TechRepublic
Real World. Real Time. Real IT.

Managing DNS in a multiple Win2K domain environment

Mar 12, 2002
Cindy Souders, MCSE

Windows NT 4.0 domains have no natural relationship to each other. They are simply a bunch of security boundaries sitting out there, waiting to be configured to see each other through the domain trust process. For those networks that use DNS for name resolution, NT4 domains can pose an administrative challenge because NT4 domains don't recognize the DNS hierarchical structure, and DNS doesn't recognize NT's domain structure.

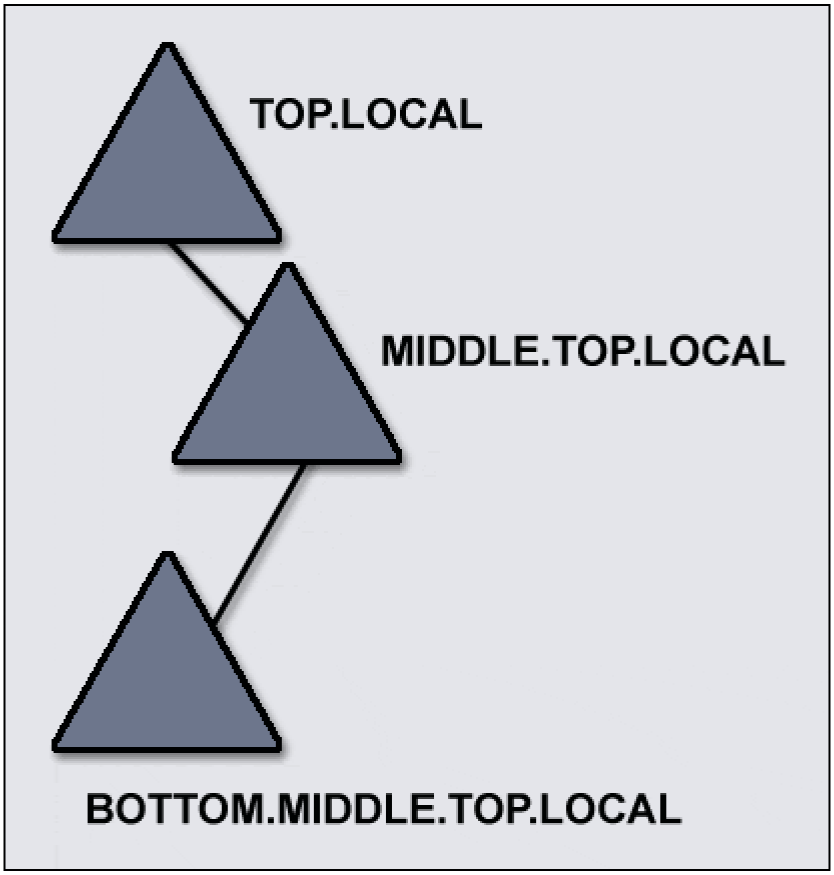
Fortunately, with the advent of Active Directory and Windows 2000, Microsoft has made some important improvements to its implementation of domain structures. The good news is that the same fully qualified domain name (FQDN) standards for contiguous name space that rule the DNS realm (and the Internet) now apply to Windows 2000 domains.

The bad news is that your DNS services in Win2K must be carefully configured or your clients in separate domains won't be able to connect to each other. The most important thing to remember when managing these configurations is that the Active Directory structure is hierarchical, just like DNS. Let's look at how to configure DNS in a network with multiple Windows 2000 domains.

Setting up the name space

In my Windows 2000 lab topology, I began with a three-domain Active Directory tree. The primary DNS service resides in the parent domain, which I'll call TOP.LOCAL for the sake of this illustration. This is not a legal FQDN, but it doesn't need to be. The lab isn't directly connected to the Internet, so my naming structure doesn't have to be registered with the powers-that-be. The child domain is MIDDLE.TOP.LOCAL, and the child of that domain is BOTTOM.MIDDLE.TOP.LOCAL. This is the contiguous name space that makes up our domain tree.

Figure A



Windows 2000 domain structure

Because some form of DNS must be in place to install Active Directory, I'll start at the top. On the DNS server in TOP.LOCAL, I configured a primary DNS server for a forward lookup zone called TOP.LOCAL. I configured a primary DNS reverse lookup zone using the network address. I configured standard primary zones instead of Active Directory-integrated zones for troubleshooting purposes. I wanted to make sure the zones were working properly before I added the complication of Active Directory integration. Note, also, that I haven’t yet addressed the child domains.

Understanding DNS resolution
At this point, it's important to understand how DNS querying works. Most users don’t realize how much work the client computer performs in the querying process. The client is usually configured with a preferred (or primary) DNS server and an alternate (or secondary) DNS server. This is configured in the client’s TCP/IP properties screen.

If the client can't contact the preferred DNS server, it will attempt to contact the alternate DNS server. If the client can't contact either server, the client’s connection will fail. This is important to understand because the error message the client receives may not point the user to DNS as the problem.

For instance, if the client is trying to access a resource, and DNS can’t find a domain controller for authentication of the client, the client may get an error message saying either Access Is Denied or Network Path Not Found. This doesn’t really help a great deal in the troubleshooting process. The error message appears to point to permissions as the problem, when DNS could very well be the issue to address. By knowing that the client must be able to contact the DNS service to access resources on the Windows 2000 network, an administrator can remember to check DNS connectivity when troubleshooting.

If the client is able to contact the DNS server, that server knows to resolve the host name as it relates to the zone the DNS server is authoritative for. For instance, if the client is trying to ping the host name *computer2*, and the user doesn't type an FQDN, the DNS server assumes that *computer2* should belong to the local domain/zone. If there is no such name in the zone, the ping will fail. If the client tries to ping the host name *computer2.otherdomain.com*, the DNS server has a better idea of how to process that query. The DNS server, through the use of Forwarding and Root Hints, will figure out that *computer2* is not a local computer, and the query must be forwarded to another DNS server that might know the answer. The client will then connect properly.

DNS troubleshooting
For more information on DNS troubleshooting in Windows 2000, see my article "When troubleshooting Win2K, start with DNS."

Making the DNS connection
Once the primary DNS server is functioning in the top domain, you have two options for making the Win2K domains connect using DNS.

Option 1
A forward lookup zone for each of the child domains can be configured on a Windows 2000 Server machine in the respective domains. The DNS server in each of the child domains should, again, be configured as Standard Primary. A reverse lookup zone for each of the child domains can also be configured, but the child domain servers should be Standard Secondary, since the Primary Server for the reverse lookup zone is in the TOP.LOCAL domain.

Don't forget: The reverse lookup zone is the same for all of the computers in the same subnet because the designation is by IP address, not domain name. As a result, the first DNS server in the TOP.LOCAL domain should be configured as a secondary to each of the child zones created for MIDDLE.TOP.LOCAL and BOTTOM.MIDDLE.TOP.LOCAL. Now, all DNS servers will be talking to each other through the zone transfer process.

Once each of these forward and reverse lookup zones is functioning properly, all zones should be changed to Active Directory-integrated. Just click the Change button in the general property page for the zone. To test each zone for functionality, try the Nslookup command. A correct answer will include the FQDN and IP address of the name server *and* the queried computer. Any message that includes "cannot find…" tells you that the servers or clients are not configured properly. Between the client TCP/IP properties, the server's DNS management console, and the command prompt, you can find out all the information necessary to troubleshoot DNS.

The challenge with multiple zones and Active Directory-integrated zones is the way that zone databases get from one server to another. Active Directory-integrated zones do not use the standard zone transfer method. The standard method entails the secondary DNS servers pulling a zone transfer from the primary server every five to 10 minutes, through the notification process. Active Directory-integrated zones are shared through Active Directory replication. The good news is that Active Directory replication doesn't interfere with zone transfers, and it is a more efficient use of bandwidth to have only replication taking up the pipe instead of replication and zone transfers.

The bad news is that Active Directory is domain-specific. It would be logical to think that with a contiguous name space, the DNS server at the top-level domain would eventually receive the information from child domains through replication and convergence. But since the Active

Directory database is shared only between domain controllers (DCs) within the domain, how would the top-level domain ever find out about the zones below it? That is where zone delegation comes in, and that's what we'll look at in option two.

Option 2
Another way to configure DNS servers is through zone delegation. This is the process of creating subdomains whose DNS server authority can be delegated to Windows 2000 Servers within each child domain. The difference here is that on the first DNS server in the top domain, a folder structure will be created that is almost identical to the Active Directory hierarchy of the Windows 2000 domain structure.

The process has two parts. The New Delegation Wizard first creates the delegated server and the folder for the subdomain. The second part is to create an identical zone on the DNS server in the child domain. This process creates a cleaner, more direct method for the DNS servers in each domain to talk to each other.

When finished, the first DNS server and all approved DNS servers (as configured on the Name Servers tab for the zone) have a hierarchical folder structure where the bottom child lives within the middle child folder, and the middle child folder lives within the parent folder. This structure mirrors the Active Directory hierarchy of the logical network and keeps all DNS servers talking to each other. For any administrator who has spent time in an Active Directory network, having all of the DNS servers talking to each other is critical for the network to function properly.

Summary
Managing DNS in a network with multiple Windows 2000 domains requires some forethought and careful planning. I've shown you two ways to integrate Windows 2000 domains so that they can communicate with each other and ensure that systems on your network can access the resources that they need.