Setup of Windows Server 2003 and Networking with Active Directory in the Network Laboratory (III)

Hiroshi NOTO

Contents

Section 6. Management of Active Directory

6.1. Active Directory Components

The Active Directory[3]-[7] is a networked-object store and service, that locates and manages resources, and that makes these resources available to authorized users and groups. The Active Directory is comprised of two primary components each of which has its logical and physical structures, respectively. The basic logical componens of the Active Directory are objects and their associated attributes. **Object classes** are merely definitions of the object **types** that can be created in the Active Directory. The **schema** is the Active Directory mechanism for storing and adding object classes which present object definitions. Active Directory objects are organized around a hierarchical **domain model** of which building blocks are **domain, domain trees, forests, organizational units,** and schema.

The Active Directory manages a hierarchical structure of networked computers with the domain as its foundation. A domain comprises computer systems and network resources that share a logical security boundary. They are viewed as groupings of resources or servers that use a common domain name, known as a

Key Words : Windows Server 2003 R2, Business-to-business(B2B) Integrated Network System, Active Directory and Domain Model, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP)

namespace. In our case, for example, all servers or resources in the **keijou.local** namespace belong to a single domain.(1)

To facilitate information storage and replications the Active Directory uses three types of data store for directory partitions, each of which is replicated as a separate unit according to its own schedule. The three Active Directory partitions are: Schema data, Configuration data, and Domain data. The **Global Catalog** (**GC**) is an abstraction of object information contained in the Active Directory data store.

When multiple domains share a schema, security trust relationships, and Global Catalog, a domain tree is created, defined by a common and contiguous namespace (Figure 6.1). For example, all domains with the ending namespace of **keijou.local** belong to the **keijou.local** domain tree. A domain tree is formed through the expansion of **child domains** (e.g. **A.keijou.local** and **B.keijou.local**). The first created domain is known as the **root domain** (in our case, **keijou.local**), which contains the configuration and schema data for the tree and the forest.

The second component of the Active Directory is the physical structure, which holds the mechanisms for data communication and replication. The physical structure constitutes Active Directory **sites** (see below) and the physical server that stores and replicates Active Directory data known as the **domain controller** and the related **Global Catalog**. A domain controller is a server that contains a copy of the Active Directory. The domain controller organizes all the domain's object data in a logical and hierarchical data store, authenticates users, provides responses to queries about network objects and replicates directory services. Each domain and each site should have more than one domain controller if possible so as to provide logical and physical structure redundancy and fault tolerance.

Trust relationships can be formed between domain trees with different namespaces. In this case, we say "A domain forest is created." The domain forest allows the company or the organization to have different domain names, such as "**keijou.local**" and "**keijou.com.**" All trees in the forest share a number of attributes, including a Global Catalog, configuration, and schema. A forest is simply a reference point between trees and does not have its own name.

The endpoint of any tree branch is an object; the branch is typically viewed as a **container** for multiple objects: a container is a special class that has both a namespace and attributes. Domains and child domains can be *internally* divided into administrative substructures known as organizational units (OUs) that act as containers and can be nested within other OUs. For example, **a.A.Keijou.local**, **b.A.keijou.local**, and **a.B.keijou.local** may be defined as organizational units and **x.a.B.keijou.local** within **a.B.keijou.local** as a suborganizational unit (see Figure 6.1).

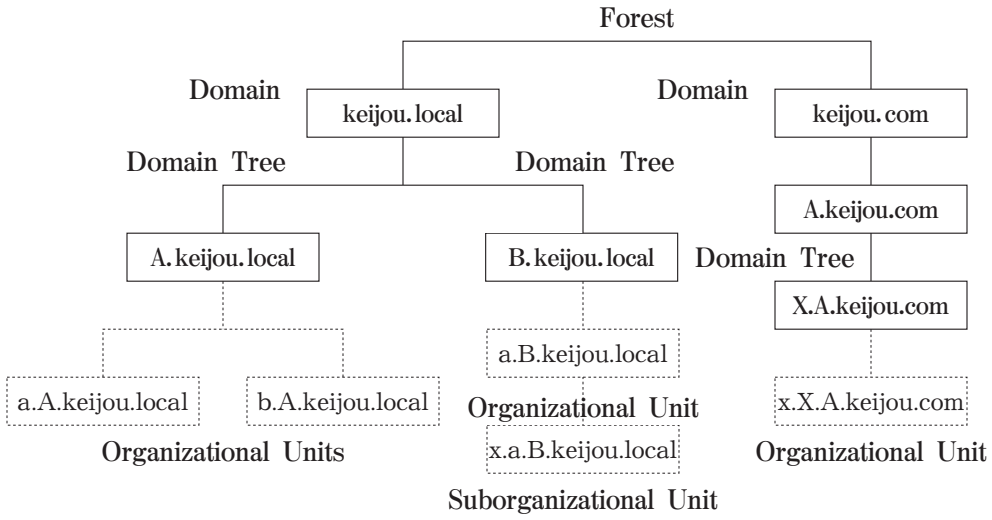

Figure 6.1 Example of a Domain Forest's Domains, Domain Trees and Organizational Units

Geographic and/or traffic limitations or others result in the need to create smaller networks, known as subnets, to facilitate communication within and between locations. The physical network structure of the Active Directory is based on a unit known as a **site**. A site is a set of well-connected subnets. The role of the administrator is to design sites that ensure the greatest network performance. Sites differ from domains: sites represent the physical structure, or topology of our network, while domains represent the logical structure of our organization,

Active Directory installation requires DNS installation. The Active Directory may be fully installed without DNS which can be installed later on such a domain controller using the "Configure Your Server" tool.

6.2. INSTALLATION OF DNS (Domain Name System) Server

Active Directory uses Domain Name System (DNS) to locate domain controllers, enabling computer joining the network to obtain a domain controller's IP address, and then to begin the process of network authentication.

As described in (I)*) we install the DNS server on our server computer. Therefore in the setup of the Active Directory we assign IP address "192.168.0.1" of our server to the **Preferred DNS server** field (Figure 6.2).

---

*) Hereafter the series of our articles "Setup of Windows Server 2003 and Networking with Active Directory in the Network Laboratory" [1],[2] will be abbreviated as (I) and (II), for example.

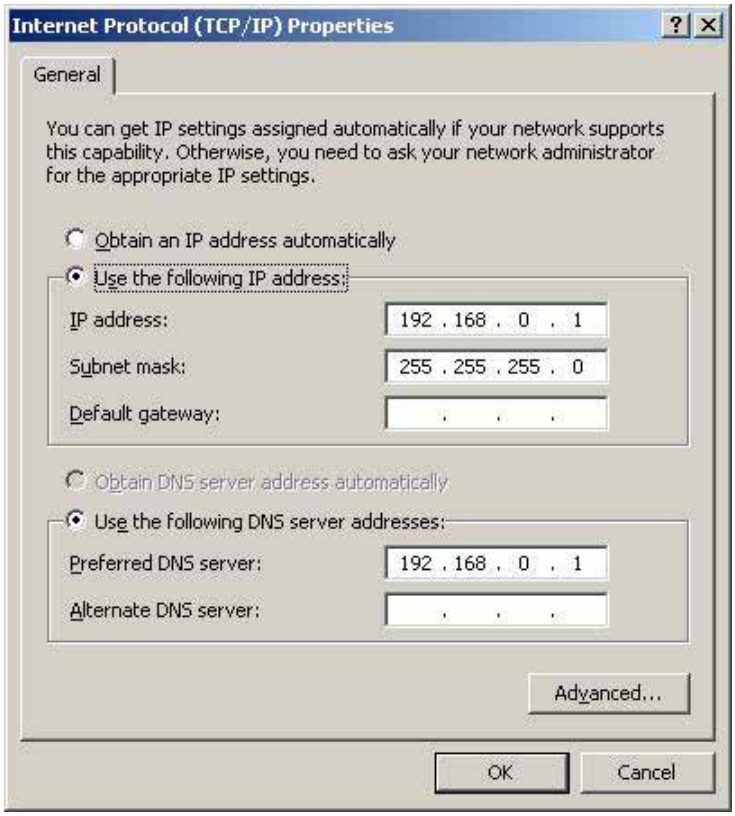

Figure 6.2 DNS Server's IP Address as our Server Computer's IP Address

SERVER-SIDE DNS CONFIGURATIONS

Through "Configure Your Server" pages, we install and configure a local DNS server on the computer where the Active Directory directory service is running.

1. In the **Select Configuration Action** window, select **Create forward and reverse lookup zones** (Figure 6.3).
2. In the **Forward Lookup Zone** window, select **Yes, create a forward lookup zone now** (Figure 6.4).
3. In the **Zone Type** Window, select **Primary zone**. Ensure that the **Store the zone in Active Directory** box is checked (Figure 6.5). This will make the DNS server integrated with Active Directory.

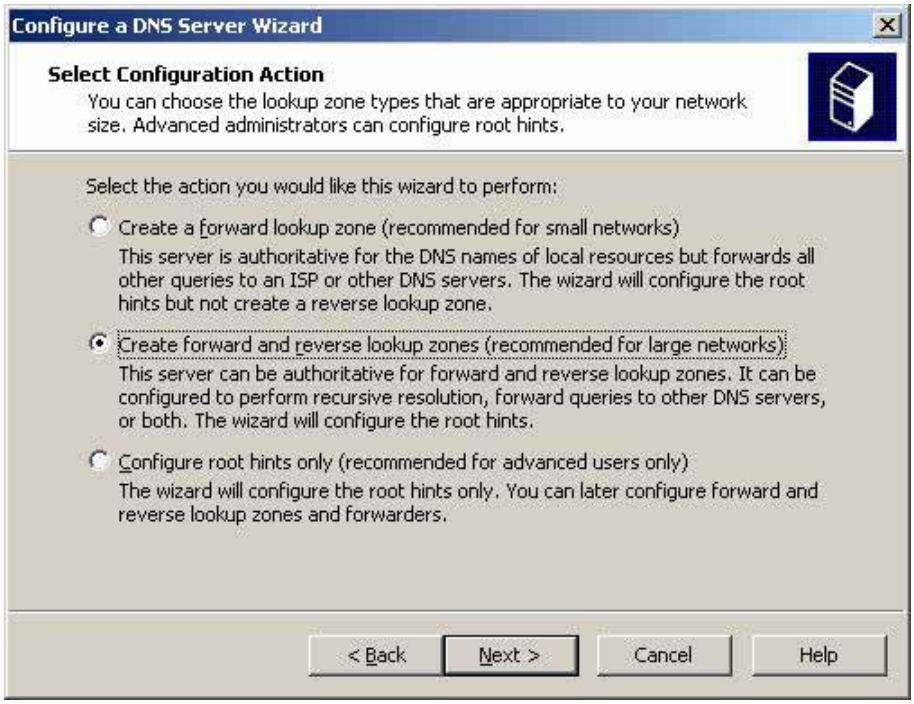

Figure 6.3 Create Forward and Reverse Lookup Zones

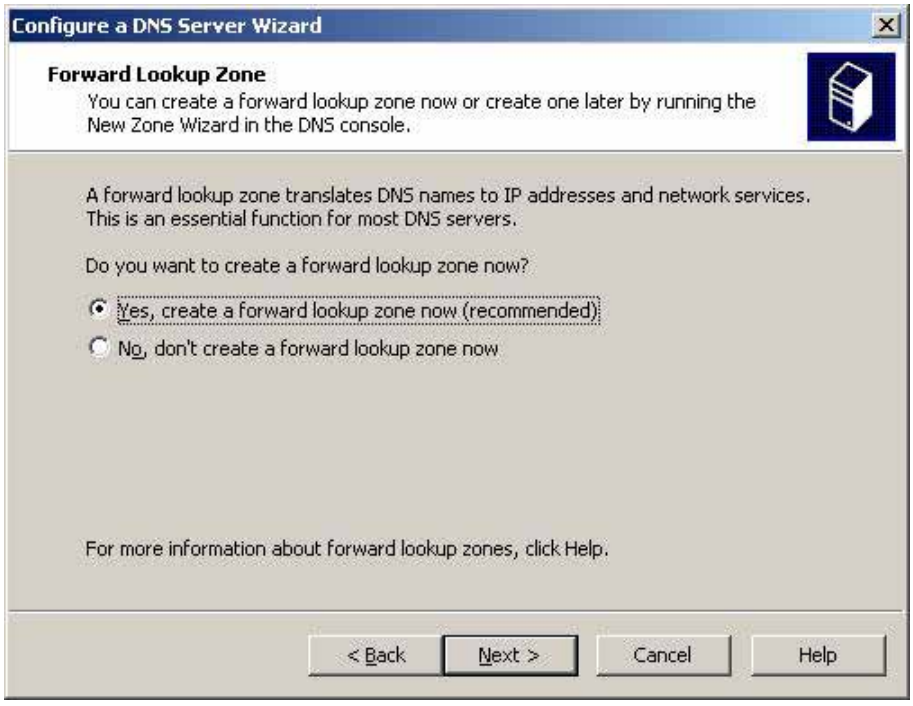

Figure 6.4 Create a Forward Lookup Zone

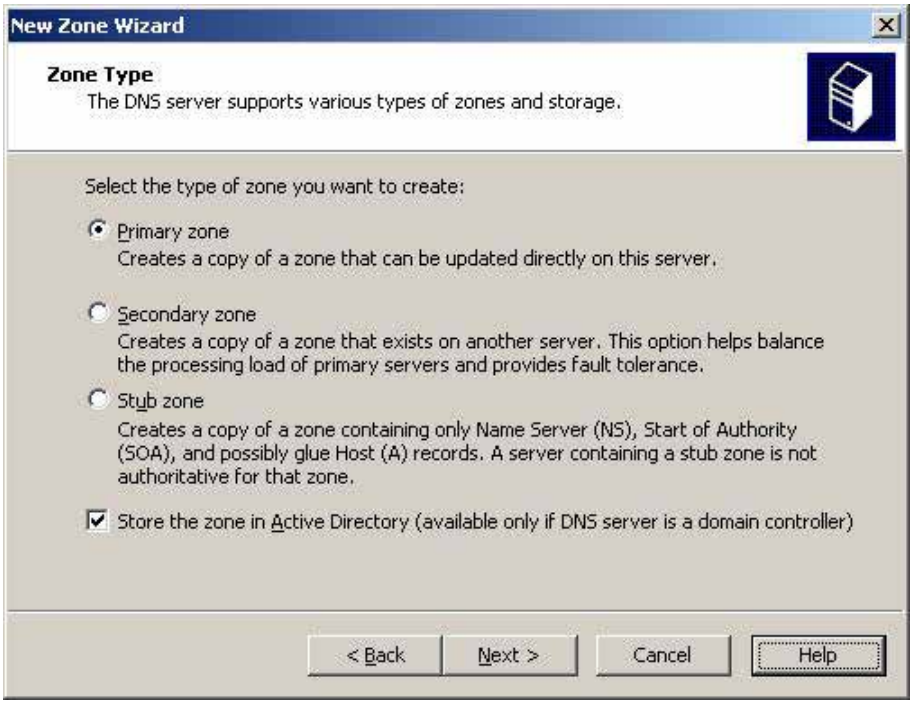

Figure 6.5 Primary Active Directory Integrated DNS Zone

In the same way we select the following items and enter the names for their fields.

4. Replicate to all domain controllers by selecting **All domain controllers in the keijou.local Active Directory domain** (Figure 6.6).

5. Enter the full DNS name for the new DNS zone (Figure 6.7).

6. We select, at the the moment, **Allow both nonsecure and secure dynamic updates** (Figure 6.8).

7. Select **Yes, create the reverse lookup zone now** (Figure 6.9).

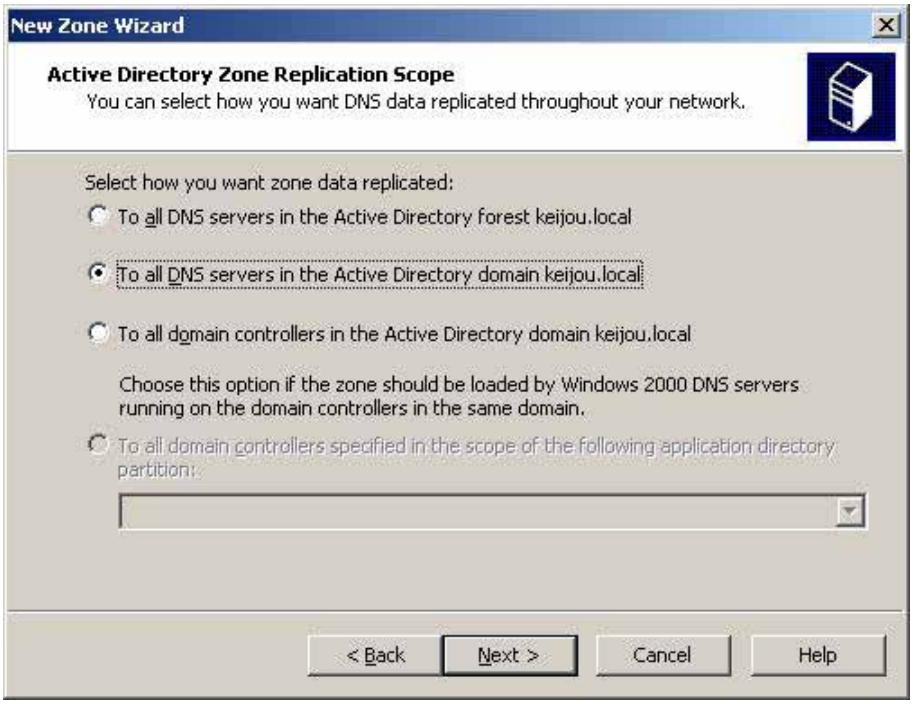

Figure 6.6 Replicate to all Domain Controllers

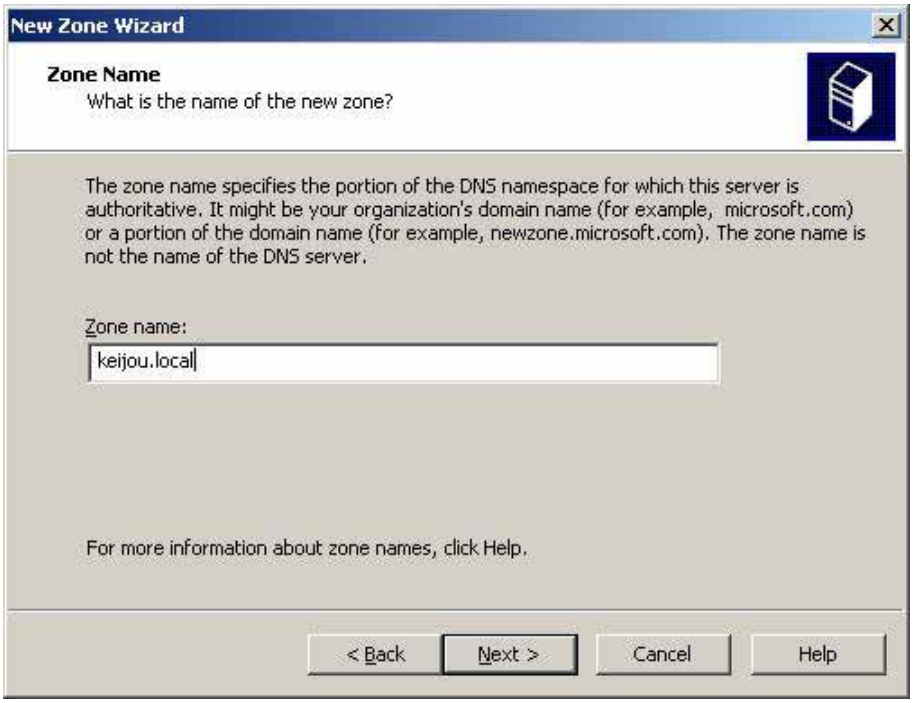

Figure 6.7 The full DNS name for the New DNS Zone

Figure 6.8　Nonsecure and Secure Dynamic Updates

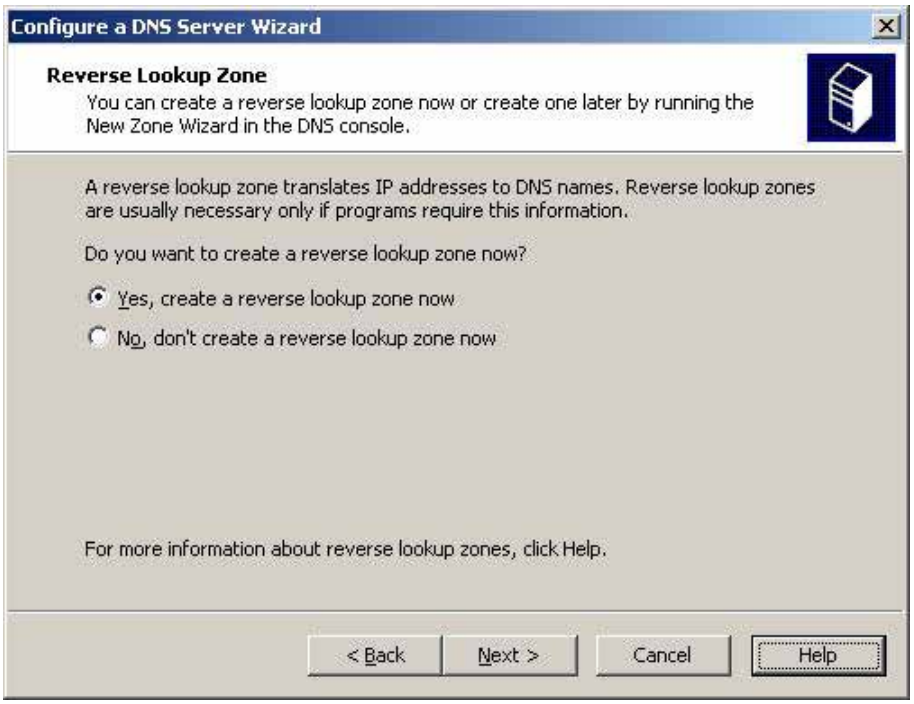

Figure 6.9　Create the Reverse Lookup Zone

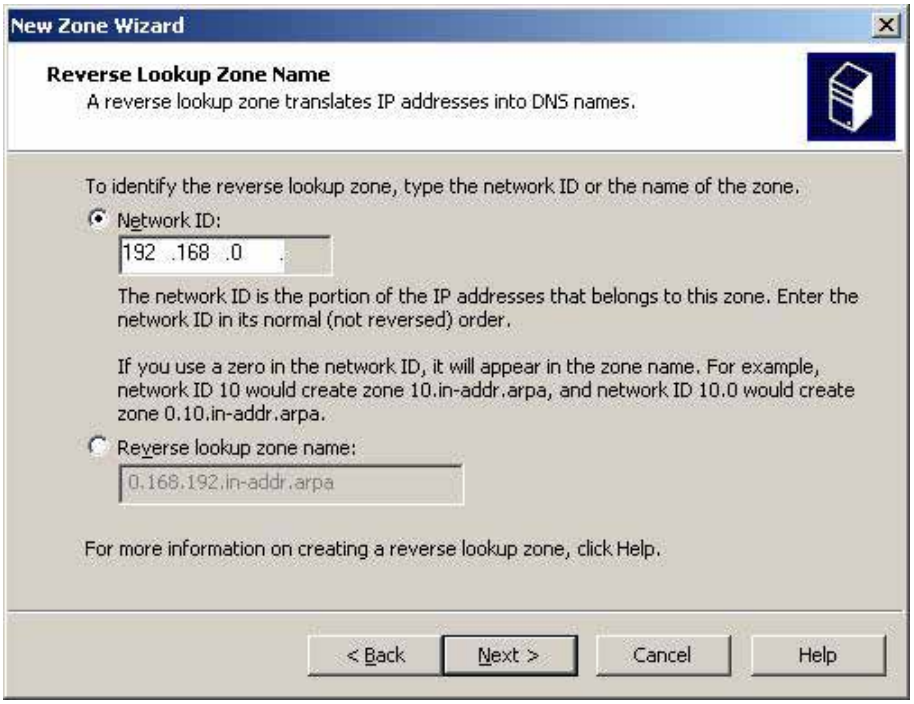

Figure 6.10 Network Address for Reverse Lookup Zone

8. Select **All DNS servers in the Active Directory domain keijou.local** (like Figure 6.6).
9. Enter the network address of the zone for reverse lookup, then click Next (Figure 6.10).
10. Select **Allow both nonsecure and secure dynamic updates** (like Figure 6.8).

In the **New Host** Window (Figure 6.11), the new reverse lookup zone should be configured with the new DNS server as the only member. We add new members to both the forward and reverse zones. We check the **Create associated pointer (PTR) record** box to simultaneously create the reverse lookup entry and click "Add Host" button (Figure 6.11).

Once the host has been added to the DNS database, the host's DNS client must be configured to the new DNS server (Figure 6.12).

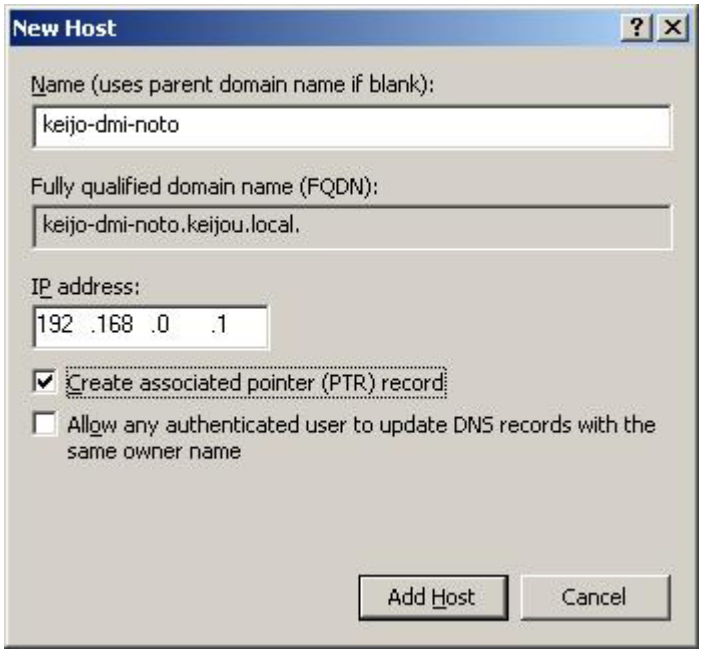

Figure 6.11　New Host Record

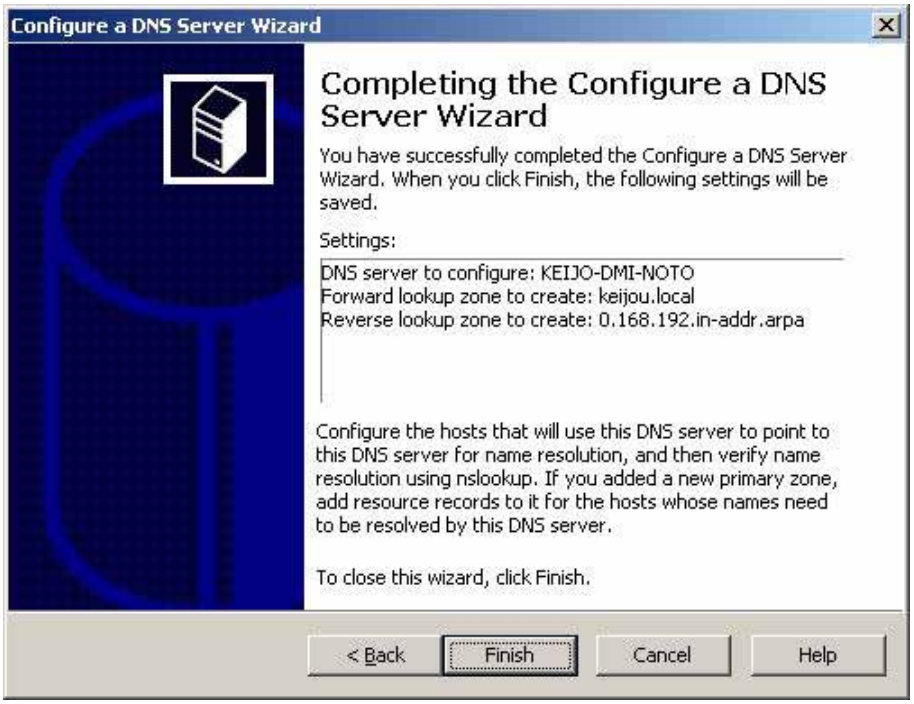

Figure 6.12　Completion of Configuring a DNS Server

A DNS server can now be configured to simultaneously forward queries for names ending in keijou.local, forward queries for names ending in, say, keijou.com to a second set of DNS servers if any, and forward all other queries to a third set of DNS servers if any. These features are configured through the DNS snap-in tool. In Figure 6.13 the current snap-in tool on our server KEIJO-DMI-NOTO is shown where, we find, the contiguous DNS domains are added in Forward Lookup Zones.

So far in this section we have been using "zone" many times without any definition. **Zone** is a contiguous portion of the domain tree of the DNS database. This administrative unit can consist of one domain or more than one child domains and is administered as a single separate entity by a DNS server. The zone contains resource records for all of the names within the zone. In other words, DNS allows a DNS namespace to be divided up into zones, which store name information about one or more DNS domains. For each DNS domain name included in a zone, the zone becomes the authoritative source for information about that domain.

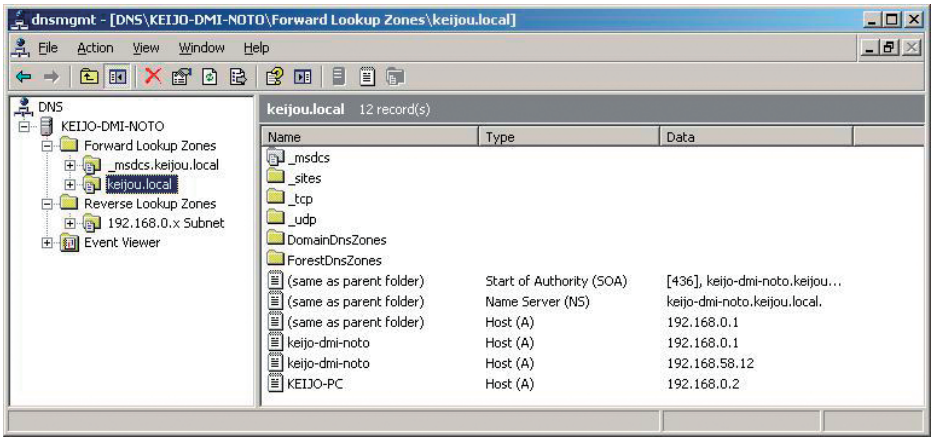

Figure 6.13 The current DNS snap-in tool on our server KEIJO-DMI-NOTO where the contiguous DNS domains are added in Forward Lookup Zones.

6.3. INSTALLATION OF DHCP (Dynamic Host Configuration Protocol) Server

Dynamic Host Configuration Protocol (DHCP) is an IP standard for simplifying management of host IP configuration. The DHCP standard provides a way to manage dynamic allocation of IP addresses and other related configuration details for DHCP-enabled clients on our network. Every computer on a TCP/IP network must have a unique IP address. The IP address together with its related subnet mask identifies both the host computer and the subnet to which it is attached. When we move a computer to a different subnet, the IP address must be changed. DHCP allows us to dynamically assign an IP address to a client from a DHCP IP address database on our local network. For TCP/IP-based networks, DHCP reduces the complexity and amount of administrative work involved in reconfiguring computers.

A DHCP **scope** is the full consecutive range of possible IP addresses for a network. Scopes typically define a single physical subnet on our network to which DHCP services are offered. Scopes also provide the primary way for the server to manage distribution and assignment of IP addresses and any related configuration parameters to clients on the network.

After we define a DHCP scope and apply exclusion ranges, the remaining addresses form the available address pool within the scope. Pooled addresses are eligible for dynamic assignment by the server to DHCP clients on our network.

Through "Configure Your Server" pages, we install and configure a local DHCP server on the computer where the Active Directory directory service is running.

The Dynamic Host Configuration Protocol (DHCP) provides a convenient and centralized method to configure and assign IP addresses on systems throughout the network. Once DHCP starts to work, the entire network may be configured to retrieve and renew these addresses whenever computers boot to get correct IP configuration for the current network. This is especially useful for mobile users and dial-in clients.

SERVER-SIDE DHCP CONFIGURATIONS

To install the DHCP server, we follow these steps:

1. Ensure that the DHCP server system is configured with a static IP address. Clients must be configured with a DHCP server address to obtain an IP address (and other information) when booting.
2. From the **Configure Your Server**, select **DHCP server** and the **New Scope Wizard** appears. Click **Cancel**.
3. Selecting **Start → Program → Administrative Tools → DHCP** (Figure 6.14).

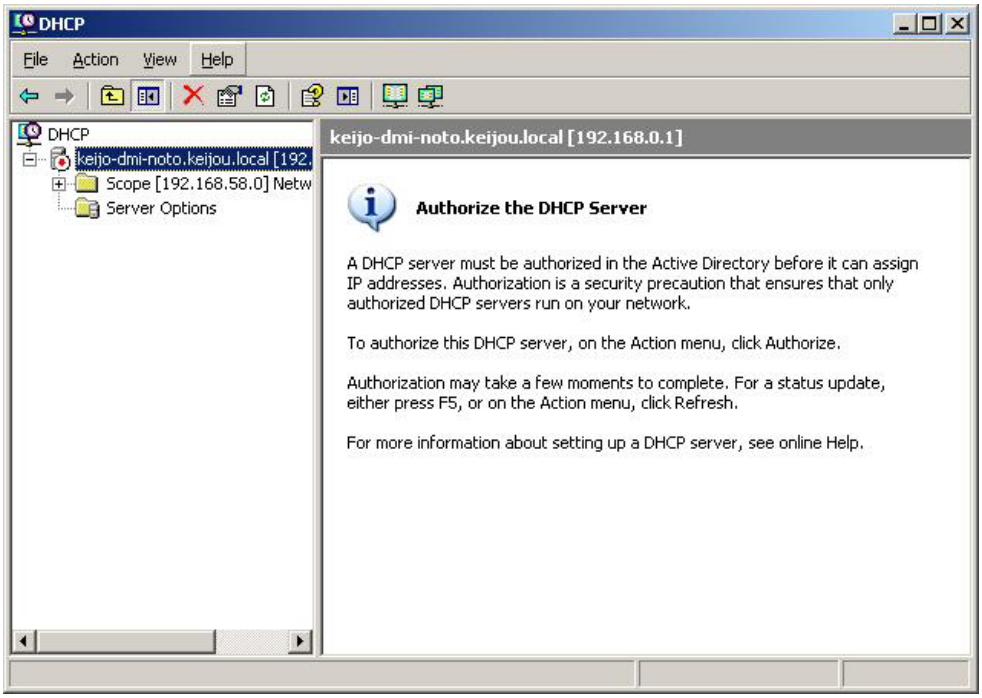

Figure 6.14 DHCP Server snap-in and Authorization of a DHCP Server

DHCP Authorization

DHCP servers can be installed on domain controllers, member servers, or standalone servers. However, the first DHCP server must participate in the Active Directory and it must be a member server or domain controller. The Active Directory maintains a list of authorized DHCP servers, which a DHCP server participating in the domain can query. If the server finds itself on the list, it will provide DHCP services. To authorize a DHCP server for the Active Directory, we follow these steps:

1. In the **DHCP** node in Figure 6.14, select **Authorize** from the drop-down list from an item **Action** in the menu bar.
2. In the **Manage Authorized Servers** dialog box, just ensure the DHCP server's DNS name and an IP address and click **OK**. Otherwise, click **Authorize** and enter the DHCP server's DNS name or an IP address and then click **OK**.

Scope and Classes

Once the DHCP server has been authorized for the domain, scopes must be created to define IP addresses and lease durations for its clients.

1. From the **Configure Your Server**, select **DHCP server** and the **New Scope Wizard** appears (Figure 6.15).

Figure 6.15 New Scope Wizard for a DHCP Server

The scope will be applied to all clients who request dynamically assigned IP addresses within its subnet; it will also determine several other client properties: Address range, Address exclusion ranges, Lease duration, DHCP options, Reservations Classes.

We take a look at these properties as we create a scope for the new DHCP server:

2. Click **Next** in **New Scope Wizard** page in Figure 6.15.
3. Enter a name and description for the new scope and click **Next** (Figure 6.16).
4. Enter a contiguous address range for the new scope by entering **a Start IP address** and an **End IP address** (Figure 6.17). This address range defines the pool of IP addresses available for DHCP clients who request them. We always assign the entire range of IP addresses to be used for the subnet and then use exclusion ranges to remove addresses from the pool. The subnet mask represents which bits of the IP address identify the subnet address. If the subnet mask bits are contiguous, we indicate in the **Length** box 24 bits from left to right.

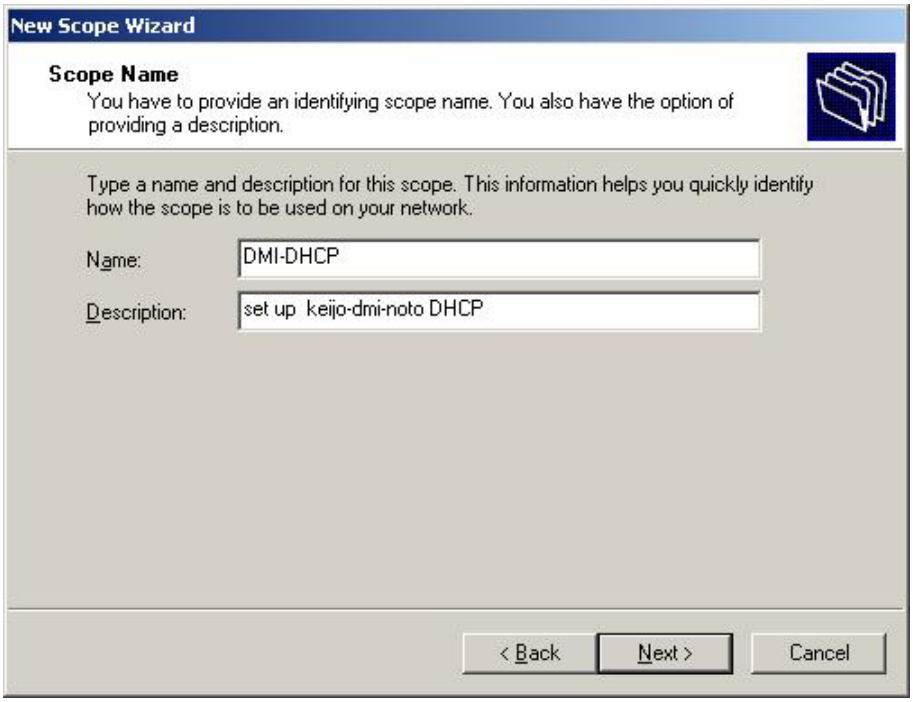

Figure 6.16 Scope Name for a DHCP Server

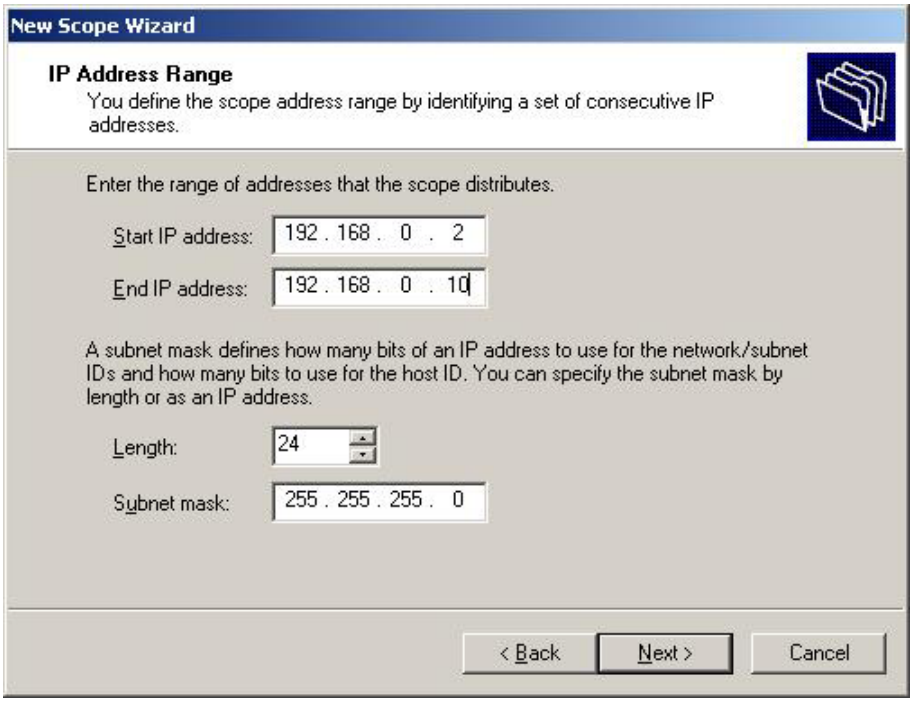

Figure 6.17 Scope Range for a DHCP Server

5. Add exclusion ranges to remove IP addresses from the available pool to lease DHCP clients. All IP addresses that have been statically configured for network interfaces should be excluded from the scope address range. Obviously, router addresses and the DHCP server's statically configured IP address should be excluded as well. To create an exclusion range, enter beginning and ending addresses, then click **Add**.

6. Enter a time interval for the duration of a DHCP client's lease of the IP address before it expires. Laptop and remote clients that regularly move networks should be assigned shorter lease periods to free up addresses sooner. More stable networks may benefit from longer lease periods (Figure 6.18).

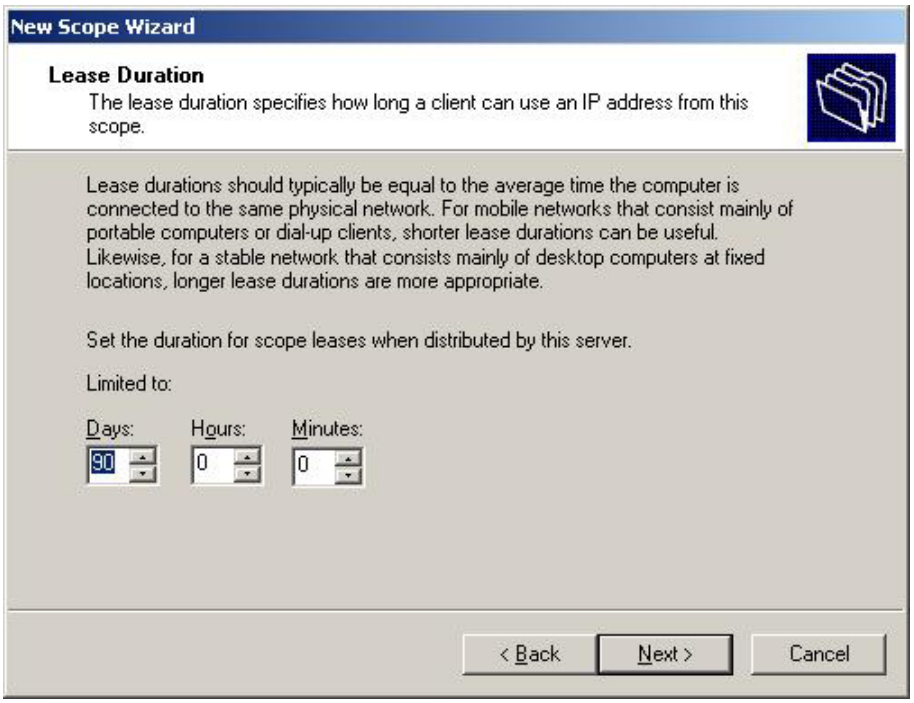

Figure 6.18 Lease Duration

7. The next **Activate Scope** dialog window (Figure 6.19) allows configuring DHCP options. Although many DHCP options are provided by the DHCP server and detailed in the DHCP standards document RFC 2132, five are supported by all Windows and MS-DOS client systems. The most common five options are Router (List of available routers), DNS Server (List of available DNS servers), DNS Domain Name (Parent Domain), WINS Server, and NetBIOS Node Type. Here we select **No, I will configure these options later** (Figure 6.19). In this case the server's default options are to work.

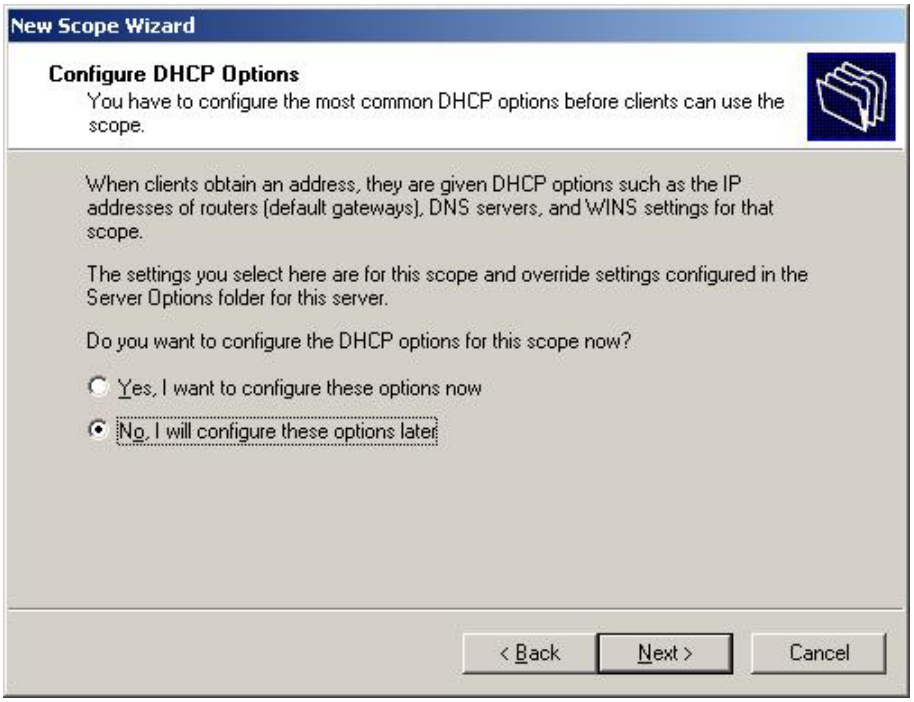

Figure 6.19 Activate Scope

8. In the last dialog box (Figure 6.20), click **Finish** to complete scope creation.

Figure 6.20 Completion of the New Scope

DHCP Options to configure

DHCP uses options to assign additional IP settings to DHCP clients on a network. The following parameters are usually included in those options:

・The default gateway IP address

・The DNS server IP address

・The DNS domain name

We can configure DHCP options for specific values and enable them to be assigned and distributed to DHCP clients based on server, scope, class, or reserved client levels.

By using the DHCP snap-in, we can configure some scope-level options, including router (default gateway), domain name and DNS servers.

1) Server Options

To configure server-level options:

1. In the DHCP snap-in, expand the server for which we want to configure options.
2. Right-click Server Options, and then click Configure Options (Figure 6.21).
3. In the Server Options dialog box, select the options we want to configure.
4. In the Data Entry section of the Server Options dialog box, type the option parameters, and then click OK (figure 6.22).

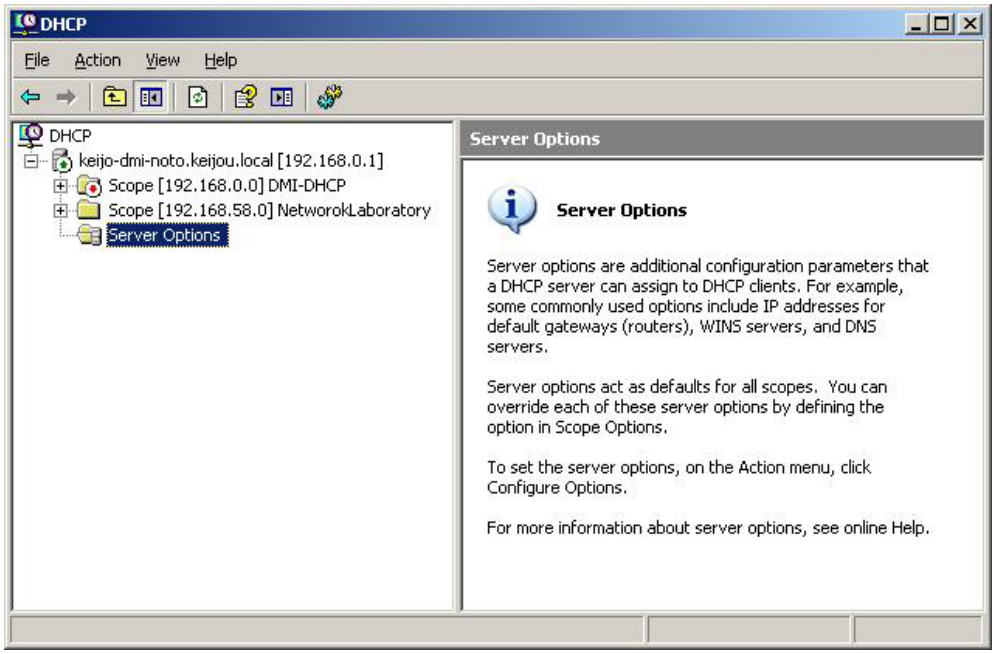

Figure 6.21 In the DHCP snap-in, **keijo-dmi-noto.keijou.local** server is expanded and “Server Options” are right-clicked.

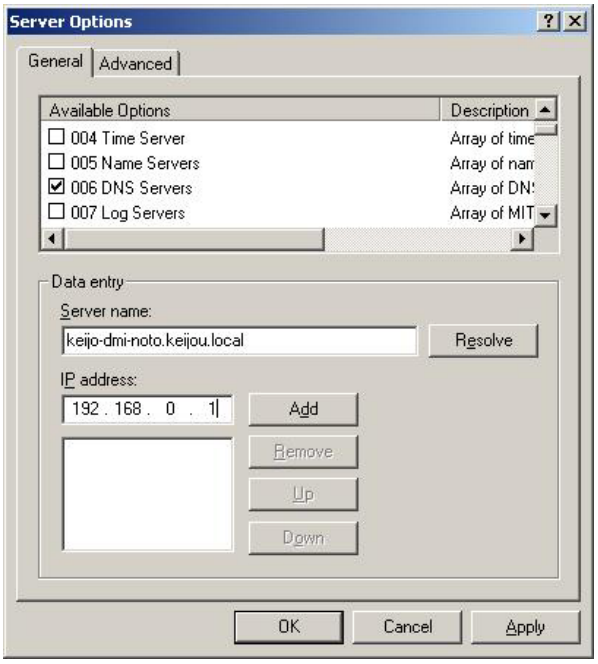

Figure 6.22 In the Server Options dialog box, the DNS server IP address on the server is assigned.

2) Scope Options

To configure scope-level options:

1. In the DHCP snap-in, expand the scope for which you want to configure options.
2. Right-click Scope Options, and then click Configure Options (Figure 6.21).
3. In the **General** tab of **Scope Options** dialog box, specify or modify DHCP options with a check mark.
4. enter proper values in their data entry fields, and then click OK (Figure 6.23).

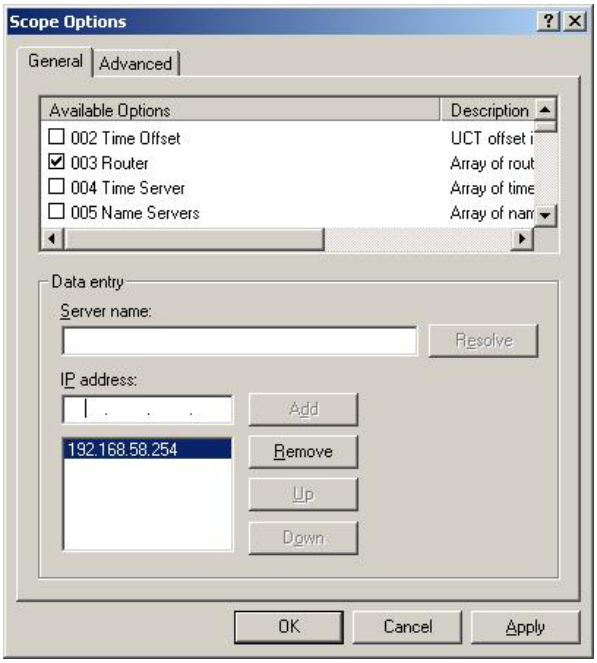

Figure 6.23　General tab in the Scope Options

In the Scope Options dialog box in Figure 6.23, the Router IP address on the server is assigned.

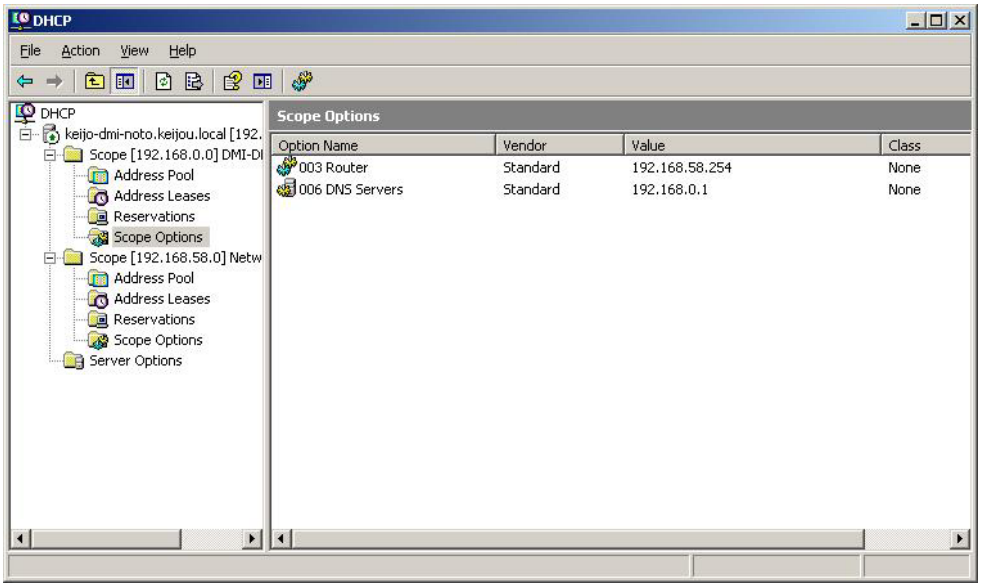

Figure 6.24　In the DHCP snap-in, **keijo-dmi-noto.keijou.local** server's scope is expanded and "Scope Options" are right-clicked.

The DHCP tool should display the newly activated scope under the Scope Option's node (Figure 6.24).

In general, there seem to be some guide lines for DHCP options to be assigned to DHCP clients. Here we quote from "Windows Server 2003 Deployment Guide ---> Deploying Network Services"[11] the guidelines to be used when configuring DHCP options for clients on a network and add an example if necessary:

- Add or define new, custom option types only if you have new software or applications that require a nonstandard DHCP option.
- If your network is large, be conservative and selective when assigning global options. These options apply to all clients of a DHCP server, unless more specific options are specified.
- Use scope-level options for most options that clients are assigned to. Setting options at the scope level allow you to take scope-related differences into account, such as different client needs or the use of a different DNS server from other scopes in the network.
- Use class-level options if you have a large network or diverse groups of clients that are able to support membership in option classes. For example we can configure user-class options to provide a shorter lease time for notebook computer users in our Network Laboratory.
- Use reserved client options only for clients that have special requirements, for example, if your intranet has a DNS server that performs forwarding for resolving Internet DNS names not authoritatively managed on your network. In this case, you need to add the IP address of an external DNS server on your DNS server computer. You can configure your DNS server as a reserved client in DHCP and set this address as another reserved client option.

Acknowledgement

The present research was supported by the Special Research Funds 2005 of Hokusei Gakuen University. The network configuration and BizTalk Server 2006[8] installation were carried out on Microsoft Windows Server 2003 R2 operating system[3] using Dell PowerEdge 800 computer in the Network Laboratory in the Comprehensive Information Center of Hokusei Gakuen University.

Keywords

⑴ Windows Server 2003 R2
⑵ Business-to-business(B2B) Integrated Network System
⑶ Active Directory and Domain Model
⑷ Domain Name System (DNS)
⑸ Dynamic Host Configuration Protocol (DHCP)

Bibliography

(1) Noto, Hirosi: Setup of Windows Server 2003 and Networking with Active Directory in the Network Laboratory (I), Hokusei Review, The School of Economics (Hokusei Gakuen University) Vol. 46, No. 2 March 2007.

(2) Noto, Hirosi: Setup of Windows Server 2003 and Networking with Active Directory in the Network Laborarory (II), Hokusei Review, The School of Economics (Hokusei Gakuen University) Vol. 47, No. 1 September 2007.

(3) Windows Server 2003 R2 Enterprise Edition system disk (2006) in MSDN Library.

(4) Windows Server 2003 R2:
http://www.microsoft.com/windowsserver2003/default.mspx

(5) Robert Williams and Mark Walla: The Ultimate Windows Server 2003 System Administrator's Guide (2003), Addison-Wesley.

(6) Amano Tukasa: Windows Server 2003 at a Glance (Official Guide book of Microsoft) (2003) Nikkei BP Soft press (in Japanese)

(7) Inoue Koji: Windows Server 2003 Network Server Build Guide (2003) Shuwa System (in Japanese).

(8) BizTalk Server 2006, Enterprise Edition system disk (2006) in MSDN Library.

(9) Microsoft BizTalk Server 2006 Help:
http://msdn2.microsoft.com/en-us/library/aa548004.aspx

(10) Daniel Woolston: Foundation of BizTalk Server 2006 (2007), APress.

(11) http://technet2.microsoft.com/windowsserver/en/library

[Abstract]

Setup of Windows Server 2003 and Networking with Active Directory in the Network Laboratory (III)

Hiroshi NOTO

The researchers planned to introduce and configure a business-to-business (B2B) integrated network system for the students in the Management and Information Department of Hokusei Gakuen University to help them understand and practice connecting applications, defining business processes, managing and monitoring business processes across an organization, and optimizing both internal and B2B processes. This B2B network system will be set up in the Network Laboratory in the Comprehensive Information Center of this university. This article describes the network system, starting with an introduction of the operating system (Windows Server 2003) and the selection of a server computer. It also describes how to install the operating system on the server computer. This article explains in detail how to setup the server system. The main component of the server systems is the Active Directory directory service that is configured to meet the B2B practice requirements on Windows Server 2003. The management of Active Directory service has to be prepared by installing a Domain Name System (DNS) server and a Dynamic Host Configuration Protocol (DHCP) server. In both cases the server-side configurations are elucidated in this article.

Key Words : Windows Server 2003 R2, Business-to-business(B2B) Integrated Network System, Active Directory and Domain Model, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP)