

Planning Name Resolution and Internet Protocol Addressing

As an enterprise administrator, you will be responsible for the overall IT environment and architecture within your organisation. Enterprise administrators translate business goals into technology decisions; design midrange to long-term strategies; and make key decisions and recommendations about, for example, network infrastructure, directory services, security policies, business continuity, administrative structure, best practices, standards and service-level agreements (SLAs).

The enterprise administrator is responsible for infrastructure design and global configuration changes. If you intend to extend your career and become an enterprise administrator (or if you already carry out enterprise administrator tasks and want to acquire a certification that matches your experience), you will already be an experienced network and server administrator with typically two or more years' experience administering corporate networks. The 70-647 exam is not designed for beginners; nor is this Course. Only 20 percent of the 70-647 exam focuses on your skills in performing tasks; it is primarily focused on strategic planning and designing Microsoft Windows Server 2008 R2 technologies to satisfy the information technology needs of the business.

As an experienced administrator, you will almost certainly be familiar with name resolution and Internet Protocol version 4 (IPv4) addressing. You will probably have come across Internet Protocol version 6 (IPv6) addresses but might not be familiar with them. This chapter does not attempt to cover old ground but, rather, looks at the new features and approaches implemented in Windows Server 2008 R2.

IMPORTANT EXAM OBJECTIVES

The objectives related to name resolution and IP addressing in the 70-647 exam are similar to those in the 70-646 Windows Server 2008 Server Administration exam. If you have previously taken Home Learning College's MCTS Self-Paced Training Kit: (Exam 70-646) Course, you will find that this chapter discusses topics that you have already studied. In this case, please treat this material as review.

Exam objectives in this chapter:

- Plan for name resolution and IP addressing.

Before You Begin

To complete the lessons in this chapter, you must have done the following:

- Installed Windows Server 2008 R2 Enterprise on a server configured as a domain controller in the contoso.internal domain. Active Directory–integrated Domain Name System (DNS) is installed by default on the first domain controller in a domain. The computer name is Glasgow. Configure a static IPv4 address of 10.0.0.11 with a subnet mask 255.255.255.0. The IPv4 address of the DNS server is 10.0.0.11. Other than IPv4 configuration and the computer name, accept all the default installation settings. You can obtain an evaluation version of the Windows Server 2008 R2 Enterprise software from the Microsoft Download Center at <http://tinyurl.com/cdxh8g>.
- Installed Windows 7 Business, Enterprise or Ultimate on a client computer joined to the contoso.internal domain. The computer name is Melbourne. Initially, this computer should have a static IPv4 address of 10.0.0.21 with a subnet mask 255.255.255.0. The IPv4 address of the DNS server is 10.0.0.11. You can obtain evaluation software that enables you to implement the Windows 7 Enterprise 30-day evaluation edition at <http://tinyurl.com/cdxh8g>.
- Created a user account with the username Kim_Akers and password P@ssw0rd and added this account to the Domain Admins, Enterprise Admins and Schema Admins groups.
- It's recommended that you use an isolated network that is not part of your production network to do the practice exercises in this Course. Internet access is not required for the exercises and you do not need to configure a default gateway. To minimize the time and expense of configuring physical computers, it's recommended that you use virtual machines. To run computers as virtual machines within Windows, you can use Virtual PC 2007, Virtual Server 2005 R2, Hyper-V Server 2008 R2 or third-party virtual machine software. To download Virtual PC 2007, visit <http://tinyurl.com/3bbjcmr>.
- To download Virtual Server 2005 R2 or Hyper-V Server 2008 R2, visit <http://tinyurl.com/3su88uc>.



REAL WORLD

Very often, one of the main causes of unexpected networking problems is the faulty or incomplete implementation of name resolution services. The variety of peculiarities reported by network users is a laundry list of seemingly unrelated phenomena. From missing icons and applications on a user's desktop, to printing failures, to failed logins and more.

Even if you run only the latest versions of the Microsoft operating systems, it is quite likely that there are NetBIOS-based applications running on the network that will periodically fail without a proper implementation of Windows Internet Name Service (WINS).

The DNS Server role in Windows Server 2008 R2 complies with all request for comments (RFCs) that define and standardise the DNS protocol. Although Microsoft's implementation of DNS should be interoperable with third-party DNS servers and appliances, very often, when DNS is causing a wrinkle in the organisation, it is just this subtle difference that can mean smooth sailing for name resolution and network service location services. Often, as the third-party DNS servers and DNS appliances are phased out, networking problems reduce dramatically.

If your environment has more than a few Windows servers, you probably should be running WINS. Additionally, you should carefully plan the DNS implementation, with a preference toward using Microsoft's DNS services, which are finely tuned to support Active Directory.

Lesson 1: Planning Name Resolution

As an experienced administrator, you will have worked with DNS and with Microsoft dynamic DNS. You should also be familiar with Network Basic Input Output System (NetBIOS) names, the NetBIOS Extended User Interface (NetBEUI) and WINS. It is not, therefore, the purpose of this lesson to explain the basic operation of these features; rather, it sets out to look at Windows Server 2008 R2 enhancements (particularly to DNS) and to discuss the planning of a name resolution infrastructure across an enterprise network.

One of the first planning decisions you need to make is whether to use WINS to resolve NetBIOS names. Microsoft describes WINS as approaching obsolescence and introduced the GlobalNames DNS zone to provide single-label name resolution for large enterprise networks that might not want to deploy WINS. This was seen as a replacement for WINS but NetBIOS name resolution is still required by many applications and legacy operating systems. For most environments, WINS is still a requirement and is, fortunately, fully supported in Windows Server 2008 R2.

When planning a DNS infrastructure, you must decide when to use Active Directory–integrated, standard primary, secondary, stub, reverse lookup and GlobalNames DNS zones. You need to plan DNS forwarding and when to use conditional forwarding, which is especially relevant to the enterprise environment in which you can have multiple Active Directory Domain Services (AD DS) forests work in the same intranet. Windows Server 2008 R2 (and Windows Vista and Windows 7) supports IPv6 by default and you need to understand and use the IPv6 records in DNS. The security of the DNS system has been enhanced in the release of Windows Server 2008 R2, with the addition of DNSSEC, DNS Cache Locking and the use of non-intuitive source ports from the DNS Socket Pool.

After this lesson, you will be able to:

- ✓ Identify the role of WINS in your IT environment.
- ✓ Consider Windows Server 2008 R2 DNS features when planning your name resolution infrastructure.
- ✓ Identify Windows Server 2008 R2 enhancements to DNS and use these in your planning process.
- ✓ Determine the need for DNSSEC to provide reliable name resolution information.
- ✓ Administer DNS using the Microsoft Management Console (MMC) snap-in and command-line tools.

Estimated lesson time: 45 minutes

Planning Domain Name System Using Windows Server 2008 R2

DNS resolves hostnames to IP addresses and can also resolve IP addresses to hostnames in reverse lookup DNS zones. The Windows Server 2008 R2 DNS server role retains the features introduced by Windows Server 2003 and Windows Server 2008 DNS (including dynamic configuration and incremental zone transfer) and introduces several new features and security enhancements. Windows Server 2008 R2 provides support for IPv4, as well as for IPv6, and is nearly essential for the support of Microsoft Active Directory directory service. This section covers the enhancements to DNS introduced in Windows Server 2008 R2 and how DNS deals with IPv6 addresses.

Microsoft recommends that you use the Windows Server 2008 R2 DNS Server service to support AD DS, although other types of DNS servers can support the AD DS deployment. A feature introduced in Windows Server 2003 DNS that can take advantage of the Directory Replication Services (DRS) of AD DS is the application directory partition for replication. A partition is a data container in AD DS that holds data for replication. You

can store application data in the application directory partitions of AD DS; you can then specify which domain controllers should receive a copy of the partition using DRS.

Configuring Windows Server 2008 R2 DNS

Close integration with other Windows services, including AD DS, WINS (if enabled) and Dynamic Host Configuration Protocol (DHCP and DHCPv6) ensures that Windows Server 2008 R2 dynamic DNS requires little or no manual configuration. Computers that run the DNS Client service register their hostnames and IPv4 and IPv6 addresses (although not link-local IPv6 addresses) dynamically. You can configure the DNS Server and DNS Client services to perform secure dynamic updates. This ensures that only authenticated, domain member computers with the appropriate rights can update resource records on the DNS server.

MORE INFO **DYNAMIC UPDATE PROTOCOL**

For more information about the dynamic update protocol, see <http://www.ietf.org/rfc/rfc2136.txt> and <http://www.ietf.org/rfc/rfc3007>.

NOTE **SECURE DYNAMIC UPDATES**

Secure dynamic updates are available only for zones that are integrated with AD DS.

Using Stub Zones

A *stub zone*, supported in Windows Server 2008 R2 DNS, is a zone copy that contains only the resource records necessary to identify the authoritative DNS servers for that zone. This includes the SOA and NS records for a namespace or zone. A stub zone also holds the A resource records for the name servers, but not for all hosts registered in the zone. Stub zones ensure that DNS servers hosting parent zones can determine authoritative DNS servers for child zones, thus helping maintain efficient DNS name resolution. Figure 1-1 shows a stub zone specified in the New Zone Wizard.

You can use stub zones when name servers in the target zone are in transition—for instance, if part or all of the company network is undergoing IP address transition and accurate resolution of names is problematic. For example, Contoso, Ltd., recently acquired the sales organisation Litware, Inc. Contoso and Litware have Windows Server 2008 R2 domains. The Litware DNS servers have a complex configuration with many resource records within many zones and subzones. As Litware uses security controls in place to securely manage its DNS namespaces, these DNS systems must remain intact. Also, you don't want to have to reproduce these numerous zones and controls on your DNS servers. You would configure stub zones on your DNS servers so they always know how to find the Litware DNS servers for accurate name and service resolution, even if the IP addresses of the Litware DNS servers change.

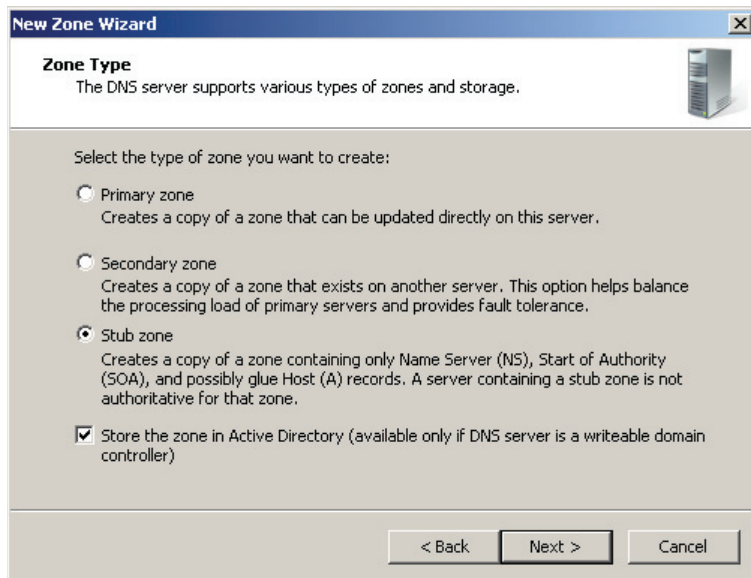


FIGURE 1-1 Creating a stub zone

In this case, your plan would include a stub zone on the Contoso DNS servers that contains resource records that identify the authoritative DNS servers for the *litware.com* domain. As the names and IP addresses of the *litware.com* DNS servers change, the stub zone on the Contoso DNS servers will be automatically updated with the changes through small zone transfers.

Stub zones are useful when child domains exist (Active Directory or namespace only). Delegation records are created in a zone for the child domain on the parent domain's DNS server. Delegation records (actually an NS and an A record for each child domain DNS server of interest) are often called *glue records* because they glue the child namespace to the parent namespace for resolution. For example, the name server for the *contoso.com* zone can delegate authority for the *sales.contoso.com* zone to a DNS server in that child domain. Then you use stub zones in child domains to hold the records for DNS servers for parent domains. You use delegation records to get resolution for names and services in child domains ('delegate down') and you can use stub zones on the child domain DNS servers to perform resolutions and services in parent domains ('stub up').

DNS Forwarding

If a DNS server does not have a zone in its database for the target host specified in a client request, it can query another (preconfigured) DNS server. When a DNS server forwards a name resolution request on behalf of a client, the upstream DNS server that hopefully can assist with the resolution is known as a *forwarder*. This process takes place recursively until either the client computer receives the IP address or the DNS server and forwarder system establish that the queried name cannot be resolved.

The Windows 2008 R2 DNS Server service uses *conditional forwarders* to extend the standard forwarder configuration. A conditional forwarder is a DNS server that forwards DNS queries according to the DNS domain name in the query. For example, you can configure a DNS server to forward all the queries that it receives for names ending with *adatum.com* to the IP address of one or more specified DNS servers that are authoritative for the *adatum.com* domain. This feature is particularly useful on enterprise extranets, where several organisations and domains access the same private internetwork. When a Windows Server 2008 R2 DNS server receives a query for an unknown namespace, the DNS server first checks to see if the query matches conditional forwarders. If it does not, then the DNS server will recursively query the forwarder. If there is no matching conditional forwarder (and the forwarder is unable to resolve the name, if configured), the DNS server will use its root hints in its attempt to resolve the name.

When the DNS server is installed on a domain controller, it is generally recommended you remove the *root hints* from the server so the DNS server (which is also a domain controller) does not attempt to perform iterative name resolution on the Internet. These DNS servers should be configured with a forwarder, often a caching-only DNS server, to perform the iterative queries with the public root server system.

NOTE REPLICATING ADDITIONAL FORWARDERS

In Windows Server 2008 R2, conditional forwarding entries can be stored in AD DS and configured to replicate to all DNS servers in the forest, all DNS servers in the domain or all domain controllers in the domain.

Figure 1-2 shows the dialog box used to create a conditional forwarder. You cannot actually configure this on your test network because you have only one DNS server.

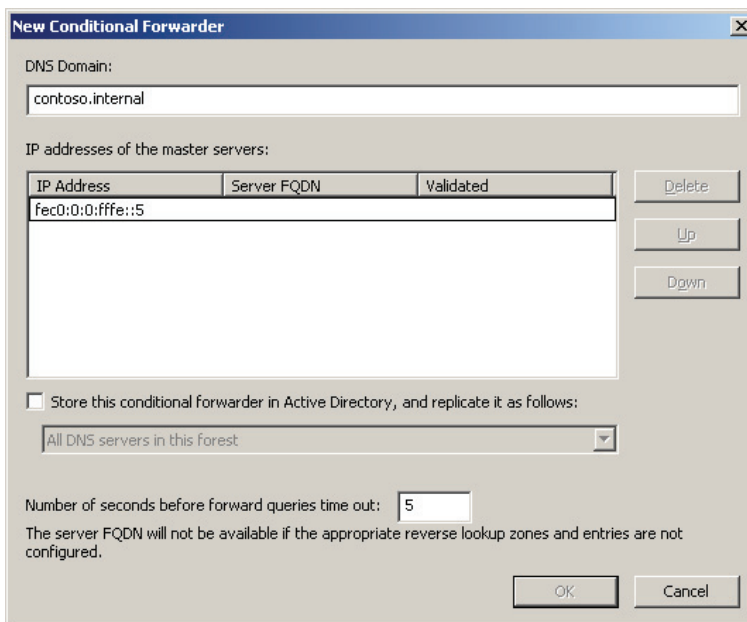


FIGURE 1-2 Specifying a conditional forwarder

Zone Transfers and Replication

Windows Server 2008 R2 DNS zones can be transferred or replicated between DNS servers for redundancy and to improve DNS name resolution efficiency. Zones are replicated to DNS servers when the zone is Active Directory–integrated and both DNS servers exist on domain controllers. Otherwise, the zone is transferred between a master and a secondary or slave DNS server. If you add a new DNS server to the network and configure it as a secondary DNS server for an existing zone, it performs a full *zone transfer* to obtain a read-only copy of all resource records in the zone. Any further changes to the authoritative zone are transferred to the secondary zone on subsequent zone refreshes. Windows Server 2003 introduced the incremental zone transfer that updates only the changes to the authoritative zone and Windows Server 2008 R2 supports this functionality. Prior to Windows Server 2003, a full zone transfer was required, which updated all records in the authoritative DNS zone to the secondary DNS server, even if the records had not changed.

You must configure zone transfers to any DNS server, to specified DNS servers only and to DNS servers listed on the Name Servers tab (any server that has registered an NS record). Figure 1-3 shows a DNS zone configured to allow zone transfers only to DNS servers listed on the Name Servers tab.

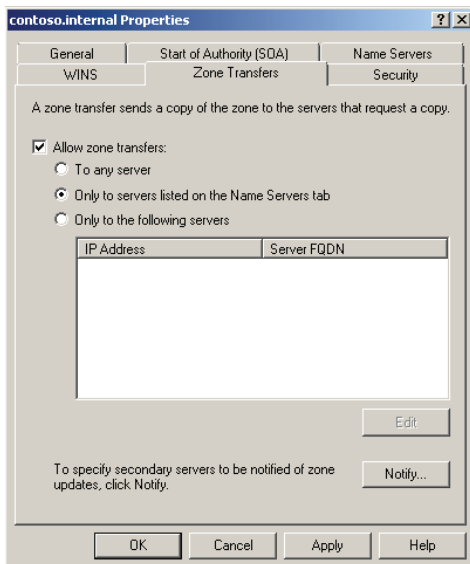


FIGURE 1-3 Configuring zone transfers

DNS Records

As a network professional, you should be familiar with standard DNS record types such as IPv4 host (A), Start of Authority (SOA), Pointer (PTR), canonical name or alias (CNAME), name server (NS), Mail Exchanger (MX), Service Location (SRV) and so on. You might use other DNS record types—such as Andrew File System Database (AFSDB) and Asynchronous Transfer Mode (ATM) address—if you are configuring compatibility with non-Windows DNS systems. If you need to create an IPv6 record for a client that cannot register itself with Active Directory, you need to create an AAAA record manually.

Administering DNS

You can use the DNS Manager MMC snap-in graphical user interface (GUI) to manage and configure the DNS Server service. Windows Server 2008 R2 also provides configuration wizards for performing common server administration tasks. Figure 1-4 shows the DNS Manager tool as well as IPv4 and IPv6 host records dynamically registered in DNS. Note that, if you access this tool at this point in the lesson, IPv6 records will not be displayed because you have not yet configured IPv6 addresses. You will do this in the practice session later in this lesson and in Lesson 2 of this chapter.

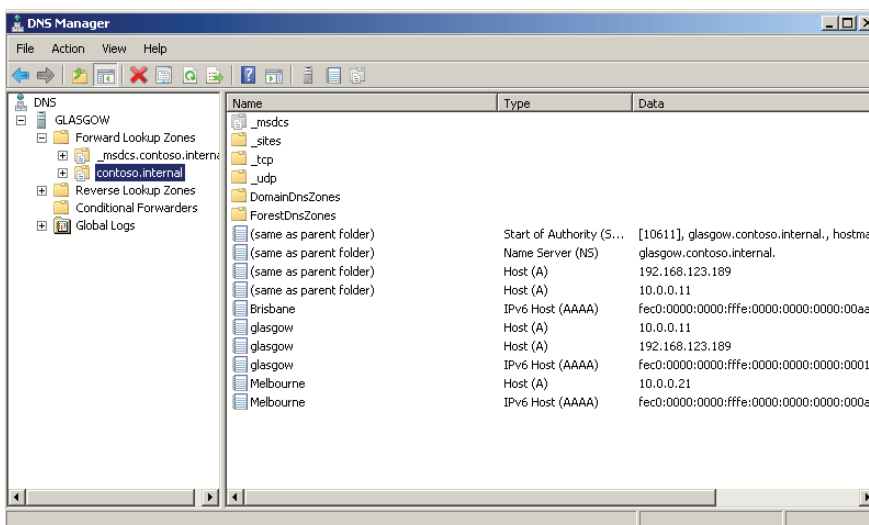


FIGURE 1-4 DNS Manager