DIVISION DE EDUCACION CONTINUA
FACULTAD DE INGENIERIA, UNAM
CURSOS ABIERTOS

CURSO: *CC065 Instalación y Manejo de Redes con Netware y Productos Novell*
FECHA: *1 al 11 de octubre del 2001*

EVALUACIÓN DEL PERSONAL DOCENTE

(ESCALA DE EVALUACIÓN: 1 A 10)

CONFERENCISTA	DOMINIO DEL TEMA	USO DE AYUDAS AUDIOVISUALES	COMUNICACIÓN CON EL ASISTENTE	PUNTUALIDAD
ADRIAN MAGAÑA CISNEROS				
JUAN CARLOS MAGAÑA CISNEROS				
SAUL MAGAÑA CISNEROS				

Promedio _____

EVALUACIÓN DE LA ENSEÑANZA

CONCEPTO	CALIF.
ORGANIZACION Y DESARROLLO DEL CURSO	
GRADO DE PROFUNDIDAD DEL CURSO	
ACTUALIZACIÓN DEL CURSO	
APLICACIÓN PRACTICA DEL CURSO	

Promedio _____

EVALUACIÓN DEL CURSO

CONCEPTO	CALIF
CUMPLIMIENTO DE LOS OBJETIVOS DEL CURSO	
CONTINUIDAD EN LOS TEMAS	
CALIDAD DEL MATERIAL DIDÁCTICO UTILIZADO	

Promedio _____

Evaluación total del curso _____

1. ¿Le agradó su estancia en la División de Educación Continua?

SI [   ]   NO [   ]

Si indica que "NO" diga porqué: _____

2. Medio a través del cual se enteró del curso:

Periódico *La Jornada*	
Folleto anual	
Folleto del curso	
Gaceta UNAM	
Revistas técnicas	
Otro medio (Indique cuál)	

3 ¿Qué cambios sugeriría al curso para mejorarlo?

_____
_____
_____
_____
_____
_____

4. ¿Recomendaría el curso a otra(s) persona(s) ?

SI [   ]   NO [   ]

5. ¿Qué cursos sugiere que imparta la División de Educación Continua?

_____
_____
_____
_____
_____
_____

6 Otras sugerencias

_____
_____
_____
_____
_____

DIPLOMADO EN REDES Y TELECOMUNICACIONES

TECNOLOGIAS DE LA INFORMACION

INSTALACION Y MANEJO DE REDES CON NETWARE

Y PRODUCTOS NOVELL

OCTUBRE DEL 2001

INSTALACION Y CONFIGURACION NETWARE 5.0

INSTALACION Y

CONFIGURACION

El Directorio de Mayor
Implantación en el mercado

¡Más de
40.000.000 de
usuarios!

NDS™

NOVELL DIR/TORY SSERVICES

Novell

'TRODUCCIÓN

Si los ordenadores y las redes son tan inteligentes, ¿Por qué no son más conscientes de ellos mismos, por qué no se ocupan de si mismos, y, por qué tengo que saber tanto para utilizar una red? Construir, gestionar, utilizar, incluso substituir su red actual es un proceso caro y complejo.

Probablemente esté planificando, o quizá ya lo haya hecho, construir una intranet corporativa, o crear una extranet con socios comerciales de confianza o hacer conexiones con Internet y mientras hace todo esto, tiene que gestionar el almacenamiento de ficheros, servicios de impresión, de fax, de mensajería o de colaboración en sistemas existentes.

¿No le gustaría poder hacer estos cambios utilizando su tecnología actual, al tiempo que simplificar todos los desafíos a los que se enfrenta a la hora de gestionar la tecnología que utiliza hoy? ¿Parece demasiado bueno para ser cierto? Bien, emerge una tecnología que hace que todo esto sea posible· los servicios de directorio.

En un futuro próximo, se oirá hablar mucho sobre servicios de directorio y cómo estos reducirán la complejidad y el coste total de propiedad de una red. Queremos que conozca este importante salto en el mundo del networking y como, hoy en día, éste está ya disponible.

Para hacerle descubrir más sobre servicios de directorio, vamos a tratar los siguientes aspectos:

Visión de la informática en red (network computing)

¿Qué es, en términos informáticos, un servicio de directorio?

Los componentes de su red y cómo un directorio puede a..narlos

Las prestaciones o ventajas de una red compatible NDS

Servicios de red basados en NDS

Grandes redes, escalables y compatibles NDS

Construir NDS según estándares

Desarrollo de las aplicaciones compatibles NDS

La prueba de que no hacemos vanas promesas

La visión de un entorno que sea seguro, universal, de fácil manejo e integrado con todo es algo que merece la pena investigar. Nos hemos asociado con los líderes mundiales del sector del networking, para compatibilizar, en el ámbito de directorio sus soluciones de red. La vida se vuelve más sencilla.

OTRO SALTO IMPORTANTE E IMPRESCINDIBLE EN LA INFORMÁTICA

Ya hemos visto el futuro. Si nos fijamos en la ciencia-ficción , encontramos una gran visión de la Informática. Hay series de televisión que nos llevan hacia el futuro, en cientos de años, y nos muestran cómo deben funcionar los ordenadores. *"Ordenador, ¿Dónde está Ensign Berk?"*, *"Ordenador, me apetece una taza de té jarvariano,"* o bien, *"Ordenador, inicializa la secuencia autodestructiva Alpha 4069."*

Todas estas órdenes futuristas requieren. que el ordenador sepa quién está hablando. que conozca los privilegios de acceso de esa persona a la información y también sería muy importante que esta persona pudiera enviar esas peticiones desde cualquier parte, incluso desde un planeta lejano Además, el ordenador debe tener acceso a la base de datos de la empresa, base de datos personal.. .-Todas las órdenes se realizan con muy poca intervención personal o premeditación. Simplemente suceden.

Sun Microsystems declara, con razón: *"El ordenador es la red"*. Quizá se pueda decir lo mismo de la informática espacial del futuro. Quizá el Capitán de Starship está realmente hablando con una red cuando pregunta. *"Ordenador, ¿Cuánto falta para que la estrella Zertoc se convierta en una estrella enana?"*. Si esta es la visión, y la visión es ciencia-ficción, ¿Cuáles son los elementos que faltan para hacer realidad de la ficción?

Tiene que ser algo que conozca como son las relaciones entre las personas y las máquinas. y entre una máquina y otra. Si no es así· ¿Cuál es la ventaja de las redes?. Este eslabón perdido es un servicio de directorio integrado, en todos los niveles de la red corporativa

El objetivo general es tener disponibles para todas las personas, todos los servicios necesarios de red, y conseguir llegar a un punto. en el que sea la red quien trabaje para uno. En otras palabras. una red tan sencilla que los usuarios no se tengan que preocupar de dónde están sus recursos. o si estos van a estar disponibles cuando los necesiten. Todo es invisible para el usuario y muy fácil de gestionar para el administrador. Esto es lo que nuestro Presidente. Eric Schmidt califica como *"mi mundo"*. Poseer nuestro propio mundo de información y recursos y poder elegir lo que se quiere compartir. cuando se quiera y con quien se quiera.

La lógica futurista que declara que *"las necesidades de la mayoría pesan más que las necesidades de unos pocos"*, es de lo que se trata el *networking*.

Sin embargo, en la vida real, las necesidades de unos pocos, a menudo, tienen prioridad ante las necesidades de la mayoría. Sólo unos pocos tienen el privilegio de utilizar la nueva tecnología, hasta que es lo suficientemente sencilla, generalizada y económica como para que todo el mundo se beneficie de ella. Simplemente, piense en el nacimiento de los ordenadores. Al principio los ordenadores eran enormes, unos cacharros caros hechos con tubos de vacío, y, solamente las personas que construían los ordenadores podían utilizarlos. Después llegaron los mainframes, miniordenadores, las estaciones de trabajo, los PCs, y ahora estamos hablando de la Informática en Red *(Network Computing)*. Con cada nuevo hito informático, los ordenadores se hicieron más complejos en su diseño pero menos caros y más fáciles de utilizar. Las interfaces de usuario se desarrollaron de la misma manera. Comenzaron con tarjetas perforadas, después llegaron los lenguajes crípticos, luego el ratón y los entornos con windows. Cada avance tecnológico, acerca la tecnología al usuario. El *Networking* está pasando por el mismo ciclo. Primero fueron unas terminales torpes, conectadas a ordenadores mainframe, que sólo eran accedidos por unas cuantas personas. Después, los PCs independientes fueron conectados en Redes de Area Local, donde más personas podían entender y utilizar la red. Hoy en día, con Internet, intranets y extranets se puede navegar a través de enormes cantidades de información y colaborar con personas de todo el mundo. Sin embargo, todavía no estamos en el mundo de "enchufar y utilizar" a la hora de imprimir por Internet, realizar conexiones seguras o compartir información con un grupo restringido de personas. Cada paso, nos acerca a la visión de una red personal e invisible, a la que llamamos "mi mundo". El siguiente paso hacia delante es la labor de los servicios de directorio.

¿VICIOS DE DIRECTORIO

Definir un servicio de directorio es sencillo, definir lo que supone para su red no lo es tanto. Pero le vamos a presentar una forma fácil de pensar en lo que es un directorio:

Una base de datos de objetos. Una base de datos de usuarios, aplicaciones, dispositivos de red, y otros recursos que se pueden encontrar en una red. Un servicio de directorio, por lo menos en parte, es una base de datos orientada a objetos que representa a los usuarios y recursos de la red. Dentro de cada objeto se almacena información específica sobre el usuario individual o el recurso de la red. Los objetos son jerárquicamente estructurados en un árbol de directorio que proporciona la plataforma que puede adaptarse a la forma en la que su negocio está organizado.

Gestiona relaciones. Cada usuario y recurso tiene relaciones con otros usuarios y recursos de la red. Un directorio controla las relaciones entre las personas y las máquinas, y entre unas máquinas y otras. Las dos formas en las que un directorio gestiona las relaciones son la autenticación y la autorización. Respecto a la autenticación, tanto el usuario como los componentes de la red, tienen que identificarse uno al otro para garantizar que ambos son quienes dicen ser y para evitar que alguien se introduzca para robar información. Respecto a la autorización, una vez que el usuario está autenticado, la red permite al usuario autenticado, gestionar o utilizar los recursos de la red a los que tiene derecho. Los derechos son distribuidos globalmente, a nivel de la organización, o entre grupos de trabajo, y después, gestionados por excepción a nivel de usuario individual.

NETWORKING COMPATIBLE NDS

Un servicio de directorio integrado prolonga todos los componentes de su red. Para hacerse una idea mejc de cómo un directorio se adapta a su red, piense en una red que consta de:

- ELEMENTOS FÍSICOS: BANCOS DE MODEMS, SERVIDORES DE ACCESO, ROUTERS
- SISTEMAS OPERATIVOS COMO INTRANETWARE, UNIX, NT
- APLICACIONES QUE SE EJECUTAN EN LA RED.
- SERVICIOS QUE MEJORAN EL TRABAJO DE LAS PERSONAS EN LA RED Y QUE TRASCIENDEN TANTO A LA INTRANET COMO A INTERNET
- INTRANET E INTERNET PARA HACER NEGOCIOS Y NO SOLO PARA PUBLICIDAD

Un servicio de directorio flexible, poderoso y seguro es lo que une a todos los niveles de la red y hace que esta sea fácil de usar y fácil de gestionar. Y NDS es el único servicio de directorio que abarca todos esos aspectos de su red, permitiendo una única identificación de entrada, un único punto de administración y la plataforma sobre la que los diseñadores puedan construir.

LAS VENTAJAS DE SER COMPATIBLE CON NDS

Las ventajas son sencillas porque hacen que su vida sea menos complicada Haciendo que las cosas sean más sencillas, se reduce el coste de propiedad.

- LOGIN ÚNICO

Se hace login una sola vez, utilizando una contraseña, después se recibe un acceso fácil y rápido a los recursos de la red a los que se está autorizado El acceso a los recursos después del login es realizado automáticamente mediante la autenticación de background. Decimos background porque uno no se da cuenta que está teniendo lugar el proceso de autenticación Su entrada en el sistema es la misma, independientemente de donde esté físicamente emplazado en la red NDS permite acceder a sus aplicaciones, archivos, impresoras, servicios y otros recursos desde cualquier ubicación geográfica y puede recibir una visualización constante de la red, independientemente de su estación de trabajo.

La estructura de base de datos jerárquica del NDS reduce el tráfico en la red y hace que sus búsquedas y operaciones sean rápidas y eficaces Puede encontrar un recurso requerido de red buscando o navegando en el árbol, con servicios de Novell u otros

- PUNTO DE ADMINISTRACIÓN ÚNICO

Un estudio del Gartner Group reveló que, el 79 por ciento del coste total de propiedad de una red consiste solamente en los gastos de administración.

Sin una red compatible de directorio, a menudo, necesitar desempeñar las mismas operaciones múltiples veces, tanto para cada usuario como para cada servidor NDS elimina la necesidad de administración redundante, proporcionando un punto único de administración para toda su empresa NDS reduce el coste total de gestión y mantenimiento de la red Se puede gestionar toda la red desde una única ubicación y con una única utilidad de administración

Además, NDS permite libertad en la gestión. En la mayoría de las organizaciones existe la necesidad , tanto de administración centralizada como de administración distribuida. Muchos de nuestros clientes centralizan los servicios de administración y de gestión, comunes a distintos departamentos. Y el resto de la administración se delega, en el ámbito de departamento o grupo de trabajo. Con ambos planteamientos de administración, solo necesita utilizar una herramienta: NWAdmin, para gestionar todos los recursos de la red

SEGURA

Usted desea un entorno de red seguro. Afortunadamente, puede construir toda una gama de control de seguridad y acceso con el NDS. NDS le permite, de una forma rápida y fiable, definir los derechos de seguridad asociados a una rama en particular del árbol de directorio, y todos los objetos dentro o por debajo de esa rama, heredan esos derechos. Este tipo de administración basado en reglas, simplifica la seguridad, por lo que solo las excepciones a la norma requieren una atención especial. La seguridad basada en reglas reduce, en gran medida, los costes de administración y evita el último coste, que su información sea conocida por su competencia.

NDS utiliza un servicio de autenticación basado en la llave pública/llave privada RSAde tecnología de encriptación. Este mecanismo de autenticación utiliza un atributo de llave privada y firma digital, para verificar la identidad del usuario. La autenticación está orientada a sesiones y la firma del cliente solo es válida durante la sesión existente. La autenticación continua o de background es transparente y tiene lugar cuando se accede a otros servicios. Solamente durante el login inicial (identificación del usuario e intercambio de contraseña), el usuario participa en el proceso de autenticación.

- TOLERANCIA A FALLOS Y ACCESIBLE

NDS es una base de datos totalmente distribuida y replicada. Pero, ¿Por qué debería importarle esto?

Segmentando la base de datos NDS, en partes gestionables (partición) y distribuyendo esta segmentación por la red (replicación) se logra tolerancia a fallos. Además, los datos NDS pueden colocarse, cerca de los usuarios que los necesitan, por lo que se obtiene un rendimiento óptimo cuando se accede a la red.

Las particiones NDS son copiadas o replicadas por toda la red, tantas veces como sea necesario. Si se pierde una partición primaria o master, la red comienza a utilizar otras copias de la partición Este directorio dinámico aumenta la fiabilidad de la red y permite que cuando falle el servidor, se haga mantenimiento del mismo, o se produzca la pérdida de un enlace de comunicación, los usuarios no se vean afectados. Las ventajas de mantener una red constante y capaz de recuperarse de un desastre, son infinitas para las redes actuales.

- A LA MEDIDA DEL CLIENTE

La estructura de un árbol de directorio se regula mediante el esquema de directorio, que es un sistema de reglas que define como se estructura el árbol de directorio Por ejemplo: qué objetos pueden definirse, qué atributo puede asociarse con objetos, qué propiedades heredan los objetos, y qué posiciones ocupan los objetos en el árbol de directorio Por ejemplo, un objeto usuario puede ampliarse para incluir un número de la seguridad social o un número de teléfono de contacto de emergencia. También, se pueden añadir servicios de terceros, como funcionalidad de servidor de fax en la red, añadiendo un objeto servidor de fax y la aplicación, en el árbol de directorio

- ESCALABLE

NDS puede ser adaptado a cualquier tipo y tamaño de red. Incluso en el caso de fusión con otra empresa y de continuo crecimiento en el futuro, NDS se acomodaría, fácilmente, a su crecimiento Añadir nuevos recurso es tan sencillo como un clic en el ratón y dado que NDS tiene una replicación tan poderosa, se puede obtener una red de una escalabilidad sin límites.

NOVELL APPLICATION LAUNCHER

Novell Application Launcher funciona junto al NDS para simplificar la gestión de las aplicaciones de la red, permitiéndole gestionar centralmente las estaciones de trabajo de los usuarios. Se pueden instalar nuevas aplicaciones en la red o actualizar las aplicaciones existentes y conseguir que los iconos de aplicación aparezcan de forma dinámica, en los desktops de los usuarios de Windows. Novell Application Launcher hace que sea más fácil para el usuario ser independiente de su ubicación

Novell Application Launcher conoce las aplicaciones y recursos necesarios para su trabajo, por lo que se puede ir a cualquier parte de la red, y al entrar al sistema se obtiene el acceso necesario, independientemente de la máquina que se está utilizando para entrar

Novell Application Launcher utiliza el NWAdmin para darle la posibilidad de crear objetos NDS que representan a las aplicaciones en la red.

Estos objetos contienen información sobre la ubicación física de las aplicaciones y sobre qué usuarios ha autorizado para utilizar esas aplicaciones. Sin tener que abandonar la estación de trabajo, puede enviar las aplicaciones a las estaciones de trabajo de los usuarios por toda la red, haciendo por tanto, que la distribución de software sea más fácil y rápida. Y no necesitará visitar cada estación de trabajo de los usuarios, para instalar las aplicaciones.

- SERVICIOS LDAP PARA NDS

Un grupo de personas de la Universidad de Michigan se dió cuenta de que si podían reducir la sobrecarga de la especificación X.500 Directory Access Protocol, podrían extraer la misma información del directorio más rápidamente, y con clientes más pequeños y llamaron a esta nueva especificación de protocolo, Protocolo Ligero

Acceso al Directorio (Lightweight Directory Access Protocol) (LDAP_RFC 1777). Estos servicios para NDS v1 le permiten publicar fácilmente información sobre su empresa en su intranet e Internet, al tiempo que mantiene el control mediante el NDS, sobre quien puede acceder a su información El mejor ejemplo de una aplicación compatible LDAPes su navegador Web, Netscape Communicator o Microsoft Explorer

Debido a que ya existen aplicaciones compatibles con LDAP, puede publicar información de su directorio corporativo a cualquier persona

El nombre Lightweight Directory Access Protocol sugiere que existe detrás, un directorio accesible, ¿no es así?. En este punto aparece NDS para proporcionar el mejor directorio LDAPdisponible en el mundo.

- SERVICIOS RADIUS PARA NDS

Los servicios RADIUS para NDS v1 representan el poder de NDS gestionando el nivel de hardware o software de su red, a través de bancos de modems, routers de acceso, y servidores de acceso. El Servicio de Autenticación de Dial-in de Usuario (RADIUS), es un estándar emergente del Grupo de Trabajo de Ingenieros de Internet (IETF) que ha sido adaptado por Novell y otros proveedores líderes de hardware de "router y dial-in" Con los servicios RADIUS para NDS, NDS se convierte en la única base de datos necesaria para servidores de acceso remoto de toda la red. Proporciona un punto único de autenticación (verificación del nombre y contraseña del usuario) y autorización para acceder o administrar los recursos de la red.

CONSTRUIDOS SEGÚN ESTÁNDARES

• NDS Y X 500

NDS es un servicio de directorio de funcionalidad integral que está basado en el estándar internacional X 500 La Organización Internacional de Estándares (ISO) y el Comité Consultivo Internacional sobre Telegrafía y Telefonía (CCITT), crearon el X.500 para proporcionar estándares que capacitaran la creación de un servicio de directorio auténticamente interoperativo y distribuido, a nivel mundial. De hecho, Sara Radicati, fundadora del grupo Radicati; una consultoría sobre servicios de directorio, declara en su libro "NDS utiliza la Tecnología X.500 de Servicios de Directorio e Implantación con la exacta especificación de diseño X.500 para el modelo de numeración, base de datos de directorio y operaciones de servidor a servidor. Sí. Todas las características y funciones descritas en el estándar X.500 son implementadas en NDS. Sin embargo, NDS ofrece una importante funcionalidad más allá de la especificación X.500, mediante una estructura completa de networking que enlaza a los usuarios con servicios de red, aplicaciones e información". A pesar de que NDS está estrechamente alineado con el X.500, existen algunas diferencias entre ambos, diferencias que residen en los protocolos utilizados en el NDS y no en la arquitectura. Novell eligió utilizar los protocolos ligeros (light protocols) en lugar del pesado Sistema Abierto de Interconexión (OSI), definido por X.500. Ya que las diferencias solo existen en los protocolos, es fácil ofrecer soluciones interoperativas para que NDS y X.500 puedan interoperar, al máximo de sus posibilidades

Asimismo, merece la pena destacar que dado que NDS está basado en X.500, y LDAPestá basado en el protocolo de acceso al directorio X.500, NDS y LDAPforman un gran equipo sinérgico, debido a su común alineación.

CONCLUSIÓN

Una red que es invisible para el usuario y que comienza a autogestionarse. Sin embargo, el objetivo está cerca con el nuevo planteamiento encaminado hacia servicios de directorio. "Mi mundo", donde todo está accesible y donde se puede gestionar y colaborar libremente con los demás, es el resultado directo de un servicio de directorio integrado. Todas las ventajas derivadas de una red compatible NDS simplifican su vida, le ahorrarán mucho dinero y crearán un entorno para el futuro de la informática distribuida

Novell

Meet System and Software Requirements

System Requirements

NetWare 5 requires the following minimum system requirements:

- A server-class PC with a Pentium* or higher processor.
- A VGA or higher resolution display adapter (SVGA recommended).
- 550 MB of available disk space (50 MB for a boot partition, 500 MB for a NetWare partition).
- 64 MB of RAM (128 MB recommended to run Java*-based applications).
- One or more network boards.
- A CD-ROM drive that can read ISO 9660-formatted CD-ROM disks. Computers with bootable CD-ROM drives must fully support the El Torito specification.

A PS/2* or serial mouse is recommended, but not required.

NOTE: The system requirements listed above are minimum requirements. You can optimize the server performance by increasing the amount of server memory, disk space, and processor speed.

Software Requirements

Before installing, make sure that you have the following software and information:

- DOS 3.3 or later. (DOS 7 is included on the NetWare 5 License diskette. Do not use the version of DOS that ships with Windows 95*, Windows 98, or Windows NT operating systems.)
- DOS CD-ROM drivers.
- NetWare 5 Operating System CD-ROM.
- NetWare 5 License diskette.
- Novell® Client for DOS and Windows 3.1x (optional, for installing from a network).
- An IP address (optional, if the server will connect to the Internet). For information on receiving an IP address, contact your Internet service provider (ISP).
- Network board and storage device properties, such as the interrupt and port address. For more information, contact your computer hardware manufacturer.

Next, you should prepare the network to receive a NetWare 5 server. If this server is not being integrated into an existing network, you can skip to Prepare the Computer for Server Installation.
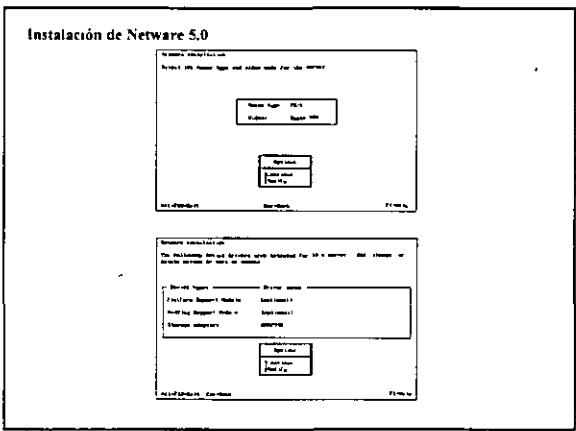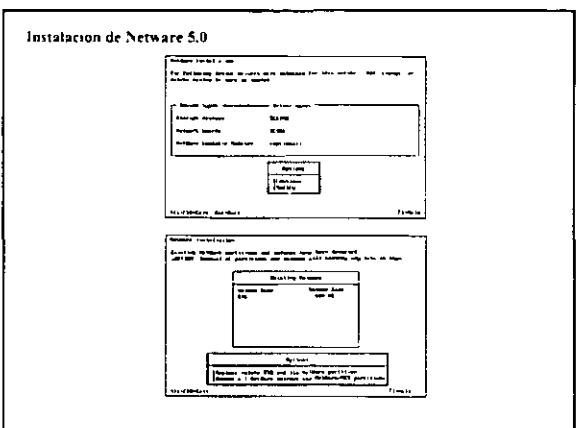
Instalación de Netware 5.0
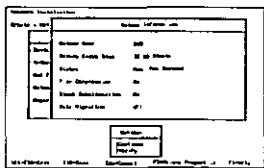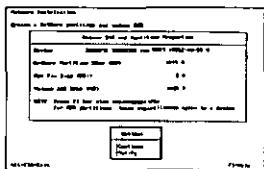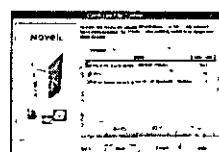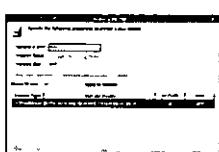
Instalación de Netware 5.0

Instalacion de Netware 5.0

Instalación de Netware 5.0

Instalación de Netware 5.0

Instalacion de Netware 5.0

2

Instalación de Netware 5.0

Instalación de Netware 5.0

Instalación de Netware 5.0

3
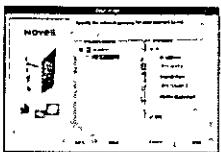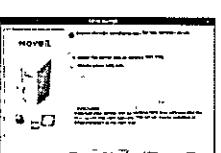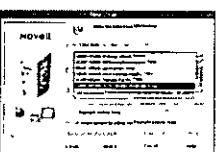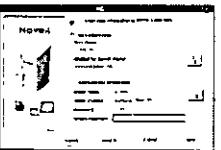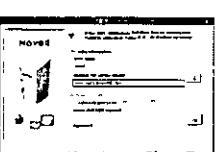
Instalación de Netware 5.0
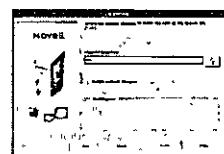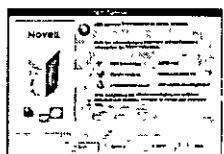
Instalación de Netware 5.0
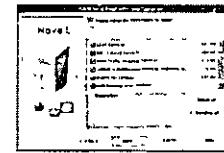
Instalación de Netware 5.0
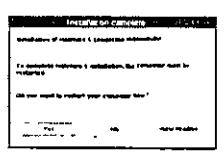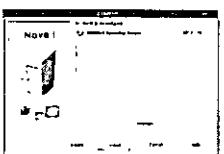
Instalación de Netware 5.0

Directory Services

NDS™ is the most mature and powerful directory service available. It is the directory service of choice for large enterprises around the world. It lays the foundation for the powerful management features in NetWare®.

NDS lets you associate network resources with objects in a database. You can then manage each network resource without leaving your desk

Network Resource Objects

You can manage every network resource from your desktop.
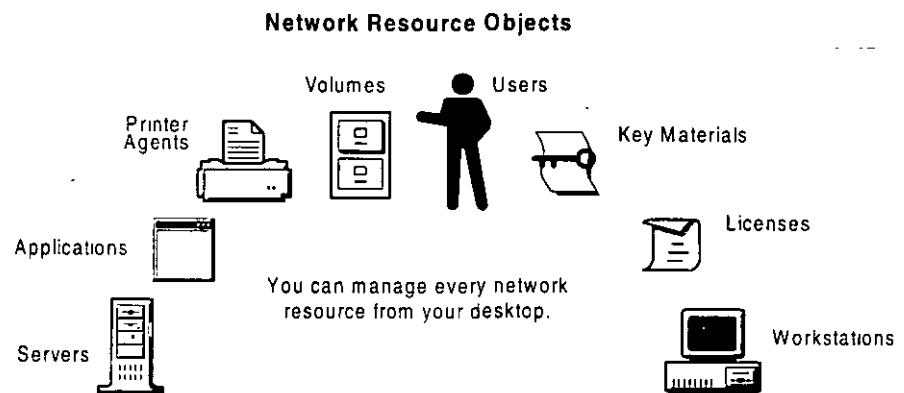
The network resource objects shown above are called "leaf" objects. They are found at the ends of branches in the NDS tree structure.

In contrast to leaf objects, container objects are the branches in the NDS tree structure. They contain leaf objects and other container objects. Container objects create a hierarchy that provides logical access to leaf objects

Benefits to Network Users

NDS provides network users a single login to the network. Once they have entered their login name and password and have been authenticated to the network, every network resource to which they have been granted rights is available to them, whether it's the printer across the aisle or the server on the other side of the world.

Furthermore, if you install Z.E.N.works, users' network and desktop environment settings are stored in NDS and are used to re-create their working environment wherever they log in to the network.

And if you are leveraging the power of Novell® Distributed Print Services™, network users can have bidirectional communications with network printers to which you have granted them access. See "Print Services" on page 29 for details.

Benefits to You and Your Organization

NDS is the foundation upon which Novell's suite of network management tools is built. NetWare 5 includes a number of powerful NDS-integrated management tools. For example.

◆ If you need to optimize WAN traffic, use WAN Traffic Manager to control the flow of NDS synchronization traffic across WAN links.

◆ If you need faster access to specific NDS information that exists on more than one partition, or if you need to speed up access to NDS object information located across WAN links, use Catalog Services to create and automatically update a local catalog of frequently accessed NDS objects.

As you work with NDS, you will discover ways to leverage the network resource information stored in it. For example, you might decide to store network user or workstation information in NDS, publish it on your intranet, and allow network users to keep it current using their Web browsers and LDAP Services for NDS.

Other Novell products also leverage the power of NDS

◆ If you have NT application servers on your network, consider using NDS for NT. This will save you the time and expense of managing trust relationships and pass-through authentication among domains.

◆ If you want to manage e-mail access and work flow from within NDS, consider the features and power of GroupWise®, yet another award-winning application from Novell.

Above all, be sure to take advantage of breakthrough NDS-integrated management tools and NDS features included in NetWare 5, as shown in the following illustration.

Volumes

Users

Printer
Agents

Key Materials

Licenses

Applications

Intranet

Internet

Servers

Workstations

NDS

Manage your network with breakthrough
management tools

Z.E.N.works manages the
relationship between
network users and their
workstation desktops.

Novell Security Services
manages all aspects of
ensuring trusted and
secure data transfers on
the Internet.

.NDPS creates and manages
network printers and automatically
installs printer drivers on users'
workstations.

Novell Licensing Services
manages and monitors the use of
licensed software on your network

IP management tools greatly
increase the manageability
of your IP network

.Role-based management·
offloads less critical
administration tasks
such as password
administration.

Requirements for Using NDS

NDS is tightly integrated and installed with the NetWare 5 server.

Each NetWare 5 server installation requires you to make decisions regarding your configuration of NDS. If your network will have fewer than 1,000 objects (users and resources), you can accept the default settings provided by the installation utility

If you have a large network or are upgrading from a version of NetWare prior to NetWare 4™, you will want to read more about installing and optimizing NDS. The Installation section of this manual contains basic guidelines and issues to consider.

In addition, see Contents > "Directory Services" in your NetWare 5 online documentation for details regarding all aspects of NDS

Print Services

Novell Distributed Print Services™ (NDPS) is the default and preferred print system in NetWare 5. NDPS™ supports IP-based as well as IPX-based printing.

Novell's legacy, queue-based print system is also fully supported in NetWare 5, allowing users to print as they always have until you complete the transition to NDPS.

Note ▼ This section contains only a brief overview of NetWare 5 print services. We urge you to view the "Multimedia Introduction to NDPS" and related links located in your NetWare 5 online documentation.

About Novell Distributed Print Services

NDPS was designed to manage modern, networked printers and to exploit the new functionality they offer. As a result, NDPS will greatly reduce your network printing management costs by providing

♦ Centralized, simplified, single-point administration for all your network printing resources

♦ Bidirectional, real-time communication between administrators/users and the printer regarding printer or job status

♦ Configurable event notification

♦ Tight integration with NDS

♦ Tight integration with management features of printer hardware

♦ Automatic printer driver download and installation

♦ Support for existing printers and other output devices

♦ Compatibility with non-Novell clients and platforms

NDPS Benefits to Network Users

With NDPS, when a user installs a printer, the printer driver is automatically downloaded and configured.

NDPS also allows network administrators to designate printers to be installed automatically when users log in to the network.

NDPS offers bidirectional communication with network printers from client workstations. Users can

♦ Inquire about the real-time status of a print job, the availability of a printer, or a printer's capabilities and current configuration.

♦ Give special instructions regarding print jobs they submit.

♦ Request that the printer notify them when specific events occur.

	is the printer available?	printer is available
	what is the printer's status?	toner is low
	what features are available?	duplex, tabloid-size, color, . . .
	how many copies are printing?	five copies
	what media is being used?	upper tray, transparency
	is the job finished?	job has printed

Network user or administrator
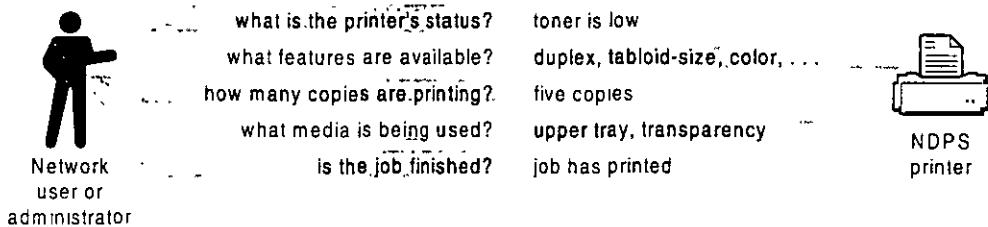
NDPS printer

NDPS Benefits to You and Your Organization

The following features will save you time.

NDPS Feature	Explanation
Bidirectional Communication	Clients and printers exchange real-time information such as job and printer status, printer features and configuration properties, job hold and scheduling information, and copies being printed.

NDPS Feature	Explanation
Streamlined Printer Creation	You need only attach the printer to the network, create an NDS Printer Agent, and grant access to network users. Some third-party gateways and embedded solutions provide automatic plug and print functionality.
Automatic Printer Driver Download and Installation	NDPS provides a printer driver database from which drivers can be downloaded and installed to workstations automatically. You can also add drivers to the database
Remote Management via NetWare Administrator	Through NetWare Administrator, you can manage all printing resources as controlled NDS objects, or you can maintain certain printers as public access printers available to everyone.
Configurable Event Notification	You specify who should be notified of a problem or event and how (pop-up message, e-mail, log file record, or a third party mechanism such as beeper notification).
	This includes notification of real time printer status such as paper mis-feeds. Some vendors even provide animated graphics of their printers to ease remote troubleshooting.

Requirements for Using NDPS

There are no hardware requirements to consider when evaluating the benefits of NDPS. There are, however, some planning issues to understand as explained in the following sections.

Printer Access Options

Any printer, regardless of its hardware type or connection mode, can be configured as either a controlled access printer or a public access printer.

The following table compares the two access methods.

Table 2-2
Differences between Controlled Access Printers and Public Access Printers

Issue	Controlled Access Printers	Public Access Printers
Integration with NDS	Associated as an NDS Printer object.	Not associated as an NDS Printer object.
Availability	Available to network users through NDS rights.	Available to everyone on the network. Can be made automatically available through third-party gateways or embedded solutions.
Administration	Created and administered through NetWare Administrator as NDS objects.	Require minimal administrative action. Managed through the Tools menu of NetWare Administrator.
Network security	Full range of network security options through NDS	No network security.
Event notification	Full range of event and status notification options including e-mail, pop-up windows, event logs, and third-party methods, such as beepers and faxes.	Provide only job event notification.

Protocol Support

NDPS is protocol independent. It can be used in an IPX-based environment. a pure IP environment. or a combination of both. Third-party gateways being developed to work with NDPS are also protocol independent

Compatibility Issues

NetWare 5 provides an enhanced client to take full advantage of NDPS features. Clients that are-not NDPS-aware can print to NDPS printers but can't take advantage of all NDPS features.

NDPS is fully compatible with all types of printers. whether or not they have been configured to take advantage of the advanced features NDPS offers.

NDPS backward compatibility ensures that all of your current printers configured with NPRINTER, queue-based technology, LPR, or RP continue to function just as they always have.

About Queue-Based Network Printing

The following table compares queue-based print services with NDPS.

Table 2-3
Differences between NDPS and Queue-Based Print Services

Task	Queue-Based Print Services	NDPS
Setting Up	Administrators create and link print queues, printers, and print servers. All three objects are maintained' separately.	Administrators create and maintain Printer Agents, allowing users to submit print jobs directly to printers. All management functions are centered on the printer itself.
Submitting a print job	Users submit jobs to queues	Users submit jobs to printers
Communicating with printers	Communications are one-directional. Event notification is via pop-up windows.	Communications are bidirectional. The only limit is the printer's capability. Event notification is configurable, including e-mail, pop-up windows, event logs and third-party methods, such as beepers and faxes.
Creating Printers	Administrators must create and configure Printer objects manually Plug-and-print is not available.	For certain printers, administrators need only plug the printer onto the network to create a public-access printer. Any printer can be configured for either public access or controlled access (See Table 2-2, "Differences between Controlled Access Printers and Public Access Printers.")
Third Party Enhancements	Does not accommodate add-ons or extensions from third parties.	Has an extensible framework for print devices, including administrative console snap-in interfaces. Several printer vendors have already created custom snap-ins to fully represent the features available with their own devices.

A detailed overview of the mechanisms involved in queue-based
printing is found in Contents > Print Services > *Queue-Based Printing* in
the NetWare 5 online documentation.

Licensing Services

Novell Licensing Services (NLS) help you manage and monitor the use of licensed software in your NDS network.

NLS includes Novell's implementation of the LSAPI standard. NLS is designed to help network administrators ensure compliance with software licensing agreements.

Novell Licensing Services is tightly integrated with NDS to facilitate

♦ The interaction between software and the licenses that allow it to run.

♦ Your ability to manage that interaction and monitor licensed software usage on your network.

NetWare 5 includes two tools you can use to install software licenses and monitor and manage license usage·

♦ **NLS Manager**—a stand-alone tool that lets you monitor and manage all aspects of configuring your licensing services, including generating reports on license usage.

♦ **NLS snap-in**—a NetWare Administrator snap-in that lets you do everything NLS Manager does except generate reports on license usage.

Note NetWare 5 connection licenses are managed through NLS. You can increase your NetWare 5 connections by purchasing additional licenses and installing them using NLS Manager or NetWare Administrator. For more information, contact your Novell Authorized Reseller representative.

Understanding NLS

You can think of NLS in terms of three basic components· NLS clients.
License Service Providers (LSPs), and License container objects in NDS.

NLS Clients

Ensuring compliance with license agreements requires confirmation of
an available license *before* software is used

In NLS this compliance is accomplished by the software making a
request for a license before the software runs. Any software that makes
a license request is referred to as an "NLS client."

If software is license-enabled. NLS client functionality is built in. and
the software can request a license, receive a response to the request. and
execute only if a license is available.

If an application is not license-enabled. you can configure Z.E.N.works
to act as an NLS client on behalf of the application.

License Service Providers (LSP)

The NLS client locates a license by contacting a License Service Provider
and asking it to check whether a license is available

A License Service Provider is simply an NLM called NLSLSP that runs
on a NetWare 4.11 or later server

To use NLS, you must have one or more LSPs in your NDS tree. The LSP
receiving the request searches the NDS tree for a license appropriate to
the software.

First it locates an NDS object called a License container object that
corresponds to the software. Then it asks the License container object
whether it has any available licenses for the software.

If the License container object has no available licenses. the LSP
continues its search until it has either found a license or contacted all
License container objects in the tree

License container objects

The License object contains NDS leaf objects called License Certificate objects, which represent software licenses. Each License object contains License Certificates for only one piece of software.

Stored with the License container object in NDS is information such as how many licenses the License object contains, what kind of licenses they are (single-use, multiple-use, etc.), and how many licenses are currently in use.

NLS Graphical Summary

NLS component functionality is illustrated by the following:
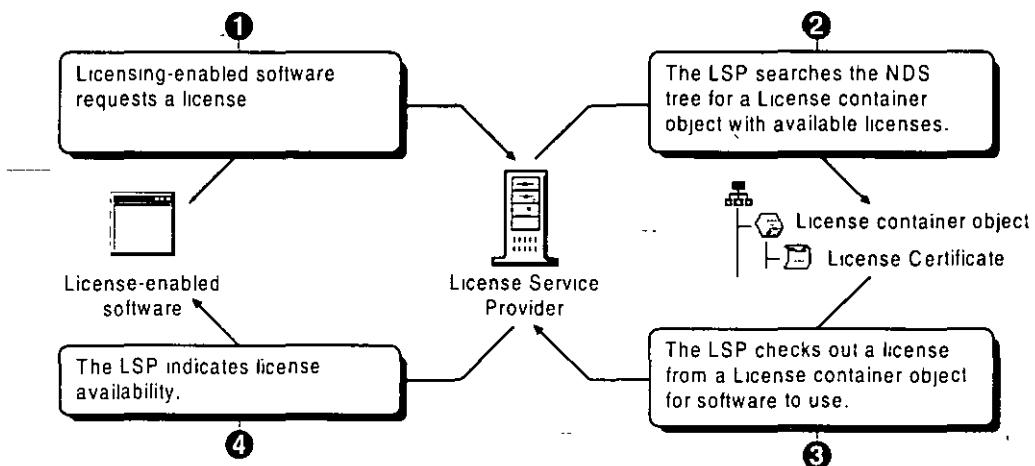
Benefits to Network Users

NLS will help your network users be certain they are using only licensed software.

Benefits to You and Your Organization

NLS allows you to manage and monitor the use of licensed software as shown in the following illustration.

Novell Licensing Services

Applications   -Workstations
Servers

NDS

Manage and monitor licensed software on
your NDS network

See at a glance your level
of compliance with
licensing agreements

Control the use of
software, allowing only
approved users
access to it.

Track software usage in the
company, by departments, and by
individuals.

Track information helpful to
passing industry and government
audits concerning licenses.

Optimize software purchase budgets by tracking
software usage so you buy only the number of
product licenses you need

Requirements for Using Licensing Services

To use Novell Licensing Services you must

♦ Ensure NLS is installed on your network. (By default, when you install a NetWare 5 server or upgrade from NetWare 3 or NetWare 4, NLS is installed on that server.)

♦ Install or create License Certificates in the appropriate NDS context.

♦ For each NDS partition, ensure that at least one server with a master or secondary replica is functioning as a License Service Provider (nlslsp.nlm is running on the server).

♦ Configure Z.E.N.works to function as the NLS client for non-license-enabled applications you want to manage.

For further information see Contents > *Novell Licensing Services* in the NetWare 5 online documentation.

Separating the protocols on network segments reduces the traffic on both segments. IPX packets such as RIP and SAP are kept on the IPX segment, while IP packets remain on the IP segment.

Domain Name Service (DNS)

Domain Name Service (DNS) is the functionality that matches text names, such as novell.com, with numbers used by computers, such as 123.45.67.89.

If you have an existing domain naming system already installed on your network, enter the Domain Name and Name Server(s).

Note ▼ If you want to install Novell's DNS on your network, you must return to the Summary screen and install Novell DNS/DHCP Services in Other Products and Services.
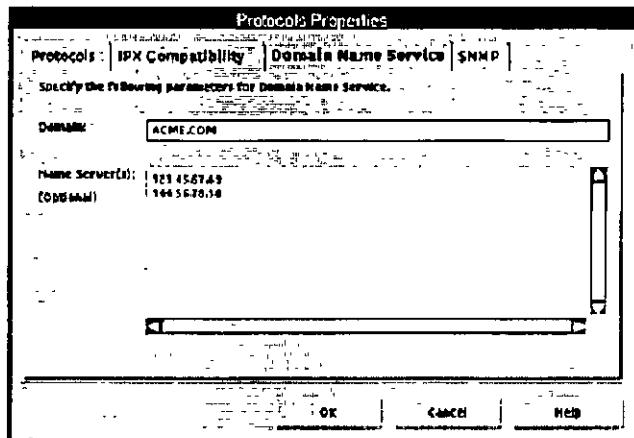
◆ Domain Name—Domain names divide the Internet into functional categories. The top level domains identify types of organizations such as commercial (com), educational (edu), government (gov), international entities (int), U.S. military agencies (mil), network providers (net), and other organizations (org).

Domain names can also use two-letter country codes to specify geographical locations such as United States (us) or United Kingdom (uk).

158 Overview and Installation

Domain names are separated into individual levels with periods, such as sales.acme.com or acct.acme.ut.us.

♦ Name Server(s)—In addition to domain names, DNS manages domain name servers. A name server is a computer that translates names into IP addresses for other devices, such as workstations on the network. To obtain the name. NetWare 5 will search the IP address of each name server in the sequence entered into the Name Server field.

Hint ▼ Enter the IP address of the name server(s)

Simple Network Management Protocol (SNMP)

Network management utilities such as Novell's ManageWise® utility use Simple Network Management Protocol (SNMP) to record and communicate information about network devices. Using an SNMP-compatible utility, you can set and monitor threshold levels and specific events such as packets per second or error rates.

When an event occurs, information such as event type, hardware description, server name, server location, and network administrator name is recorded. The information is then sent to the destination address of the workstation running the SNMP-compatible management utility.
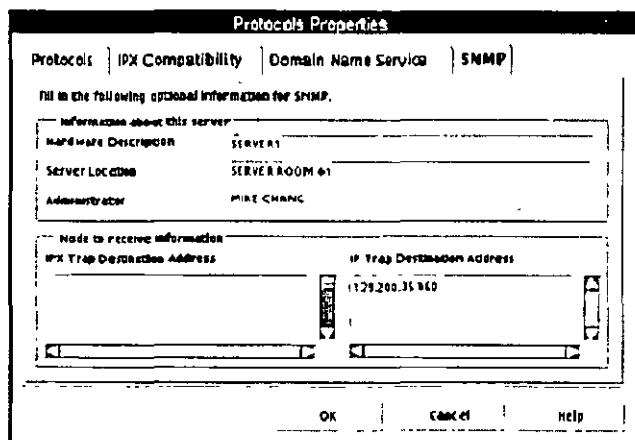
DNS/DHCP Management Console

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

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

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

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

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

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

Installing the DNS/DHCP Management Console

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

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

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

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

1. Map a drive to the SYS: volume on a server on which you have installed NetWare 5.

2. Click Start, then select Run.

3. Use the browse button to select the drive mapped to the SYS: volume on the selected server. Then select the Public and DNSDHCP folders.

4. Double-click Setup, then click OK in the Run dialog box.

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

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

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

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

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

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

Using the DNS/DHCP Management Console

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

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

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

- DNS and DHCP server objects
- DNS Zone object
- Subnet container object
- Subnet Pool object

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

Managing DNS

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

ᶜyou are using Dynamic DNS (DDNS), when a client receives an address assignment from the ᴅHCP server, a request is made to update NDS. The only way to override DDNS is by using the

DNS/DHCP Management Console.

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

Managing DHCP

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

Deciding which DHCP options to use depends on your implementation. Refer to "DHCP Options" for information about available DHCP and BOOTP options.

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

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

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

Events and Alerts

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

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

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

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

Auditing Server Activity

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

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

Refer to "Configuring DNS Auditing" for information about configuring a DNS server for auditing. Refer to "Configuring DHCP Auditing" for information about configuring a DHCP server for auditing.

Server Status

Server status is represented by the server icons displayed in the lower pane of the DNS/DHCP Management Console. Figure 4-1 shows icons representing two DNS servers. The server icon on the left indicates that this server, DNS_SJF-TPUBS1, is operational. The red slash through the server icon on the right indicates that the server might not be operational.

Figure 4-1.
Server Status

DNS_SJF-TPUBS1   DNS_SJF-TPUBS2
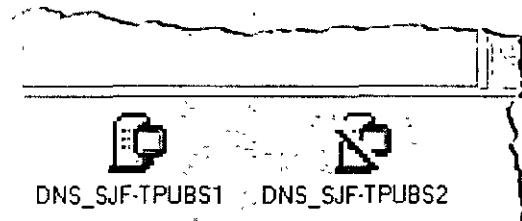
Even though the server icon has a red slash through it, the server might still be operational. If the DNS/DHCP Management Console is unable to establish communications with the server, perhaps because of telecommunications problems, the utility displays the red slash through the server icon. In Figure 4-2, the operation of the DNS server on the right, DNS_JAPAN, has been suspended.

Figure 4-2.
Server Operation Suspended

DNS_CANADA   DNS_JAPAN

Configuring DNS

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

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

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

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

Importing DNS Configuration Information

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

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

1. Launch the DNS/DHCP Management Console by double-clicking the icon.

2. Click the DNS Service tab.

3. Click Import DNS Database.

    The Import-File Input window is displayed, requesting the location of the DNS BIND Master file.

4. Enter the drive and path to the DNS database file, or click the browse button to navigate your way to the file.

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

5. Click Next.

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

6. Select the Zone Context and click Next.

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

8. Click Import.

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

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

Setting Up DNS

This section provides the basic steps required to set up DNS. This section does not describe how to enable all the available features. For detailed configuration information, refer to "Detailed DNS Configuration."

Prerequisites

The following steps must be completed before setting up DNS:

1. Install Novell® NetWare 5 on the selected server or servers.
2. Load the Novell Client software delivered with NetWare 5 on client computers that will be used to administer DNS and DHCP.
3. Install the DNS/DHCP Management Console on client computers that will be used to administer DNS and DHCP. For detailed information about installing client software, refer to "Installing the DNS/DHCP Management Console."

Logging In to the Tree

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

To login to the tree, complete the following steps:

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

   The NetWare Client login dialog box is displayed.

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

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

Launching the DNS/DHCP Management Console

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

The first time you launch the DNS/DHCP Management Console, you are prompted to enter the name

of the NDS^{TM} tree where you want to set up DNS. You can click in the Enter NDS Tree Name field to select an NDS tree that you are logged in to.

Creating a DNS Server Object

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

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

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

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

2. Click Create on the tool bar.

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

3. Select DNS Server and click OK.

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

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

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

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

Creating a Primary DNS Zone Object

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

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

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

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

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

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

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

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

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

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

6. Click Create.

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

Starting the DNS Server

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

LOAD NAMED

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

Configuring Clients to Use DNS

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

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

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

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

2. Select TCP/IP, then click Properties.

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

3. Click the DNS Configuration tab.

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

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

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

Detailed DNS Configuration

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

Creating a DNS Name Server Object

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

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

1. Click Create on the tool bar.

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

2. Select DNS Server and click OK.

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

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

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

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

Modifying a DNS Name Server Object

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

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

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

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

The DNS Server IP Address field contains the addresses of any DNS servers assigned to this zone.

This field is read-only and is received from the DNS Server.

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

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

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

Creating a Zone Object

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

Creating a Secondary DNS Zone Object

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

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

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

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

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

5. Under Zone Type, select Secondary.

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

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

   You can optionally select to assign an authoritative DNS server.

7. Click Create.

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

Creating an IN-ADDR.ARPA Zone Object

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

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

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

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

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

3. Select Create IN-ADDR.ARPA.

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

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

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

6. Under Zone Type, select Primary or Secondary.

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

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

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

8. Click Create, then click Save.

Creating an IP6.INT Zone Object

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

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

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

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

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

3. Select Create IP6.INT.

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

5. Under Zone Type, select Primary or Secondary.

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

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

7. Click Create, then click Save.

Modifying a Zone Object

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

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

1. Select the Zone object you want to modify.

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

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

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

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

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

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

- Zone master
- E-mail address
- Serial number
- Interval values
    - Refresh (default is 180 minutes)
    - Retry (default is 60 minutes)
    - Expire (default is 168 hours)
    - Minimal caching (default is 24 hours)

Creating Resource Records

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

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

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

   The Create New DNS Object window is displayed.

2. Select Resource Record and click OK.

   The Create Resource Record dialog box is displayed, prompting you for the domain name of the resource record you want to create. You can select the A record (the default) to create an Address record or the CNAME record to create a canonical name,-or you can check the Others box to create a resource record from the displayed list of supported resource record types. Table 2-2 provides a complete list of supported resource records and their fields. The information required for each resource record depends on the resource record type.

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

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

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

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

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

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

Modifying Resource Records

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

Configuring DNS Features

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

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

Configuring an NDS Server to Forward Queries to Root Name Servers

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

Configuring a Cache-Only Server

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

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

Configuring to Support Child Zones

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

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

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

Configuring DHCP

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

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

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

Importing DHCP Configuration Information

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

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

1. Launch the Management Console by double-clicking the icon.

2. Click the DHCP Service tab.

3. Click Import.

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

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

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

5. Click Next.

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

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

7. Select the Subnet Context and click Next.

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

9. Click Import.

10. The Server Input window is displayed, prompting you to select a default NCP server to manage

the newly imported subnet.

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

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

Setting Up DHCP

This section provides basic information about the steps required to set up DHCP. This section does not describe how to enable all the available features. For more information refer to "Detailed DHCP Configuration."

Prerequisites

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

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

Logging In to the Tree

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

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

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

   The NetWare Client login dialog box is displayed.

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

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

Launching the DNS/DHCP Management Console

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

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

Setting Global DHCP Options

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

To set global DHCP options, complete the following steps:

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

2. Click Global Preferences on the Tool Bar.

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

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

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

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

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

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

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

5. Click the DHCP Options Table tab.

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

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

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

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

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

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

Creating a DHCP Server Object

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

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

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

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

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

2. Click Create on the Tool Bar.

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

3. Select DHCP Server and click OK.

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

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

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

Creating a Subnet Object –

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

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

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

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

2. Click Create on the Tool Bar.

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

3. Select Subnet and click OK.

   The Create Subnet dialog box is displayed. For each subnet you create, enter the following information in the fields provided: subnet name, NDS context, subnet address, and subnet

mask. If you have setup a default DHCP server, its name is displayed and can be changed.

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

4. Enter the required information, then click Create.

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

Creating Subnet Address Ranges

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

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

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

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

    The Create New DHCP Record dialog box is displayed.

3. Select Subnet Address Range and click OK.

    The Create New Subnet Address Range dialog box is displayed.

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

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

Creating IP Address Objects

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

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

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

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

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

The Create New DHCP Object dialog box is displayed.

3. Select IP Address and click OK.

   The Create IP Address dialog box is displayed.

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

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

Starting the DHCP Server

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

LOAD DHCPSRVR

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

Configuring Clients to Use DHCP

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

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

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

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

2. Select TCP/IP and click Properties.

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

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

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

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

Detailed DHCP Configuration

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

Refer to "Setting Up DHCP" for information about setting up DHCP and creating DHCP objects. The following sections provides detailed information about modifying DHCP objects.

Modifying a DHCP Server Object

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

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

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

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

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

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

Modifying an Existing Subnet Object

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

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

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

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

You can also modify the subnet's default DHCP Server on the Address tab page and enter up to 256

characters of information in the Comments field.

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

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

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

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

Modifying a Subnet Address Range Object

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

The following range type options are available:

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

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

Modifying an Existing IP Address Object

Refer to "Creating IP Address Objects" for information about creating IP Address objects. After an IP Address object has been created. its detailed information window displays three tab pages:

- Address
- Usage
- Other DHCP Options

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

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

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

- 20, Serial Line
- 21, Asynchronous Transfer Mode (ATM)

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

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

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

Creating a Subnet Pool Object

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

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

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

1. Click Create on the tool bar.

2. Select Subnet Pool and click OK.

3. Enter a unique name for the Subnet Pool object.

4. Use the browse button to select the NDS context in which to create the Subnet Pool object.

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

Modifying a Subnet Pool Object

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

Web Services

The NetWare 5 product package includes

♦ The Netscape* FastTrack* Server for NetWare, a powerful Web server you can install on a NetWare 5 server.

♦ Support for the major Web scripting languages so you can leverage your scripting expertise in creating customized server-side applications.

Netscape FastTrack Server for NetWare

Your NetWare 5 server can function as an extremely fast and efficient intranet and/or Web server.

Netscape FastTrack Server for NetWare delivers

- The fastest single-processor Web server available
- Better performance than 80 percent of dual-processor Web servers tested by SPEC
- Dramatic price-performance advantages over slower dual-processor solutions

Netscape FastTrack
Server for NetWare
software loaded

NetWare 5 Server

Note ▼ The performance statistics listed in this graphic are based on recent benchmark tests conducted by the Standard Performance Evaluation Corporation (SPEC).

Benefits to You and Your Organization

With no additional investment in hardware or software, you can install a Web server to benefit network users and your company. For example.

♦ You can create a company intranet to provide network users with easy access to company news, department information, company policies and procedures, and other information they need in order to be more efficient and productive.

♦ You can create a Web server to publish company information on the Internet.

Requirements for Using Netscape FastTrack Server for NetWare

To install the Netscape FastTrack Server from the CD included in the NetWare 5 product package, you must have the following system resources:

♦ A Windows 95 or Windows NT 4.0 client machine that

♦ is running the appropriate Novell 32-bit Client.

♦ Is running a Netscape 3 or later browser.

♦ Has a CD-ROM drive.

♦ Has 100 MB free disk space (for use only during the install process).

♦ A target NetWare server that

♦ Is running NetWare 4.11 or a later version.

♦ Has at least 32 MB of free RAM (64 MB is recommended).

♦ Has at least 100 MB free disk space on the sys volume.

For more information regarding the Netscape FastTrack Server for NetWare, see Contents > Web Services > "Netscape FastTrack Server for NetWare. Getting Started" in the NetWare 5 online documentation.

Scripting and Component Support in NetWare 5

NetWare 5 supports the major scripting languages available, including

- Perl 5

- NetBasic* 6.0

- NetBasic 7.0 (a VB Script-compatible language)

- JavaScript*

Java* programmers can write servlets using the LCGI servlet Gateway running alongside the Netscape FastTrack Server for NetWare. In addition, pre-built NetBasic 7.0 components, Java Beans, and ActiveX controls make it easy to assemble powerful and effective network applications.

Using the development environment of choice, web scripters and RAD developers can quickly and easily embed network services into Web pages and construct server-side applications that leverage the security and power of NetWare.

Benefits to Network Users

Scripting languages and reusable components afford server and Web developers the power, versatility, and compatibility to respond to the needs of network users.

Developers can incorporate NDS, login and authentication, file management, printing, Oracle* and Btrieve* database management, and other NetWare services into network solutions tailored to the specific needs of the enterprise. Timely and targeted network solutions allow both the end user and network developer the ability to be more productive.

Benefits to You and Your Organization

NetWare 5 scripting and component services offer you choice, compatibility, and speed.

You can choose the best scripting option to run on the fastest network and Web server. The Netscape FastTrack Server for NetWare running on

NetWare 5 delivers twice the performance of its closest competitor. And by using the scripting and component technology that fits you best, you not only leverage your current network and scripting investment, you also leverage your existing development expertise.

Requirements for Using Scripting Services

Requirements depend on your scripting choice.

♦ Support for NetBasic 6.0 and Perl 5 scripting is available on the NetWare 5 CD.

♦ JavaScript components are installed with the Netscape FastTrack Server for NetWare (included in the NetWare 5 product package).

♦ NetBasic 7.0, and the LCGI servlet Gateway for Java are available on the Novell developer Web site.

To obtain these, go to http://developer.novell.com and follow the appropriate links to the kits and download area. Download the Web Services pack.

You will need to subscribe to DeveloperNet and obtain a password. There is no charge for DeveloperNet services