3 4

Chapter 9

DNS in Name Resolution Designs

About This Chapter

The majority of the networking services designs that you create will utilize Internet Protocol (IP) to access resources within the organization and resources on the Internet. These resources can be accessed by the IP address assigned to the resource. Although accessing these resources by IP address is technically possible, many users are unable to cope with the complexities of accessing resources by IP address.

Most of the designs that you create will provide the facility to associate a meaningful name to the resources within the organization and on the Internet. Your design must translate these meaningful resource names to IP addresses. Also, most of your designs will require you to perform the reverse operation (translate an IP address into a meaningful resource name).

Your designs will often include migrating networks from Microsoft Windows NT 4.0 to Microsoft Windows 2000. The majority of Windows NT 4.0–based networks run on the Transmission Control Protocol/Internet Protocol (TCP/IP) and rely heavily on Windows Internet Name Service (WINS) for accessing resources within the organization. Your design must be capable of integrating WINS–based name resolution into your name resolution design.

You can use the Domain Name System (DNS) services in Windows 2000 to translate or *resolve* these meaningful resource names to IP addresses and to translate an IP address to a meaningful resource name. The DNS services in Windows 2000 can automatically register the organization's computers in DNS, reducing the amount of time required to administer DNS.

You can integrate WINS-based computers into a DNS-based network by using the integration between the DNS services and WINS services in Windows 2000. Windows 2000 allows users on your network to transparently resolve names by using DNS or WINS.

This chapter answers questions such as:

- In what situations are the name resolution services provided by DNS appropriate for your design?
- What must you include in your DNS design to support Active Directory?
- How can you integrate DNS in Windows 2000 with other DNS servers?
- What must you include in your design to integrate DNS with WINS?
- How can you ensure the integrity of the DNS database?
- What can you include in your design to ensure that DNS name resolution is always available to network users?
- How can you improve the performance of DNS name resolution during peak periods of activity?

Before You Begin

Before you begin, you must have an overall understanding of

- Network technologies (including Ethernet, Token Ring, hubs, switches, and concentrators)
- Common transport protocol configuration for IP (such as IP address, subnet mask, or default gateway for IP)
- IP routed networks (including subnets, network segments, routers, and IP switches)
- DNS usage in a network (including DNS namespace conventions, resource-record types, and name resolution)
- Integration between DNS and WINS (when both DNS and WINS are included in the same name resolution design)
- Integration between DNS and Dynamic Host Configuration Protocol (DHCP) (when both DNS and DHCP are included in the same name resolution design)

3 4

Lesson 1: Designs That Include DNS

This lesson presents the requirements and constraints, both business and technical, that identify the name resolution services in DNS as a solution.

After this lesson, you will be able to

- Identify the situation in which DNS is the appropriate choice for name resolution

- Describe the relationship between DNS and Windows 2000
- Identify the business and technical requirements and constraints that must be collected to create a DNS design
- Identify the DNS design decisions
- Evaluate scenarios and determine which capabilities and features of DNS are appropriate in name resolution solutions

Estimated lesson time: 30 minutes

DNS and Name Resolution in Networking Services Designs

In the "About This Chapter" section, the primary requirement for including DNS in your design was presented—name resolution. However, there are solutions other than DNS that you can include in your design to provide name resolution.

In addition to DNS, you can provide name resolution by using

- A HOSTS file on the local computer
- A LMHOSTS file on the local computer or on shared computers
- WINS

Table 9.1 lists each of the methods of DNS and the advantages and disadvantages of including that method in your design.

Table 9.1 *Advantages and Disadvantages of DNS Methods*

Method	Advantages	Disadvantages
HOSTS	Available on all network operating systems Independent of other computers because the HOSTS file is stored locally	Requires administration on every computer Integrity of the HOSTS file can be compromised because users can modify the file
LMHOSTS	Provides enhanced support above HOSTS file for WINS (NetBIOS) names Can reference a centralized copy of a LMHOSTS file to reduce administration	Available only on Microsoft operating systems Requires administration on every computer Integrity of the LMHOSTS file can be compromised because users can modify the file
WINS	Supports automatic registration of client computers Centralized name resolution database to reduce administration and configuration errors	Designed for name resolution for NetBIOS names [fully qualified domain names (FQDNs) aren't fully supported]
DNS	Only name resolution method that supports Active Directory directory service Centralized name resolution to reduce administration and configuration errors Provides full support for FQDNs Can provide name resolution for NetBIOS names in addition to FQDNs	Name registration may not be automatic (requires dynamically updateable DNS servers) Not all versions on other operating systems support Active Directory Complexity associated with configuring DNS might be daunting for some administrators or organizations

Although other methods are available, DNS is the only method that provides all of the following:

- Centralized administration
- Support for Active Directory
- Support for FQDN name resolution
- Support for NetBIOS name resolution

This chapter focuses on designs that include DNS for FQDN name resolution. For more information on NetBIOS name resolution and WINS, see Chapter 10, "WINS in Name Resolution Designs."

DNS and Windows 2000

DNS is an industry standard protocol that provides *forward name resolution* and *reverse name resolution*. In forward name resolution, a DNS server receives FQDNs from DNS clients and returns corresponding IP addresses. In reverse name resolution, a DNS server receives IP addresses and returns corresponding FQDNs.

The DNS services in Windows 2000 can be divided into

- **DNS Client** You can configure the IP stack for all versions of Windows to resolve FQDNs by using DNS. The DNS Client is an integral part of the IP implemented in Windows 2000. The DNS Client receives requests for FQDN name resolution from applications running on the same computer and forwards the requests to DNS servers.

NOTE

Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT 4.0, UNIX, Macintosh, and other operating systems include DNS clients as well.

- **DNS Server** The DNS Server service in Windows 2000 can provide forward and reverse name resolution to DNS clients in your design. From the Windows 2000 perspective, DNS Server is a service that runs on Windows 2000. The DNS Server service utilizes IP and the file services of Windows 2000.

The DNS Server service communicates with DNS clients, other DNS servers, Active Directory domain controllers, WINS servers, and Dynamic Host Configuration Protocol (DHCP) servers by using the IP stack in Windows 2000. You must specify a fixed IP address for all network interfaces on the DNS server that communicate with the DNS Server service.

The DNS Server service in Windows 2000 manages a database stored locally on the DNS server. The DNS database contains the DNS records for forward and reverse name resolution that are resolved by the DNS server.

The DNS Server service is available in Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, and Microsoft Windows 2000 Datacenter Server. The DNS Server service isn't available in Microsoft Windows 2000 Professional.

In this chapter, you learn how to create name resolution designs with DNS and Windows 2000. Figure 9.1 illustrates the interaction between DHCP and the other networking services in Windows 2000.

To successfully create DNS designs, you must be familiar with

- General IP and IP routing theory
- General DNS and Berkeley Internet Name Domain (BIND) server theory
- Common DNS resource records types and formats
- General domain namespace design theory

NOTE

A full discussion of domain namespace design is beyond the scope of this chapter. Domain namespace design is only discussed as how domain namespace design affects DNS networking services designs.

DNS Design Requirements and Constraints

Before you create your DNS design, you must gather the requirements and constraints, both business and technical, of the organization. As you create your design, you make design decisions based on the requirements and constraints you collect.

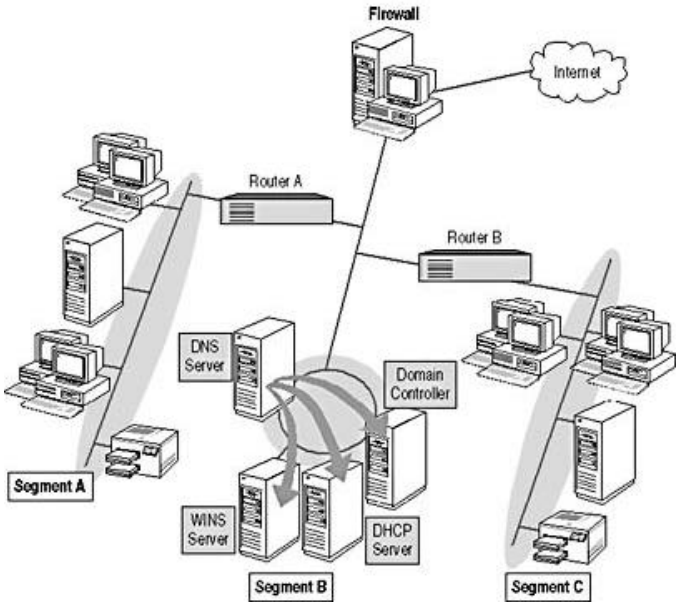


Figure 9.1 *The interaction between DNS and other Windows 2000 networking services*

The list of the design requirements and constraints that you collect will include

- The amount of data transmitted between the existing network segments containing the DNS clients and the DNS server
- Number of locations and network segments that require name resolution
- Wide area network (WAN) connections in use
- Plans for network growth
- Current domain namespace design for the organization
- Characteristics of existing DNS servers including
  - Number of DNS resource records in existing DNS databases
  - DNS server placement
  - Operating systems running current DNS servers
  - Versions of DNS servers running on other operating systems

DNS Design Decisions

After you determine the business and technical requirements and constraints, apply the information you gathered to make DNS design decisions.

To create your DNS design, you must choose the

- Methods for integrating DNS into the existing network based on the
  - Existing domain namespace design
  - Operating systems and the DNS or BIND versions of any existing DNS servers
  - Placement of existing DNS servers
  - Existing WINS servers
  - Type of DNS zones required in the design
- Method of ensuring that DNS name resolution is always available to DNS clients
- Method of optimizing the network traffic between DNS clients and DNS servers

The lessons that follow in this chapter provide the information required for you to make specific DNS design recommendations.

DNS and Active Directory Designs

Most of the DNS solutions that you create must support Active Directory directory service. When the organization's requirements include Active Directory, you must include DNS in your design. Your primary concern in Active Directory is ensuring that domain controllers, member servers, and client computers can resolve IP addresses for Active Directory objects stored in DNS.

Making the Decision

In DNS and Active Directory designs, you must decide the DNS features utilized by Active Directory. Some of the DNS features must be included in your design because Active Directory requires them. Other features aren't required, but can reduce the complexity and administration associated with your design.

Table 9.2 lists the DNS features to include, whether the feature is required, and the versions of DNS that support the feature.

Table 9.2 *DNS Features That Support Active Directory*

Feature	Required	DNS Versions
Support for SRV (service) resource records	Required	BIND 4.9.6 and later versions DNS in Windows 2000
Dynamically updated zones	Optional	BIND 8.1.2 and later versions DNS in Windows 2000
Incremental zone updates	Optional	BIND 8.2.1 and later versions DNS in Windows 2000

TIP

Although BIND 4.9.6 and later versions can support Active Directory, BIND version 8.2.2 is recommended because it's the latest version and supports all the enhanced DNS features.

In addition to the features provided by BIND DNS servers, the DNS services in Windows 2000 provide these additional features:

- **Store DNS zone databases in Active Directory** When you include Active Directory directory service in your design, you can store the zone database resource records in Active Directory. To store zone database resource records in Active Directory, you must specify the zone an Active Directory integrated zone.
- **Replicate DNS zone databases between DNS servers by using Active Directory replication** Any Active Directory integrated zones in your design can be replicated by using traditional DNS zone replication or by using Active Directory. Because the zone database is stored in Active Directory, the zone database is replicated along with the other data stored in Active Directory.
- **Automatic management of DNS resource records for computers running Windows 2000 or for computers configured by using DHCP** You can specify that any computer running Windows 2000 or any computer configured by the DHCP Server service in Windows 2000 dynamically update corresponding resource records in DNS. When the DNS zone is an Active Directory integrated zone, you can restrict the computers, groups, or users that can modify the DNS zone information.

DNS and DHCP integration are discussed further in Lesson 2, "Essential DNS Design Concepts," and Lesson 3, "Name Resolution Protection in DNS Designs," later in this chapter. For more information on DHCP, see Chapter 8, "DHCP in IP Configuration Designs."

- **Integration with WINS servers** You can forward unresolved DNS queries to WINS servers in the organization. The WINS servers search the WINS database to resolve host names. In addition, you can forward unresolved WINS queries to DNS servers. The DNS servers search the specified domain namespace to resolve NetBIOS names.

DNS and WINS integration are discussed further in Lesson 2, "Essential DNS Design Concepts, " later in this chapter. For more information on WINS, see Chapter 10, "WINS in Name Resolution Designs."

Applying the Decision

Figure 9.2 illustrates a scenario where Active Directory is the primary reason for including DNS. DNS Server A provides name configuration for Active Directory domain controllers, member servers, and client computers. DNS Server A is placed centrally in the private network to provide equal access to all domain controllers, member servers, and client computers.

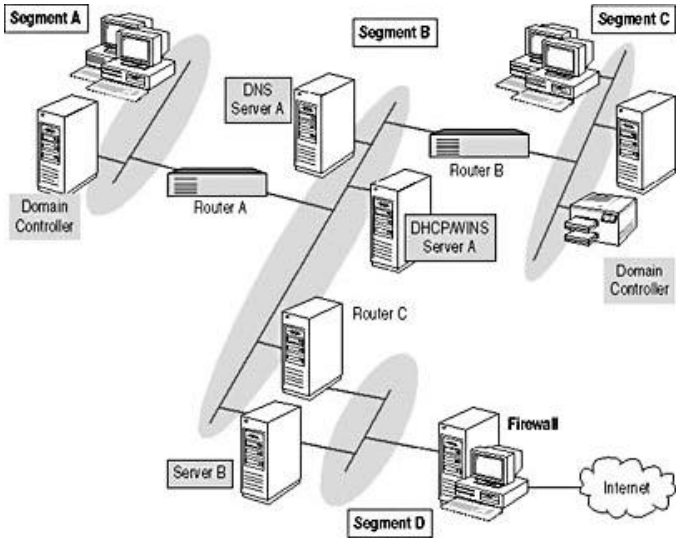


Figure 9.2 *Scenario that includes DNS to support Active Directory*

For the purposes of this scenario, assume that

- Approximately 400 client computers exist on Segments A and C
- The organization has decided to standardize its Active Directory as directory service
- The organization wants to reduce the administration by automatically registering client computers in DNS
- DHCP servers in the organization configure all client computers
- Any unresolved DNS queries must be forwarded to the organization's WINS servers

The DNS in Windows 2000 is the only solution that meets the requirements of the organization. As a result, HOSTS files, LMHOSTS files, WINS, or other implementations of DNS aren't appropriate solutions.

Traditional DNS Designs

There might be instances when you require DNS services, but Active Directory isn't one of the requirements of the organization. Traditional DNS designs require only a subset of the features in designs that include Active Directory.

Your traditional DNS designs interact with DNS servers on the Internet and within the organization's private network. In these situations, your primary concern in these designs is providing Request for Comments (RFC)-compliant interoperability with other DNS servers.

Making the Decision

You can achieve interoperability with other DNS servers by ensuring that your DNS server design supports

- **A common character set** The character set approved for Internet host names is restricted to the US-ASCII-based characters. These restrictions limit names that include upper- and lower-case letters (A-Z, a-z), numbers (0-9), and hyphens (-). These restrictions were included in RFC 1035 as part of the core specifications for DNS.

The DNS server in Windows 2000 supports all the requirements for RFC 1035. In addition, the DNS server in Windows 2000 supports Unicode transformation format-8 (UTF-8). UTF-8 supports extended ASCII to incorporate other languages. In addition UTF-8 can incorporate names that use characters beyond the RFC 1035 restrictions.

To support interoperability with other DNS servers, you must specify that all DNS servers adhere to the specifications of RFC 1035.

- **The same DNS zone transfer method** DNS servers can exchange updates to resource records in DNS zones by performing *incremental zone transfers* or *full zone transfers*. Incremental zone transfers send only the resource records that change. Full zone transfers send the entire contents of the zone.

Complete zone transfers are supported by all versions of DNS. Incremental zone transfers are supported only on DNS servers that are compliant with RFC 1995, such as BIND versions 8.2.1 and later. To ensure proper interoperability, all DNS servers must use either incremental zone transfers or full zone transfers.

- **The same compression method in DNS zone transfers** DNS servers can perform incremental DNS zone transfers by using a *slow transfer method* or *fast transfer method*. The slow transfer method transfers a single resource record in an uncompressed format. The fast transfer method transfers multiple resource records at a time in a compressed format.

The DNS services in Windows 2000 transfer resource records by using the fast transfer method as the default. When your designs include DNS servers running BIND versions 4.9.4 or earlier, you must specify that all DNS servers support the slow transfer method.

- **The appropriate DNS resource record types** Different implementations of DNS servers can support different DNS resource record types. Most DNS servers reject any DNS resource records that aren't supported by the DNS server.

For example, assume that a DNS server doesn't support service (SRV) resources records. If another DNS server transfers SRV resource records to the DNS server, the DNS server rejects the SRV resource records.

You must ensure that all the DNS servers in the design support the DNS resource records in use by the organization.

- **Dynamic DNS zone update protocol** If the organization requires dynamic updates to DNS, you must ensure that all DNS servers in your design support dynamic updates. The DNS services in Windows 2000 support dynamic updates compatible with RFC 2136. DNS servers running BIND versions 8.1.2 or later are compatible with RFC 2136 and support dynamic updates.

Applying the Decision

Figure 9.3 illustrates a design where the DNS services in Windows 2000 are incorporated with BIND DNS servers. For the purposes of this scenario, assume that

- DNS Servers A and B in the organization are running Windows 2000
- DNS Servers C, D, and E in the organization are BIND version 4.9.4
- DNS Server A replicates zone information to DNS Server C and E
- DNS Server D replicates zone information to DNS Server B

To provide interoperability between the DNS servers running on Windows 2000 and the BIND DNS servers, you must ensure that your design includes

- Only standard ASCII characters for host names as specified in RFC 1035
- Full zone transfers between DNS servers

- Slow zone transfers between DNS servers

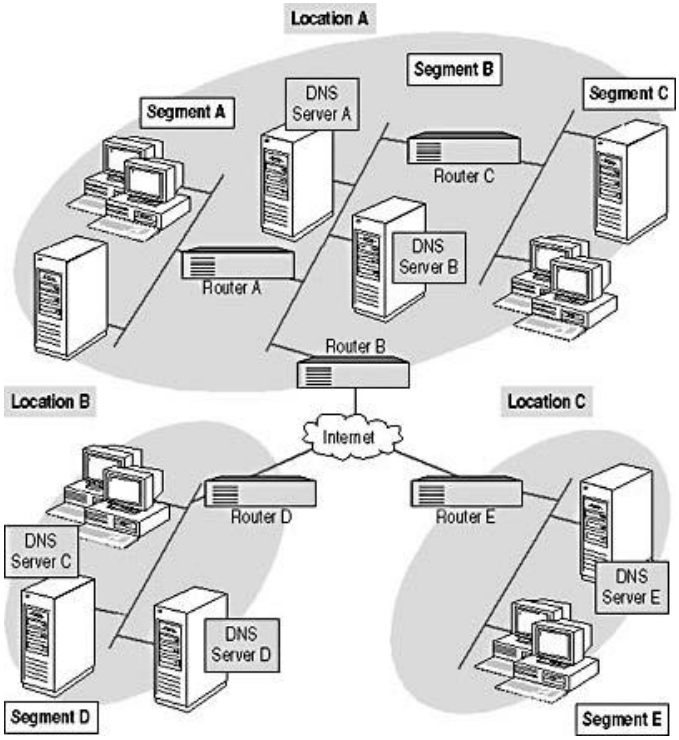


Figure 9.3 *Scenario that incorporates DNS services in Windows 2000 with BIND DNS servers*
3 4

Lesson 2: Essential DNS Design Concepts

This lesson discusses the requirements, constraints, and design decisions used in establishing the essential specifications in a DNS design. This lesson discusses the design concepts common to all DNS designs.

After this lesson, you will be able to

- Determine how the organization's domain namespace affects your design
- Select the appropriate zone types to include in your design
- Determine the placement of DNS servers in your design
- Select the appropriate method for integrating DNS with other versions of DNS
- Select the appropriate method for integrating DNS name resolution and WINS name resolution

Estimated lesson time: 45 minutes

Determining Domain Namespace Influences on DNS

You must determine the structure of the organization's domain namespace to create your DNS design. The domain namespace is represented in your design by the DNS resource records managed by the DNS servers.

The organization's domain namespace affects the type of zones you can include in your design. In addition, the placement of DNS servers in your design is partially based on the organization's domain namespace.

Making the Decision

To determine how the organization's domain namespace affects a DNS design, you must evaluate the relationships between

- The organization's domain namespace and Internet naming conventions
- The external and internal namespaces of the organization
- Active Directory and the organization's domain namespace
- The organization's namespace and subdomains that exist within the namespace

- The domain namespace and DNS zones

Domain Namespaces and Internet Naming Conventions

The majority of the designs you create will include domain namespaces accessed by Internet users. Domain namespaces you expose to the Internet must adhere to specific naming conventions. All domain namespace designs you encounter are based, at least in part, on these Internet naming conventions.

The DNS domain namespace is based on the concept of a hierarchical tree structure of named domains. Each level in the tree structure of your domain namespace is either a *branch level* or a *leaf level* of the tree. The branch level domain names in your design contain other domain names (branch levels) or multiple DNS resource records (leaf levels). The leaf level domain names in your design are resource records that represent a specific resource.

The structure of any domain name is interpreted from right to left. The rightmost portion of any domain name is the highest portion in the domain name's hierarchical structure. The leftmost portion of any domain name is the lowest portion in the domain name's hierarchical structure.

Table 9.3 lists the types of domain names found in a domain namespace and a description of each type.

Table 9.3 *Descriptions of Domain Namespaces*

Domain Name Type	Description
Domain root	The highest portion of the domain namespace tree. The domain root is an unnamed portion of a domain name space that is designated by a trailing period ".". You must include the domain root to specify a FQDN.
Top-level domain	Two or three letter names that designate the country, region, or type of organization using the name. You must obtain top- level domain names from Internet governing originations (currently managed by Network Solutions, Inc.).
Second-level domain	Variable length domain names that designate the organization or individual for use on the Internet. You must obtain second- level domain names from Internet governing originations (currently managed by Network Solutions, Inc.).
Subdomains	Additional variable length domain names that designate an organization's internal structure (for example geographic or departmental). You can specify any number and levels of subdomains within your domain namespace design.
Host or resource name	Name of computers or groups of computers (such as clusters) within the organization. You can specify any number of resource names within your design.

Figure 9.4 illustrates an example of a domain namespace structure. In the example, you can see the following name structure:

- msft is the top-level domain name
- contoso is the second-level domain name
- asia is a subdomain name
- sales is a subdomain name
- ServerA is a host or resource name

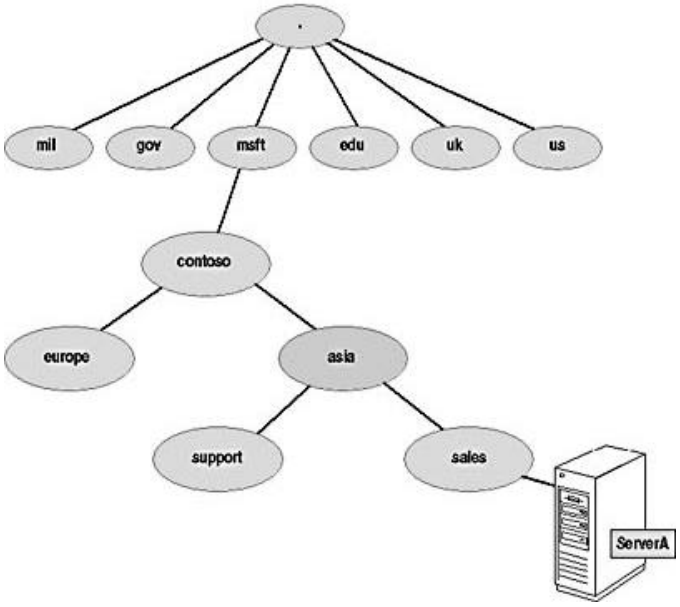


Figure 9.4 *Example of a domain namespace structure*

You can access ServerA from the Internet by specifying the FQDN for ServerA: *ServerA.sales.asia.contoso.msft.* (note the trailing period to specify the root).

NOTE

Although *msft* isn't an appropriate top-level domain, for the purposes of the example, assume that msft is a valid top-level domain name.

External and Internal Domain Namespaces

You can specify an organization's domain namespace as an *external* domain namespace, an *internal* domain namespace, or a combination of both. An external namespace is visible to Internet users and computers. An external namespace is the domain namespace that you're probably the most familiar with. All Internet domain names that you access are found in external namespaces. An internal domain namespace is visible only to the users and computers within the organization.

Figure 9.5 illustrates an example of an organization that has a combination of external and internal domain namespaces. In the example, Server-A resides in an external namespace (*external.contoso.msft.*) accessible by Internet users or private network users. Server-B resides in an internal namespace (*support.internal.contoso.msft.*) accessible by only private network users.

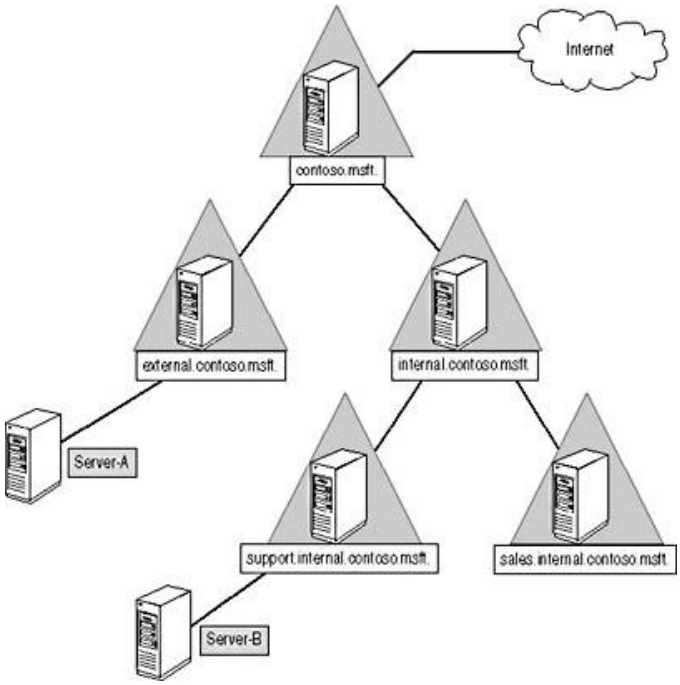


Figure 9.5 *Example where an organization has a combination of external and internal domain namespaces*

An organization's internal domain namespace root can be a part of the same namespace root as the organization's external domain namespace root or a completely separate namespace. Ensure that your design's internal domain namespace root is different from *external* domain namespace roots for *other* organizations.

Figure 9.6 illustrates an example of an organization that has separate external and internal domain namespaces. In the example, *contoso.msft.* is the external namespace and Server-A resides in the external namespace. The internal namespace, *contoso-i.msft.*, contains the domain names for all the organization's resources that are accessed only by private network users. Server-B resides in the internal namespace and can be accessed only by private network users.

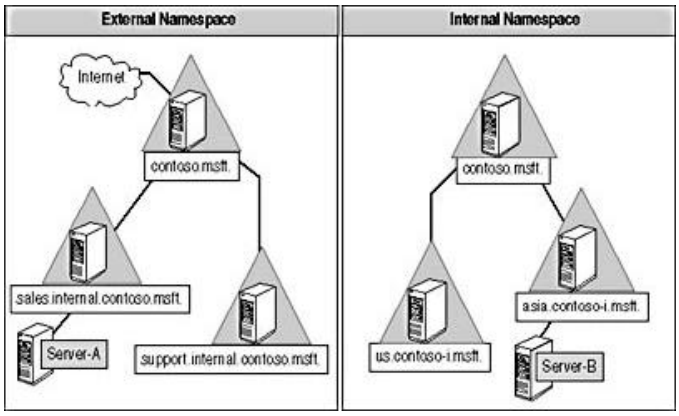


Figure 9.6 *Example where an organization has separate external and internal domain namespaces*

In the example in Figure 9.6, the organization requires two domain namespace roots (*contoso.msft.* and *contoso-i.msft.*). In the example in Figure 9.5, the external and internal namespace share the same domain namespace root (*contoso.msft.*).

Although other organizations are unaware of your internal domain namespace root, private network users access the internal domain namespace root to access resources within the private network. If your *internal* domain namespace root is identical to *another* organization's external domain namespace, the private network users aren't able to access resources in the *other* organization.

Figure 9.7 illustrates an example where an organization's internal domain namespace is identical to another organization's external domain namespace. When clients in Organization A attempt to access external domain names in Organization B (*salesco.msft.*), the DNS servers in Organization A attempt to resolve DNS requests for *salesco.msft.* by using the internal DNS namespace servers. The DNS requests aren't forwarded to the DNS servers in Organization B.

Domain Namespace and Subdomains

After you establish your external and internal namespaces, you must determine the subdomains that exist in the namespace design. You can include subdomains in your design to organize resources within an organization by departmental, geographic, or other specifications.

You can include subdomains in the organization's external or internal namespace. You can create any number of levels in your DNS tree structure by nesting subdomains.

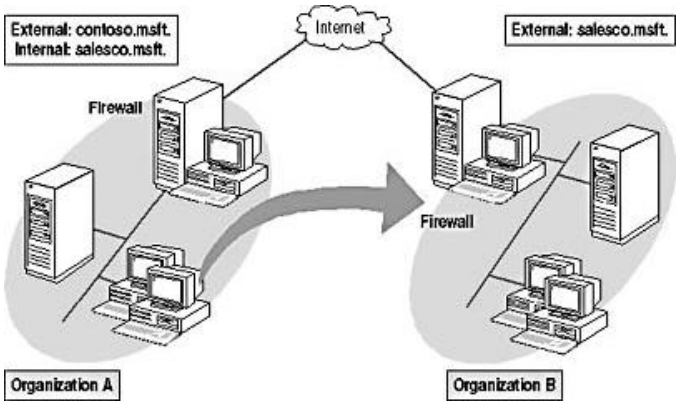


Figure 9.7 *Example where an organization's internal domain namespace is identical to another organization's external domain namespace*

Figure 9.8 illustrates an example where an organization's domain namespace includes subdomains. The organization has one namespace (*contoso.msft.*) that is subdivided by subdomains (*asia.contoso.msft.* and *europe.contoso.msft.*). The subdomain *europe.contoso.msft.* is further subdivided by subdomains (*support.europe.contoso.msft.* and *sales.europe.contoso.msft.*).

You can use subdomains to separate the external and internal namespaces when your namespace design contains a single domain namespace root. The examples in Figure 9.5, *external.contoso.msft.* and *internal.contoso.msft.*, are subdomains that divide the organization's internal and external namespace.

Domain Namespace and Active Directory

In the designs you create, you must determine how Active Directory is integrated into the organization's domain namespace. Active Directory domains correspond to DNS domain or subdomain names in your DNS designs.

In the DNS designs you create, ensure that the domains, and subdomains, used by Active Directory reside in the internal namespace. For more information on internal and external namespaces, see the previous section, "External and Internal Domain Namespaces."

For each domain in your Active Directory design, you must

- Include a DNS domain or subdomain in your DNS design
- Enable dynamically updated DNS zones when you want Active Directory to automatically create the domains or subdomains (when the DNS servers support dynamically updated DNS zones)

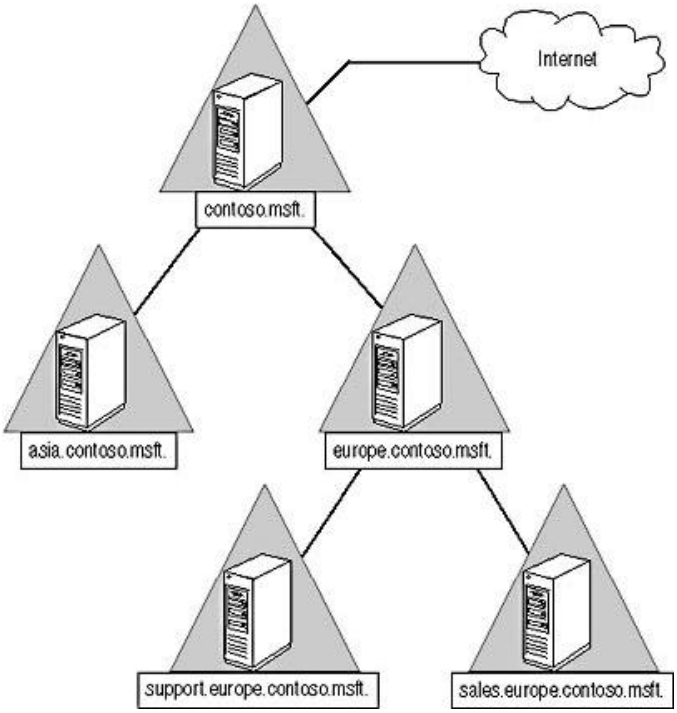


Figure 9.8 *Example where an organization's domain namespace includes subdomains*

- Manually create DNS domains or subdomains (when the DNS servers don't support dynamically updated DNS zones)

Domain Namespace and DNS Zones

After you analyze the organization's domain namespace, you must convert the domain namespace to DNS zones.

You can convert the domain namespace to DNS zones by

- **Including all domains, subdomains, and resource records in a single DNS zone** You place the entire domain namespace in a single DNS zone when the

- Size of the organization's domain namespace is relatively small (to reduce the amount of zone replication between DNS servers)
- Administration of the DNS servers is centrally performed (only one DNS zone to be administered)
- Entire namespace is entirely an internal or external namespace
- Entire namespace is entirely dynamically updated or manually updated

- **Specifying multiple DNS zones for corresponding domains and subdomains** You can specify multiple DNS zones for corresponding domains and subdomains when the

- Size of the organization's domain namespace is large and you want to reduce the number of resource records in a DNS zone (to reduce the amount of zone replication between DNS servers)
- Administration of the DNS servers must be decentralized (each geographic region, department, or other subdomains must be individually administered)
- Domain namespace includes the internal or external namespace (so you can segregate the internal namespace from the external namespace)
- Domain namespace includes dynamically updated zones and manually updated zones

For each resource you want to advertise in DNS, create a corresponding DNS resource record. Resource records can include individual computers or cluster IP addresses.

Applying the Decision

Figure 9.9 depicts a scenario where the domain namespace must be converted to DNS zones. For the purposes of this scenario, assume that

- The *activedir* subdomain contains the organization's Active Directory domain information
- The *europe*, *asia*, and *africa* subdomains must be individually administered
- The *headq* and *admin* subdomains must be individually administered
- *msft* is a top-level domain name

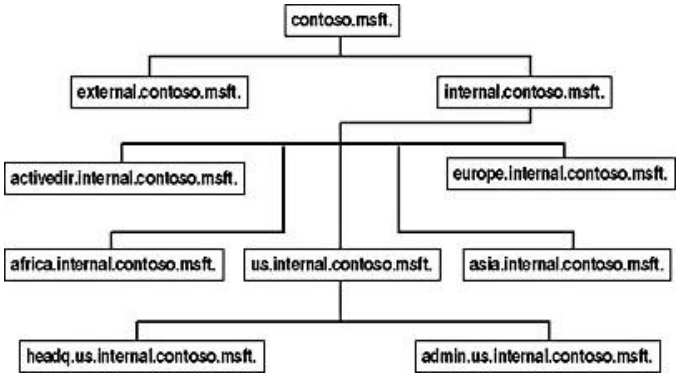


Figure 9.9 *Scenario that illustrates the appropriate decisions in converting a domain namespace to DNS zones*

Table 9.4 lists the DNS zones that can be created to achieve the organization's requirements and reason for including the DNS zones in your design.

Table 9.4 *Reasons for Including DNS Zones in Your Design*

DNS Zone	Reason for Including Zone
contoso.msft.	Organization's root domain that contains the external and internal namespace subdomains.
external.contoso.msft.	Subdomain that contains all resource records for resources accessed by Internet users.
internal.contoso.msft.	Subdomain that contains the subdomains for the organization's internal namespace.
activedir.internal.contoso.msft.	Subdomain that contains all the subdomains and resource records for Active Directory. In most designs, this zone is dynamically updated.
europe.internal.contoso.msft.	Subdomain that contains all resource records for the Europe geographic region that is administered by administrators in the same region.
africa.internal.contoso.msft.	Subdomain that contains all resource records for the Africa geographic region that is administered by administrators in the same region.
us.internal.contoso.msft.	Subdomain that contains all the subdomains for the United States geographic region that is administered by the administrators in the same region.
asia.internal.contoso.msft.	Subdomain that contains all resource records for the Asia geographic region that is administered by administrators in the same region.
headq.us.internal.contoso.msft.	Subdomain that contains all resource records for the United States geographic region and headquarters department that is administered by administrators in the same region and department.
admin.us.internal.contoso.msft.	Subdomain that contains all resource records for the United States geographic region and administration department that is administered by administrators in the same region and department.

Selecting the Zone Types

After you have evaluated the organization's domain namespace and converted the domain namespace to zones, you must determine the zone types to include in your design. Each DNS server in your design can manage one or more zones. Each zone you include on a DNS server can be a different zone type.

Making the Decision

Your design can include any combination of the following zone types:

- Active Directory integrated zones
- Traditional DNS zones

You can base your DNS design on Active Directory integrated or traditional DNS zones. DNS zone designs based on Active Directory integrated zones require that Active Directory be a part of your design. You can use traditional DNS zones with or without Active Directory.

Active Directory integrated zones are all the same in features and functions. Traditional DNS zones are either standard primary zones or standard secondary zones. Each traditional DNS zone type has unique features and functions.

The most important decision in your DNS design is the type of zone that will be *predominant* in your design. Your DNS design can be comprised of

- Only traditional DNS zones
- Only Active Directory integrated zones
- A combination of Active Directory integrated and traditional DNS zones

Traditional DNS Zones

Traditional DNS zones are identical to the DNS zones in BIND DNS servers. Traditional DNS zones

- **Store zone information in operating system files** The zone information (resource records) is stored in separate files (one for each respective zone) by the operating system. The DNS service in Windows 2000 scans these files to resolve queries within the zone.
- **Store a *single*, read-write copy of the zone information in primary zones** Traditional DNS zones can include only *one* read-write copy of the zone information, and the primary zone contains the *only* read-write copy of the zone information. The primary zone can be copied to secondary zones by using full or incremental zone transfers.

  You include primary zones in your design when you must provide read-write copies of the zone information to

  - Administer the domain namespace
  - Dynamically update the zone information
  - Create subdomains within the namespace and decrease the number of resource records within a domain
- **Store *multiple* read-only copies of the zone information in secondary zones** Traditional DNS zones can include any number of read-only copies of the zone information. The secondary zone contains these read-only copies of the zone information. A secondary zone must be replicated from an existing primary zone. A secondary zone can't contain zone information from more than one primary zone.

  You include secondary zones in your design when you need to provide additional read-only copies of the zone information

  - To unsecured portions of the network
  - For DNS servers at remote locations to reduce WAN network traffic
  - For redundancy if the primary DNS zone becomes unavailable
  - For load balancing between DNS servers
- **Replicate zone information between DNS servers by using the same zone transfer methods available to BIND DNS servers** You can replicate from primary zones to secondary zones by using full or incremental zone transfers.

You include traditional DNS zones as the predominant zone type in your design when

- **Interoperability with BIND DNS servers is desired** You can transfer zone information between BIND DNS servers and the DNS services in Windows 2000. The DNS services in Windows 2000 can support standard primary zones or standard secondary zones in relation to BIND DNS servers.
- **The organization is unwilling or unable to include Active Directory in the design** When requirements of the organization preclude Active Directory, you must include traditional DNS zones in your design.
- **Existing network support staff is familiar with BIND DNS servers** When the existing staff is experienced in the support and administration of BIND DNS servers, you can include traditional DNS zones to reduce the training and learning curve when deploying the DNS services in Windows 2000.
- ***Secured* dynamic zone updates aren't a requirement in the design** Primary DNS zones can't provide secured dynamic zone updates. Only Active Directory integrated zones can provide secured dynamic zone updates.
- **Read-only copies of the zone information must be placed on unsecured network segments** When you must place a DNS server on unsecured network segments, you want to ensure that unauthorized users can't change the DNS zone information. You can include secondary DNS zones to ensure the integrity of the DNS zone information.

Active Directory Integrated Zone Designs

Active Directory integrated zones are unique to the DNS services in Windows 2000. Active Directory integrated zones

- **Store zone information in Active Directory** The zone information (resource records) is stored in Active Directory. The DNS service scans Active Directory to resolve the DNS queries. The DNS service in Windows 2000 creates a

separate organizational unit (OU) for each zone.
- **Store a *multi-master,* read-write copy of the zone information** All copies of the Active Directory integrated zones are read-write copies of the zone information. You can modify any copy of an Active Directory integrated zone. Modifications to the Active Directory integrated zone are automatically replicated to other copies of the Active Directory integrated zone.

You include Active Directory integrated zones as your predominant zone type in your design when

- **Dynamically updated DNS zones are included in the design** Because Active Directory integrated zones are multimaster copies of the zone information, you can perform dynamic updates to *any* copy of the zone. Traditional DNS zones only support a *single* read-write copy of a zone.
- ***Secured* dynamic zone updates are a requirement in the design** Only Active Directory integrated zones can provide secured dynamic zone updates.
- **You want to reduce the administration associated with DNS replication** Because Active Directory integrated zones store the zone information in Active Directory, zone information is replicated just like any other Active Directory data.

Traditional and Active Directory Integrated Zones

You can incorporate traditional and Active Directory integrated zones in the same design. You can substitute Active Directory integrated zones for any standard primary zones in your DNS design. Active Directory integrated zones can replicate zone information to secondary zones by using traditional DNS zone replication.

Applying the Decision

In Figure 9.10, a scenario illustrates the appropriate DNS zones in the design. For the purposes of this scenario, assume that

- The organization is standardizing Active Directory as its directory service
- Each geographic region must be individually administered
- All zones must be dynamically updated

You can include Active Directory integrated zones or traditional DNS zones to create a solution. All DNS zones must be either Active Directory integrated zones or standard primary zones because all zones must be dynamically updated.

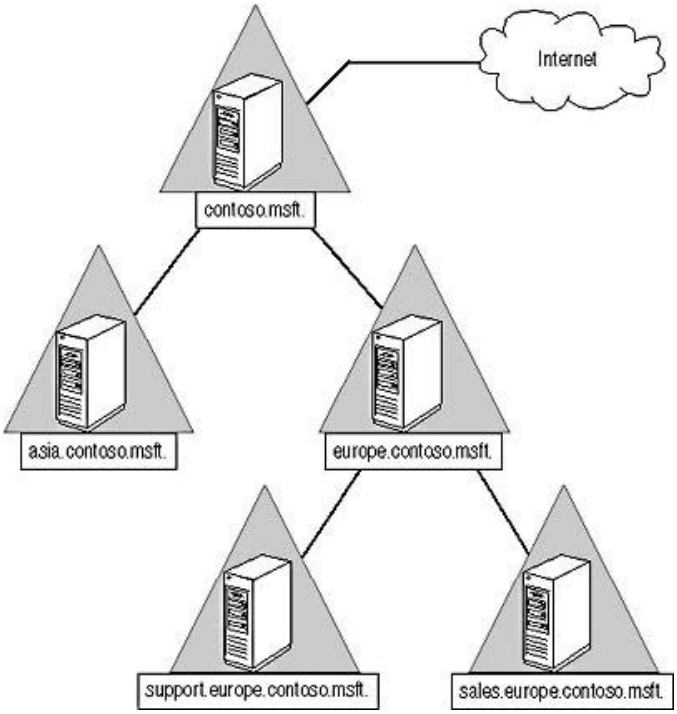


Figure 9.10 *Scenario that illustrates the appropriate selection of DNS zones in the design*

Determining the Placement of DNS Servers

You must determine where to place the DNS servers in your design so you can specify the appropriate number of DNS servers. Your design must include enough DNS servers to support the DNS zones, and ultimately the domain namespace, in your design.

Making the Decision

You must include DNS servers at each location within the organization to

- **Reduce WAN network traffic** When your design includes multiple locations, include a DNS server at each location to reduce network traffic over WAN network segments that connect the locations. By including a DNS server at each location, you allow DNS queries to be resolved locally.
- **Provide support for Active Directory domain controllers** Active Directory domain controllers make extensive use of DNS to resolve names for Active Directory objects. Include a DNS server in each location that you place an Active Directory domain controller.
- **Administer DNS at each location** Any locations that must be locally administered must include a local DNS server. The local DNS servers must manage the portion of the domain namespace that contains local subdomains and resource records.
- **Improve DNS query response times** By including a DNS server in each location, you allow DNS clients to resolve names locally. The local DNS server must contain the portion of the domain namespace commonly queried by the local DNS clients to improve query response times.
- **Provide load balancing between multiple DNS servers within the location** You can place additional DNS servers at each location to distribute DNS query traffic across the multiple DNS servers and improve performance. For more information on improving DNS performance with multiple DNS servers, see Lesson 4, "DNS Design Optimization," later in this chapter.
- **Provide redundancy with multiple DNS servers in the event of a DNS server failure** You can place additional DNS servers at each location to provide fault-tolerance for existing DNS servers within the location. For more information on enhancing DNS availability with multiple DNS servers, see Lesson 4, "DNS Design Optimization," later in this chapter.

Applying the Decision

In Figure 9.11, a scenario illustrates the appropriate placement of DNS servers in the DNS design. For the purposes of this scenario, assume that

- Performance or availability issues aren't to be considered
- The organization wants to reduce the network traffic between locations
- DNS domains and resource records that correspond to each location must be individually administered
- Active Directory domain controllers are placed at each location

You must place at least one DNS server at each location to meet the requirements of the organization. Additional DNS servers aren't required currently because performance and availability issues aren't currently considered.

Integrating DNS with Other Versions of DNS

Many of the DNS designs that you create will require you to integrate the DNS services in Windows 2000 with other versions of DNS. The most common versions of DNS that you will encounter include BIND-based and Windows NT 4.0–based DNS servers.

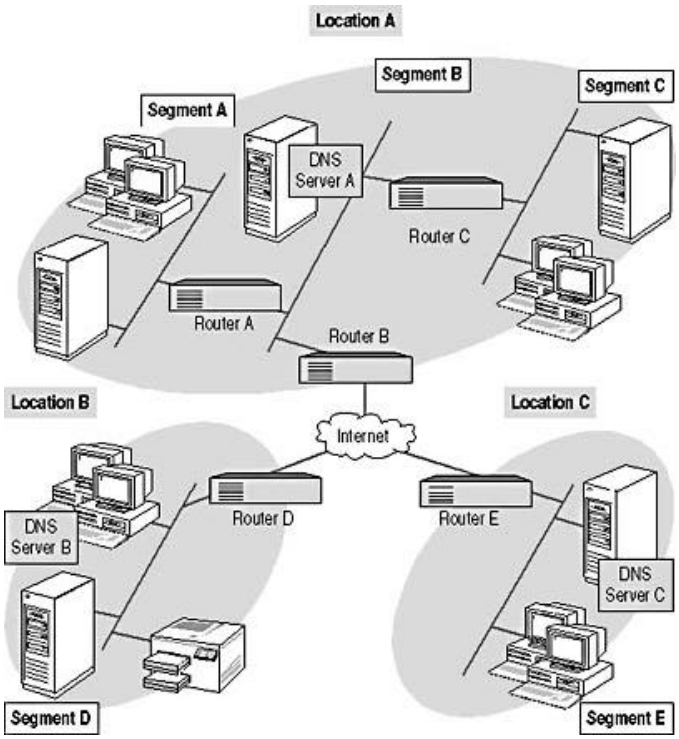


Figure 9.11 *Scenario that illustrates the appropriate placement of DNS servers*

Making the Decision

BIND DNS servers and the DNS services in Windows NT 4.0 support only traditional DNS zone types (standard primary and standard secondary zones). The design decisions for BIND-based and Windows NT 4.0–based DNS servers are the same as Window 2000–based DNS servers with traditional DNS zones.

Although Window 2000–based, BIND-based, and Windows NT 4.0–based DNS servers all support traditional DNS zones, the types of DNS resource records supported by each version of DNS server are different. In addition, not all versions of BIND-based and Windows NT 4.0–based DNS servers support dynamically updated DNS zones.

In your DNS design, you must examine each of the following integration features for all DNS servers in your design:

- Dynamically updated DNS zones
- Character set support
- RFC compliant and non-RFC compliant resource records

Dynamically Updated DNS Zones

Many solutions require *dynamically updated* DNS zones (especially those that include Active Directory) to reduce the administration of resource records in the zones. In dynamically updated DNS zones, desktop computers or automatic IP configuration servers, such as DHCP servers, automatically add and remove resource records from DNS zones. As a result, the DNS zones require little administration by network administrators.

Table 9.5 lists the type of DNS servers and the support for dynamically updated DNS zones.

Table 9.5 *Dynamically Updated DNS Zone Support Based on the Type of DNS Server*

DNS Servers	Dynamically Updated DNS Zone Support
Windows 2000	All zone types, Active Directory integrated and traditional DNS zones, support dynamic updates. Active Directory integrated zones are required to support *secured* dynamic updates. For more information on secured dynamically updated zones, see Lesson 3, "Name Resolution Protection in DNS Designs," later in this chapter.
BIND	Requires BIND 8.1.2 and later versions to support dynamically updated DNS zones.
Windows NT 4.0	Dynamically updated DNS zones aren't supported.

Character Set Supported in Zones

The DNS servers that manage the same zone must support the same character set. When you're including interoperability with other DNS servers in your design, include character sets as specified in RFC 1035. RFC 1035 is one of the core specifications for DNS on the Internet. All versions of DNS servers support the character sets as specified in RFC 1035.

The RFC 1035 specifications specify that characters you include in DNS zones include

- Only US-ASCII characters
- Uppercase and lowercase letters (A-Z, a-z)
- Numbers (0-9)
- Hyphens (-)

To provide compatibility with BIND-based and Windows NT 4.0–based DNS servers, ensure that all domain names within your domain namespace adhere to the specifications in RFC 1035. The names you must consider include

- Computer names
- Domain names
- NetBIOS names

Windows 2000 supports UTF-8 compatible characters in DNS zones. UTF-8 is a 16-bit Unicode character that supports extended ASCII characters and multiple languages. Include UTF-8 characters in your design only when all DNS servers are running Windows 2000.

Resource Records Supported in Zones

The DNS servers that manage the same zone must support the same types of resource records. The majority of DNS resource records, such as host address (A) and canonical name (CNAME) resource records, are common to all versions of DNS and are RFC compliant.

By default, most DNS servers ignore invalid resource records that are in the zone database. In addition, when most DNS servers receive invalid resource records during zone transfers, the DNS server can

- Ignore the invalid resource records
- Terminate the zone transfer when any invalid resource records are encountered

When Active Directory or WINS interoperability are included in your DNS design, your DNS zones include SRV, WINS forward lookup (WINS) resource records, or WINS reverse lookup (WINS-R) resource records. SRV records are required when Active Directory is included in your design.

WINS and WINS-R resource records are required when you want to integrate WINS and DNS in your design. For more information on WINS and DNS integration, see the following section, "Integrating DNS and WINS."

Table 9.6 lists the types of DNS resource records you may need to include in your design and the versions of DNS that support the resource record types.

Table 9.6 *Resource Record Type Support in Operating Systems*

Resource Records	Supported By
SRV	Windows 2000, Windows NT 4.0 with Service Pack 4 or later, and BIND 4.9.6 and later versions
WINS and WINS-R	Windows 2000 and Windows NT 4.0

Applying the Decision

In Figure 9.12, a scenario illustrates the integration of Windows 2000 and other DNS servers. For the purposes of this scenario, assume that

- Active Directory support is a requirement
- Future expansion might include DNS servers running on operating systems other than Windows 2000
- Secured dynamic updates must be performed on all DNS zones
- Names can also be resolved by using WINS servers

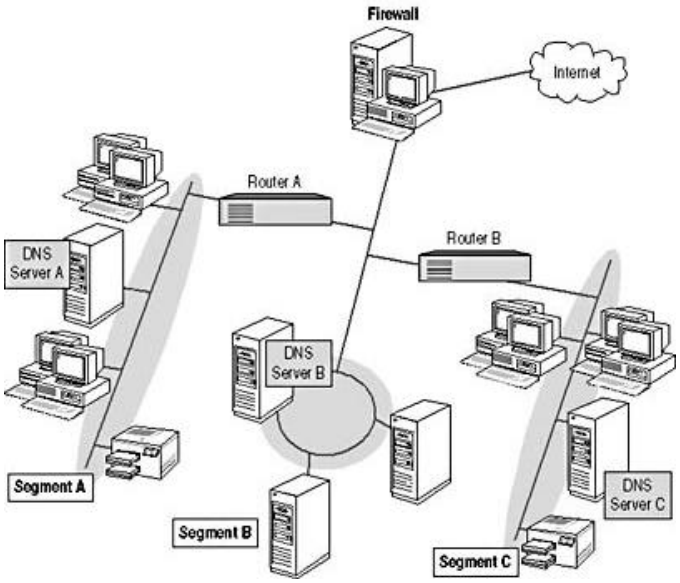


Figure 9.12 *Scenario that illustrates the integration of Windows 2000 and other DNS servers*

To fulfill the requirements of the organization, Active Directory integrated zones must be used for all zones on DNS Servers A, B, and C. Active Directory integrated zones are required because secured dynamic updates must be performed on all DNS severs.

Integrating DNS and WINS

Many of the organizations for which you create designs will have existing networks based on Windows NT 4.0. Windows NT 4.0 depends on NetBIOS names to locate network resources. As a result, the majority of organizations based on Windows NT 4.0 include WINS to register and resolve NetBIOS names.

In contrast, networks based on Windows 2000, especially network designs that include Active Directory, depend on domain

names to locate network resources. As discussed previously in this chapter, networks based on Windows 2000 include DNS to register and resolve domain names.

You can resolve domain names in WINS by integrating the DNS service and WINS Server service in Windows 2000. You can integrate DNS and WINS as part of your migration strategy or as part of your permanent solution.

Making the Decision

Networks based on Windows NT 4.0 contain all the existing computer names and domain names in the WINS databases managed by the WINS servers. You can integrate the WINS NetBIOS names into DNS by specifying

- **A subdomain in your namespace for WINS resolution** You must specify a subdomain within your namespace that acts as a container for the NetBIOS names that are resolved by WINS. When your domain namespace design includes external and internal namespaces, create the subdomain for WINS in the internal namespace.

To reduce WAN traffic, create a subdomain for each location in your design. Ensure that the subdomain includes the WINS servers in the corresponding location.

- **The order in which names are resolved** You must specify the order for name resolution in your design. You can resolve names from DNS and then WINS or from WINS and then DNS.
- **The WINS servers to integrate with DNS** You must specify the IP address for the WINS servers that provide WINS name resolution for your design. To improve the availability in your name resolution design, reference more than one WINS server in your design.

NOTE

You can integrate WINS servers running on Windows 2000 or Windows NT 4.0 in your DNS design.

Applying the Decision

In Figure 9.13, a scenario illustrates the proper integration of DNS and WINS. For the purposes of this scenario, assume that

- The existing WINS servers are running Windows NT 4.0
- The WINS databases' content on WINS Servers A, B, and C is identical
- The organization has an external namespace (*external.contoso.msft.*) and internal namespace (*internal.contoso.msft.*)

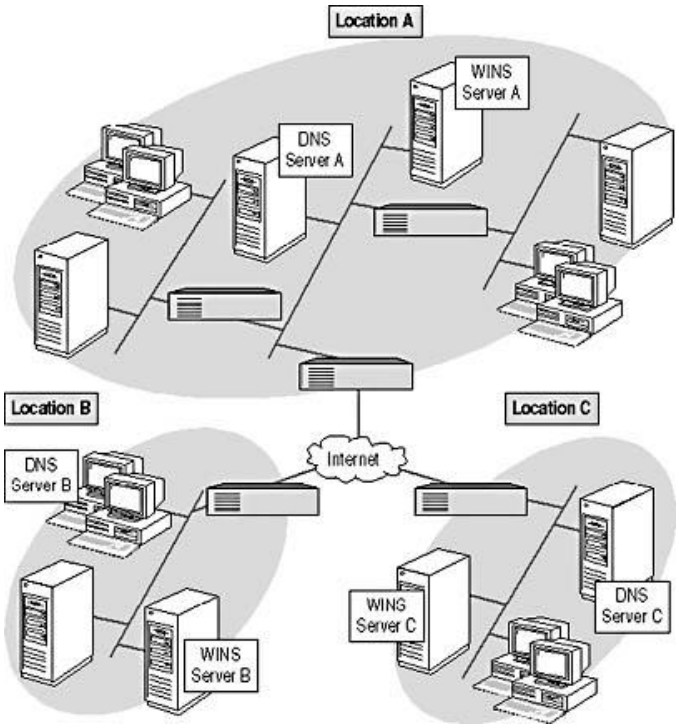


Figure 9.13 *Scenario that illustrates the integration of DNS and WINS*

You can integrate WINS into your DNS design by specifying

- Subdomains named wins.location-a.internal.contoso.msft., wins.location-b.internal.contoso.msft., and wins.location-c.internal.contoso.msft.

- Specify WINS Servers A, B, and C for each of the corresponding subdomains

Activity 9.1: Evaluating a DNS Design

In this activity, you're presented with a scenario. To complete the activity:

1. Evaluate the scenario and determine the design requirements
2. Answer questions and make design recommendations

In Figure 9.14, you see a map that illustrates the location of research facilities in a biotech consortium. The biotech consortium is comprised of eight biotech research firms working on a joint project to develop enhanced DNA sequencing equipment. Within *each* biotech research firm, a research facility is dedicated for use by the consortium.

Figure 9.14 *Map that illustrates the location of research facilities in a biotech consortium*

The consortium is deploying Windows 2000 and Active Directory for use within the research facilities dedicated for use by the consortium. Scientists working within the research facilities must be able to access resources in other research facilities.

Each research facility's private network must

- Be administered by network support engineers within the biotech firm where the research facility is located
- Provide a unique domain namespace for the consortium

Answer the following questions concerning your design recommendations. Answers to the questions can be found in the Appendix, "Questions and Answers."

1. The consortium wants to allow the biotech firm's network support engineers to select the type of DNS servers in their own locations. As a consultant to the consortium, what recommendations can you make?
2. The director of information services for the consortium wants to reduce the administration for DNS zones. The director of technology is also concerned about the security of any automated updates to DNS zones. How can you minimize the DNS administration while ensuring integrity of DNS zones?
3. While collecting requirements from the biotech firms, you discover that many of the biotech firms have existing WINS servers. The biotech firms want to incorporate these WINS servers in their DNS designs (separate from the consortium's DNS design). What recommendations can you make to the biotech firms?

3 4

Lesson 3: Name Resolution Protection in DNS Designs

This lesson discusses how to create designs that protect the integrity of the name resolution by using DNS. This lesson focuses on preventing unauthorized updates to the DNS zones.

After this lesson, you will be able to

- Prevent unauthorized dynamic updates to DNS zones
- Prevent unauthorized administration of or access to DNS servers

Estimated lesson time: 30 minutes

Preventing Unauthorized Dynamic Updates to DNS Zones

When your designs include dynamically updated DNS zones, you can prevent unauthorized users or computers from dynamically updating the DNS zones. You can dynamically update DNS zones by using client operating systems (such as Windows 2000) or IP configuration servers (such as the DHCP Server in Windows 2000).

Making the Decision

You must determine how dynamic zone updates are performed and how to secure the updates to the zone in your design.

Performing Dynamic Zone Updates

You can dynamically update the host (A) and pointer (PTR) resource records in DNS by using

- **DHCP Server in Windows 2000** Any IP configuration leased from a DHCP server in Windows 2000 can automatically update a DNS zone. You specify the DNS zone(s) that you want the DHCP server to update. On the corresponding DNS server, you specify that the DHCP server is the only computer authorized to update the records.

  Allowing DHCP to dynamically update DNS zones

  - Allows updates to DNS zone information for *any* DHCP client
  - Reduces the administration required because the DHCP server updates DNS for many clients
- **Windows 2000 DNS Client** You can specify that the DNS Client in Windows 2000 automatically update DNS zone information. You specify the DNS zone(s) you want the DHCP server to update. On the corresponding DNS server, you specify that the computer running the DNS Client is the only computer authorized to update the records.

  Allowing the DNS Client to dynamically update DNS zones

  - Requires the DNS Client in Windows 2000
  - Increases administration because each DNS Client must be configured to perform dynamic updates (however, they can be configured by using DHCP)

Securing Dynamic Zone Updates

To provide secured dynamic zone updates in your design, you must

- **Specify Active Directory integrated zones for each dynamically updated zone** You can provide secured dynamic zone updates only by using Active Directory integrated zones. Standard primary zones can't provide secured dynamic zone updates.
- **Specify the permissions to update the dynamically updated zones in Active Directory** DNS zone updates are made to the DNS zone container in Active Directory. You must specify the computer, group, or user account that is authorized to perform dynamic updates. You can assign the permissions to the entire DNS zone or to individual resource records.

  For zones that are dynamically updated by DHCP servers, you must grant the DHCP servers permissions to

  - Dynamically update corresponding zones
  - Modify all the resource records in the zone

  For zones that are dynamically updated by DNS Clients, you must grant each DNS client permission to

  - Dynamically update corresponding zones
  - Modify only the corresponding resource records in the zone

Applying the Decision

Figure 9.15 illustrates the appropriate method for securing dynamically updated zones. For the purposes of this scenario, assume that the business and technical requirements of the organization include

- Unauthorized updates to any dynamically updated DNS zones in the design must be prevented
- DHCP Server A provides automatic IP configuration for Segments A, B, and C
- Routers A and B are Routing and Remote Access-based routers that have the DHCP Relay Agent enabled and configured
- Client computers on Segments A, B, and C are running Windows 95, Windows 98, Windows Me, Windows NT 4.0, and Windows 2000

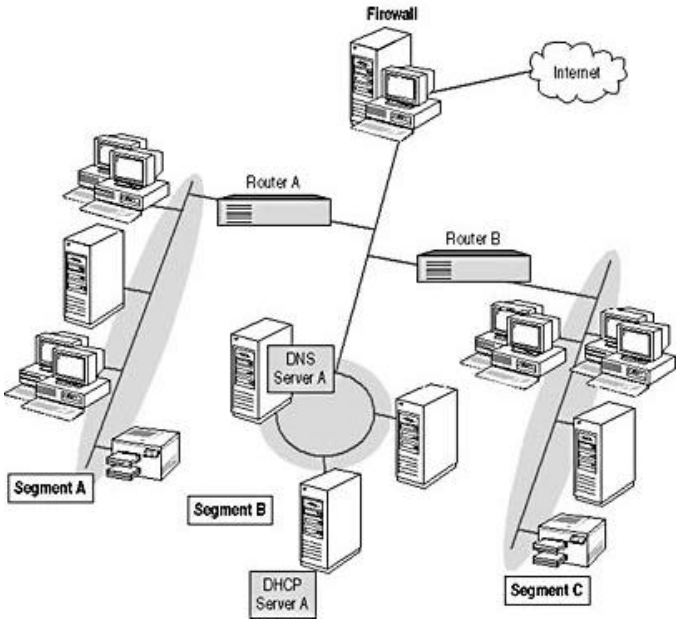


Figure 9.15 *Scenario to illustrate the appropriate method for securing dynamically updated zones*

To ensure that you achieve the requirements of the design, you must specify that

- All zones on DNS Server A are Active Directory integrated zones
- DHCP Server A dynamically updates DNS zones
- Only DHCP Server A has the permission to update the *entire* DNS zone(s)

DHCP updates to the DNS zones are required because the client computers run operating systems other than Windows 2000. Only the DNS Client in Windows 2000 can dynamically update DNS zones.

Preventing Unauthorized Access to DNS Servers

To ensure the integrity of the DNS zones, you must prevent unauthorized users from directly accessing the DNS server. You can include various methods of preventing unauthorized access to DNS servers based on the zone types (such as Active Directory integrated or standard primary zones).

Making the Decision

You can prevent unauthorized users from compromising the integrity of the DNS zones by

- **Restricting DNS administrators** Grant only authorized network administrators the permission to manage DNS servers. Create a Windows 2000 group and assign the group permissions to manage DNS servers in the organization. Include the authorized network users in the Windows 2000 group that you created.
- **Isolating read-write copies of DNS zones from public networks, such as the Internet** Ensure that unauthorized or anonymous users can access *only* standard secondary zones. Because secondary zones are read-only, the unauthorized or anonymous users can't modify the contents of the DNS zone.
- **Isolating zones that manage internal namespaces from public networks, such as the Internet** Ensure that unauthorized or anonymous users can access *only* the external portions of the organization's namespace. Ensure that *all* the computers, or clusters, in the external namespace meet one of the following criteria:
  - Can be accessed by unauthorized or anonymous users
  - Provide sufficient security to protect confidential data from unauthorized or anonymous users
- **Requiring only Active Directory integrated zones** Within the private network, Active Directory integrated zones provide enhanced security because users don't have direct access to the zone information. Include Active Directory integrated zones to protect the integrity of the zones within your private network.

Applying the Decision

Figure 9.16 illustrates the proper methods for preventing unauthorized user access to DNS servers. For the purposes of this scenario, assume that the business and technical requirements of the organization include

- Active Directory must be supported within the organization
- Unauthorized access to DNS servers that manage the organization's internal namespace must be prevented
- DNS Servers A, B, and C manage the DNS zones that contain the organization's internal namespace
- DNS Server D manages the DNS zone that contains the organization's external namespace

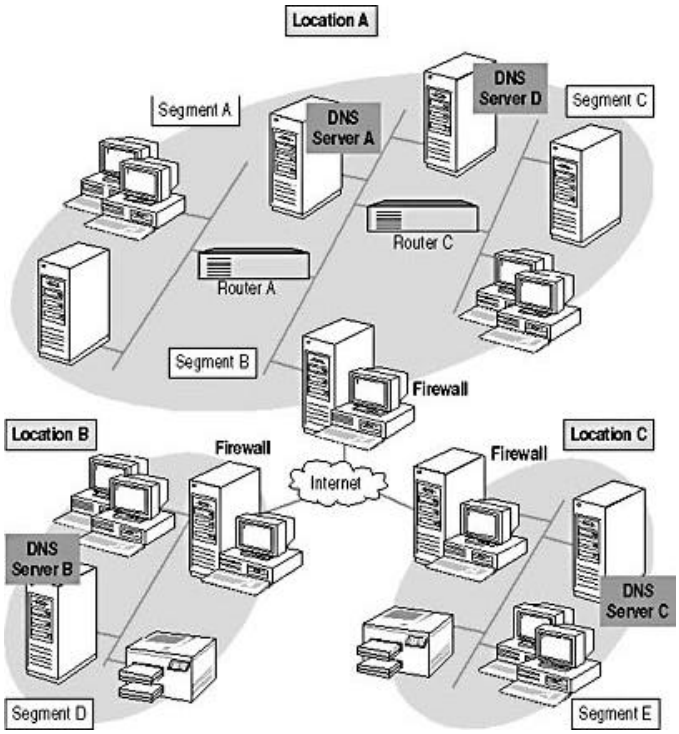


Figure 9.16 *A scenario that illustrates the proper methods for preventing unauthorized user access to DNS servers*

To ensure that you achieve the requirements of the design, you must specify that

- All zones on DNS Server D are standard secondary zones
- All zones on DNS Servers A, B, and C are Active Directory integrated zones
- Firewalls prevent unauthorized access to DNS Servers A, B, and C
- The firewall at Location A allows unauthorized or anonymous access to DNS Server D
- All resource records in the zones managed by DNS Server D point to servers that should be accessed by Internet users

3 4

Lesson 4: DNS Design Optimization

This lesson discusses how to optimize DNS designs to improve the availability and performance characteristics in your design. This lesson focuses on the strategies that increase the percentage of time that computers can resolve DNS queries and that decrease any latency in resolving DNS queries.

After this lesson, you will be able to

- Select the appropriate method for enhancing the availability characteristics in your DNS design
- Select the appropriate methods for improving the performance characteristics in your DNS design

Estimated lesson time: 20 minutes

Enhancing DNS Availability

Once you have established the essential aspects and security aspects of your DNS design, you can optimize the design for availability. The business requirements of the organization may require your design to ensure DNS query resolution at all

times, and as such, require you to provide redundancy for the DNS servers in your design, regardless of a single point of failure.

Making the Decision

You can improve the availability of your DNS designs by

- Replicating DNS zones across multiple DNS servers
- Using Microsoft Windows Clustering server clusters
- Dedicating a computer to running DNS

Multiple DNS Servers with Replicated Zones

You can distribute DNS query traffic for a DNS zone across two DNS servers. You can replicate the zones between the two DNS servers to ensure that both servers return the same responses to DNS queries. If one DNS server fails, the remaining DNS server can provide DNS name resolution.

You must specify that the DNS clients in the design include both DNS servers in the list of DNS servers to use for name resolution. If you specify only one of the DNS servers in the DNS clients, the DNS clients are unaware of the remaining DNS server.

You can replicate zone information between

- **Two Active Directory integrated zones** You can replicate zone information between any two DNS servers that support Active Directory integrated zones. Querying either DNS server returns the same DNS query results.
- **Standard primary and secondary zones** You can replicate zone information between a DNS server that supports a standard primary zone and a DNS server that supports a standard secondary zone. Querying either DNS server returns the same DNS query results.

If the DNS server that supports the standard primary zone fails, no updates can be made to the zone (including dynamic zone updates). To ensure that zone updates can always be performed, select Active Directory integrated zones or Windows Clustering server clusters instead.

The primary advantage of multiple DNS servers with replicated zones in comparison to server clusters is that no additional hardware and software resources are required. The disadvantage of multiple DNS servers with replicated zones is that there is no automatic *failover*. If the failed DNS server is configured in the DNS clients to be queried first, the DNS clients experience a delay in DNS query resolution. The delay in query resolution results from the DNS client waiting for a response from the first (and now failed) DNS server, before timing out and proceeding to the next DNS server in the list.

Figure 9.17 illustrates how multiple DNS servers with replicated zones provide enhanced availability. For the purposes of this scenario, assume that the business and technical requirements of the organization include

- Active Directory must be supported within the organization
- Dynamic updates must always be performed, regardless of the failure of any DNS server
- DNS Servers A and B manage the same DNS zones that contain the organization's namespace

To ensure that you achieve the requirements of the design, you must specify that

- All zones are Active Directory integrated zones
- All zones are replicated between DNS Servers A and B
- DNS clients and all network segments are configured to use both DNS Servers A and B to perform name resolution

Active Directory integrated zones are required because the organization requires dynamic updates to be performed, regardless of which DNS server fails.

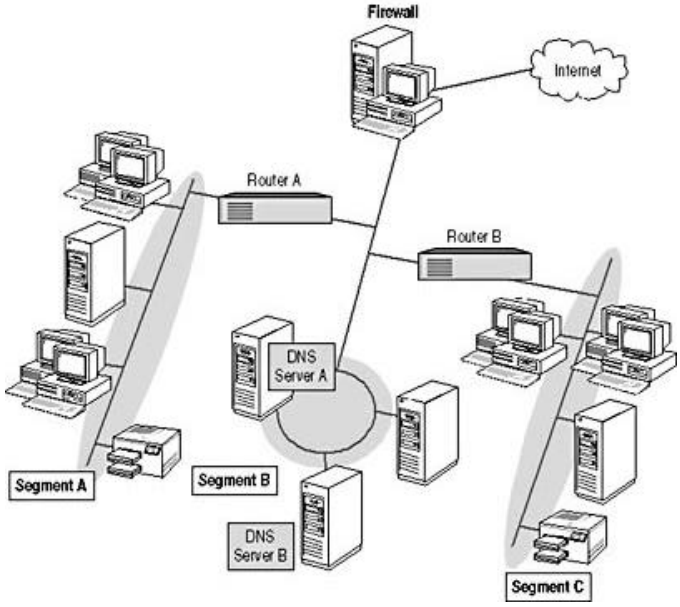


Figure 9.17 *Example of how multiple DNS servers with replicated zones provide enhanced availability*

Windows Clustering Server Clusters

For DNS servers that use standard DNS zones, you can utilize Windows Clustering server clusters to provide enhanced availability. The DNS Server service in Windows 2000 is a *cluster-unaware* application. *Cluster-aware* applications can interact with Windows Clustering server clusters by using Windows Clustering application programming interfaces (APIs). Cluster-unaware applications can run on Windows Clustering server clusters, but can't communicate with the cluster by using Windows Clustering APIs.

NOTE

Active Directory integrated zones store the zone resource records in Active Directory. As a result, you cannot use Windows Clustering server clusters to improve the availability of DNS servers that manage Active Directory integrated zones.

You can store the DNS zones on a common *cluster drive* between two computers. The cluster drive is attached to a SCSI bus common to both computers, also known as *cluster nodes*, in the cluster.

Figure 9.18 illustrates the components in a Windows Clustering server cluster. The DNS Server service actually runs on only one of the cluster nodes at a time. The DNS zones are stored on the shared cluster drive. The cluster node currently running the DNS Server services is known as the *active node* for DNS.

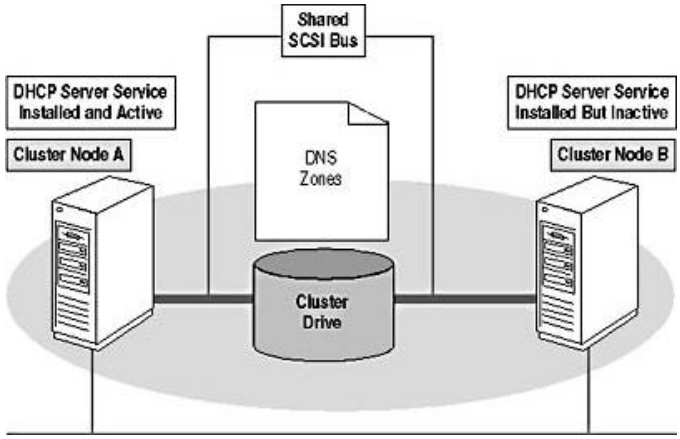


Figure 9.18 *Components in a Windows Clustering server cluster*

If the DNS active node fails, the remaining cluster node automatically starts the DNS Server service. Because the DNS zones are stored on the shared cluster drive, the redundant DNS Server service has the current DNS zone contents from the failed cluster node.

The primary advantages to DNS on server clusters are

- The redundant cluster node automatically starts and no action is required on the part of the network administrators
- The DNS zones are stored on the cluster drive and are available to either cluster node. As a result, DNS clients will be

unaware of the failure

For more information on Window Clustering server clusters, see the Windows 2000 help files on how to support cluster-unaware applications.

Dedicating a Computer to DNS

By dedicating a computer to running DNS, you improve availability by preventing other applications or services from becoming unstable and requiring the DNS server to be restarted.

Applying the Decision

Figure 9.19 illustrates the proper methods for enhancing the availability of a DNS design.

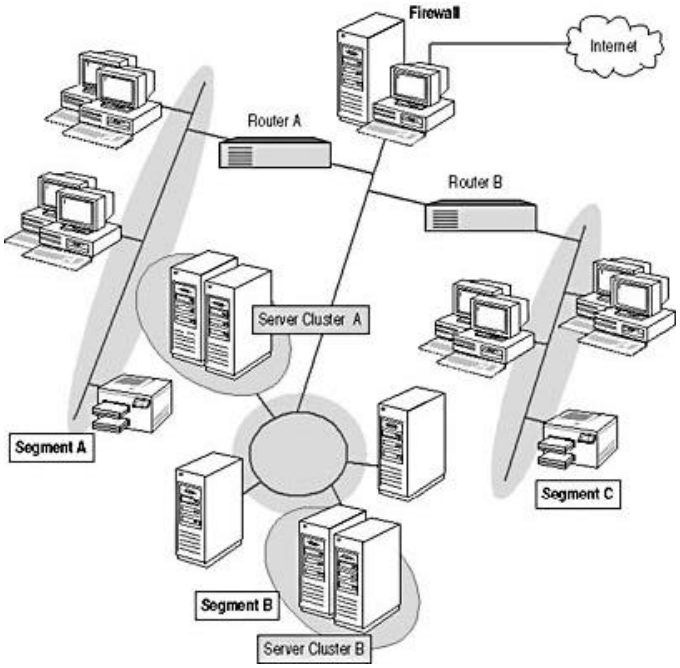


Figure 9.19 *Scenario to illustrate the proper methods for enhancing the availability of a DNS design*

For the purposes of this scenario, assume that the business and technical requirements of the organization include

- Any failure of a DNS server is automatically corrected
- DNS clients perceive no changes in the DNS server configuration
- Secured dynamic updates must be performed at all times
- Server Cluster A supports the internal namespace of the organization
- Server Cluster B supports the external namespace of the organization

To provide the proper solution, Windows Clustering server clusters must be used to achieve the business and technical requirements of the organization. Server Clusters A and B have the DNS Server service installed on both cluster nodes, but active on only one cluster node. Server Cluster A provides DNS name resolution for all network segments within the private network. Server Cluster B provides DNS name resolution for all network segments within the private network and the Internet.

Improving DNS Performance

Once you have established the essential aspects, the security aspects, and availability aspects of your DNS design, you can optimize the design for performance. The business requirements may include that DNS name resolution must occur within a given period of time, based on the number of simultaneous DNS queries.

Making the Decision

You can improve the performance of your DNS designs by

- Reducing DNS query resolution latency
- Reducing or rescheduling DNS zone replication traffic
- Dedicating a computer to running DNS

Reducing DNS Query Resolution Latency

You can reduce the length of time to perform DNS queries by

- **Placing DNS servers at remote locations** You can reduce the WAN traffic between locations by placing DNS servers at remote locations. By providing local name resolution, the DNS server improves DNS query response times within the remote location.
- **Load balancing DNS queries across multiple DNS servers** When the existing DNS servers are saturated and you can't upgrade the hardware to improve performance, you can add additional DNS servers to your design.

Evenly distribute the DNS clients across the multiple DNS servers, ensuring that each DNS server responds to approximately the same number of DNS queries over a period of time. You must configure the DNS clients in your network to utilize different servers as their primary DNS server to distribute DNS queries across the multiple DNS servers. You can utilize DHCP to reduce the administration in configuring the DNS clients to distribute DNS queries between the multiple DNS servers.

- **Dividing domains into subdomains** As the number of resource records in a zone becomes larger, the DNS server requires a longer period of time to find a resource record in the zone. To improve query resolution time, you can

- Specify two or more subdomains beneath the current domain
- Divide the existing resource records evenly between the new subdomains
- Specify that the original domain forward appropriate DNS queries to the new subdomains

When you create subdomains in the manner previously described, you create *delegated domains*. Delegated domains contain a subset of the parent domain. The parent domain *delegates* the responsibility for query resolution to these subdomains.

Because the delegated domains contain a subset of the resource records in the original domain, the DNS server spends less time searching the zone, and subsequently resolves DNS queries faster.

- **Including caching-only DNS servers** Caching-only DNS servers don't store DNS zone information in file or Active Directory, but rather cache responses to DNS queries in local memory. Because the caching-only DNS server locally caches responses to DNS queries, you can reduce traffic to other DNS servers in the network.

The advantages of caching-only DNS servers include

- Responses to DNS queries are cached locally
- Zone transfers aren't required

You can include caching-only DNS servers in your design to provide local caching of DNS queries at remote locations without performing zone transfers. However, caching-only DNS servers require another DNS server to forward DNS queries to and receive DNS query replies from.

Placing caching-only DNS servers at remote locations is recommended when the

- Network connections between locations are reliable
- Caching-only DNS servers forward queries to reliable DNS servers

Placing a DNS server at remote locations with an Active Directory integrated or traditional DNS zone is recommended when

- Network connections between locations are unreliable
- DNS servers at other locations are unreliable
- Network traffic generated by zone replication is acceptable

Reducing or Rescheduling DNS Zone Replication Traffic

You can reduce network capacity utilized by DNS zone replication traffic by

- **Placing caching-only DNS servers at remote locations** Because caching-only DNS servers don't store a complete copy of the zone locally, zone replication isn't necessary.
- **Perform incremental zone transfers** You can perform incremental zone transfers to reduce the network traffic in comparison to full zone transfers. Incremental zone transfers utilize less network traffic because only updates to the zone resource records are transmitted. Full zone transfers resend all zone resource records.
- **Perform fast zone transfers** DNS servers running Windows 2000 support fast zone transfers. Fast zone transfers send multiple zone resource records updates at a time and compress the zone updates. The combination of sending multiple zone resource records at a time and the compression of zone updates results in a reduction in network utilization.

You can also prevent zone replication traffic from overutilizing network capacity by performing zone updates during nonpeak periods of network activity.Although rescheduling zone replication doesn't reduce the network traffic, the impact on the network capacity is averted during peak periods of operation.

Dedicating a Computer to DNS

By dedicating a computer to running DNS, you improve the performance because you prevent other applications or services from consuming system resources.

Applying the Decision

Figure 9.20 illustrates a DNS design prior to optimization for performance. For the purposes of this scenario, assume that the business and technical requirements of the organization include

- Active Directory must be supported as the directory service
- DNS Server A manages the internal namespace for the organization
- DNS Server B manages the external namespace for the organization
- Locations B and C must be able to provide DNS name resolution if the Internet connection is lost or the DNS servers at Location A fail
- Network utilization between locations is currently 14 percent of capacity with no significant increases over the last 12 months
- Organization's e-commerce Web site is expected to expand more than 300 percent over the next 12 months

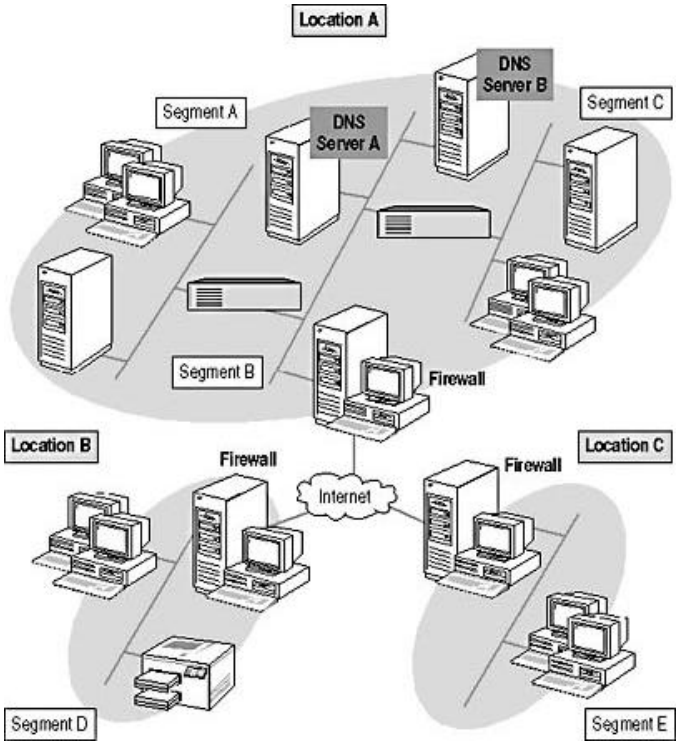
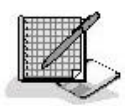


Figure 9.20 *Scenario to illustrate a DNS design prior to optimization for performance*

Figure 9.21 illustrates a DNS design after optimization for performance. The following performance optimization changes were made to the design.

- DNS Server C is installed to provide local DNS name resolution at Location B.
- DNS Server D is installed to provide local DNS name resolution at Location C.
- DNS Server E is installed to distribute DNS queries between DNS Servers B and E because of the increase in the e-commerce Web site.

Activity 9.2: Completing a DNS Design



In this activity, you're presented with a scenario. To complete the activity:

1. Evaluate the scenario and determine the design requirements
2. Answer questions and make design recommendations

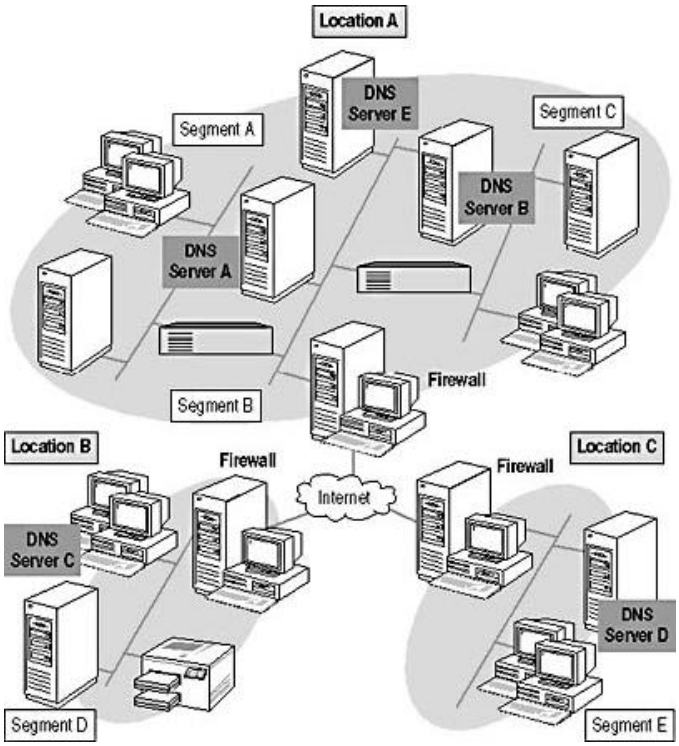


Figure 9.21 *Scenario to illustrate a DNS design after optimization for performance*

In Figure 9.22, you see a map that illustrates the location of research facilities in a biotech consortium. As the consultant retained to create the original DNS design, you're in the process of revising the design to incorporate technical changes and differences in business practices. You're revising the design to reflect the current security, availability, and performance requirements of the biotech consortium.

Answer the following questions concerning your design recommendations. Answers to the questions can be found in the Appendix, "Questions and Answers."

1. The biotech consortium is concerned about Internet users gaining access to the servers and resources in each research facility. What specifications can you include in your design to prevent Internet users from modifying the contents of consortium's DNS zones?

Figure 9.22 *Map that illustrates the location of research facilities in a biotech consortium*

2. Six months after the initial deployment of your DNS design, some of the research facilities are experiencing delays in domain name resolution. What recommendations can you make to improve the DNS query response times?
3. The director of research for the biotech consortium obtained a Web-based groupware application that allows research scientists to collaborate on their research. Because the research scientists are located throughout the world, the servers that host the groupware application must be accessible at all times. How can you ensure that these requirements are achieved?

Lab: Creating a DNS Design

After this lab, you will be able to

- Evaluate a scenario and determine the design requirements
- Create a DNS based on the design requirements

Estimated lab time: 45 minutes

In this lab, you're the director of information services for a university and are responsible for creating a DNS design for the university. The university has 12 buildings arranged in a campus setting.

To complete this lab:

1. Examine the networking environment presented in the scenario, the network diagrams, the business requirements and constraints, and the technical requirements and constraints
2. Use the worksheet(s) for each location and router to assist you in creating your DNS design (you can find completed sample design worksheets on the Supplemental Course Materials CD-ROM in the Completed Worksheets folder)

NOTE

For each location there are four worksheets, one worksheet for each DNS server. If your design contains fewer than four DNS servers, leave the remaining worksheets blank.

3. Create, eliminate, or replace existing networking devices and network segments when required
4. Ensure that your design fulfills the business requirements and constraints and technical requirements and constraints of the scenario by

- Determining the number of DNS servers to include in each building
- Including the appropriate zones that each DNS server will manage
- Including dynamic updates, or secured dynamic updates, for the appropriate zones
- Including the appropriate WINS lookups for appropriate zones
- Including the appropriate zone replication method for each zone
- Optimizing your design to provide security, availability, performance, and affordability

NOTE

To reduce the length of time for this lab, create a DNS design for only three of the university buildings.

Scenario

A science and engineering university is migrating its existing DNS design to accommodate the increase in student population and faculty. The university has 12 buildings organized in a campus setting.

Figure 9.23 is a map of the buildings in the university's campus. Point-to-point leased lines currently connect the buildings to one another. The university is migrating the existing point-to-point leased lines to a public ATM backbone. The new ATM backbone will provide higher speed data rates between the buildings in the campus. The university is connected to the Internet by three T3 leased lines in the Administration Building.

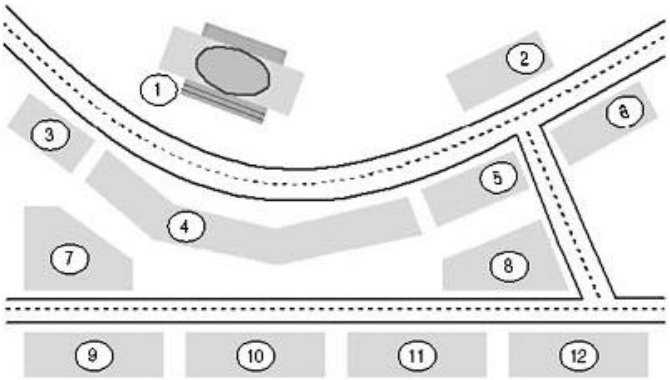


Figure 9.23 *Map of the buildings in the university's campus*

Building	Description	Building	Description
1	Administration Building	2	Student Union and Campus Security
3	Chemistry	4	Mathematics and Computer Science
5	Physics	6	Mechanical Engineering
7	Field House/Gymnasium	8	Performing Arts Center
9	Electrical Engineering	10	Civil Engineering
11	Fine Arts	12	Liberal Arts

The network in each university building supports

- The administrative staff, faculty, and student work-study program participants who work in the individual university departments
- Interactive kiosks that students can use to access their own information, class schedules, professor office schedules, and other pertinent information
- 10BaseT Ethernet connectivity for students who use laptops
- Computer-based labs for use by the students to complete course assignments

The following table lists each building on the university's campus and the corresponding figure that illustrates the existing network in that building.

Building	Figure
Administration Building	Figure 9.25
Student Union and Campus Security	Figure 9.26
Chemistry and Physics	Figure 9.27
Mathematics and Computer Science	Figure 9.28

Business Requirements and Constraints

The university has a number of requirements and constraints based on the business model of the university. As you create your DNS design, ensure that your design meets the business requirements and stays within the business constraints.

To achieve the business requirements and constraints, your design must

- Prevent students from accessing resources and data that are for exclusive use by the faculty and administrative staff
- Prevent Internet users from accessing resources and data that are for exclusive use by the faculty and administrative staff
- Provide Internet access to all faculty, administrative staff, and students
- Support Active Directory as the directory service for the university
- Provide an Internet presence for the university that is hosted on the Web servers in the Administration Building
- Ensure that the Internet presence for the university is available 24 hours a day, 7 days a week
- Ensure that the interactive student kiosks are available during normal hours of operation for each respective building

Technical Requirements and Constraints

The existing physical network, hardware, and operating systems place certain technical requirements and constraints on your design. As you create your DNS design, ensure that your design meets the technical requirements and stays within the technical constraints.

In addition, the applications that run within the university require connectivity within each building, with other buildings, and

with the Internet. These applications run on the computers used by the faculty, administrative staff, and student work-study program participants and on computers used in interactive kiosks. These applications require DNS domain name resolution to function properly.

To achieve the technical requirements and constraints, your design must

- Utilize the university's existing domain namespace
- Isolate the university's internal namespace from Internet access
- Isolate the internal namespaces that are designated for use by the students from the network segments designated for use by the faculty, administrative staff, and student work-study program participants
- Integrate with the existing DHCP servers in the design that provide IP configuration for desktop and laptop computers
- Integrate with the existing WINS servers in the design that provide NetBIOS name resolution
- Reduce the administration associated with DNS while ensuring that DNS zone integrity is maintained
- Ensure that in the future BIND version 8.2.1 DNS servers can be integrated into the design (although none are to be included in your initial design)

The university's domain namespace, shown in Figure 9.24, can be described as follows.

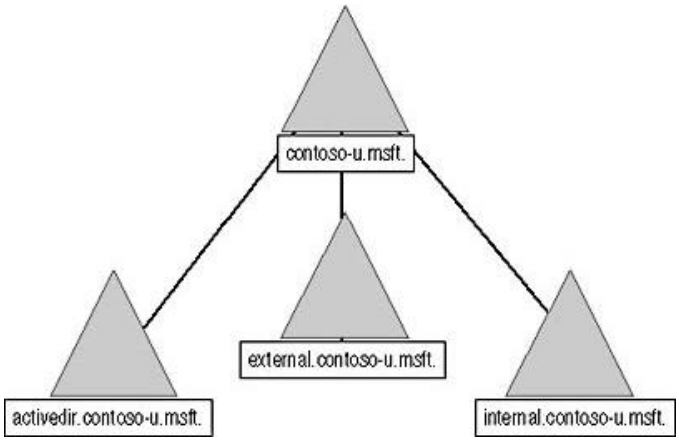


Figure 9.24 *Diagram of the university's existing domain namespace*

- *activedir.contoso-u.msft.* is the domain that contains the Active Directory domain namespace. All subdomains and resource records required by Active Directory are contained beneath this domain. The domain must be available to each network segment if ATM backbone fails.
- *external.contoso-u.msft.* is the domain that contains the resource records for all the resources accessed by Internet users. Network administrators located on Segment F administer the domain. The domain must be accessible to Internet users that access the Web servers on Segment B (Internet users can only access Segment B).
- *internal.contoso-u.msft.* is the domain that contains the resource records for all the resources and computers that aren't defined by Active Directory (such as computers running UNIX or Macintosh operating systems). Network administrators located on Segment F administer the domain. The domain must be available to each network segment if the ATM backbone fails.

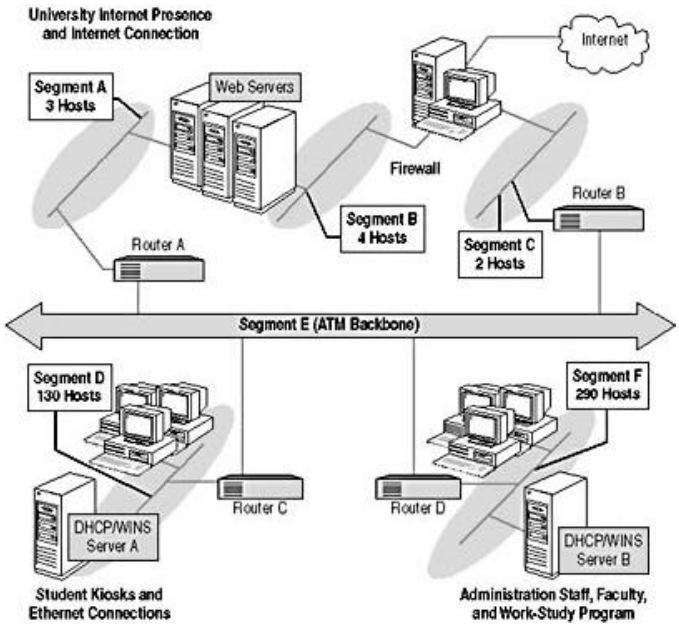


Figure 9.25 *Existing network at the Administration building*

Design Worksheet – Figure 9.25
Administration Building – DNS Server A

DNS Server A Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.25
Administration Building – DNS Server B

DNS Server B Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.25
Administration Building – DNS Server C

DNS Server C Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.25
Administration Building – DNS Server D

DNS Server D Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated (specify replica zones in Comments column)	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.25
Administration Building – DNS Clients

Segment	DNS Client Specifications	Comments
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	

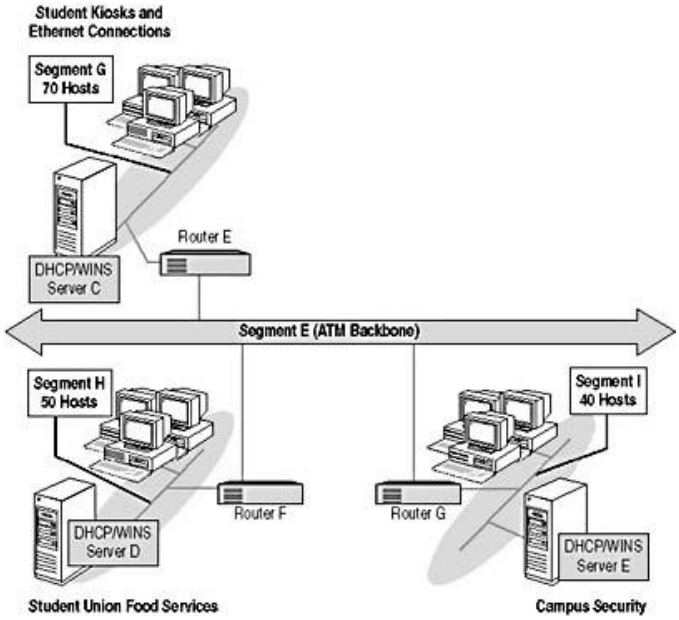


Figure 9.26 *Existing network at the Student Union and Campus Security building*

Design Worksheet – Figure 9.26
Student Union and Campus Security Building – DNS Server A

DNS Server A Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.26
Student Union and Campus Security Building – DNS Server B

DNS Server B Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.26
Student Union and Campus Security Building – DNS Server C

DNS Server C Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.26
Student Union and Campus Security Building – DNS Server D

DNS Server D Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated (specify replica zones in Comments column)	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.26
Student Union and Campus Security Building – DNS Clients

Segment	DNS Client Specifications	Comments
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	

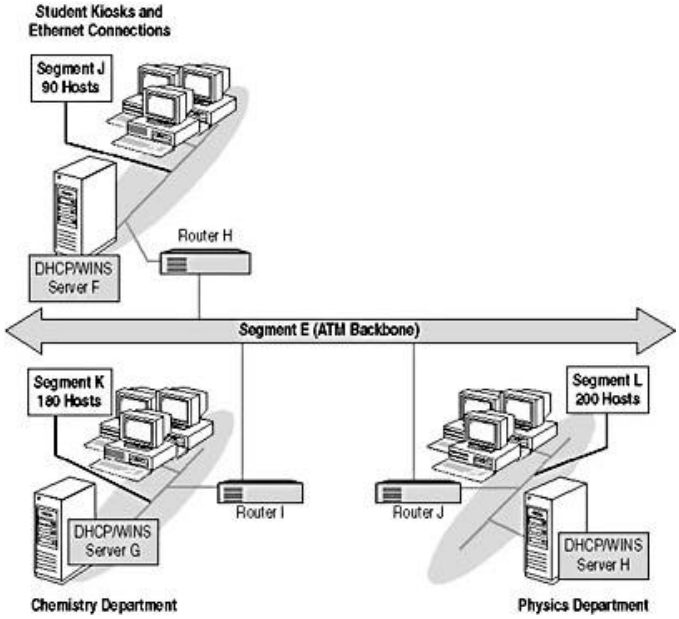


Figure 9.27 *Existing network at the Chemistry and Physics buildings (assume that these buildings have the same network configuration)*

Design Worksheet – Figure 9.27
Chemistry and Physics Building – DNS Server A

DNS Server A Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.27
Chemistry and Physics Building – DNS Server B

DNS Server B Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.27
Chemistry and Physics Building – DNS Server C

DNS Server C Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.27
Chemistry and Physics Building – DNS Server D

DNS Server D Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated (specify replica zones in Comments column)	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.27
Chemistry and Physics Building – DNS Clients

Segment	DNS Client Specifications	Comments
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	

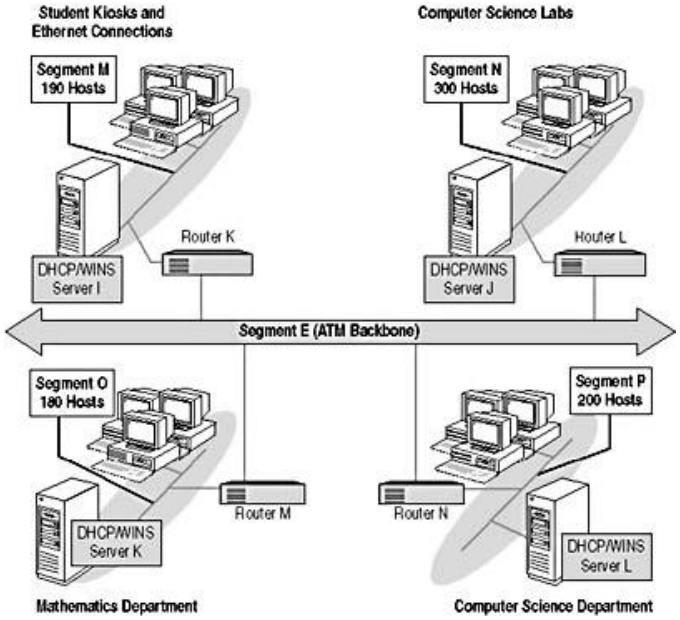


Figure 9.28 *Existing network at the Mathematics and Computer Science building*

Design Worksheet – Figure 9.28
Mathematics and Computer Science Building – DNS Server A

DNS Server A Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.28
Mathematics and Computer Science Building – DNS Server B

DNS Server B Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.28
Mathematics and Computer Science Building – DNS Server C

DNS Server C Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.28
Mathematics and Computer Science Building – DNS Server D

DNS Server D Specifications	Comments
DNS server connects to segment: _____	
❑ Install on cluster node Cluster name: _____	
Zone A Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone B Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	
Zone C Domain name: _____	
❑ Active Directory integrated	
❑ Standard Primary (specify DNS servers to replicate to in Comments column)	
❑ Standard Secondary (specify DNS servers to replicate from in Comments column)	
❑ Incremental zone transfers and or fast zone transfers	
❑ Dynamic updates ❑ Secured (specify permissions in Comments column)	
❑ Update with DHCP Server DHCP server: _____	
❑ Update with DNS Client	
❑ WINS lookup WINS server: _____	
Character set ❑ ASCII ❑ UTF-8	

Design Worksheet – Figure 9.28
Mathematics and Computer Science Building – DNS Clients

Segment	DNS Client Specifications	Comments
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	
	❑ Enable dynamic DNS zone updates DNS Server List 1: _____ 2: _____ 3: _____ 4: _____	

3 4

Review

The following questions are intended to reinforce key information in this chapter. If you're unable to answer a question, review the lesson and then try to answer the question again. Answers to the questions can be found in the Appendix, "Questions and Answers."

1. An organization is creating a design in preparation for the deployment of Windows 2000 and Active Directory. The organization has an existing DNS infrastructure based on BIND version 8.2.1 DNS servers. What additional information must you collect to determine the requirements and constraints for a DNS design?
2. You're creating a DNS design for an organization that has existing BIND DNS servers. The organization is deploying Active Directory and requires the DNS design to support the Active Directory deployment. The organization has an existing external and internal namespace and wants to reduce the administration of DNS by automatically populating the DNS zone resource records. However, the organization wants to protect the integrity of the DNS resource records. What recommendations can you make to the organization?
3. You're evaluating an existing DNS design for an Internet-based auction firm that has a significant e-commerce Web presence. The auction firm sells collectibles, memorabilia, celebrity estate items, and other rare goods. The director of information services for the auction firm is concerned about the ability of the Windows 2000–based DNS servers to provide name resolution at all times, regardless of a single point of failure. What changes to the design can you recommend to ensure that customers always *transparently* resolve domain names and subsequently access the e-commerce Web site?
4. An aerospace engineering firm that designs and builds satellite launch vehicles has retained your services to evaluate the existing DNS design. The firm started three years ago as a small entrepreneurial firm. In the last three years, the number of users, and corresponding computers, in the firm has tripled each year. Users are noticing a delay when initially accessing resources and accessing Active Directory. You determine that the DNS query response times are the root cause for the delays users are experiencing. After examining the network segment and router utilization, you determine that the network segments and routers aren't the source of the DNS query latency. What changes to the DNS design can you recommend to resolve these performance issues?