Exam Manual

LearnSmart

Microsoft Server 2003 Network Infrastructure (70-291)

Microsoft Certified Systems Administrator (MCSA)

Smarter Training

This LearnSmart exam manual is designed to prepare you for the Server 2003 Network Infrastructure exam (70-291). By studying this exam manual, you will become familiar with an array of exam-related content, including:

- IP Addressing
- Name Resolution
- Network Security
- Routing and Remote Access
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Windows Server 2003
Network Infrastructure (70-291)
LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC
Product ID: 10012
Production Date: July 18, 2011
Total Questions: 25

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

Included in this Exam Manual is the knowledge required to pass the *70-291: Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*. What that means is that this exam manual contains the information you need to know to pass the 70-291 exam, according to Microsoft's exam topics. This exam is a core exam in the MCSA & MCSE Windows 2003 Tracks. This exam is for new MCSA and MCSE candidates as upgrade exams would be recommended for existing MCSAs and MCSEs.

What to Know

The topics covered by this exam include:

- Implementing, Managing, and Maintaining IP Addressing
- Implementing, Managing, and Maintaining Name Resolution
- Implementing, Managing, and Maintaining Network Security
- Implementing, Managing, and Maintaining Routing and Remote Access
- Maintaining a Network Infrastructure

Tips

This test won't be easy but, as with any test, preparedness always reduces stress and greatly increases the odds of passing.

- Know your material. This will increase your confidence and allow you to really prove that you do know the topics that you are being tested on.
- Take the entire test time provided. Use this time, if allowed, to go back and review your answers.
- As you go through the exam, use the marking feature, which is typically provided, to mark questions that you are unsure about. When you complete the exam, you can usually see an overview of the exam and go back to review the questions that you have marked.
- Get hands-on experience. It is difficult to replace actual experience on whatever you are being tested over. Even if you only spend a short amount of time, this is much better than no time spent at all. Most of us are, in part, visual learners. Because of this, you will learn, understand, and remember the things you learn if you have seen how they work and experienced them. As this is an upgrade test for persons who already have their MCSA, Microsoft, basically, wants you to show that you know the same information you already learned about Windows 2000 Server but, now, under Windows 2003 Server.
- Get to the test site early. While sitting in the waiting room may increase anxiety, this is better than arriving late and being irritated. When arriving early, you should use this time to think about the things you have learned and mentally prepare yourself for the "task at hand".
- When you first site down at the testing desk, use the pieces of paper that are provided to make some notes on topics that you have learned about and had difficulty committing to memory. If you feel you've not been given enough paper, ask if you may take an additional sheet or two.

Implementing, Managing, and Maintaining IP Addressing

The IP Protocol is the de-facto protocol on the World Wide Web and is used on virtually every computer in the world today, thus just about every computer in the world has an IP address. These may be private IP addresses but they are still IP addresses. Therefore, understanding how IP addresses work, how IP devices communicate, how to manage and properly assign new IP addresses, and how to take care of the ones that you have, is invaluable for any Windows administrator or engineer.

Configure TCP/IP addressing on a server computer

Before you can configure the IP address on your server, your client, or your server's DHCP scope, you must first understand how IP addressing works. Important concepts to understand about IP addressing are:

- **IP address** – This 32-bit binary number uniquely identifies the device on the IP network. If it is a public IP address, it uniquely identifies the device on the global Internet. If it is a private IP address, it uniquely identifies the device on your local, private, Intranet network. IP addresses are usually expressed in dotted decimal format. For example, you might have an IP address of 10.1.1.1 on your server.

- **Binary** number system and binary math – All processing inside a computer is done in binary math. As you know, humans usually use the decimal numbering system (1-10, and up). Computers use the binary numbering system (0 and 1, only) for all storage, calculations, and decisions. IP addressing and subnetting boils down to binary math. Sure, you can do this on a calculator but really being able to understand it and do it with a pencil and paper is what sets a network engineer / administrator apart from a power-user. As we are so used to using the decimal numbering system, learning the binary numbering system takes us humans a great deal of explanation, even though it is much less complex than the decimal numbering system.

- **Subnet Mask** – This number, when combined with the IP address, tells the device what networks are local and what networks are remote. If you line up the IP address and mask, you will get the Network address portion and the Host address portion.
  For example:

  IP address 192.168.1.1 in binary is
  11000000 10101000 00000001 00000001

  The Subnet mask 255.255.255.0 in binary is
  11111111 11111111 11111111 00000000

  When you *AND* these together (a math function that results in putting a 1 where there is a 1 in both columns and a 0 in all columns that have either all 0's or a 1 and a 0). The result of an AND of these two would be:

  11000000 10101000 00000001 00000000

  Or, 192.168.1.0. This is the Network address portion (the network that the host resides on). The Host portion would be what was left over, or the X.X.X.1-254. In our case, this is the X.X.X.1 portion.

KNOWLEDGE CHECK:

- You should be able to answer how many networks and hosts are in a /21 network.
- You should know what would be the best subnet to use for a network with 13 hosts.
- You should know what the network address and broadcast address would be for an address like 192.1.2.231 in a /28 subnetted network.

If you read the above and said "huh??" or just aren't able to answer these questions in under one minute each, I **highly** recommend that you spend time learning to subnet quickly. Being able to perform subnet calculations, in your head, quickly, and correctly could make the difference between you passing and failing any of the Microsoft networking exams. Check out these links covering tips for learning to subnet:

- Cramsession – Quick and Dirty Subnetting
- Cramsession – Learn to Subnet Part I
- Cramsession – Learn to Subnet Part II
- **Gateway** – When a packet comes in from a host, an *AND* is performed by the router with the host's IP address and the local subnet mask. From this, the device determines if the remote host is on our local network. If the host is not on the local network, the device must go to the gateway to communicate with that host. Just like the IP address and subnet mask, the default gateway can either be statically configured or dynamically configured through DHCP (discussed in great detail later).
- **IP Addresses Classes** – IP addresses are broken up into classes. They are:
    - Class A
        - IP range 1.0.0.0 to 126.0.0.0
        - First bit always a zero (0)
        - There are 126 class A networks
        - You can put 16,777,214 hosts on each class A
    - Class B
        - IP range 128.0.0.0 to 191.255.0.0
        - First two bits always 10
        - There are 16,384 class B networks
        - You can put 65,532 hosts on each class B

    - Class C
        - IP range 192.0.0.0 to 223.255.255.0
        - First three bits always 110
        - There are 2,097,152 class C networks
        - You can put 254 hosts on each class C
    - Class D
        - IP range 224.x.x.x to 227.x.x.x
        - First four bits always 1110
        - Class D addresses are special multicast addresses based on RFC 1112
    - Class E
        - IP range 248.x.x.x 254.x.x.x
        - First four bits always 1111
        - IP addresses in this range are reserved for experimental use only
- **Private IP Addresses** – Certain IP addresses are reserved for private network use. These IP Addresses are not routable over the Internet. This idea is based on RFC 1918. They are:
    - 10.0.0.0 -> 10.255.255.255
    - 172.16.0.0 -> 172.31.255.255
    - 192.168.0.0 -> 192.168.255.255
- **Loopback IP address 127.0.0.1** – Another special IP address is the loopback adaptor IP address. This IP address is non-routable and is reserved for loopback and inter-process communication on the local host.

Manage DHCP

With IP networks growing and every client needing its own address, the Dynamic Host Configuration Protocol (DHCP) has become the standard way of delivering IP addresses to clients. DHCP provides not only the IP address but also the subnet mask, default gateway, domain suffix, DNS server addresses, WINS server addresses, and other parameters. Windows 2003 Server provides an easy interface to manage client DHCP information. You should be familiar with its in's and out's.

Manage DHCP clients and leases

Prior to managing your clients and their leases, you first need to have your server configured as a DHCP server. Windows 2003 Server uses "roles" to describe the different services that the server provides. Thus, you need to add "DHCP server" as a role of your server.

The easiest way to add DHCP as a service is to use the "Configure your server Wizard" or "Manage Your Server Wizard". Under either of these programs, you indicate that you want to add the role of DHCP Server to your Window system. With this, you can go through the "new scope wizard". This will manual you through the process of adding a scope. You will be asked the following:

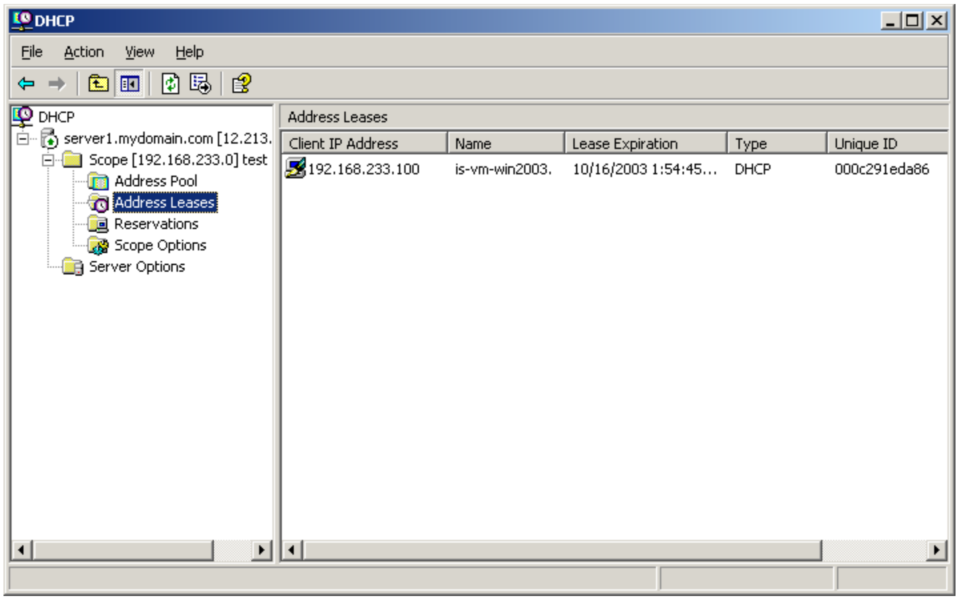
- Name for the scope.
- Description for the scope.
- Starting IP address.
- Ending IP address.
- Subnet mask for your scope.
- Exclusions to the scope, if any.
- Duration of the lease.
- Options for the scope, like default gateway, domain, DNS servers, and WINS servers.

IMPORTANT POINTS to remember for the exam:

- Every DHCP server must be authorized in the Windows AD before domain computers will be able to receive an address from that server. To authorize a DHCP server, you must be a member of the group Enterprise Administrators.
- Each DHCP scope must be **activated** before the DHCP server will lease addresses from that scope.
- The DHCP server must have an interface that is in the subnet that the created DHCP scope is derived from.
- For network redundancy, you may want to have two DHCP servers on the same network so that if one goes down, the other will provide IP addresses to your clients. When both servers are available, the client will take the address from the server that responds the first. Microsoft recommends the 80/20 rule when dividing scopes between servers:

  The 80/20 Rule states that you should divide your TCP/IP address scope between two DHCP servers. Give the primary server 80% of the addresses and give the backup server 20% of the addresses. By doing this, the backup server will be available should the primary server go down or run out of IP addresses. You might have both primary and backup servers on the same LAN of a large network or you may have a primary server, for each network, at each remote site and the backup servers at a central site. These choices are determined by the size and redundancy you wish to design into the network.
- It is not recommended to use a domain controller as a DHCP server.

Once your DHCP server is authorized and your scope is activated, you can begin leasing IP addresses. DHCP clients use **DORA** (Discover, Offer, Request, and Acknowledgements) to obtain a DHCP IP address lease. To see the active DHCP leases, use the DHCP administrative tool. Below is a screen shot of a DHCP server with an active lease. You can see that the "address leases" tab has been selected and there is one lease active. Note the client's name, leased IP address, when the lease will expire, and the client's MAC address.



Client IP Address	Name	Lease Expiration	Type	Unique ID
192.168.233.100	is-vm-win2003.	10/16/2003 1:54:45...	DHCP	000c291eda86

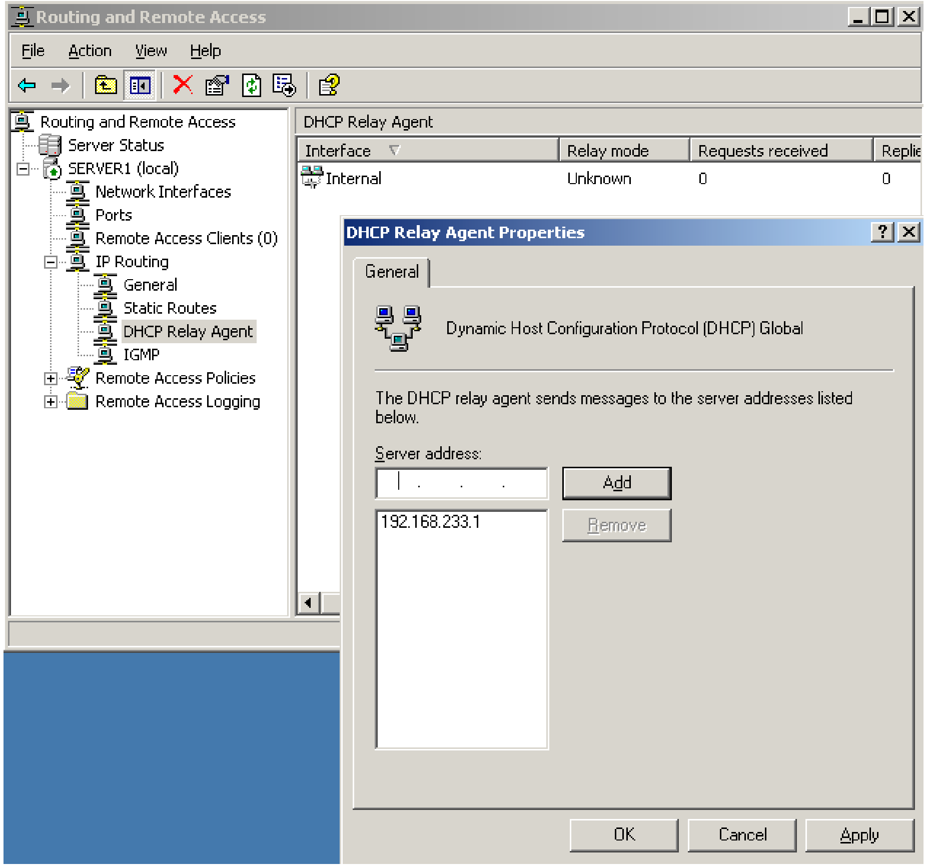
Figure 1

Manage DHCP Relay Agent

Routers do not forward broadcast packets. DHCP Discovers (the type of packet that a client uses to find a DHCP server) are broadcast packets. Thus, if you have a DHCP server on one side of a routed network and a client on the remote network, the DHCP server will never receive the client's request for an IP address. Enter the DHCP Relay Agent. DHCP relay agents reside on the remote network. They grab the client's broadcast request, turn it into a unicast request and forward it directly to the DHCP server on the other side of the WAN. The only configuration involved in doing this is telling the DHCP relay agent the IP address of the DHCP server it needs to forward the request to.

To clarify, DHCP Relay agents are used when you have a DHCP server on one side of a routed network and the DHCP client on the other side of the routed network. The DHCP Relay agent is used on the DHCP client side of the network to send the DHCP client requests to the DHCP server.
Make sure that you understand the difference between a DHCP Relay agent and a BOOTP forwarder. A Relay Agent takes the DHCP broadcast, turns it into a unicast, and sends it to the DHCP server. On the contrary, a BOOTP forwarder just takes the broadcast and sends it as a directed broadcast (not a unicast) to the DHCP server.

You could use either Windows 2003 Server or Unix as your DHCP Relay agent. If you are using Windows 2003 as your DHCP Relay Agent, you would configure this with the Routing and Remote Access administrative tool. You must have at least one type of routing/remote access configured and enabled. With that comes the ability to configure the DHCP relay agent. This 2003 Server does not need to be actually routing between the subnets. It can be just a server on the subnet. Configuring it is as simple as selecting DHCP relay agent properties and adding the IP address of the DHCP server that you want the agent to relay the client DHCP broadcast requests to. Doing this looks like this:



Interface	Relay mode	Requests received	Replie
Internal	Unknown	0	0

Dynamic Host Configuration Protocol (DHCP) Global

The DHCP relay agent sends messages to the server addresses listed below.

Server address:

192.168.233.1

Figure 2

After configuring the relay agent, you can select the relay agent and see statistics on how many requests have been received, replies received, and requests discarded.

Manage DHCP databases

Part of managing a DHCP server database is backing up the database, restoring the database, and reconciling the database.

Most likely, you will do all of these within the DHCP manager, by right-clicking on the DHCP server (as you can see below). However, these tasks can also be performed from the command line.

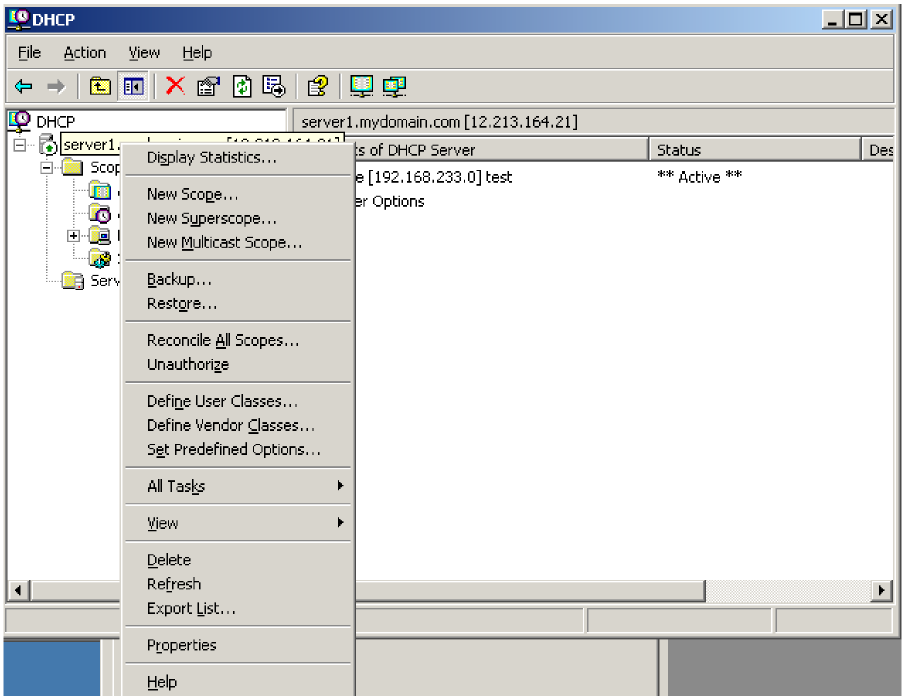


Figure 3

Typical tasks:

Backup the DHCP database:

> As you can see from the above screen shot, manually backing up the database is as simple as right-clicking on the server and selecting backup. You will be prompted for the location that you want to store the backup file. By default, this is \windows\system32\dhcp\backup.
>
> By default, the DHCP server automatically backs up its data every 60 minutes. These automatic backups are used only if the DHCP server detects that its database is corrupt. These automatic backups cannot be used to manually restore the DHCP data or to migrate the data to another server.

Restore the DHCP database:

> Restoring the DHCP database is as simple as backing it up. If your DHCP server is already running, restoring it will require stopping the DHCP Server Service restoring the database and then restarting the DHCP Server Service. When restoring, you will be prompted for the location of the file that it will be restored from.

Reconcile the DHCP database:

> It is possible that the DHCP database can become corrupt. The DHCP server database is stored in MS Jet format, and thus is more susceptible to corruption.
>
> This is so likely that Microsoft includes a utility to cleanup and resolve the corruption. This is call "reconciling the database".
>
> The DHCP database stores information on leases obtained in a summary (indexed) format and a detailed (record) format. When you opt to reconcile the database the index and records are compared to make the database consistent again. Just like doing a backup or restore, reconciling the database is done by right-clicking on the server. At this point, you would select Reconcile All Scopes.
>
> You will either be told that the database is consistent or contains inconsistencies.
>
> You may also want to watch the Event Viewer for DHCP server errors.

Manage DHCP scope options

For every DHCP scope that is configured, there are (of course) scope options that can be configured. In fact, there are over 70 scope options that may be configured. These scope options are such things as:

- 004 - Time server to assign to client
- 006 - DNS Name server to provide to client
- 015 - DNS Domain name
- 044 - WINS server to provide to client
- 046 - WINS Node type
- 003 - Default router IP address for client to use

You may or may not need these scope options; however, most networks are going to want to provide information on the DNS servers, WINS servers, and default routers. This is because these options, along with the IP address and subnet mask, really complete the end client configuration on most networks today. Scope options can be configured by selecting the Scope Options folder under the Scope that you want to configure the options in, then selecting Configure Options.

Scope options are options (like default gateway, WINS servers, or DNS servers) that the DHCP server will assign, along with the IP address, from the scope that the options are configured for.

On the other hand, Server options (like the options mentioned above) are the default options for any scope that is configured on the server. Server options can be overridden by scope options.

Manage reservations and reserved clients

It is easy to get confused when first looking at DHCP reservations. On one hand you have static IP addressing (hard coded on the client) vs. dynamic IP addressing (assigned by DHCP each time the client is booted up). Once you decide to use DHCP, you can either have the client get its address from the DHCP scope by taking the next one available or you can configure a reservation for the client. A reservation means that you hard code on the DHCP server the client's Ethernet MAC address and pair that with an IP address that you assign. This IP address may be from the scope of IP addresses that you defined.

Note that the client still must be configured to get its IP address via DHCP. Reservations are used for things like printers and some dedicated servers as you have a central database (on the DHCP server) of all (or most all) of the devices on your network. Other dedicated servers also require that the IP address be statically defined. For instance, an email server, web server, or domain controller will probably need its IP addresses statically defined.

Troubleshoot TCP/IP addressing

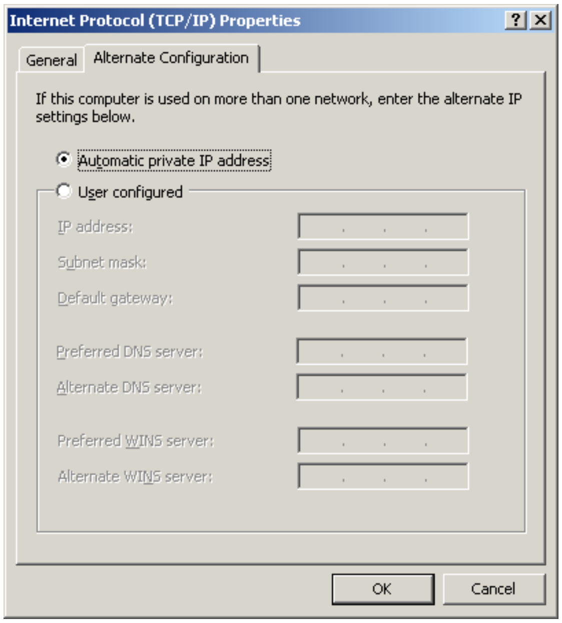
As TCP/IP is a complex protocol which runs on simple, small networks and up to large complex networks, troubleshooting it can be, well, complex. Nonetheless, if you can master troubleshooting TCP/IP on a two-machine network I would estimate that 90% of this will be applicable on your company's network or the largest network in the world, the Internet.

Diagnose and resolve issues related to Automatic Private IP Addressing (APIPA)

Automatic Private IP Addressing is a concept unique to Windows machines. APIPA is designed for small, single-segment networks (meaning no routers) and without DHCP servers. APIPA is enabled by default. Basically, if no IP address is defined and no DHCP server is available, the Windows system will assign itself an IP address from a certain range. The range is 169.254.0.1 to 169.254.255.254.

At a Command Prompt, you can type **IPCONFIG /ALL** or **WINIPCFG** (depending on your machine's Windows version) to determine if your IP address is in the APIPA range. If after obtaining an APIPA address, your machine later contacts its DHCP server, it will use the DHCP server's assigned IP address.

The process of disabling **APIPA** addressing varies by version of Windows. In Windows Server 2003 you could disable APIPA addressing by modifying your network connection's TCP/IP properties and going to the Advanced tab. (See the screen shot below.)



Internet Protocol (TCP/IP) Properties

If this computer is used on more than one network, enter the alternate IP settings below.

● Automatic private IP address

○ User configured

Figure 4

Most of the time, on a network that uses DHCP, if you find that your machine has an IP address from the APIPA range, you know that there is a communication problem. This problem is most likely with your Window system, your network card, cable, network switch, router (if on a routed network), WAN circuit (if applicable), and finally, DHCP server.

Diagnose and resolve issues related to incorrect TCP/IP configuration

You can use Network Monitor (covered later in this exam manual) to troubleshoot your network connectivity. Most network trouble can be resolved with the following actions:

- Check network card link lights and network switch link lights. If the NIC is communicating with the switch, there will be a link light. If these two are not communicating, then the NIC cable or card is defective. There is no need to move on to any TCP/IP troubleshooting as the connection will never work without a link on the NIC and the switch.
- Check and double-check your TCP/IP configuration. Use IPCONFIG /ALL to see your configuration. Compare this to a working machine. Compare this to the server that your machine is attempting to communicate with. Make sure that the machines are on the same network subnet (if they are supposed to be on the same network), verify the default gateway, double-check the DNS server IP, etc.
- Use the **ping.exe** command to ping the default gateway, DNS server, or a known working machine.
- Use **tracert.exe** or **pathping.exe** if the communication trouble involves a WAN connection.
- Install the Windows Server 2003 Support tools and run the netdiag.exe command. This tool will perform a long list of tests on your machine.

Troubleshoot DHCP

For those who use DHCP everyday on a large network, you know that being able to troubleshoot DHCP is a valuable skill. Microsoft recognized that and I am sure that is why it is on this exam. Some of the DHCP troubleshooting skills you should be familiar with are below.

Diagnose and resolve issues related to DHCP authorization

In a Windows environment, DHCP servers must be authorized in the Windows Active Directory. If they are not, new versions of DHCP servers will automatically shutdown. Older Windows DHCP servers and DHCP servers using other operating systems won't check to see if they are authorized. When you have an authorized Windows 2000 or 2003 DHCP server and an unauthorized Windows 2000 or 2003 server, running on the same subnet, the unauthorized server is known as a rogue server. The rogue Windows 2000 or 2003 server will detect that there is an authorized server running and will automatically shut itself down.

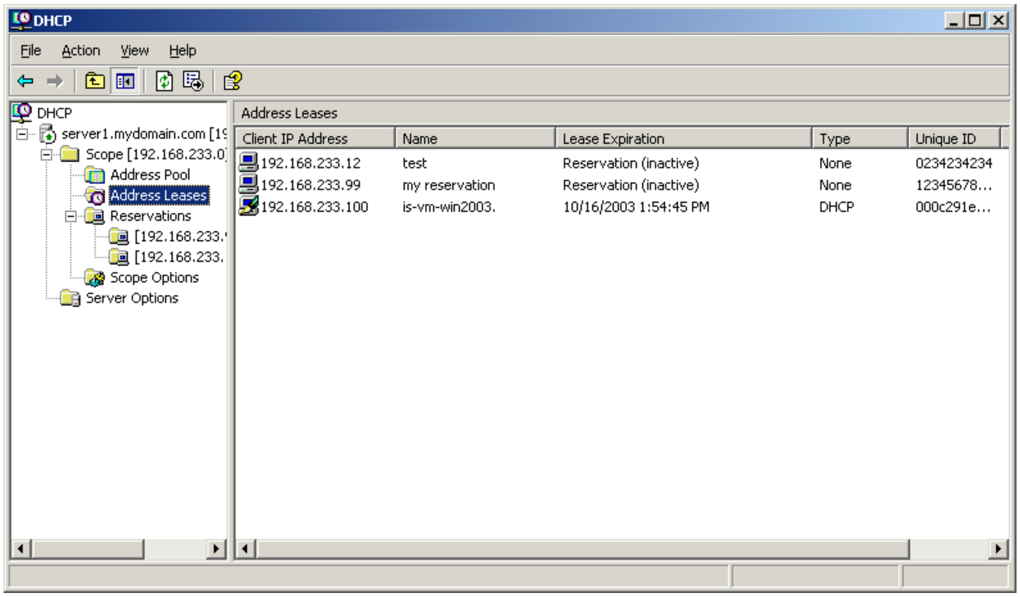
To detect unauthorized DHCP servers on your network, use the ***dhcploc.exe*** utility. This command line utility is included in the Windows support tools and can tell you if there is an unauthorized DHCP server operating on the subnet and what its IP address is.

Verify DHCP reservation configuration

Administrators can become confused between an exclusion and a reservation. When you make an **exclusion**, that client (MAC address) can never obtain an IP address from that DHCP server. Exclusions are defined within the DHCP server address pool. A **reservation**, on the other hand, ensures that the DHCP client always receives the same IP address from the DHCP server.

To make a reservation, open the DHCP scope you want to make the reservation within and find the reservation folder. If you right-click the reservation folder, you will see the "New Reservation" option. After selecting that, you will get a window where you can define the reservation name, IP Address, MAC address, description and supported type (DHCP or BOOTP).

Once you have made a reservation, you may want to assign options to that particular reservation. To do this, once the reservation is completed, right-click on the reservation and you will find "configure options." From here, configure options for this reservation, just as you would for the entire scope.
Once the reservation is created, how do you know if that client has requested it and it is in use? Simply go to "Address Leases" under that DHCP scope. Here you will find a screen that looks like this:



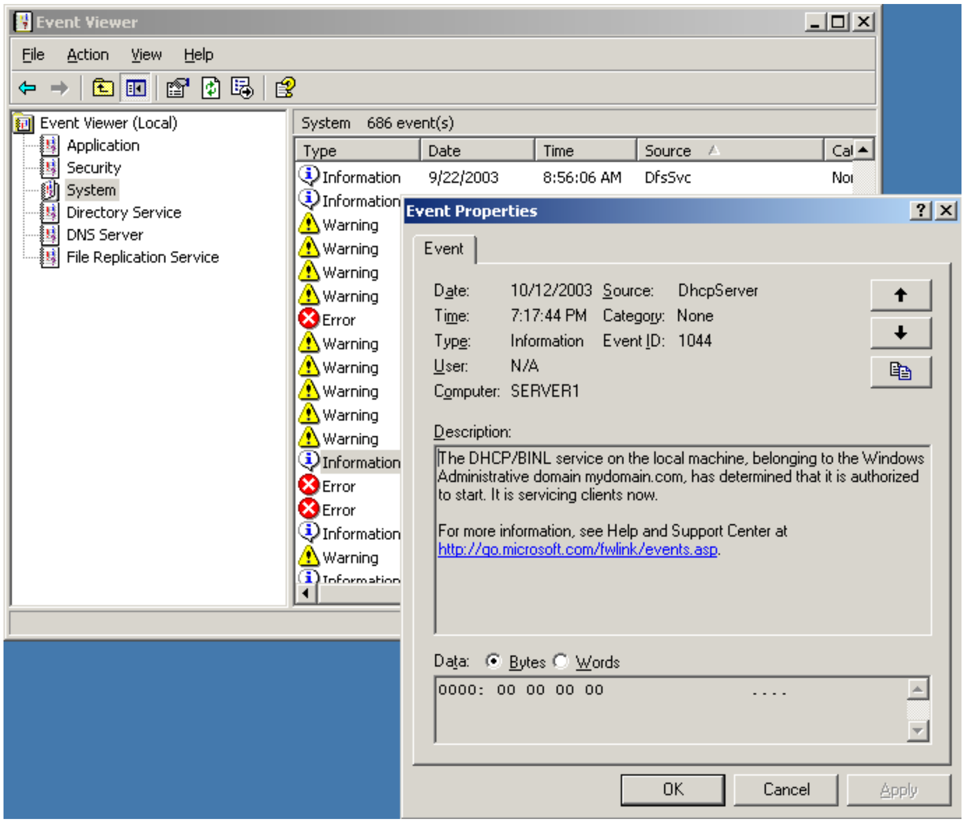
Client IP Address	Name	Lease Expiration	Type	Unique ID
192.168.233.12	test	Reservation (inactive)	None	0234234234
192.168.233.99	my reservation	Reservation (inactive)	None	12345678...
192.168.233.100	is-vm-win2003.	10/16/2003 1:54:45 PM	DHCP	000c291e...

Figure 5

You can see in this list of three address leases that there the first two in the list are reservations and that neither is in use (by the note that it is "inactive"). There is a third lease, which has an active expiration date.

Examine the system event log and DHCP server audit log files to find related events

Important DHCP Server events will be found in the Windows event viewer under **System**. DHCP Server does not have a separate event viewer log file like DNS. Look for the DHCP events in the system file by using the source column. Viewing these events is just like viewing any other event viewer events. The DHCP server events will have the source of "DhcpServer". Here is an example of what one looks like:



System 686 event(s)

Type	Date	Time	Source	Cat
Information	9/22/2003	8:56:06 AM	DfsSvc	Noı
Information				
Warning				
Warning				
Warning				
Warning				
Error				
Warning				
Warning				
Warning				
Warning				
Warning				
Information				
Error				
Error				
Information				
Warning				
Information				

Date: 10/12/2003 Source: DhcpServer
Time: 7:17:44 PM Category: None
Type: Information Event ID: 1044
User: N/A
Computer: SERVER1

Description:

The DHCP/BINL service on the local machine, belonging to the Windows Administrative domain mydomain.com, has determined that it is authorized to start. It is servicing clients now.

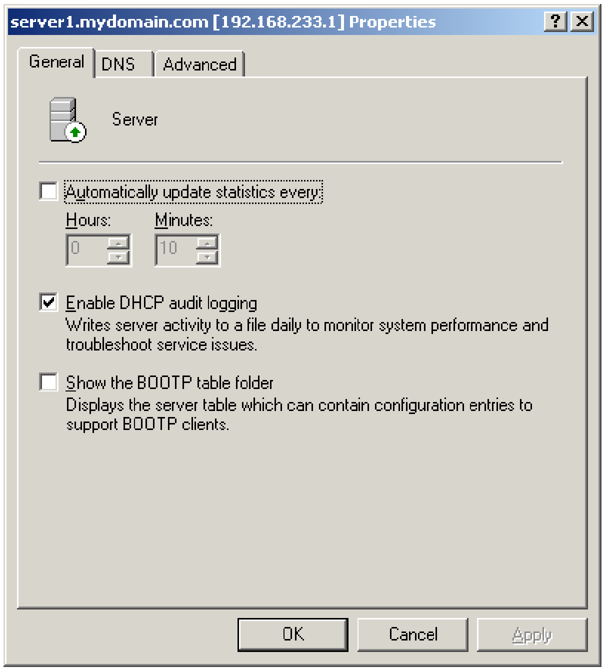
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0000: 00 00 00 00                    ....
```

Figure 6

If needed, you can enable **DHCP audit logging**. To do this, inside the DHCP MMC menu, right-click on the DHCP server in question and select properties. You will see a window that looks like this:



Server

□ Automatically update statistics every:

Hours: 0 Minutes: 10

☑ Enable DHCP audit logging
Writes server activity to a file daily to monitor system performance and troubleshoot service issues.

□ Show the BOOTP table folder
Displays the server table which can contain configuration entries to support BOOTP clients.

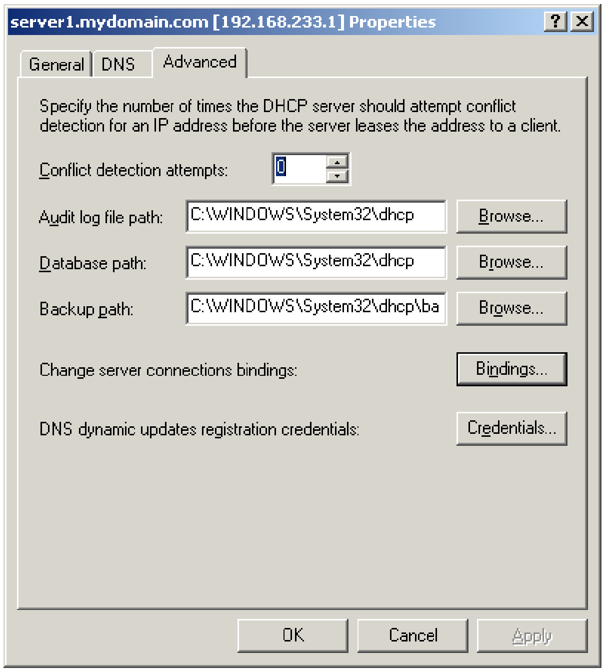
Figure 7

As you can see, enabling audit logging is as simple as selecting the check box.

Once audit logging is enabled, the log files are stored in %windir%\system32\Dhcp, by default. Windows will create a log file for each day of the week in a rolling 7 day rotation so that disk space is not consumed by these logs. For instance, if the log file was created on Wednesday, the log file would be named Dhcp-SrvLog-Wed. These files are comma delimited and will product a code for each DHCP transaction. Using the Windows DHCP help files, you can decipher this code. For instance, an event code of 62 indicates that another DHCP server was found on the network. An event code of 51 indicates that the DHCP attempted to authorize and it succeeded.

Diagnose and resolve issues related to configuration of DHCP server and scope options

Issues can occur where you may need to validate or change the DHCP server configuration. For instance, a server may have multiple adaptors and you only want the DHCP server bound to a particular adaptor. To see what adaptor the DHCP server is bound to, and if needed, make changes go to the server properties window. From here, select the advanced tab (shown below).



server1.mydomain.com [192.168.233.1] Properties

Specify the number of times the DHCP server should attempt conflict detection for an IP address before the server leases the address to a client.

Conflict detection attempts: 0

Audit log file path: C:\WINDOWS\System32\dhcp

Database path: C:\WINDOWS\System32\dhcp

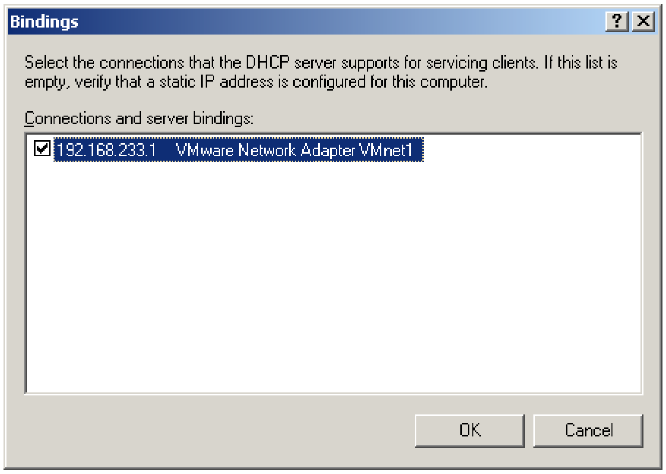
Backup path: C:\WINDOWS\System32\dhcp\ba

Change server connections bindings:

DNS dynamic updates registration credentials:

Figure 8

On this tab are a variety of important options, including the paths to the DHCP audit files, database file, and backup files. The option we are looking for is the "bindings" button. By clicking this button, you will see this screen:



Bindings

Select the connections that the DHCP server supports for servicing clients. If this list is empty, verify that a static IP address is configured for this computer.

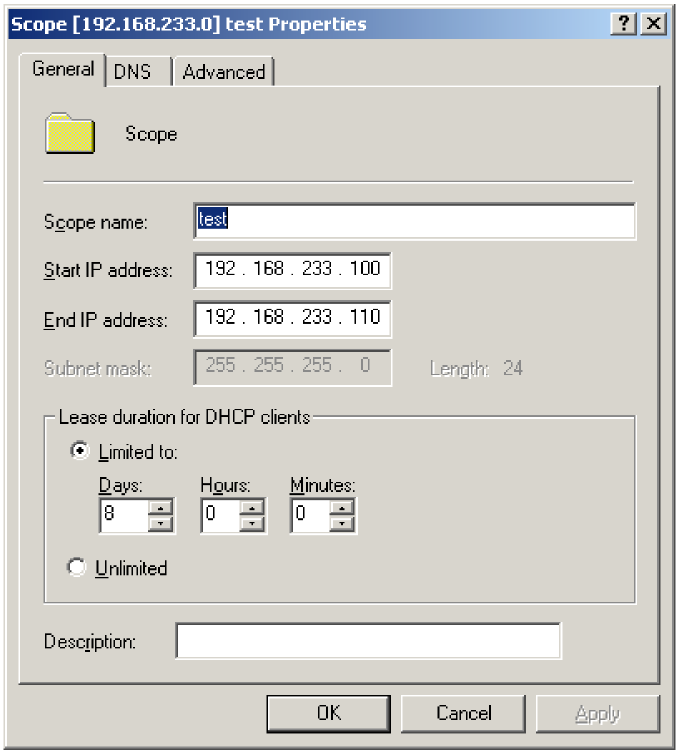
Connections and server bindings:

☑ 192.168.233.1 VMware Network Adapter VMnet1

Figure 9

This is the number of available adaptors on the system. The system shown only has one adaptor with an IP address. From the checkbox, you can see that this DHCP server is bound to the only adaptor on the system. On your system, you can bind the DHCP server process to multiple adaptors, if you would like.

Another possible issue may be that you have too many clients for the size of your IP address scope. In this case, what would you try to do? The answer is that you would shorten the default IP address lease. This way, as the clients come on and off the network, the addresses would be used and then given back quickly for other clients to use. To do this, you would right click on the DHCP scope that is created and click properties. The window below will appear.


Scope [192.168.233.0] test Properties

General | DNS | Advanced

Scope

Scope name: test

Start IP address: 192 . 168 . 233 . 100

End IP address: 192 . 168 . 233 . 110

Subnet mask: 255 . 255 . 255 . 0 Length: 24

Lease duration for DHCP clients

● Limited to:

Days: 8 Hours: 0 Minutes: 0

○ Unlimited

Description:

Figure 10

As you can see, you can change the "lease duration for DHCP clients" option from the default of 8 days, down to just a few hours. This will create more DHCP renewal requests but it will also free up more IP addresses from the scope for other clients as clients lease and release their IP addresses. Of course, at peak periods, your network may still be short of needed IP addresses.

Yet another possible problem with your DHCP configuration is that you may have a routed wide-area network and a centralized DHCP server. Say that you would like your DHCP server to provide IP addresses to each of the remote subnets. Perhaps you are having trouble with this. Some things to note about doing this are:

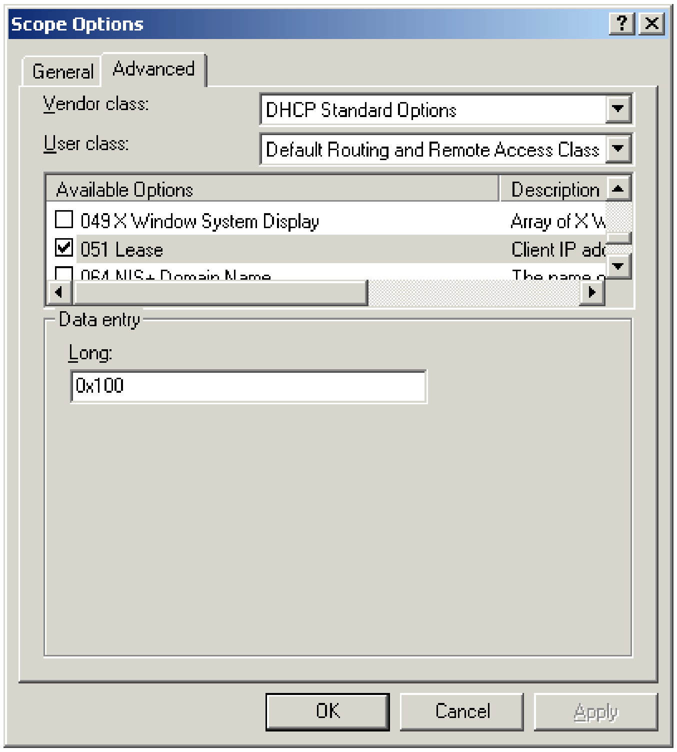
1. You must be using the DHCP **relay agent** or have a remote router that is **RFC 1542 compliant** to send the remote request on to the DHCP network.

2. On the DHCP server, you must have a scope setup for each of the remote subnets.

3. Each of the scopes on the DCHP server must be configured with the same network ID as the remote router or DHCP relay agent.

And finally, you should be familiar with the concept of DHCP **option classes**. As you know, there are DHCP option types. Option types are parameters that you can assign to a DHCP client when issuing a DHCP lease. Option classes are ways to group these options types. I would call the option classes templates that you assign to certain types of devices or users obtaining an IP address. In Windows 2003 Server, there are two types of option classes. They are the **user class** and **vendor class**. The vendor class is used to apply options to a group of clients that all use the same vendor's hardware or software. A user class is used to apply options to a group of users that all have something in common. For instance, by default, under the user class, there is the "Routing and Remote Access Class". This class would be used to apply options to all remote access users.

In the real world, you may want to apply an option to only your remote access users. An example might be that remote access users should have a shorter lease duration than regular DHCP clients. To do this, you would change the 051 option "lease duration" in the routing and remote access option class. Actually doing this would look like this:



Vendor class: DHCP Standard Options

User class: Default Routing and Remote Access Class

Available Options	Description
☐ 049 X Window System Display	Array of X W
☑ 051 Lease	Client IP adc
☐ 064 NIS+ Domain Name	The name o

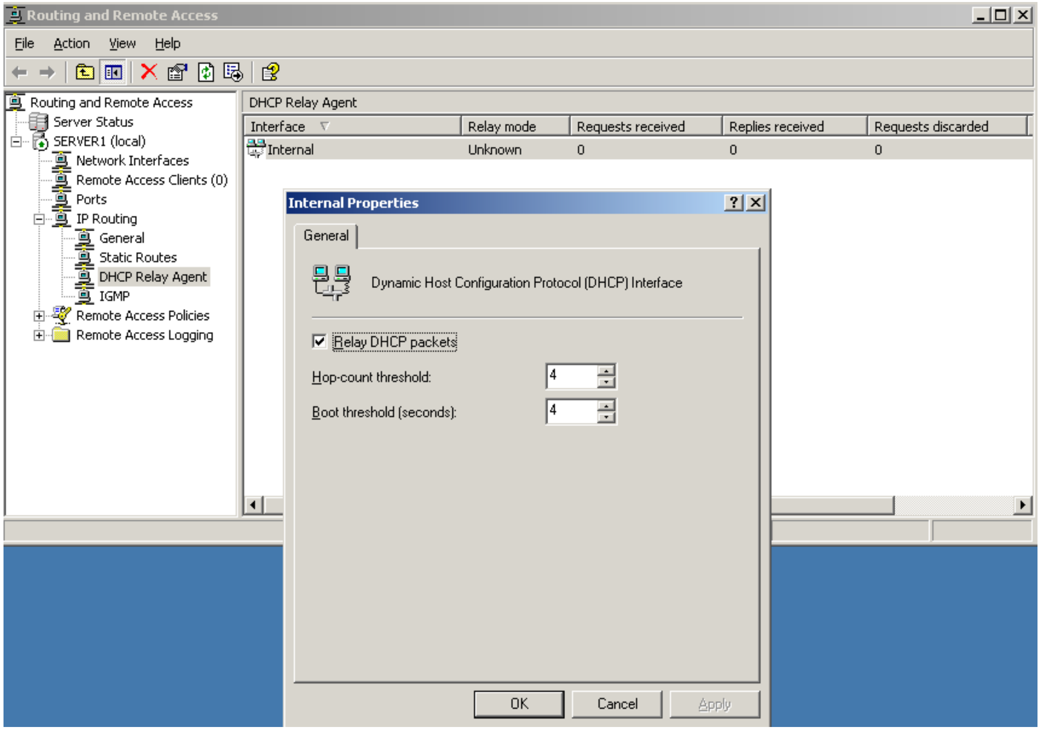
Data entry

Long: 0x100

Figure 11

Verify that the DHCP Relay Agent is working correctly

The configuration of the DHCP Relay Agent was covered in the "Manage DHCP Relay Agent" section. After configuring the relay agent, you can select the relay agent and see statistics on how many requests have been received, replies received, and requests discarded.



DHCP Relay Agent

Interface	Relay mode	Requests received	Replies received	Requests discarded
Internal	Unknown	0	0	0

Dynamic Host Configuration Protocol (DHCP) Interface

☑ Relay DHCP packets

Hop-count threshold: 4

Boot threshold (seconds): 4

Figure 12

As you can see from this screen shot, this DHCP relay agent has not received any requests or forwarded any requests. If you believe that your server should have received and forwarded requests, there may be a problem.

By clicking on the DHCP Relay Agent Interface, you will get the Internal Properties window (shown above). As you can see, you may need to modify the hop-count if the DHCP requests are traversing a network with many hops.

Verify database integrity

DHCP databases can, and will, become corrupt. You will need to know how to reconcile the DHCP database to resolve this corruption. DHCP Reconciliation was covered in the "Managing DHCP databases" section of this exam manual.

Implementing, Managing, and Maintaining Name Resolution

Install and configure the DNS Server service

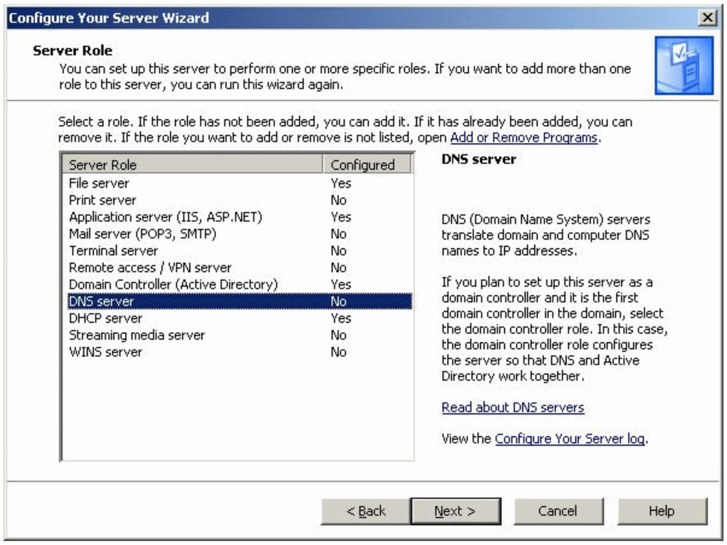
Configure DNS server options

Some new and improved DNS-related features in Windows 2003 Server are:

- You are now able to rename your domain and/or NETBIOS domain name. Also, the design of your AD structure can be changed after it is installed.
- In a release, separate to Windows Server2003, there will be a package called AD Application Mode, or AD/AM. This would allow you to run Active Directory services on a server that is NOT a Windows Domain Controller (DC).
- **Conditional DNS Forwarders** – Only forwards DNS requests based on part of the name in the DNS query.
- **Stub Zones** – A DNS zone that only has enough information to contact the Authoritative DNS server in the parent zone.
- DNS Zone Replication in AD – DNS zones can be stored in Windows AD or in Windows partitions and replicated to other AD controllers.
- Enhanced DNS Security features – There are three levels of DNS security: low, medium and high.
- Round Robin all resource records (RR) types – By default, Windows 2003 DNS will round-robin (simply load-balance) RR DNS entries.
- **DNSSEC** – DNS Security Extensions are provided with Windows 2003 DNS Server. These are based on RFC2535.
- **EDNS0** – Extension Mechanism for DNS enables DNS clients to advertise the size of their UDP packets and for the DNS server to respond appropriately.

Example of how you would install and configure DNS
You install DNS by using the "Manage your Server" tool. Hopefully, you are already familiar with this tool. It is the handy application that pops up, by default, when you login to your new Windows 2003 Server.

To configure your server as a DNS server, you can use the "Manage your Server" tool to make this quite easy. First, click on "Add or remove a role" within this tool. Click the Next button on the "Preliminary Steps" screen.



Server Role

You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.

Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open Add or Remove Programs.

Server Role	Configured
File server	Yes
Print server	No
Application server (IIS, ASP.NET)	Yes
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	Yes
DNS server	No
DHCP server	Yes
Streaming media server	No
WINS server	No

DNS server

DNS (Domain Name System) servers translate domain and computer DNS names to IP addresses.

If you plan to set up this server as a domain controller and it is the first domain controller in the domain, select the domain controller role. In this case, the domain controller role configures the server so that DNS and Active Directory work together.

Read about DNS servers

View the Configure Your Server log.

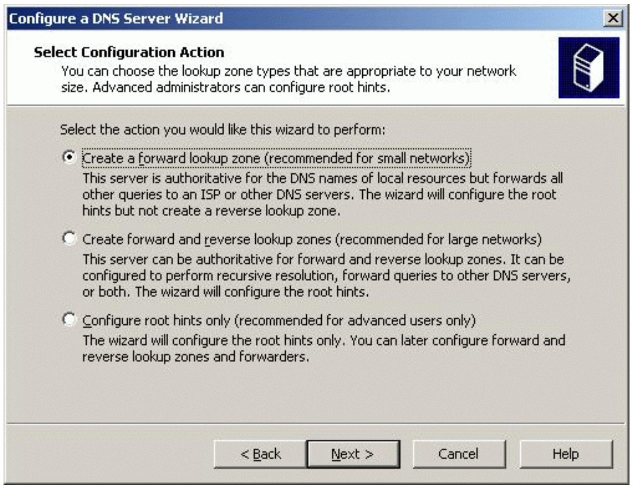
Figure 13

On this screen, you will be able to see all the possible roles your server can perform, along with which of the roles are currently "turned on", or not.

As you can see from the screen shot, this server is currently not configured to be a DNS server. So, we'll select the DNS Server role (which we have already done in the snapshot, above). Now, click next.
Then, you'll see the "Summary of selections" screen. This is mainly useful if you have chosen to configure more than one role at a time. You can just click "Next" to confirm here.

Note that you must have a static address on this machine for it to be a DNS server. If you have a dynamically assigned address, you will be presented with the network configuration screen, where you can configure a static address.

You will then be led though the "Configure a DNS Server Wizard."
From here you will be asked exactly what action you want the DNS Wizard to help you perform.


Configure a DNS Server Wizard

Select Configuration Action

You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.

Select the action you would like this wizard to perform:

● Create a forward lookup zone (recommended for small networks)
This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.

○ Create forward and reverse lookup zones (recommended for large networks)
This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers, or both. The wizard will configure the root hints.

○ Configure root hints only (recommended for advanced users only)
The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.

Figure 14

The dialog asks you which of these you want to configure this server as: 1) Only a forward lookup zone server (for a network that is going to forward all DNS queries NOT for this domain to another domain, like an ISP); 2) A forward and reverse lookup zone that can lookup both local and non-local domains or; 3) To only configure the root hints (advanced users only).

If we choose to only configure this server as a forward lookup zone, for our small network, we are prompted as to whether this server or the ISP maintains the zone.

Then, we enter the zone name.

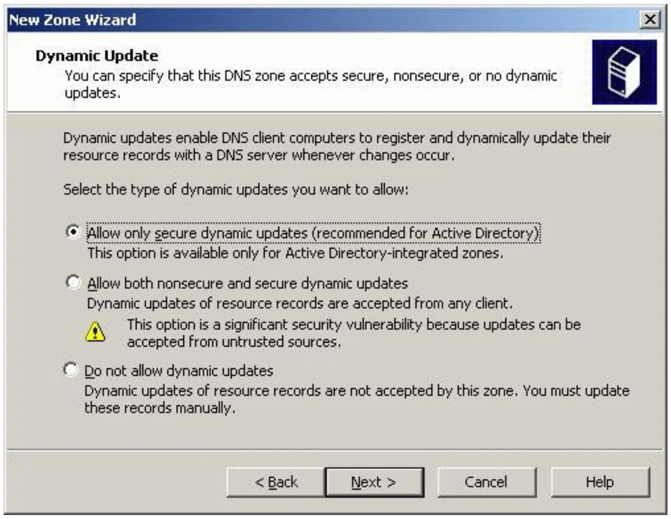
Note that the zone name is not the name of the DNS server and it is only the part of the DNS namespace that this server is authoritative for.

Dynamic DNS Updates
Now, the wizard wants to know if this DNS server will accept **dynamic DNS (DDNS) updates** and, if so, will they be **secure**. Dynamic DNS updates are DNS changes that come from a DHCP server (on behalf of a changed machine) or on behalf of the machine itself. If a DHCP server is registering a DNS change on behalf of a machine, this means that when a new device comes on the network and receives an IP address from a DHCP server, the DNS server will accept the new registration of the new device's IP address and name, making an entry in the DNS server.

For instance, say that you connect a new PC on your network (where you have a DHCP and DDNS server). The new PC is configured to DHCP and you give it a name of PC12 in the domain Mydomain.com. When it requests its IP address, the DHCP server provides one for it and maps it to the MAC of the new PC. The PC provides its name, PC12, to the DHCP server and the DHCP server tells the Dynamic DHS (DDNS) server that PC12 has come online in the domain Mydomain.com. The DDNS server makes a DNS entry for PC12. Mydomain.com and maps it to the IP address that the DHCP server provided.

Secure DDNS
As far as **Secure DDNS** updates are concerned, these are DDNS updates that come from a machine that has authenticated, using AD credentials, with the DNS server. This is the recommended method for Active Directory.

For this example, we will take the default of allowing DDNS entries but only ones that are secure.



New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

● Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

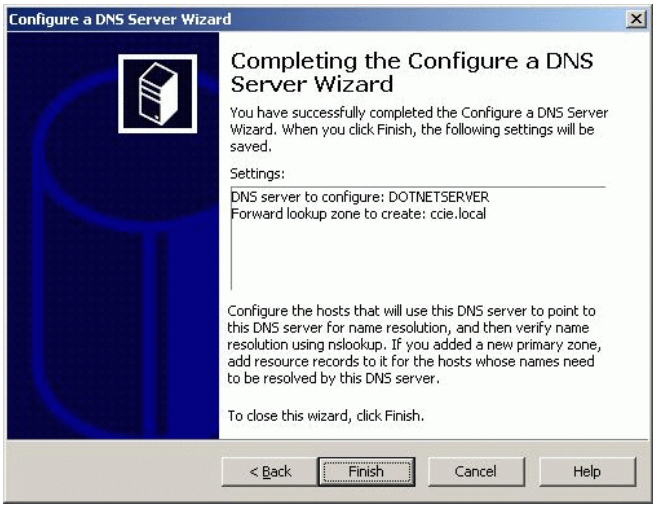
○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.

○ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Figure 15

Next, the wizard asks if you would like this new DNS server to forward DNS queries that it cannot resolve to another DNS server. You would typically do this in small-to-medium sized businesses where you have an Internet Service Provider (ISP) who probably has a large cache of DNS information. In this case, you might want to offload the resolution of thousands of DNS queries off to them and leave your DNS server free to do other things.

And finally, the confirmation screen provides you with the summary of tasks that you are about to perform and is asking you if you are sure.



Configure a DNS Server Wizard

Completing the Configure a DNS Server Wizard

You have successfully completed the Configure a DNS Server Wizard. When you click Finish, the following settings will be saved.

Settings:

DNS server to configure: DOTNETSERVER
Forward lookup zone to create: ccie.local

Configure the hosts that will use this DNS server to point to this DNS server for name resolution, and then verify name resolution using nslookup. If you added a new primary zone, add resource records to it for the hosts whose names need to be resolved by this DNS server.

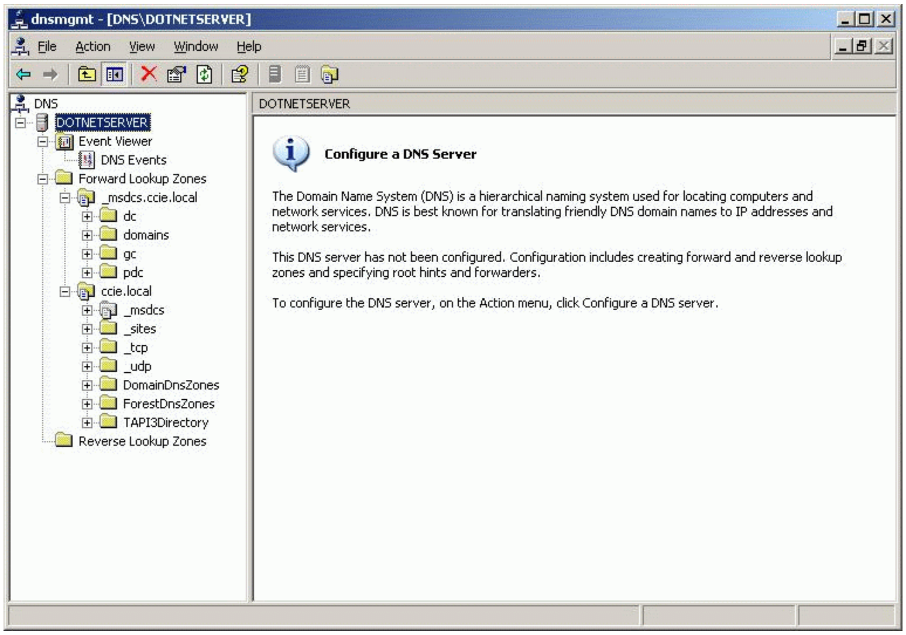
To close this wizard, click Finish.

Figure 16

And the task is complete.

DNS Management Tool
Hopefully, you are already familiar with the Windows Server DNS management MMC add-in. If you are not, here is a brief overview. The primary method of management for the Windows 2003 Server DNS server is the DNS Mgmt MMC Add-in. You can access this add-in by going to **Start -> Administrative Tools -> DNS**.

Once started, the DNS Management MMC add-in looks like this:



Configure a DNS Server

The Domain Name System (DNS) is a hierarchical naming system used for locating computers and network services. DNS is best known for translating friendly DNS domain names to IP addresses and network services.

This DNS server has not been configured. Configuration includes creating forward and reverse lookup zones and specifying root hints and forwarders.

To configure the DNS server, on the Action menu, click Configure a DNS server.

Figure 17

As you can see from the graphic above, the DNS Management console is broken down by starting at the DNS server (DOTNETSERVER, in our case), then going down into three categories:

- Event Viewer
- Forward Lookup Zones
- Reverse Lookup Zones

Right clicking on the name of the DNS server provides you with a variety of tasks that can be performed.

NOTE: To administer Windows DNS from the command line, you need to install **dnscmd**. This is a command-line DNS administration program; however, it is only available in the Windows Support Tools, found on the Windows 2003 Server Installation CD. As this component is considered an optional installation, I won't go into its commands.

We will now go into the variety of common and new tasks that can be performed in 2003 DNS, below.

Configure DNS zone options

How to Create a Forward Lookup Zone

To create a forward lookup zone in Windows 2003 Server DNS, open the DNS MMC Management console.

On your existing DNS server, right click. You will see "New Zone". Select this.

Next, you will be asked if this is to be a primary, secondary, or stub zone.

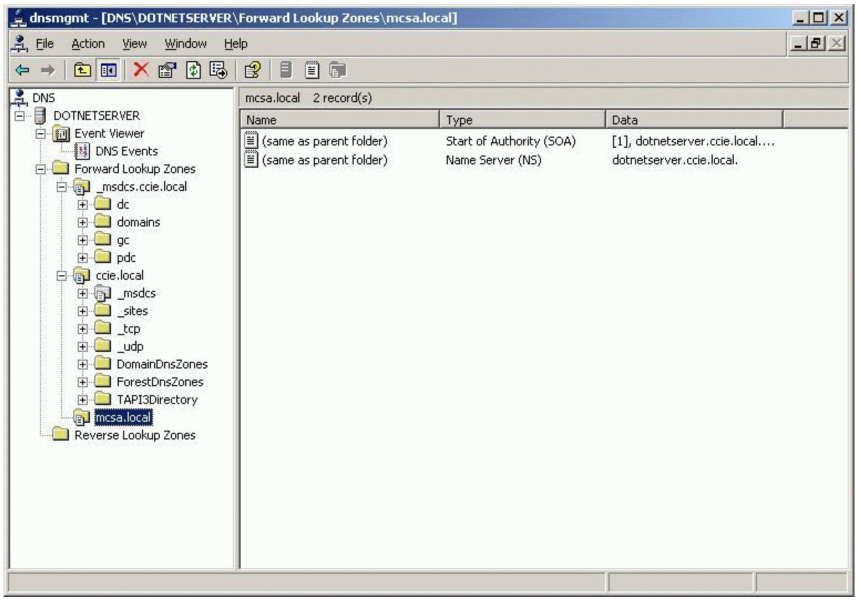
Then, the wizard will ask how you want this zone data replicated. The default is to replicate the DNS zone data to all Domain Controllers in the AD domain.

Now, specify that you want this to be a **Forward lookup zone**. Just a reminder that a Forward lookup zone maps names to IP addresses. On the other hand, a Reverse lookup zone maps IP addresses to DNS names. Of course, you must specify the name of the lookup zone.

Again, we must specify if we want to allow dynamic DNS updates and, if so, whether we will require that they be secure.

And, finally, the wizard confirms your choices before making the new zone. Click Finish.

You can now go back to the DNS Management console and verify that your new forward lookup zone was successfully created:



mcsa.local 2 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], dotnetserver.ccie.local....
(same as parent folder)	Name Server (NS)	dotnetserver.ccie.local.

Figure 18

How to Create Reverse Lookup Zones

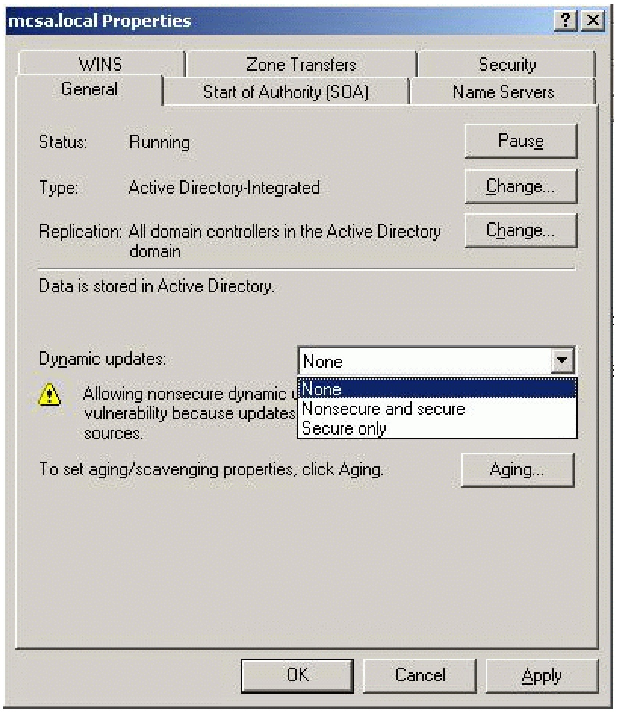
Creating a reverse lookup zone is similar to creating a forward lookup zone.
Remember that reverse lookup zones map IP addresses to DNS names.

Zones for Secure Dynamic Update

By default, zones are not configured to allow dynamic updates. Dynamic updates are a nice feature and provide convenience to network administrators as DNS entries are managed more automatically. On the other hand, DDNS can be a security threat as DNS entries can be created automatically. The "happy-medium" in this is Secure Dynamic Updates. With **Secure dynamic updates**, only workstations that can be positively authenticated, in the AD domain, are allowed to create DNS entries via DDNS.

Take a look at the Properties of a DNS zone, below. You can see that there are three choices for Dynamic Updates:

- None
- Nonsecure and secure
- Only secure



Status: Running

Type: Active Directory-Integrated

Replication: All domain controllers in the Active Directory domain

Data is stored in Active Directory.

Dynamic updates: None

Allowing nonsecure dynamic u
vulnerability because updates
sources.

To set aging/scavenging properties, click Aging.

Figure 19

Active Directory Integrated Zones

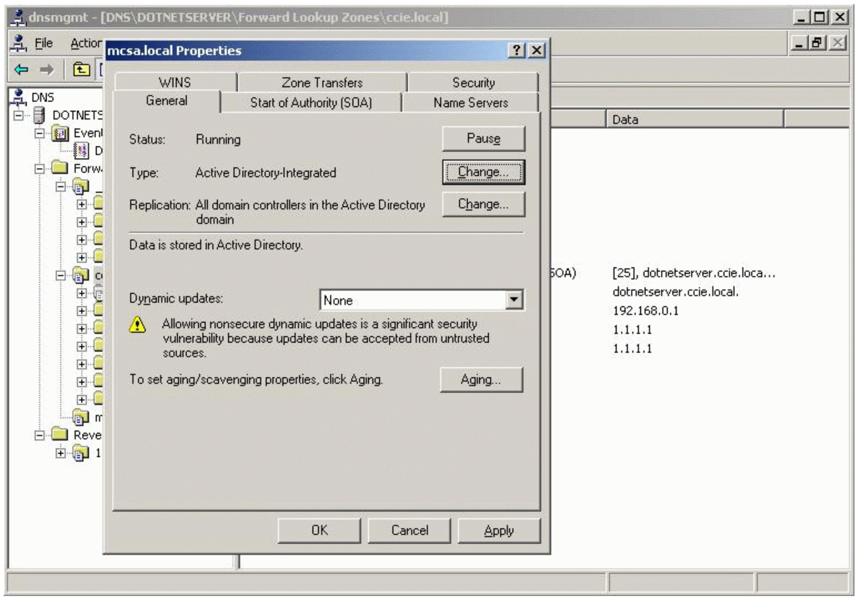
Keep the following in mind concerning AD and DNS integrated zones:

- With Windows Server 2003, DNS is required for locating domain controllers. The netlogon service also uses DNS to register these domain controllers.
- DNS servers that also contain the Active Directory can use AD replication (secure dynamic updates) to also replicate the DNS zone information to all DNS servers.

- When installing a new domain controller, you must either have a Dynamic DNS server available or you must promote that server to be a DDNS server.
- **Directory-integrated** primary zones are highly recommended by Microsoft as they provide multimaster DNS replication and high security for DNS. With multimaster DNS replication, there is no single point of DNS failure.
- Whenever you add a new DC, the DNS zone data is automatically synchronized to it.
- With AD and DNS integration, management of both is done together.
- Windows AD replication is faster than normal DNS replication.

You cannot store secondary DNS zones in the Windows AD, only primary zones. Secondary DNS zones will be stored in a text file.

To view or modify whether a zone is an AD integrated zone, right-click on the zone properties. Under the general tab, you will see the zone type, like this:



dnsmgmt - [DNS\DOTNETSERVER\Forward Lookup Zones\ccie.local]

mcsa.local Properties

Status: Running

Type: Active Directory-Integrated

Replication: All domain controllers in the Active Directory domain

Data is stored in Active Directory.

Dynamic updates: None

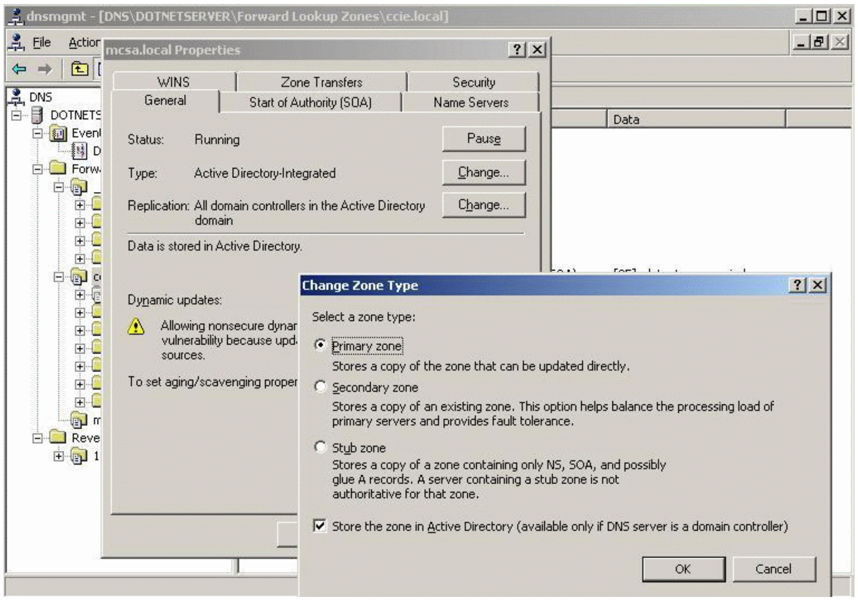
Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.

To set aging/scavenging properties, click Aging.

Figure 20

This shows you the current zone type of your zone. As you can see, this zone is an Active Directory Integrated Zone.

If you select to change the zone type, the following screen will appear:



Status: Running

Type: Active Directory-Integrated

Replication: All domain controllers in the Active Directory domain

Data is stored in Active Directory.

Dynamic updates:

Allowing nonsecure dynar vulnerability because upd sources.

To set aging/scavenging proper

Select a zone type:

● Primary zone
Stores a copy of the zone that can be updated directly.

○ Secondary zone
Stores a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Stores a copy of a zone containing only NS, SOA, and possibly glue A records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a domain controller)

Figure 21 - A

It shows you the three zone types that are available, as well as a check box that allows you to select if you want the zone in the AD.

Creating DNS Stub Zones
A **stub zone** is a copy of an authoritative DNS zone that only contains the records needed to reach the authoritative server. Use stub zones to ensure that the authoritative parent zone DNS server automatically receives updates to the child zone stub DNS server.

Creating a stub zone is very similar to creating a forwarding zone or reverse zone as you use the New Zone wizard.

Configure DNS forwarding

What is a Forwarder?
A DNS **forwarder** is a DNS server that can resolve unresolved queries from other DNS servers. By designating a particular server as the server to forward queries to, that server becomes the forwarder. Usually, the queries being sent are forwarded on to an external DNS server, like an ISP's DNS servers.
By forwarding all unresolved queries to a particular server to have that server forward those queries out to the Internet, you are reducing security concerns because you are limiting all your external DNS traffic to one server.

A DNS server that is configured to use a forwarder will first use its primary and secondary DNS server entries, then, if not resolved, send the request off to the forwarder. If a response is not received within the time specified, the server will attempt to use its root hints.

Configuring DNS Forwarding
To configure DNS forwarding, it is as simple as getting the properties of your current DNS server and clicking on the Forwarders tab.

Next, look at the section entitled "Select domain forwarder's IP Address". Enter the IP address of the DNS server that you will send your unresolved queries to and click the Add button.
Note that the forwarder's IP addresses are listed in the order that they will be queried, so order is important here.

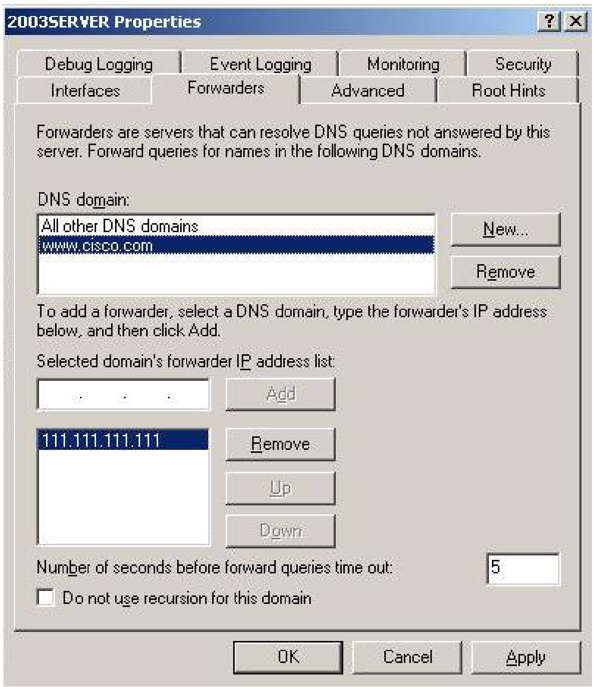
You have now configured a forwarder for your domain.

Configure DNS Conditional Forwarding
What is conditional forwarding?

Conditional forwarding occurs where a server only forwards queries for certain domains to certain DNS servers. In other words, instead of blatantly forwarding all unresolved queries to a forwarder DNS server, you are specifying that you will only forward requests for certain domains to certain forwarders.

Conditional forwarding is primarily used to improve performance of DNS queries. DNS performance is increased because, with conditional forwarding, DNS servers do not have to query the domain root servers, or Internet root servers, but can instead go directly to the DNS server that hosts that domain.

To configure conditional DNS forwarding, it is very similar to configuring regular forwarding. The extra step is to configure the "conditional" part. Basically, you must define what domains you want to go to a particular DNS forwarder. In the example below, I have configured DNS such that all DNS requests for the domain cisco.com will be forwarded to the forwarder 111.111.111.111



Forwarders are servers that can resolve DNS queries not answered by this server. Forward queries for names in the following DNS domains.

DNS domain:
All other DNS domains
www.cisco.com

To add a forwarder, select a DNS domain, type the forwarder's IP address below, and then click Add.

Selected domain's forwarder IP address list:
111.111.111.111

Number of seconds before forward queries time out: 5

□ Do not use recursion for this domain

Figure 21 - B

Manage DNS

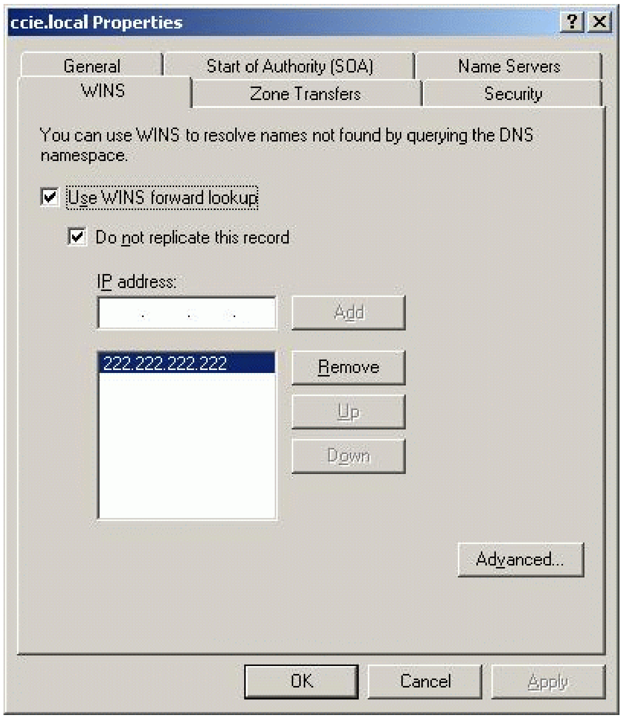
Manage DNS zone settings

In the above section on configuring DNS zones, we went through each of the tabs on the zone properties screen, so you should be now familiar with those. Now, let's focus on some of the more specific DNS zone settings and features.

Using WINS Lookup
You can configure your DNS server to contact a WINS server to lookup DNS names that are not being resolved. Microsoft calls this "WINS Lookup Integration". Clients such as Windows NT and Windows 98 that are not "DNS aware" can use WINS for resolution instead of DNS.

When you configure WINS lookup integration, the DNS management console will automatically create resource records for this. There is the WINS Resource Record (RR) and the WINS-Reverse Resource Record (WINS-R RR). You will notice that once you fill out the WINS integration tab (in either the forward or reverse lookup domains) and click "Apply", the appropriate records will be created.

To access and configure WINS Lookup (WINS lookup integration), go to a zone's properties in DNS management. There is a tab in the zone properties that looks like this:



You can use WINS to resolve names not found by querying the DNS namespace.

☑ Use WINS forward lookup

☑ Do not replicate this record

IP address:

222.222.222.222

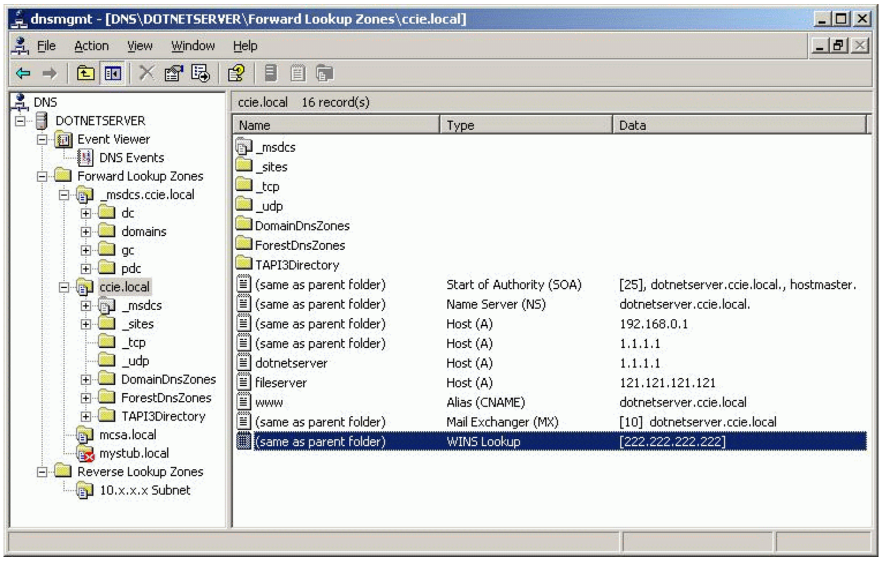
Figure 22

To enable WINS lookup, you must first check the check box marked "Use WINS forward lookup" and then enter the IP address of the WINS server on your network. You can enter more than one, if you have multiple, and set the order in which the servers will be used.

As you can see from the graphic, above, I have configured this zone to use WINS lookup by checking the checkbox and entering the IP address of my WINS server.

The other checkbox on this tab tells your Windows DNS server NOT to replicate these WINS records. This would be used if you had non-Microsoft DNS servers on your network, as Microsoft Windows DNS servers can only use this feature.

Once you have clicked apply or OK, you will notice that in this zone's list of records, there is a new record of the type "WINS Lookup" which points to the IP address of the WINS server that you specified.



dnsmgmt - [DNS\DOTNETSERVER\Forward Lookup Zones\ccie.local]
File
Action
View
Window
Help

- DNS
  - DOTNETSERVER
    - Event Viewer
      - DNS Events
    - Forward Lookup Zones
      - _msdcs.ccie.local
        - dc
        - domains
        - gc
        - pdc
      - ccie.local
        - _msdcs
        - _sites
        - _tcp
        - _udp
        - DomainDnsZones
        - ForestDnsZones
        - TAPI3Directory
      - mcsa.local
      - mystub.local
    - Reverse Lookup Zones
      - 10.x.x.x Subnet

ccie.local 16 record(s)

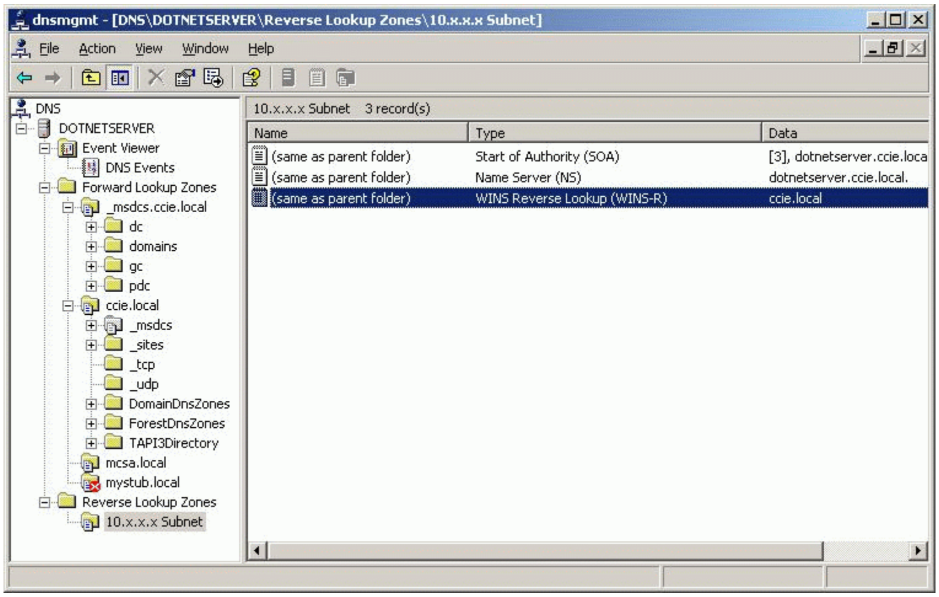
Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
TAPI3Directory		
(same as parent folder)	Start of Authority (SOA)	[25], dotnetserver.ccie.local., hostmaster.
(same as parent folder)	Name Server (NS)	dotnetserver.ccie.local.
(same as parent folder)	Host (A)	192.168.0.1
(same as parent folder)	Host (A)	1.1.1.1
dotnetserver	Host (A)	1.1.1.1
fileserver	Host (A)	121.121.121.121
www	Alias (CNAME)	dotnetserver.ccie.local
(same as parent folder)	Mail Exchanger (MX)	[10] dotnetserver.ccie.local
(same as parent folder)	WINS Lookup	[222.222.222.222]

Figure 23

If you go over to your reverse lookup zones and right-click on properties, you will notice a WINS-R tab.

Just as with configuring forward WINS lookup, to configure reverse WINS lookup, just check the box to enable "WINS-R Lookup" and fill in the name to append to the returned name (like Microsoft.com).

Once you click apply or OK on this box, you will notice that a WINS-R RR is automatically created in the reverse lookup zone.



10.x.x.x Subnet 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[3], dotnetserver.ccie.loca
(same as parent folder)	Name Server (NS)	dotnetserver.ccie.local.
(same as parent folder)	WINS Reverse Lookup (WINS-R)	ccie.local

Figure 24

Comparing Stub Zones vs. Conditional Forwarding

With the introduction of DNS conditional forwarding in Windows 2003 Server, it can be confusing trying to decide if you need a stub zone or conditional forwarding. To try to clear up some of this confusion, below is a list of comparisons between a stub zone and conditional forwarding:

- What the two have in common is that both stub zones and conditional forwarding result in a DNS server responding to a query with a referral to another DNS server or by forwarding a query to that server. This is where the similarity ends.
- Conditional forwarding cannot be used to keep a parent zone updated on the authoritative servers in a child zone. Stub zones DO provide this feature.
- Conditional forwarding will forward requests for only certain domains to certain servers. Stub zones do not but instead return a list of all servers that might be able to service the request.

Delegating Zones

You can hand out the responsibility of certain DNS zones to certain servers. This is known as "delegating zones". You would only want to delegate zones if you have any of the following needs:

- To entrust management of DNS zones over to another department or group.
- To divide traffic load for a large zone into smaller zones to even out DNS requesting traffic.
- To add a large number of sub domains at the same time.

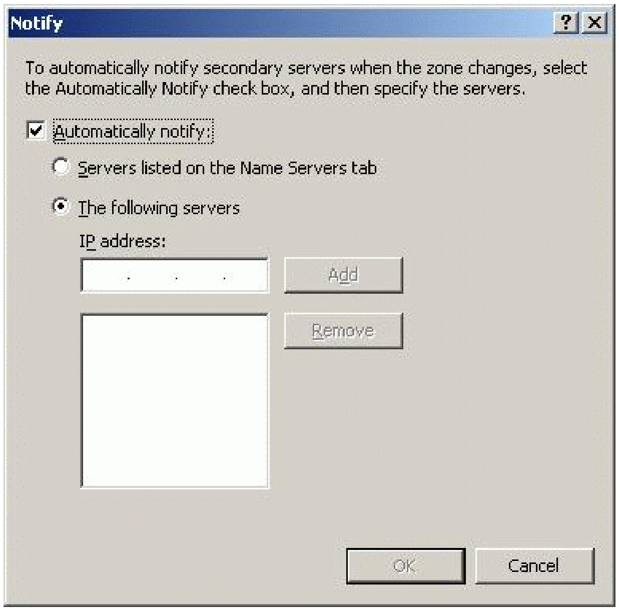
Benefits to using DNS delegation are:

- To provide redundancy of zones.
- To reduce DNS network traffic.
- To supply secondary servers to reduce loads on primary servers.

DNS Notify Lists

DNS Notify lists are a list of DNS secondary servers that will be notified when there are zone changes on the primary server. DNS servers on the secondary notify list will be told that a change has occurs and they will do a zone transfer (copy the zone database to themselves) so that they can become current again. DNS notify works off of pushing the notification message out to the secondary servers and then the secondary servers pulling the zone transfer data back.

To configure DNS Notify, go to the zone properties window of your zone and select the **Zone Transfers** tab. You must select to "Allow zone transfers". Now, click on the "Notify" box. That step will bring up this window:



Notify

To automatically notify secondary servers when the zone changes, select the Automatically Notify check box, and then specify the servers.

☑ Automatically notify:

○ Servers listed on the Name Servers tab

● The following servers

IP address:

Figure 25

This is the notify window. To complete the DNS notification configuration, you would want to check "Automatically Notify" here and then you must fill in the IP Addresses of the secondary DNS servers that you would like to have DNS notify enabled for.

Note that this is not needed for DNS zones that are Active Directory integrated zones as these zones are replicated on all domain controllers and there are no secondary DNS servers with multimaster DNS.

Manage DNS record settings

Managing Authority Records

A DNS server, when first loading zone information, must determine the authority of the zone. It uses start of authority (**SOA**) records and name server (**NS**) records to do this.

- The Start of Authority (SOA) record defines the DNS zone name of origin, primary server name, and basic zone properties.
- The Name Server (NS) record defines what DNS servers are authoritative for this zone. Any DNS server listed as a "NS RR" is an authoritative resource for this DNS zone. In other words, requests that are responded to by the NS server are, with certainty, accurate responses.

- The New Zone wizard automatically creates the SOA and NS records when creating a new zone. Both the SOA and NS records are required records in the zone and are considered the most important records in the zone.
- To view your SOA and NS records, go to the MMC DNS Management console and click on the zone name in question.

Managing Resource Records
There are five main types of Resource Records in a DNS zone. They are:

- Host (A)
- Alias (CNAME)
- Mail Exchanger (MX)
- Pointer (PTR)
- Service Locator (SRV)

Let's cover each of them, just to make sure you are familiar with them:

Host (A) records are your standard DNS to IP static mapping records that make an entry for a specific host (server) in the DNS system. You would typically think of these for things like a web server or any PC in your organization. These records can be either: 1) created manually; 2) created by a DHCP server that issued an IP address and wants to help by registering the DNS name for the client; or 3) a DDNS client PC that registers its own DNS Host record when it boots or receives a new IP Address.

You can create a new Alias Record by right clicking on the current zone and selecting "New Host (A)". After selecting that, you will be asked for the basic information needed to create the simple Host record. Of course, you will need your desired host's DNS name and IP address.

After filling out the required information and clicking "add host", you should be told that it was successfully created. Now, if you look back in your zone information screen, you should see it listed there, along with the SOA and NS records (as well as others).

Alias (CNAME) records map a given domain name to another domain name. Alias records are also known as **canonical** names. Canonical means "in a standard format." For instance, say you created a Host record for a web server named myweb in the domain mcsa.com. You could create an Alias record to map www.mcsa.com to the web server myweb.mcsa.com.

Mail Exchanger (MX) records are used by email servers to locate the email server for a particular DNS domain. An email server will look up the MX record for a domain, like Microsoft.com, and get a particular server to send the email to.

Pointer (PTR) records are DNS records that are used for reverse queries. A PTR record is the reverse of a host record and used in a reverse lookup domain. Just like a host record, PTR records can be created manually, via a DHCP server (DDNS), or through a DDNS Client PC/Server. You won't find PTR records, or an option to configure them, in a forward lookup zone but only in a reverse lookup zone.

Service Locator (SRV) records are DNS records that can be used to locate a service. For instance, the Windows AD uses SRV records for the Netlogon service to locate Domain Controllers. Assuming a DDNS server is available when the AD is installed, these records are created automatically.

Service Locator records can also be used to locate services on the network for applications that support the SRV records. For instance, the finger, ldap, or ftp services might be an example.

Manage DNS server options

A DNS Server's options are primarily controlled, and viewed, through the Properties screen on the DNS server entry in the DNS Management Console.
The tabs on the Properties screen are:

- Interfaces
- Forwarders
- Advanced
- Root Hints
- Debug Logging
- Event Logging
- Monitoring
- Security

From the **Interfaces** tab, you can configure which interfaces the DNS server will listen for requests on. We have already covered the Forwarders tab in the "Configure DNS forwarding" section.

The next tab is the **Advanced** tab. On this tab, you can see such things as the server revision number, whether to load zone data on system startup, when/if the server should scavenge DNS records, and other Advanced DNS server options.

Now we move on to the **Root Hints** tab. This tab shows the root DNS servers on the network that this machine could contact with a request that it could not resolve through it usual chain of servers. You can instruct your DNS server to copy these from another server or you can manually add/delete them.

Next is the **Debug Logging** tab. On this tab, you can configure all the options you may need to diagnose problems with your DNS server by debugging. You can set the types of packets or DNS requests to log as well as the file/folder name and maximum file size.

The **Event Logging** tab configures the DNS server to the level that you would like the DNS server to record messages in the DNS server log. You can specify that you would like No Event, Errors only, Errors & warnings, or All Events logged.

With the **Monitoring** tab, you can configure manual or automatic testing of your server. This testing can be as simple as you selecting to do a simple query and clicking "test now". Or, you can configure to schedule simple or recursive testing on a set schedule.

The last tab of the DNS Server options box is the **Security** tab. This tab is simply the security on this object in the AD. It is broken down by group and user, just as a file or folder would be. This is not something that you would, typically, want to change.

Monitor DNS. Tools might include System Monitor, Event Viewer, Replication Monitor, and DNS debug logs

Why is the proper operation of DNS so important to you, the system administrator? This is because if DNS is not functioning, neither is Active Directory or Internet connectivity. If AD and Internet access are not working, neither are many other critical pieces of your network. In the following, we will cover how to keep an eye on DNS, identify when it isn't working, and know where to go to find out what is wrong when it breaks.

The simplest way to find out if DNS resolution is working is to use the **nslookup** command prompt command. Take a look at the following successful test:

```
C:\> nslookup www.preplogic.com
Server:  ns5.attbi.com
Address:  204.127.202.4

Name:    www.preplogic.com
Address:  63.146.189.41
```

Now, here is an example of an unsuccessful query, when your DNS server is not responding:

```
C:\> nslookup www.preplogic.com
*** Default servers are not available
Server:  UnKnown
Address:  127.0.0.1

*** UnKnown can't find www.preplogic.com: No response from server
```

Nslookup has a great number of options. To take a look at all the nslookup options, just type *nslookup*, by itself, to enter interactive mode. From there, type the ? key to get the full list.

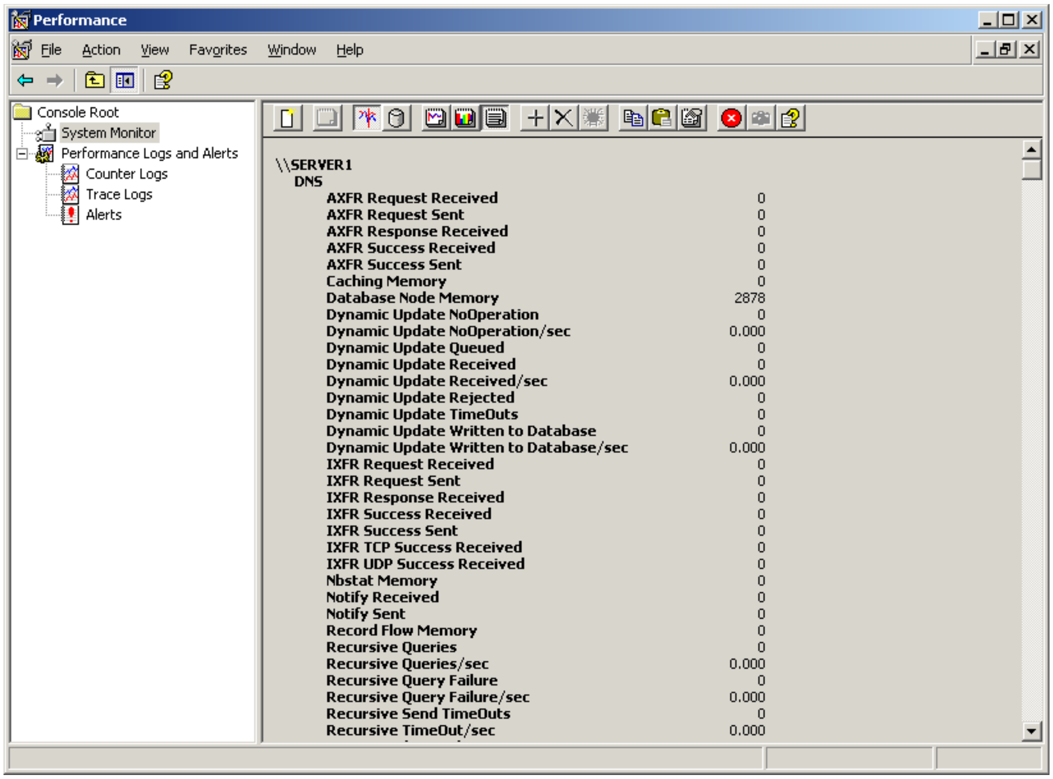
Other tools include:

- System Monitor
- Event Viewer
- Replication Monitor
- DNS debug logs

System Monitor

The Windows Performance Monitor is now called System Monitor. Please keep this in mind as it could confuse you on the exam, causing you to get the wrong answer.

To use the System Monitor, go to Start-> Administrative Tools and click Performance (as if this isn't confusing). With this utility, you can add DNS performance counters such as # of queries received, # of zone transfers, and errors (or you can add them all). These can be viewed real-time or logged to the disk for later viewing. The interface looks like this (this screen shot is in "report view"):



```
\\SERVER1
  DNS
      AXFR Request Received                                   0
      AXFR Request Sent                                       0
      AXFR Response Received                                  0
      AXFR Success Received                                   0
      AXFR Success Sent                                       0
      Caching Memory                                          0
      Database Node Memory                                 2878
      Dynamic Update NoOperation                              0
      Dynamic Update NoOperation/sec                      0.000
      Dynamic Update Queued                                   0
      Dynamic Update Received                                 0
      Dynamic Update Received/sec                         0.000
      Dynamic Update Rejected                                 0
      Dynamic Update TimeOuts                                 0
      Dynamic Update Written to Database                      0
      Dynamic Update Written to Database/sec              0.000
      IXFR Request Received                                   0
      IXFR Request Sent                                       0
      IXFR Response Received                                  0
      IXFR Success Received                                   0
      IXFR Success Sent                                       0
      IXFR TCP Success Received                               0
      IXFR UDP Success Received                               0
      Nbstat Memory                                           0
      Notify Received                                         0
      Notify Sent                                             0
      Record Flow Memory                                      0
      Recursive Queries                                       0
      Recursive Queries/sec                               0.000
      Recursive Query Failure                                 0
      Recursive Query Failure/sec                         0.000
      Recursive Send TimeOuts                                 0
      Recursive TimeOut/sec                               0.000
```

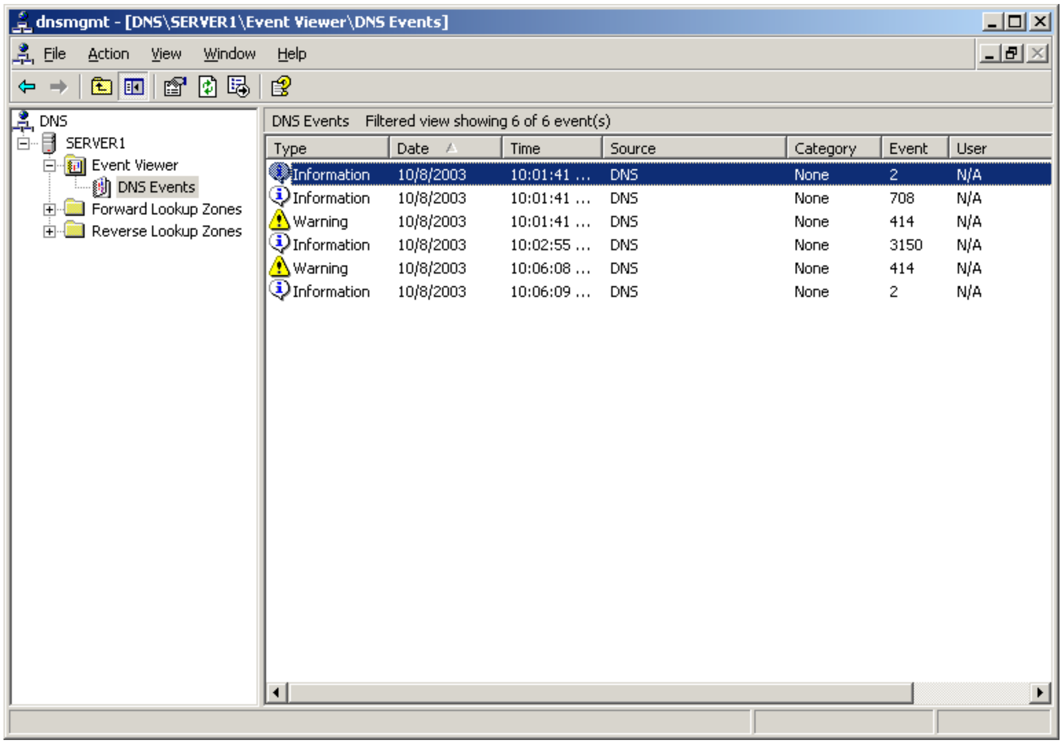
Figure 26

Performance information can be used remotely and viewed across the network, from a client machine. In other words, you don't have to be on the server to perform these functions.

Event Viewer

Once DNS is installed on a server, Event Viewer has another category of events to be viewed, called DNS Server events. Event Viewer is one place you can go to view these events. Event viewer information can be used remotely and viewed across the network, from a client machine. In other words, you don't have to be on the server to perform these functions.

The second place that you can go to view these same events is in the DNS Manager. Within DNS manager, there is an event viewer category with a DNS Events sub-category. This interface looks like this:



dnsmgmt - [DNS\SERVER1\Event Viewer\DNS Events]

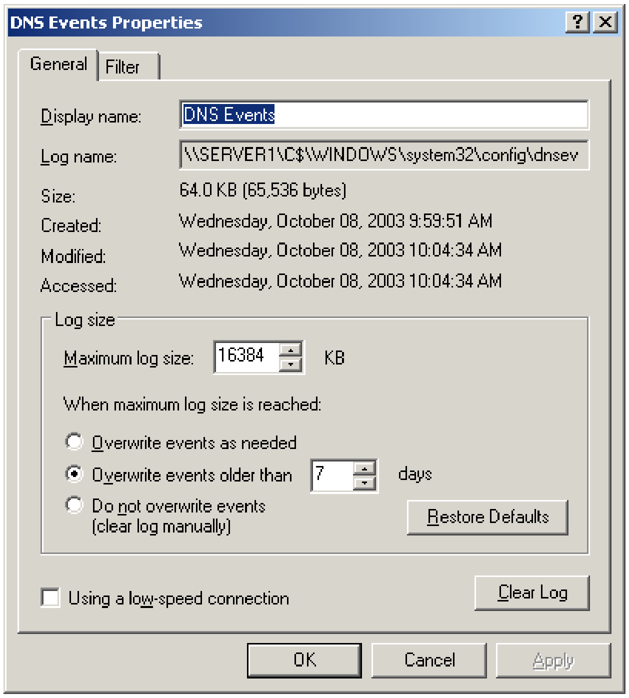
- DNS
  - SERVER1
    - Event Viewer
      - DNS Events
    - Forward Lookup Zones
    - Reverse Lookup Zones

DNS Events Filtered view showing 6 of 6 event(s)

Type	Date	Time	Source	Category	Event	User
Information	10/8/2003	10:01:41 ...	DNS	None	2	N/A
Information	10/8/2003	10:01:41 ...	DNS	None	708	N/A
Warning	10/8/2003	10:01:41 ...	DNS	None	414	N/A
Information	10/8/2003	10:02:55 ...	DNS	None	3150	N/A
Warning	10/8/2003	10:06:08 ...	DNS	None	414	N/A
Information	10/8/2003	10:06:09 ...	DNS	None	2	N/A

Figure 27

If you right-click on the DNS Events category and select Properties, you will get this window:



Display name: DNS Events
Log name: \\SERVER1\C$\WINDOWS\system32\config\dnsev
Size: 64.0 KB (65,536 bytes)
Created: Wednesday, October 08, 2003 9:59:51 AM
Modified: Wednesday, October 08, 2003 10:04:34 AM
Accessed: Wednesday, October 08, 2003 10:04:34 AM

Log size
Maximum log size: 16384 KB
When maximum log size is reached:
○ Overwrite events as needed
● Overwrite events older than 7 days
○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

Figure 28

This window is the same as the normal event viewer properties configuration window for each of the other event viewer categories (like System, Application, and Security). With DNS Event Properties, you can configure the log size, whether to overwrite the log when full, clear the log, and (with the filter tab) filter the types of events you would like to see (or not see) in the DNS log.

Replication Monitor

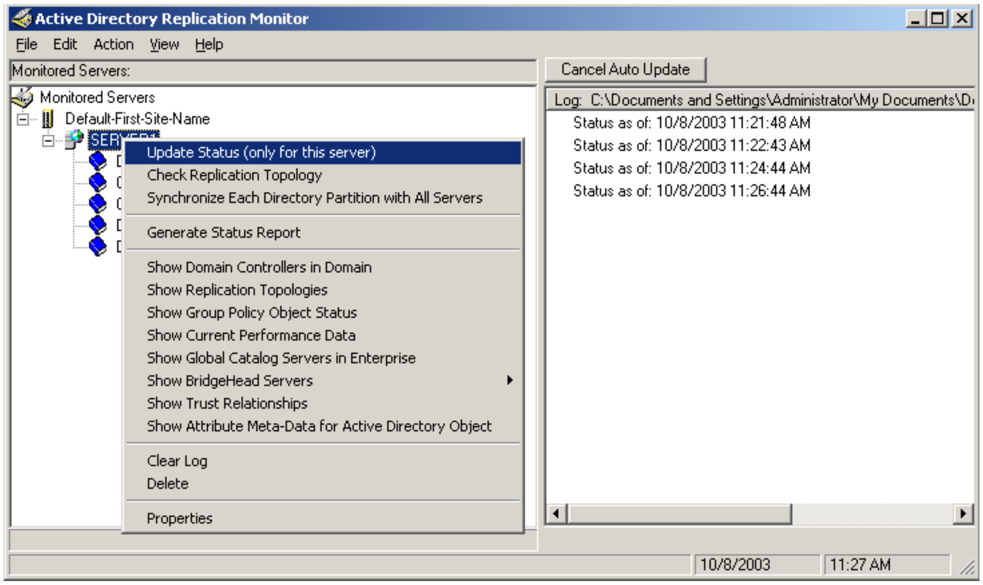
A very powerful tool to obtain DNS information is the Windows Replication Monitor. This tool is not installed by default and must be installed from the Windows Server CD by installing the Support Tools. These are installed by running the support tools installation program, located on the Windows Server CD at \Support\Tools\SupTools.msi.

Once this is installed, you can run **replmon.exe**. Once running, you can do the following with Replication Monitor:

- Check the status of your server, and all other servers, within your domain.
- See which server has which role within the domain.
- Verify replication topology.
- Force replication with other servers.
- Query (test) domain servers supporting the **FSMO** (Flexible Single Master Operations) roles.

- Create a log file of all AD information for each server.

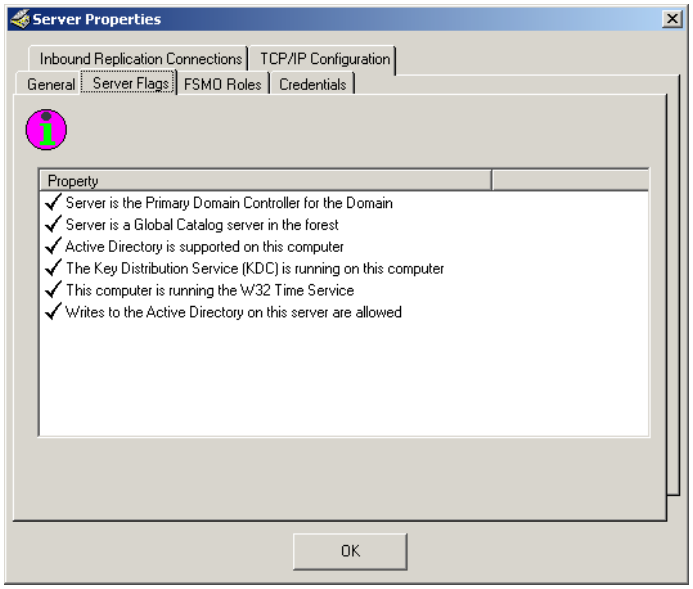
Replication monitor looks like this:


Active Directory Replication Monitor
File Edit Action View Help
Monitored Servers:
Monitored Servers
Default-First-Site-Name
SERVER1
Update Status (only for this server)
Check Replication Topology
Synchronize Each Directory Partition with All Servers
Generate Status Report
Show Domain Controllers in Domain
Show Replication Topologies
Show Group Policy Object Status
Show Current Performance Data
Show Global Catalog Servers in Enterprise
Show BridgeHead Servers
Show Trust Relationships
Show Attribute Meta-Data for Active Directory Object
Clear Log
Delete
Properties
Cancel Auto Update
10/8/2003
11:27 AM

```
Log:  C:\Documents and Settings\Administrator\My Documents\D
    Status as of: 10/8/2003 11:21:48 AM
    Status as of: 10/8/2003 11:22:43 AM
    Status as of: 10/8/2003 11:24:44 AM
    Status as of: 10/8/2003 11:26:44 AM
```

Figure 29

This is an example of the many AD server services that can be checked with replication monitor:

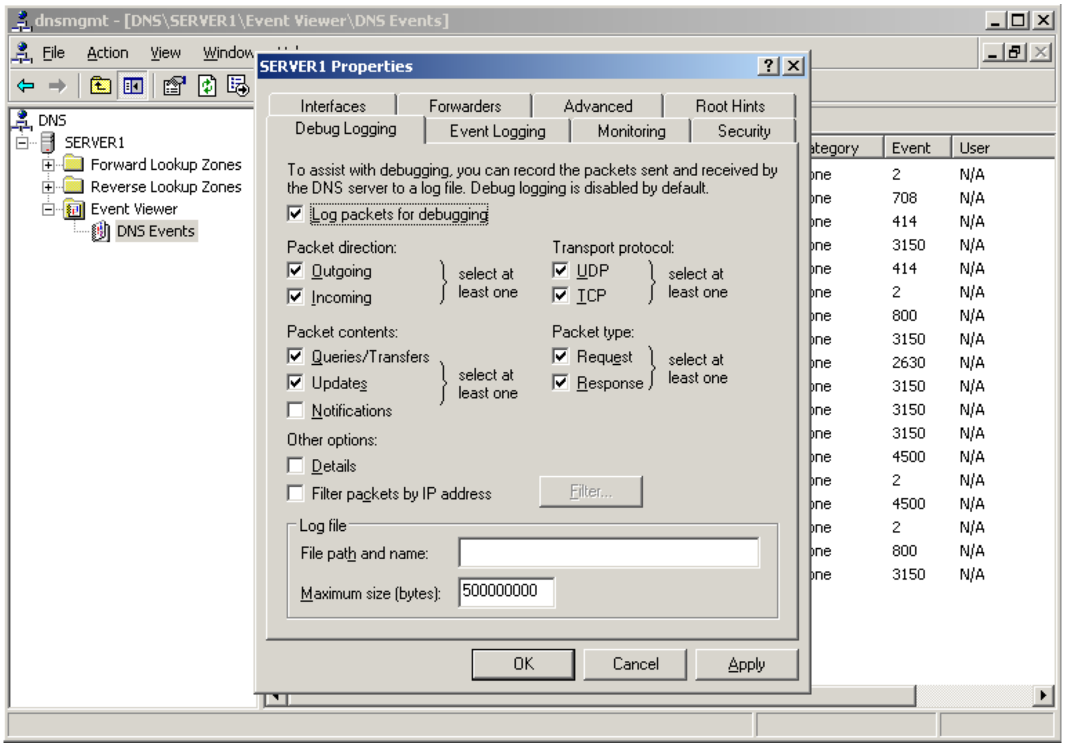


✓ Server is the Primary Domain Controller for the Domain
✓ Server is a Global Catalog server in the forest
✓ Active Directory is supported on this computer
✓ The Key Distribution Service (KDC) is running on this computer
✓ This computer is running the W32 Time Service
✓ Writes to the Active Directory on this server are allowed

Figure 30

DNS Debug Logs

By default, the Microsoft DNS Server creates and uses the log file named c:\windows\system32\dns\dns.log. However, this log normally only contains DNS errors. If you would like to modify the DNS server to log more than just errors, use the DNS Manager and go to the DNS Server Properties. Under the Debug Logging tab, you can enable the server to log all types of DNS information to this log file. This tab looks like this:



To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

☑ Log packets for debugging

Packet direction:
☑ Outgoing
☑ Incoming
select at least one

Transport protocol:
☑ UDP
☑ TCP
select at least one

Packet contents:
☑ Queries/Transfers
☑ Updates
□ Notifications
select at least one

Packet type:
☑ Request
☑ Response
select at least one

Other options:
□ Details
□ Filter packets by IP address

Log file
File path and name:
Maximum size (bytes): 500000000

ategory	Event	User
ne	2	N/A
ne	708	N/A
ne	414	N/A
ne	3150	N/A
ne	414	N/A
ne	2	N/A
ne	800	N/A
ne	3150	N/A
ne	2630	N/A
ne	3150	N/A
ne	3150	N/A
ne	3150	N/A
ne	4500	N/A
ne	2	N/A
ne	4500	N/A
ne	2	N/A
ne	800	N/A
ne	3150	N/A

Figure 31

This log file is actively in use by the DNS server so the DNS server service must be stopped before you can view the file. Also, the dns.log is created in RTF format so you must use Word or WordPad to view the file.

Implementing, Managing, and Maintaining Network Security

Implement secure network administration procedures

Some new Windows 2003 Server features are:

- Windows 2003 completely supports **IPV6**.
- PPPoE, or PPP over Ethernet. This is used by many ISP's to connect to the Internet.
- Bridging, to connect network segments.
- IPSec over NAT, also known as **L2TP/IPSec NAT-T**. This relieves the difficulties in using NAT and IPSec together. See Knowledge Base article 818043.
- Internet Connection Firewall (**ICF**). This is used to provide a basic firewall for PC's connected to the Internet.
- IPSec Load Balancing provides load balancing for VPN servers.
- Wireless Security with **802.1x** provides wireless networking using Windows username/password credentials without having to use certificates.

Principle of Least Privilege and Security Baselines

Microsoft Recommends the Following "Best Practices" (taken from the Microsoft Help documentation):

Physical Access
Limit access to servers as much as possible. Lock down computer rooms, the network room, and wiring closets. The servers that are most important to secure, on the network, are domain controllers. Domain controllers contain all the domain's username and passwords. These items are the keys to all network resources. Only the most trusted systems/network administrators should have physical access to the servers. Once physical access is obtained, access to the software can be accomplished, one-way or the other. With physical access, the server can be rebooted and, using the console, the intruder could access the hard disks of the server from the command line. For the persons that have physical access, you should attempt to log entry, exit, and actions electronically, along with implementing video and/or security systems.

The Principle of Least Privilege
For those of you who aren't familiar with the principle of least privilege, it requires that a user be given no more privilege than necessary to perform his job. To do this, you must first identify what the person's exact job duties are, determine the security required to perform that job, and then provide the user that access (and no more). If you allow persons more privilege than necessary to do their job, you are, in effect, creating a security hole.

Besides just applying to how to assign privileges to users, the principle of least privilege applies also to how administrators use administrative accounts. You should always login as yourself then, if you need to perform an administrative action, become the administrator account. To "become" the administrator after logging in as yourself, you would use the **runas** command. This allows you to enter the administrator's password and assume his access. The runas command in Windows is the same as the "su" (super-user) command in Unix. Both allow you to assume the privileges of another user. Never login as administrator. This is because someone could place a script in the administrative profile or use the account after you walk off and neglect to log out.

This goes back to using the runas service to run administrative programs. This is the best practice that all administrators should take. To use the runas service, the "secondary logon service" must be running. Besides running programs with runas at the command line, you can use the secondary login (runas) when you are running a shortcut or graphical program.

Develop a Security Policy
A very important part of securing your company, servers, and network is developing a security policy. The security policy is considered the governing "law" of the company, with respect to security. Just like without laws, a government and society cannot function, without a security policy, network security cannot function. Without a security policy users do not know what is and is not expected of them, network administrators cannot audit and enforce policies, and logs cannot be interpreted.

Implement security baseline settings and audit security settings by using security templates

Key items:

- **Security Baseline** - Just as you should have a performance baseline for your servers and a network baseline for your network, believe it or not, you should also have a security baseline for your servers and network. A baseline will define for you what is the "norm." What is the normal number of password violations, failed logins, denied firewall packets, etc, per day, per hour, per minute, and where do they normally come from? Know how to find these statistics and how to view them. You will need to know these types of things should you ever suspect an attack, suspect that activity has mysteriously gone up, or want to know if someone has violated security. If you don't have a baseline, you'll never know where to start.

While you could create a baseline manually, as complex as the Windows operating system is today, this could be difficult and prone to errors. Microsoft knows this and has created a tool to assist in this. This tool is the Microsoft Baseline Security Analyzer (**MBSA**). It can be found at this site.

MBSA can analyze your local system, or remote systems, and deliver a report to you on missing patches, accounts with poorly configured passwords, or applications with less secure settings. To use it, you simply download it, install it, run it, and tell it what you want to scan.

- **Audit Security Settings by using security templates** - Once you have baselines and have a policy, you can use these to make security templates. These will be cookie-cutter-like settings that you can set on every machine or every server to make sure that each machine is applying the appropriate security policies.

Next, you will have to audit those policies. If you configure a server to audit every file in the payroll directory that is modified, how will you know that there is a violation if you do not have a record of who and how it was accessed?

Microsoft has provided nine built-in security templates to aid in securing your Windows network. All of these security templates end in the .inf extension. Here are some of these templates and their purpose:

- **Securews** – Strengthens local account policies, and is used on workstations.
- **Hisecws** – Stronger than Securews and used on workstations.
- **Compatws** – Allows more legacy applications to work by changing file and registry permissions.

- **Setup Security** – This is the template that was created when your server or workstation was installed. Without your knowledge, it captured the security settings at the time the operating system was freshly installed. This can be very useful to compare current versus default installation security settings.
- **DC Security** – Used to secure a domain controller (DC). You would apply this to a DC to ensure that it has the default security settings for a DC.
- **Securedc** – Templates beginning with "secure" are least likely to impact applications. These templates enhance security on things like password complexity, lockout settings, and audit settings. The "securedc" template is designed to do these types of things on a domain controller.
- **Hisecdc** – The High Secure templates are stronger than the secure templates and provide additional security enhancements, such as authentication and encryption on connections. The "hisecdc" template does this for domain controllers. If you use the "hisecdc" templates, one of the many enhancements is that all domain controllers must be running Windows Server 2000 or 2003.

More information is available on these predefined templates.

In general, some templates are created at system or domain controller installation to provide a baseline of what security was at installation time. These make excellent baselines to compare against, as many security administrators were not around when systems were installed. Other templates apply to particular applications, like making a server a domain controller, running a server as a terminal server, or the Windows root drive security.

These templates are located in %windir%\Security\Templates and can be viewed as text files.

You use the Security Configuration and Analysis Tool, along with the templates, to perform these tasks. How to use this tool is discussed later in this section.

Defining proper group membership and privileges
As we talked above about the principle of least privilege, you must assign each user to a group and assign privileges to a group (and the proper privileges, at that!).

Many of the privileges you will assign have to do with what level of privileges the user's applications will require. For instance, old legacy applications must have direct access to hardware. With these types of applications you must assign more privileges to users. By assigning more privileges to a user, you are opening up more access on the network. Thus, certain, older, legacy applications (on 2000 and XP) can actually create security concerns for a network. With older legacy applications, you may have to put regular users in the "Power Users" group. Being a member of the Power Users group provides greater access to hardware devices. On the other hand, normal Windows applications should keep security more intact and allow you to just put regular users into the Windows "Users" group. This will not allow the users any more privileges than usual.

Secure local PC systems
Although it might seem like overkill, locking down software, operating system, and hardware configurations on a local PC system is a very prudent security measure. Many of the security breaches of your servers and network will begin by a local PC being compromised.

If at all possible, do not give users administrative control (or any special access for that matter) on their local PC systems. For example, do not allow them access to the Windows Registry on local systems.

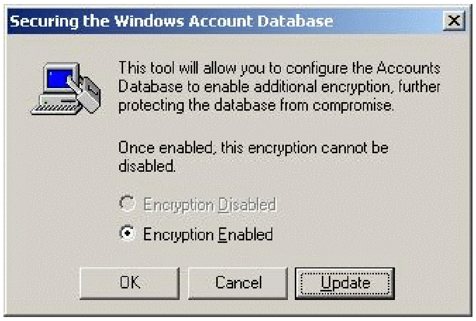
Securing the Windows Security Account Manager (SAM) database with SYSKEY
The Security Account Manager (**SAM**) Database is the registry on workstations and member servers. This database stores the usernames and passwords for the domain or local workstation (depending on where the SAM is that we are talking about).

As this database contains the usernames and passwords it is of extreme importance. If an intruder could gain access to this database and retrieve domain usernames and passwords, especially the administrator account, then the intruder could have full access to the network.

As hackers know that the administrator username and password is the target to get, the SAM is the first place they will typically attempt to gain access to. There are numerous password-cracking programs available that are especially designed to gain access to the SAM database usernames and passwords.

To protect the SAM, Microsoft recommends using the **SYSKEY** utility. This program, *syskey.exe* (stands for system key) will encrypt the SAM database to make it more difficult to crack.

When you run the *syskey.exe* utility, you will see this dialog box:



Securing the Windows Account Database

This tool will allow you to configure the Accounts Database to enable additional encryption, further protecting the database from compromise.

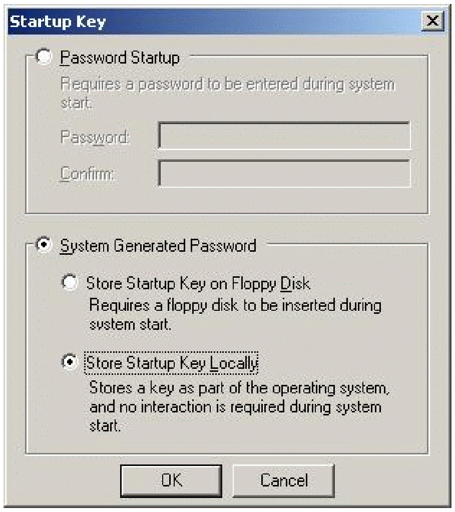
Once enabled, this encryption cannot be disabled.

○ Encryption Disabled

● Encryption Enabled

Figure 32

This shows if the SAM database encryption is enabled or disabled. In this case, it is already enabled. If you click Update, you will see this dialog box:



Startup Key

○ Password Startup

Requires a password to be entered during system start.

Password:

Confirm:

● System Generated Password

○ Store Startup Key on Floppy Disk

Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally

Stores a key as part of the operating system, and no interaction is required during system start.

Figure 33

This Update box allows you both to view your current syskey settings as well as change them. As you can see from the picture, currently this system is set to store the syskey, locally, as part of the operating system.

With this setting the encryption and password are transparent to the user.

The other two options are to require the syskey to be entered each time the system starts OR to have the syskey located on a floppy disk that must be inserted when the system boots. While these might be a little extreme for just a "regular" PC, either of these are good ways to protect domain controllers.

Enforce a Strong Password Policy

An important part of a secure network is a strong password policy. Usernames and Passwords are the "keys" to our network. If a user sets their password to "1234", this is, virtually, an open door to your network. Read more about what Microsoft says about complex passwords. Complex passwords include using letters, numbers and at least one symbol in the password like a hyphen, for example.

Do not run unknown or untrusted programs

Any normal user can run a virus, worm, or Trojan program and wreak havoc on a network. Consider what would happen if a person logged on with system administrator privileges were to run the same destructive program. This could cause much greater company network chaos, simply by the change in user credentials.

Ensure that virus software definitions and scanning programs are up to date

In order to catch these viruses, worms, and Trojans that I wrote about in the previous paragraph, you must have current virus definitions and software. The virus definitions are the characteristics that virus software uses to identify a harmful program. If the virus scanner does not know what to look for, the harmful program could get through. As new viruses, worms, and Trojans come out every day, maintaining current virus definitions and programs is critical to a secure network.

Ensure that Operating System patches are kept current

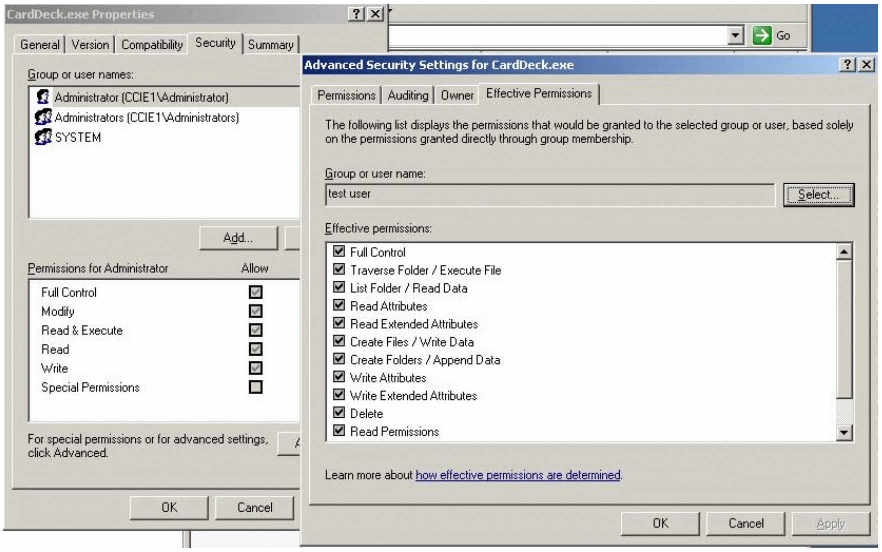
Just as we must keep virus definitions current to detect harmful software, we also must keep operating system software current, as the holes that these patches will fill are certain to be exploited by these harmful programs. Unfortunately, there are new operating system holes found almost daily. Fortunately, Microsoft provides the Software Update Service that can be used to more automatically update systems, virtually, real-time.

Common Tasks of Windows Security Administration

Determine the effective NTFS permissions for files and folders

Multiple users and groups have a variety of permissions on a file. You want to find the real permissions of a file for a single user, let's say, after combining all the different group, user, and folder permissions. How do you do this?

Locate the file in Windows Explorer, right click on it and select Properties. When the properties window appears, select the Security tab on the top. On the Security tab, select Advanced. Next, when the advanced Window comes up, select the Effective Permissions tab. A snapshot of the Security window and advanced window are shown below:



CardDeck.exe Properties

General | Version | Compatibility | Security | Summary

Group or user names:

- Administrator (CCIE1\Administrator)
- Administrators (CCIE1\Administrators)
- SYSTEM

Permissions for Administrator	Allow
Full Control	☑
Modify	☑
Read & Execute	☑
Read	☑
Write	☑
Special Permissions	□

For special permissions or for advanced settings, click Advanced.

Advanced Security Settings for CardDeck.exe

Permissions | Auditing | Owner | Effective Permissions

The following list displays the permissions that would be granted to the selected group or user, based solely on the permissions granted directly through group membership.

Group or user name: test user

Effective permissions:

- ☑ Full Control
- ☑ Traverse Folder / Execute File
- ☑ List Folder / Read Data
- ☑ Read Attributes
- ☑ Read Extended Attributes
- ☑ Create Files / Write Data
- ☑ Create Folders / Append Data
- ☑ Write Attributes
- ☑ Write Extended Attributes
- ☑ Delete
- ☑ Read Permissions

Learn more about how effective permissions are determined.

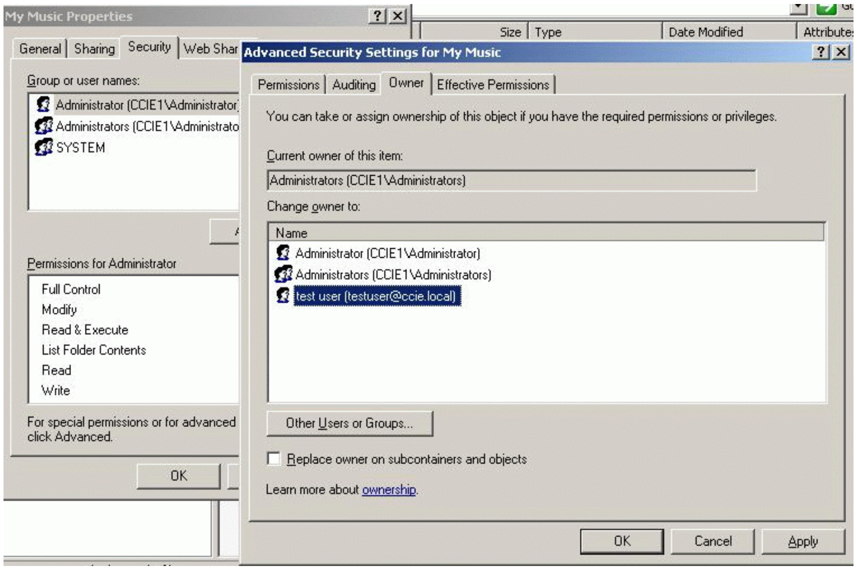
Figure 34

On the effective permissions tab, you will have to enter an AD (domain) user/group or local user/group name. Once you verify the name, you will see the effective permissions for the file or folder that you selected. Remember that these are only estimated permissions based on if the user you specified did login to this system. The user could access this file/folder through a share, proxy server, or other method and that would change the actual permissions. Also, once the user logs into the system, the local policies or group memberships could affect the effective permissions the user has to the file/folder you are inquiring on. Just to clarify, remember that effective permissions are "estimated permissions", not actual permissions.

In other words, effective permissions are the combination of folder and file permissions. The most restrictive permission prevails. For example, if a user has the Everyone group full control and a file read permission, the effective permission is read. If the user is a member of several groups that have full, read, and read/execute permissions, the less restrictive permission applies - in this case full permission.

Change the owner for an existing file or folder
So, how do you change the owner of a file or folder?

Let's find out. Locate the file or folder in Windows Explorer, right click on it and select Properties. When the properties window appears, select the Security tab. On the Security tab, select Advanced. Next, when the Advanced window comes up, select the Owner tab. A snapshot of the Security window and advanced window are below:



You can take or assign ownership of this object if you have the required permissions or privileges.

Current owner of this item: Administrators (CCIE1\Administrators)

Change owner to:

- Administrator (CCIE1\Administrator)
- Administrators (CCIE1\Administrators)
- test user (testuser@ccie.local)

□ Replace owner on subcontainers and objects

Learn more about ownership.

Figure 35

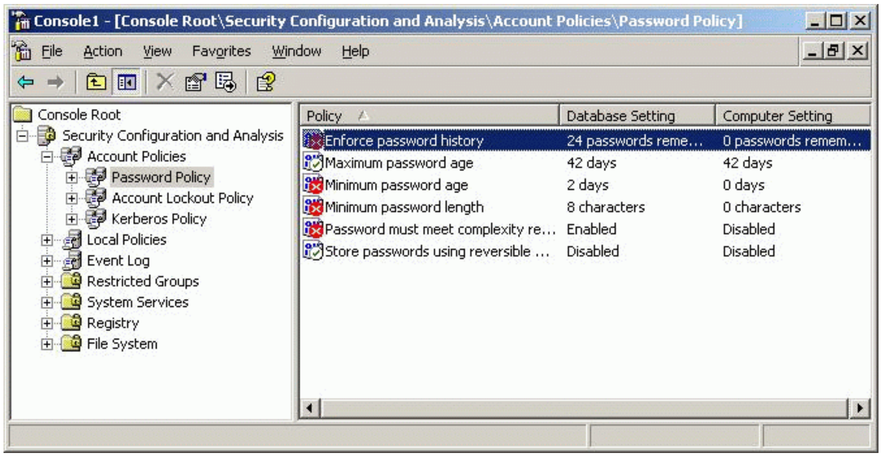
From here, you can select to change the owner of the file or folder to another user.

Using Security Configuration and Analysis
Know the following:

- Security Configuration and Analysis is an MMC add-in tool that can be used, with security templates, to analyze, audit, and configure a system's security.
- To access the Security Configuration and Analysis tool, start by typing **MMC** in the Run text box, choose Add/Remove Snap-in, choose Add and add it, just like all the other system administration MMC tools.
- Once you have it up, if you have not used it before, you will have to create a new database by choosing "open new database" and entering the name of the database. You then import one of the built-in security templates.
- Next, you can "Analyze Computer Now" based on the template you selected. By selecting to "analyze computer now", you are comparing the predefined template that you selected to the current settings on the computer you are analyzing. Once the analysis is completed, you will be able to see how the system's security settings have changed or how its settings compare to the template chosen. If you want to use other templates, you can select "Import Template" from the menu and analyze the computer based on that template.

- Then, you may want to "Configure Computer Now", based on the template or the settings you have chosen. When you "configure computer now", you are choosing to automatically change security settings on your system, based on the settings contained in the template that you chose.
- This tool uses a tree structure to present all the possible security information it has access to. From this structure you can go in and change individual settings, and then apply these, as a whole, to your system.

The tool looks like this:



Policy	Database Setting	Computer Setting
Enforce password history	24 passwords reme...	0 passwords remem...
Maximum password age	42 days	42 days
Minimum password age	2 days	0 days
Minimum password length	8 characters	0 characters
Password must meet complexity re...	Enabled	Disabled
Store passwords using reversible ...	Disabled	Disabled

Figure 36

Software Update Services

Although not mentioned specifically in the list of test topics, Software Update Services (**SUS**) is an important part of maintaining and managing a secure network. Why? For machines to be secure, they must have the latest security patches. So, how do you do this in a network with many machines- enter Software Update Services.

Some SUS features are:

- The Windows Catalog Site can be used by administrators to download patches and drivers for later distribution.
- Auto updating can be configured such that patches and drivers can be automatically installed via either the Internet or through intracompany distribution.
- Dynamic Update can be configured to provide drivers to machines that require them during setup.
- Installable version of Windows update for internal company use. Internal company users can point machines to go to an internal Windows update host. Client machines would use the automatic update client, which can be configured with group policy.

Install and configure software update services

SUS is a downloadable installation from Microsoft. You must download the 32MB SUS and install it from the website, listed below. As of this writing, there is an SUS SP1, as well, that should be applied after installation (if you don't download the version with SP1 already integrated). IIS (Internet Information Services) is required to install SUS. Once you install SUS, it runs as a service.

To download SUS, go to the SUS website and look for the Download link.

Tips:

- Before installation, you should read the Microsoft Software Update Services Overview Whitepaper and the Microsoft Software Update Services Deployment Guide.
- You can download the SUS installation program from the Microsoft Software Update Services website.
- SUS can only be installed on a server running Windows 2000 Server (with SP3 or higher) or Windows 2003 Server. Also, potential servers must have IIS5 (or higher) and IE5.5 (or higher). SUS must also be installed on an **NTFS** partition.
- Assuming you have met the installation requirements (operating system and IIS installed already) there are only a couple of questions asked of you when installing SUS. You will be asked what the URL will be for the SUS clients to contact your SUS server. If you take the typical installation method, then that is all you will be asked. If you take the custom installation method, then you will have to provide settings like the installation location, etc.

Install and configure automatic client update settings

Note that Microsoft SUS only updates Windows 2000 (Professional, Server, and Advanced Server), Windows XP (Home and Professional), and Windows Server 2003 operating systems. SUS will not update any other operating systems. The updates that SUS distributes are ONLY security rollup packages and critical update packages. Packages like Office updates, SQL server updates, or any other Microsoft application updates are NOT distributed via SUS.

SUS requires Windows 2000 SP3, or greater. Machines running Windows 2000 SP2 or Windows XP without SP1 will need the client installation. Machines running Windows 2000 SP3 (and up) or Windows XP SP1 (and up) will not.

A nice benefit to using SUS is that it can be used on systems that do not have Internet access and the updates only have to be downloaded once from the Internet and then are, most likely, distributed via a fast-Ethernet internal LAN.

The Automatic update client supports the following features:

- Approval of updates prior to delivery to clients.
- Scheduling of downloaded updates.
- The flexibility of being configurable via group policy or via the registry.
- The ability to install updates on systems where there is no local administrator logged on.

To manually configure the Automatic update client that is installed with the more recent operating systems, go to Control Panel, then to the System settings. Click on the Automatic Updates tab.

From this tab, you can configure whether you want automatic update to run and how you want the updated process to behave: to be notified before updates are installed, to download and install updates automatically, or to download and install updates at a set time.

Know the answers to the following: What is the benefit of using SUS? Can other servers be updated? How is SUS set up? What are the configuration options?

Configure software updates on earlier operating systems

For those clients that are not running Windows 2000 SP3 or Windows 2003 Server, you will need to install the SUS client update.

Once you have installed this update, these SUS clients will have the features that are available in SUS SP1.

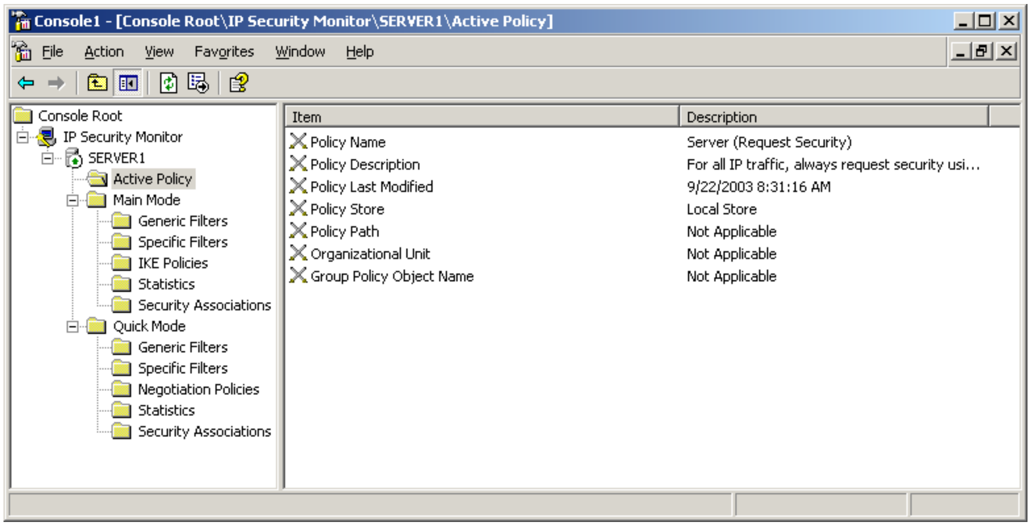
Monitor network protocol security. Tools might include the IP Security Monitor Microsoft Management Console (MMC) snap-in and Kerberos support tools.

You will not know if you have configured network security properly unless you monitor it. So how do you create an IP Security policy? Use the **IP Security Policies** MMC snap-in or **Netsh** command. Once your IP Security policy is created, how do you monitor network security? You can use the IP Security Monitor MMC snap-in and Netsh/Netdiag. In this section, we will cover a couple of handy network security tools: the IP Security Monitor MMC and the Kerberos Support Tools. Let's look at each.

IP Security Monitor

The IP Security Monitor MMC snap-in is accessible by typing MMC in the Run text box and adding the IP Security Monitor snap-in. By default, there is not a link to this under administrative tools but you could create one.

Once you have started the MMC and added the snap-in, the tools looks like this:



Console1 - [Console Root\IP Security Monitor\SERVER1\Active Policy]

Item	Description
Policy Name	Server (Request Security)
Policy Description	For all IP traffic, always request security usi...
Policy Last Modified	9/22/2003 8:31:16 AM
Policy Store	Local Store
Policy Path	Not Applicable
Organizational Unit	Not Applicable
Group Policy Object Name	Not Applicable

Figure 37

Notice that this server has an active policy that requests IP Security.

Policies must already be activated with either IP Security or Netsh for you to be able to monitor them with IP Security Monitor.

With IP Security Monitor, you can retrieve the particulars about the policy that is applied, the main and quick mode statistics, and what the current security associations are.

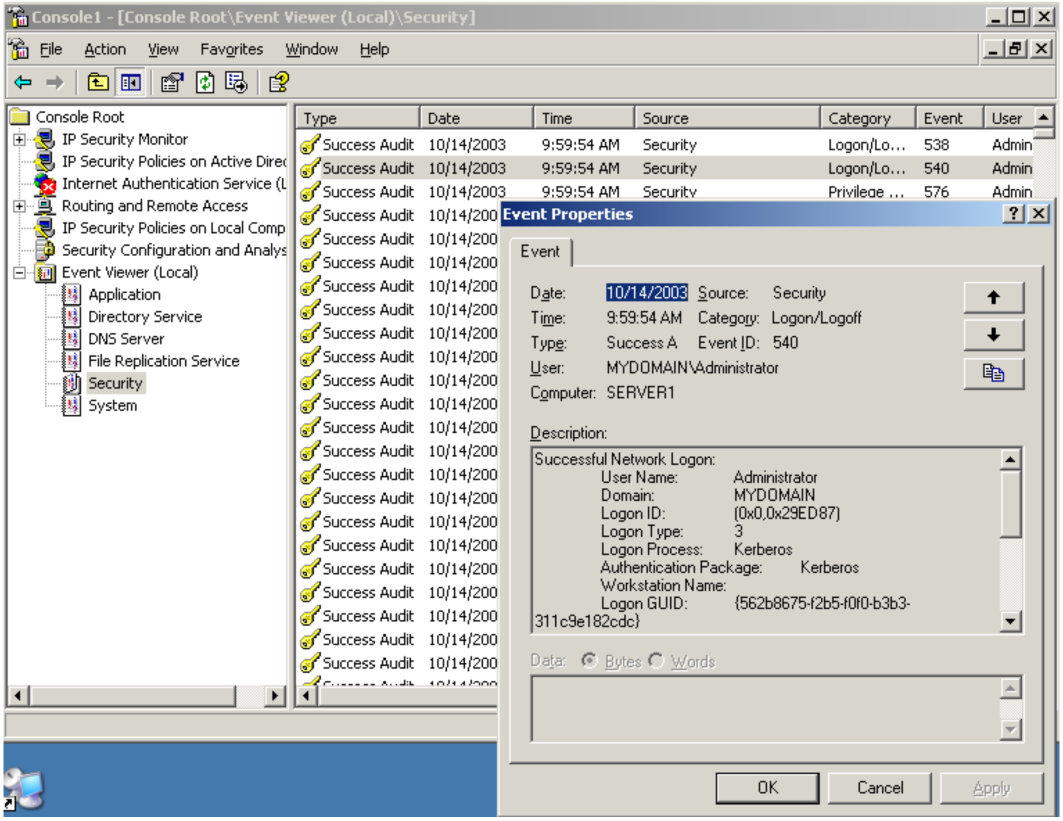
Kerberos Support Tools

Kerberos is the authentication protocol used in a Windows 2000 and 2003 domain. **Kerberos** replaced **NTLM** as it is more secure and an industry standard.

Below is a list of ways that Kerberos authentication information can be monitored, along with a screen shot of each:

- The **Security Event log** in Event log viewer (you must first enable auditing of logon events)

  You can use this tool to see every logon and logoff to your domain. Kerberos will be used as the authentication protocol for this (by default) and you can open the details of each event to see the intricate Kerberos details, if you wish.


Console1 - [Console Root\Event Viewer (Local)\Security]
File
Action
View
Favorites
Window
Help
Console Root
IP Security Monitor
IP Security Policies on Active Direc
Internet Authentication Service (L
Routing and Remote Access
IP Security Policies on Local Comp
Security Configuration and Analys
Event Viewer (Local)
Application
Directory Service
DNS Server
File Replication Service
Security
System
Event Properties
Event
OK
Cancel
Apply

Type	Date	Time	Source	Category	Event	User
Success Audit	10/14/2003	9:59:54 AM	Security	Logon/Lo...	538	Admin
Success Audit	10/14/2003	9:59:54 AM	Security	Logon/Lo...	540	Admin
Success Audit	10/14/2003	9:59:54 AM	Security	Privilege ...	576	Admin
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					
Success Audit	10/14/200					

Date: 10/14/2003 Source: Security
Time: 9:59:54 AM Category: Logon/Logoff
Type: Success A Event ID: 540
User: MYDOMAIN\Administrator
Computer: SERVER1

Description:

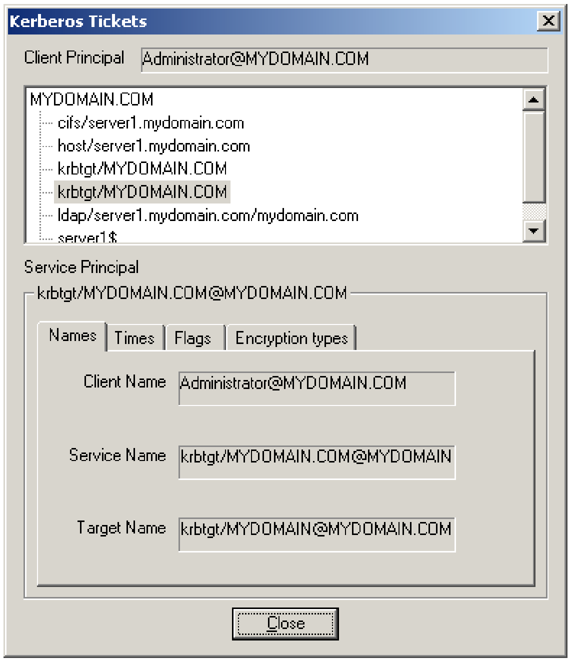
```
Successful Network Logon:
	User Name:		Administrator
	Domain:		MYDOMAIN
	Logon ID:		(0x0,0x29ED87)
	Logon Type:	3
	Logon Process:	Kerberos
	Authentication Package:	Kerberos
	Workstation Name:
	Logon GUID:	{562b8675-f2b5-f0f0-b3b3-
311c9e182cdc}
```

Data: ● Bytes ○ Words

Figure 38

- **Kerbtray.exe** from the Windows 2003 Server Resource Kit

  Kerbtray will run in your system tray. When you bring it up, it will report to you a considerable amount of Kerberos information.



Client Principal Administrator@MYDOMAIN.COM

MYDOMAIN.COM
cifs/server1.mydomain.com
host/server1.mydomain.com
krbtgt/MYDOMAIN.COM
krbtgt/MYDOMAIN.COM
ldap/server1.mydomain.com/mydomain.com
server1$

Service Principal
krbtgt/MYDOMAIN.COM@MYDOMAIN.COM

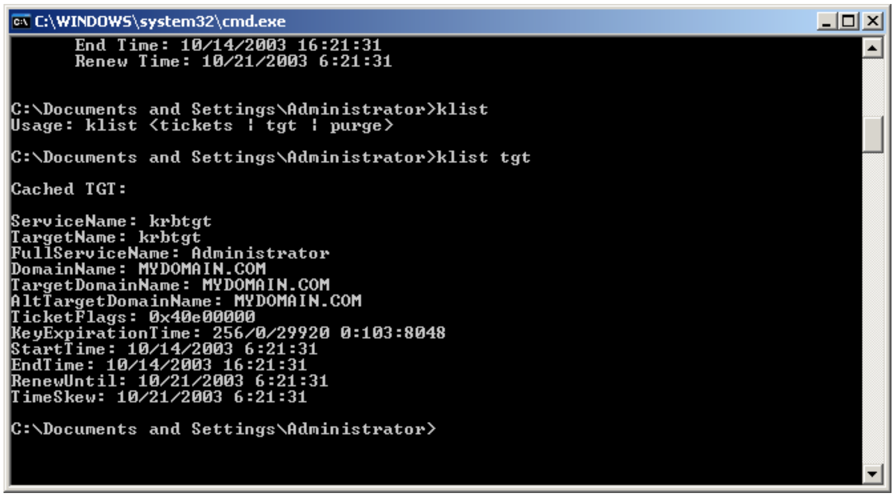
Client Name Administrator@MYDOMAIN.COM

Service Name krbtgt/MYDOMAIN.COM@MYDOMAIN

Target Name krbtgt/MYDOMAIN@MYDOMAIN.COM

- **Kerblist.exe** from the Windows 2003 Server Resource Kit

  This is a command line utility that can be used to gather similar information that kerbtray reports.

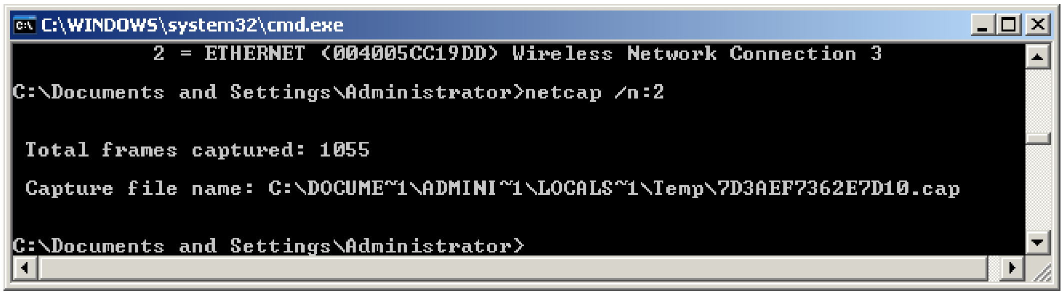


```
      End Time: 10/14/2003 16:21:31
      Renew Time: 10/21/2003 6:21:31


C:\Documents and Settings\Administrator>klist
Usage: klist <tickets | tgt | purge>

C:\Documents and Settings\Administrator>klist tgt

Cached TGT:

ServiceName: krbtgt
TargetName: krbtgt
FullServiceName: Administrator
DomainName: MYDOMAIN.COM
TargetDomainName: MYDOMAIN.COM
AltTargetDomainName: MYDOMAIN.COM
TicketFlags: 0x40e00000
KeyExpirationTime: 256/0/29920 0:103:8048
StartTime: 10/14/2003 6:21:31
EndTime: 10/14/2003 16:21:31
RenewUntil: 10/21/2003 6:21:31
TimeSkew: 10/21/2003 6:21:31

C:\Documents and Settings\Administrator>
```

Figure 39

- **Network Monitor** or **Netcap.exe**

  Network Monitor is the graphical tool that can capture and analyze captured network data. Netcap.exe is a new tool that comes with the Windows 2003 Support tools. Netcap.exe is a command line tool that only captures network data. This data can be analyzed with Network Monitor later. Netcap.exe can be run on Windows XP machines that do not have Network Monitor installed and netcap.exe data can then be moved to a machine with Network Monitor for analysis. Below is a screen shot of capturing data with netcap.exe. As you can see, it is very simple:



```
           2 = ETHERNET (004005CC19DD) Wireless Network Connection 3

C:\Documents and Settings\Administrator>netcap /n:2

 Total frames captured: 1055

 Capture file name: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\7D3AEF7362E7D10.cap

C:\Documents and Settings\Administrator>
```

Figure 40

By default, running netcap.exe results in it running until the 1MB buffer is full and placing the file in your temp directory with a .cap extension. However, this behavior can be modified.

Troubleshoot network protocol security. Tools might include the IP Security Monitor MMC snap-in, Event Viewer, and Network Monitor

Troubleshooting IP Security can be tricky. IPSec is a complex protocol that is designed so that hackers cannot get information about it. As a network administrator, you have some additional privileges (like access to tools on each of the systems that are attempting to communicate) that a hacker does not have. However, troubleshooting IPSec and its policies is generally complex. Here are some pointers to keep in mind when troubleshooting IP Sec:

- **Troubleshooting Methodology** - In troubleshooting, you should always have a logical, scientific process that you follow to solve the problem. "Trial and Error" may be needed to solve some problems, but it must be done methodically and scientifically, not haphazardly. Some good troubleshooting habits include creating a plan, making only one change at a time, and documenting the results.
- **IP Security Policies** - Incorrect or mismatched IP Security Policies are almost always the problem when faced with an IP Security issue. IP Security Monitor can be used to compare policies on each side of the connection and is thus a handy troubleshooting technique.

  Three IP Security policies are included, by default, with Windows 2003 Server. They are:

- Client (Respond Only) – Contains only the default response rule. Respond only means that a system with this policy only uses IP Security when the remote system requests it.
- Server (Request Security) – Contains the default response rule (mentioned above) and the unencrypted initial incoming communication rule (negotiate). With this second rule, the server negotiates IP Security on the incoming connections. Clients that do not support IP Security will be allowed to be communicated with.
- Secure Server (Require Security) - Contains the default response rule (mentioned above) and the unencrypted initial incoming communication rule (require). With this second rule, the server REQUIRES IP Security on the incoming connections. Clients that do not support IP Security will NOT be allowed to be communicated with.

These policies, as well as your own custom policies, can be assigned either on the domain level (through GPO), at the OU level (through GPO), or on the local system (a local policy). Microsoft's guide to deploying IP Security can provide additional information on this topic.

- **IP Security Monitor Statistics** - With IP Security Monitor, you can also compare statistics on each side of the connection. This could be useful to see exactly what types of IPSec failures are occurring and if they are in main mode or quick mode.
- **Event Logging** - The Event Viewer Security log can be used to troubleshoot IP Security issues. However, you may want to increase the auditing level to its maximum. This can be done with netsh.

The following book was referenced in the creation of this section:
Windows Server 2003 Network Infrastructure by JC Mackin and Ian McLean

Implementing, Managing, and Maintaining Routing and Remote Access

With the proliferation of Internet access anytime and anywhere, the demand for remote access to company data has gone from just a couple executives and the Information Technology department to many employees at most organizations. Because of this, the proper implementation, management, and maintenance of remote access is more important than ever before. This applies especially for this exam!

Configure Routing and Remote Access user authentication

Windows 2003 can be used for more networking uses than ever before: a dialup remote access server, VPN server, or router.

To configure any of these services, you must have first installed "routing and remote access" (**RRAS**) as a role for your server. Assuming you have already done this, let's move on to how to configure its authentication protocols.

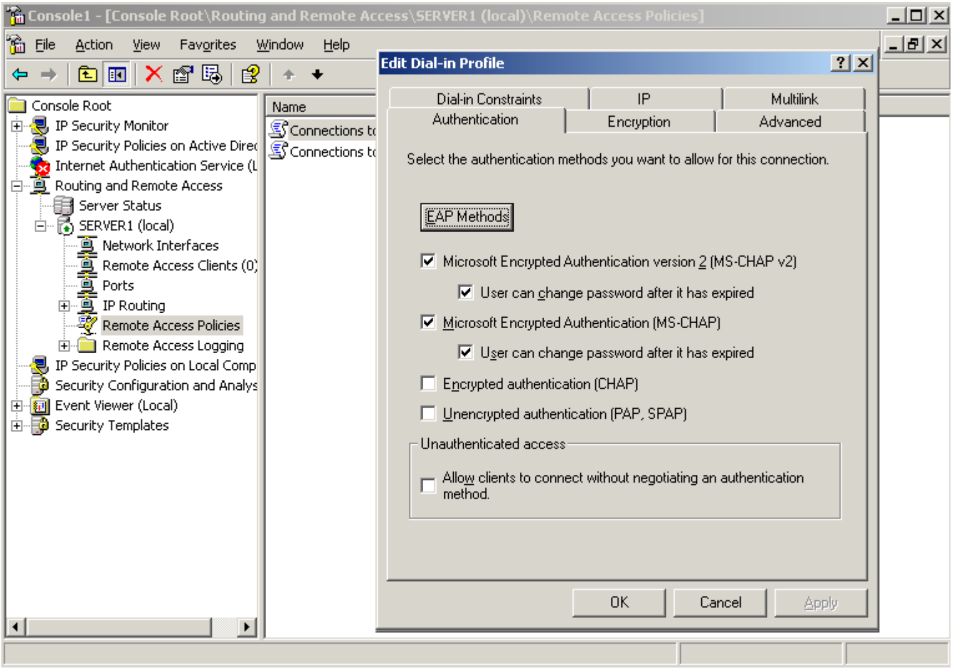
Configure remote access authentication protocols

If someone or something is connecting to your server or network from some outside source, you want to know who they are and make sure that they are really who they say they are. To do these things, you need an authentication protocol.

Windows 2003 Server supports the following authentication methods (from least secure to most secure):

- **No authentication** – A possible option where there is no authentication required for access.
- **PAP** (Password Authentication Protocol) – An unencrypted method which does not allow for data encryption.
- **SPAP** (Shiva PAP) – An inadequately encrypted method used with Shiva equipment that does not allow for data encryption.
- **CHAP** (Challenge-Handshake Authentication Protocol) – Uses the MD5 hash and does not send the password over the line. It's a standard that will work with non-Windows clients but does not allow for data encryption.
- **EAP MD5-CHAP** – CHAP using EAP. This allows for credential encryption but not data encryption.
- **MS-CHAP V1** – Provides one-way authentication that supports data encryption.
- **MS-CHAP V2** – Provides a two-way authentication that supports data encryption. This is the default on Windows 200, XP, and 2003.
- **EAP** with **TLS** (transport layer security) – Uses certificates for authentication and is commonly used with smart cards. It supports encryption of authentication and transport data. Servers using this method must be members of the Windows AD.

These different authentication methods are selected from the Routing & Remote Access -> Remote Access Policies folder by double-clicking a policy, then selecting to edit that policy's settings, and finally going to the Authentication tab for the policy.



Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☑ User can change password after it has expired

□ Encrypted authentication (CHAP)

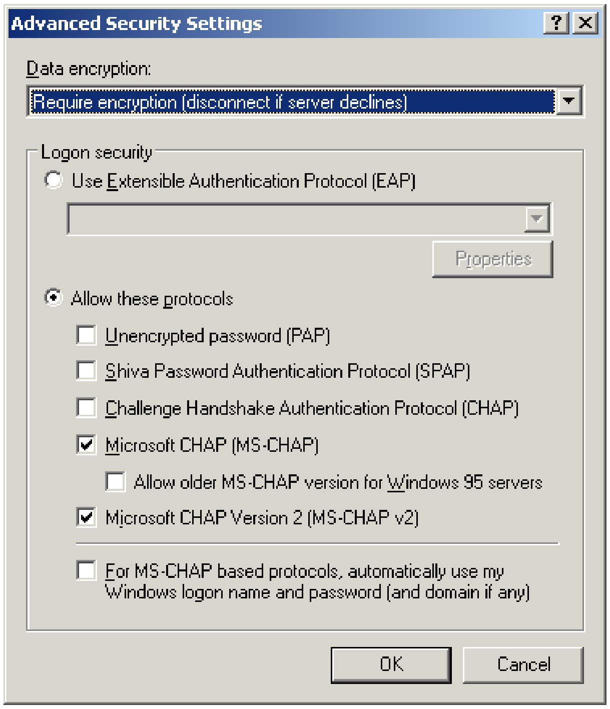
□ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

Figure 41

On the client connecting to the Windows RRAS server, you would configure your connection's authentication methods by going to the connection's properties, the security tab, and selecting advanced (custom) settings. From this point, you would see the window below:



Advanced Security Settings

Data encryption: Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP (MS-CHAP)

□ Allow older MS-CHAP version for Windows 95 servers

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

Figure 42

As you can see, here is where you would manually select the authentication method that you wish to use (from the client side).

Configure Internet Authentication Service (IAS) to provide authentication for Routing and Remote Access clients

RADIUS (Remote Authentication Dial-In User Service) is an industry standard authentication protocol used in larger organizations with multiple network access servers. RADIUS allows an organization to have a central database of usernames and passwords. Besides authentication, RADIUS can also perform authorization and accounting (logging). The great thing about Microsoft's **IAS** is that it uses the Windows Active Directory as its username and password database. That way, Windows users can use the same username and password for remote access as they do when they login to their PC while they are in the office.

To use IAS as a RADIUS server for authorization with Routing and Remote Access, you must configure both IAS and RRAS. Here is how to do it:

- Configure RRAS

Right-click on your RRAS server and select properties within its MMC. Select the Security tab. Change the authentication provider from Windows authentication to RADIUS authentication.

Next, specify the RADIUS server that will be used with RADIUS authentication. To do this, click configure, and then add. You will need to know the RADIUS server name or IP, its secret password, and port number. If you wish to use IAS for accounting (logging) of authentication data as well, perform the same steps on the Accounting provider menu of the RRAS server properties, Security tab.

- Configure IAS

To configure the IAS server to provide authentication for the RRAS server, bring up the IAS MMC. Like a DHCP server, the IAS server musts be registered in the Windows AD. To do this, right click on the server and select Register Server in Active Directory.

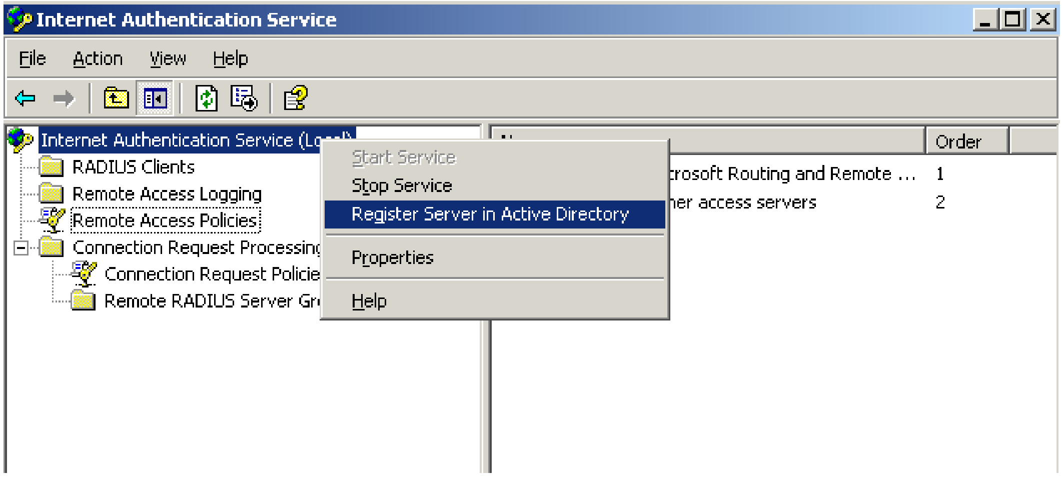

Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Connection Request Policie
Remote RADIUS Server Gr
Start Service
Stop Service
Register Server in Active Directory
Properties
Help
Order
rosoft Routing and Remote ... 1
er access servers 2

Figure 43

Next, you must tell the IAS server who is authorized to be a client that it will provide authentication services to. To do this, right-click the RADIUS Clients folder (seen above) and select New RADIUS Client. You will be prompted for the friendly name, IP address or domain name, type of network access server (NAS), and secret password. The type of access server, in our case for RRAS, would be Microsoft. At this point, you have done what you need to do for the Routing and Remote Access server to use the IAS server for authentication. By default, the IAS (RADIUS) server will use Windows authentication as the credentials to determine if authentication is successful.

Configure Routing and Remote Access policies to permit or deny access

Remote access policies are what determines what users or machines gain access, through what method, when, and what restrictions are put on them once they have access.

By default, there are two policies created. One controls access to the remote access server itself. The other controls access to network resources outside of the remote access server.

You can create your own policies to control access. To do this, right-click on remote access policies and select "New Remote Access Policy". From here, you will be asked if you want to use the wizard to guide you through policy creation or you can choose to create a custom policy.

If you use the wizard, it will guide you through the process of creating the new policy. You will be asked questions like what service this is for (VPN, Ethernet, dial-up, wireless, etc.), is this for a group or individual users, authentication protocols to be used, encryption methods to be used, and other settings, based on the type of remote connection you are configuring.

If you choose to create a custom policy, you will be asked to select the user or group that the policy applies to. Then, you will be prompted to create "conditions." **Conditions** determine when the policy is applied. For example, a policy might apply only to the group "HR-users" and it could be set up to assign them a different default gateway.

Manage remote access

If you are going to allow remote access to your network, you will want to configure this properly and be knowledgeable about what is going on. That is what this section is all about.

Manage packet filters

If you are going to allow remote access to your network, you want to allow the users the access that they require and nothing more (recall the principle of least privilege). Remote access packet filters are used to do this.

To set up **filters**, go to the properties of whatever policy applies. Under the IP tab of the policy configuration, there are two buttons: input filters and output filters. Using these options you can filter the packets that enter your remote access server (and, most likely, its network) through this remote access connection or packets that exit.

From here, you can select to "permit only the packet below" or "deny only the packets below". The more difficult option is specifying the source and destination IP addresses, ports, and protocols.

Manage Routing and Remote Access routing interfaces

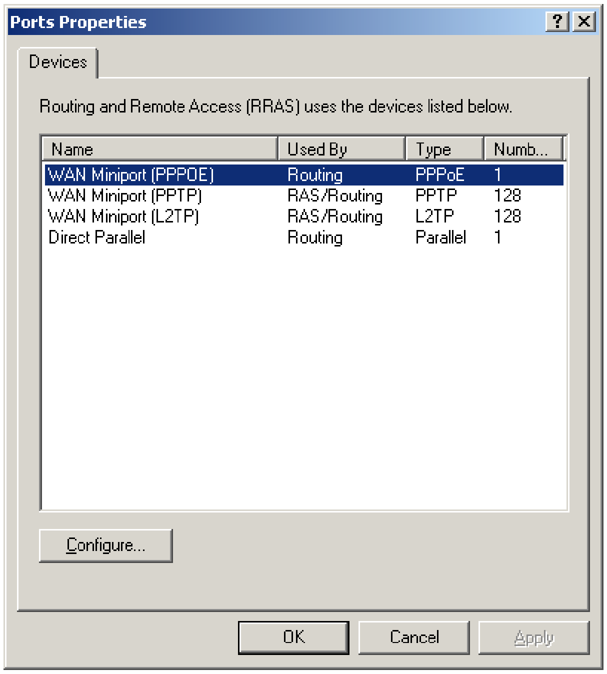
Within RRAS there are three types of network interfaces. They are:

- **Private Interface** – A network adaptor connected to a private network. These should be configured within the private IP address range (discussed earlier in this document).
- **Public Interface** – A network adaptor that is connected to a public network. This is almost always the public Internet. If you want to have private IP addressing on your internal network and public addressing on your public interface, you may want to use **NAT** (Network Address Translation). As this type of interface is connected to a public network, this is the type of interface where you face the greatest security risks.
- **Demand-dial Interface** – These are special interfaces that connect other routers. These interfaces can be **static** (always up) or **dynamic** connections (up only when needed). These interfaces may use private or public IP addressing.

Each of these interfaces has its own addressing, packet filtering, authentication, and encryption configurations. You can view these interfaces from the RRAS MMC, under "Network Interfaces".

Manage devices and ports

Remote access ports are created based on the type of remote access you are providing. If you right-click on Ports under your RRAS server, you will get the following window:



Routing and Remote Access (RRAS) uses the devices listed below.

Name	Used By	Type	Numb...
WAN Miniport (PPPOE)	Routing	PPPoE	1
WAN Miniport (PPTP)	RAS/Routing	PPTP	128
WAN Miniport (L2TP)	RAS/Routing	L2TP	128
Direct Parallel	Routing	Parallel	1

Figure 44

As you can see, there are four types of devices that the RRAS server can use:

- Point to Point Protocol over Ethernet (**PPPoE**)
- Point to Point Tunneling Protocol (**PPTP**)
- Layer 2 Tunneling Protocol (**L2TP**)
- Parallel

From here, you can configure the maximum number of ports for each and whether they will be for inbound or outbound use. By going into the Ports window, you will see every device that is configured and its status. At this point, you can check the statistics on each of the devices (for example: see active VPN connections and their packets sent/received) and disconnect connections.

Manage routing protocols

This is discussed more in the "Manage TCP/IP Routing" section, below.

Manage Routing and Remote Access clients

Once clients are connected to your remote access server, you may want to see who is on, send messages to them while they are on, or disconnect them. To do this, go to the RRAS MMC snap-in, navigate to your RRAS server, then to Remote Access Clients. Once you click on Remote Access Clients, you can see who is on (their username) and how long they have been on.

To send them a message or disconnect them, you can right click the user and select either "send message" or "disconnect."

Manage TCP/IP routing

Just like a hardware-based Cisco® router, a Windows 2003 Server can be used as a fully functioning software-based router. Windows 2003 support **static routing** and **dynamic routing** with Open Shortest Path First (**OSPF** – link state type of routing) and Routing Information Protocol (**RIP Version 2** – distance vector type of routing). One advantage that a hardware-based router usually has over a Windows router is the number and types of interfaces offered. A Windows router is limited by its number of network cards, and other interfaces, that may be installed.

Before you can use Windows 2003 Server as a router, you must enable Routing and Remote Access. All of the routing functions in Windows may be configured with the RRAS MMC snap-in.

Manage routing protocols

Static routing is a very useful method of configuring IP routing. Static routing means that the paths that a packet may take are "hard-coded" on the router. That means that someone must manually enter these routes. Also, although these routes may be entered, they may not be functioning or may not be valid routes. Static routing works great for a small network but is too difficult to maintain on a large network. **Dynamic** routing, on the other hand, means that routes are automatically "learned" from other routers. Routers communicate and send routes that they can offer to their neighbor. Depending on the routing protocol, the router may only send the best routes or it may send ALL routes to its neighbor. Compared to static routing, dynamic routing is more useful on a larger network.

Windows 2003 Server supports two dynamic routing protocols. They are:

- RIP V2
- OSPF

RIP V2
RIP is best for a small or medium size network as a RIP network cannot exceed 15 hops, from one side to the other. RIP sends the entire routing table to its neighbor in every routing update.
Pros:

- Simple to use.
- Well known.
- RIP V2 supports simple text authentication and multicast router announcements.
- RIP V2 supports classless networks and variable length subnet masks, as the subnet mask is included in the routing update.
- RIP uses **hold-downs**, **split horizons**, and **poison reverse** updates in order to attempt to reduce the possibility of a loop in the network.

Cons:

- 15 hop limitation.
- Only uses hops from one router to the next to measure the distance over the link. RIP does not take into account the speed of the link, latency of the link, or cost of the link.
- In larger networks, RIP can take too long to converge (where all routers have the same view of the network).
- It provides no encrypted authentication of routing updates.

To learn more about RIP V2, read about it both in the Windows 2003 help pages and at this Internet link: RFC 2453.

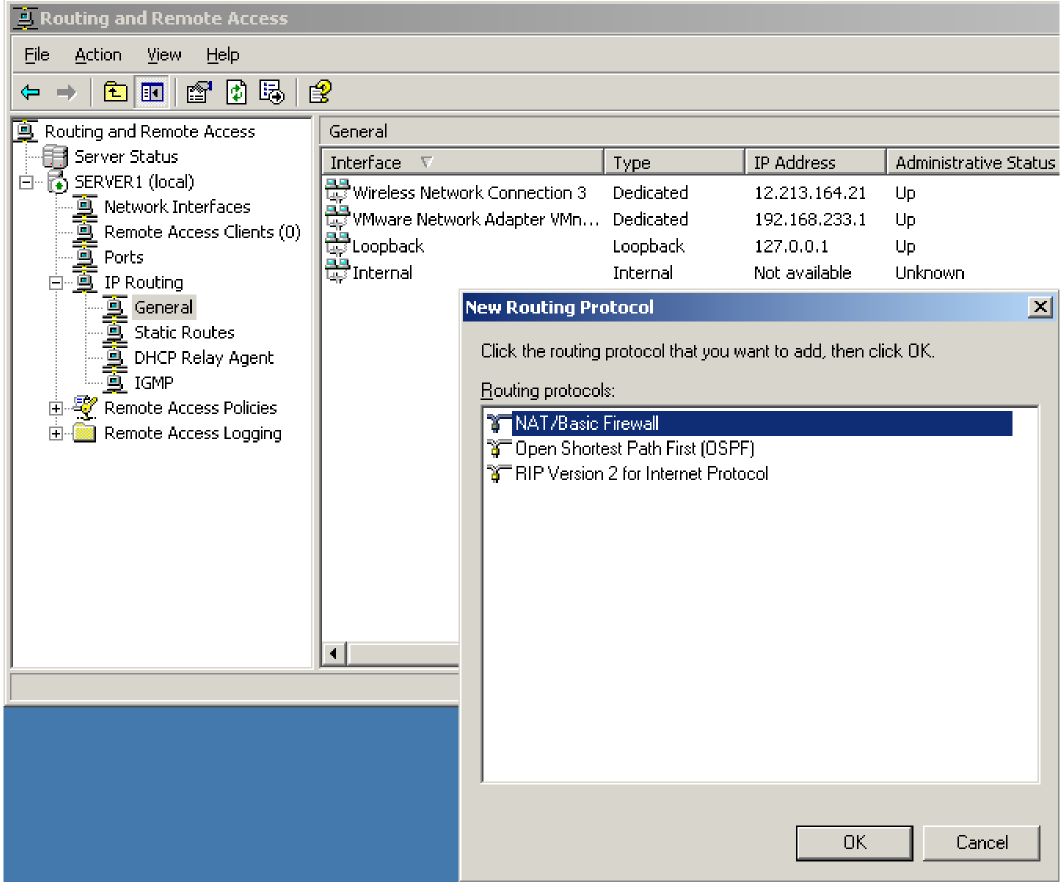
OSPF
OSPF is designed for very large networks and is an efficient protocol for this type of need. OSPF routing tables will never contain loops. OSPF runs the Shortest Path First (SPF) algorithm on each router to compute the best path. Only the best paths are placed into the routing table. With large routing tables, running the SPF algorithm can be CPU intensive. Once the entire routing table has been exchanged between routers, only changes are sent after that, thus supplying efficiency.
Pros:

- Best for large networks.
- Loop free.
- Efficient.
- Uses less network bandwidth with large routing tables as only the changes are sent after the initial exchange.
- Fast convergence.

Cons:

- Complex to administer.
- CPU and memory intensive with large routing tables or many routing table changes.
- No encrypted authentication of routing updates, uses simple text authentication.

To configure either of these routing protocols, use the RRAS MMC snap-in. To install either RIPV2, OSPF, or NAT, you must go to the IP Routing folder and right-click on the General sub-folder. From here, you will see "New Routing Protocol".



Interface	Type	IP Address	Administrative Status
Wireless Network Connection 3	Dedicated	12.213.164.21	Up
VMware Network Adapter VMn...	Dedicated	192.168.233.1	Up
Loopback	Loopback	127.0.0.1	Up
Internal	Internal	Not available	Unknown

Click the routing protocol that you want to add, then click OK.

Routing protocols:

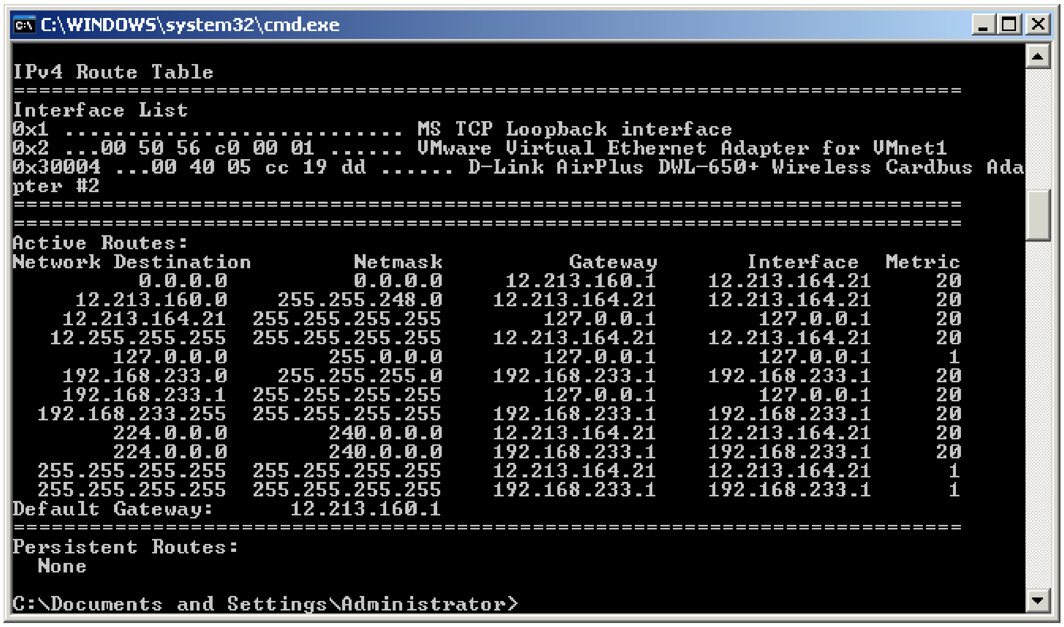
- NAT/Basic Firewall
- Open Shortest Path First (OSPF)
- RIP Version 2 for Internet Protocol

Figure 45

Say that you select OSPF, you will have a new sub-folder called OSPF under the IP Routing folder. To configure OSPF on an interface, you must then right-click on OSPF and select "New Interface." Configuration of OSPF is complex. OSPF is very configurable. OSPF uses the concept of areas to defines areas of management domains. There are different types of areas, such as stub areas. There are different network types, such as point-to-point, non-broadcast, or broadcast. To learn more about OSPF, read up on its configuration both on the Windows 2003 help documents and at this Internet link: RFC 2328.

Manage routing tables

Every IP device has its own routing table. This routing table is used to determine what gateway/next hop to use to send any packet to that is not on its local network. You can view the routing table on a Windows 2003 machine from the command line by running "route print". The output looks like this:



```
IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 01 ...... VMware Virtual Ethernet Adapter for VMnet1
0x30004 ...00 40 05 cc 19 dd ...... D-Link AirPlus DWL-650+ Wireless Cardbus Ada
pter #2
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     12.213.160.1    12.213.164.21     20
     12.213.160.0    255.255.248.0    12.213.164.21    12.213.164.21     20
    12.213.164.21  255.255.255.255        127.0.0.1        127.0.0.1     20
   12.255.255.255  255.255.255.255    12.213.164.21    12.213.164.21     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
    192.168.233.0    255.255.255.0    192.168.233.1    192.168.233.1     20
    192.168.233.1  255.255.255.255        127.0.0.1        127.0.0.1     20
  192.168.233.255  255.255.255.255    192.168.233.1    192.168.233.1     20
        224.0.0.0        240.0.0.0    12.213.164.21    12.213.164.21     20
        224.0.0.0        240.0.0.0    192.168.233.1    192.168.233.1     20
  255.255.255.255  255.255.255.255    12.213.164.21    12.213.164.21      1
  255.255.255.255  255.255.255.255    192.168.233.1    192.168.233.1      1
Default Gateway:      12.213.160.1
===========================================================================
Persistent Routes:
  None

C:\Documents and Settings\Administrator>
```

Figure 46

You can see that the basic concept of the routing table falls into five columns:

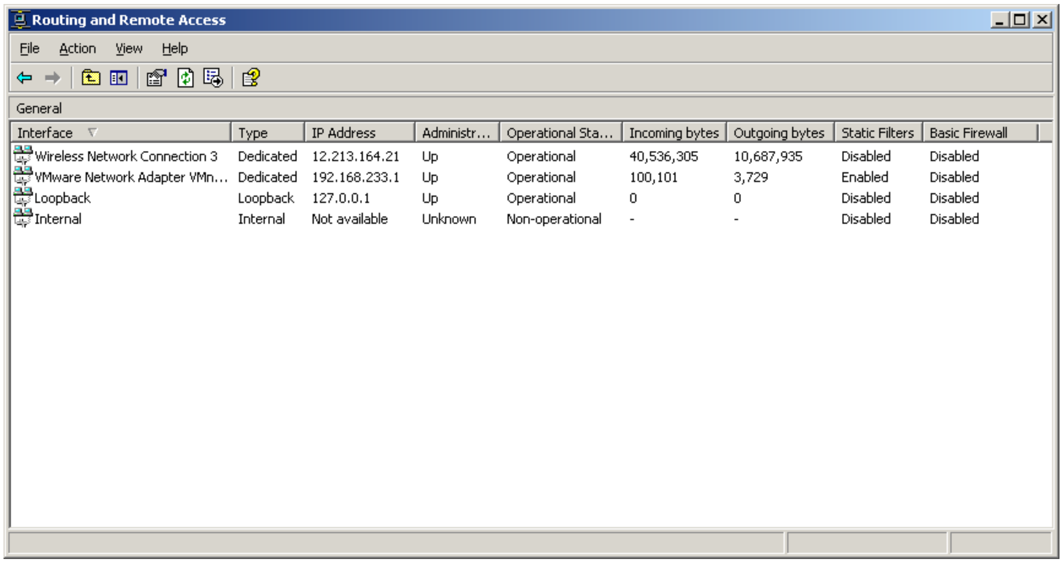
- **Destination** – The destination network address for that routing entry.
- **Netmask** – The subnet mask for the network destination. You'll notice that the sixth network down is 192.168.233.0 and the network mask is 255.255.255.0. This means that any traffic for the IP address 192.168.233.1 through 192.168.233.255 should be sent to the gateway in this network entry.
- **Gateway** – The router that will deliver the packet for the network entry. This is the router that your system will send the packet, not destined for your network, to. For the 192.168.233.0 network entry we just talked about, the gateway is 192.168.233.1.
- **Interface** – This is the IP address of the interface, on your computer, that can access this gateway. Thus, in our example with 192.168.233.0, we send it out the interface with the IP address of 192.168.233.1.
- **Metric** – This is a number that represents which of these routes should be used first. In our example above, most of them have the same metric. However, it is likely that you will run into two network routes that go to different places and have different metrics. In that case, the one with the lowest metric would be used first. If that route was not working, the entry with the next higher metric would be used next.

You can use the **route command** to add, delete, or change routing table entries. Entries in the routing table may come from either static or dynamic (like RIP and OSPF) protocols.

The routing protocol can also be viewed and modified through the MMC snap-in for Routing and Remote Access, under "IP Routing" and "Static Routes".

Manage routing ports

To see what your possible routing interfaces are, and their status, you can either use the "route print" command (as seen above) or the RRAS MMC snap-in. To use the MMC snap-in, go to IP Routing and click on General. You will see a window similar to the one below:



Interface	Type	IP Address	Administr...	Operational Sta...	Incoming bytes	Outgoing bytes	Static Filters	Basic Firewall
Wireless Network Connection 3	Dedicated	12.213.164.21	Up	Operational	40,536,305	10,687,935	Disabled	Disabled
VMware Network Adapter VMn...	Dedicated	192.168.233.1	Up	Operational	100,101	3,729	Enabled	Disabled
Loopback	Loopback	127.0.0.1	Up	Operational	0	0	Disabled	Disabled
Internal	Internal	Not available	Unknown	Non-operational	-	-	Disabled	Disabled

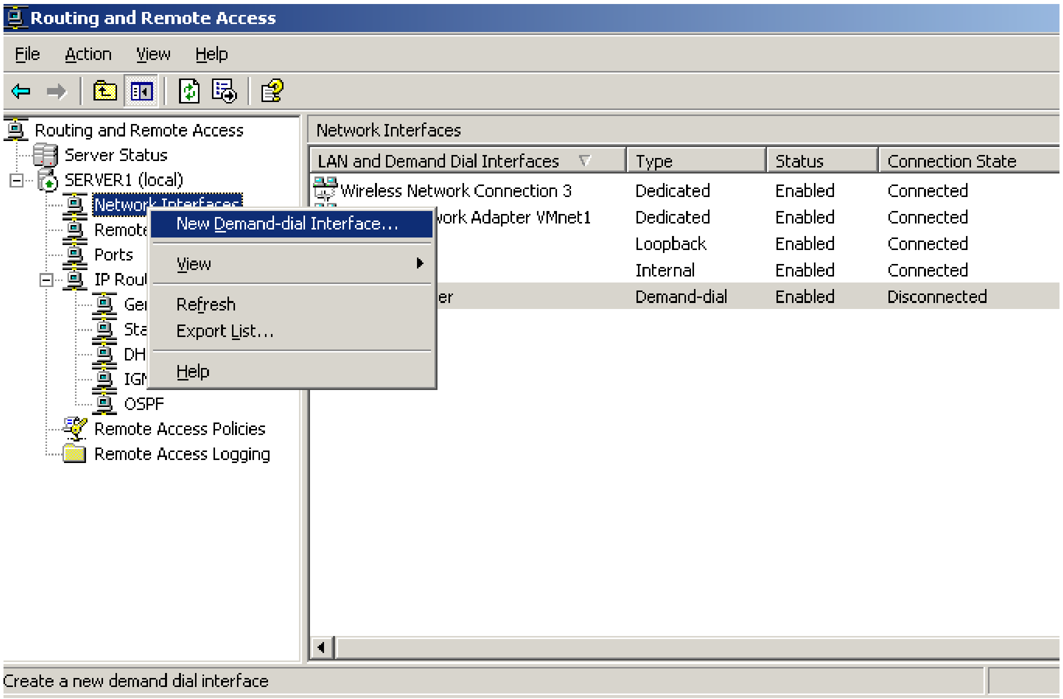
Figure 47

From here, you can see your possible routing interfaces, type of interface, IP address, status, statistics, filters enabled, and firewall status.

Implement secure access between private networks

A very practical trend today is the connection of private networks, over the Internet, through a VPN tunnel. You should be able to configure two Windows 2003 Servers, with RRAS, so that they can securely connect to one another over a public network. To do this, you should be familiar with authentication, encryption, and IPSec.

Whether this connection is over a dialup modem or over the Internet, you will need to create a new "Demand-dial interface." This concept can be confusing for someone attempting to configure a **VPN** tunnel, as there is really no "dialing". To create one, right-click on the network interfaces of your R&RA server and select "New Demand Dial Interface". (Seen below.)



LAN and Demand Dial Interfaces	Type	Status	Connection State
Wireless Network Connection 3	Dedicated	Enabled	Connected
ork Adapter VMnet1	Dedicated	Enabled	Connected
	Loopback	Enabled	Connected
	Internal	Enabled	Connected
er	Demand-dial	Enabled	Disconnected

Create a new demand dial interface

Figure 48

Once inside this window, you will be asked the name of the connection, IP address, type of encryption used (**L2TP or PPTP**), static routing information, and finally a username/password/domain combo for authentication to the remote server. Of course, you are going to have to do this on the remote system as well. These connections may either be permanent or demand connections that come up only when there is traffic to be passed.

Wireless

A new feature of Windows Server 2003 is support for IEEE 802.1x wireless access points and switches. The Internet Authentication Service (IAS) will provide authentication, authorization, and accounting (AAA) for these devices. With 802.1x, clients must provide authentication credentials before their wireless access point (WAP) or switch port allows the device to send data onto the network. The IAS server authenticates the user information to allow the device (user) access to the network. Keep in mind that these wireless access points and switches must support RADIUS and 802.1x. Additionally, the wireless AP must support wired equivalent privacy (WEP) encryption.

802.1x uses the Extensible Authentication Protocol (EAP) for exchanging data during the authentication process. However, you must still use another authentication method to authenticate the wireless connection. You can choose from any of the following three methods:

- EAP Transport-Level Security (TLS) – Uses certificates on the server side and either smart cards or certificates on the client.
- Protected EAP (PEAP) with EAP-Microsoft-CHAP (EAP-MS-CHAPv2) – Uses certificates on the server and username/password on the client.

- PEAP with EAP-TLS – Uses certificates for server authentication and either smart cards or certificates for client authentication.

The strongest of these is PEAP with EAP-TLS.

The easiest of these to deploy is PEAP with EAP-MS-CHAPv2.

Troubleshoot user access to remote access services

Undoubtedly, once you have your users connected via remote access they will, at some point, have trouble. Microsoft knows that these issues are typical and wants you to be prepared for it. I am sure that this is why they made this a test topic. For each of these three test topics, successfully troubleshooting these issues will only be done by combining all the skills you have obtained in other sections of this manual, other books you may have read, and hands-on experience you accumulate.

Diagnose and resolve issues related to remote access VPNs

Some of the many issues that could be causing trouble with remote access **VPNs** are (this list was taken from the Microsoft Windows 2003 Troubleshooting Documentation):

- Invalid username/password/domain credentials being used for the remote access attempt.
- Expired account being used for remote access attempt.
- RRAS service is not running on remote access server.
- Remote access has not been enabled or configured on the remote access server.
- PPTP or L2TP ports are not enabled on the RRAS server.
- LAN Protocols do not match between the server and client (TCP/IP, IPX, NETBIOS, AppleTalk, etc.).
- All PPTP or L2TP WAN ports on the remote access server are already used (by default, there are 5 of each).
- Authentication methods do not match.
- The user being used for remote access does not have dial-up permissions (VPN remote access permissions).
- There are not enough IP addresses in the remote access server pool for the client connection being attempted.
- The remote access server cannot access the Windows AD and AD is being used for authentication.
- The remote access server cannot access the RADIUS server and RADIUS is being used for authentication.
- The remote client’s modem is not configured properly (if using dialup access or Internet dialup to VPN). In other words, if the remote VPN client that is attempting to connect to your RAS server is connecting to the Internet via a dial up modem and experiencing trouble, the trouble may be caused by the remote client’s modem not being configured properly or just not connecting at all. In this case, you would want to double check the remote client’s modem configuration settings, verify that the modem can connect to the Internet provider, that the modem gets the proper IP address information, and that it can send and receive data.
- The remote client’s Internet provider or connection is not working properly. This could be tested by the client attempting to ping the remote access server (assuming the server’s firewall allows ICMP in).

Diagnose and resolve issues related to establishing a remote access connection

Issues that could be causing trouble with remote access connections include all of the above except the VPN policy issues. Also, additional possible can stem from issues with the dial-up modem and modem configuration.

Diagnose and resolve user access to resources beyond the remote access server

Some of the many issues that could be causing a remote user to not be able to access resources beyond the remote access server are (this list was taken from the Microsoft Windows 2003 Troubleshooting Documentation):

- IP Routing not enabled on the RRAS server.
- A static IP address pool is configured on the RRAS server but there are no routes back to the remote access clients from the servers (resources) on the network that is trying to be accessed.
- Packet filters prevent traffic from flowing from the remote access client beyond the remote access server network and/or packet filters prevent the servers/resources on the remote access server network from sending traffic back to the remote access clients.

Troubleshoot Routing and Remote Access routing

Troubleshooting any technology is difficult to learn from solely reading about it. This is because troubleshooting is very fluid. Because real-world networks are usually more complex than theoretical networks and often develop problems that one doesn't foresee, real-world troubleshooting is also usually more complex. Thus, I highly recommend that you create a test network to hone your troubleshooting skills.

Troubleshoot demand-dial routing

As you probably know, demand-dial routing doesn't necessarily have to do with dial-up networking or modems. Demand-dial routing simply means that the connection between the two networks is dynamic and not connected all the time. Terminology of a demand-dial network deals with the "calling" router and "called" router. This can also be confusing as you know that demand-dial connections may be periodic VPN connections over a permanent network (like the Internet).

If you are having trouble with your demand-dial connection, you should consider the following as possible causes of the trouble (this list taken from the Windows 2003 Server help documentation):

- If the on-demand connection is not made automatically, you should look at the following possibilities:
    - IP routing not enabled.
    - Static routes not configured properly.
    - The checkbox to "use this route to initiate demand-dial connection" must be selected.
    - Dial-out hours prevent connection.
    - Demand-dial filters are preventing the dial-out.

- If you are unable to make the demand-dial connection, you should look at the following possibilities:
    - RRAS service is not running on the "called" router.
    - Demand dial interface is in an "unreachable" state.
    - LAN/WAN routing is not enabled on the "called" router.
    - Demand-dial connections for the protocols being used is not allowed.
    - Dial-up, PPTP, or L2TP ports are not enabled for demand-dial connections.
    - All ports are in use on the "called" routers.
    - The authentication credentials are invalid or have expired.
    - Dialup permission is not enabled for the user you are authenticating with.
    - Verify remote access policies and security policies.

    (Note: This list continues in the Windows 2003 Help documentation under "Troubleshooting demand-dial routing.")
- If you are unable to access resources beyond the called router, you should consider the possibilities listed above in the section titled, "Diagnose and resolve user access to resources beyond the remote access server."

Troubleshoot router-to-router VPNs

The difference between a demand-dial connection VPN and router-to-router VPN is that in a router-to-router VPN, each side can answer and initiate the connection. Also, in a router-to-router VPN, the successful connection of these routers depends on the successful authentication of the interfaces, not the authentication of a particular user.

Thus, the possible issues that would cause a router-to-router VPN not to connect are the same as the list of possibilities surrounding the demand-dial connection, above, with the difference being that the individual user issues would not be a problem but interface authorization would. Also, each side of the connection would need to be able to accept or initiate the connection. So, each side would need to have IP routing enabled, each side would need to be able access its authentication server (RADIUS or Windows AD), each side would have to have RRAS running, etc.

Maintaining a Network Infrastructure

Hopefully, most of your day to day duties as a network administrator are spent maintaining what you have already done your implementation and troubleshooting of. Daily maintenance is also very important in preventing future troubleshooting and downtime.

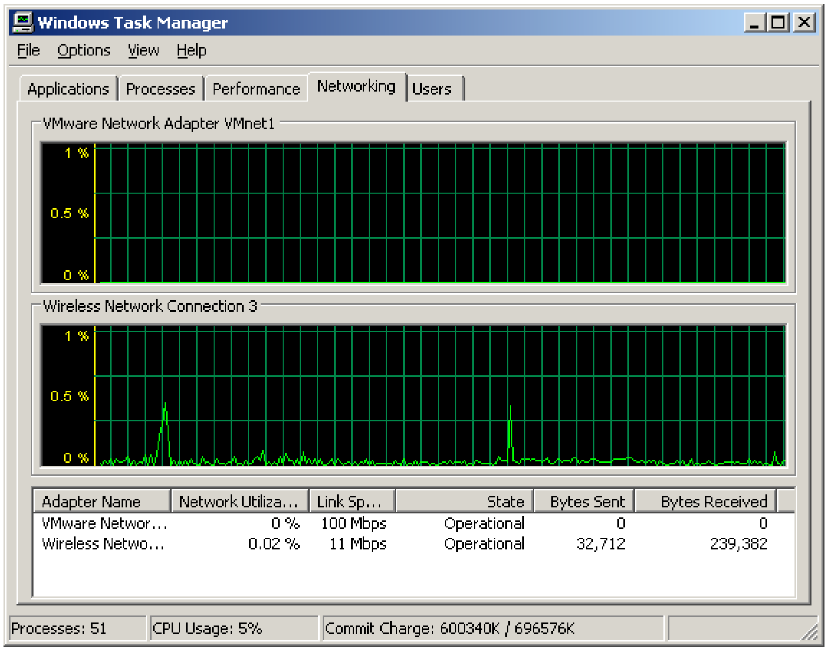
Monitor network traffic. Tools might include Network Monitor and System Monitor

To monitor network traffic in Windows 2003, you can use a variety of tools. These include:

- **Task Manager**
- **System Monitor**
- **Network Monitor** (netmon.exe)
- **Netstat**
- **Nbtstat**

Task Manager

Most Windows administrators are familiar with Windows Task Manager. The Windows 2003 version of it has five tabs: Applications, Processes, Performance, Networking, and Users. Of greatest interest for network monitoring is the Networking tab. With this tab, you not only see a graphical representation of your network adaptor utilization but you can also customize the columns so that they can show a wide variety of statistics about each adaptor.



Adapter Name	Network Utiliza...	Link Sp...	State	Bytes Sent	Bytes Received
VMware Networ...	0 %	100 Mbps	Operational	0	0
Wireless Netwo...	0.02 %	11 Mbps	Operational	32,712	239,382

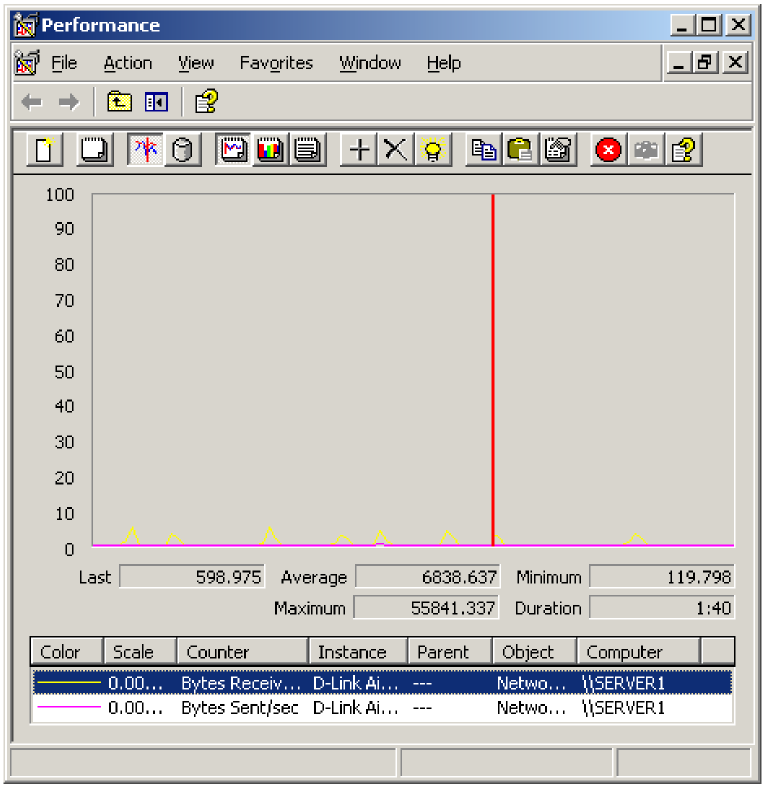
Processes: 51 CPU Usage: 5% Commit Charge: 600340K / 696576K

Figure 49

System Monitor (Performance Monitor / Console) – perfmon.exe

This tool was briefly covered in the section on DNS Server monitoring ("Monitor DNS. Tools might include System Monitor, …"). System Monitor can be used to monitor just about any facet of system performance: network, disk, CPU, memory, swap, and most every application or service. To uses it to monitor network performance, you can monitor TCP, UDP, IP, interface, or individual network applications or service statistics. Adding counters and viewing data in either a graphical, histogram, or text report format is essentially the same, no matter what you are monitoring. System Monitor can be used to send an alert if a monitored parameter exceeds thresholds. You can also send data to log files.

A sample screen shot of what it looks like to view network interface statistics of bytes sent and received is below:



Last 598.975 Average 6838.637 Minimum 119.798
Maximum 55841.337 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
───	0.00…	Bytes Receiv…	D-Link Ai…	---	Netwo…	\\SERVER1
───	0.00…	Bytes Sent/sec	D-Link Ai…	---	Netwo…	\\SERVER1

Figure 50

Network Monitor (netmon.exe)

Network Monitor is a packet analyzer. This tool will show you everything from summary statistics all the way down to the raw binary bits of each packet. With this tool, you can see real-time DHCP registrations, TCP/IP, DNS requests, RRAS, ARP requests, Web requests, Routing updates, etc.

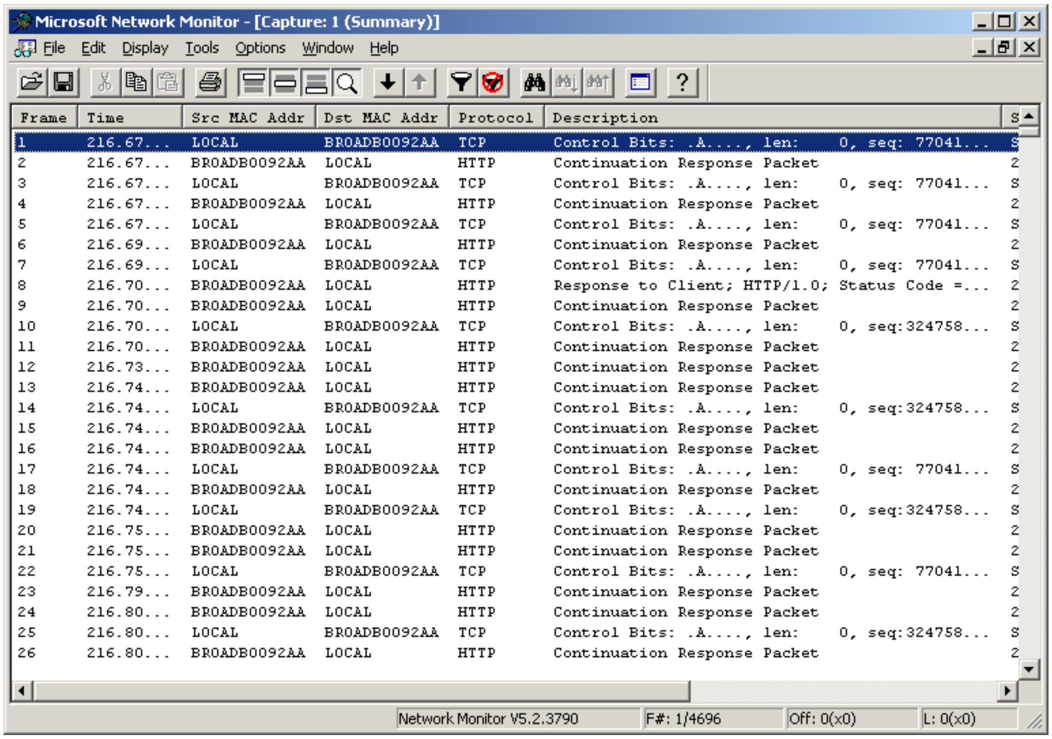
The idea is that it will show you summary data, but if you want to see more than that, you must initiate a "capture". This means that the program stores every packet that comes in or out of the system that it is running on. Once the data is captured, you can view this data, filter it, or store it for later.

The version of Network Monitor that comes with Windows Server will only capture packets to or from the system that it is running on. If you install the Windows SMS version of Network Monitor, it will run in promiscuous mode and be able to capture all traffic that comes across the wire to the system it is running on. There is a command line program called **netcap.exe** (discussed earlier in this manual) that can do command-line captures. The captured data can then be analyzed with the graphical Network Monitor.

To capture data with the graphical Network Monitor, once Network Monitor is installed, you simply open the program and click the "start capture" button. This button looks like a CD or DVD player "Play" button.

Alternatively, you can go up to the capture menu and click "Start". If you are using the command-line program, netcap.exe, and only have a single network adaptor, simply running it at the command line, with no parameters, will capture data until its buffer is full.

A sample of captured data with Network Monitor is shown below:



Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	S
1	216.67...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq: 77041...	S
2	216.67...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
3	216.67...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq: 77041...	S
4	216.67...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
5	216.67...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq: 77041...	S
6	216.69...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
7	216.69...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq: 77041...	S
8	216.70...	BROADB0092AA	LOCAL	HTTP	Response to Client; HTTP/1.0; Status Code =...	2
9	216.70...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
10	216.70...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq:324758...	S
11	216.70...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
12	216.73...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
13	216.74...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
14	216.74...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq:324758...	S
15	216.74...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
16	216.74...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
17	216.74...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq: 77041...	S
18	216.74...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
19	216.74...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq:324758...	S
20	216.75...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
21	216.75...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
22	216.75...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq: 77041...	S
23	216.79...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
24	216.80...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2
25	216.80...	LOCAL	BROADB0092AA	TCP	Control Bits: .A...., len: 0, seq:324758...	S
26	216.80...	BROADB0092AA	LOCAL	HTTP	Continuation Response Packet	2

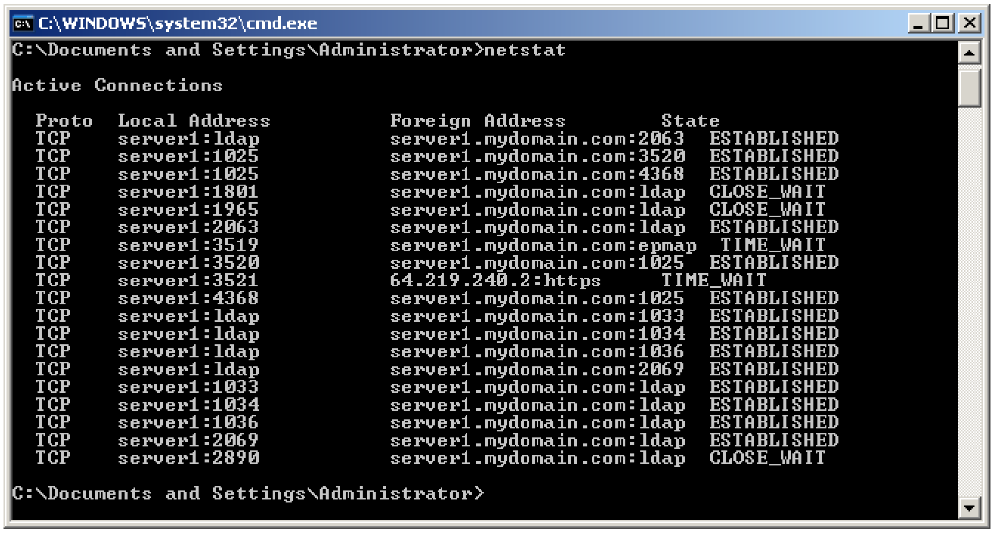
Network Monitor V5.2.3790 F#: 1/4696 Off: 0(x0) L: 0(x0)

Figure 51

Netstat

Netstat displays TCP/IP protocol statistics (like TCP, UDP, and others), open connections to your system, the routing table, and Ethernet statistics. Running netstat from a command prompt without any switches will result in a list of the active connections on your system.

An example of this output is below:

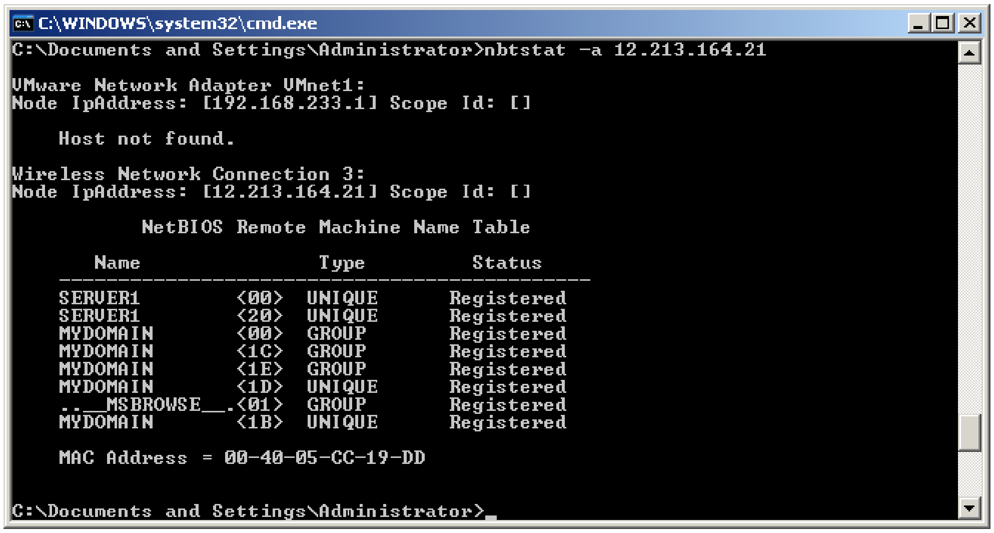


```
C:\Documents and Settings\Administrator>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    server1:ldap           server1.mydomain.com:2063  ESTABLISHED
  TCP    server1:1025           server1.mydomain.com:3520  ESTABLISHED
  TCP    server1:1025           server1.mydomain.com:4368  ESTABLISHED
  TCP    server1:1801           server1.mydomain.com:ldap  CLOSE_WAIT
  TCP    server1:1965           server1.mydomain.com:ldap  CLOSE_WAIT
  TCP    server1:2063           server1.mydomain.com:ldap  ESTABLISHED
  TCP    server1:3519           server1.mydomain.com:epmap  TIME_WAIT
  TCP    server1:3520           server1.mydomain.com:1025  ESTABLISHED
  TCP    server1:3521           64.219.240.2:https     TIME_WAIT
  TCP    server1:4368           server1.mydomain.com:1025  ESTABLISHED
  TCP    server1:ldap           server1.mydomain.com:1033  ESTABLISHED
  TCP    server1:ldap           server1.mydomain.com:1034  ESTABLISHED
  TCP    server1:ldap           server1.mydomain.com:1036  ESTABLISHED
  TCP    server1:ldap           server1.mydomain.com:2069  ESTABLISHED
  TCP    server1:1033           server1.mydomain.com:ldap  ESTABLISHED
  TCP    server1:1034           server1.mydomain.com:ldap  ESTABLISHED
  TCP    server1:1036           server1.mydomain.com:ldap  ESTABLISHED
  TCP    server1:2069           server1.mydomain.com:ldap  ESTABLISHED
  TCP    server1:2890           server1.mydomain.com:ldap  CLOSE_WAIT

C:\Documents and Settings\Administrator>
```

Figure 52

Nbtstat

Nbtstat will show the protocol statistics for NETBIOS over TCP/IP. It can show this for your local system, as well as remote systems. This is especially handy in diagnosing just about any NETBIOS issue. Below is a sample of a NETBIOS table produced with NBTSTAT:



```
C:\Documents and Settings\Administrator>nbtstat -a 12.213.164.21

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.233.1] Scope Id: []

    Host not found.

Wireless Network Connection 3:
Node IpAddress: [12.213.164.21] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SERVER1        <00>  UNIQUE      Registered
    SERVER1        <20>  UNIQUE      Registered
    MYDOMAIN       <00>  GROUP       Registered
    MYDOMAIN       <1C>  GROUP       Registered
    MYDOMAIN       <1E>  GROUP       Registered
    MYDOMAIN       <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
    MYDOMAIN       <1B>  UNIQUE      Registered

    MAC Address = 00-40-05-CC-19-DD


C:\Documents and Settings\Administrator>_
```

Figure 53 - A

Troubleshoot connectivity to the Internet

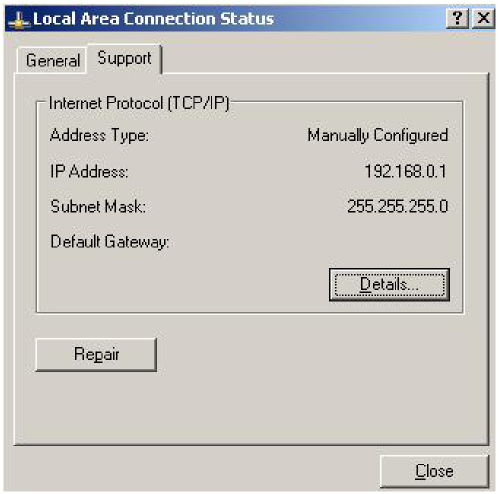
Since the Internet is used for so many tasks today, when Internet connectivity is down, for an end-user or for an entire organization, critical business does not get done. When critical business does not get done, that costs everyone involved time and money.

So how do you troubleshoot Internet connectivity efficiently (and save everyone time and money)? First you have to find the problem before you can fix it. Check the following to isolate the trouble:

Verify Name resolution with the **ping** command. If pinging a name resolves an IP address, regardless of whether the ping is successful, then name resolution is functioning. If the name cannot be resolved, it could be a DNS issue or all connectivity could be down.

Verify IP address settings. Does the machine have an IP address? Does it have an Automatic IP address (indicating a problem)?

Use the Repair button on the Local Area Connection Support tab (shown below). You can get here two ways. One way is, if your LAN adaptor is shown on the taskbar, double-click it then choose the Support tab. Or, the other way is, go to Control Panel, Network Connection, then bring up properties on your LAN adaptor. From there, click on the Support tab.



Internet Protocol (TCP/IP)

Address Type: Manually Configured

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Default Gateway:

Figure 53 - B

What does the repair button do? It provides these functions:

- Ipconfig /renew
- Arp –d *
- Nbtstat –R
- Nbtstat –RR
- Ipconfig /flushdns

- Ipconfig /registerdns

If the DHCP client cannot get an IP address then it you should check the DHCP relay agent, the DHCP server, and general physical connectivity (verify there is a link light on the network card to the computer).

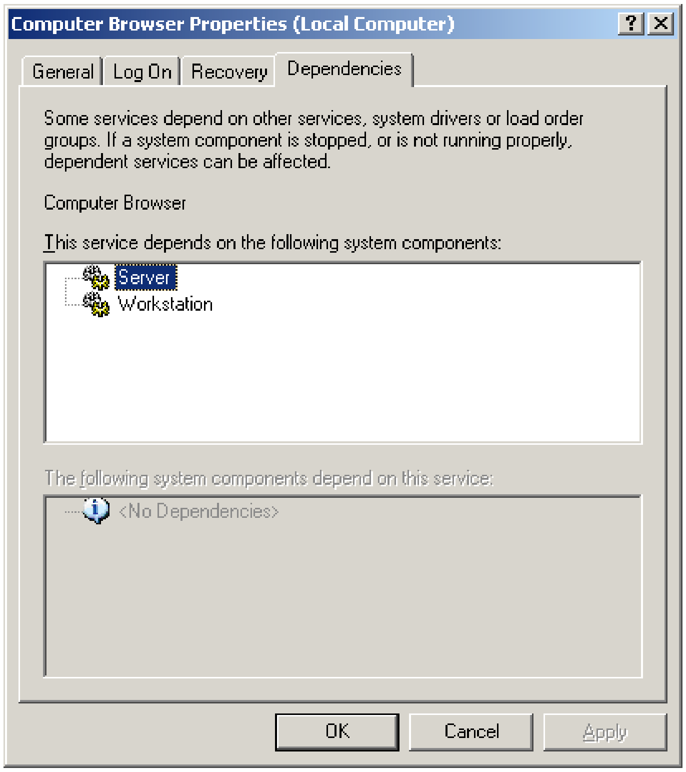
Troubleshoot server services

There are over 100 services on a Windows 2003 Server. Many of these services are dependant on other services. Trouble with a single service can cause trouble for many dependency services. Thus, diagnosing and resolving service trouble efficiently and quickly can be very valuable.

Diagnose and resolve issues related to service dependency

Services are either configured as **Automatic, Manual, or Disabled**.
When one service depends on another service before it will start, this is known as "service dependency." Double clicking on an individual service and selecting the dependencies tab will tell you what services this service is dependant on and what services are dependant on this service.

As you can see below, the computer browser service is dependant on the server and workstation services and no services are dependant on the computer browser service:



Some services depend on other services, system drivers or load order groups. If a system component is stopped, or is not running properly, dependent services can be affected.

Computer Browser

This service depends on the following system components:

- Server
- Workstation

The following system components depend on this service:

- <No Dependencies>

Figure 54

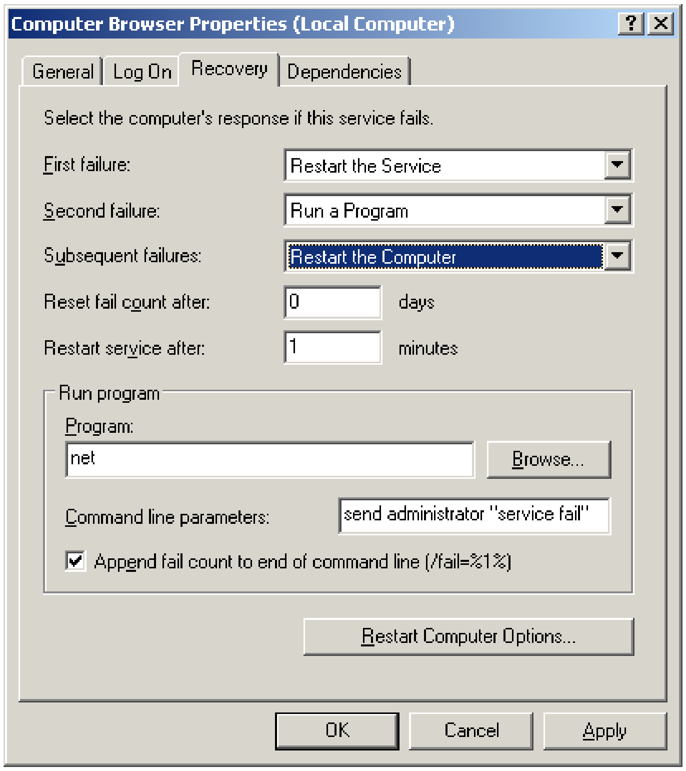
Use service recovery options to diagnose and resolve service-related issues

Many times, services use Windows accounts to perform their actions. It is very possible that these Windows accounts may not have the proper privileges, may have expired, or may have invalid passwords that may cause the service to fail. To change the account and password that services log on as, double-click the service and select the log on tab.

Services can be configured to take an action when they fail. You may configure them to run a program, restart the computer, or restart the service. By running a program, you could configure it such that you were alerted when the service failed.

As you can see below, we have configured the computer browser service to do the following:

- On first failure, restart the service
- On second failure, send a message using "net send"
- On third failure, restart the server



Computer Browser Properties (Local Computer)

Select the computer's response if this service fails.

First failure: Restart the Service

Second failure: Run a Program

Subsequent failures: Restart the Computer

Reset fail count after: 0 days

Restart service after: 1 minutes

Run program

Program: net

Command line parameters: send administrator "service fail"

☑ Append fail count to end of command line (/fail=%1%)

Figure 55

The following book was referenced in the creation of this section:
Windows Server 2003 Network Infrastructure by JC Mackin and Ian McLean.

Practice Questions

Chapter 1 Implementing Managing and Maintaining IP Addressing

1. You have decided to add a new Windows Server 2003 system in the role of a DHCP server to reduce bottlenecks on your current Windows 2000 DHCP server. All IP addresses within the current subnet have been split into two scopes. Everything was working well for a little over a week, and then some clients reported that they could not connect to the network. You cannot detect a pattern with the clients reporting the problem; however, you can ping the DHCP servers from the problematic machines using their NetBIOS names. What is required to resolve this problem?

Select the best answer.

○ A. Create separate sites for the two portions of the subnet. Place one DHCP server in each site using the Active Directory Sites and Services MMC snap-in.
○ B. Place a Global Catalog server with DNS and WINS services in the local subnet. Configure all machines to use the new server for all name service support.
○ C. Remove the old server to eliminate potential scope conflicts.
○ D. Authorize the new DHCP server for the domain.
○ E. Set the affected client systems for static IP addressing.

2. Katherine is a network administrator at IC International. She has been asked to research the most cost effective way to implement DHCP on a new subnet that does not currently have a Windows Server 2003 system installed in the role of a DHCP server. The network contains a subnet that contains a DHCP server but the existing router cannot forward DHCP/BOOTP broadcasts. What is the most viable solution?

Select the best answer.

○ A. Install the DHCP Relay Agent on the new subnet.
○ B. Purchase a new DHCP server.
○ C. Purchase a router capable of forwarding the DHCP/BOOTP broadcasts.
○ D. Install a DNS Forwarder to enable the DHCP broadcasts to cross the existing router.

3. Thomas is an employee at IC International, where you manage the network. He has moved to a new office in an adjacent building, taking his desktop computer with him. Thomas discovers that he can no longer communicate on the network from his new office, although his coworkers at the new location can communicate with the network. Both buildings have subnets using Windows Server 2003 DHCP servers. What could be the problem?

Select the best answer.

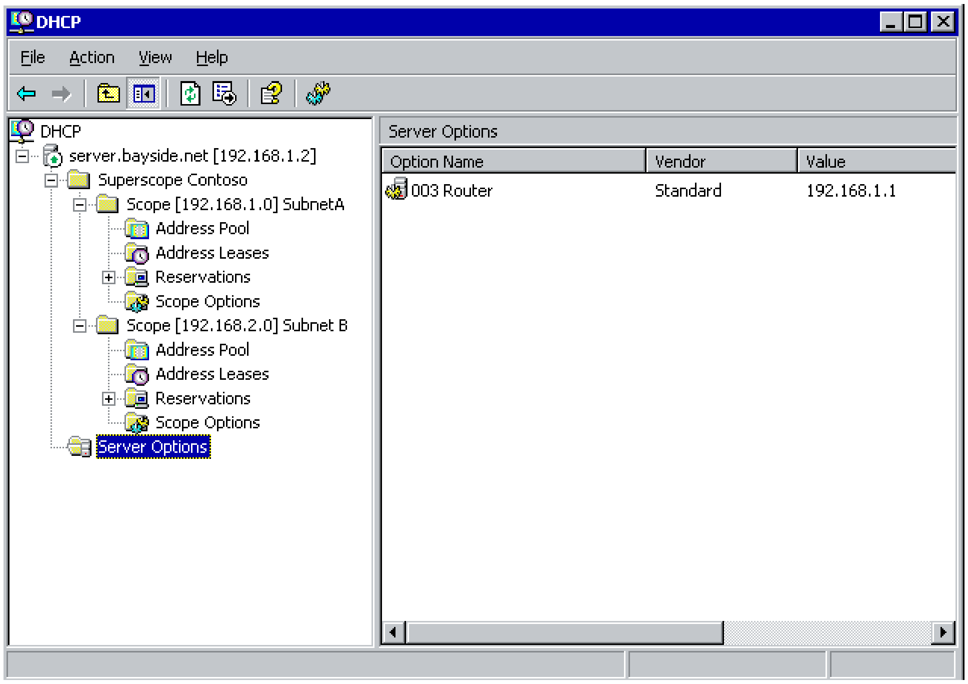
○ A. The DHCP server at the new location is down.
○ B. The DHCP lease has expired.
○ C. The computer has a static IP configuration.
○ D. The DHCP server at the new location has an incorrect default gateway set for the subnet scope.

4. You are the network administrator for Contoso Ltd. You have implemented the DHCP service on a Windows Server 2003 member server in your domain to automate IP addressing on the ne work. There is a single DHCP server configured, as shown in the exhibit. Users on Subnet B report that they cannot access resources outside of their local subnet. What is causing the problem?

Select the best answer.

○ A. The DHCP server has not been authorized in Active Directory.
○ B. The scope for Subnet B has not yet been activated.
○ C. The scopes must be removed from the superscope.
○ D. The 003 router option is misconfigured.

Exhibit(s):



- DHCP
  - server.bayside.net [192.168.1.2]
    - Superscope Contoso
      - Scope [192.168.1.0] SubnetA
        - Address Pool
        - Address Leases
        - Reservations
        - Scope Options
      - Scope [192.168.2.0] Subnet B
        - Address Pool
        - Address Leases
        - Reservations
        - Scope Options
    - Server Options

Server Options

Option Name	Vendor	Value
003 Router	Standard	192.168.1.1

5. What is the valid order when a client leases an IP address?

To answer, drag the appropriate options to the right in the correct order as they occur during the lease process.

A. DHCPOFFER ____
B. DHCPREQUEST ____
C. DHCPACK ____
D. DHCPDISCOVER ____

Chapter 2 Implementing Managing and Maintaining Name Resolution

1. Victoria is the network administrator at IC International. She is combining the old public Web server (public.ici.com) and the new production Web server (prod.ici.com), while allowing developers to continue using the name prod.ici.com. She has removed the DNS entry from the old Web server, and now needs to create a record directing users looking for publc.ici.com to the new server's current IP address. What type of record should Victoria create?

   Select the best answer.

   ❍ A. Host (A) Record
   ❍ B. CNAME Record
   ❍ C. MX Record
   ❍ D. PTR Record

2. Katherine has been asked for her opinion on increasing the fault tolerance of the corporate ne work, which uses TCP/IP, Active Directory, and Windows 2000 computers. Specifically, the one DNS server on subnet A. Users may run into serious problems if that machine ever experiences downtime, or if the link between the two subnets goes down. Each subnet has its own Windows 2003 domain controller. What would you suggest to provide fault tolerance for the network?

   Select the best answer.

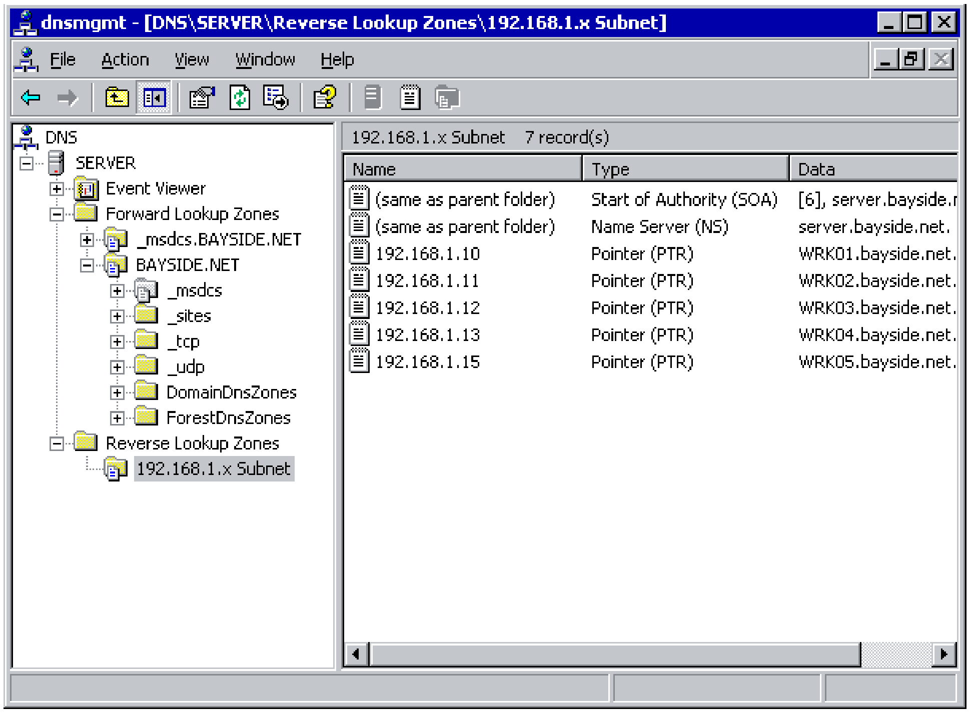
   ❍ A. Set up a secondary DNS server on subnet B and configure it to request refreshes from the master DNS server on subnet A.
   ❍ B. Set up a secondary DNS server on subnet B. Configure the primary DNS server on subnet A to send notifications of zone changes to the secondary DNS server.
   ❍ C. Install a caching-only DNS server on subnet B.
   ❍ D. Configure DNS on both domain controllers using Active Directory Integrated zones.

3. You are the network administrator for your Windows Server 2003 domain. You are trying to determine the hostname associated with the IP address of 192.168.1.14. You issue the nslookup command from WRK02 but are unsuccessful. You can successfully determine the hostname associated with the IP address of 192.168.1.15. You open up the DNS console shown in the exhibit. What is causing the problem?

   Select the best answer.

   ❍ A. There is no A record that maps the hostname to the IP address of 192.168.1.14.
   ❍ B. The DNS server is not available.
   ❍ C. A record for the IP address of 192.168.1.14 does not exist in the reverse lookup zone.
   ❍ D. There is no PTR record for the IP address of 192.168.1.15.

Exhibit(s):



dnsmgmt - [DNS\SERVER\Reverse Lookup Zones\192.168.1.x Subnet]

192.168.1.x Subnet 7 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[6], server.bayside.r
(same as parent folder)	Name Server (NS)	server.bayside.net.
192.168.1.10	Pointer (PTR)	WRK01.bayside.net.
192.168.1.11	Pointer (PTR)	WRK02.bayside.net.
192.168.1.12	Pointer (PTR)	WRK03.bayside.net.
192.168.1.13	Pointer (PTR)	WRK04.bayside.net.
192.168.1.15	Pointer (PTR)	WRK05.bayside.net.

4. Chris is the administrator of a Windows Server 2003 network for DKP International. The parent domain for DKPIntl.net is hosted on DNS01. A delegation is created for the child domain sales DKPIntl.net. A few weeks later, the DNS administrator adds two additional DNS servers to the child domain. However, because Chris was not notified, the DNS01 is unaware of the new authoritative DNS servers. What should he do to ensure this does not occur again?

Select the best answer.

○ A. Manually edit the zone file and add the resource records for the new DNS servers.
○ B. Enable DNS forwarding on the DNS servers in the child domain.
○ C. Configure a stub zone on the DNS server in the parent domain.
○ D. Enable dynamic updates for the DKPIntl.net zone.

5. Jim has configured his company DNS server. He installed DNS on a Windows Server 2003 member server. The zone is currently standard primary. He wants Windows 2000 Professional clients to be able to update their own host records. What should he do?

Select the best answer.

○ A. Upgrade the member server to a domain controller.
○ B. Change the zone to Active Directory Integrated.
○ C. Configure all clients to perform dynamic updates through the properties of TCP/IP.
○ D. Enable the zone for nonsecure and secure updates.

Chapter 3 Implementing Managing and Maintaining Network Security

1. Servers on your company network are running Windows 2000 and Windows Server 2003. All servers are configured to use IPSec. You want to monitor IPSec communications for these servers. You use the IP Security Monitor snap-in. However, you soon discover that you are unable to monitor any of the Windows 2000 Servers. What is causing the problem?

   Select the best answer.

   ○ A. You are running IP Security Monitor in a computer running Windows Server 2003.
   ○ B. You are trying to monitor multiple servers at one time.
   ○ C. You do not have administrative permission.
   ○ D. You must install service pack two on the Windows 2000 servers.

2. One of the Windows Server 2003 file servers on your network is used to store confidential information. The server's IPSec policy was configured to require secure communications. You soon discover that secure communication between clients and this server are not occurring. You suspect someone has changed the IPSec policy settings without your approval.

   What should you do to try to investigate this? (Choose the best answer.)

   ○ A. Use the IP Security Monitor to verify that secure communication is not occurring.
   ○ B. Use the Security log with Event Viewer to determine who made the policy change and when it occurred.
   ○ C. Use Network Monitor and analyze the traffic coming to and from the server.
   ○ D. Use System Monitor to gather performance statistics for the server.

3. Diane is the network administrator for a Windows Server 2003 network. There are five servers being added to the network. She wants each server to be configured with the same security settings. What is the most efficient way for Diane to accomplish this task?

   Select the best answer.

   ○ A. Manually configure the local security settings on each server.
   ○ B. Create a new template using the Security Configuration and Analysis Tool and deploy it through a group policy object.
   ○ C. Create a new template using the Security Templates tool. Deploy the template through a group policy object.
   ○ D. Create a new template using the Security templates snap-in. Deploy the template to all servers using Software Updates Services.

4. Felicia is the network administrator for a Windows Server 2003 network. There are several junior network administrators employed. Felicia suspects that changes have been made to the security settings on several servers. There is a standard security template with which all new servers are configured. What tool can Felicia use to verify the current security settings against those within the original template?

   Select the best answer.

   ○ A. Security Templates
   ○ B. Active Directory Users and Computers
   ○ C. IP Security Monitor
   ○ D. Security Configuration and Analysis
   ○ E. System Monitor

5. Mike is the network administrator of a Windows Server 2003 network. His company has decided to implement Software Update Services. Mike needs to purchase a new server that will run the service. Which of the following are considered recommended hardware requirements to install Software Update Services?

   Each answer presents part of the solution. Choose three.

   □ A. Pentium III 500 MHZ
   □ B. Pentium III 700 MHZ
   □ C. 256 MB of RAM
   □ D. 512 MB of RAM
   □ E. 6 GB free space
   □ F. 10 GB free space

Chapter 4 Implementing Managing and Maintaining Routing and Remote Access

1. Jim is configuring the IP security policy for a computer running Windows Server 2003. Some of the client computers on the network are not IPSec aware, while others are. Jim wants all data to be encrypted and still allow those computers that do not support IPSec to authenticate. Which of the following settings should he select?

   Select the two best answers.

   □ A. Server Secure (require security)
   □ B. Server (request security)
   □ C. Client (respond only)
   □ D. Client (request security)

2. Greg has a computer running Windows Server 2003 configured for remote access. He is configuring the encryption settings within the remote access policy. He selects Basic encryption. Which of the following encryption levels will be used?

Choose two correct answers.

❑ A. MPPE 40-bit
❑ B. MPPE 56-bit
❑ C. MPPE 128-bit
❑ D. IPSec 56-bit DES
❑ E. IPSec Triple DES (3DES)

3. Dayton Street Cooling has 10 users that require remote access. Sean, the network administrator for the compnay's Windows Server 2003 domain needs to allow these 10 users remote access during business hours only. Remote access clients should be allowed to dial into the company's remote access server during the hours of 8 a.m. and 6 p.m. How should Sean configure remote access?

Select the best answer.

○ A. Configure the day and time restrictions using the Dial-in tab of each user account.
○ B. Configure the day and time restrictions by editing the conditions of the remote access policy.
○ C. Configure the day and time restrictions by editing the profile settings of the remote access policy.
○ D. Create a group for the 10 remote access users. Configure day and time restrictions through the group's properties window.

4. Mary has just finished making changes to the IP security policy for users in the company's Windows Server 2003 domain. She wants the changes to be applied immediately. Which of the following command should she use?

Select the best answer.

○ A. GPUPDATE
○ B. NETSH
○ C. SECEDIT
○ D. GPRESULT

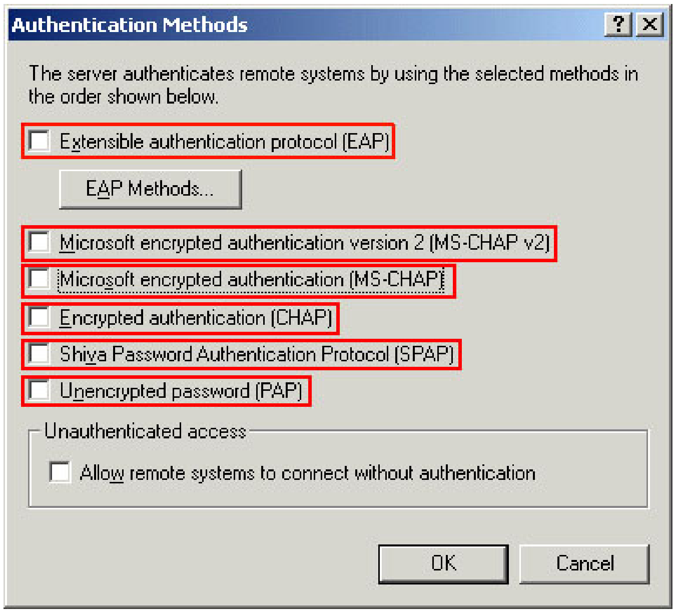
5. Your company has recently upgraded to Windows Server 2003 and is currently running their network at a Domain Functional Level of Windows 2000 mixed. None of the default settings have been changed. You have created a new remote access policy that grants permission to remote access clients. You attempt a dial-up connection using a user account but you are unsuccessful. What is most likely causing the problem?

Select the best answer.

○ A. The permissions for the user account are set to deny access.
○ B. The dial-in properties for the user account in set to control access through remote access policies.
○ C. The permissions of the remote access policy deny access.
○ D. The profile settings of the remote access policy deny remote access to all users.

6. Mary is the network administrator for a small company. All remote access computers have recently been configured with smart cards.

Which of the following authentication protocols must Mary enable? To answer, select the control in the exhibit.



Authentication Methods

The server authenticates remote systems by using the selected methods in the order shown below.

☐ Extensible authentication protocol (EAP)

EAP Methods...

☐ Microsoft encrypted authentication version 2 (MS-CHAP v2)

☐ Microsoft encrypted authentication (MS-CHAP)

☐ Encrypted authentication (CHAP)

☐ Shiva Password Authentication Protocol (SPAP)

☐ Unencrypted password (PAP)

Unauthenticated access

☐ Allow remote systems to connect without authentication

Chapter 5 Maintaining a Network Infrastructure

1. Mary is the network administrator for Humongous Insurance, which is running their Windows Server 2003 domain at a domain Functional Level of Windows 2000 mixed. She wants to give a junior network administrator the ability to view real-time data that is captured with System Monitor without granting any more permissions than are necessary to perform this task.

What should she do?

○ A. Add the user account to the Performance Log Users group.
○ B. Add the user account to the Administrators group.
○ C. Add the user account to the Server Operators group.
○ D. Add the user to the Performance Monitor Users group.

2. The junior network administrator for Contoso Ltd. is using Network Monitor to capture and analyze network traffic. He runs Network Monitor on the company's Windows Server 2003, Standard Edition system that is running the IIS 6 service. Once the capture is complete, he wants to view traffic only for a specific protocol. What should he do?

   Choose the best answer.

   ○ A. Within Network Monitor, configure a capture filter.
   ○ B. Within the Properties window for Internet Protocol (TCP/IP), configure a packet filter.
   ○ C. Within Network Monitor, configure a trigger.
   ○ D. Within Network Monitor, configure a display filter.

3. You have enabled Internet Connection Sharing on a system running Windows Server 2003. The Internet connection is shared among eight computers running Windows XP Professional from the server system which uses a demand dial modem connection. One of the users reports that they are unable to access the Internet. You soon discover that the problem is affecting all computers on the private network. You want to verify that the modem is working on the server. What should you do?

   Choose the best answer.

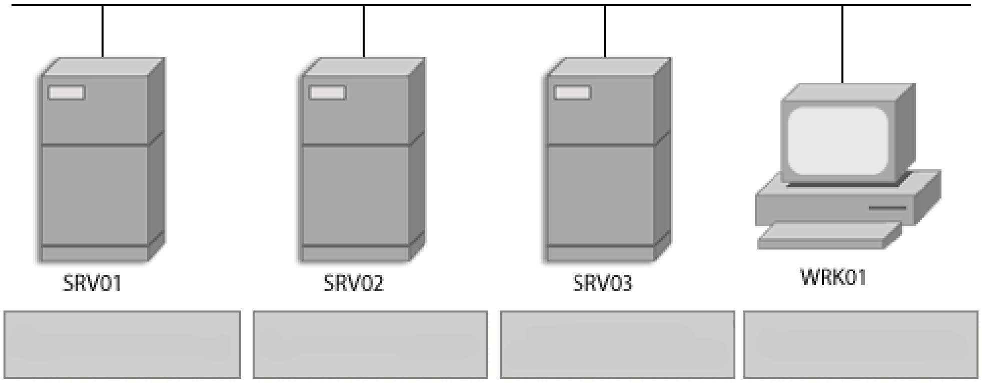
   ○ A. Use System Monitor to verify that the modem is working correctly.
   ○ B. Use Device Manager to verify that the modem is working.
   ○ C. Use Network Diagnostics to verify that the modem is working correctly.
   ○ D. Use Network Monitor to verify that the modem is functioning properly.

4. David is the network administrator of DKP International. There are three servers on the network: SRV01, SRV02, and SRV03. David has his own workstation named WRK01. SRV01 is configured as a Web server. SRV02 hosts the company's database. David wants to monitor traffic between SRV01 and SRV02 from his own workstation.

   On which computer(s) should he install the Network Monitor driver and which computer(s) the Network Monitor tools?

   To answer, drag the selections on the left and drop them on the appropriate elements.

   A. Network Monitor driver B. Network Monitor Tools C. No Network Monitor Implementation



Answers and Explanations

Chapter 1

1. Answer: D

Explanation A. This is not the best action to take. A site includes one or more subnets and DHCP servers will respond to DHCPDISCOVER broadcast messages automatically.

Explanation B. This is not the best answer for this scenario. The goal was to resolve a bottleneck problem. Adding a Global Catalog server with DNS and WINS will not rectify the problem.

Explanation C. This is not the best answer for this scenario. The scopes have already been separated to avoid conflicts between the two servers.

Explanation D. This is the best answer. DHCP servers must be authorized before they can provide leases to domain clients. Because the client systems will respond to the first offer they receive from a DHCP server, some may be provided with lease offers from DHCP servers not authorized for the Active Directory domain, therefore causing the clients to loose connectivity to the network.

Explanation E. Because the static IP addressing would require a free address in the subnet, and all addresses have already been included in the DHCP scopes, conflicts between two systems with the same IP address would result.

2. Answer: A

Explanation A. This is the best answer for this scenario. The DHCP Relay Agent will allow the new subnet to forward DHCP broadcasts to the DHCP server on the existing subnet.

Explanation B. This is not the best answer. Implementing a new DHCP server would allow for automatic IP addressing but is not the most cost effective choice.

Explanation C. This is not the best answer. A new router would allow communication to the DHCP server but is not the cost effective choice.

Explanation D. This action would not work. A DNS Forwarder is a DNS server that accepts request to resolve host names from another DNS server. It will not enable the gateway to forward DHCP/BOOTP broadcasts.

3. Answer: C

Explanation A. This is not the best answer. Co-workers at the new location can communicate with the network so the DHCP server is working.

Explanation B. This is not the best answer. If Thomas' system was a DHCP client, it would negotiate a new lease when the old one expired, at which point Thomas would receive a valid IP address.

Explanation C. This is the best answer. With a static IP address, Thomas' system would work on the original subnet, but when he changed subnets, the old address forced his system to try using the old network ID, which does not match the new subnet's network ID.

Explanation D. Co-workers at the new location can communicate with the network so the DHCP server is working.

4. Answer: D

Explanation A. This is not a correct answer. If the DHCP server is not authorized, it would appear with a red arrow within the DHCP console. Users on Subnet A would not be able to obtain an IP address.

Explanation B. This is not a correct choice as the information within the figure indicates that the scopes are both active.

Explanation C. This is not a correct answer. Superscopes are used when a DHCP server must lease IP addresses to multiple IP address ranges.

Explanation D. This is the best answer. The 003 router option should be configured at the scope level because each subnet requires a unique default gateway.

5. Answer:

A. DHCPOFFER	D.
B. DHCPREQUEST	A.
C. DHCPACK	B.
D. DHCPDISCOVER	C.

Explanation: The correct order is DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK.

Chapter 2

1. Answer: B

Explanation A. This is not the best answer for this scenario as it is unnecessary to create a new Host (A) record for an IP address already in use and this may cause unexpected behavior when attempting a reverse lookup from IP address to FQDN naming.

Explanation B. This is the best answer. Creating a CNAME (Alias) record for the name public.ici.com will allow both names to resolve to the same address.

Explanation C. This is not the best answer for this question as an MX record is used for mail redirection and is not used to allow more than one name to resolve to the same address.

Explanation D. It is unnecessary to create a PTR record because it is used in a reverse lookup zone and associates an IP address with its equivalent FQDN.

2. Answer: D

Explanation A. The solution is valid; however, not the best choice.

Explanation B. The solution is valid; however, not the best choice.

Explanation C. This is not a correct answer. The caching-only DNS server would not have a local copy of the DNS database; therefore, database redundancy would not be achieved.

Explanation D. By configuring DNS on both domain controllers using Active Directory, you can take advantage of Active Directory integration. The configuration of the DNS replication does not need to occur separately.

3. Answer: C

Explanation A. This is not a correct answer. Nslookup requires the use of PTR record to resolve the hostname associated with the IP address.

Explanation B. This is not the issue in this situation. Because you can successfully resolve other hostnames, this is eliminated as a possible cause.

Explanation C. This is the best answer for this question. To use Nslookup, the required PTR records must exist in the reverse lookup zone. There is no PTR record for the IP address of 192.168.1.14.

Explanation D. This is not a correct answer. Nslookup successfully resolves this IP address to a hostname and therefore, the PTR record must exist.

4. Answer: C

Explanation A. This is not the best answer. While manually editing the zone file and adding the resource records for the new DNS servers solves the immediate problem, it does not ensure the problem does not occur again.

Explanation B. This is not a correct answer as DNS forwarding allows you to specify the DNS server to which the request should be forwarded.

Explanation C. This is the best answer for the question. Stub zones are used to determine which DNS servers are authoritative for a specific portion of a DNS namespace.

Explanation D. This is not a correct answer. Dynamic updates allow clients within a specific zone to dynamically register their resource records with a DNS server.

5. Answer: D

Explanation A. This is not the best answer for this question. To store zone information within Active Directory, the DNS service must be running on a domain controller.

Explanation B. This is not the best answer for this scenario. The zone type must be changed from standard primary to Active Directory Integrated if secure updates are required.

Explanation C. This is not the best answer as Windows 2000 clients will update their own records by default.

Explanation D. Of the choices provided ,this is the best answer. A standard primary zone supports dynamic updates. There is no need to change the zone to Active Directory Integrated because the question does not mention using secure updates.

Chapter 3

1. Answer: A

Explanation A. This is the correct answer. The version of IP Security Monitor that is included with Windows Server 2003 cannot be used to monitor IPSec on Windows 2000 computers. If you need to monitor IPSec on a computer running Windows 2000 you would need to use the IPSecmon command at the Windows 2000 command prompt on the computer that is being monitored.

Explanation B. This is not a correct answer as the IP Security Monitor can be used to monitor multiple servers at once.

Explanation C. This is not a correct choice for this question. It has already been established that you can successfully monitor servers running Windows Server 2003. Therefore, permissions are not causing the problem.

Explanation D. This is not the best answer as installing the latest service pack will not solve the problem in this situation.

2. Answer: B

Explanation A. This is not the best answer as it has already been determined that unsecure communication between clients and the server are taking place.

Explanation B. This is the best answer for this scenario. As long as auditing is enabled, you can use the security log to determine when and who made the policy the change.

Explanation C. This is not the best answer. Capturing and analyzing the network traffic at this point will not do any good because it's already been determined that the IPSec policy has been changed.

Explanation D. System Monitor is used to monitor and log the performance of various components.

3. Answer: C

Explanation A. Although this is a viable solution, it is not the most efficient one as it does not produce the least amount of administrative effort.

Explanation B. This is not a correct choice as Security templates cannot be created through the Security Configuration and Analysis Tool.

Explanation C. This is the best answer. This is the most efficient way to configure all servers with the same security settings. Create a new template within the Security Templates snap-in, and deploy it using a group policy object.

Explanation D. This is not a correct choice as Software Update Services cannot be used to deploy security templates.

4. Answer: D

Explanation A. This is not the best answer. The Security Templates tool is used to create and configure security templates and it cannot be used easily to verify the current security settings of systems.

Explanation B. This is not the best answer Active Directory Users and Computers is used to administer OUs, computers, and user accounts; and cannot be directly used to verify the current security settings of systems.

Explanation C. IP Security Monitor is used to monitor IPSec communications and cannot be used to verify the current security settings of systems.

Explanation D. Of the choices provided, this is the best answer. Security Configuration and Analysis can be used to compare the security settings configured on a local computer with those in a security template to identify any discrepancies.

Explanation E. This is not a correct answer. System Monitor is used to monitor the real-time performance of system components, services, and applications; and cannot be used to verify the current security settings of systems.

5. Answers: B, D, E

Explanation A. This is not a correct answer as the recommended hardware requirements to install Software Update Services includes a Pentium III 700 MHZ processor, 512 MB of RAM, and 6 GB of free disk space.

Explanation B. This is one of the correct answers. The recommended hardware requirements to install Software Update Services includes a Pentium III 700 MHZ processor, 512 MB of RAM, and 6 GB of free disk space.

Explanation C. This is not a correct answer as the recommended hardware requirements to install Software Update Services includes a Pentium III 700 MHZ processor, 512 MB of RAM, and 6 GB of free disk space.

Explanation D. This is one of the correct answers. The recommended hardware requirements to install Software Update Services includes a Pentium III 700 MHZ processor, 512 MB of RAM, and 6 GB of free disk space.

Explanation E. This is one of the correct answers. The recommended hardware requirements to install Software Update Services includes a Pentium III 700 MHZ processor, 512 MB of RAM, and 6 GB of free disk space.

Explanation F. This is not a correct answer as the recommended hardware requirements to install Software Update Services includes a Pentium III 700 MHZ processor, 512 MB of RAM, and 6 GB of free disk space.

Chapter 4

1. Answers: B, C

Explanation A. This is not one of the best answers. This setting will force all communications to not be allowed for those clients that are not IPSec aware. The scenario indicated that all data needed to be encrypted and still allow those computers that do not support IPSec to authenticate.

Explanation B. This is one of the correct answers for this question. When using this setting, the server will request secure communications. Unsecured communications will be allowed if the client does not support IPSec.

Explanation C. This is one of the correct answers. The server will respond to requests for secure communications, but will not attempt to secure all communications.

Explanation D. This is not a correct option. There are only three options available for IPSec policies: Client (respond only), Server (request security), and Server Secure (require security).

2. Answers: A, D

Explanation A. This is one of the correct answers. When Basic encryption is enabled, remote access clients can connect using MPPE 40-bit or IPSec 56-bit encryption.

Explanation B. This is not a correct choice. When Basic encryption is enabled, remote access clients can connect using MPPE 40-bit or IPSec 56-bit encryption.

Explanation C. When Basic encryption is enabled, remote access clients can connect using MPPE 40-bit or IPSec 56-bit encryption.

Explanation D. This is one of the correct answers. When Basic encryption is enabled, remote access clients can connect using MPPE 40-bit or IPSec 56-bit encryption.

Explanation E. When Basic encryption is enabled, remote access clients can connect using MPPE 40-bit or IPSec 56-bit encryption.

3. Answer: B

Explanation A. This is not the best answer. Remote access day and time restrictions cannot be configured through the account properties.

Explanation B. This is the correct answer. To put day and time restrictions in place for remote access clients, you must edit the conditions of the remote access policy.

Explanation C. This is not the best answer. To put day and time restrictions on place for remote access clients, you must edit the conditions of the remote access policy.

Explanation D. This is not the best answer. To put day and time restrictions on place for remote access clients, you must edit the conditions of the remote access policy.

4. Answer: A

Explanation A. This is the correct answer as GPUPDATE is the command that is used to propagate policy changes immediately.

Explanation B. This is not a correct answer. The NETSH command is used to view and modify the network configuration of a local computer or remote computer and cannot be used to propagate policy changes immediately.

Explanation C. This is not a correct answer. SECEDIT is the command used in Windows 2000 to update policy settings. It is replaced by the GPUPDATE command in Windows Server 2003.

Explanation D. This is not a correct choice as the GPRESULT command is used to display group settings for a user or computer.

5. Answer: A

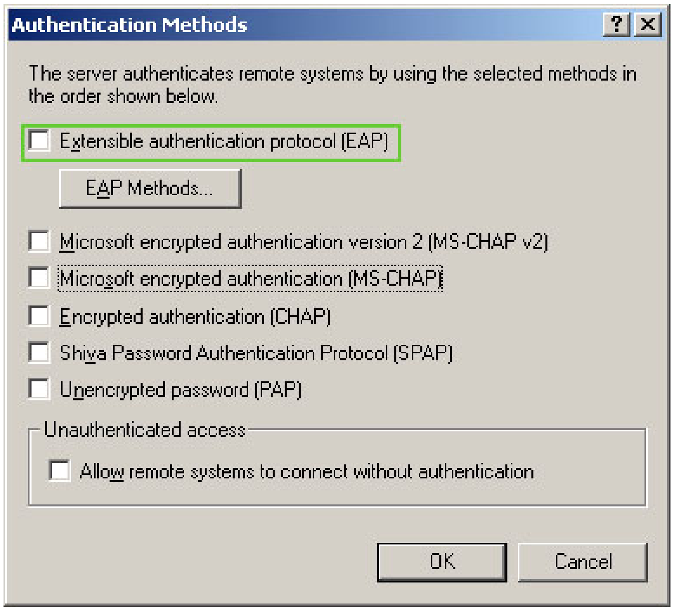
Explanation A. This is the correct answer. Because the domain is running in Windows 2000 mixed mode, the dial-in properties for user accounts is set to deny access.

Explanation B. This is not a correct answer as this option is not available for domain running in Windows 2000 mixed mode.

Explanation C. This is not a correct answer. It has already been stated that the permissions have been granted in the remote access policy.

Explanation D. This is not a correct answer. The profile settings of a remote access policy are not evaluated unless the user has been granted remote access.

6. Answer:


Authentication Methods

The server authenticates remote systems by using the selected methods in the order shown below.

□ Extensible authentication protocol (EAP)

EAP Methods...

□ Microsoft encrypted authentication version 2 (MS-CHAP v2)

□ Microsoft encrypted authentication (MS-CHAP)

□ Encrypted authentication (CHAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Unencrypted password (PAP)

Unauthenticated access

□ Allow remote systems to connect without authentication

Explanation: The Extensible Authentication Protocol is an authentication mechanism that allows the authentication scheme to be negotiated between a remote access client and a remote access server or RADIUS server. It is required for smart card authentication.

MS-CHAP is a password-based authentication protocol.

CHAP is a protocol used to encrypt data.

PAP is a password-based authentication protocol that sends credentials clear text; therefore it is not recommended.

SPAP is a password-based authentication protocol used by Shiva clients or Windows clients that must authenticate to Shiva LAN Rover.

Chapter 5

1. Answer: D

Explanation A. This is not the best answer. The junior network administrator requires permission to view real time performance counters, but adding them to the Performance Log Users group gives them more permissions than required.

Explanation B. This is not the best answer. The junior network administrator requires permission to view real time performance counters, but adding them to the Administrators group gives them more permissions than required.

Explanation C. This is not the best answer. The junior network administrator requires permission to view real time performance counters, but adding them to the Server Operators group gives them more permissions than required.

Explanation D. This is the best answer. Adding the user account to the Performance Monitor Users group gives the user the necessary permission to perform the required task.

2. Answer: D

Explanation A. This is not the best answer. A capture filter is configured so Network Monitor will capture only specific types of traffic.

Explanation B. This is not the best answer. A packet filter is configured to determine which types of traffic can pass through the computer.

Explanation C. This is not the best answer for this scenario as Triggers are created to have a certain actions performed when certain criteria is met.

Explanation D. This is the best answer for this question. A display filter is configured so Network Monitor displays only information that meets the criteria specified. A display filter is configured after you have performed a capture.

3. Answer: B

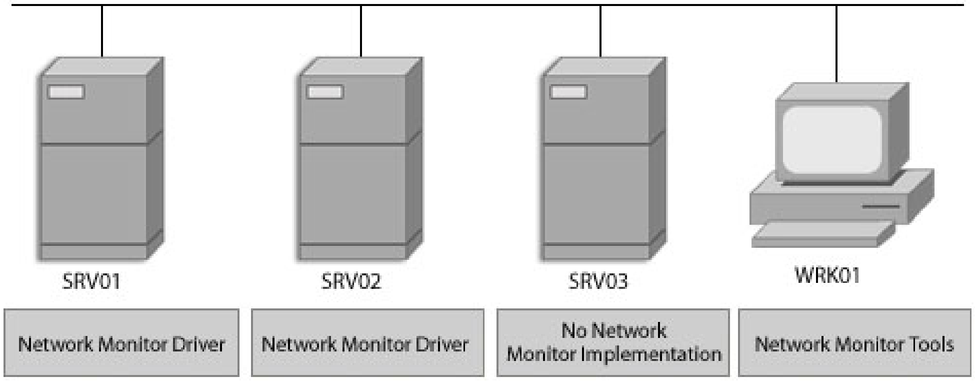
Explanation A. This is not a correct choice as the System Monitor cannot be used to test whether a device is working properly.

Explanation B. Of the choices provided, this is the best answer. Device Manager can be used to verify that a device is functioning properly.

Explanation C. This is not a correct answer. Network Diagnostics is used to determine the hardware, software, and services running on a computer and may not necessarily work in this situation. The best, first action to take is to verify that the hardware itself is running correctly.

Explanation D. This is not a correct answer. Network Monitor is used to capture and analyze network traffic; it cannot be used to verify that the modem is working on the server.

4. Answer:



Explanation: Install the Network Monitor tools on WRK01. Install the Network Monitor driver on SRV01 and SRV02.

Because traffic is being viewed from WRK01, the Network Monitor tools must be installed on the workstation. The Network Monitor driver must be installed on SRV01 and SRV02 to capture network traffic. Because traffic is not being captured or analyzed on SRV03, there is no need to install Network Monitor Tools or the Network Monitor driver on that server.