must be specified as the Designated Secondary or zone in server. The Designated Secondary server receives zone transfer information from the non-Novell master server and provides updates to eDirectory. Other Novell secondary name servers can then access the information within eDirectory.

You might operate a Novell secondary name server to a non-Novell master name server for the following reasons:

- ◆ You are 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:

- ◆ [“Forwarding Requests” on page 54](#)
- ◆ [“Restricting Forwarding \(No-Forwarding\)” on page 54](#)

Forwarding Requests

When you configure your name servers, you must provide information about where to forward requests that the servers 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 (No-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 not to 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.

If you want to restrict some external domains, you can use No-Forwarding. You can configure your servers not to forward queries to the specified external domains and the server will send a negative response to queries for those external domain.

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 in reverse. 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 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:

- ◆ Your existing network topology (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 eDirectory implementation should be incorporated into your planning. Place the Locator object near the top of your eDirectory tree where it can be easily accessed by all servers.
- ◆ The length of time you set for your leases affects traffic on the network.

For more information, see the following:

- ◆ [“Network Topology” on page 55](#)
- ◆ [“eDirectory Implementation” on page 56](#)
- ◆ [“Lease Considerations” on page 56](#)
- ◆ [“IP Address Availability” on page 58](#)
- ◆ [“Hostnames” on page 59](#)

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. See the following sections:

- ◆ [“Migrating from Another DHCP Solution” on page 55](#)
- ◆ [“Initiating the DHCP Service” on page 55](#)

Migrating from Another DHCP Solution

You can import your existing Novell DHCP 2.0 database or BOOTP-based configuration files using the iManager utility or 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. Although there is no limitation on the size or number of subnets when you configure DHCP, we recommend that the IP address in each subnet is not more than 2048. A Novell DHCP server can support several large subnets in a DHCP configuration. However, higher the number of IP addresses, the greater the impact on DHCP run-time performance.

eDirectory Implementation

Plan to create an Organizational Unit (OU), Country (C), or Locality (L) container object near the top of your eDirectory 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 of your contiguous strings of IP addresses.

Place the NetWare Core Protocol™ (NCP™) servers that will provide DHCP 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. Having only one replica might be unsafe because of fault tolerance considerations, but three might be too costly in terms of eDirectory performance.

Lease Considerations

In deciding how long to set your client leases, consider the following factors:

- ◆ 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 amount of time required for all leases to be renewed.

before the changes take effect. If your site policy is to turn off workstation power 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:

- ◆ “Lease Length” on page 57
- ◆ “Controlling Client Access to Leases” on page 58

Lease Length

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 clients than IP addresses?

If you have more clients than IP addresses, keep leases short to allow access to more users. A short lease could be 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 negligible 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.

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.

The following table lists examples of lease times and the reasons these times were chosen.

| Lease Time | Reason |
|------------|--|
| 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 eDirectory |
| 6 hours | Covers a DHCP server outage of 6 hours |
| 12 hours | Ensures that retraction of an address assignment takes less than one day |
| 3 days | Used by many sites simply because of software defaults |
| 6 days | Allows for 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 is usually a trade-off when you attempt to control specific client access to leases. Typically, you would manually configure each client and dedicate an IP address permanently to each client. However, Novell's DHCP server 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 DHCP, another vendor's product, or another method of tracking your IP address information, information about your addresses should be close at hand. To prevent communication problems, we recommend verifying the accuracy of your IP address records by performing a site audit.

If you are unsure of the range of your IP addresses, contact your Internet Service Provider (ISP) or check other records you have on file.

Subnetting Your Addresses

One of the more difficult configuration tasks is 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 static address to a device and still provide configuration information using DHCP.

To ensure that the assigned addresses are not used by DHCP, use the iManager utility or 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 eDirectory

IP addresses are represented by IP Address objects under Subnet container objects. Novell DNS/DHCP Services stores the 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 eDirectory. You can view this information using the iManager utility or 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 by setting DHCP Global Preferences. To invoke the DHCP Global Preferences window, click DHCP Global Configuration > DHCP Global Preferences.

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.

The following simple rules are used for hostnames to conform 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.

3

Installing DNS/DHCP Services

This section explains how to install the DNS/DHCP Services, the iManager utility, and the Management Console on NetWare® 6.5.

- ♦ [“Installation” on page 61](#)
- ♦ [“Management Utilities” on page 62](#)
- ♦ [“Upgrade” on page 65](#)
- ♦ [“Validating the DNS/DHCP Services Installation” on page 66](#)
- ♦ [“Repair Utility” on page 66](#)
- ♦ [“Uninstallation” on page 67](#)

Installation

Pattern deployment is a new concept introduced for installing services. Generally, when you install a certain service, you need a group of components or products. For a service to function properly, all the dependent products must be installed. Pattern deployment provides patterns for different services. Selecting a pattern automatically selects and installs its dependencies.

You can install the DNS/DHCP services using either of two patterns.

To install DNS/DHCP using the Customized NetWare pattern:

- 1** On the Choose a Pattern page, select Customized NetWare and click Next.
- 2** Select DNS/DHCP from the Components page.

Also, select iManager 2.0, Apache2 Web Server, and Tomcat4 if you want to use the iManager utility for managing DNS/DHCP services on the NetWare server.

To install DNS/DHCP using the DNS/DHCP Server pattern:

- 1** On the Choose a Pattern page, select the DNS/DHCP Server pattern.

The patterns are listed along with the customized NetWare Server/Basic NetWare File Server.

The DNS/DHCP services pattern installs Novell® iManager 2.0, Apache2 Web Server, and the Tomcat 4 Servlet container along with the DNS/DHCP services.

When you install DNS/DHCP services for the first time in a tree, you are prompted to enter the contexts for base objects, that is, Group, Locator, and RootSrvrInfo zone object. These objects will be created in the user-specified contexts. We recommend that these objects be placed high up in the Novell® eDirectory™ tree to simplify the management of Novell DNS/DHCP Services. For more information, see [Chapter 2, “Planning Your DNS/DHCP Implementation,” on page 51](#).

You are not prompted for this information for subsequent installations of DNS/DHCP services on other servers in the same tree. You should select the DNS/DHCP services while installing on all servers where you want to run DNS or DHCP.

DNS/DHCP installation adds commented load statements for DNS (load named.nlm) and DHCP (load dhcpsvr.nlm) services to the autoexec.ncf file. The load statements are commented because the DNS and DHCP Server objects should be created before DNS and DHCP services can be loaded. Load statements can be uncommented after creating the DNS and DHCP Server objects. The required command line options can be added to the load statements. For a list of available command line options, refer to “[NAMED Command Line Options](#)” on page 102 and “[DHCP SRVR Command Line Options](#)” on page 136.

IMPORTANT: An eDirectory tree must have only one Group, Locator, and RootSrvrInfo Zone object each.

Management Utilities

Before you use the management utilities, the DNS/DHCP services must be successfully installed as described in “[Installation](#)” on page 62.

- ◆ “[DNS/DHCP iManager Utility](#)” on page 62
- ◆ “[DNS/DHCP Java-Based Management Console](#)” on page 64
- ◆ “[eDirectory Rights Required to Manage DNS/DHCP Configuration](#)” on page 65

DNS/DHCP iManager Utility

Prerequisites

- ◆ Novell iManager 2.0 must be installed along with Novell DNS/DHCP services on the NetWare server to be managed.
- ◆ Internet Explorer 5.5 SP2, or Internet Explorer 6.0 must be installed on the client where you will manage DNS/DHCP services.


Installation

The snap-ins for the DNS-DHCP iManager utility are included with iManager 2.0 and are installed as part of the iManager 2.0 installation.

For more information, see the *iManager 2.0 Administration Guide* (<http://www.novell.com/documentation/lg/imanager20/index.html>).

Configuration

To install the DNS/DHCP snap-in:


- 1 Click Configure  on the iManager toolbar.
- 2 Click Create Collection, if the RBS collection object is not already created, and specify the name and context of the collection.

A collection is a container object that holds all RBS roles and module objects.
- 3 Click the Plug-in Setup and Install role.
- 4 Click Install Plug-in.
- 5 Select the dnshcp plug-in from the list.

6 Provide the container context created in **Step 2**.


7 Click OK.

To set up roles and tasks:

- 1** Click Configure  on the iManager toolbar.
- 2** Click Role Configuration to create new roles.
- 3** Click Task Configuration to create new tasks.
- 4** After assigning the newly created DNS/DHCP roles to users, add the users as trustee of DNS-DHCP Locator object and assign Write rights to all attributes of the Locator object.

For more information, see the *iManager 2.0 Administration Guide* (<http://www.novell.com/documentation/lg/imanager20/index.html>).

Launching the DNS/DHCP iManager Utility


- 1** Open Internet Explorer from any machine running Windows.
- 2** Type the following URL in the address bar of the Internet Explorer window:
`http://xxx.xxx.xxx.xxx/nps/iManager.html`
where `xxx.xxx.xxx.xxx` is the IP address of the NetWare server.
- 3** To log in to the iManager utility, provide the username and password, then click Login.
- 4** Click the Roles and Tasks  icon in the taskbar.

The iManager utility roles appear in the left pane.

To manage DNS services, click DNS and select from the available options.

To manage DHCP services, click DHCP and select from the available options.

To log in to a different tree:

- 1** Click the Login to a different tree  icon in the taskbar and provide the following:
 - ◆ Username
 - ◆ Password
 - ◆ eDirectory context
 - ◆ eDirectory tree
- 2** Click Login.

Recommended Settings

The recommended settings for the iManager utility are as follows:

| Display Settings | Font Size | Browser Setting |
|------------------|-----------|-----------------|
| 1024 * 768 | Small | Any size |

DNS/DHCP Java-Based Management Console

Prerequisites

- ◆ Microsoft* Windows NT* or Windows 95 and later
- ◆ Latest version of Novell Client™ or the ZENworks® client installed
- ◆ Minimum PC monitor resolution of 800 x 600 or above with a minimum color setting of 256
- ◆ Minimum 32 MB of system memory (64 MB recommended)
- ◆ Minimum 55 MB of free disk space

Installation

The installation application for the Management Console is located at `sys:\public\dnsdhcp\` directory on a NetWare 6.5 server.

To install the DNS/DHCP Management Console on a client workstation:

- 1** Map a drive to the `sys: volume` on a server where NetWare 6.5 is installed.
- 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 command prompt by entering:

```
x:\public\dnsdhcp\setup.exe
```

where x is the drive mapped to sys volume on the server where NetWare 6.5 has been installed.

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

During the installation, you have the option of installing the NetWare Administrator snap-in DLL. Check the Copy Snap-in DLL option box if you want to launch the DNS/DHCP Management utility from NetWare Administrator by selecting DNS/DHCP Management Console from the Tools menu.

Launching the Java-Based Management Console

- 1** Log in to the tree where DNS/DHCP services are installed. For more information, refer to [“Logging In to the Tree for DNS Setup” on page 90](#).
- 2** Double-click the shortcut to the `dnsdhcp.exe` program located on the desktop.
- 3** Select the name of the eDirectory tree that you are logged in to and where you want to manage the DNS/DHCP services.

You can use the Enter NDS Tree Name field to select an eDirectory tree that you are logged in to.

eDirectory Rights Required to Manage DNS/DHCP Configuration

To manage Novell DNS/DHCP Services, you must have sufficient rights for the type of operation you are performing. Assigning rights is done through ConsoleOne®. For more information, see the *ConsoleOne 1.3.x User Guide* (<http://www.novell.com/documentation/lg/consol13/index.html>).

Administrators who will add new objects and modify new objects must have Add rights to the appropriate eDirectory container object. The following table lists the rights required:

| DNS/DHCP Objects | Object Rights | All Property Rights |
|------------------|---------------|---------------------|
| Locator object | Browse | Supervisor |
| Group object | Browse | Supervisor |
| Existing objects | Supervisor | Supervisor |

Administrators who manage a given set of DHCP subnets or DNS zones must have rights to create or delete IP addresses, ranges of addresses, or resource record sets. The following table lists the rights required:

| DNS/DHCP Objects | Object Rights | All Property Rights |
|------------------|------------------------|---------------------|
| Locator object | Browse | Read |
| Group object | Browse | Read |
| Existing objects | Browse, Create, Delete | Supervisor |

Administrators or users who need to view the DNS/DHCP configuration must have the following rights:

| DNS/DHCP Objects | Object Rights | All Property Rights |
|------------------|---------------|---------------------|
| Locator object | Browse | Read |
| Group object | Browse | Read |
| Existing objects | Browse | Read |

Upgrade

All existing DNS/DHCP services can be upgraded from NetWare 5.1 SP6 or NetWare 6.0 SP3 to DNS/DHCP services in NetWare 6.5.

To upgrade:

- 1** In the Graphical Console of the NetWare server, select Novell > Install > Add new product path, then select the root directory of the source media.
- 2** Select PRODUCTS.NI, then select DNS/DHCP services the same as you would for an installation.

If you don't select DNS/DHCP during upgrade, you can still do a post-installation by executing [Step 1 on page 65](#) and [Step 2 on page 65](#) by selecting POSTINST.NI instead of PRODUCTS.NI.

Before performing a post-installation, the operating system must be upgraded to NetWare 6.5.

While upgrading DNS/DHCP services to NetWare 6.5, DNS/DHCP install comments out the existing load statements of DNS service and retains the new load statement “load named.nlm“. The existing load statements are commented because they might contain some command line options that are not supported by the NetWare 6.5 DNS server. For a list of command line options supported by NetWare 6.5 DNS server, refer to “[NAMED Command Line Options](#)” on page 102 and “[DHCP SRVR Command Line Options](#)” on page 136.

Validating the DNS/DHCP Services Installation

To validate that the DNS/DHCP Services installed correctly:

- 1 Create a DNS server object using any of the management utilities.
- 2 Create a zone and populate it with resource records.
- 3 At the NetWare server console, enter **named** to run the DNS Services.

Repair Utility

A NetWare integrated installation (using NIS) is the recommended way of installing or upgrading DNS/DHCP services. The dnipinst.nlm program is capable of performing the installation or upgrade of DNS/DHCP services. This NLM™ must be used for fixing post-installation problems and while removing the DNS/DHCP schema and objects from the tree. For example, if base objects (Group, RootSrvrInfo zone, Locator) are deleted, if the DNS/DHCP services schema is corrupted, or if you need to remove DNS/DHCP schema and objects from the tree.

The DNS/DHCP services installation extends the necessary schema and creates the base objects. The DNS server object is not created as part of this installation. You can create the DNS server object using the management utilities.

This NLM provides the following functionality:

- ◆ If used without any option, this NLM checks the presence of the DNS server 6.0.0 and the DHCP server 3.11.1 schema extensions. If the DNS/DHCP services schema is not found or is corrupted, the schema is extended and the base objects are created at the user-specified contexts.
- ◆ If used with the `-f` option, this NLM checks the presence of base objects. These objects (except the RootSrvrInfo zone) are created only if they are not already present. The RootSrvrInfo zone object is re-created if the TTL value present in the existing root hint RRs (RootSrvrInfo zone) does not match the value 3600000.
- ◆ If used with the `-r` option, all DNS/DHCP related objects are deleted from the tree.
- ◆ If used with the `-rs` option, all DNS/DHCP related objects and the DNS/DHCP services schema are deleted from the tree.

The usage display for this NLM can be seen on the logger screen by using the `-?` option.

NOTE: The dnipinst.nlm utility might prompt for the contexts of the base objects. The contexts of the existing base objects must be entered correctly. If the wrong context is provided, multiple base objects will be created in the tree. These base objects will cause the management utilities and DNS/DHCP services to malfunction.

Uninstallation

To uninstall DNS/DHCP Services or the management utilities, see:

- ◆ “DNS/DHCP Services” on page 67
- ◆ “Uninstalling the iManager Utility” on page 67
- ◆ “Uninstalling the Java-Based Management Console” on page 67

DNS/DHCP Services

To uninstall the DNS/DHCP services:

- 1 Run NIS uninstall on the individual servers in the tree.

This will remove all the products.dat entries for the DNS/DHCP product and all load statements of DNS/DHCP services from the autoexec.ncf file.

NOTE: This does not remove any objects or schema for the DNS/DHCP services from the tree. Deleting the schema and objects is not necessary because another DNS server might be using them. Because removing the schema and objects will have a tree-level impact, this action does not occur until the DNS/DHCP services are removed from all servers using NIS.

- 2 Use the `-r` option of the `dnipinst.nlm` to remove the DNS/DHCP objects and the schema for the complete tree.

Uninstalling the iManager Utility

Uninstalling iManager 2.0 automatically uninstalls the DNS/DHCP iManager utility because the DNS/DHCP services uses iManager snap-ins.

Uninstalling the Java-Based Management Console

- 1 From the Client workstation, click Start > Settings > Control Panel, then click Add or Remove Programs.
- 2 Select `dnsdhcp` and click Remove.

4

Configuring DNS

This section provides information about the following:

- ◆ “Configuring Clients to Use DNS” on page 69
- ◆ “DNS Server Configuration Parameters” on page 69
- ◆ “Using the iManager Utility to Configure DNS” on page 75
- ◆ “Using the Java-Based Management Console to Configure DNS” on page 89
- ◆ “Configuring DNS Features” on page 99
- ◆ “Loading the DNS Server” on page 102
- ◆ “NAMED Command Line Options” on page 102

Configuring Clients to Use DNS

To configure Windows NT, Windows 95/98/2000/XP and later client workstations to use DNS:

- 1** At the client desktop, click Start > Settings > Control Panel, then double-click Network.
The Network window opens, listing the network components installed on the client workstation.
- 2** Select TCP/IP, then click Properties.
The TCP/IP Properties window is displayed.
- 3** Click the DNS Configuration tab.
- 4** Provide a hostname and domain name for each client.
- 5** Specify 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 server.

DNS Server Configuration Parameters

Following are the various options and configuration parameters that you can view or modify for the DNS server:

Zone List: This list displays all zones that are serviced by the selected server and the server’s role for each zone. To change the role of the selected server for any zone in the list, change the zone’s configuration.

DNS Server IP Address: This field contains the IP addresses that the DNS server listens on for queries.

DNS Server Domain Name: Displays the domain name of the DNS server.

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

Forwarding List: Specifies the IP addresses of DNS servers to which queries will be forwarded from this server when it is unable to resolve that query from its authoritative data or cache. Unresolved queries are sent to these servers before they are sent to the root servers.

No-Forward List: Specifies a list of domain names whose unresolved queries will not be forwarded to other DNS servers.

Events Log: Specifies the degree of event data the server should collect. Major or critical events denote a significant change in the state of server processing. The events log can be configured for the following modes of event generation:

- ◆ None: Turns off event logging (default)
- ◆ Major Events: Logs only critical events
- ◆ All: Logs both major and minor events

Audit Log: Enable this option to make the selected server log audit trails and events.

NetWare 6.5 DNS Server Options

The following options can be configured only for DNS servers running on NetWare® 6.5:

SNMP Traps Option: SNMP traps are generated for various events depending on the configuration for this option. You can generate SNMP traps in the following modes:

- ◆ None: Turns off SNMP traps generation (default)
- ◆ Major Events: Generates SNMP traps only for critical events
- ◆ All: Generates SNMP traps for both major and minor events

Maximum Cache Size: Specifies the maximum amount of memory the server can use to cache responses. When the amount of data in the cache reaches this limit, the server will cause existing records in cache to expire prematurely so that the limit is not exceeded. The default value is 0 referring to unlimited cache. That is, records are purged from the cache only when their TTLs expire.

Max Recursion Lookups: Allows you to configure the maximum number of simultaneous recursive lookups the server will perform on behalf of the clients. The default is 1000. The value of this option might need to be decreased on hosts with limited memory because each recursive lookup uses a fair amount of memory, around 20 kilobytes.

Zone Out Filter: Allows you to configure which hosts are allowed to receive zone transfers from the server. If hosts are not specified, the default is to allow transfers from all hosts. Zone Out filter can be specified in the address match list format for the server.

The value specified for the zone will override the value specified for the server.

Allow Recursion: Specifies which hosts are allowed to submit recursive queries to the server. If hosts are not specified, the default is to allow recursive queries from all hosts. Allow recursion can be specified in the address match list format.

NOTE: If you disallow recursive queries for a host, it prevents the host from retrieving data that is already in the server's cache.

Query Filter: Allows you to configure which hosts are allowed to query the server. If hosts are not specified, the default is to allow queries from all hosts. Query Filter can be specified in the address match list format.

The value specified for the zone will override the value specified for the server.

Also Notify: Defines a global list of IP addresses of name servers that also receive notify messages when a fresh copy of the zone is loaded, in addition to the servers listed in the zone's NS records. This helps to ensure that the copies of the zones will quickly converge on stealth servers.

When a zone's notify option is set to No, notify messages are not sent to the IP addresses in the global Also Notify list for that zone. The default is the empty list (no global notification list).

The value specified for the zone will override the value specified for the server.

Black Listed Servers: Defines the list of addresses that the server does not accept queries from or use to resolve a query. Queries from these addresses are not responded to. The default is none.

Additional-from-auth, additional-from-cache: These options control the behavior of an authoritative server when answering queries which have additional data, or when following CNAME and DNAME chains.

When the additional-from-auth option is set to yes and a query is being answered from authoritative data, the additional data section of the reply is filled in using data from the other authoritative zones.

When the additional-from-cache option is set to yes and a query is being answered from authoritative data, the additional data section of the reply is filled in using data from the cache.

Allow-notify: Specifies the hosts that are allowed to notify the server about changes in a secondary zone serviced, in addition to the zone masters. If hosts are not specified, the default is to process notify messages only from a zone's master.

The value specified for the zone will override the value specified for the server.

Cleaning-interval: Specifies the time interval, in minutes, at which the server removes expired resource records from the cache. If set to 0, no periodic cleaning will occur. The default value is 60 minutes.

Forward: This option can be configured only if the Forwarding list is not empty. If the value is set to first (default), the server queries the forwarders first, and if that does not answer the query, the server will then look for the answer. If the value is set to only, the server will only query the forwarders.

Lame-ttl: Sets the number of seconds to cache a lame server indication. 0 disables caching. This is not recommended. The maximum value is 1800 (30 minutes).

Listen-on: Specifies the interfaces and ports that the server will answer queries from. It takes an optional port and an address match list. If a port is not specified, port 53 will be used.

Max-cache-ttl: Sets the maximum time for which the server will cache ordinary (positive) answers.

Max-ncache-ttl: The server stores negative answers to reduce network traffic and increase performance. This option is used to set a maximum retention time for these answers in the server. The maximum value is 7 days.

Minimal-responses: If this option is set to yes, while generating responses the server will add records to the authority and additional data sections only when they are required (for example, delegations, negative responses). This might improve the performance of the server.

Notify: If this option is set to yes, DNS notify messages are sent when a zone for which the server is authoritative for changes. The messages are sent to the servers listed in the zone's NS records (except the master server identified in the SOA MNAME field) and to any servers listed in the also-notify option. If this option is set to explicit, notifies are sent only to servers explicitly listed using also-notify. If this option is set to no, no notifies are sent.

Notify-source: Determines the local source address, and optionally the UDP port, that will be used to send notify messages. The slave servers should also be configured to receive notify messages from this address.

Novell_dyn-reconfig: Specifies the time interval at which dynamic reconfiguration will take place. The minimum value is 10 minutes and maximum is 24 hours.

Provide-ixfr: Determines whether the local server, acting as master, will respond with an incremental zone transfer when the given remote server, a slave, requests it. If this option is set to yes, incremental transfer will be provided whenever possible. If this option is set to no, all transfers to the remote server will be non-incremental.

Query-source: Specifies the address and port used for querying other name servers, if the server does not know the answer to a query.

Recursion: If this option is set to yes, and a DNS query requests recursion, then the server attempts to do everything required to answer the query. If this option is set to no, and the server does not already know the answer, it will return a referral response.

Request-ixfr: Determines whether the local server, acting as a slave, will request incremental zone transfers from the given remote server, a master.

RRset-order: Permits the ordering of the records in a multiple record response to be configured. If this option is set to fixed, records are returned in a fixed order. If this option is set to random-cyclic, the server chooses a record within the RRset as the starting point and returns the records in the starting order at that point.

Serial-query-rate: Slave servers periodically query the master servers to find out if the zone serial numbers have changed. Each query uses a small amount of the slave server's network bandwidth. You can limit the rate at which queries are sent and therefore limit the amount of bandwidth used. The value can be an integer, which is the maximum number of queries sent per second.

Tcp-clients: Specifies the maximum number of simultaneous TCP client connections that the server will accept.

Transfer-format: Zone transfers can be sent using two different formats, one-answer and many-answers. This option is used on the master server to determine the format of zone transfer. One-answer uses only one DNS message per resource record transferred and many-answers places as many resource records as possible into a message. Many-answers is more efficient.

Transfer-source: Determines the local address that is bound to the IPv4 TCP connections used to fetch the zones transferred inbound by the server. It also determines the source IPv4 address, and optionally the UDP port, used for the refresh queries and forwarded dynamic updates.

Transfers-in: Specifies the maximum number of inbound zone transfers that can concurrently run. Increasing the transfers-in might speed up the convergence of the slave zones, but it might also increase the load on the local system.

Transfers-out: Specifies the maximum number of outbound zone transfers that can run concurrently. Zone transfer requests in excess of the limit will be refused.

Transfers-per-ns: Specifies the maximum number of inbound zone transfers that can be transferred concurrently from a given remote name server. Increasing the value of this option might speed up the convergence of slave zones, but it might also increase the load on the remote name server.

Zone-statistics: Zone-statistics can be configured to yes so that the server will collect statistical data for the zones.

The value specified for the zone will override the value specified for the server.

Zone Configuration Parameters

The following options and configuration parameters, can be viewed or modified for the DNS Zone:

Zone Type: Specifies whether the zone is a primary or a secondary zone. If this option is set as primary, the Novell DNS servers will act as primary servers for this zone. If this option is set as secondary, the servers will act as secondary servers.

Zone Master IP Address: Specifies the IP address of the primary DNS server for the secondary zone.

Available DNS Servers: Displays all the available DNS servers that can service the zone.

Authoritative DNS Server: Displays all servers that are servicing the zone. All servers in this list are authoritative for the zone. For a primary zone, all servers listed are passive primary servers except the one specified in the Designated Primary field.

The server in the Designated Primary field will act as a designated primary server. For a secondary zone, all servers listed are passive secondary servers except the one specified in the Designated Secondary field. The server in the Designated Secondary field will act as the designated secondary server.

Designated Primary (for Primary Zone): Specifies the designated primary server for the zone. If you specify a server as designated primary, it will be the server designated for receiving dynamic updates.

Designated Secondary (for Secondary Zone): Specifies the designated secondary server for the zone. If you specify a server as designated secondary, it will be the server designated for receiving zone-in transfers.

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

Zone Out Filter: Specifies which hosts are authorized to do a zone out transfer for this zone from primary servers of this zone. If this field is not configured, each DNS server servicing this zone will use its own Zone Out filter list value (if configured). Otherwise, the default value is used.

NOTE: Zone Timer is used to initiate the zone maintenance. This value is not configurable (it is set to 15 minutes). This timer is set when the zone gets the first dynamic update. The zone maintenance is done at the expiry of this timer or during dynamic reconfiguration, whichever happens first. The zone timer is useful when the dynamic reconfiguration is set to a higher value.

Zone Master: Displays the domain name for the master server of the zone (also called designated primary server).

E-mail Address: Displays the e-mail address (with '@' replaced by '.') of the person responsible for this zone.

Serial Number: This is used for zone data versioning. Serial numbers are automatically incremented to reflect any changes to the zone data such as creation, deletion, or modification of resource records; dynamic updates; zone transfers; etc. This parameter is primarily used to notify the slave zones of a change in the zone data.

Refresh: The refresh interval indicates the time interval at which the secondary server of this zone checks with the master server to see whether its data is up to date. If the data in the master server is the latest, the secondary server will transfer it from the master server. The default is 180 minutes.

Retry: If the slave fails to contact the master server after the refresh period, then it starts contacting the master server after every retry interval. The default is 60 minutes.

Expire: If the slave fails to contact the master server for expire, the slave server expires this zone data. The default is 168 hours.

Minimum TTL: Specifies the minimum TTL value for the resource record. This value applies to all resource records in the zone data. The name server supplies this TTL in query responses, allowing other servers to cache the data for the TTL interval. The default is 24 hours.

Query Filter: Allows you to configure which hosts are allowed to query the servers for data in this zone. If a value is not specified, the default is to allow queries from all hosts. Query filter can be specified in the address match list format. If this field is not configured, each DNS server servicing this zone will use its own query filter list value if it is configured. Otherwise, the default value is used.

Also Notify: Defines a list of IP addresses of name servers that also receive notify messages whenever a fresh copy of the zone is loaded, in addition to the servers listed in the zone's NS records. This helps to ensure that copies of the zones will quickly converge on stealth servers.

The value specified for the zone will override the value specified for the server. When a zone's notify option is set to no, no notifications will be sent to any server about changes in the zone data. The default is an empty list.

Allow Update: Specifies which hosts are allowed to submit dynamic DNS updates for primary zones. The default is to deny updates from all hosts. This control list is applicable only to RFC 2136 standards-based Dynamic Updates. This option can be configured only for a primary zone.

Allow-notify: Specifies the hosts that are allowed to notify slaves of a zone change in addition to the zone masters. This can be configured only for a secondary zone. If this field is not configured, each DNS server servicing this zone will use the allow-notify value if it is configured. Otherwise, the default value is none.

Notify: If this option is set to yes, DNS notify messages are sent by the authoritative servers of this zone when the zone data changes. The messages are sent to the servers listed in the zone's NS records (except the master server identified in the SOA MNAME field) and to other servers listed in the also-notify option. If this option is set to explicit, notifies are sent only to the servers explicitly listed using also-notify. If this option is set to no, no notifies are sent.

Notify-source: Determines the local source address, and optionally UDP port, that will be used to send NOTIFY messages when this zone data changes. The slave server should also be configured to receive notify messages from this address.

Transfer-source: Determines the local address that is bound to the IPv4 TCP connections used to fetch the zones transferred inbound by the server. It also determines the source IPv4 address, and optionally the UDP port, used for the refresh queries and forwarded dynamic updates.

Zone-statistics: Zone-statistics can be configured to yes so that the server will collect statistical data for the zone.

The value specified for the zone will override the value specified for the server.

Using the iManager Utility to Configure DNS

This section provides information about configuring DNS objects and importing and exporting database information using the iManager utility.

- ◆ [“Scope Settings” on page 75](#)
- ◆ [“DNS Prerequisites” on page 76](#)
- ◆ [“DNS Server Management” on page 76](#)
- ◆ [“Zone Management” on page 83](#)
- ◆ [“Resource Record Management” on page 87](#)

Scope Settings

For better performance results with the iManager utility, particularly in a distributed DNS/DHCP setup, you should configure the DNS/DHCP scope settings for the session before you proceed with other administrative tasks.

If you do not configure the DNS/DHCP scope settings for the session, you will receive a warning before every task you attempt to perform indicating that the scope settings are not set. However, you can still proceed with the task.

Setting the scope of the DNS/DHCP services requires two specifications for the session: the Novell[®] eDirectory[™] context of the Locator object and the administrative scope of the session. Specifying the eDirectory context of the Locator object at the start of the session significantly improves performance because it eliminates the need to search for the Locator object. Specifying the administrative scope of the session also improves performance significantly because it restricts the retrieval of DNS/DHCP objects for viewing to the scope you specify.

When you configure the DNS/DHCP scope settings for a session, they only last as long as the session lasts. If you start a new session, you must configure the DNS/DHCP Scope Settings again.

IMPORTANT: If you configure DNS/DHCP Scope Settings for a session for either DNS or DHCP, the settings apply across the session to both roles.

To configure DNS/DHCP scope settings:

- 1** Click DNS or DHCP > DNS/DHCP Scope Settings to open the DNS/DHCP Scope Settings window.
- 2** Specify the eDirectory context of the DNS/DHCP Locator object or browse to select it.
- 3** Specify the eDirectory context of the container object that will provide the administrative scope of the current session.

If you specify only the eDirectory context of the DNS/DHCP Locator object and not the administrative scope of the current session, you can proceed with administrative tasks without receiving a warning message. However, performance is further optimized if you also define the administrative scope.

- 4** Click OK.
- 5** Click Repeat Task to configure the scope settings again.

A message indicates that the scope request was successful.

DNS Prerequisites

Ensure that you have met the following prerequisites prior to setting up DNS:

- Install NetWare 6.5 on the selected servers.
- Install Novell iManager.
- Install Internet Explorer 5.5 Support Pack 2, or Internet Explorer 6.0 on a Windows client.

DNS Server Management

The DNS Server Management role consists of the following tasks:

- ◆ [“Creating a DNS Server Object” on page 76](#)
- ◆ [“Viewing or Modifying a DNS Server Object” on page 77](#)
- ◆ [“Deleting a DNS Server” on page 79](#)
- ◆ [“Starting or Stopping a DNS Server” on page 79](#)
- ◆ [“Viewing the DNS Event Log” on page 82](#)
- ◆ [“Viewing the DNS Audit Trail Log” on page 81](#)
- ◆ [“Loading or Unloading a DNS Server” on page 80](#)
- ◆ [“Moving a DNS Server” on page 80](#)
- ◆ [“Configuring DNS Auditing” on page 81](#)

Creating a DNS Server Object

Use the iManager utility to create and set up a DNS server object for each DNS server you plan to operate.

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Create Server and click OK to open the Create DNS Server window.
- 3** Type the NCP™ server name or browse to select an NCP server from the eDirectory tree.
- 4** Specify a unique hostname for the DNS server object.
- 5** Specify a domain name for the server object.
- 6** Click Create.

A message indicates that the new DNS server was created.

Viewing or Modifying a DNS Server Object

After you create a DNS server object, you can modify its configuration parameters.

- 1 Click **DNS > DNS Server Management** to open the DNS Server Management window in the main panel.
- 2 From the drop-down menu, select **View/Modify Server** and click **OK** to open the **View/Modify Server** window.
- 3 Select the DNS Server from the drop-down list, then click **OK**.

You are led through a set of steps that allow you to view and modify the following DNS server configuration parameters:


- ◆ **List of Zones:** Lists the names of the zones that the server manages along with the roles of this server for each of the zones. This field cannot be edited.
- ◆ **DNS Server IP Address:** Contains the IP addresses on which the DNS server listens for queries. This field cannot be edited.
- ◆ **DNS Server Domain name:** Lists the domain name of the DNS server.
- ◆ **DNS Server Comments:** You can add your comments about the DNS server in this box. This parameter is optional.
- ◆ **Forward List:** Specifies a list of IP addresses of DNS servers to which unresolved queries will be forwarded.
 - ◆ To add servers to the Forward List, click **Add**, specify the IP address of the server, then click **Add** again.
 - ◆ To remove servers from the Forward List, select the IP address of the server from the Forward List, then click **Delete**.
- ◆ **No-Forward List:** Specifies a list of domain names whose unresolved queries will not be forwarded to other DNS servers.
 - ◆ To add domain names to the No-Forward List, click **Add**, specify the domain name of the server, then click **OK**.
 - ◆ To remove domain names from the Forward List, select the domain name from the No-Forward List, then click **Delete**.
- ◆ **Events Log:** Specifies the degree of event data the server should collect. Major or critical events denote a significant change in the state of server processing. To configure the event log, select from the following options:
 - ◆ **None:** Turns off event logging (default)
 - ◆ **Major Events:** Logs only the critical events
 - ◆ **All:** Logs both major and minor events
- ◆ **Audit Log:** Check **Enable Audit Trail Log** to log audit trails and events.
- ◆ **SNMP Traps Option:** SNMP traps are generated for various events depending on the configuration for this option.


You can select from the following options:

- ◆ **None:** Turns off the SNMP traps generation (default)
- ◆ **Major Events:** Generates SNMP traps only for critical events
- ◆ **All:** Generates SNMP traps for both major and minor events

- ◆ **Allow Recursion:** Specifies a list of IP addresses or networks that can submit recursive DNS queries. If you want to disable recursion, specify a value of None.


To add the address match list element:


- ◆ Click 
- ◆ Specify the IP address and the mask length.
The network number is optional.
- ◆ If you want to add a generic option, check the Predefined match-list to select from the available options in the drop-down list.
- ◆ Click OK.

To delete the address match list element, select the item to be deleted, then click .

- ◆ **Query Filter:** Specifies a list of IP addresses or networks that are authorized to query the DNS server. If no IP address is specified, queries are allowed from all hosts.


To add the address match list element:


- ◆ Click 
- ◆ Specify the IP address and the mask length.
The network number is optional.
- ◆ If you want to add a generic option, check the Predefined match-list to select from the available options in the drop-down list.
- ◆ Click OK.

To delete the address match list element, select the item to be deleted, then click .

- ◆ **Zone Out Filter:** Specifies a list of IP addresses or networks that are authorized to perform zone transfer from the DNS server.


To add the address match list element:

- ◆ Click 
- ◆ Specify the IP address and the mask length.
The network number is optional.
- ◆ If you want to add a generic option, check the Predefined match-list to select from the available options in the drop-down list.
- ◆ Click OK.

To delete the address match list element, select the item to be deleted, then click .


- ◆ **Also Notify:** Specifies a list of IP addresses of name servers that receive Notify messages, when a fresh copy of the zone is loaded.


To add the IP address,

Click , specify the IP address, then click OK.

To delete the IP address, select the IP address you want to delete, then click .

- ◆ **Blacklist Server:** Specifies a list of IP addresses of servers that are not approved. The DNS server will not answer queries from or forward queries to the servers listed.

To add the IP address, click , specify the IP address, then click OK.

To delete the IP address, select the IP address you want to delete, then click .

- ◆ **Maximum Cache Size:** Specifies the maximum amount of memory in kilobytes that the server can use as cache.
- ◆ **Maximum Recursion Lookups:** Specifies the maximum number of simultaneous recursive lookups the server performs on behalf of the clients.
- ◆ **Current set of Additional Options:** Specifies the additional global server and zone options. To view the options, click Modify to open the View/Modify Server window.
 - ◆ To add an available additional option, select the option and click Add.
 - ◆ To add all available additional options, click Add All.
 - ◆ To remove an available additional option, select the option and click Remove.
 - ◆ To remove all available additional options, click Remove All.
 - ◆ To delete all option names in the list, click the top-level check box, then click Delete.
 - ◆ To remove one or more option names, click the check box next to it, then click Delete.

Deleting a DNS Server

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Delete Server and click OK to open the Delete DNS Server window.
 - ◆ To remove all DNS servers in the list, click the top-level check box and click Delete.
 - ◆ To remove one or more DNS servers, click the check box next to it and click Delete.

Starting or Stopping a DNS Server

The DNS server must be loaded before you can start or stop the server activity.

The Start/Stop service can be used to load zone data along with the modified configuration without unloading and reloading the DNS server. When you stop the DNS server using this option, it will still be loaded in the memory. However, no services are provided. You can use the iManager Management utility or the Java-Based Management Console to update the zone data. When you restart the DNS server using this option, the server is reconfigured with the new configuration settings and the zone data is also reloaded.

This option can also be used to remotely start and stop the DNS server.

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Start/Stop Server and click OK to open the Start/Stop Server window.
- 3** Select the DNS server.
- 4** Click OK.
- 5** Depending on the state of the DNS server module, one of the following will appear:
 - ◆ Failure notification message: This appears if the DNS server module (named.nlm) is not loaded. In order to start the server, load the DNS server module through the system console.
 - ◆ Start button: If the DNS server module is loaded but is in Stop mode, click the button to start the DNS server.

- ◆ Stop button: If the DNS server module is loaded but is in Start mode, click the button to stop the DNS server.

Loading or Unloading a DNS Server

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Load/Unload Server and then click OK to open the Load/Unload Server window.
- 3** Select the DNS server and specify the port number that the DNS server is configured on.
The port is required to check whether the DNS Server is running or not. By default, port 53 is used if no other port number is specified.
- 4** Click OK.

Depending on the state and the version of the DNS Server, one of the following appears:

- ◆ If the NLM™ is not loaded on the machine, you are prompted to load named.nlm.
Based on the DNS Server version that is selected, the supported command line options are displayed.
 - ◆ Enter the command line options to load the NLM with, then click Load.
- ◆ If the NLM is already loaded on the machine, you are prompted to unload named.nlm.
To unload the NLM, click Unload.

- 5** Click OK to complete the task.

When you click Load or Unload the corresponding command is sent to the server. The success status in iManager indicates only that the command was issued to the server. This does not necessarily mean that the command execution was successful.

Moving a DNS Server

This task enables you to move DNS Services from one NCP server to another NCP server. You can also convert a DNS server into a cluster-enabled DNS server by moving it to a virtual NCP server.

This feature is supported for DNS servers running on NetWare 6.5 or later.

To move a DNS server:

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Move DNS Server and click OK to open the Move DNS Server window.
- 3** Select the DNS Server name from the drop-down list.
DNS servers prior to NetWare 6.5 will not be available in this list.
- 4** Enter the name of the NCP Server that the DNS Services will be moved to or use the Object Selector icon to browse and select it.
- 5** Click Move.

Configuring DNS Auditing

To configure a DNS server to audit activities:

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select View/Modify Server and click OK to open the View/Modify Server window.
- 3** Select the DNS Server from the drop-down menu.
- 4** Click OK.
- 5** Click Next three times, then select Major Events or All under Event Log.
- 6** Click the Enable Audit Trail Log check box.
- 7** Click Next.
- 8** Click Done.

Viewing the DNS Audit Trail Log

To view the audit trail log, csatpxy.nlm must be running on the server.

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Audit Trail Log and click OK to open the DNS Audit Trail Log window.
- 3** Select the server from the DNS Server drop-down menu.
- 4** If you want to filter the Audit Period, modify the starting and ending dates in the appropriate fields.

The following date format is accepted:

mm-dd-yyyy

- 5** Click OK.

This opens the DNS Audit Trail Log table, which lists the following data:

- ◆ Entry Time: Date and time the event occurred
 - ◆ Type: Type of event
 - ◆ IP Address: IP address at which the event occurred
 - ◆ Domain Name: Domain Name at which the event occurred
- 6** To define a view filter on the Audit Trail Log, click the Display Options button.
You can now filter events on the following parameters:
 - ◆ Start Date: Sets a start date for monitoring the DNS audit trail.
 - ◆ End Date: Sets an end date for monitoring the DNS audit trail.
 - ◆ Agent Ready: The SNMP (Simple Network Mail Protocol) agent is ready to receive or transmit requests.
 - ◆ Query Received: The DNS server acknowledges the receipt of a query by making an entry in the log file.

- ◆ Query Forwarded: The DNS server forwards a query to a client or from another DNS server.
- ◆ Response Received: The DNS server responds to a query from a client or another DNS server.

Saving the DNS Audit Trail Log

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Audit Trail Log and click OK to open the DNS Audit Trail Log window, then click Next.
- 3** Click the Click here to Download File link, then save the audit trail log file on your local machine.

Viewing the DNS Event Log

To view the event log, csatpxy.nlm must be running on the server.

- 1** Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2** From the drop-down menu, select Event Log and click OK to open the DNS Event - Events Log window.
- 3** Select the server from the DNS Server drop-down menu.
- 4** If you want to filter the Audit Period, modify the start and end dates in the appropriate fields.

The following date format is accepted:

mm-dd-yyyy

- 5** Click OK.

This opens the DNS Event Log table, which lists the following data:

- ◆ Entry Time: Date and time the event occurred
- ◆ Severity: Severity of the event - critical, major, warning, and informational
- ◆ State: State of the server - operational, degraded, and inoperative
- ◆ Description: Description of the event that occurred

- 6** To define a view filter on the DNS Event Log, click the Display Options button.

You can now filter events on the following parameters:

- ◆ Start and end date settings regulate the time recorded by the event logger.
- ◆ Severity options define which event levels are recorded: critical, major, warning, and informational.
- ◆ State settings define the condition of events recorded: operational, degraded, and inoperative.

Saving the DNS Event Log

- 1 Click DNS > DNS Server Management to open the DNS Server Management window in the main panel.
- 2 From the drop-down menu, select Event Log and click OK to open the DNS Event - Events Log window, then click Next.
- 3 Click the Click here to Download File link, then save the Event Log file on your local machine.

Zone Management

The DNS Zone object is an eDirectory container object that comprises Resource Record Set (RRSet) objects and resource records.

- ◆ [“Creating a Primary Forward Zone” on page 83](#)
- ◆ [“Creating a Secondary Forward Zone” on page 84](#)
- ◆ [“Creating a Primary IN-ADDR.ARPA Zone” on page 84](#)
- ◆ [“Creating a Secondary IN-ADDR.ARPA Zone” on page 85](#)
- ◆ [“Viewing or Modifying a Zone Object” on page 85](#)
- ◆ [“Deleting a Zone Object” on page 86](#)
- ◆ [“Importing a Zone Object” on page 86](#)
- ◆ [“Exporting a Zone Object” on page 87](#)

Creating a Forward Zone Object

- ◆ [“Creating a Primary Forward Zone” on page 83](#)
- ◆ [“Creating a Secondary Forward Zone” on page 84](#)

Creating a Primary Forward Zone

- 1 Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2 From the drop-down menu, select Create Zone and click OK to open the Create DNS Zone window.
- 3 Select Create New Zone.
- 4 Specify the eDirectory context for the zone or browse to select it.
- 5 Specify a name for the zone object.
- 6 Under the Zone Type, select Primary (default).
- 7 Select a DNS server from the Assigned Authoritative DNS Server drop-down menu.
or
Specify a unique hostname in the Name Server Host Name box and, optionally, select a domain from the Domain drop-down menu, then click OK.
- 8 Click Create.
A message indicates that the new primary zone has been created.

Creating a Secondary Forward Zone

- 1 Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2 From the drop-down menu, select Create Zone, then click OK to open the Create DNS Zone window.
- 3 Select Create New Zone.
- 4 Specify the eDirectory context for the zone or browse to select it.
- 5 Specify a name for the zone object.
- 6 Under the Zone Type, select Secondary.
- 7 Specify the IP address of the DNS server that will provide zone out transfers for this secondary zone.
- 8 Select a DNS server from the Assigned Authoritative DNS Server drop-down menu. This parameter is optional.
or
Specify a unique hostname in the Name Server Host Name box and optionally, select a domain from the Domain drop-down menu, then click OK.
- 9 Click Create.

A message indicates that the new secondary zone has been created.

Creating an IN-ADDR.ARPA Object

- ♦ [“Creating a Primary IN-ADDR.ARPA Zone” on page 84](#)
- ♦ [“Creating a Secondary IN-ADDR.ARPA Zone” on page 85](#)

Creating a Primary IN-ADDR.ARPA Zone

- 1 Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2 From the drop-down menu, select Create Zone and click OK to open the Create DNS Zone window.
- 3 Select Create IN-ADDR.ARPA.
- 4 Specify the eDirectory context for the zone or browse to select it.
- 5 Specify the network address of the zone in the Network Address field.
For example, specify 143.72.155 only for 155.72.143.IN-ADDR.ARPA.
The IN-ADDR.ARPA zone name is displayed in the Zone Domain Name field.
- 6 Under the Zone Type, select Primary (default).
- 7 Select a DNS server from the Assigned Authoritative DNS Server drop-down menu.
or
Specify a unique hostname in the Name Server Host Name box and, optionally, specify a domain name or select it from the Domain drop-down menu.
- 8 Click Create.

A message indicates that the new Primary IN-ADDR.ARPA Zone object has been created.

Creating a Secondary IN-ADDR.ARPA Zone

- 1 Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2 From the drop-down menu, select Create Zone, then click OK to open the Create DNS Zone window.
- 3 Select Create IN-ADDR.ARPA.
- 4 Specify the eDirectory context for the zone or browse to select it.
- 5 Specify the network address in the Network Address field.
The IN-ADDR.ARPA zone name is displayed in the Zone Domain Name field.
- 6 Under the Zone Type, select Secondary.
- 7 Select a DNS server from the Assigned Authoritative DNS Server drop-down menu.
or
Specify a unique hostname in the Name Server Host Name box and, optionally, specify a domain name or select it from the Domain drop-down menu.
- 8 Type the IP address of the DNS server that will provide zone-out transfers for this secondary zone.
- 9 Click Create.
A message indicates that the new Secondary IN-ADDR.ARPA Zone object has been created.

Viewing or Modifying a Zone Object

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

- 1 Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2 From the drop-down menu, select View/Modify Zone and click OK to open the View/Modify Zone window.
- 3 Select the DNS Zone object from the drop-down menu.
- 4 Click OK.

You can now modify the following DNS Zone configuration parameters:

- ♦ Zone Type: Specifies whether the zone is a primary or a secondary zone.
- ♦ Zone Master IP Address: If the zone type is secondary, specify the IP address of the master server for this zone.
- ♦ Available DNS Servers: Lists the available DNS Servers that are not assigned to this zone.
- ♦ Authoritative DNS Servers: Lists all authoritative servers for this zone.
 - ♦ Add All: Click this to assign all available DNS servers to a zone.
 - ♦ Remove All: Click this to remove all authoritative DNS servers from a zone.
- ♦ Designated DNS Server: The DNS Server selected in this field will act as a designated primary or designated secondary server depending on the zone type being primary or secondary respectively.
- ♦ Comments: You can provide information about the zone in this field. This parameter is optional.

- ◆ **Modify Zone Out Filter:** Specifies a list of IP addresses or networks authorized to perform zone transfers for this zone from the DNS server managing it.
- ◆ **Zone Master:** Specifies the domain name of the master DNS Server.
- ◆ **E-mail Address:** Specifies the e-mail address (with '@' replaced by '.') of the person responsible for this zone.
- ◆ **Serial Number:** Use this field to set a version number for the Start of Authority.
- ◆ **Interval values:** Select from the following values:
 - ◆ **Refresh:** Specifies the time in which the secondary name server transfers a copy of the zone data to the primary name server. The default is 180 minutes.
 - ◆ **Retry:** Specifies the time that a secondary name server waits after a transfer has failed and before it tries to download the zone database again. The default is 60 minutes.
 - ◆ **Expire:** Specifies the time after which a secondary name server will be unable to download a zone database. The default is 168 hours.
 - ◆ **Minimal TTL:** Specifies the minimum TTL for a resource record. This parameter determines the period for which a DNS server retains an address mapping in the cache. The default is 24 hours.

Deleting a Zone Object

- 1** Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2** From the drop-down menu, select Delete Zone and click OK to open the Delete DNS Zone window.
- 3** Select the DNS zones that are to be deleted.
To delete all the Zone objects in the list, click the top-level check box.
- 4** Click Next.
- 5** Select the zones whose sub-zones are to be deleted.
To delete all the sub-zone objects in the list, click the top-level check box.
- 6** Click Delete.

Importing a Zone Object

- 1** Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2** From the drop-down menu, select Import Zone and click OK to open the Import DNS Zone window.
- 3** Click Next to select the context where the zone object must be created.
- 4** Select a target DNS server distinguished name.
This server will subsequently manage the zone data.
- 5** Under the Zone Type, select either Primary (default) or Secondary.
- 6** If you select Secondary as the Zone type, specify the IP address of the zone.
- 7** Specify or browse to select the DNS Bind File location.
- 8** Click OK.

If the import operation encounters any problems, you can view the error details by downloading the log file. Also, if any of the resource records are ignored because of this problem, you can create them using the task [“Creating Resource Records” on page 87](#).

Exporting a Zone Object

- 1 Click DNS > Zone Management to open the Zone Management window in the main panel.
- 2 From the drop-down menu, select Export Zone and click OK to open the Export DNS Zone window.
- 3 From the drop-down menu, select the DNS Zone to which the file will be exported.
- 4 Click OK.
- 5 Click the Click here to download link to open the File Download dialog box.
- 6 Select Save this file to disk, then click OK.
- 7 Specify the name of the file or browse to select it, then click Save.
- 8 Click Done.

Resource Record Management

An RRSet object represents an individual domain name within a DNS zone. Each RRSet object has one or more resource records beneath it that contain additional information about the domain.

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.

The Resource Record Management role consists of the following tasks:

- ◆ [“Creating Resource Records” on page 87](#)
- ◆ [“Viewing or Modifying Resource Records” on page 88](#)
- ◆ [“Deleting Resource Records” on page 88](#)

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:

- 1 Click DNS > Resource Record Management to open the Resource Record Management window in the main panel.
- 2 From the drop-down menu, select Create Resource Record and click OK to open the Create Resource Record window.
- 3 From the drop-down menu, select the domain name where the resource record is to be created, then click Create.

Resource records cannot be created in a secondary zone.

- 4 Specify the owner name under which you want to create the resource record or click the Object Selector icon to search for an existing owner name.

If the owner name is not specified, the resource record is created under "@".

- 5** From the Others drop-down menu, select the Resource Record Type (RR Type) from the available options and specify the appropriate resource record data corresponding to the type chosen.
- 6** Click Create.
- 7** Click OK after the resource record is created.
- 8** Click Done to automatically increment the serial number and complete the task.

For more information on Resource Record Types, see [“Types of Resource Records” on page 174](#).

NOTE: Start of Authority (SOA) is defined as part of a Zone object's attributes. A Pointer (PTR) record is created automatically when any new A resource record is created and if a primary IN-ADDR.ARPA zone exists to which the IP address belongs. Similarly, an A type resource record is created when any new PTR record is created and if a primary zone exists to which the domain name pointed by PTR record belongs.

Viewing or Modifying Resource Records

- 1** Click DNS > Resource Record Management to open the Resource Record Management window in the main panel.
- 2** Select View/Modify Resource Record from the drop-down menu and click OK to open the Modify RRSets - Resource Record window.
- 3** From the Select Domain drop-down menu, select the domain that contains the host or RRSets. Resource records cannot be created in a secondary zone.
- 4** Specify or search to select the values for the following fields: Host Name, Resource Record, and Resource Record Type.

To use the search feature to select these values:

- ◆ Click the Object Selector icon to open the Object Selector window.
- ◆ Select the Resource Record type from the drop-down menu, select the number of search results to be displayed per page, click Search, and then click the hostname.

This automatically fills in the Host Name, Resource Record, and Resource Record Type fields.

- 5** Click Modify to modify the resource record data.
- 6** Modify the resource record data for all but the following types of resource records:
 - A (or IPv4)
 - AAAA (or IPv6)
 - A6
 - PTR
- 7** Enter new comments or modify existing comments for the resource record data.
- 8** Click Done to save the changes.

Deleting Resource Records

You can delete one, more than one, or all resource records and RRSets, using the multi-select deletion feature in the iManager utility.

- 1** Click DNS > Resource Record Management to open the Resource Record Management window in the main panel.

- 2** From the drop-down menu, select Delete Resource Record and click OK to open the Delete RRSet - Resource Record window.
- 3** From the Select Domain drop-down menu, select the domain that contains the host or RRSet. Resource records cannot be created in a secondary zone.
- 4** Delete either the entire RRSet or one or more resource records in the RRSet.
To delete one or more hosts or RRSets:
 - ◆ To search for RRSets by owner name, specify the name of the RRSet owner.
 - ◆ Select the RRSet option from the Search Type drop-down menu.
 - ◆ Click Search to list the available RRSets that match the specified owner name.
 - ◆ To delete all RRSets listed, click the top-level check box and click Delete. To delete one or more RRSets, click the corresponding check boxes and click Delete.
- 5** To delete one or more resource records:
 - ◆ To search for a resource record by owner name, specify the name of the Resource Record owner.
 - ◆ Select Resource record from the Search Type drop-down menu.
 - ◆ Select the resource record type from the RR Type drop-down menu.
 - ◆ Click Search to list the available resource records that match the specified owner name.
 - ◆ To delete all resource records listed, click the top-level check box and click Delete. To delete one or more resource records, click the corresponding check boxes and click Delete.

NOTE: When the A and PTR type resource records are deleted, the corresponding PTR and A resource records will also be deleted.

Using the Java-Based Management Console to Configure DNS

This section provides information about configuring DNS, and importing and exporting database information using the Java-based Management Console.

- ◆ [“DNS Prerequisites” on page 89](#)
- ◆ [“Logging In to the Tree for DNS Setup” on page 90](#)
- ◆ [“DNS Server Management” on page 90](#)
- ◆ [“Zone Management” on page 94](#)
- ◆ [“Resource Record Management” on page 97](#)
- ◆ [“Command Line Options” on page 99](#)

DNS Prerequisites

Complete the following prerequisites before setting up DNS:

- Install NetWare 6.5 on the selected servers.
- Install the Novell Client™ software on client computers that will be used to administer DNS and DHCP.
- Install the Management Console on client computers that will be used to administer DNS and DHCP.

For detailed information about installing client software, refer to [“Launching the Java-Based Management Console” on page 64](#).

NOTE: You must use a client workstation that is bound to TCP/IP to use the Management Console. Using the Management Console on the client workstations that are bound to IPX-only networks will result in Server objects being displayed as inactive, and will also disable the Start and Stop Service button and the Audit Trail/Event Log buttons.

Logging In to the Tree for DNS Setup

In order to use the Management Console to configure the DNS objects, you must first log in to the tree that contains the DNS objects.


- 1 Right-click Network Neighborhood and select NetWare Login on a Windows client workstation where the Management Console is installed.
- 2 Under the Login tab, provide your username and password, then click Advanced.
- 3 To log in, enter the tree, context, and server names.
- 4 Click OK.

DNS Server Management

DNS Server Management involves the following tasks:

- ♦ [“Creating a DNS Server Object” on page 90](#)
- ♦ [“Viewing or Modifying a DNS Server Object” on page 91](#)
- ♦ [“Deleting a DNS Server” on page 92](#)
- ♦ [“Starting or Stopping a DNS Server” on page 92](#)
- ♦ [“Configuring DNS Auditing” on page 92](#)
- ♦ [“Viewing or Saving the DNS Audit Trail Log” on page 93](#)
- ♦ [“Viewing or Saving the DNS Event Log” on page 93](#)
- ♦ [“Moving a DNS Server” on page 94](#)

Creating a DNS Server Object

- 1 Click the DNS Service tab of the Management Console, if necessary.
- 2 Click Create  on the toolbar.
- 3 Select DNS Server in the Create New DNS Object dialog box, then click OK.

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

- 4 Specify the desired server’s name or use the browse button to select the server.
- 5 Specify the server’s Domain name.
- 6 Click the Define Additional Properties check box to view the newly created server property pages.
- 7 Click Create.

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

Viewing or Modifying a DNS Server Object

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

On this 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 the zone information, you must modify the specific Zone object. This information cannot be modified from the server page.

The DNS Server IP Address field is read-only and is received from the DNS Server.

- ◆ Forwarding List

This page displays a list of all forwarding IP addresses.

- ◆ To add an address to the list, click Add. Specify the IP address in the Add Forward IP Address field, then click OK.
- ◆ To delete an address from the list, select an IP address and click Delete.

- ◆ No-Forward List

This page displays a list of all domain names to which queries are not sent.

- ◆ To add a domain name to the No-Forward List, click Add. Specify 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.

- ◆ Options

This page allows you to configure audit and event logging. SNMP traps, maximum cache size, and max recursion lookups can be configured only for a new DNS Server. You can configure the SNMP traps options.

- ◆ Control Lists

This page displays various lists that can be configured to control the behavior of the DNS Server. You can configure the zone out filter, allow recursion, query filter as address match lists. You can also configure the also notify and black listed servers as a list of IP addresses.

- ◆ To add an element to the address match list, click Add. Specify the element to be added and click OK.
To delete elements from the list, select the element to be deleted and click Delete.
- ◆ To add an address into the list, click Add. Specify the IP address and click OK.
To delete an address from the list, select the address to be deleted and click Delete.

- ◆ Advanced


This page displays all advanced configuration options. It displays the configured values and the default values for each option. The default value that is displayed is the value that the server assumes if it is not configured.

- ◆ To modify the options, click Modify and specify the new value, then click OK.
- ◆ To clear the configured values, select the option, then click Clear.

The allow-notify and listen-on options are multi-valued. You can also specify a port value, which is optional for listen-on.

- ♦ To add an element to the list, specify the address, then click Add. This populates the list with the new entry.
- ♦ To delete elements from the list, select the elements to be deleted, then click Delete.
- ♦ Click Modify to modify the configured elements.
- ♦ Click OK to populate the Configured Value column with the elements.

Deleting a DNS Server


- 1 Select the DNS Server from the lower pane of the Management Console.
- 2 Click Delete  on the toolbar and confirm the deletion.

Starting or Stopping a DNS Server

The DNS server (named.nlm) must be loaded before you can start or stop the server activity.


The Start/Stop service can be used to load zone data along with the modified configuration without unloading and reloading the DNS server. When you stop the DNS server using this option, it will still be loaded in the memory. However, no services are provided. You can use the iManager Management utility or the Java-Based Management Console to update the zone data. When you restart the DNS server using this option, the server is reconfigured with the new configuration settings and the zone data is also reloaded.

This option can also be used to remotely start and stop the DNS server.

- 1 Select the DNS Server from the lower pane of the Management Console.
- 2 Click Start/Stop Service  on the toolbar.
- 3 Depending on the state of the DNS Server module, one of the following operations will occur:
 - ♦ Start action: If the DNS Server module is loaded but is in Stop mode, it is started.
 - ♦ Stop action: If the DNS Server module is loaded and is in Start mode, it is stopped.

Configuring DNS Auditing


To configure a DNS server to audit activities:

- 1 Log in to the tree containing the service you want to begin auditing, launch the Management Console, then click the DNS Service tab.
- 2 Select the desired server to perform auditing, then 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 toolbar.

NOTE: Auditing is supported for DNS servers running on prior versions of NetWare 6.5 only.

Viewing or Saving the DNS Audit Trail Log

To view the audit trail log, csatpxy.nlm must be running on the server.

- 1** Log in to the desired tree, launch the Management Console, then click the DNS Service tab.
- 2** Select the server that has been configured to perform auditing, then click View Audit Trail  on the toolbar.

The Events Period-Audit Trail Log dialog box displays the start and end 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.

- 5** Click Save to save the audit log information.

Viewing or Saving the DNS Event Log

To view the event log, csatpxy.nlm must be running on the server.

- 1** Log in to the desired tree, launch the Management Console, then click the DNS Service tab.
- 2** Select the server that has been configured to perform event logging and click View Events/ Alerts  on the toolbar.

The Events Period-Events Log dialog box displays the start and end 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 start and end dates, display one or more types of event severity, and view specific operational states.

- 5** Click Save to save the audit log information.

Moving a DNS Server

This task enables you to move the DNS Services from one NCP server to another NCP server. You can also convert a DNS server to a cluster-enabled DNS server by moving it to a virtual NCP server.

This feature is supported for DNS servers running on NetWare 6.5 or later.

- 1 Select the DNS Server name from the bottom panel.
- 2 Click the Move DNS Server  icon on the toolbar.
- 3 In the Move DNS Server Dialog box, select the NCP server that the DNS services will be moved to, then click Move.

Zone Management


See the following sections for zone management information:

- ♦ [“Creating a Zone Object” on page 94](#)
- ♦ [“Creating an IN-ADDR.ARPA Object” on page 95](#)
- ♦ [“Viewing or Modifying a Zone Object” on page 95](#)
- ♦ [“Deleting a Zone Object” on page 96](#)
- ♦ [“Importing a Zone Object” on page 96](#)
- ♦ [“Exporting a Zone Object” on page 97](#)

Creating a Zone Object

The DNS Zone object is an eDirectory container object that comprises Resource Record Set (RRSet) objects and resource records.

To create a zone object:

- 1 Click the DNS Service tab of the Management Console.
- 2 Click Create  on the toolbar, select Zone, then click OK.
- 3 Click Create New Zone to create a forward zone.
- 4 Use the browse button to select the eDirectory context for the zone.
- 5 Specify a name for the Zone object in the Zone Domain Name field.
- 6 Select the zone type.

Novell DNS servers will act as primary or secondary depending on the zone type that you select.

- 7 If you select zone type as secondary, specify the IP address of the master DNS server that will provide zone out transfers for this secondary zone.


Select a DNS server to act as an authoritative DNS server for this zone.

- 8 Click Create.

A message is displayed indicating that the new zone has been created. If you have created a primary zone, 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 Object

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

- 1 Click the DNS Service tab of the Management Console.
- 2 Click Create  on the toolbar, 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 eDirectory context for the zone.
- 5 Specify the network address in the Network Address field.

For example, specify 143.72.155 only for 155.72.143.IN-ADDR.ARPA.

After you specify the IP address, it is reversed and prepended to .INADDR. ARPA and reflected in the Zone Domain Name field.

- 6 Under the Zone Type, select Primary or Secondary.

If you select Secondary, you must specify 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.

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

- 8 Click Create.

Viewing or Modifying a Zone Object

To modify an existing Zone object, click the Zone object to be modified in the left pane of the DNS Service window. A Zone object's detailed information window displays the following tab pages:

- ◆ Attributes

This page allows you to configure the zone type and zone servers.

- ◆ To change a primary zone to a secondary zone, click the secondary zone box and specify the IP address of the primary DNS server in the Zone Master IP Address field.
- ◆ To assign a server to the zone, select the server to which the zone should be assigned from the Available DNS Servers and click Add. The server will then be displayed in the Authoritative DNS Servers field. To delete a DNS server assignment to a zone, select the server to be removed from the Authoritative DNS Servers field, then click Remove.
- ◆ To configure one of the DNS servers as the designated server for the zone, select the server from the Designated Primary field in the case of a primary zone. This server is responsible for DHCP updates for the zone.

In the case of a secondary zone, select the server from the Designated Secondary field. This server is responsible for receiving the zone-in transfers.

- ◆ You can enter new comments or modify existing comments for the zone.

- ◆ Zone Out Filter

This page allows you configure the zone out filters for the zone.

- ◆ To add an entry into the list, click Add.

Specify the subnet address and the subnet mask for the network, then click OK.

- ◆ To delete the elements in the list, select the elements to be deleted, then click Delete.

- ◆ SOA Information

This page allows you to configure zone master, e-mail address, serial number, refresh, retry, expire, and minimum TTL values.

- ◆ Control Lists

This page displays various lists that can be configured for the Zone. You can configure the query filter, also notify, and allow update options.

The query filter and allow update options can be configured as address match lists.

- ◆ To add an element, click Add. Specify the element to be added, then click OK.
- ◆ To delete elements from the list, select the element to be deleted, then click Delete.

The also notify option can be configured as a list of IP addresses.


- ◆ To add an address into the list, click Add. Specify the IP address, then click OK.
- ◆ To delete an address from the list, select the address to be deleted, then click Delete.

- ◆ Advanced

This page displays all advanced configuration options for the zone. It displays the configured values for each option. If any option is not configured at the zone level, the default behavior is server specific. The value configured for the zone will override the server value. If no value is configured at the server, then the default value specified for the server is used.

- ◆ To modify the option, click Modify, specify the value, then click OK.
- ◆ To add an element, specify the address, then click Add. This populates the new entry into the list.
- ◆ To delete elements from the list, select the elements to be deleted, then click Delete. Click OK to populate the Configured Value column with the elements.
- ◆ To clear the configured values for the options, select the option, then click Clear.

Deleting a Zone Object


- 1 Select the Zone object you want to delete.
- 2 Click Delete  on the toolbar.

A warning message is displayed to confirm the zone deletion. You can also delete subzones by selecting the option from the message window.

Importing a Zone Object

Use the Import dialog box to convert BIND-formatted DNS files and transfer them into the eDirectory database.

To import a Zone object:

- 1 Click the DNS Service tab of the Management Console.
- 2 Click Import DNS Database  on the toolbar.
- 3 Specify the DNS BIND formatted filename in the field provided. You can browse to select filenames from the File Selection dialog box.

4 Click Next to select the context where the zone object should be created.

5 Click Next to select the server name that manages the zone.

You can select an existing DNS server or an NCP server where the DNS server object will be created. The selected DNS server must have DNS/DHCP services installed on it. If you select this zone type as primary, this DNS server will act as a designated primary; or if you select zone type as secondary, it will act as a designated secondary.

If you do not want to assign a DNS server for this zone at this point, leave this field blank.


6 Click Next to specify this zone type.

If you select the zone type as primary, Novell DNS servers act as primary servers for this zone; if you select secondary, they act as secondary DNS servers.

7 Click Next to view the configuration that you have selected.

8 Click Import to start the import operation.

If the import operation encounters any errors while transferring data, the Details button is enabled. Click Details to view the errors.


If some resource records are not transferred because of incorrect data, you can create them by clicking Create  on the toolbar.

9 Click Finish to complete the import operation.

Exporting a Zone Object

Use the Export dialog box to copy the eDirectory database to a text file. The text file enables you to save the DNS zone data to BIND master file format files. These files can be imported to other applications, including BIND servers, or they can be imported back into the eDirectory database using the Management Console.

1 Click the DNS Service tab of the Management Console.

2 In the DNS Service window, select the zone you want to export and click Export Database  on the toolbar.

3 In the Export - DNS window, specify the name of the destination file or browse to select a filename from the dialog box.

4 Click Export to export the database into a file.

Resource Record Management

- ◆ [“Creating Resource Records” on page 97](#)
- ◆ [“Viewing or Modifying Resource Records” on page 98](#)
- ◆ [“Deleting Resource Records” on page 98](#)


Creating Resource Records

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

Every domain name in the zone will have a corresponding RRset object under that zone container object. An RRset is not created directly. Initially, when a resource record is created and is assigned a unique domain name within a zone, the corresponding RRset is created first; then, the RR is associated with the RRset.

If you select an existing RRset and click Create on the toolbar to create a new RR, the Management Console will set the new RR domain name to read-only and will assign the newly created resource record to the selected RRset. Resource records cannot be created in a secondary zone. All changes to the resource record data should be done at the master server; the secondary servers will receive the changes through zone transfers.

To create resource records:

- 1** In the DNS Service window, select the zone in which the resource record will be created. If you want to add another resource record to an already existing RRset, select that RRset.
- 2** Click Create  on the toolbar.
- 3** In the Create New DNS Object window, select the resource record, then click OK.
- 4** If you have selected an RRset, the owner name field will be filled with the RRset name. This field does not need to be edited.

If you have selected a zone and want to create a new RRset, specify the domain name of that resource record in the owner name field.

The zone name part of the domain name will already be filled. Only the remaining portion need to be filled.

If you are creating a resource record to zone domain name, the owner name field does not need to be filled because the zone domain name is already present.

- 5** In the Create Resource Record window, select the RR type to be created.
- 6** Specify the required data for the selected resource record, then click Create.

NOTE: Start of Authority (SOA) is defined as part of a Zone object attribute. A Pointer (PTR) record is created automatically when any new A resource record is created and if a primary INADDR.ARPA zone exists to which the IP address belongs. Similarly, an A type resource is created when any new PTR record is created and if a primary zone exists to which the domain name pointed by PTR record belongs.

Several resource record types correspond with a variety of data stored in the domain namespace. For a list and description of resource record types, see [“Types of Resource Records” on page 174](#).

Viewing or 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. You can modify the resource record data and save changes by clicking Save on the toolbar.

You can modify resource record data and the associated comments for all resource records except the AAA, A6, SRV, LOC and HINFO records.

Deleting Resource Records

You can delete one, more than one, or all resource records and RRsets, using the multi-select deletion feature in the Management Console. RRsets and resource records in a secondary zone cannot be deleted. They should be deleted from a primary server.

- 1** Click the DNS Service tab of the Management Console.
- 2** From All Zones, select the domain that contains the host or RRSet.
- 3** Select the item to be deleted.

You can delete either the entire RRSet or one or more resource records in the RRSet.

To delete one or more objects:

- ◆ Press the Shift key and select the objects.
- ◆ Click Delete.

NOTE: When the A and PTR type resource records are deleted, the corresponding PTR and A resource records will also be deleted.

Command Line Options

The following are the command line options that can be specified while launching the java-based Management console:

| Option | Use |
|--------|--|
| -c | Specifies the context in which the DNS/ DHCP locator object is present. When you use this option, you can eliminate the search for the DNS/DHCP Locator object and obtain a quicker start up of the DNS/DHCP Management Console. |
| -p | Specifies the port to which the audit and event log request will be sent. By default, the csatpxy.nlm listens on port 2000 and hence the Management Console also sends its requests to port 2000 by default. If you change the port used by csatpxy.nlm, specify that value here using this option. |
| -s | Limits the administrative scope of the DNS/DHCP Management console. If you manage only objects under ctp.novell context, you can set option as “-s ctp.novell” and launch the management Console. With this option set, you can view only those DNS/DHCP objects that are under ctp.novell eDirectory context. Using this option might improve the server performance because not all DNS/DHCP objects are read. If you do not set this option, all the DNS/DHCP objects present in the tree will be displayed. |
| -mx | Specifies the maximum heap size to be used by the DNS/DHCP management console. The default heap size is 64 MB. If you have a large amount of DNS/DHCP objects to be displayed, you can increase the maximum heap size using this option. To specify 100 MB as the heap size, you can set this option as “-mx 100m”. |

You can edit the target of the Management Console shortcut to permanently set these options instead of specifying every time you launch the management Console. For example, you can set the above options by editing the target as shown below:

```
"C:\program files\novell\dnsdhcp\dnsdhcp.exe" -c dnsdhcp.novell -p 1000 -s ctp.novell -mx 100m
```

Configuring DNS Features

This section describes the following procedures:

- ◆ [“Configuring Roles for Novell DNS Server” on page 100](#)
- ◆ [“Configuring a DNS Server to Forward Queries to Root Name Servers” on page 100](#)
- ◆ [“Configuring a DNS Server as a Cache-Only Server” on page 100](#)
- ◆ [“Configuring Child \(Sub\) Zone Support” on page 101](#)
- ◆ [“Configuring a Multi-Homed Server” on page 101](#)
- ◆ [“Configuring Dynamic DNS” on page 101](#)

Configuring Roles for Novell DNS Server

Novell DNS servers act in the following roles for a zone:

- ◆ Designated primary server
- ◆ Passive primary server
- ◆ Designated secondary server
- ◆ Passive secondary server

The role played by the server for a zone depends on the zone type. If the zone type is primary, the server acts as a designated primary or a passive primary. All servers that are managing a primary zone will act as primary servers for that zone, and among all the primary servers, one server can be assigned as a designated primary server for that zone. All other servers are called passive primary servers. The designated primary server accepts dynamic updates for that zone. All primary servers respond to queries for this zone and notify slave servers of this zone about changes in data that can occur due to dynamic update or changes by users.

If the zone type is secondary, the server acts either as a designated secondary or a passive secondary. All servers that are managing a secondary zone will act as secondary (or slave) servers for the zone, and among all of the secondary servers, one server can be assigned as a designated secondary server. All other secondary servers are called as passive secondary servers. The designated secondary server is the one who do zone-in transfer for the zone from the master server and writes the data into eDirectory.

To configure a server as a passive primary for a zone, specify the server name in the Authoritative servers field of that zone. Make sure this server name is not in the designated primary field.

To configure a server as designated primary, specify the server name in the authoritative servers field of that zone and select that server name from the designated primary field.

To configure a server as a passive secondary for a zone, specify the server name in the Authoritative servers field of that zone. Make sure this server name is not in the designated secondary field.

To configure a server as designated secondary server, specify the server name in the authoritative servers field and select that server name in the designated secondary field.

To do this using the iManager utility, see [“Viewing or Modifying a Zone Object” on page 85](#).

Configuring a DNS Server to Forward Queries to Root Name Servers

When you install NetWare 6.5, the root server information is automatically loaded into your system. No additional steps are required to configure your system to forward queries to the root name servers.

Configuring a DNS Server as 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 Server Object” on page 76](#) or [“Creating a Zone Object” on page 94](#). After you create the DNS server object, do not assign it to any zone. Configure this server to

forward its queries to a DNS server connected to the Internet. You can do this by specifying the DNS server IP address in the Forwarders option.

Configuring Child (Sub) Zone Support

If you create a child zone, you must configure the glue records to associate the child zones with the parent zone.

The parent zone should contain an NS record for the child zone domain name. If the child zone name server domain name belongs to the parent zone or the child zone, the parent zone should have an A record for that name server domain name.

When configured as described above, queries to the parent zone name server 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 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 might be on different networks.

If you have a DNS server with more than one IP address, and if you have specified one of the IP addresses in the listen-on option of the server, make sure the same IP address is used in the A record for the DNS server domain name.

NOTE: An NS resource record specifies a domain name for an authoritative name server for the specified class and domain.

Configuring Dynamic DNS

Dynamic DNS (DDNS) provides automatic updates of DNS with address and pointer records for addresses and hostnames that are assigned using the DDNS feature. To use DDNS, the following configuration must already exist:

- ◆ The DNS Zone object to receive DHCP updates must be created. For all networks that are served by the DNS server, the DNS zones must have reverse zones configured. For more information on configuring the reverse zones, refer [“Creating an IN-ADDR.ARPA Object” on page 84](#) and [“Creating an IN-ADDR.ARPA Object” on page 95](#).
- ◆ Subnet Address Range objects that use the DDNS must be set to range type Dynamic BOOTP and DHCP or Dynamic DHCP.

To activate the DDNS feature:

- 1** Select the Subnet object of the Subnet Address Range on which you want to activate DDNS, then 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.

Loading the DNS Server

After you have created and set up a DNS server object and DNS Zone objects, specify the following command at the NetWare system console:

load named

After named.nlm is loaded, the DNS server can respond to queries. After creating the DNS server object, you can edit the autoexec.ncf file to uncomment the named.nlm load statement. This will enable you to avoid the manual loading of the named.nlm every time you restart NetWare. For detailed information about named.nlm command line options, see [“NAMED Command Line Options” on page 102](#).

After named.nlm is loaded, you can use the management utilities to start and stop the DNS server. For information on starting and stopping the DNS server, see [“Starting or Stopping a DNS Server” on page 79](#) or [“Starting or Stopping a DNS Server” on page 92](#).

NAMED Command Line Options

All command line options for DNS server are optional.

If the DNS server is loaded without any options, default values for all of the options, wherever applicable, are used.

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

load named

Command line options can be specified in three different scenarios:

- ◆ Load: This is the first time the DNS server is loaded.
- ◆ Stop state: The server can be stopped using the management utilities. The NLM remains loaded, but it supports only a limited set of services.
- ◆ Reload: The load named command can be issued repeatedly after a new load. After a new load, the load named command is used to issue command line options.

The command line options are listed in the table below.

| CLO | Syntax | Default Value | Load Support | Stop-State Support | Reload Support |
|-------------------------|---|--|--------------|--------------------|----------------|
| Cluster Enabling | -v <i>volumename</i> | SYS | Yes | No | No |
| Debug | -dl <i>level</i> -dc <i>categories</i> | Global level =0 and all categories are enabled | Yes | Yes | Yes |
| DNS Port | -p <i>portnumber</i> | 53 | Yes | No | No |
| Dynamic Reconfiguration | -r on off | On | Yes | Yes | Yes |
| Fault Tolerance | -ft on off | On | Yes | No | No |
| Force Zone-in | -zi <i>zonename</i> | NA | No | No | Yes |
| Number of CPUs | -n <i>number of cpus</i> | 1 | Yes | No | No |

| CLO | Syntax | Default Value | Load Support | Stop-State Support | Reload Support |
|-----------------------------|----------------------------------|---------------|--------------|--------------------|----------------|
| Purge all Cache | -pa | NA | No | No | Yes |
| Replace Characters | -rp <i>character</i> | NA | Yes | Yes | Yes |
| Screen Logging | -s | NA | Yes | Yes | Yes |
| Server Statistics | -mstats -qstats | NA | No | Yes | Yes |
| Usage Display | -? | NA | Yes | Yes | Yes |
| Zone Information | -info [<i>file_name</i>] | NA | No | No | Yes |
| Journal Log File Size Limit | -jsize <i>size in Kilo Bytes</i> | NA | Yes | Yes | Yes |

Some command line options can be specified only at load time. These options control the behavior that can be set only once for a particular running session (load, followed by multiple reloads, and finally the unload) of the DNS server. If you specify an invalid value for such an option at the load time, the server exits, because once the server is up and running, these options cannot be used again. These options are ignored at reload time or when the server is in the stop state. However, the server will come up if the options are also available in reload because the user can set the desired behavior later.

Syntax: named [-dc *categories*] [-dl *debuglevel*] [-ft *on|off*] [-jsize] [-info] [-mstats] [-n *no_of_cpus*] [-p *port_no*] [-pa] [-qstats] [-r *on|off*] [-rp *character*] [-s] [-v *volumename*] [-zi *zonename*] [-?]

Description of Command Line Options

Usage Syntax: -?

Cluster Enabling Syntax: -v *volume_name*

By default, the DNS server uses the sys volume to store backup zone files, journal files, and other files.

This option enables clustering, by providing a volume other than sys. The volume name specified as the argument should exist and mounted on the NetWare server.

Example: Load named -v *new_volume*

If *new_volume* exists and is mounted on the NetWare server, the DNS server stores all files to this volume. For example, the log file named.run is created at *new_volume:named.run* and the zone data files are stored at *new_volume:etc\dns*.db*.

Debugging Categories Syntax: -dc *categories*

Logging is enabled for the categories specified with this option. For all other categories, no information is logged. When you specify the value all, logging is enabled for all the categories. By default, logging is enabled for all categories with the current debugging level as specified by the -dl option.

| Category | Abbreviation | Description |
|-----------------|--------------|---|
| Default | d | Defines the logging options for those categories where no specific configuration has been defined |
| General | g | Many things are not classified into categories, and they are placed here |
| Config | c | Configuration file parsing and processing |
| Notify | n | The notify protocol |
| Database | D | Messages relating to the databases used internally by the name server to store zone and cache data |
| Security | s | Approval and denial of requests |
| Resolver | r | DNS resolution, such as the recursive lookups performed on behalf of clients by a caching name server |
| Xfer-in | xi | Zone transfers the server is receiving |
| Xfer-out | xo | Zone transfers the server is sending |
| Dispatch | di | Dispatching incoming packets to the server modules where they will be processed |
| Lame-servers | l | These are misconfigurations in remote servers, discovered when trying to query those servers during resolution |
| Client | C | Processing of client requests |
| Network | N | Network operations |
| Update | u | Dynamic updates |
| Queries | q | Query related information |
| Unmatched | un | Messages that named was unable to determine the class of or for which there was no matching view |
| Novell-specific | nov | Log messages for fault tolerance, dynamic reconfiguration, eDirectory interaction, start server, stop server, proprietary DDNS, and Audit/Event |
| Oldconfig | o | Backward compatibility |
| ALL | all | Enable all categories |

Debugging Level Syntax: `-dl level`

This option sets the level of information to be logged. If `-dl` is given 0 as the input, the debug messages of type information (level -1)/notice/warning/error/critical (level -5) are logged for all categories. For a positive level, for example `n`, all debug messages upto level `n` are logged.

It is recommended that the debug level should be less (not more than +2) while running `named` in a live environment as this impacts the server performance.

The default value for logging is notice [-2]. Only critical and error messages will be displayed on the named screen. All other messages will be logged in *volume_name*:named.run file, where *volume_name* is the volume that is specified with -v option. The default volume is sys.

DNS Port Syntax: -p *port_number*

The port specified in this option is used by the DNS server to listen for queries. The values for this option can be in the range 1-65535. The default port number is 53. This option is ignored if it is specified at the reload or in the stop state.

Dynamic Reconfiguration Syntax: -r on|off

If dynamic reconfiguration is enabled, the DNS server will periodically check the configuration data for the server and zones. As part of this activity, it will automatically detect added, deleted, and modified zones. This option has no effect on periodically checking the directory for changes in the zone data. Even if the dynamic reconfiguration is set to off, periodic detection of zone data will occur. The default period for dynamic reconfiguration is 15 minutes.

Fault Tolerance Syntax: -ft on|off

When this option is set to on, the DNS server will be able to start using the backup files if eDirectory is inaccessible. If off is specified for a new load, the DNS server will not service the zones for which eDirectory is not available.

Force Zone-In Syntax: -zi *zone_name*

Zone transfers can be initiated using this option for secondary zones. The domain name of the zone should be specified as the argument to the command line option. Force zone-in is only initiated if the zone is secondary and the DNS server is a designated secondary server for the zone. This option is ignored in the Stop mode or fresh load.

Number of CPUs Syntax: -n *number_of_cpus*

Specifies the number of CPUs available. The default value is 1 and the maximum value that can be specified is 32.

Replace Characters Syntax: -rp *characters*

A set of characters that are not allowed in the hostnames. The current list is ~!@#%&^*+=?`";'<> \()[]{}|. This option can be used to add characters to this list. If these characters are found in the hostnames, the DNS server replaces these characters with a dash(-) before storing them in eDirectory. This option is included for backward compatibility and only allows adding one more character to the existing list.

Memory Statistics Syntax: -mstats

This option saves the memory usage information for the DNS server to a file named.mem in the *volume_name*:sys/etc\ directory. This information is very important to determine the load on the DNS server.

Named.mem contains information for each memory pool. The following information is saved to the named.mem file.

- ◆ Name of the memory pool
- ◆ Size of each item in the pool
- ◆ Maximum number of items allowed
- ◆ Number of items currently allocated

- ◆ Number of items in the reserved list
- ◆ Number of items allowed in the free list
- ◆ Number of items to fetch in each fill
- ◆ Number of requests to this pool
- ◆ Pool locked YES (Y)/NO (N)

Query Statistics Syntax: -qstats

This option saves the DNS server query statistics information to `volume_name:etc\dns\named.sta`. This information is similar to the memory statistics information and helps to determine the load on the DNS server. Using this information, the DNS server can be configured for better performance. The following information is saved to the `named.sta` file:

- ◆ Number of queries answered successfully
- ◆ Number of queries referred to other servers
- ◆ Number of queries that were replied with non-existent RRset error code
- ◆ Number of queries that were replied with non-existent domain error code
- ◆ Number of queries that caused recursion
- ◆ Number of queries that failed

Purge All Cache Syntax: -pa

This option causes the server to purge all cache maintained in it.

Screen Logging Syntax: -s

Displays the log information on the `named` screen along with the `named.run` file.

Zone Information Syntax: -info *info_file*

This option provides information about the zones that are currently loaded in the server.

The syntax of the information is: Zone `ZONE_NAME` of type `MASTER/SLAVE` has `N` nodes and SOA `sr no`, is `SOA_SR_NO`

This information is saved to the file, if specified in the command line. Otherwise, it is displayed on the console screen.

Restricting Journal Log File Size Syntax: -jsize *Size in Kilo Bytes*

Journal log file is used by the DNS servers for incremental zone transfers and the size of the file increases based on the changes made. By default, there is no restriction on the size of a journal log file. This option can be used to specify the size (in Kilo Bytes) of the journal log file.

During dynamic reconfiguration, the journal log file is deleted if its size exceeds the specified one. As the journal log files are deleted only on the lapse of the dynamic reconfiguration interval (Minimum 10 minutes and maximum of 1 day), adequate size must be allocated for the journal log files.

Example. `Named -jsize 5000`.

During dynamic reconfiguration, this command deletes all the journal log files exceeding 5000 KB (or 5MB).

5

Configuring DHCP

This section provides information about the following:

- ◆ “Configuring Clients to Use DHCP” on page 107
- ◆ “Logging In to the Tree for DHCP Setup” on page 107
- ◆ “Using the iManager Utility to Configure DHCP” on page 108
- ◆ “Using the Java-Based Management Console to Configure DHCP” on page 123
- ◆ “Configuring Multiple Logical Networks” on page 135
- ◆ “Loading the DHCP Server” on page 135
- ◆ “DHCP SRVR Command Line Options” on page 136
- ◆ “Monitoring DHCP” on page 136

Configuring Clients to Use DHCP

To configure Windows NT and Windows 95/98/2000/XP client workstations to use DHCP:

- 1** At the client desktop, click Start > Settings > Control Panel, then double-click Network.
The Network window is displayed, listing the network components installed on the client workstation.
- 2** Click TCP/IP > Properties.
The TCP/IP Properties window is displayed.
- 3** Select Obtain an IP Address Automatically, then click OK.

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

IMPORTANT: 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 the TCP/IP Properties window.

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® 6.5 is installed.

To log in to the server:

- 1** Right-click Network Neighborhood and select NetWare Login on a NetWare 6.5 client workstation on which you have installed the Management Console.
The NetWare Client login dialog box is displayed.
- 2** Under the Login tab, provide your username and password, then click Connection.
- 3** Under the Connection tab, specify the Tree, Server, and Context of the server on which NetWare 6.5 is installed, then click OK.

Using the iManager Utility to Configure DHCP

This section provides information about the following:

- ◆ “Scope Settings” on page 108
- ◆ “DHCP Prerequisites” on page 109
- ◆ “Global DHCP Configuration” on page 109
- ◆ “DHCP Server Management” on page 112
- ◆ “Subnet Pool Management” on page 116
- ◆ “Subnet Management” on page 117
- ◆ “Address Range Management” on page 119
- ◆ “IP Address Management” on page 121

Scope Settings

For better performance results with the iManager utility, particularly in a distributed DNS/DHCP setup, you should configure the DNS/DHCP scope settings for the session before you proceed with other administrative tasks.

If you do not configure the DNS/DHCP scope settings for the session, you will receive a warning before every task you attempt to perform indicating that the scope settings are not set. However, you can proceed with the task by ignoring the messages.

Setting the scope of the DNS/DHCP services involves two specifications for the session: the Novell® eDirectory™ context of the Locator object and the administrative scope of the session. Specifying the eDirectory context of the Locator object at the start of the session significantly improves performance because it eliminates the need to search for the Locator object. Specifying the administrative scope of the session also improves performance significantly because it restricts the retrieval of DNS/DHCP objects for viewing to the scope you specify.

When you configure the DNS/DHCP scope settings for a session, they last only as long as the session lasts. If you start a new session, you must configure the DNS/DHCP scope settings again.

IMPORTANT: If you configure DNS/DHCP scope settings for a session for either DNS or DHCP, the settings apply across the session to both roles.

To configure DNS/DHCP scope settings:

- 1** Click DNS or DHCP > DNS/DHCP Scope Settings to open the DNS/DHCP Scope Settings window.
- 2** Specify the eDirectory context of the DNS/DHCP Locator object.
- 3** Specify the eDirectory context of the container object that will provide the administrative scope of the current session.
NOTE: If you specify only the eDirectory context of the DNS/DHCP Locator object and not the administrative scope of the current session, you can proceed with administrative tasks without receiving a warning message. However, performance is further optimized if you also define the administrative scope.
- 4** Click OK.
- 5** Click Repeat Task to configure the scope settings again.

A message indicates that the scope request was successful.

DHCP Prerequisites

Complete the following prerequisites before setting up DHCP:

- Install NetWare 6.5 on the selected servers.
- Install Novell iManager.
- Install Internet Explorer 5.0, Internet Explorer 5.5 Support Pack 2, or Internet Explorer 6.0.

Global DHCP Configuration

DHCP (and BOOTP) options can be assigned at three levels:

- ◆ Globally
- ◆ At the subnet level
- ◆ At the 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.

The Global DHCP Configuration role consists of the following tasks:

- ◆ [“Viewing or Setting Global DHCP Preferences” on page 109](#)
- ◆ [“Viewing or Setting Global DHCP Defaults” on page 110](#)
- ◆ [“Configuring DHCP Options” on page 110](#)
- ◆ [“Importing a DHCP Configuration” on page 111](#)
- ◆ [“Exporting a DHCP Configuration” on page 111](#)

These tasks are available from the iManager interface.

Viewing or Setting Global DHCP Preferences

To define a global DHCP option:

- 1** Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2** From the drop-down menu, select View/Set Global Preferences, then click OK to open the Global DHCP Preferences window.
- 3** Click Modify to open the DHCP Options window.
- 4** The DHCP Options you can configure globally are listed in the Available DHCP Options list box. To configure an option:
 - 4a** Select the option from the Available DHCP Options list box, then click Add.
 - 4b** Specify the required supporting information as prompted.
- 5** Click Done to close the DHCP Options window.

The global DHCP Option you added or configured is displayed in the Global DHCP Options list.

Viewing or Setting Global DHCP Defaults

- 1 Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2 From the drop-down menu, select View/Set Global Preferences, then click OK to open the Global DHCP Preferences window.
- 3 Click Next to open the Excluded Hardware Addresses list in the Global DHCP Defaults window.

This list contains the MAC addresses of clients that should not receive IP addresses from DHCP servers. These exclusions apply to all DHCP servers in the eDirectory tree.

3a Click Add, specify the MAC Address of the client, and then specify the hardware type.

3b Click OK.

- 4 Click Next to open the Included Hardware Addresses list in the Global DHCP Defaults window.

This list contains the MAC addresses of clients that will receive IP addresses from DHCP servers.

- ♦ Click Add, specify the MAC Address of the client, and then specify the hardware type.
- ♦ Click OK.

The MAC address is added to the Pooled (Included) Hardware Addresses list. This assignment applies to all DHCP servers in the eDirectory tree.

IMPORTANT: The Excluded and Included Hardware Addresses lists are mutually exclusive. You should configure only one of these lists and ensure that the other list is empty.

Configuring DHCP Options

The DHCP Options Table provides a list of parameters that can be defined for use on the network. After an option is defined, you can assign a value to the option using Global DHCP Options.

Viewing a DHCP Option

- 1 Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2 From the drop-down menu, select View/Set Global Preferences, then click OK to open the Global DHCP Preferences window.
- 3 Click Next three times to open the DHCP Options Table window that lists both the system-defined and user-defined DHCP options.
- 4 Click Done to return to the home page.

Adding a DHCP Option

- 1 Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2 From the drop-down menu, select View/Set Global Preferences, then click OK to open the Global DHCP Preferences window.
- 3 Click Next three times to open the DHCP Options Table window that lists both the system-defined and user-defined DHCP options.
- 4 Click Add, select the DHCP option code, select the data syntax, add the description of the new option, then click OK.

Deleting a DHCP Option

- 1** Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2** From the drop-down menu, select View/Set Global Preferences, then click OK to open the Global DHCP Preferences window.
- 3** Click Next three times to open the DHCP Options Table window that lists both the system-defined and user-defined DHCP options.
- 4** Select the option code, then click Delete.

Importing a DHCP Configuration

The Import DHCP Configuration feature enables you to copy DHCP 2.0 and 3.0 user files into the eDirectory database.

- 1** Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2** From the drop-down menu, select Import DHCP Configuration, then click OK to open the Import DHCP Configuration File window.
- 3** Specify the eDirectory context or browse to select it.
- 4** Select the default DHCP server name from the drop-down menu.
- 5** Specify the name of the DHCP configuration file or browse to select it.
- 6** Click OK.

The DHCP Subnet configuration information is displayed.

- ◆ To add an available DHCP Subnet to the list of selected subnets, click Add.
- ◆ To include all available DHCP Subnets to the list of selected subnets, click Add All.
- ◆ To delete a subnet from the list of selected subnets, click Remove.
- ◆ To delete all subnets from the list of selected subnets, click Remove All.

Exporting a DHCP Configuration

The Export DHCP Configuration allows you to copy the eDirectory database to a text file. The text file enables you to import DHCP subnet configuration data to other applications. You can also import the file back into the eDirectory database by using the iManager utility.

- 1** Click DHCP > Global DHCP Configuration to open the Global DHCP Configuration window in the main panel.
- 2** From the drop-down menu, select Export DHCP Configuration, then click OK to open the Export DHCP Configuration File window.
- 3** Add or remove DHCP subnet information:
 - ◆ To add an available DHCP subnet to the list of selected subnets, click Add.
 - ◆ To include all available DHCP subnets in the list of selected subnets, click Add All.
 - ◆ To delete a subnet from the list of selected subnets, click Remove.
 - ◆ To delete all selected DHCP subnets, click Remove All.
- 4** Click Download File and save the file when prompted.
- 5** Click Done to export the file.

DHCP Server Management

The DHCP Server Management role consists of the following tasks:

- ◆ “Creating a DHCP Server” on page 112
- ◆ “Viewing or Modifying a DHCP Server” on page 112
- ◆ “Deleting a DHCP Server” on page 113
- ◆ “Starting or Stopping a DHCP Server” on page 113
- ◆ “Loading or Unloading a DHCP Server” on page 114
- ◆ “Configuring DHCP Auditing” on page 114
- ◆ “Viewing the DHCP Event Log” on page 115
- ◆ “Viewing or Saving the DHCP Audit Trail Log” on page 114
- ◆ “Viewing the DHCP Event Log” on page 115
- ◆ “Saving the DHCP Event Log” on page 116

Creating a DHCP Server

Use the iManager utility 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:

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select Create Server, then click OK to open the Create DHCP Server window.
- 3** Specify the name of the NCP server or browse to select it.
- 4** Click Create.

A message indicates that the new DHCP server object has been created.

Viewing or Modifying a DHCP Server

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select View/Modify Server, then click OK to open the View/Modify Server window.
- 3** Select the DHCP Server object from the drop-down menu.
- 4** Click OK.

You will be led through a set of steps by where you can modify the following parameters:

- ◆ Subnet Address Range Serviced by this Server: Displays information about the range of addresses that can be dynamically assigned by the server.

- ◆ Subnet Serviced by this Server: Displays information about the subnet to which the server can assign addresses.
- ◆ Comments: You can type comments about the DHCP server in this box. This parameter is optional.
- ◆ Set SNMP Traps Option: SNMP traps control DHCP server event trapping. Select from the following options:
 - ◆ None: Turns off SNMP traps
 - ◆ Major Events: Traps only the critical events (default)
 - ◆ All: Traps both major and minor events
- ◆ Audit Trail and Alerts Option: Auditing allows you to analyze the historical data and diagnose operational difficulties. Select from the following options:
 - ◆ None: Disables auditing
 - ◆ Major Events: Audits only major events such as SNMP traps (default)
 - ◆ All: Audits all events
- ◆ Enable Audit Trail Log: Check this to log audit trails and events.
- ◆ Mobile User Option: The DHCP server can be configured to support mobile users such as laptop users. Select from the following options:
 - ◆ No Mobile Users Allowed: Disables support for mobile users
 - ◆ Allow Mobile Users but Delete Previously Assigned Address: Deletes previously assigned addresses while granting an address to a mobile user (default)
 - ◆ Allow Mobile Users but Do Not Delete Previously Assigned Address: Caches previously assigned addresses while granting an address to a mobile user
- ◆ Ping Address: Check this to ping an address to ensure that the address is not in use before it is assigned. Note that enabling ping increases traffic on the network.

Deleting a DHCP Server

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select Delete Server, then click OK to open the Delete DHCP Server window.
 - ◆ To remove all DHCP servers in the list, click the top-level check box, then click Delete.
 - ◆ To remove one or more DHCP servers, click the check box next to it, then click Delete.

Starting or Stopping a DHCP Server

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select Start/Stop Server, then click OK to open the DHCP Server Start/Stop Services window.
- 3** From the drop-down menu, select the server from the Select DHCP.
- 4** Click OK.

5 Depending on the state of the DHCP Server module, one of the following is displayed:

- ◆ Failure notification message: This appears if the DHCP Server module (dhcpsrvr.nlm) is not loaded. In order to start the server, load the DHCP Server module through the system console.
- ◆ Start button: If the DHCP Server module is loaded but is in Stop mode, click the button to start the DHCP server.
- ◆ Stop button: If the DHCP Server module is loaded but is in Start mode, click the button to stop the DHCP server.

NOTE: To use the Start/Stop DHCP service, load the dhcpsrvr.nlm.

Loading or Unloading a DHCP Server

This task enables you to load or unload a DHCP server.

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select Load/Unload Server and then click OK to open the Load/Unload Server window.
- 3** Select the DHCP server, then click OK.

Depending on the state the DHCP Server, one of the following appears:

- ◆ If the NLM is not loaded on the machine, you are prompted to load dhcpsrvr.nlm.
The supported command line options are displayed.
 - ◆ Enter the command line options to load the NLM with, then click Load.
- ◆ If the NLM is already loaded on the machine, you are prompted to unload dhcpsrvr.nlm.
 - ◆ To unload the NLM, click Unload.

- 4** Click OK to complete the task.

When you click load or unload, the corresponding command is sent to the server. The success status in iManager indicates only that the command was issued to the server. This does not necessarily mean that the command execution was successful.

Configuring DHCP Auditing

To configure a DHCP server for auditing, use the Audit Trail and Alerts Option.

- 1** Click DHCP > DHCP Server Management > View/Modify Server.
- 2** Select the DHCP server, click OK, then click Next.
- 3** Click Next, click the Enable Audit Trail Log check box, then click Done.

Viewing or Saving the DHCP Audit Trail Log

To view the audit trail log, csatpxy.nlm must be running on the server and the DHCP server must have been started at least once with a subnet assigned to it.

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select Audit Trail Log, then click OK to open the DHCP Audit Trail Log window.

- 3** Select the server from the DHCP Server drop-down menu.
- 4** If you want to filter the Audit Period, modify the start and end dates in the appropriate fields.
Use the following date format:
mm-dd-yyyy
- 5** Click OK.
This opens the DHCP Audit Trail Log table which lists the following data:
 - ◆ Entry Time
 - ◆ IP Address
 - ◆ Type
 - ◆ Status
 - ◆ Hostname
 - ◆ Hardware Address
 - ◆ Client ID
 - ◆ Lease Type
- 6** To define a view filter on the DHCP Audit Trail Log, click Display Options.
You can filter events on the following parameters:
 - ◆ Start Date: Sets a start date for monitoring the DHCP audit trail
 - ◆ End Date: Sets an end date for monitoring the DHCP audit trail
 - ◆ Transaction Type: Manual, dynamic, automatic, exclusion, unauthorized or IPCP, and Fix Host Dynamic
- 7** Click Next in the DHCP Audit Trail Log window.
- 8** Click the Click here to Download File link, then save the Audit Trail Log file on your local machine.

Viewing the DHCP Event Log

To view the event log, csatpxy.nlm must be running on the server and the DHCP server must have been started at least once with a subnet assigned to it.

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, select Event Log, then click OK to open the DHCP Event - Events Log window.
- 3** Select the server from the DHCP Server drop-down menu.
- 4** If you want to filter the Audit Period, modify the start and end dates in the appropriate fields.
Use the following date format:
mm-dd-yyyy
- 5** Click OK.
This opens the DHCP Event Log table that lists the following data:
 - ◆ Entry Time: Date and time the event occurred
 - ◆ Severity: Severity of the event (critical, major, warning, and informational)

- ◆ State: State of the server (operational, degraded, and inoperative)
 - ◆ Description: Description of the event that occurred
- 6** To define a view filter on the DHCP Events Log, click Display Options.
- You can filter events on the following parameters:
- ◆ Start Date: Sets a start date for monitoring the DHCP Event Log
 - ◆ End Date: Sets an end date for monitoring the DHCP Event Log
 - ◆ Severity: Defines the severity level of the event: critical, major, warning, and informational
 - ◆ State settings: Defines the condition of events recorded, such as operational, degraded, and inoperative

Saving the DHCP Event Log

To view the event log, csatpxy.nlm must be running on the server.

- 1** Click DHCP > DHCP Server Management to open the DHCP Server Management window in the main panel.
- 2** From the drop-down menu, Select Event Log and click OK to open the DHCP Event - Events Log window, then click Next.
- 3** Click the Click here to Download File link, then save the event log file on your local machine.

Subnet Pool Management

The Subnet Pool object provides support for multiple subnets through a DHCP relay agent or BOOTP forwarder by identifying a pool of subnets for remote LAN address assignments.

The Subnet Pool Management role consists of the following tasks:

- ◆ [“Creating a Subnet Pool Object” on page 116](#)
- ◆ [“Viewing or Modifying a Subnet Pool Object” on page 117](#)
- ◆ [“Deleting a Subnet Pool Object” on page 117](#)

Creating a Subnet Pool Object

- 1** Click DHCP > Subnet Pool Management to open the Subnet Pool Management window in the main panel.
- 2** From the drop-down menu, select Create Subnet Pool, then click OK to open the Create Subnet Pool window.
- 3** Specify a unique subnet pool name in the Subnet Pool Name field.
- 4** Specify the eDirectory context where the subnet pool record will be placed.
- 5** Click Create.

A message indicates that the new subnet pool object has been created.

Viewing or Modifying a Subnet Pool Object

- 1 Click DHCP > Subnet Pool Management to open the Subnet Pool Management window in the main panel.
- 2 From the drop-down menu, select View/Modify Subnet Pool, then click OK to open the View/Modify Subnet Pool window.
- 3 Select the Subnet object from the drop-down menu.
- 4 Click OK.

You can modify the Subnet Type configuration parameter. You can add a subnet to a subnet pool or remove a subnet from the pool.

To add a subnet to a subnet pool, click Add, select the subnet, then click OK.

To remove a subnet from a subnet pool, select the subnet, then click Delete.

Deleting a Subnet Pool Object

- 1 Click DHCP > Subnet Pool Management to open the Subnet Pool Management window in the main panel.
- 2 From the drop-down menu, select Delete Subnet Pool, then click OK to open the Delete Subnet Pool window.
 - ♦ To remove all the Subnet Pool objects in the list, click the top-level check box, then click Delete.
 - ♦ To remove one or more Subnet Pool objects, click the check box next to it, then click Delete.

Subnet Management

You can use the iManager utility to create and set up a DHCP Subnet object for each subnet to which you will assign addresses.

A Subnet object's specific DHCP options and configuration parameters apply to the entire subnet and override global options.

The Subnet Management role consists of the following tasks:

- ♦ [“Creating a Subnet Object” on page 117](#)
- ♦ [“Viewing or Modifying a Subnet Object” on page 118](#)
- ♦ [“Deleting a Subnet Object” on page 119](#)

Creating a Subnet Object

- 1 Click DHCP > Subnet Management to open the Subnet Management window in the main panel.
- 2 From the drop-down menu, select Create Subnet, then click OK to open the Create Subnet window.
- 3 Specify a unique subnet name.
- 4 Specify or browse to select the eDirectory context where the new subnet record will be stored.
- 5 Specify a subnet IP address, a subnet mask, and the name of a default DHCP server in the fields provided.

The default DHCP server field designates the principal DHCP server for a subnet. This server is assigned all the address ranges created under the subnet, unless a different server is specified when the range is created. The default server is the only server that responds to BOOTP requests for the subnet.

6 Click Create.

A message indicates that the new subnet has been created.

NOTE: The IP address objects are simultaneously created to exclude routing and broadcast addresses.

Viewing or Modifying a Subnet Object

1 Click DHCP > Subnet Management to open the Subnet Management window in the main panel.

2 From the drop-down menu, select View/Modify Subnet, then click OK to open the View/Modify Subnet window.

3 Select the Subnet object from the drop-down menu.

4 Click OK.

You will be led through a set of steps where you can modify the following parameters:

- ◆ DNS Zone for Dynamic Update: Specifies the DNS zone where dynamic updating occurs. The specified DNS zone is then notified of any changes to the subnet.
- ◆ Domain Name: Specifies the domain name that will be combined with the hostname received from the client computer. This name will be given to DNS during dynamic DNS update. The domain name must be part of the zone specified for dynamic DNS.
- ◆ Subnet Pool Reference: Specifies the subnet pool to be used by the subnet. This parameter setting is optional. Subnet pools enable the DHCP server to assign addresses to multiple logical networks on a single physical network. A subnet pool groups logical networks.
- ◆ Default DHCP Server: Specifies a default DHCP server that will assign address ranges for the subnet. This server is also the only server that will respond to BOOTP requests for the subnet.
- ◆ Comments: You can type your comments about the subnet. This parameter is optional.
- ◆ Lease Type: Specifies the length of time for an address assignment. A lease type can be permanent or timed. Permanent leases never expire; the client is assigned an IP address for an indefinite period. Timed leases are defined in days, hours, and minutes. Timed leases expire, unless the client renews the lease.
- ◆ Set Boot Parameter Options: Check this to specify the Server Address, Server Name, and Boot File Name for the BOOTP service. This information, provided at boot time, includes the address and name of a server that the client can contact for a boot image, as well as a boot filename.
- ◆ Other DHCP Options: To configure an option:
 - ◆ Click Modify to open the DHCP options page that lists the available DHCP Options.
 - ◆ Select the DHCP option and provide the necessary DHCP information.
 - ◆ To add an available DHCP option to the list of selected options, click Add.
 - ◆ To include all available DHCP options to the list of selected options, click Add All.
 - ◆ To delete a DHCP option from the list of selected options, click Remove.

- ◆ To delete all DHCP options from the list of selected options, click Remove All.
- ◆ Click Done.

To remove a DHCP option:

- ◆ To remove all DHCP options, click the top-level check box, then click Delete.
- ◆ To remove one or more DHCP options, click the check box next to it, then click Delete.

Deleting a Subnet Object

- 1 Click DHCP > Subnet Management to open the Subnet Management window in the main panel.
- 2 From the drop-down menu, select Delete Subnet, then click OK to open the Delete Subnet window.
 - ◆ To remove all Subnet objects in the list, click the top-level check box, then click Delete.
 - ◆ To remove one or more Subnet objects, click the check box next to it, then click Delete.

Address Range Management

Use the iManager utility to create and set up Subnet Address Range objects for each pool of addresses you want to be dynamically assigned by DHCP. Optionally, the Address Range object stores the start of a hostname that can be assigned to clients when addresses are assigned.

The Address Range Management role consists of the following tasks:

- ◆ [“Creating a Subnet Address Range Object” on page 119](#)
- ◆ [“Viewing or Modifying a Subnet Address Range Object” on page 120](#)
- ◆ [“Deleting a Subnet Address Range Object” on page 121](#)

Creating a Subnet Address Range Object

- 1 Click DHCP > Address Range Management to open the Address Range Management window in the main panel.
- 2 From the drop-down menu, select Create Address Range, then click OK to open the Create Address Range window.
- 3 Select the subnet where the address range will be created.
- 4 In the Address Range Name field, type the name of the subnet address range.
- 5 Click Add Trustee, then select the subnet address range from the list of address ranges displayed in the Subnet Address Range window.

This automatically fills the Start Address and End Address fields that specify the lower and upper limits of the range.

- 6 Click Create.

A message indicates that the new subnet address range has been created.

Viewing or Modifying a Subnet Address Range Object

- 1** Click DHCP > Address Range Management to open the Address Range Management window in the main panel.
- 2** From the drop-down menu, select View/Modify Address Range, then click OK to open the View/Modify Subnet Address Range window.
- 3** From the Select Subnet drop-down menu, select the subnet that contains the address range you want to modify.
- 4** From the Select Address Range drop-down menu, select the address range to be modified.
- 5** Click OK.

You will be led through a set of steps where you can modify the following address range parameters:

- ◆ Range Type: Indicates the range of addresses used by the DHCP server in response to requests from clients.

From the Select Range Type drop-down menu, select one of the following:

- ◆ Dynamic DHCP: A range of addresses used by the DHCP server to assign addresses to clients making only DHCP requests. If the Dynamic DHCP range type is assigned, the DNS Update Option parameter can be enabled. If Always Update is selected, the DHCP server will update DNS as dynamic addresses are assigned and released.
- ◆ Dynamic BOOTP: A range of addresses used by the DHCP server to assign addresses to clients making only BOOTP requests.
- ◆ Dynamic BOOTP and DHCP: A range of addresses used by the DHCP server to assign addresses to clients making either DHCP or BOOTP requests. If the Dynamic BOOTP and DHCP range type is assigned, the DNS Update Option parameter can be enabled. If Always Update is selected, the DHCP server will update DNS as dynamic addresses are assigned and released.
- ◆ Dynamic DHCP with Automatic Host Name Generation: A range of addresses used by the DHCP server to assign addresses to clients making only DHCP requests. The hostnames for this pool will be generated and specified into the DNS system. These hostnames are provided to clients as a DHCP option. If you select this option, ensure that you create the corresponding IN-ADDR.ARPA zone.
- ◆ Excluded: A range of addresses that is excluded by the DHCP server while assigning IP addresses.

If the Dynamic DHCP with Automatic Host Name Generation range type is assigned, the Auto Host Name Starts With parameter can be set. This parameter appends a unique integer to the hostname, generating a unique hostname for each client.

Additionally, the name of the DHCP Server can be specified by selecting it from the DHCP Server drop-down menu.

- ◆ Comments: You can type your comments about the Subnet Address Range in this box. This parameter is optional.

Deleting a Subnet Address Range Object

- 1 Click DHCP > Address Range Management to open the Address Range Management window in the main panel.
- 2 From the drop-down menu, select Delete Address Range, then click OK to open the Delete Subnet Address Range window.
 - ◆ Select the subnet that contains the address range.
 - ◆ To delete all address ranges in the subnet, click the top-level check box and click Delete.
 - ◆ To delete one or more Address Range objects, click the check box next to it and click Delete.

IP Address Management

Use the iManager utility 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 device or address. Assigning a specific address to a client requires that you 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.

The IP Address Management role consists of the following tasks:

- ◆ [“Creating an IP Address Object” on page 121](#)
- ◆ [“Viewing or Modifying an IP Address Object” on page 122](#)
- ◆ [“Deleting an IP Address Object” on page 123](#)

Creating an IP Address Object

- 1 Click DHCP > IP Address Management to open the IP Address Management window in the main panel.
- 2 From the drop-down menu, select Create IP Address and click OK to open the Create IP Address window.
- 3 From the drop-down menu, select the subnet where the IP address will be created.
- 4 Specify the IP address.
- 5 Select an assignment type for the IP address object.

Assignment types for an IP address object are Dynamic, Manual, and Exclusion. If the IP address is dynamically assigned by the DHCP server, it will be automatically displayed.

Valid types that can be created manually are Manual and Exclusion. A manual assignment type must have either a MAC Type or a Client Identifier in order for the IP address object to be created.

Client Identifier uniquely identifies the client.

MAC Type specifies the MAC address type.

MAC Address specifies the hardware address of the NIC (Network Interface Card).

- 6 Click Create.

A message is displayed indicating that the new IP address object has been created.

Viewing or Modifying an IP Address Object

- 1** Click DHCP > IP Address Management to open the IP Address Management window in the main panel.
- 2** From the drop-down menu, select View/Modify IP Address, then click OK to open the View/Modify IP Address window.
- 3** Select the subnet that contains the IP address you want to modify.
- 4** Select the IP Address.
- 5** Click OK.

You will be led through a set of steps where you can modify the following IP address object parameters:

- ◆ Assignment Type: Specifies Exclusion or Manual IP address assignment types.
 - ◆ Exclusion: Address objects are created to identify IP addresses that should be excluded from DHCP server address assignment. An Excluded assignment type designates that the IP address will not be used.
 - ◆ Manual: Address objects are created to identify an IP address to be assigned to a device. A client identifier or MAC address must be configured for the manual address so that the DHCP server can identify the appropriate client. Manual assignment types specify client identifiers, MAC types, MAC addresses, or hostname parameters
- ◆ Client Identifier: Uniquely identifies the client.
- ◆ MAC Type: Specifies the MAC address type.
 - ◆ 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)
- ◆ MAC Address: Specifies the hardware address of the NIC (Network Interface Card).
- ◆ Host Name: Specifies the name of the host server.
- ◆ Associated eDirectory Object: Use this field to select another object in the eDirectory database to maintain a reference to. For example, identify a user who typically uses the device associated with this address.
- ◆ Comments: You can type comments about the address object in this box. This parameter is optional.
- ◆ Lease Expiration Option: A lease type can be permanent or timed. Permanent leases never expire; the client is assigned an IP address for an indefinite period. Timed leases are defined in days, hours, and minutes. Timed leases expire, unless the client renews the lease.
- ◆ Last Used: Displays when the IP address was last used.

- ◆ Other DHCP Options: Use this to add, delete, update, or specify default DHCP options for a manually assigned address type. Default is used to display DHCP options inherited from global preferences and the Subnet object that the address object is under.

Deleting an IP Address Object

- 1 Click DHCP > IP Address Management to open the IP Address Management window in the main panel.
- 2 From the drop-down menu, select Delete IP Address, then click OK to open the Delete IP Address window.
 - ◆ Select the subnet that contains the IP address.
 - ◆ To remove all IP Address objects in the list, click the top-level check box, then click Delete.
 - ◆ To remove one or more IP Address objects, click the check box next to it, then click Delete.

Using the Java-Based Management Console to Configure DHCP

This section provides information about the following:

- ◆ [“DHCP Prerequisites” on page 123](#)
- ◆ [“Global DHCP Configuration” on page 123](#)
- ◆ [“DHCP Server Management” on page 127](#)
- ◆ [“Subnet Pool Management” on page 130](#)
- ◆ [“Subnet Management” on page 131](#)
- ◆ [“Address Range Management” on page 132](#)
- ◆ [“IP Address Management” on page 133](#)
- ◆ [“Command Line Options” on page 135](#)

DHCP Prerequisites

Complete the following prerequisites before setting up DHCP:

- Load NetWare 6.5 on the selected servers.
- Load the Novell Client™ software delivered with NetWare 6.5 on client computers that will be used to administer DNS and DHCP.
- Install the Management Console on client computers that will be used to administer DNS and DHCP.

Global DHCP Configuration


This section describes the following tasks:

- ◆ [“Viewing or Setting Global DHCP Preferences” on page 124](#)
- ◆ [“Viewing or Setting the Global DHCP Defaults” on page 124](#)
- ◆ [“Configuring DHCP Options” on page 125](#)

- ◆ “Importing a DHCP Configuration” on page 126
- ◆ “Exporting a DHCP Configuration” on page 126

Viewing or Setting Global DHCP Preferences

Use the Management Console to set global DHCP options. Note that setting the global DHCP options is not required to set up DHCP.

- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.


The Global Preferences window is displayed listing the code, option name, and value of any global DHCP options selected. Three other tab pages are available: Exclude Address, Include Address, and DHCP Options Table.

- 3** Click the Global DHCP Options tab, then click Modify.
- 4** The DHCP options you can configure globally are listed in the Available DHCP Options list box. To configure an option:
 - ◆ Select the desired option from the Available DHCP Options list box, then click Add.
 - ◆ Specify the required supporting information as prompted.
- 5** Click OK to close the DHCP Options window.

The global DHCP option you added or configured is displayed in the Global DHCP Options list.


Viewing or Setting the Global DHCP Defaults

To add a hardware address to the Exclude Address list:


- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.
- 3** Click the Exclude Address tab.
- 4** Click Add to open the Add Exclude Hardware Address window.
- 5** From the drop-down menu, select the hardware type of the client and specify the MAC address to be excluded.
- 6** Click OK.

The MAC address is added to the Exclude Hardware Addresses list. This assignment applies to all DHCP servers in the eDirectory tree.

To delete a hardware address from the Exclude Address list:


- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.
- 3** Click the Exclude Address tab.
- 4** Click the MAC address to be deleted from the Exclude Hardware Addresses list.
- 5** Click Delete.

To add a hardware address to the Include Address list:

- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.
- 3** Click the Include Address tab.
- 4** Click Add to open the Add Include Hardware Address window.
- 5** From the drop-down menu, select the hardware type of the client and specify the MAC address to be excluded.
- 6** Click OK.

The MAC address is added to the Include Hardware Addresses list. This assignment applies to all DHCP servers in the eDirectory tree.


To delete a hardware address from the Include Address list:

- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.
- 3** Click the Include Address tab.
- 4** Click the MAC address to be deleted from the Include Hardware Addresses.
- 5** Click Delete.


Configuring DHCP Options

The DHCP Options Table provides a list of parameters that can be defined for use on the network. After an option is defined, you can assign a value to the option using Global DHCP Options.


To view a DHCP option:

- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.
- 3** Click the DHCP Options Table tab.
A list of both the system-defined and user-defined DHCP options is displayed.
- 4** Click OK.

To add a DHCP option:

- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.
- 3** Click the DHCP Options Table tab.
A list of both the system-defined and user-defined DHCP options is displayed.
- 4** Click Add to open the Define New DHCP Option window.
- 5** Select the DHCP option code, select the data syntax, add the description of the new option, then click OK.

To delete a DHCP option:

- 1** Click the DHCP Service tab of the Management Console.
- 2** Click Global Preferences  on the toolbar.

- 3 Click the DHCP Options Table tab.

A list of both the system-defined and user-defined DHCP options is displayed.

- 4 Select the option code, then click Delete.

Importing a DHCP Configuration

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

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

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

- 4 Specify the drive and path to the DHCP database file, or use the browse button to navigate 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, then click Add, or click AddAll to import all subnets on the list.

- 7 Select the Subnet Context, then 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.

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

- 10 Use the browse button to select the target server, then click OK.

Exporting a DHCP Configuration

You can use the Management Console to export DHCP configuration information. You can also import the file back into the eDirectory database by using the Management Console.

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

The Export-DHCP window is displayed, requesting the filename.

- 4 Specify the drive and path for the DHCP database file, or use the browse button to navigate to the file.

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

- 5 Click Next.

The Export 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** Click Export.
The Export Status window is displayed, indicating the status.
- 8** Click Finish.

DHCP Server Management

This section describes the following tasks:


- ◆ [“Creating a DHCP Server” on page 127](#)
- ◆ [“Viewing or Modifying a DHCP Server” on page 127](#)
- ◆ [“Deleting a DHCP Server” on page 128](#)
- ◆ [“Starting or Stopping a DHCP Server” on page 128](#)
- ◆ [“Configuring DHCP Auditing” on page 128](#)
- ◆ [“Viewing or Saving the DHCP Audit Trail Log” on page 129](#)
- ◆ [“Viewing or Saving the DHCP Event Log” on page 129](#)

Creating a DHCP Server

Use the 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:

- 1** Click the DHCP Service tab of the Management Console.
The Our Network object is the only object displayed on the Management Console’s left pane.
- 2** Click Create  on the toolbar.
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, then 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 Management Console.

Viewing or Modifying a DHCP Server

On the Server tab page, you can view the Subnet Address Ranges Serviced by this Server and Subnets Serviced by this Server. You can also type comments (up to 256 characters) about the server in the comments field. (Refer to [“Creating a DHCP Server” on page 127](#) 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 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. Use this option to have the server ping an address before the address is assigned to a device. This ensures that the address is not already in use. Note that pinging the address also increases network traffic.

Deleting a DHCP Server

- 1** Select the DHCP Server from the lower pane of the Management Console.
- 2** Click Delete  on the toolbar.

Starting or Stopping a DHCP Server

The existing DHCP Server object is displayed in the lower pane of the Management Console.

- 1** Select the DHCP Server from the lower pane of the Management Console.
- 2** Click Start/Stop Service  on the toolbar.
- 3** Depending on the state of the DHCP Server module, one of the following is displayed:
 - ◆ Failure notification message: This appears if the DHCP Server module (dhcpsrvr.nlm) is not loaded. In order to start the server, load the DHCP Server module through the system console.
 - ◆ Start button: If the DHCP Server module is loaded but is in Stop mode, click the button to start the DHCP server.
 - ◆ Stop button: If the DHCP Server module is loaded but is in Start mode, click the button to stop the DHCP server.


NOTE: To use the Start/Stop DHCP service, dhcpsrvr.nlm must be loaded.

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:

- 1** Log in to the tree containing the service you want to begin auditing, launch the Management Console, then click the DHCP Service tab.
- 2** Select the desired server to perform the auditing, then 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 toolbar.

Viewing or Saving the DHCP Audit Trail Log

To view the audit trail log, csatpxy.nlm must be running on the server.

- 1** Log in to the desired tree, launch the Management Console, then click the DHCP Service tab.
- 2** Select the server that has been configured to perform auditing, then click View Audit Trail  on the toolbar.

The Events Period-Audit Trail Log dialog box displays the start and end 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 one or more specific lease types.

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

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

Viewing or Saving the DHCP Event Log

To view the event log, csatpxy.nlm must be running on the server.

- 1** Log in to the desired tree, launch the Management Console, then click the DHCP Service tab.
- 2** Select the server that has been configured to perform event logging, then click View Events/ Alerts  on the toolbar.

The Events Period-Events Log dialog box displays the start and end 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 specific event's severity and state.

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

Subnet Pool Management

This section describes the following tasks:


- ◆ “Creating a Subnet Pool Object” on page 130
- ◆ “Viewing or Modifying a Subnet Pool Object” on page 130
- ◆ “Deleting a Subnet Pool Object” on page 130

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:


- 1 Click Create  on the toolbar.
- 2 Select Subnet Pool, then click OK.
- 3 Specify a unique name for the Subnet Pool object.
- 4 Use the browse button to select the eDirectory context where the Subnet Pool object will be created.

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

Viewing or 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 eDirectory distinguished name is updated in the Subnet object's Subnet Pool List attribute.

Deleting a Subnet Pool Object

- 1 Click the DHCP Service tab of the Management Console.
- 2 Select the Subnet Pool Object you want to delete.
- 3 Click Delete  on the toolbar.

Subnet Management

This section describes the following tasks:

- ◆ [“Creating a Subnet Object” on page 131](#)
- ◆ [“Viewing or Modifying a Subnet Object” on page 131](#)
- ◆ [“Deleting a Subnet Object” on page 132](#)

Creating a Subnet Object

Use the Management Console to create and set up a DHCP Subnet object for each subnets where you will assign addresses.

- 1 Click the DHCP Service tab of the Management Console.

The Our Network object is the only object displayed on the Management Console’s left pane.

- 2 Click Create  on the toolbar.

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

- 3 Select Subnet, then click OK.

The Create Subnet dialog box is displayed. For each subnet you create, type the following information in the fields provided: subnet name, eDirectory context, subnet address, and subnet mask. If you have set up 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 information, including DHCP options specific to each subnet.

- 4 Provide the required information, then click Create.

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

Viewing or Modifying a Subnet Object

After a Subnet object has been created, you can use the Management Console to display three tab pages of detailed information about the Subnet object, Address, Subnet Options, and Other DHCP Options. (For information about creating a Subnet object, refer to [“Creating a Subnet Object” on page 131.](#))

Addressing tab page

This page displays Subnet Address, Mask, and Type attributes from information provided when the object was created. If you need to make changes to these attributes, you must delete the Subnet object and re-create it.

If you plan to use Dynamic DNS, this is 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 type up to 256 characters of information in the Comments field.

Subnet Options tab page

You can configure lease types. 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.

Other DHCP Options tab page

The DHCP options can be configured from this 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 can add DHCP options from the Available DHCP Options list.


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

IP Address Utilization tab page

This page provides the details about the usage of IP addresses in a subnet such as the Total IP Addresses, the Utilized IP Addresses, the Available IP Addresses, the Excluded IP Addresses, and the Percentage Utilization.

Click Get Details to view the IP address utilization details of the subnet.

Deleting a Subnet Object

- 1 Click the DHCP Service tab of the Management Console.
- 2 Select the Subnet Object you want to delete.
- 3 Click Delete  on the toolbar.

Address Range Management

This section describes the following tasks:

- ◆ [“Creating a Subnet Address Range Object” on page 132](#)
- ◆ [“Viewing or Modifying a Subnet Address Range Object” on page 133](#)
- ◆ [“Deleting a Subnet Address Range Object” on page 133](#)

Creating a Subnet Address Range Object

Use the 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:

- 1 Click the DHCP Service tab of the Management Console.
- 2 Select the Subnet object where 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, then click OK.

The Create New Subnet Address Range dialog box is displayed.

- 4 Specify a name for the Subnet Address Range, specify the starting and ending address of the range, 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.

Viewing or Modifying a Subnet Address Range Object

- 1 Select the object you want to modify.

This will display the objects in the left pane of the DHCP Service window.

- 2 Click the Subnet Address Range object.

This will display its detailed information in the right pane.


- 3 You can modify the following range type options:

- ◆ 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.

Refer to [“Creating a Subnet Address Range Object” on page 132](#) for information about creating a Subnet Address Range object.

Deleting a Subnet Address Range Object

- 1 Click the DHCP Service tab of the Management Console.
- 2 Select the Subnet Address Range you want to delete.
- 3 Click Delete  on the toolbar.

IP Address Management

This section describes the following tasks:


- ◆ [“Creating an IP Address Object” on page 133](#)
- ◆ [“Viewing or Modifying an IP Address Object” on page 134](#)
- ◆ [“Deleting an IP Address Object” on page 135](#)

Creating an IP Address Object

You use the 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 that you 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:

- 1 Click the DHCP Service tab of the Management Console.
- 2 Select the Subnet object of the target IP address, then click Create  on the toolbar.

The Create New DHCP Object dialog box is displayed.

- 3 Select IP address, then click OK.

The Create IP Address dialog box is displayed.

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

If you select 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.

Viewing or Modifying an IP Address Object

After an IP address object has been created, its detailed information window displays three tab pages: Address, Usage, and Other DHCP Options. (Refer to [“Creating an IP Address Object” on page 133](#) for information about creating IP address objects.)

Address tab page

On this 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 type the IP address's MAC address, hostname, and DNS domain suffix, and identify an eDirectory object to use a specific IP address on this page.


Usage tab page

This 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.

Other DHCP Options tab page

DHCP options can be configured from this page. Any options that are set for this IP address object are displayed here. You can set additional DHCP options by clicking Modify.

Deleting an IP Address Object

- 1 Click the DHCP Service tab of the Management Console.
- 2 Select the IP Address Object you want to delete.
- 3 Click Delete  on the toolbar.

Command Line Options

See [“Command Line Options” on page 99](#) for information.

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 you can modify an existing subnet can be modified.

To configure multiple logical networks or VLANs:

- 1 Create a Subnet Pool object.
For more information see [“Creating a Forward Zone Object” on page 83](#).
- 2 Select a Subnet object or create and configure a new Subnet object.
- 3 Click Subnet Pool Management > Modify Subnet Pool, then add the subnet to the subnet pool where you want to associate the subnet object.
- 4 Click OK.
- 5 Repeat Steps 2 through 4 for each subnet you want to associate with the Subnet Pool object.

Loading the DHCP Server

- 1 Create a DHCP Server object.
For more information, see [“Creating a DHCP Server” on page 112](#).
- 2 Create a Subnet object, then assign a default DHCP server to it.
For more information, see [“Creating a Subnet Object” on page 117](#).
- 3 Specify 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. After creating the DHCP server object, you can edit the `autoexec.ncf` file to uncomment the `dhcpsrvr.nlm` load statement. This will enable you to avoid the manual loading of the `dhcpsrvr.nlm` every time you restart NetWare. For information about other command line options, see [“DHCP SRVR Command Line Options” on page 136](#).

After `dhcpsrvr.nlm` is loaded, you can use the iManager utility to start and stop the DHCP Server. For more information on starting and stopping the DHCP server, see [“Starting or Stopping a DHCP Server” on page 113](#).

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 the server to read from and write to the master replica |

Monitoring 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. See [“DHCP Options” on page 38](#) for information about available DHCP and BOOTP options.

Events and Alerts

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

You can configure 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.

See [“Viewing the DHCP Event Log” on page 115](#) for more information about viewing and saving the DHCP event logs using the iManager utility.

See [“Viewing or Saving the DHCP Event Log” on page 129](#) for more information about viewing and saving the DHCP event logs using the Java-based Management Console.

Auditing Server Activity

The audit trail log records a history of activity logged by DHCP servers. You can use the audit trail log to diagnose network trends. 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 were in use when pinged.

See [“Configuring DHCP Auditing” on page 114](#) for information about configuring DHCP auditing using the iManager utility.

See [“Configuring DHCP Auditing” on page 128](#) for information about configuring DHCP auditing using the Java-based Management Console.

DHCP SNMP Events

Following are examples of DHCP SNMP events logged/trapped for SNMP event generation and the severity level that can be associated with them.

Minor events

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

Warning events

- ♦ An eDirectory update to the subnet failed, causing degraded operation (incomplete transactions are logged to a local file named `dhcpllog.log`).
- ♦ SNMP recovered from an internal fault and the error code was logged.
- ♦ A subnet was not configured and addresses are not available, causing degraded operation.

Major events

When the `dhcpsrvr.nlm` is loaded and the server is operational and ready for LAN-based clients, the following events are logged or trapped for SNMP event generation:

- ♦ Found unknown subnets with prior records.
- ♦ The eDirectory objects are not synchronized.
- ♦ A DNS update for adding a resource record is dropped.
- ♦ A DNS update for deleting a resource record is dropped.
- ♦ An unknown zone with resource records have been found.

Critical events

- ♦ The logger fails to open the recovery log file or is having difficulty in opening it (the server is inoperative).
- ♦ The main thread fails to process the lease expiration (the server is inoperative).
- ♦ The server detects a configuration change in the directory.

6

Troubleshooting

This section contains information for troubleshooting common problems you might encounter using DNS and DHCP.

- ◆ “DNS” on page 139
- ◆ “DHCP” on page 154
- ◆ “Console and Debug Logs” on page 157

DNS

This section provides the following troubleshooting information for DNS:

- ◆ “Troubleshooting Checkpoints” on page 139
- ◆ “Common Installation and Upgrade Problems” on page 140
- ◆ “Common Configuration Problems” on page 141
- ◆ “Common Operational Problems” on page 145
- ◆ “Troubleshooting Windows 95 TCP/IP Problems” on page 149
- ◆ “Using the -F Command Line Option for Dnipinst.nlm” on page 153
- ◆ “Server Access to DNS/DHCP Locator Object Not Required” on page 153

Troubleshooting Checkpoints

If you experience problems related to DNS or TCP/IP, try the following:

- ◆ Run the WINIPCFG utility (Windows 95/98) or enter **ipconfig** at the command prompt (Windows NT, 2000, XP) 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 exist:

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

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

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

- ◆ 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 configured incorrectly.

- ◆ 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.

- ◆ 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.

In addition to using ping to troubleshoot DNS configuration problems, you can also use the nslookup utility at your server. For information on using this utility, see “Nslookup” in the *NetWare 6.5 Utilities Reference*.

Common Installation and Upgrade Problems

The following problems could occur during an installation or upgrade:

The installation for DNS/DHCP services completed with one of the following error messages:

The DNS master file RootSrvr.dat is invalid. The RootSrvrInfo zone object will be created with default values for the root servers' information.

The DNS master file RootSrvr.dat could not be found. The RootSrvrInfo zone object will be created with default values for the root server's information.

Cause: The RootSrvr.dat file, which is copied to the sys:\etc\dns directory during the installation, is corrupted or missing. This data file contains information about the DNS root servers and is required to populate the root server's information in the RootSrvrInfo zone object.

Solution: If the installation program cannot find or use this file, it creates the required zone object with default values. The installation process uses the default values for the DNS root servers. The contents of RootSrvrInfo zone object should be compared with the most recent information on the root server. Changes to this information can be made in the RootSrvrInfo zone object using the DNS/DHCP management utilities.

The installation for the DNS/DHCP services completed with one of the following error messages:

The preferences data file NDDPrefs.dat is invalid. The Locator object will be created with default values for the configuration preferences.

The preferences data file NDDPrefs.dat could not be found. The Locator object will be created with default values for the configuration preferences.

Cause: The data file NDDPrefs.dat, which is copied to the sys:\system\ directory during the installation, is corrupted or is missing. This data file contains information for global configuration preferences. Currently, only the DHCP global options are configured using this data file.

Solution: If the installation program is unable to find or use this file, it creates the Locator object with default values for these options. This information can be edited using the management utilities. In the Management Console, edit this option by selecting DHCP Service > Global Preferences. This page allows you to delete and modify the existing DHCP options and to add new DHCP options.

In the iManager utility, edit these options by clicking DHCP under Roles and Tasks. Then click Global DHCP Configuration > View/Set Global Preferences from the drop-down list and click OK. The Global DHCP Options, DHCP Options, and DHCP Options Table pages allow you to delete and modify the existing DHCP options and to add new DHCP options.

After you upgrade to NetWare 6.5, the DNS Server does not come up when you load the DNS Server with the ncf file

Cause: While upgrading to NetWare 6.5, if you have the command load named in the existing autoexec.ncf file, with any option that is not supported by NetWare 6.5, the DNS Server will not load automatically when the autoexec.ncf is executed after upgradation.

If you have an unsupported option in the autoexec.ncf file, the usage details will be displayed on the logger screen.

Solution: In order to avoid this, before upgrading to NetWare 6.5, ensure that the autoexec.ncf file does not contain the -m, -u, -l, -r, -f, -a, -b, -pc, -strict [on|off], -s, -v, -q options. For information on DNS server option, see [“NAMED Command Line Options” on page 102](#).

Common Configuration Problems

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

- ◆ Check the consistency of glue records that are shared between parent and child zones. Make sure that the name server (NS) and Address (A) records within the parent zone match those in the child zone.
- ◆ Update the IP addresses of the root name servers configured in the RootServerInfo zone. Changes to this information are not automatically propagated through a domain; you must update them manually. The most recent update of root name server information is available through FTP at <ftp://rs.internic.net/domain/named.root>.
- ◆ Check the consistency between pointer records in the IN-ADDR.ARPA domain and other domains.
- ◆ If you change the IP address of a name server, ensure that the parent zone reflects that change.
- ◆ Verify that you have configured a name server to correctly service every zone.
- ◆ Verify that the zone transfers are occurring properly. Ensure that the secondary name server can identify the primary name server.
- ◆ If you cannot access a particular host, verify that the PTR records exist. When you create a zone, always select Yes when prompted to create a companion zone. If you have created a companion zone, verify that the IP address and hostname are correct.

Merging DNS-DHCP Services

You can use the DSmerge utility to merge two trees into a single tree. However, the merged tree will continue to have two DNS/DHCP setups represented by two sets of DNS-DHCP base objects.

Each DNS-DHCP setup contains the following base objects:

- ◆ **RootServerInfo:** contains information about all top-level domains.
- ◆ **Locator:** contains lists of all the DNS and DHCP servers, zones (including RootServerInfo), subnets, and subnet pools, as well as the global definitions and configuration for the DHCP server.
- ◆ **Group:** enables the DNS and DHCP servers to read/write data from/to eDirectory. All DNS-DHCP objects have this Group object assigned as a trustee. The NCP server hosting the DNS or DHCP Services has a membership to the Group object.

A proper DNS-DHCP setup should have exactly one instance for each of the base objects.

You can use ConsoleOne or iManager to merge the DNS-DHCP Services. If you choose to use iManager, complete the following steps:

- 1** From the Roles and Tasks menu, select eDirectory Administration.
- 2** Identify the set of final base objects (RootServerInfo, Locator, and Group objects) that are to be retained.

Tip: Retain the RootServerInfo that has latest information about the top-level domains. Retain the Locator object that has references to larger number of zones and subnets. Also, retain the Group object that is referenced by this Locator.

When you first select the final Locator object, it will contain lists of references to some of the DNS-DHCP objects. The remaining DNS-DHCP objects are being referenced by the other locator object.

- 3** Copy the remaining references into the corresponding lists of the final Locator object.
 - 3a** Copy the DNS Server references from the DNIP:DNSServers attribute of the other Locator object to the DNIP:DNSServers attribute of the final Locator object.
 - 3b** Copy the DHCP Server references from the DNIP:DHCPServers attribute of the other Locator object to the DNIP:DHCPServers attribute of the final Locator object.
 - 3c** Copy the Zone object references from the DNIP:DNSZone attribute of the other Locator object to the DNIP:DNSZone attribute of the final Locator object.
 - 3d** Copy the Subnet object references from the DNIP:Subnet Attr attribute of the other Locator object to the DNIP:Subnet Attr attribute of the final Locator object.
 - 3e** Copy the Subnet Pool object references from the DNIP:Subnet Pool List attribute of the other Locator object to the DNIP:Subnet Pool List attribute of the final Locator object.
- 4** For all DNS Servers, DHCP Servers, and Subnet Pool objects whose references were copied in **Step 3a**, **Step 3b**, and **Step 3e**, assign the final Group object as a trustee with the following rights:
 - ◆ All Attributes Rights: Supervisor
 - ◆ Entry Rights: Browse, Delete

- 5** For all DNS Zones and Subnet objects whose references were copied in **Step 3c** and **Step 3d**, assign the final Group object as a trustee with the following rights:
 - ◆ All Attributes Rights: Supervisor rights that can be inherited
 - ◆ Entry Rights: Browse, Create, and Delete rights that can be inherited
- 6** For the final Locator object, assign the final Group object as a trustee with the following rights:
 - ◆ All Attributes Rights: Supervisor
 - ◆ Entry Rights: Browse
- 7** For the final RootServerInfo object, assign the final Group object as a trustee with the following rights:
 - ◆ All Attributes Rights: Supervisor rights that can be inherited
 - ◆ Entry Rights: Browse rights that can be inherited
- 8** For all NCP Servers that have a reference to the other Locator object, you must change the reference to the final Locator object.
- 9** In the final Locator object, set the desired Global Preferences in the following attributes:
 - ◆ DNIP:Included MAC
 - ◆ DNIP:Excluded MAC
 - ◆ DNIP:Config Options
 - ◆ DNIP:CfgPreferences (this is required to be merged only if there are any user-defined options)
- 10** Delete the base objects that are not part of the final set of base objects identified in **Step 2**.

Potential Issues

- ◆ If subnets corresponding to private IP addresses exist and there is an overlap among such subnets across the trees, the administrator must decide how to merge these subnets.
- ◆ In case both the Locator objects have some user-defined DHCP options with the same option codes, and these options are configured at the Locator/Subnet/IP Address level, the administrator must make sure that the interpretation of these options do not change even after the merge.

DNS/DHCP iManager Utility

The following configuration problems might occur while using the DNS/DHCP iManager utility:

- ◆ If you encounter the `Cannot access the LDAP server` error while configuring the Novell exteNd Director™ 4.1 Standard Edition by typing `http://server ip address/nps/servlet/configure` on the browser, ensure that the LDAP server is running. Also, set the `ldapTLSRequired` option to `false`.
- ◆ If you encounter the `HTTP Status 500 - Server Internal Error` error towards the end of configuring exteNd Director 4.1 Standard Edition, stop Tomcat and Apache by typing `tc4stop` and `ap2webdn` at the server console. Restart Tomcat and Apache by typing `tomcat4` and `ap2webup` at the server console. Access iManager 2.0 by typing `http://serveripaddress:8080/nps/index.html` on the browser and click the iManager link on the top of the page.

Common Operational Problems

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

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 DNS based on Novell eDirectory 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 DNS based on eDirectory. If the primary server is not eDirectory based, you might need to change the serial number manually in order for the secondary server to recognize that a change has occurred.

DHCP updates from a Novell DHCP server fails

Cause: The receiving DNS server is not a Designated Primary for the reverse/forward zones.

Solution: For dynamic updates from Novell DHCP servers, the targeted forward zone and its corresponding reverse zone should be serviced by the same DNS server in Designated Primary mode. This is to ensure that the DNS server is authoritative for both the forward and the reverse zones.

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 additional information, refer to RFCs 1537 and 1713.

Cause 2: The host is down or is unreachable.

Solution 2: Use the ping utility 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.

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 specify the IP address when prompted. Verify that all parent zones have the same address information.

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.

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: Specify the correct domain name or name server address in the host's `resolv.cfg` file (or equivalent).

Hosts cannot access an entire external domain.

Cause 1: The root name server information is invalid; therefore, the root servers are unreachable. For non-eDirectory 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://rs.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 eDirectory.

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 eDirectory.

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 the ping utility 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 the ping utility 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.

A Resource Record object change is not reflected in the server cache and the zone transfer fails.

Cause 1: The Zone SOA serial number is not automatically updated after the change is made.

Solution 1: After you modify the Resource Record, change the Zone SOA serial number manually.

Cause 2: The server cache is not automatically refreshed after changes are made.

Solution 2: Unload the `named.nlm` module and reload it to refresh the DNS server settings.

The client is not assigned an IP address.

Cause: The DHCP server object is not properly configured.

Solution: Make sure you have created the DHCP server object, at least one Subnet object and Subnet Address Range object each. Verify that when you load the DHCP server module, `dhcpsrvr.nlm`, a message from the NetWare[®] system console indicates that the IP database is loaded

Problem in dynamic reconfiguration of DNS server (DNIP:DNS server object configuration changes in eDirectory, add/remove zones (update zone data out-of-band) in eDirectory does not get updated to the server in-memory)

Cause 1: Frequently changing the server roles to passive primary from designated secondary.

Solution 1: Do not change the server roles to passive primary from designated secondary when the server is running. Although the server will be able to recognize the changes in roles, there are some issues in synchronizing these roles.

Cause 2: The dynamic reconfiguration interval is not set properly.

Solution 2: Make sure that the dynamic reconfiguration interval is not set too high (20-24 hours) because this slows down the synchronizing mechanism. Also, setting this interval very low (less than 10 minutes) slows down the DNS query/update/transfer mechanism. The recommended value for this option is 15 minutes. The dynamic reconfiguration interval can be set through the management utilities.

Dynamic update request (2136) sent from non-Novell DHCP server failed

Cause: The value for the update filter is not set properly.

Solution: Set the ACL value of the update filter to the IP address of the DHCP server, or set the value to any. The value is set to none by default and all dynamic updates are refused by the DNS server. This can be set through the management utilities.

Dynamic Update (Novell proprietary update) sent from Novell DHCP servers failed

Cause: Reverse (IN-ADDR.ARPA) zone does not exist for the corresponding forward zone update.

Solution: Verify that the reverse (IN-ADDR.ARPA) zone exists for the corresponding forward zone update. The logic for Novell proprietary update is to first create/update the data (PTR resource record) in the reverse zone and then create the corresponding A record in the forward zone. If the reverse zone does not exist, the response will be negative for a dynamic update request.

Zone-out fails — Ten A type resource records are created in the abc.xyz.com zone hosted by a Novell primary DNS server (DNS server version 6.0 and above). The user waited for the time specified in the Novell Dynamic Reconfiguration option. The query

to a Novell secondary server (prior versions DNS servers 6.0) for the newly created resource records is unsuccessful.

Cause: The notify and transfer-format values are not set properly.

Solution: Ensure that the value for the notify option is set to Yes and the value for the transfer-format option is set to one-answer in the primary server (older versions of DNS servers support only one-answer format of zone transfer).

Server does not listen to any incoming requests

Cause 1: The address list in the query filter option is not configured properly.

Solution 1: Ensure that this attribute is configured properly in the DNS server and the DNS zone (the value specified in the DNS zone overrides the value specified in the DNS server). If this attribute is not set with any value, the default behavior of the server is to allow queries from all hosts. Ensure that the address of the specific client (the client who has requested the server) is set explicitly that the address falls in an address range as specified in this attribute, or that the attribute value is set to any.

Cause 2: Query from this client (from which the request came) is considered bogus.

Solution 2: Ensure that the address of this client (from which the request came) is not listed in the Blacklist server attribute.

DNS server exits while loading

Cause: The DNS server is not registered with a valid IP address and port.

Solution: Make sure that the IP address and port combination allocated for the DNS server does not conflict with any other services running on the NetWare server.

DNS server exits in clustered environment

Cause: ncssdk.nlm is not loaded on the NetWare server (this NLM™ provides all of the required APIs for cluster support).

Solution: Load the ncssdk.nlm by typing **NCSSDK** at the server console.

Error in creating, modifying, or deleting DNS-DHCP objects through the iManager utility for the first time (after exteNd Director 4.1 Standard Edition configuration)

Cause: The DNS-DHCP schema, DNS-DHCP base objects (Locator, DNS-DHCP Group, RootServerZone Info) does not exist in eDirectory.

Solution: Extend the DNS-DHCP schema and create the base objects in eDirectory by typing **DNIPINST** at the server console.

Novell Border Manager error when performing any DNS/DHCP operation using the iManager utility

Cause: Memory intensive operations such as deleting a large zone, deleting large number (1000 or more) of zones at the same time, or deleting 1,000,000 or more resource records at the same time.

Solution: Wait for a period of time to let these long operations complete. Use the ndstrace utility to track these operations. If no changes occur, click the Refresh button on the browser.

Disordered pages in DNS/DHCP iManager utility

Cause: The display settings or resolution are not correct on the client's machine.

Solution: The typical screen resolution for running the DNS/DHCP iManager utility is 1024 x 768 or more.

DNS/DHCP java-based console does not come up

Cause: The display settings or resolution are not correct on the client's machine.

Solution: The minimum screen resolution for running the DNS/DHCP java-based console is 600 x 800 with at least 256 colors.

Error Messages with error codes 35082, 35088, 35323 and 35087

Cause: The reason could be eDirectory errors. For instance Remote eDirectory could be down, while DNS Server tries to get zone data.

Solution: No action is required. DNS Server will automatically recover after eDirectory access is restored.

Malformed Transaction messages on the server

Cause: This error is caused due to heavy load during zone in. The error message is displayed on designated secondary server.

Solution: This error message can be ignored as it's only an information and server continues to function normally.

Example: 'error: malformed transaction: testzone.db.jnl last serial 20030412127 != transaction first serial 20030412192'. This error message can be ignored.

Troubleshooting Windows 95 TCP/IP Problems

This section provides information about 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, type **wipcfg**, then 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, go to the command prompt and 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 are using 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 exist:

- ◆ The DNS server or DNS domain name is not configured properly on the client.
- ◆ If using DHCP, the DNS server and 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
```

The following table explains the use of the 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 |

NOTE: You can find unauthorized addresses in an exported DHCP configuration by searching for IP Address objects with an Assignment Type value of 32. Use the Find feature in a text editor to quickly identify addresses that have been marked as unauthorized.

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, go to a command prompt and 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
```

The following table explains the use of the Tracert options.

| Option | Meaning |
|-----------------|---|
| -d | Do not resolve addresses to hostnames |
| -h maximum_hops | Maximum number of hops to search for target |

| Option | Meaning |
|--------------|--|
| -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]
```

The following table explains the use of the 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. |
| -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]
```

The following table explains the use of the Netstat options.

| Option | Meaning |
|----------|--|
| -a | Displays all connections and listening ports, but not those on the server. |
| -e | Displays ethernet statistics. This might be combined with the <code>-s</code> 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 <code>-s</code> option to display per protocol statistics, proto can be TCP, UDP, or IP. |
| -r | Displays the contents of the routing table. |
| -s | Displays per protocol statistics. By default, statistics are shown for TCP, UDP, and IP. The <code>-p</code> 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 this option is 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.

Using the -F Command Line Option for Dnipinst.nlm

The `dnipinst.nlm` program is a backup method of extending the schema and creating the DNS/DHCP Locator and Group objects and the `RootSrvrInfo` zone. `Dnipinst.nlm` can be used if problems occurred during the NetWare 6.5 installation process. Most administrators will not need to use this NLM program.

You can use the `-F` command line option in the `dnipinst.nlm` to re-create the DNS/DHCP configuration objects if the initial attempt to set up Novell DNS/DHCP Services fails during the configuration object creation stage.

When a failure occurs during the object creation phase, we recommend that you delete the DNS-DHCP (DNS/DHCP Locator), `DNSDHCP-GROUP` (DNS/DHCP Group), and the `RootSrvrInfo` objects (if they have been created), then use `dnipinst.nlm` with the `-F` flag. When the `-F` command line option is specified, an initial console message confirms the action and the eDirectory login window appears. After a successful login, the object eDirectory context query window is displayed. You can enter the data and create the objects. If a schema extension error occurs, execute `dnipinst.nlm` in the regular mode.

Server Access to DNS/DHCP Locator Object Not Required

The requirement that the DNS and DHCP servers always have access to the DNS/DHCP Locator object has been relaxed.

The first time the server loads, it requires access to the DNS/DHCP Locator object to obtain a copy of any global configuration from the object. The DHCP server saves a copy of the global configuration in `sys:\etc\dhcp\dhcploc.tab`.

In subsequent loads, the DHCP server will try to obtain the global configuration information from the DNS/DHCP Locator object. If the information is not available, the DHCP server will read the information from the last saved copy of SYS:\ETC\DHCP\DHCPLOC.TAB. Each time the DHCP server loads and the DNS/DHCP Locator object is available, the DHCP server updates the dhcploc.tab file.

The DNS server also does not require access to the DNS/DHCP Locator object. It has been enhanced to require access to the DNS/DHCP Locator object only if the named command line arguments are specified to create zones in eDirectory. The DNS server no longer requires access to the RootSrvrInfo zone stored in eDirectory. The DNS server now first tries to find the RootSrvrInfo zone in eDirectory, but if it is not available, the DNS server uses the copy of the information found in sys:\etc\dns\rootsrvr.dat.

DHCP

This section provides the following troubleshooting information for DHCP:

- ◆ “[Troubleshooting Checkpoints](#)” on page 154
- ◆ “[Common Operational Problems](#)” on page 155
- ◆ “[Releasing and Renewing DHCP Addresses](#)” on page 157

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 dhcpupd.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 client's 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 eDirectory 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 information describes the most common operational errors.

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.

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.

Using mobile clients causes fewer leases to be available.

Cause 1: The mobile client's 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: Do one of the following:

- ◆ 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 eDirectory 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.

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 the parameters assigned by DHCP are properly configured.

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.

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.

Dhcpserver.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 1: 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.

Dhcpserver.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 eDirectory 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, use the iManager utility to ensure that each local subnet is properly configured.

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 using a laptop computer in different locations on a given network.

Windows 95

To manually release and renew a DHCP-assigned IP address in Windows 95:

- 1** Select Start > Run.
- 2** Type **wiipcfg** 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:

- 1** Select Start > Programs > MS-DOS Command Prompt.
- 2** From the command prompt, execute the command
ipconfig /release
A message is displayed indicating that the assigned IP address has been successfully released.
- 3** From the command prompt, execute the command
ipconfig /renew
A message is displayed indicating the new IP address that has been assigned.
- 4** From the command prompt, execute the following command to review DHCP settings:
ipconfig /all

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 NetWare Alert 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 `dhcprsvr.log` file (in ASCII text) in the server's `\etc\dhcp` directory. When loading `dhcprsvr`, 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 |
|------------------|--|
| <code>-d1</code> | Turns on a background screen log of DHCP packets. |
| <code>-d2</code> | Turns on a background screen log of debug statements and DHCP packets. |
| <code>-d3</code> | Turns on a background screen log of debug statements and DHCP packets and writes the log to the server's <code>\etc\dhcp\dhcprsvr.log</code> file. |

7

DNS/DHCP Advanced Features

This section describes how to configure the ICE zone handler and using the cluster support of Novell® DNS/DHCP Services.

- ◆ “DNS/DHCP Advanced Features” on page 159
- ◆ “Cluster Support” on page 163
- ◆ “DNS/DHCP Advanced Features” on page 159

Configuring the ICE Zone Handler

This section provides information about configuring the ICE zone handler.

- ◆ “Modifying the ice.cfg File” on page 159
- ◆ “Importing Configuration and Script Files” on page 160
- ◆ “Exporting Configuration and Script Information” on page 162

Modifying the ice.cfg File

The source and destination handlers available to the application, with other information such as the version of the handlers and the modes in which they operate must be provided in the ice.cfg file in the sys:\system directory. You modify the ice.cfg file by appending the zone handler information.

```
[Zone]
```

```
Version 1.0
```

```
Mode: FromFile, FromServer, ToFile
```

```
Module name: zone
```

```
Flags: 1
```

The mode is used to convey the information about the functionality supported by the handler. In the example above, the mode is FromFile, FromServer, ToFile because zone handler can read from the file, read from the server, and write to the file.

The LDAP handler is used to write to the directory. Ensure ice.cfg also contains the following:

```
[LDAP]
```

```
Version: 1.0
```

```
Mode: FromServer, ToServer
```

```
Module Name: ldaphdlr
```

```
Flags: 1
```

The module name specifies the handler name. Flags specifies the flags that should be sent to the destination handler. Currently, the only flag available is for LBURP.

Enabling Clear-Text Passwords

Clear-text passwords should be enabled in the LDAP group object to avoid LDAP bind operation failure. You can do this using ConsoleOne®.

Importing Configuration and Script Files

Using the ICE zone handler, the named.con file, along with the corresponding zone master files can be migrated to Novell® eDirectory™, or a script file can be formed in a particular format. This script file is used to migrate the zone master files of the desired zones, without changing the server and zone configuration information.

The import operation generates an output script file that indicates the status of zone import with a token “done:” at the beginning of zones imported successfully. If an import fails for a particular zone, the corresponding output script file generated will not have a “done:” tag for that particular zone and the script file can be reused to import the failed zone later.

Command Line Parameters for ICE Zone Import

You can access online help for the command line parameters for zone handlers by typing **ice -h zone** at the system console of the NetWare® server.

Zone Source Handler Parameter: ice -S ZONE -f <input file> [-t scr | conf] -x <zone context> -b <DNS server DN> [-l <log file name>] [-r] [-s <LDAP server name>] [-p <port no>] [-d <bind dn>] [-w <password>] -D {Destination Handler with options ...}

| Options | Descriptions |
|--------------------|---|
| -f <input file> | The absolute name of the input file. The input file can be either a configuration file (typically named.con) or a script file. The type of the file passed is specified with the -t option. |
| -t {scr conf} | The type of the file passed with the -f option. scr is used to indicate that a script file is being passed and conf is used to indicate that a configuration file is being passed. scr is the default option used when -t is not specified. |
| -l <log file name> | The name of the log file, where the messages are logged. By default, sys:\zoneimp.log file is created. If any error is encountered, the important messages are printed on the ICE screen. NOTE: The ICE utility will create a log file named sys:\ice.log |
| -x <zone context> | The context under which the zone objects are created. |
| -b <DNS Server DN> | The distinguished name of the DNS server in Novell eDirectory. The imported zones are associated with this DNS server. This is required to link the imported zone objects to the DNS server and vice versa. |
| -r | The zone object, if already present, should be replaced. If this option is not specified, the existing zone objects are not disturbed. |

| Options | Descriptions |
|-----------------------|---|
| -s <LDAP server name> | The LDAP server name or IP address to which the zone and configuration information will be imported. Default: local machine (127.0.0.1/"local host") NOTE: The server name specified here should be the same as specified in the destination LDAP handler options (-s option). |
| -p <port no> | The port number where the LDAP server is listening. The default value is 389. NOTE: The port number specified here should be the same as specified in the destination LDAP handler options (-p option). |
| -d <bind dn> | The distinguished name with which you want to bind to the LDAP server. NOTE: The fully distinguished name specified here should be the same as specified in the destination LDAP handler options (-d option). |
| -w <password> | The password for the Bind DN. NOTE: The password specified here should be the same as specified in the destination LDAP handler options (-w option). If you do not specify the password for bind DN, only those LDAP operations that do not need authentication will pass and the rest will fail. |

LDAP Destination Handler Parameter: This can be obtained using the `ice -h LDAP` command at the system console of the NetWare server.

Example for Command Line Options: `ice -S ZONE -f sys:/etc/dns/named.conf -t conf -s 164.10.1.1 -x o=novell -b cn=DNS_MYSERVER,o=novell -d cn=admin,o=novell -w mypassword -D LDAP -s 164.10.1.1 -d cn=admin,o=novell -w mypassword`

Script File Format: A typical line from a script file contains the following fields.

<type of zone> <zone name> [master server IP] <master file name> [zone context] [comments] /
* end of line */

Type of Zone: Primary or Secondary.

Zone Name: The domain name for which the resource records are to be imported.

Master Server IP: The IP address of the master server, in case the zone is a secondary zone.

Master File Name: The file that contains the resource records.

Zone Context: The context where the zone object should be created.

Comments: Any ASCII pattern, the first character being a semicolon (;)

For example, `primary novell.com sys:/etc/dns/novell.com.db; primary zone secondary novell.com 164.1.1.1 sys:/etc/dns/novell.com.db;`

Named.conf File Format: The handler supports BIND 9.2 named.conf format only. It interoperates with Novell-extended attributes in the named.conf file. That is, it ignores those attributes during import. The existing BIND4 and BIND8 conf files must be converted to BIND9 format before passing them to this utility.

Exporting Configuration and Script Information

Using the ICE zone handler, the DNS server, zone configuration information, and data can be exported from eDirectory and written to the files.

Command Line Parameters for ICE Zone Export

Source Handler Options: ice -S ZONE -s<source server> [-p<source LDAP port>] [-d<user name in source server>] [-w<password for source server>] <[-b <DNS Server DN>] [-x <Zone context>]> [-F <LDAP filter>] -D {Destination Handler with options...}

| Options | Descriptions |
|--------------------|---|
| -s <server name> | Specify the server name or IP address that contains the zone and configuration information. The default is the local machine (127.0.0.1) |
| -p <port no> | Specify the port number where the server is listening. The default value is 389. |
| -d <bind dn> | Specify the distinguished name with which you want to bind to the LDAP server. |
| -w <password> | Specify the password for the Bind DN. NOTE: If the bind DN or password is not given, the result is based on the LDAP anonymous bind operation, and might not export all of the data. |
| -b <DNS Server DN> | Specify the FDN of the DNS server object. The handler uses this information to read the configuration information and also to detect zone objects that fall under the administrative domain of this server. NOTE: If -b option is not specified, the configuration information is not exported and only the zone master files will be formed. |
| -x <Zone Context> | Specify the context, from which the zone objects will be exported. x or b option must be specified. If b option is specified without the x option, all zones belonging to that DNS server will be exported. If both these options are specified, the configuration information is exported from the specified DNS server and the zone data with configuration from the specified zone objects. |
| -F <LDAP filter> | Specify the LDAP compliant filter. This acts in conjunction with the -x option described above to specify the zone objects to export. The default value is objectClass=* The -F options works only with -x option, to export all zones under the given context which match the given filter, and not when both -b and -x are specified. |

Destination Handler Options: D ZONE -p <path>

<path> - The path where the output files are created. The files that are created are named.conf and the zone master files, with the corresponding names of the zone objects as in the eDirectory.

By default, all zone information is created in the sys: \etc\dns\export volume and files, with names corresponding to the domain names.

For example, `ice -S ZONE -b cn=DNS_MYSERVER,o=novell -s 143.72.1.1 -p 389 -d cn=admin,o=novell -w mypassword -D ZONE -p sys:\export\`

Cluster Support

This section provides the following:

- ◆ “Clustering in NetWare 6.0” on page 163
- ◆ “Clustering in NetWare 6.5” on page 163
- ◆ “Creating a Cluster-Enabled DNS Server” on page 163
- ◆ “Configuring a DNS Server in a Clustered Environment” on page 164

Clustering in NetWare 6.0

In NetWare 6.0, you deployed older versions of DNS servers in a clustered environment and configured a DNS server on each of the nodes in the preferred node list corresponding to the resource. If the current node failed, the DNS server migrated from the current node to another node, depending on the sequence of nodes in the preferred node list. The number of DNS server objects equaled to the number of nodes in the preferred node list.

Although older versions of DNS servers supported clustering, it was limited to starting a DNS server and had its own identity. This server identity was different from the DNS server running on the next node.

For example, consider the following scenario:

- ◆ The preferred node list has Node 1, Node 2, and a designated primary DNS server (DNS server object 1) running on Node 1. This DNS server is supposed to handle the dynamic updates received from the DHCP server.
- ◆ An outage happens on Node 1 and the DNS server migrates to Node 2.
- ◆ Node 2 uses another DNS server (DNS server object 2), which is not a designated primary DNS server. It cannot handle the dynamic updates, so the identity of the DNS server is lost during a node outage.

For more information about cluster services, see the *Cluster Services Overview and Installation Guide* (<http://www.novell.com/documentation/lg/ncs65/index.html>).

Clustering in NetWare 6.5

In a clustered environment, the new DNS server, by default, supports the functionality provided by the older versions of DNS server. In addition, you can configure a new DNS server to maintain its identity after a node outage. In such case, only one DNS server is required per failover path (preferred node list) instead of one DNS server per node, as was the case with the older versions of DNS server.

Creating a Cluster-Enabled DNS Server

Consider the following scenario for an existing DNS server:

- ◆ The old DNS server is running in a cluster with one DNS server per node in the preferred node list. For any set of zones, only one of these can be a designated DNS server and the rest are passive DNS servers.
- ◆ A second DNS server running without a cluster.

To migrate this setup, you must consider the following points if you want the DNS server to take advantage of the new functionality and maintain its identity after an outage:

- ◆ All NCP™ servers in the preferred node list should be upgraded to NetWare 6.5.
- ◆ DNS server objects should not be created on an NCP server that is part of any existing preferred node list.
- ◆ Before moving any server, the DNS server should be brought down.
- ◆ Any node that is considered as a potential candidate to host DNS Services should be part of the only preferred node list.

You must also decide the following:

- ◆ Identify the DNS server object that has to be retained from the DNS servers corresponding to all nodes in the preferred node list. All other DNS server objects must be removed.
- ◆ If you want to retain all DNS server objects, create a separate failover path for every DNS server object.

Configuring a DNS Server in a Clustered Environment

- 1** Make sure that the server has been upgraded to NetWare 6.5.
- 2** Run `nwdeploy.exe` from the root of the NetWare 6.5 Operating System CD to upgrade the cluster software.
- 3** Launch `ConsoleOne`.
- 4** Create a Virtual NCP server by making a shared volume as cluster-enabled.
- 5** Identify the Volume Resource corresponding to the Virtual NCP server object.

A Virtual NCP server object has a reference to the Volume Resource in the attribute `Resources`.

- 6** Verify the load script in the volume resource as follows:

```
add secondary ipaddress xxx.xxx.xxx.xxx  
load named -v volume name
```

where `xxx.xxx.xxx.xxx` is the IP address of the Netware server.

- 7** Verify the unload script in the volume resource as follows:

```
unload named  
del secondary ipaddress xxx.xxx.xxx.xxx
```

- 8** Configure the desired policies for startup, failover, and failback in the Policies tab.
- 9** Select the Nodes tab and specify the desired available nodes and node preference order.
- 10** Launch any of the DNS/DHCP management utilities.
- 11** Click `Create > DNS Server` in the Java-based Management Console
or
Click `Create DNS Server` from the `iManager` roles.
- 12** Select the Virtual NCP server object created in [Step 4 on page 164](#).
- 13** Provide other inputs to create the DNS server, then click `OK`.

In order to make an existing non-cluster-enabled DNS server support clustering, use the move DNS server feature as follows:

- 1** Upgrade the server to NetWare 6.5.
- 2** Launch one of the DNS/DHCP management utilities.
- 3** Identify the NCP server and the corresponding DNS server object that should be retained.
Make sure that the DNS Services is not running on this NCP server.
- 4** Identify the Virtual NCP server where DNS Services will be based.
Unlike old DNS servers that were cluster-enabled as a cluster resource, this should be cluster-enabled as a volume resource corresponding to the shared volume. Do this with the ConsoleOne snap-ins for Clustering Services.
- 5** Make sure that none of the nodes in the preferred node list has an associated DNS server (except the NCP server selected in [Step 4](#) if it is part of the preferred node list).
Do this by deleting all other DNS servers in the preferred node list or moving them out of the preferred node list.
- 6** Use one of the DNS/DHCP management utilities to move the DNS server from the NCP server identified in [Step 3 on page 165](#) to the Virtual NCP server identified in [Step 4 on page 165](#).

For more information, see [“Moving a DNS Server” on page 80](#) and [“Moving a DNS Server” on page 94](#).

Adding a Node to a Cluster-Enabled DNS Server

To add a new node to the preferred node list of a DNS server that has been configured to maintain its identity across outage:

- 1** Make sure that each new node has been successfully added to the preferred node list.
- 2** Using ConsoleOne, add a reference to the corresponding physical NCP server to the group object's Members and EquivalentToMe list for each newly added node.

Alternatively, you can temporarily move the DNS server to another NCP server, and then move it back to the original NCP server.

After the DNS server has been created or moved to a Virtual NCP server, you can start the DNS server by doing the following:

- 1** Launch ConsoleOne.
- 2** Select the Netware Cluster object.
- 3** Click View > Cluster State to change to the cluster state view.
- 4** Click the DNS Cluster Resource to start the Resource Manager.
- 5** Click Online to start the resource.
- 6** Configure your clients to use the new resource as their primary DNS server.

We recommend that you configure your DHCP server to pass this name server address to clients by using DHCP.

All the entities that require the IP address of the DNS server should be configured with the secondary IP address of the virtual NCP server.

Deleting Empty Resource Records

A new command line utility (dnsmaint.nlm) that supports deletion of empty RRs that have accumulated over time, is introduced in NetWare® 6.5SP3 release.

This utility must be executed on a NetWare 6.5 SP3 machine in the eDirectory tree. The usage of the utility is specified below.

```
dnsmaint -User [-Password] [-Zonelist] [-LocatorObject] [-NotUsedSince]
```

The command line options are listed in the table below:

| Options | Description |
|----------------|---|
| -User | Refers to the FQDN of the eDirectory user. |
| -Password | eDirectory password of the user. Can be passed either as a command line parameter or can be entered later at the password prompt, when the utility is run. |
| -ZoneList | eDirectory FDQNs of the list of zones to be processed. Replace all occurrences of dot '.' in zone name with underscore '_'. Zone names must be separated by a semicolon(;). If this option is missing, LocatorObject must be specified. |
| -LocatorObject | eDirectory FQDN of the DNS locator object. This option must be used only if -Zonelist option is not specified. |
| -NotUsedSince | Empty RR's not used since the specified number of days are deleted. By default all the empty RRs are deleted. Any number between 1 and 360 can be used. |

Examples:

For all the samples, it is assumed that the eDirectory distinguished name of DNS locator object is dns-dhcp.novell.

- ◆ To delete all the empty Rrs from all the zones in the eDirectory tree.

```
dnsmaint -User:admin.novell -Password:novell -LocatorObject:.dns-dhcp.novell
```

- ◆ To delete all the empty RRs not used since 3 days, from all the zones.

```
dnsmaint -User:admin.novell -Password:novell -LocatorObject:.dns-dhcp.novell -NotUsedSince:3
```

- ◆ To delete all empty RRs from the zone blr.novell.com which is under eDirectory context dns-zones.

```
dnsmaint -User:admin.novell -Password:novell Zonelist:blr_novell_com.dns-zones
```

NOTE: All the '.' (dots) in the zone name blr.novell.com are replaced with '_' (underscores).

- ◆ To delete empty RRs not used since 5 days from the zone 155.72.143.IN-ADDR.ARPA which is under eDirectory context novell.

```
dnsmaint -User:admin.novell -Password:novell -  
Zonelist:155_99_164_IN-ADDR_ARPA.novell -NotUsedSince:5
```


8

OES Coexistence and Migration Issues

One of the top priorities in designing Novell® Open Enterprise Server (OES) was to ensure that new OES components, running on either NetWare® or Linux, can be introduced into an existing network environment without disrupting any of the products and services that are in place. It was also deemed important that there be a clear migration path for moving existing products or services and related data onto the OES platform.

This section discusses the issues involved in the coexistence and migration of the DNS server in OES. It is divided into the following sections:

- ◆ “Coexistence” on page 169
- ◆ “Migration” on page 170

For a general discussion of coexistence and migration issues in OES, see the *OES Coexistence and Migration Guide*.

Coexistence

This section provides information regarding the coexistence of NetWare 6.5 DNS server with SLES DNS server.

Compatibility

The following table summarizes the compatibility of DNS server with various network operating systems.

| | |
|--------------------------|--------------------------------|
| NetWare Operating System | OES NetWare |
| | NetWare 6.5 |
| | NetWare 6.0 |
| | NetWare 5.1 |
| Linux Operating System | SUSE LINUX Enterprise Server 9 |

Coexistence Issues

Among the various security mechanisms available for DNS, DNS Security Transaction Signatures (TSIG) and DNS Security Extensions (DNSSEC) are not supported in the NetWare DNS server. Due to this limitation, following issues need to be considered in environments running SLES and NetWare DNS servers:

- ◆ DNSSEC mechanism should not be used for interactions between a SLES DNS server and NetWare DNS server.

- ◆ NetWare DNS server cannot be configured to accept dynamic updates using TSIG feature.

For example:

Dynamic updates from SLES DHCP server

Updates from nsupdate using TSIG feature

Migration

This section provides information on how to migrate from NetWare 6.5 DNS server to SLES DNS server.

Migration steps mentioned in this document are only for zone data migration from NetWare 6.5 to SLES. Migrating DNS server and Zone configuration is not covered as part of this documentation.

Pre-requisites

- ◆ The administrator migrating DNS server from NetWare 6.5 to SLES should be familiar with DNS on SLES. For more details on SLES DNS server, refer to SLES Documentation and [Internet Systems Consortium \(http://www.isc.org\)](http://www.isc.org) web site.
- ◆ The DNS server should be installed on SLES system.

Recommended Procedure

To migrate zone data of a master zone from NetWare 6.5 DNS server to SLES DNS server:

- 1** Create a slave zone in the SLES, the steps are as follows:

Edit named.conf and configure to create the slave zone

```
zone "acme.com" in {
masters { 10.1.1.1; };
file "slave/acme.com";
type slave;
};
```

In the above sample configuration, SLES DNS is configured as a slave server for acme.com zone. The IP Address 10.1.1.1 is of the current zone master, which is the NetWare 6.5 DNS server.

- 2** Stop and restart the SLES DNS server using YaST utility. SLES DNS server transfers the zone from NetWare DNS server and the Zone DB file acme.com is created in /var/lib/named/slave
- 3** Change the role of the SLES DNS server to master:
 - 3a** Stop the DNS service on both NetWare and SLES server.
 - 3b** Move acme.com from /var/lib/named/slave to /var/lib/named/master on the SLES server.

3c Edit named.conf in the acme.com zone section and modify the following:

```
zone "acme.com" in {  
    masters { 10.1.1.1; };  
    file "slave/acme.com";  
    type slave;  
};
```

3d Remove the entry master { 10.1.1.1; };

3e Change the file location from file "slave/acme.com"; to file "master/acme.com";

NOTE: On changing the file location the owner and group of the file changes, from named to root. Restore the owner and group attribute values to named. If this is not done named will not have permissions to read the data from the file.

3f Change the type from type slave; to type master;

Currently, YaST does not support changing of zone type from master to slave and vice versa. So, this change should be done manually by editing the file.

3g After the modification, zone section should read

```
zone "acme.com" in {  
    file "master/acme.com";  
    type master;  
};
```

4 Change the role of NetWare DNS server for acme.zone from master to slave.

5 Using the YaST utility, create NS and A records for the server which is authoritative for acme.com zone.

6 Start the DNS service on both NetWare and SLES server.

Migration Issues

The following features of the NetWare DNS server are not available in SLES DNS server:

- ◆ eDirectory™ integration
- ◆ Dynamic reconfiguration
- ◆ SNMP Traps
- ◆ Java Based management utility and iManager

SLES DNS server can not accept dynamic updates from NetWare DHCP server.

A Appendix

This section provides the following information:

- ◆ “Supported RFCs” on page 173
- ◆ “Types of Resource Records” on page 174
- ◆ “DHCP Option Descriptions” on page 176
- ◆ “DNS-DHCP SNMP Events” on page 184
- ◆ “DNS Root Servers” on page 185

Supported RFCs

Novell[®] DNS/DHCP Services supports the following RFCs:

- ◆ 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 1884—IP Version 6 Addressing Architecture

- ◆ RFC 1876—Location Information in the DNS
- ◆ RFC 1886—DNS Extensions to Support IP Version 6
- ◆ RFC 1912—Common DNS Operations and Configurations Errors
- ◆ RFC 1995—Incremental Zone Transfer in DNS
- ◆ RFC 1996—A mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- ◆ RFC 2010—Operations Criteria for Root Name servers
- ◆ RFC 2136—Dynamic Updates in the DNS
- ◆ RFC 2163—Using the Internet DNS to distribute MIXER Conformant Global Address Mapping (MCGAM)
- ◆ RFC 2308—Negative Caching of DNS Queries (DNS NCACHE)
- ◆ RFC 2317—Classless IN-ADDR.ARPA delegation
- ◆ RFC 2672—Non-Terminal DNS Name Redirection
- ◆ RFC 2782—A DNS RR for specifying the location of services (DNS SRV)
- ◆ RFC 2874—DNS Extensions to Support IPv6 Address Aggregation and Renumbering

Types of Resource Records

A Resource Record (RR) contains data associated with domain names. This data is represented by and is subordinate to the Resource Record Set (RRset) of a zone container.

The following types of Resource Records can be created:

- ◆ A6: Maps a domain name to an IPv6 address.
Specify the following for this option:
 - ◆ Prefix Length: This can be any value between 0 and 128.
 - ◆ Address Suffix: The Address Suffix need not be specified if the prefix length is 128.
 - ◆ Prefix Name: The domain name of the server. This need not be specified if the prefix length is 0.
- ◆ A: Maps a domain name to an IP address.
You must specify the 32-bit IPv4 address that will map to the associated domain for this option.
- ◆ AAAA: A 128-bit IPv6 address that is encoded in the data portion of the resource record in the network byte order.
- ◆ AFSDDB: The AFS system uses the DNS to map from a domain name to the name of an AFS cell database server. It contains the following data:
 - ◆ Subtype: A 16-bit integer.
 - ◆ Hostname: The domain name of the host server.
- ◆ CNAME: Specifies the canonical or primary name for the owner. Because the owner name is an alias, you must specify the domain name of the aliased host if you select this option.
- ◆ DNAME: Specifies an alternate name to map the entire subtree of the domain namespace.
You must specify the Target Domain name for this option.

- ◆ HINFO: Specifies host information in the form of the following parameters:
 - ◆ CPU: A character string that specifies the CPU type.
 - ◆ OS: A character string that specifies the operating system type.
- ◆ ISDN: An ISDN (Integrated Service Digital Network) number is a telephone number integrating the telephone and data network service to a common service. It contains the following parameters:
 - ◆ ISDN Address: A character string specifying the ISDN address.
 - ◆ Sub Address: A character string specifying the subaddress. This parameter is optional.
- ◆ LOC: Specifies the location information in the globe. If you select this option, you must specify the following:
 - ◆ Latitude: Specify the degree of the latitude, minutes, and seconds of the globe enclosing the specified host. Select the direction.
 - ◆ Longitude: Specify the degree of the latitude, minutes, and seconds of the globe enclosing the specified host. Select the direction.
 - ◆ Altitude: Specify the altitude of the globe enclosing the specified host in meters.
 - ◆ Size: Specify the diameter of the globe enclosing the specified host in meters.
 - ◆ Horizontal precision: Specify the horizontal precision of the globe enclosing the specified host in meters.
 - ◆ Vertical precision: Specify the vertical precision of the globe enclosing the specified host in meters.
- ◆ MB: Specifies the domain name of the mailbox address.
- ◆ MG: A domain name that specifies a mailbox that is a member of the mail group specified by the domain name.
- ◆ MINFO: Specifies mailbox or mail list information in the form of the following parameters:
 - ◆ Responsible MailBox: A domain name that specifies the mailbox that is responsible for the mailing list or mailbox.
 - ◆ Error Message MailBox: A domain name that specifies the mailbox that is to receive error messages related to the mailing list or mailbox.
- ◆ MR: A domain name that specifies the mailbox that is the proper rename of the specified mailbox.
- ◆ MX: Specifies a mail exchange resource record in the form of the following parameters:
 - ◆ Preference: A 16-bit integer that specifies the preference given to this resource record among others at the same owner.
 - ◆ Exchange: A domain name that specifies a host willing to act as a mail exchange for the owner name.
- ◆ NS: Specifies a domain name for an authoritative name server for the specified class and domain.
- ◆ PTR: A domain name that points to some location in the domain namespace.
- ◆ PX: Contains X.400 mail mapping information with the following parameters:
 - ◆ Preference: A 16-bit integer that specifies the preference given to this resource record among others at the same owner.

- ◆ MAP822: A domain name element containing the RFC822 part of the MCGAM.
- ◆ MAPX400: A domain name element containing the value derived from the X.400 part of the MCGAM.
- ◆ RP: Provides a standard method of associating responsible person identification with any name in the DNS with the following parameters:
 - ◆ Responsible Person's Mailbox: A domain name that specifies the mailbox for the responsible person.
 - ◆ TXT-RR Domain Name: A domain name for which TXT RRs exist.
- ◆ RT: Specifies the routing information with the following parameters:
 - ◆ Preference: A 16-bit integer representing the preference of the route.
 - ◆ Intermediate: The domain name of a host that will serve as an intermediate in reaching the host specified by the owner.
- ◆ SRV: Specifies the location of services with the following parameters:
 - ◆ Service: The symbolic name of the desired service.
 - ◆ Proto: The TCP and UDP are the most useful values for this field.
 - ◆ Priority: The priority of the target host.
 - ◆ Weight: A load balancing mechanism when selecting a target host among those that have the same priority.
 - ◆ Port: The port on the target host running the service.
 - ◆ Target: The domain name of the target host.
- ◆ TXT: Specifies text data in the form of a character string.
- ◆ WKS: Describes the well-known services supported by a protocol on a particular host with the following parameters:
 - ◆ Address: A 32-bit Internet address.
 - ◆ Protocol: An 8-bit IP protocol number.
 - ◆ Available Services: A variable-length bitmap.
- ◆ X25: Specifies a PSDN (Public Switched Data Network) address.

DHCP Option Descriptions

The following table describes the DHCP option codes and names:

| Code | Option Name |
|------|--------------------|
| 2 | Time Offset |
| 3 | Router |
| 4 | Time Server |
| 5 | Name Server |
| 6 | Domain Name Server |

| Code | Option Name |
|-------------|-----------------------------------|
| 7 | Log Server |
| 8 | Cookie Server |
| 9 | LPR Server |
| 10 | Impress Server |
| 11 | Resource Location Server |
| 13 | Boot File Size |
| 14 | Merit Dump File |
| 16 | Swap Server |
| 17 | Root Path |
| 18 | Extension Paths |
| 19 | IP Forwarding Enable/Disable |
| 20 | Non-Local Source Routing |
| 21 | Policy Filter |
| 22 | Maximum Datagram Re-assembly size |
| 23 | Default IP Time-to-live |
| 24 | Path MTU Aging Time-out |
| 25 | Path MTU Plateau Table |
| 26 | Interface MTU |
| 27 | All subnets are local |
| 28 | Broadcast Address |
| 29 | Perform Mask Discovery |
| 30 | Mask Supplier |
| 31 | Perform Router Discovery |
| 32 | Router Solicitation Address |
| 33 | Static Route |
| 34 | Trailer Encapsulation |
| 35 | ARP Cache Time-out |
| 36 | Ethernet Encapsulation |
| 37 | TCP Default TTL |
| 38 | TCP Keep-alive interval |

| Code | Option Name |
|-------------|--|
| 39 | TCP Keep-alive garbage |
| 40 | NIS Domain |
| 41 | NIS Servers |
| 42 | Network Time Protocol Servers |
| 43 | Vendor Specific Option |
| 44 | NetBIOS over TCP/IP options-name server |
| 45 | NetBIOS over TCP/IP options-datagram distribution server |
| 46 | NetBIOS over TCP/IP options-node type |
| 47 | NetBIOS over TCP/IP options-Scope |
| 48 | X Window System Font Server |
| 49 | X Window System Display Manager |
| 58 | Renewal (T1) Time |
| 59 | Renewal (T2) Time |
| 60 | Vendor Class Identifier |
| 62 | NWIP Domain Name |
| 63-05 | Perform NSQ Broadcast |
| 63-06 | Preferred DSS |
| 63-07 | Nearest NWIP Server(s) |
| 63-08 | Number of Auto Retries |
| 63-09 | Auto Retry Interval |
| 63-10 | Support NWIP 1.1 |
| 63-11 | Primary DDS |
| 63-12 | IPX Network Number |
| 63-13 | IPX Stale Time |
| 63-14 | Migration Agents |
| 64 | NIS+ Domain |
| 65 | NIS Servers |
| 66 | TFTP Server Name |
| 67 | Boot File Name |
| 68 | Mobile IP Home Agent |

| Code | Option Name |
|------|---|
| 69 | SMTP Server |
| 70 | POP3 Server |
| 71 | NNTP Server |
| 72 | WWW Server |
| 73 | Default Finger Server |
| 74 | Default IRC Server |
| 75 | Street Talk Server |
| 76 | Street Talk Directory Assistance server |
| 78 | SLP Directory Agent |
| 79 | SLP Service Scope |
| 85 | NDS Servers |
| 86 | NDS Tree Name |
| 87 | NDS Context |

The DHCP Options are described as follows:

Time Offset: Specifies the offset time of client's subnet in seconds. This is expressed as a two's complement 32-bit integer preference value. Two types of offset can be set: positive and negative offset. A positive offset indicates a location to the east of the zero meridian and a negative offset indicates a location to the west of the zero meridian.

Router: Specifies the routers on the client's subnet as a list of IP addresses. The routers should be listed in the order of preference.

Time Server: Specifies a list of RFC time servers available to the client. The servers should be listed in the order of preference.

Name Server: Specifies a list of IEN 116 [7] name servers available to the client. The name servers should be listed in the order of preference.

Domain Name Server: Specifies a list of DNS name servers available to the client. The DNS servers should be listed in the order of preference.

Log Server: Specifies a list of MIT-LCS UDP log servers available to the client. The log servers should be listed in the order of preference.

Cookie Server: Specifies a list of RFC 865 cookie servers available to the client. The cookie servers should be listed in the order of preference.

LPR Server: Specifies a list of RFC 1179 line printer servers available to the client. The LPR servers should be listed in the order of preference.

Impress Server Option: Specifies a list of Imagen Impress servers available to the client. The impress servers should be listed in the order of preference.

Resource Location Server: Specifies a list of RFC 887 resource location servers available to the client. The resource location servers should be listed in the order of preference.

Boot File Size: Specifies the length in 512-octet blocks of the boot image for the client. The length is specified as an unsigned 16-bit integer.

Merit Dump File: Specifies the location of a file where the core image of the client should be dumped if the client crashes.

Swap Server: Specifies the IP address of the swap server for the client.

Root Path: Specifies the path name for the client's root disk.

IP Forwarding Enable/Disable: Specifies whether the client should forward an IP address. Values can be either True or False. True indicates that IP forwarding should be enabled and False indicates that IP forwarding should be disabled.

Nonlocal Source Routing Enable/Disable: Specifies whether the client should forward datagrams with non-local source routing. Values can be either True or False. True indicates to enable datagram forwarding and False indicates to disable datagram forwarding.

Policy Filter: Specifies the policy filters for non-local source routing. The policy filters consist of a list of IP addresses and masks that filter the incoming source routes.

Maximum Datagram Reassembly Size: Specifies the maximum size of the datagram that the client should reassemble.

Default IP TTL: Specifies the time-to-live used by the client on outgoing datagrams.

Path MTU Aging Time-out: Specifies the time-out (in seconds) used when the aging path MTU values are discovered by the mechanism defined in RFC 1191.

Path MTU Plateau Table Option: Specifies a table of MTU sizes used when performing path MTU discovery as defined in RFC 1191.

Interface MTU: Specifies the MTU used on this interface. The minimum value for MTU is 68.

All subnets are local: Specifies whether the client can assume that all subnets of IP network connected to the client use the same MTU as the subnet of the network to which the client is directly connected. Values can be either True or False. True indicates that all subnets share the same MTU. False indicates that some subnets of the network that is directly connected have smaller MTU values.

Broadcast Address: Specifies the broadcast address being used on the client's subnet.

Perform Mask Discovery: Specifies whether the client should perform subnet mask discovery using ICMP. Values can be either True or False. True indicates that the client should perform subnet mask discovery. False indicates that the client should not perform subnet mask discovery.

Mask Supplier: Specifies whether the client should respond to subnet mask requests using ICMP. Values can be either True or False. True indicates that the client should respond and False indicates that the client should not respond.

Perform Router Discovery: Specifies whether the client should solicit routers using the Router Discovery mechanism as defined in RFC 1256. Values can be either True or False. True indicates that the client should perform router discovery and False indicates that the client should not perform router discovery.

Router Solicitation Address: Specifies the IP address to which the client can send router solicitation requests.

Static Route: Specifies a list of static routes that the client can install in its routing cache. Multiple routes to the same destination are listed in descending order. Static routes consists of a list of IP address in pairs. The first address in the pair is the destination address and the second is the router for the destination.

Trailer Encapsulation: Specifies whether the client can negotiate encapsulating trailers when using the ARP protocol. Values can be either True or False. True indicates that the client should use trailers and False indicates that the client should not use trailers.

ARP Cache Time-out: Specifies the time-out (in seconds) for ARP cache entries.

Ethernet Encapsulation: Specifies whether the client can use Ethernet version 2.0 (RFC 894) or IEE 802.3 (RFC 1042) encapsulation if it is an Ethernet interface. Values can be either True or False. True indicates that the client should use RFC 1042 encapsulation and False indicates that the client should use RFC 894 encapsulation.

TCP Default TTL: Specifies the default TTL that the client should use when sending TCP segments.

TCP Keep-alive interval: Specifies the interval (in seconds) that the TCP client should wait before sending a keep-alive message on a TCP connection.

TCP Keep-alive Garbage: Specifies whether the client should send TCP keep-alive messages with a garbage octet for compatibility with older implementations. Values can be either True or False. True indicates that a garbage octet should be sent and False indicates that a garbage octet should not be sent.

NIS Domain: Specifies the NIS domain name of the client.

NIS Servers: Specifies a list of the NIS server's IP addresses available to the client. The NIS servers should be listed in the order of preference.

Network Time Protocol Servers: Specifies a list of IP addresses indicating Network Time Protocol Servers (NTP servers) available to the client. The NTP servers should be listed in the order of preference.

Vendor-Specific Information: Specifies the vendor-specific information that can be used by the clients and servers.

NetBIOS over TCP/IP Name Server: Specifies a list of RFC 1001 and RFC 1002 NetBIOS over TCP/IP Name Server listed in order of preference.

NetBIOS over Datagram Distribution Server: Specifies a list of RFC 1001 and RFC 1002 NetBIOS over Datagram Distribution servers listed in order of preference.

NetBIOS over TCP/IP Node Type: Allows NetBIOS over TCP/IP clients that can be configured as described in RFC 1001 and RFC 1002. Node types include B-node, P-node, M-node, and H-node.

NetBIOS over TCP/IP Scope: Specifies the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001 and RFC 1002.

X Window System Font Server: Specifies a list of X Window System Font servers available to the client. These servers should be listed in order of preference.

X Window System Display Manager: Specifies a list of IP addresses of systems that use the X Window System Display Manager and are available to the client. The IP addresses should be listed in order of preference.

T1 Time Value: Specifies the time interval from the address assignment until the client reaches the renewing state.

T2 Time Value: Specifies the time interval from the address assignment until the client reaches the rebinding state.

Vendor Class Identifier: Specifies the vendor type and configuration of a DHCP client.

NetWare/IP Domain: Enables the server to convey the NetWare/IP domain name used by the NetWare/IP product.

Preferred NSQ Broadcast: Specifies whether the client should perform a NetWare Nearest Server Query (NSQ) to find out its nearest NetWare/IP server. Values can be either True or False. True indicates that the client should perform a NetWare NSQ and False indicates that the client should not perform a NetWare NSQ.

Preferred DSS: Specifies a list of addresses for a NetWare Domain SAP/RIP Server (DSS).

Nearest NWIP Server(s): Specifies a list of addresses for the Nearest NetWare/IP (NWIP) servers.

Number of Auto Retries: Specifies the number of times a NetWare/IP client can attempt to communicate with a DSS server at startup.

Auto Retry Interval: Specifies the delay interval (in seconds) that each NetWare/IP client uses when attempting to communicate with a DSS server at startup.

Support NWIP 1.1: Specifies whether the NetWare/IP client should support NetWare/IP version 1.1. This is required only if it contacts a NetWare/IP version 1.1 server. Values can either be True or False. True indicates that the client should support NetWare/IP version 1.1 and False indicates that the client should not support NetWare/IP version 1.1.

Primary DDS: Specifies the Primary Domain SAP/RIP Service server (DSS) for the NetWare/IP domain. The NetWare/IP administration utility uses this as the Primary DSS server when configuring a secondary DSS server.

NIS+ Domain: Specifies the name of the client's NIS+ domain.

NIS+ Servers: Specifies a list of IP addresses indicating Network Information Service (NIS)+ servers available to the client. The NIS+ servers should be listed in order of preference.

TFTP Server Name: Specifies the name of the TFTP server for the client.

Boot File Name: Specifies the name of the boot file for the client.

Mobile IP Home Agent: Specifies a list of IP addresses that indicates the mobile IP home agents available to the client. These agents should be listed in order of preference.

SMTP Server: Specifies a list of Simple Mail Transport Protocol (SMTP) servers available to the client. The SMTP servers should be listed in order of preference.

POP3 Server: Specifies a list of POP3 servers available to the client. The POP3 servers should be listed in order of preference.

NNTP Server: Specifies a list of Network News Transport Protocol (NNTP) servers available to the client. The NNTP servers should be listed in order of preference.

WWW Server: Specifies a list of World Wide Web (WWW) servers available to the client. The WWW servers should be listed in order of preference.

Default Finger Server: Specifies a list of Finger servers available to the client. The Finger servers should be listed in order of preference.

Default IRC Server: Specifies a list of Internet Relay Chat (IRC) servers available to the client. The IRC servers should be listed in order of preference.

StreetTalk Server: Specifies a list of StreetTalk* servers available to the client. The StreetTalk servers should be listed in order of preference.

StreetTalk Directory Assistance Server: Specifies a list of StreetTalk Directory Assistance (STDA) servers available to the client. The STDA servers should be listed in order of preference.

Directory Agent: Specifies a list of IP addresses for Directory Agents. The Directory Agents should be listed in order of preference.

Service Scope: Specifies the scope that an SLP agent is configured to use.

NDS Servers: Specifies one or more NDS[®] servers for the client to contact to access the NDS database. The NDS servers should be listed in order of preference.

NDS Tree Name: Specifies the name of the NDS tree that the client contacts.

NDS Context: Specifies the initial NDS context that the client should use.

Assigning Options

DHCP and BOOTP options can be assigned at three levels:

- ◆ Globally
- ◆ At the subnet level
- ◆ At the 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 the following table.

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

The following table lists the effective options for the client with the IP address referred to in the preceding table.

| 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 |

DNS-DHCP SNMP Events

The following list shows the DNS-DHCP events for SNMP traps:

DNS_SNMP_SERVER_LOADED: DNS server is ready (up and running).

DNS_SNMP_SERVER_LOADFAIL: DNS server load failure.

DNS_SNMP_NDSWRITE_FAIL: Write operation of DNS events failed in NDS.

DNS_SNMP_NDSREAD_FAIL: Read operation of DNS events failed in NDS.

DNS_SNMP_UNAUTH_UPDATE: Unauthorized updates to the DNS Server.

DNS_SNMP_XFROUT_FAIL: **Zone out** transfer failure.

DNS_SNMP_XFRIN_FAIL: **Zone in** transfer failure.

DNS_SNMP_ZONE_EXPIRY: Events that occur when zone data expires.

DNS_SNMP_ZONELOAD_FAIL: Events that occur when zone load fails.

DNS_SNMP_QUERYBLOCK: Queries that are blocked because of the query filter.

DNS_SNMP_REQ_QUERYBLOCK: Recursive queries that are blocked by the recursive filter.

DNS_SNMP_QUERY_NOFRD: Queries that are in the no-forward list.

DNS_SNMP_XFR_BLOCK: Zone transfer blocked.

DNS_SNMP_UNAUTH_STOPSTART: Unauthorized start or stop operation.

DNS_SNMP_SERVER_UNLOAD_FAIL: DNS server unload failure.

DNS_SNMP_TERMINATION_INIT: Do not send any SNMP traps. Although the SNMP trap flag is set and this trap number is passed, SNMP traps are not generated.

DNS Root Servers

The rootsrvr.dat file contains information about DNS Root servers. When the DNS services are installed, the RootSrvrInfo Zone object is created by reading the contents from this file. The RootSrvrInfo zone holds information on the root name servers needed to initialize the cache of Internet domain name servers. The rootsrvr.dat file is the Novell's version of named.root, which is made available by Inter NIC registration services

```
under anonymous FTP as  
file /domain/named.root  
on server FTP.RS.INTERNIC.NET
```

-OR-

```
under Gopher at RS.INTERNIC.NET  
under menu InterNIC Registration Services (NSI)  
submenu InterNIC Registration Archives  
file named.root
```

The related version number of Root Zone is 1997082200 and was last updated on Aug 22, 1997

The data for the root servers is as follows:

SOA and NS RRs:

```
$ORIGIN RootServerInfo.  
@ SOA server. root. (  
 1997082200 3600 3600 604800 86400 )  
. 3600000 NS A.ROOT-SERVERS.NET.  
. 3600000 NS B.ROOT-SERVERS.NET.  
. 3600000 NS C.ROOT-SERVERS.NET.  
. 3600000 NS D.ROOT-SERVERS.NET.  
. 3600000 NS E.ROOT-SERVERS.NET.  
. 3600000 NS F.ROOT-SERVERS.NET.  
. 3600000 NS G.ROOT-SERVERS.NET.  
. 3600000 NS H.ROOT-SERVERS.NET.  
. 3600000 NS I.ROOT-SERVERS.NET.  
. 3600000 NS J.ROOT-SERVERS.NET.  
. 3600000 NS K.ROOT-SERVERS.NET.  
. 3600000 NS L.ROOT-SERVERS.NET.  
. 3600000 NS M.ROOT-SERVERS.NET.
```

Glue RRs:

```
A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4
```

| | | | |
|---------------------|---------|---|----------------|
| B.ROOT-SERVERS.NET. | 3600000 | A | 128.9.0.107 |
| C.ROOT-SERVERS.NET. | 3600000 | A | 192.33.4.12 |
| D.ROOT-SERVERS.NET. | 3600000 | A | 128.8.10.90 |
| E.ROOT-SERVERS.NET. | 3600000 | A | 192.203.230.10 |
| F.ROOT-SERVERS.NET. | 3600000 | A | 192.5.5.241 |
| G.ROOT-SERVERS.NET. | 3600000 | A | 192.112.36.4 |
| H.ROOT-SERVERS.NET. | 3600000 | A | 128.63.2.53 |
| I.ROOT-SERVERS.NET. | 3600000 | A | 192.36.148.17 |
| J.ROOT-SERVERS.NET. | 3600000 | A | 198.41.0.10 |
| K.ROOT-SERVERS.NET. | 3600000 | A | 193.0.14.129 |
| L.ROOT-SERVERS.NET. | 3600000 | A | 198.32.64.12 |
| M.ROOT-SERVERS.NET. | 3600000 | A | 202.12.27.33 |

B

Glossary

This section describes the most commonly used terms in DNS/DHCP Services.

Additional Options: An attribute of the DNS server and Zone, which allows fine-tuning of options for server performance. The values specified at the zone level override the values specified in the DNS server.

Additional from Auth: Controls the behavior of an authoritative server when answering queries that have additional data, or when following CNAME and DNAME chains. When this option is set to yes, and when a query is being answered from authoritative data, the additional data section of the reply is filled in using data from other authoritative zones.

Additional from Cache: Controls the behavior of an authoritative server when answering queries that have additional data, or when following CNAME and DNAME chains. When this option is set to yes, and when a query is being answered from authoritative data, the additional data section of the reply is filled in using data from the cache.

Allow Notify: Specifies the hosts that are allowed to notify slaves of a zone change in addition to the zone masters. This can be configured only for a secondary zone.

Allow Recursion: A list of IP addresses or networks from which DNS server will accept query recursively. If a value is not specified, the default is to allow recursive queries from all hosts.

Also Notify: A list of IP addresses of name servers that are also sent notify messages, when a new copy of the zone is loaded, in addition to the servers listed in the Zone's NS records. This is primarily meant to converge stealth servers. The default is empty list (no additional notification list). The value specified in the zone overrides the value specified in the server.

Audit: A set of security-related events that need to be audited.

Audit policy: A set of rules that controls how the audit services function.

Auditing Trailing: Tracks the activities of users by recording the selected types of events in the security log/database of a server or a workstation. The process defines policies that determine the security events to be reported to the network administrator or auditor.

Authoritative: DNS data that is served by the resident DNS server. The server can be either primary or secondary. This is the DNS data that belongs to a resident domain and is managed by the administrator of that domain, or it is the DNS data that is imported through a zone transfer.

Blacklist servers: These are fake servers; the DNS server will not answer queries from or forward queries to these servers. This list is maintained in the “dnipBlacklistServers” attribute of the DNS server object in Novell® eDirectory™.

Bulk Zone Export: Transferring one or more zones' configuration and data from eDirectory to files. This can be done using the Import-Convert-Export (ICE) utility, which uses ICE zone handlers.

Bulk Zone Import: Transferring one or more zones' configuration and data from files to eDirectory. This can be done using the Import-Convert-Export (ICE) utility, which uses ICE zone handlers.

Cleaning Interval: With this option set, the server removes expired resource records from the cache after every cleaning interval. If it is set to 0, no periodic cleaning will occur.

Cluster: Novell DNS cluster services is a server clustering solution that provides high availability and manageability of critical network resources including data, applications, and services. It is enabled for eDirectory and supports failover, fallback, and migration (load balancing) of individual managed services.

Co-existence: Both the old and new servers interoperate on the same eDirectory configuration. The underlying platform / configuration is the same and allows different versions of the server to work on it. Co-existence of a new DNS server with a current DNS server allows customers to do a phased upgrade and migration from old DNS servers to new DNS servers.

Designated Primary Server: The master primary server, which serves a primary zone and honors zone-out transfer requests. It is the only primary server in the zone that will accept dynamic updates. There is only one designated primary server per zone.

Designated Secondary Server: The master secondary server, which serves a secondary zone and honors zone-out transfer requests. It is the only secondary server in the zone that will perform inbound zone transfer requests to the primary server in the zone. There is only one designated secondary server per zone.

Dynamic Reconfiguration: Detects the changes in the DNS server and DNS Zone configuration data and applies it from eDirectory to DNS server in-memory while the DNS server is in running mode (without shutting down the server).

Dynamic Update - Novell proprietary: Novell DHCP server sends the updates to DNS server using a Novell proprietary update format. The proprietary dynamic update message has a different format from the standard RFC 2136 and also has security signature associated with the message. There is a logic for establishing credentials for each connection from DHCP to DNS. After the credentials are established, the DHCP server sends the actual packet of DNS data for update to the DNS server.

Dynamic Update - RFC 2136: The new DNS servers accept dynamic update requests in standard RFC 2136 format. For more information, refer to [RFC 2136 \(http://www.ietf.org/rfc/rfc2136.txt?number=2136\)](http://www.ietf.org/rfc/rfc2136.txt?number=2136).

Event: The occurrence of an action on an object of interest.

Event Logging: Any significant occurrence in the system or an application that requires administrators to be notified or an event to be added to a log.

Event logging is primarily for:

- ◆ Application monitoring: that is, monitoring the critical and some of the important operations related to the application/server.
- ◆ Error monitoring: that is, monitoring failure in some operations.

Fault tolerance: Handles temporary disruptions of eDirectory unavailability, with graceful degradation in functionality. This can be categorized as:

- ♦ **Full Fault Tolerance:** The state when eDirectory is down and access to the DNS server object is broken. The server will not accept the following:

- Dynamic Update

- Zone-in

- Notify

No write operation can be performed until eDirectory is up.

The server will resolve only normal queries and zone-out transfer. Full Fault-Tolerance mode is applicable to all zones that are being serviced by the DNS server.

- ♦ **Partial Fault Tolerance:** The state when eDirectory is up but access to some zones is broken (because some eDirectory partitions are down or are not accessible). The server will not accept:

- Dynamic Update

- Zone-in

- Notify

No write operation to these zones is performed until the partition is down

The server will only resolve normal queries for this zone. The queries are responded only until the expiration for a secondary zone and forever for a primary zone.

Forward: This option can be configured only if the forwarding list is not empty. A value of First, which is the default, causes the server to query the forwarders first. If that does not answer the query, the server will then look for the answer. If Only is specified, the server will query only the forwarders.

Forwarder: A DNS server that forwards queries to other DNS servers, if the requested information is not found on the local server.

FQDN: Fully Qualified Distinguished Name

Group: The DNS/DHCP Group object is a standard eDirectory group object. The DNS and DHCP servers gain the rights to DNS and DHCP data within the tree through the Group object.

ICE: The utility to import or export the DNS server, zone configuration information, and data to or from the eDirectory database.

Journal Log: All changes made to a zone using dynamic update are stored in the zone's journal log. The server automatically creates this log when the first dynamic update takes place. The extension .jnl is appended to the name of the corresponding zone to form the journal log file. The journal log is in a binary format and should not be edited manually.

Lame TTL: Sets the number of seconds to cache a lame server indication (these are misconfigurations in the remote servers, discovered by the DNS service when trying to query those servers during resolution). 0 disables caching (not recommended). The maximum value is 1800 (30 minutes).

Listen On: Specifies the interfaces and ports that the server will answer queries from. It takes an optional port and an address match list. If a port is not specified, port 53 will be used.

Locator: The DNS/DHCP Locator object contains a reference to global defaults and DHCP options, and list of all DNS and DHCP servers, subnets, and zones in the tree.

Maximum Cache Size: The maximum amount of memory (in bytes) used for the server's cache. When the amount of data in the cache reaches this limit, the server will cause records to expire prematurely so that the limit is not exceeded. The default is 0 (unlimited cache).

Maximum Cache TTL: Sets the maximum time for which the server will cache ordinary (positive) answers.

Maximum NCache TTL: Sets a maximum retention time for negative answers in the server. The server stores negative answers to reduce network traffic and increase performance. The maximum value is 7 days.

Maximum Recursion Lookups: The maximum number of simultaneous recursive lookups that the server performs on behalf of the clients. This allows you to set limits on the servers' resource consumption. The default value is 1000.

NOTE: Each recursive client uses about 20 KB of memory

Minimal Responses: Allows the server to add records to the authority sections, and optionally to the additional section depending on the value set for this option. If this is set to No, the server will add records to both the authority and additional sections when generating responses. If this is set to Yes, the server will add records only to the authority section when generating responses. The performance of the server increases if this option is set to No.

Non-Authoritative: DNS data that is not served by the resident DNS server. This is the DNS data that belongs to a foreign domain and is not managed by the resident DNS administrator. This data is cached through responses to forwarded queries.

Notify: When this option is set to yes, DNS notify messages are sent when the contents of a zone for which the server is authoritative changes. The messages are sent to the servers listed in the zone's NS records (except the master server identified in the SOA MNAME field), and to any servers listed in the also-notify option.

Notify Source: Determines the local source address, and optionally the UDP port, that will be used to send notify messages. The slave should also be configured to receive notify messages from this address.

Novell Dynamic Reconfigure: Specifies the time interval at which dynamic reconfiguration will take place. The minimum value is 10 minutes and the maximum is 24 hours.

Out-of-band update: Any update to DNS Zone data in eDirectory by-passing the DNS server (that is, all updates except dynamic update).

Passive Primary Server: A DNS server that serves a primary zone and honors zone-out transfer requests. This server is passive because it cannot update the zone data. There can be multiple passive primary servers serving the same primary zone.

Passive Secondary Server: A DNS server that serves a secondary zone and does not issue inbound zone transfer requests to the primary server of the zone. It will answer queries to the zone and honors zone-out transfers requests to the zone. There can be multiple passive secondary servers serving the secondary zone.

Performance: This parameter measures the throughput of the server in handling requests and is indicated as the response time for processing concurrent requests (queries, updates, zone transfers, etc.).

Primary Zone: A zone that is authoritative and is serviced by a designated primary DNS server and one or more passive primary DNS servers.

Provide IXFR: Determines whether the local server, acting as the master, will respond with an incremental zone transfer when the given remote server, a slave, requests it. If set to Yes, incremental transfer will be provided whenever possible. If set to No, all transfers to the remote server will be non-incremental (AXFR). The default is Yes.

Query Filter: List of IP addresses or networks from which DNS server will accept query. If this option is not specified, the default is to allow queries from all hosts. The value specified for this option in the zone will override the value specified in the server.

Query Source: Specifies the address and port used for querying other name servers, if the server does not know the answer to a query.

Recursion: If this option is set to Yes, and a DNS query requests recursion, then the server will attempt to do everything required to answer the query. If this option is set to No and the server does not already know the answer, it will return a referral response.

Role: A role is an object in the iManager framework that is associated with user objects in eDirectory.

Rollback: Revert to the previous state if transaction fails.

RootSrvrInfo: The RootSrvrInfo Zone is a Zone object, an eDirectory container object that contains RRsets for the DNS Root servers. The RootSrvrInfo Zone object is the equivalent of the BIND db.root file.

Request IXFR: Determines whether the local server, acting as a slave, will request incremental zone transfers from the given remote server, a master. The default is true.

RR Set Order: Permits ordering of the records in a multiple record response in an RRset. Currently, Novell DNS server supports two orders: random-cyclic and fixed. The default is random-cyclic.

Scalability: This parameter measures how the server scales with load in terms of the number of zones, number of RRs per zone, number of DNS queries, and zone transfers or dynamic updates handled by the server in a typical deployment scenario. It also identifies the limits of the above parameters to which the server offers consistent performance without degradation.

Scope settings: Setting the scope and context of Locator object in the eDirectory tree enables better search responses for DNS-DHCP objects. This avoids searching the entire tree by limiting the search within the current scope set.

Secondary Zone: A zone that is serviced by a designated secondary DNS server and one or more passive secondary DNS servers.

Serial Query Rate: Through this option, the slave servers will periodically query master servers to find out if the zone serial numbers have changed. Each such query uses a small amount of the slave server's network bandwidth. In order to limit the amount of bandwidth used, limit the rate at which queries are sent. The value of the serial-query-rate option is an integer, which is the maximum number of queries sent per second.

Slave Server: A DNS server that answers queries from its authoritative data and cached data, but relies completely on the forwarders for external information. It does not contact other servers if the forwarders do not give it an answer. A slave server can be a primary or secondary for its authoritative data.

SNMP: Simple Network Management Protocol. For complete information, refer [RFC 1067 \(http://www.ietf.org/rfc/rfc1067.txt?number=1067\)](http://www.ietf.org/rfc/rfc1067.txt?number=1067).

Task: A task is an object in the iManager framework that is associated with a role object in eDirectory. Each task describes some action that a role can play to create, modify, or delete objects in eDirectory.

TCP Clients: Specifies the maximum number of simultaneous client TCP connections that the server will accept.

Transaction support: DNS server supports transaction for a dynamic update request. This means committing the update to eDirectory, in-memory rbt (red-black tree) database, and in the journal log. If the transaction to any of these fails, the update is rolled back and a negative response is sent to the dynamic update request.

Transfer Format: Through this option, zone transfers can be done using two different formats, one-answer and many-answers. This option is used on the master server to determine which format it sends. One-answer uses one DNS message per resource record transferred; many-answers place as many resource records as possible into a message. Many-answers is more efficient.

Transfers In: Specifies the maximum number of inbound zone transfers that can run concurrently. Increasing the transfers-in might speed up the convergence of slave zones, but it might also increase the load on the local system.

Transfers Out: Specifies the maximum number of outbound zone transfers that can run concurrently. The zone transfer requests that are in excess of the limit are refused.

Transfers per NS: Specifies the maximum number of inbound zone transfers that can be transferred concurrently from a given remote name server. Increasing the value of this option might speed up the convergence of slave zones, but it might also increase the load on the remote name server.

Transfer Source: Determines the local address that is bound to the IPv4 TCP connections used to fetch the zones transferred inbound by the server. It also determines the source IPv4 address, and optionally the UDP port, used for the refresh queries and forwarded dynamic updates.

Update Filter: List of IP addresses or networks from which the DNS server will accept dynamic DNS updates for primary zones. The default is to deny updates from all hosts. This attribute is effective only on a primary designated server.

Write-through: Writing the dynamic update data immediately to eDirectory (primary data), server in-memory, and the journal log at the time of request (that is, before replying to dynamic update request).

Zone Export: Transfers a single zone configuration/data from eDirectory into a file. This can be done using the DNS/DHCP Management utilities.

Zone Import: Transfers a single zone configuration and data from a file into eDirectory. This can be done using the DNS/DHCP Management utilities.

Zone-in: Zone data received by a secondary server from a primary server.

Zone-out: Transfer of data from a primary server to a secondary server.

Zone Statistics: If this option is set to ON, the DNS server collects statistical data on all zones in the server.