Introduction to Implementing and Administering a Windows 2000 Network

CERTIFICATION OBJECTIVES

1.01 What Is a Network Infrastructure
1.02 Overview of Exam 70-216
1.03 What We’ll Cover in this Book
1.04 Networking Terminology
1.05 For “Newbies” and “Old Pros”
✓ Two-Minute Drill
Q&A Self Test
Welcome to Windows 2000 and one of Microsoft’s most important core topics for the Windows 2000 Microsoft Certified Systems Engineer (MCSE) certification track. Networking is what Microsoft’s new operating system—and computing in general—is all about today. Understanding how to build, use, maintain, and troubleshoot the network infrastructure is essential to performing the duties of an administrator, and must be mastered in order to obtain certification as a systems engineer.

Knowledge of NT networking provides a good foundation for studying for this exam, but it’s not enough. Although networking fundamentals remain the same at the physical level, administration of a Windows 2000 network requires many skills that were not required of an NT 4.0 administrator. With new features such as Active Directory, and a new emphasis on topics that were only touched on lightly, such as DNS, Windows 2000 is changing the world of networking and the way administrators perform common tasks. To understand and troubleshoot the new operating system, you must first have a thorough understanding of basic TCP/IP concepts such as Domain Name Services (DNS), the Dynamic Host Configuration Protocol (DHCP), Routing and Remote Access Services (RRAS) including Network Address Translation (NAT), the Windows Internet Name Service (WINS), Certificate Services, and the TCP/IP and NWLink protocol suites upon which modern networks are based.

**Correlation Between Windows 2000 and NT 4.0 Exams**

It might be tempting to try to draw a correlation between the NT 4.0 core exams and the new Windows 2000 core exams. In so doing, you might conclude that Exam 70-216, the core exam that covers implementation and administration of a Windows 2000 network infrastructure, is a replacement for the old Networking Essentials exam (70-058). However, the Windows 2000 Networking Infrastructure exam goes far beyond the basic networking terminology and concepts covered by the Networking Essentials exam.

**Target Audience**

Microsoft’s stated “target audience” for this exam is somewhat different from the intended audience for the Networking Essentials exam (70-058), for which Microsoft lists no prerequisites on the exam preparation Web page. There has been a lot of talk, with the advent of the Windows 2000 certification track, about Microsoft’s desire to
“raise the bar” and restore the MCSE to the status of a “premium” certification. This is reflected in the suggested prerequisites.

Experienced Networking Professionals

According to the Microsoft Web site and documentation, exam candidates are presumed to be networking personnel operating in medium-to-very-large computing environments with a minimum of a year’s experience in administering and implementing Windows networking components and supporting 200 or more users in five or more physical locations. It is also presumed that the exam taker is familiar with typical network services and applications, such as file and print sharing, databases, messaging services, proxy and/or firewalls, dial-in remote access servers, Web hosting, and desktop management and control.

What If You’re New to Networking?

The above does not mean that if you don’t have on-the-job experience as a network administrator you won’t be able to pass the Windows 2000 exams. It does mean that if you don’t meet the description of the exam’s “target audience,” you will need to study harder, and in particular you will need to get more hands-on practice in working with the products.

This book contains a large number of practical exercises that walk you through the steps of procedures common to working network professionals. In order to really understand the concepts and skills covered by the exam, it is essential that you do more than read through the exercises—you must work through them on a Windows 2000 computer. This can be done on a relatively simple home network, and we highly recommend that you consider setting up a two- or three-system lab if you don’t have access to a network on the job or in a classroom situation. The cost of doing so is an investment that can quickly pay for itself in terms of time saved in obtaining the certification.

CERTIFICATION OBJECTIVE 1.01

What Is a Network Infrastructure?

*Infrastructure* is a big word that can be used to describe many things. It is often used to refer to the basic facilities, services, and installations necessary for a community or
a society to function (such as roads, communications systems, water and sewer services, electrical power lines, and so forth.). The dictionary gives the following broad definition:

An underlying base or foundation of an organization or system.

From this, we can extrapolate that the infrastructure of a computer network consists of the basic components upon which it is built. We could further divide these into two subcategories:

- Those making up the physical infrastructure (the machines themselves, the cables and network interface cards, and hubs and routers)
- Those making up the logical infrastructure (the networking protocols, the DNS namespace and services, the IP addressing scheme and DHCP strategy, the remote access services, security protocols)

The first category is hardware-related, while the second is dependent on software components and their configuration.

**New Focus on the Logical Infrastructure**

The old Networking Essentials exam in the Windows NT 4.0 certification track focused primarily (although not exclusively) on the physical infrastructure. That exam was more knowledge-based than skills-based, and many questions measured the ability to recognize or recite such factual information as the layer of the OSI networking model at which specific protocols and connectivity devices operate, the number of bytes in a fixed-length ATM cell, or the number of nodes allowed on a segment in a particular type of network. Exam candidates were required to identify specifications of the Institute of Electrical and Electronics Engineers (IEEE) by specification number, name the characteristics of various wide area networking (WAN) technologies, and differentiate between common networking topologies, media access methods, and architectures.

The Windows 2000 core networking exam, Implementing and Administering a Windows 2000 Network Infrastructure, is focused almost entirely on the logical infrastructure. This doesn’t mean Microsoft no longer believes a network
The administrator needs to know about hardware issues; rather, it appears to presume two things:

- The Windows 2000 exam candidate has prior networking experience and is already familiar with physical issues.
- The typical Windows 2000 exam candidate will be working in a company that has a medium-to-very-large network, and in this environment there is more likely to be a division between the personnel who do actual administrative tasks and the technicians who care for the hardware.

**Components of the Logical Infrastructure**

The physical infrastructure is, for many, easier to understand because its components are tangible; you can see and touch them. The logical infrastructure is more abstract and includes the following, which are covered in Exam 70-216:

- Network Protocols
- IP Addressing Schemes
- Name Resolution Services
- Remote Access
- Routing and Network Address Translation
- The Security Infrastructure (Certificate Services)

**Networking Protocols**

An important component of the logical foundation of a group of networked computers is the protocol(s) those computers use to communicate.

A protocol is a set of rules, or a standardized order of procedures, that the networking components of the systems follow when they transmit data over the network. There are physical layer protocols, which consist of specifications or standards governing the hardware components, and there are numerous other protocols that operate at higher layers of the networking model. But the term “network protocol” is usually used to refer to the network and transport layer
Chapter 1: Introduction to Implementing and Administering a Windows 2000 Network

protocols (often part of a protocol “stack” or “suite”) used for communication over a local area network (LAN).

Although Windows 2000, like Windows NT and the Windows 9x operating systems, supports other LAN protocols such as NWLink (a Microsoft implementation of Novell’s IPX/SPX protocol stack) and NetBEUI (a simple, fast, low-overhead protocol used primarily in small, nonrouted networks), the “protocol stack of choice” for Windows 2000 networks is, not coincidentally, the set of protocols upon which the global Internet is based—the Transmission Control Protocol/Internet Protocol, or TCP/IP suite of protocols.

Networking Models In order to fully understand how networking protocols function, you should be familiar with some of the popular networking models that describe the networking architecture and serve as the framework for standardization of the steps involved in network communications. The Open Systems Interconnection, or OSI model has become a common reference point for discussion of network protocols and connection devices.

The OSI model uses seven layers or levels to represent the communications process. This layered approach provides a logical division of responsibility, where each layer handles prescribed functions. The OSI model is used as a broad guideline for describing the network communications process. Not all protocol implementations map directly to the OSI model, but it serves as a good starting point for gaining a general understanding of how data is transferred across a network.

Figure 1-1 shows a graphical representation of the OSI networking model, from the “top down.”

Communication takes place between corresponding layers on the Sending and Receiving computers. The data that is created by a user application (such as an e-mail message) enters the network communication process at the Application layer, and travels down the levels, with each layer adding header information that will be processed by its corresponding layer on the other side. At the Physical layer, the data is turned into electrical impulses, pulses of light, or radio signals (depending on the physical media being used) and sent out over the cable or over the air to the destination computer. When it arrives there, the networking components on that system process the data in the opposite order, finally delivering it (with the intervening headers stripped off) to the user application program (such as the recipient’s e-mail program) at that end.
Note that the Data Link layer as represented in the original implementation of the OSI model was later divided into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

Figure 1-2 shows how this process works.

The model is important to understanding protocols, because in a protocol stack such as TCP/IP, different protocols work at different layers, in conjunction with one another. We will discuss the separate functions of TCP, UDP, and IP a little later in this chapter.

The OSI model is not the only networking model in use. If you do much study of TCP/IP, you will also encounter the DoD (Department of Defense) model, and Microsoft has developed its own Windows networking model that intersperses layers called “boundary layers” representing open standards with vendor-specific components of its networking software.

OSI is an international standard, however, and Microsoft exams have traditionally required some knowledge of its structure and which protocols operate at which levels.
Why TCP/IP? The TCP/IP protocol suite is the current standard for large networks, up to and including the Internet itself. Although it is slower and requires more resource overhead than other common network/transport protocol stacks, it has the advantages of being easily routable and compatible with most platforms and operating systems. Using the TCP/IP protocols to connect to the Internet, a computer user in Los Angeles using a Windows system can communicate with someone in London using a Macintosh or someone in Tokyo using a Sun Solaris workstation. TCP/IP is the common “language” that makes it possible.

It would be difficult for an administrator to find a network environment today in which knowledge of TCP/IP is not required. Even Novell’s NetWare server operating system, which for a long time relied on the IPX/SPX protocol stack for communications, has with the debut of NetWare 5.0 included support for “pure IP.” TCP/IP was originally designed for use on the ARPAnet, the predecessor of the Internet. The U.S. Department of Defense, in conjunction with major universities, developed the nation-wide system (which then was extended throughout the world) to provide highly reliable, redundant communications links that could withstand
even a nuclear war. TCP/IP has also survived efforts to replace it with other protocols, most notably the OSI suite.

Because of its continuing popularity and its role as a foundation of communications on large (and more and more small) networks today, TCP/IP is an essential topic of study for an aspiring MCSE. The Windows NT 3.51 and 4.0 certification tracks included an elective exam devoted to TCP/IP. The Windows 2000 track does not. This is not because a mastery of TCP/IP is less important in the new certification track; rather, it is because it has become so much more important that the fundamentals of TCP/IP are now incorporated into the required core exams. A thorough understanding of TCP/IP and those topics formerly included in the TCP/IP exam material (DNS, WINS, DHCP) is required to pass the Networking Infrastructure exams (both the core 70-216 and the elective Designing a Windows 2000 Network Infrastructure, Exam 70-221).

**What Is a Network Infrastructure?**

Microsoft is focusing on the mastery of practical skills in the Windows 2000 exams, and because some exams may contain interactive simulations, it is imperative that you be intimately familiar with such processes as configuring and modifying TCP/IP properties.

Microsoft has made installation and configuration of TCP/IP and other supported protocols a relatively painless procedure, but there is still quite a bit of information that you will need to know in order to properly configure the TCP/IP stack on a Windows 2000 computer, including the following:

- The IP address that will be used by the computer (see the following section on IP address schemes) or that the computer will use the Dynamic Host Configuration Protocol (DHCP) to obtain an IP address—in which case, there must be a DHCP server on the network.
- The subnet mask, which determines which part of the IP address represents the network ID and which part represents the host ID.
- The default gateway(s), if the network is routed. You can configure multiple default gateways for each network interface in Windows 2000, although only one will be used (however, the others serve as “backup” gateways in case the first gateway is unavailable).
The IP address of a DNS server that will be contacted to resolve fully qualified domain names (FQDNs) to IP addresses. Windows 2000 is far more dependent on DNS than was Windows NT, and in a network with a Windows 2000 domain controller using Active Directory, DNS is not an optional component.

The IP address of a WINS server that will be contacted to resolve NetBIOS names to IP addresses. In a “pure” Windows 2000 environment, NetBIOS over TCP/IP (NetBT) can be disabled and WINS can be decommissioned; however, many networks will still need WINS for “downlevel” clients and application software that uses NetBIOS.

Note that much of this information, in addition to just the IP address, can be assigned by a DHCP server if the computer is configured to be a DHCP client.

Figure 1-3 shows the TCP/IP properties sheet for a Windows 2000 computer, where TCP/IP related settings are configured.
Although TCP/IP is Windows 2000’s default protocol and is necessary for Internet connectivity, in the business world there are sometimes reasons to use a different protocol stack for LAN communications. One of these is heightened security. If you have internal computers that don’t need Internet connectivity (for instance, the workstations in a department that deals with highly sensitive data), you may wish to run that part of the internal network on IPX/SPX. Then even if those computers are also connected to a server that has both TCP/IP and IPX/SPX running, outsiders using TCP/IP will not be able to access the internal systems whose only protocol is IPX/SPX (NWLink).

TCP/IP Components For the Networking Infrastructure exam, it will be important that you recognize the roles played by the major TCP/IP protocols that work at the Transport and Network layers of the networking model to get data packets to the proper destination in a reliable manner. These include TCP and UDP (the User Datagram Protocol) at the Transport layer, and IP at the Network layer:

- **Transmission Control Protocol (TCP)** The “mission” of TCP is to ensure reliable transfer of data. TCP is called a “connection-oriented” protocol because it establishes a virtual connection between the sending and receiving computers before sending data. A connection-oriented protocol such as TCP offers better error control, but its higher overhead means a loss of performance. TCP is also known as a “reliable” protocol because it requires an acknowledgment that the data sent was in fact received. If no acknowledgment (referred to as an ACK) arrives, TCP re-sends that data packet.

- **User Datagram Protocol (UDP)** Like TCP, UDP works at the Transport layer of the OSI model. Unlike TCP, it is a “connectionless” protocol, which means that although it suffers in the reliability department, it is faster because it is unhampered by error-checking duties. UDP is used for messages that don’t require high levels of reliability.

- **Internet Protocol (IP)** At the Network layer, IP is responsible for actually getting the data packets to the correct destination. You could think of IP as the “navigational” protocol, since it maps out the route that will be taken over the network from sending to receiving computer. IP uses logical, assigned IP addresses (see IP Addressing Schemes later in the chapter) to perform both simple and complex routing functions.
Chapter 1: Introduction to Implementing and Administering a Windows 2000 Network

TCP/IP Application Layer Protocols  The TCP/IP suite consists of much more than just TCP/UDP and IP. There is a whole collection of Application layer protocols as well as utilities that can be used for monitoring, troubleshooting, and information gathering. You will need to know the functions of these, including:

- **File Transfer Protocol (FTP)**  The File Transfer Protocol is used for copying files from one computer to another. Windows 2000 includes both a command-line FTP client program and the FTP server service that is installed as part of Internet Information Server 5.0. The Trivial File Transfer Protocol (TFTP) is a connectionless version.

- **Simple Network Management Protocol (SNMP)**  The Simple Network Management Protocol provides a way to gather statistical information. An SNMP management system makes requests of an SNMP agent, and the information is stored in a Management Information Base (MIB). The MIB is a database that holds information about a networked computer (for example, how much hard disk space is available).

- **Telnet**  Telnet is a TCP/IP-based service that allows users to log on to, run character-mode applications, and view files on a remote computer. Windows 2000 Server includes both Telnet server and Telnet client software.

- **Simple Mail Transfer Protocol (SMTP)**  The Simple Mail Transfer Protocol is used for sending e-mail on the Internet. SMTP is a simple ASCII protocol and is non-vendor specific.

- **HyperText Transfer Protocol (HTTP)**  The HyperText Transfer Protocol is perhaps the most familiar of the Application layer protocols, since it is used on the World Wide Web—the most popular of Internet services. HTTP is the protocol that allow computers to exchange files in various formats (text, graphic images, sound, video, and other multimedia files) via client software called a Web browser. A computer running a Web server program, such as Microsoft’s Internet Information Server, stores files in HyperText Markup Language (HTML) format that can be accessed by the client browser. These HTML “pages” often contain hyperlinks for quickly and automatically connecting to other files on the Internet, on an intranet, or on the local machine.

- **Network News Transfer Protocol (NNTP)**  The Network News Transfer Protocol is used for managing messages posted to private and public
newsgroups. NNTP servers provide for storage of newsgroup posts that can be downloaded by client software called a newsreader. Windows 2000 Server includes an NNTP server with IIS, and Outlook Explorer version 5, which is part of the Internet Explorer software included with Windows 2000, provides both an e-mail client and a newsreader.

**TCP/IP Utilities** The following are some of the handy command-line utilities included with the Windows 2000 TCP/IP suite:

- **IPCONFIG** Used to gather information about the TCP/IP configuration on the computer. Typing IPCONFIG at the command line will display the computer's IP address, subnet mask, and default gateway. Adding the /all switch will display additional information such as the host name, MAC address, node type, and much more.

- **NETSTAT** Used to display protocol statistics and current TCP/IP network connections.

- **NBTSTAT** Used to display the local NetBIOS name table, a table of NetBIOS names registered by local applications, and the NetBIOS name cache, a local cache listing of NetBIOS computer names that have been resolved to IP addresses.

- **NSLOOKUP** Used to check records, domain host aliases, domain host services, and operating system information by querying DNS servers.

- **ROUTE** Used to display or make modifications to the local routing table.

- **TRACERT** Used to trace the route a packet takes to a destination.

- **PING and PATHPING** Used to verify configurations and test IP connectivity by name or IP address. PATHPING combines features of PING and TRACERT with added functionality, and is used to trace the route a packet takes to a destination and display information on packet losses for each router in the path. PATHPING can also be used to troubleshoot Quality of Service (QoS) connectivity.

- **ARP** Used to display and modify the Address Resolution Protocol (ARP) cache.
IP Addressing Schemes

In addition to the protocols themselves, another important component of the infrastructure of a TCP/IP-based network is the addressing scheme used by IP to ensure that data transmissions reach the proper destination.

Version 4 of the Internet Protocol (IPv4), the current implementation, uses 32-bit binary addresses, which are expressed in most cases as their equivalent in “dotted decimal,” the familiar four-octet format (such as 192.168.1.45). This is also sometimes referred to as “dotted quad” because there are four groups of digits separated by dots.

IP Address Assignment

Address assignment—both manual assignment in which an administrator individually configures the TCP/IP properties of each computer on the network and automatic addressing methods such as DHCP and NAT—must be understood and mastered in order to work with TCP/IP. An administrator also needs to understand the “internals” of IP, how the logical addresses assigned at this level are mapped to the physical (Media Access Control) addresses that are ultimately used to get the data to its intended destination.

This means you need to know about protocols such as ARP (the Address Resolution Protocol) and RARP (Reverse ARP) and how they work.

Windows 2000 includes some new features that pertain to IP addressing, as well. Automatic Private IP Addressing (APIPA), which allows a DHCP client computer that is unable to find a DHCP server to assign itself a temporary address, and the auto addressing used by Internet Connection Sharing (ICS) are likely to be subjects of exam questions as well.

You should also be aware of the differences between “classful” and “classless” IP addressing, and know the default subnet masks for the common network classes, as shown in the following reference.

### SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>Question</th>
<th>Default Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which default mask should I use for a Class A network?</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>Which default mask should I use for a Class B network?</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>Which default mask should I use for a Class C network?</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
The Dynamic Host Configuration Protocol (DHCP), derived from BOOTP, allows a server computer configured to be a DHCP server to automatically assign IP addresses from a specified pool to client machines that are configured to be DHCP clients.

The Windows 2000 implementation of DHCP includes new functionality, such as integration with DNS, better logging, the ability to create multicast scopes, detection of “rogue” (unauthorized) Windows 2000 DHCP servers, and support for automatic client configuration via APIPA.

### FROM THE CLASSROOM

**IP Addresses vs. Media Access Control Addresses**

Don’t confuse the IP address, used at the Network layer by IP, with the Media Access Control address used to identify each network interface at the lower levels of the OSI model. The IP address is a “logical” address, assigned by the network administrator. It bears no direct relation to the network interface card’s “physical” address (often referred to as the MAC address because it is used at the Media Access Control sublayer of the OSI’s Data Link layer). Changing a computer’s (or more precisely, an individual NIC’s) IP address is a software function. If you have administrative privileges, it’s as simple as clicking the mouse a few times to open the proper dialog box and typing in a new number (the hardest part is knowing what number to type in). The MAC address, on the other hand, is hard-coded into the chip on the network card in the typical Ethernet network. Some network cards provide for a way to change the MAC address via jumper settings or software configuration, but this is not usual and you are limited to only a few possible settings.

—Debra Littlejohn Shinder, MCSE, MCP+I, MCT

**DHCP** The Dynamic Host Configuration Protocol (DHCP), derived from BOOTP, allows a server computer configured to be a DHCP server to automatically assign IP addresses from a specified pool to client machines that are configured to be DHCP clients.

The Windows 2000 implementation of DHCP includes new functionality, such as integration with DNS, better logging, the ability to create multicast scopes, detection of “rogue” (unauthorized) Windows 2000 DHCP servers, and support for automatic client configuration via APIPA.

**IP Subnetting** An important (and, both for network newbies and many experienced administrators, difficult) part of IP addressing is subnetting. This is the art and science of properly dividing a network into smaller connected IP networks (subnets), using a 32-bit number called the subnet mask to indicate the network ID.
Although some study guides and instructors may tell you that all you need to do to pass the IP subnetting portion of the Microsoft exams is to memorize tables defining subnet masks based on number of network and/or host IDs, there is no way to truly understand subnetting without learning to work with binary. Being able to convert dotted decimal addresses and masks to binary and then calculate and perform common operations such as ANDing on the binary digits will give you a big edge in answering subnetting questions on the exams. Not only will you be able to determine the correct answer, you’ll know why it’s correct.

The binary (base two) numbering system may seem confusing if you’ve never worked with anything but our common base ten system. However, you’ll find that it’s really pretty simple once you know the “tricks.” In binary, there are only two digits: 0 and 1. This is particularly appropriate for computer calculations because it’s easy to represent these two digits as electrical impulses or pulses of light—if the current or light is off, that’s a 0, and if it’s on, that’s a one. This is the basis of digital signaling and is also called discrete state signaling.

Using this system, every possible number in our familiar base ten system can be represented by the 0s and 1s. Converting binary to decimal is not difficult, and is a necessary skill for learning IP subnetting, because the “real” numbers that the computer works with (and that you should work with in order to understand the process) are binary, but the software converts them to the “dotted decimal” format for entry into properties boxes.

Of course, the easiest way to convert decimal to binary or vice versa is to use the Windows calculator in scientific mode (choose “Scientific” from the View menu). Just check the “dec” radio button and enter the number in decimal, then click on the “bin” radio button, and tada! As if by magic, you have the binary equivalent.

Microsoft certification exams generally make the Windows calculator available for your use in performing these calculations; however, it is a good idea to know how to convert binary to decimal without the calculator.

The problem with using the calculator is that if you don’t really understand how binary is converted to decimal, you may be confused by the calculator’s results. For instance, when you convert the decimal 1 to binary, the result is 1. Let’s say you are converting the last (rightmost) octet in the IP address 192.168.1.1 to binary.

You know that an octet has eight digits, but the calculator only displays one. Do you put seven zeros before or after the 1? If you know how to do the conversion manually, it’s obvious.
We have eight binary digits, and each of them represents a decimal value, beginning with the rightmost digit and working our way back to the leftmost. Note that the rightmost digits are sometimes referred to as the low order bits, and the leftmost as the high order bits.

Each bit that is “turned on” (that is, shows a 1 instead of a 0) represents the value of that bit as shown in Figure 1-4. As you can see, the value increases by a power of 2 as you move from right to left. A bit that is “off” (represented by a 0) counts as 0. All we have to do then is add up the values of the bits that are “on.”

You can use this simple formula to convert an octet in binary form, such as 10111001, to decimal. To do so, start at the right and look at which digits are turned on. We see that the bits represented by ones have decimal values of 1, 8, 16, 32, and 128. If we add up those values, we get a total of 185 for the octet, which matches with the value we get when we use the scientific calculator to convert 10111001 to decimal.

Another way of seeing how this is done when you’re first learning how to convert to binary is to “line” up the numbers in three columns like this:

\[
\begin{align*}
128 \times 1 &= 128 \\
64 \times 0 &= 0 \\
32 \times 1 &= 32 \\
16 \times 1 &= 16 \\
8 \times 1 &= 8 \\
4 \times 0 &= 0 \\
2 \times 0 &= 0 \\
1 \times 1 &= 1 \\
\end{align*}
\]

Then add up the number in the last column, which in this case is 185.
Chapter 1: Introduction to Implementing and Administering a Windows 2000 Network

If all bits in an octet are “off,” the decimal value is 0, and if all are “on,” the value (total of 1, 2, 4, 8, 16, 32, 64, and 128) is 255.

The intricacies of subnet masking will be covered in chapter 6, “Installing, Configuring, Managing, Monitoring, and Troubleshooting Network Protocols.”

Name Resolution Services

Another very important component of a networking infrastructure is name resolution. Why is this important? Because computers and humans are inherently different. The machines can only recognize and work with numbers (and only binary numbers, at that). To your computer, another system on the network with which it communicates is identified by numbers. We human beings are more comfortable if we can use “friendly names” to identify computers, Web sites, and other network resources that we wish to access.

A good example of this occurs when you browse the Web. If you want to access Microsoft’s Web site, you type www.microsoft.com into your browser’s URL box. Imagine having to remember, instead, the IP address 207.46.130.14—or worse yet, the binary form of that: 11001111 00101110 10000010 00001110—and having to type that in each time you wanted to go to the Microsoft site.

Well, without some form of name resolution, we would be stuck with keeping track of at least the dotted decimal version of all those Web sites. Incidences of Web addiction might decrease, but it would certainly make for a more frustrating user experience. Name resolution services, such as the Domain Name System service (DNS) and the Windows Internet Name Service (WINS), allow you to use friendlier names while they take over the task of getting those names converted into an IP address that the computer can use.

One of the most common problems that network support personnel are called on to deal with is the case of the user whose Web browser “doesn’t work”; that is, he or she isn’t able to access Web pages by typing the URL into the address box. If you find that the browser will bring up the Web site when you type in its IP address instead of the “friendly name,” you can be almost certain the culprit is a DNS problem. Either the DNS server is down, or if the client machine is using manual IP addressing, there is no DNS server address set in its TCP/IP properties.
DNS and WINS servers are machines that maintain databases matching up names to IP addresses, and accept queries from other machines on the network that need this information. Think of them as similar to the directory assistance service provided by your phone company; if you know the person’s name but not his phone number, you call up and query directory assistance and then you can connect directly (by calling) to the person with whom you want to communicate.

DNS and WINS work similarly, but deal with different types of names. DNS resolves fully qualified domain names (also referred to as FQDNs) to IP addresses. These are the “dotted” or hierarchically structured names such as those used for Web sites. WINS resolves NetBIOS names, used by Windows operating systems prior to Windows 2000 and by many applications, to IP addresses. These are “flat” names, such as COMPUTER12 (the same computer’s DNS name might be computer12.mydomain.com).

**DNS** The certification exams will expect you to know not only the theory behind DNS, but—because the Windows 2000 exams are performance-based—how to install and configure a DNS server and how to set up DNS clients, as well as how to troubleshoot problems that occur in the DNS name resolution process.

The DNS in Windows 2000 is dynamic (thus the term Dynamic DNS or DDNS). Unlike the DNS service in Windows NT 4.0, which had to be manually updated, the Windows 2000 DDNS database supports a new specification to the DNS standard for dynamic update. This permits hosts that store name information in DNS to dynamically register and update their records in zones maintained by DNS servers that can accept and process dynamic update messages.

In Windows 2000, DNS can be integrated with the Active Directory, making for more efficient replication of the DNS records. The certification exam is likely to focus heavily on planning the DNS namespace for a Windows 2000 network, and you will be expected to know how to monitor and troubleshoot the DNS service, and how DNS interacts with such new features as Network Address Translation (NAT).

You will also need to understand how a DNS server deployment is planned and implemented, and the different types of DNS servers. The following scenario and solution is a handy summarization of the server types and how you would use each in real world networking situations.
Despite the fact that Windows 2000 provides for the eventual decommissioning of WINS and disabling of NetBIOS, Microsoft obviously has not counted WINS out yet. In fact, many improvements have been made to the service in Windows 2000. Because in the “real world,” the majority of networks will still be using NetBIOS for some time to come, the Networking Infrastructure exam will expect you to know how to configure WINS servers and clients, how WINS replication works, and how to use the MMC to manage the service.

Enhancements to WINS in Windows 2000 include

- **Persistent connections** Now you can configure each WINS server to maintain a persistent connection with one or more of its replication partners. This will increase the speed of replication and do away with the overhead involved in opening and terminating connections.
Manual tombstoning  Windows 2000 allows you to manually mark a record to eventually be deleted (this is called tombstoning). The tombstone state of the record replicates to other WINS servers, and this prevents any replicated copies of the deleted records from reappearing at the same server where they were originally deleted.

Better management utility  WINS is now managed through the MMC. This provides you with a powerful and more user-friendly environment that can be customized for better efficiency. The new MMC-based utilities are easier to use and operate more predictably, as they follow a common design.

Easier configuration of features  Several of the WINS features from earlier versions of Windows NT Server that required editing of the Registry to configure can now be configured more easily and directly. These include the ability to block records by a specific owner or WINS replication partner (formerly known as Persona Non Grata), or allow override of static mappings (formerly known as Migrate On/Off).

Better filtering and search of records  Improved filtering features and new search functions allow you to locate records more easily, by displaying only those that fit the criteria you specify.

Dynamic record deletion and multi-select  The WINS MMC snap-in allows you to point, click, and delete one or more WINS static or dynamic entries. (In NT, you had to use command-based utilities, such as Winscl.exe, to accomplish this). Windows 2000 also makes it possible to delete records that use names based on nonalphanumeric characters.

Record verification and version number validation  You can now check the consistency of names stored and replicated on your WINS servers quickly and easily. Record verification compares the IP addresses returned by a NetBIOS name query of different WINS servers. Version number validation examines the owner address-to-version number mapping tables.

Export  Using the Export feature, you can place WINS data in a comma-delimited text file and then export this file to Microsoft Excel or similar programs for analysis and reporting purposes.

More and better fault tolerance for clients  WINS clients running Windows 2000 or Windows 98 can now specify more than two WINS servers (up to a maximum of 12 addresses) per interface. This provides fault tolerance, as the extra WINS server addresses are used only if the primary and secondary WINS servers fail to respond.
Dynamic reinsertion of client names  WINS clients in Windows 2000 don’t have to be restarted after they use WINS to force reinsertion and update of local NetBIOS names. There is a new option available in the Nbstat command, –RR, that provides the means of doing this. The –RR option can also be used with WINS clients that are running Windows NT 4.0, updated to Service Pack 4 or later.

Read-only feature on the WINS console  You can add members to a special group, the WINS Users group, which is automatically added when WINS is installed, and provide read-only access in the WINS console to WINS-related information on the server for members of the group. This way you can allow non-administrators to view WINS-related information, but they cannot make changes.

Command-line WINS administration tools  Although Windows 2000 Server includes a full graphical user interface for managing WINS servers, there is also a fully equivalent WINS command-line based tool for those who prefer to work at the command line.

Better WINS database engine  WINS in Windows 2000 uses the same performance-enhanced database engine technology that is used in Active Directory.

Remote Access
The remote access service is another very important component of the Windows 2000 networking infrastructure. Remote access is becoming a more and more common way of connecting to the enterprise network, as well as being used by home users and small businesses to connect to an Internet Service Provider (ISP) to gain access to Internet resources.

A remote access connection most typically uses common telephone lines and modems to establish a temporary, dial-in connection to a server. Windows 2000 also supports a second type of RAS connection, via virtual private networking (VPN). A remote access node (a node is a computer or device on the network) is able to function in the same way as a computer that is physically cabled to the network onsite, except that the connection will generally be slower. Windows 2000’s RRAS (Routing and Remote Access Services) provides for a robust and easy-to-use remote access server service, as well as the ability to function as an RAS client.
For the exam, you will need to understand the basic concepts of remote access, and be familiar with the WAN protocols used to establish a remote link. The same network/transport protocols used on your LAN (TCP/IP, IPX/SPX, NetBEUI) can be used with RAS, but another protocol, which operates at the Data Link layer, is required for the wide area part of the connection. Windows 2000 supports the same two WAN link protocols (also sometimes referred to as “line protocols”) as Windows NT 4.0:

- **PPP**  The Point to Point Protocol (PPP) can be used by a Windows 2000 machine acting as an RAS client or by a Windows 2000 remote access server. PPP is the most popular of the wide area link protocols, and supports encryption, compression, and dynamic IP address assignment.

- **SLIP**  The Serial Line Interface Protocol (SLIP) is an older WAN link protocol that does not support encryption or compression, and requires a manually configured static IP address. It can be used only on the Windows 2000 RAS client, and is used now primarily to connect to remote servers running the UNIX operating system.

**Be sure that, for the exam, you know the two supported WAN link protocols and the features and functions of each, as well as the two types of RAS connections supported by Windows 2000.**

Because the Windows 2000 exams are performance-based, you will also be expected to know the procedural steps in creating and configuring a dial-up or VPN connection. This is done through the Network and Dialup Connections applet, accessed via Settings from the Start menu. As with many other configuration processes, Windows 2000 provides you with a wizard that walks you through the steps of setting up your new connection.

**IP Routing**

Routing refers to the process of forwarding computer communications traffic along the pathways of an internetwork (a network of networks). A computer set up to support routing receives transmitted messages and forwards them to their correct destinations over the most efficient available route, even if many routes are possible. The distance traveled from one router to the next is called a hop, and at each router, the destination IP address on the packet is compared to the routing table, and the best route is used to decide the endpoint of the next hop.
Fast, efficient, reliable routing of data is at the heart of all large networks, up to
and including the global Internet.

IP routing can be done by specialized dedicated devices called routers, or by
a computer whose operating system supports IP forwarding. Windows 2000 is
designed to function as an IP (or IPX) router.

A router is also often referred to as a gateway. When an exam question
mentions the “default gateway,” it means the router (or computer functioning
as a router) that serves as the “way out” of the network or subnet for sending
of data to other networks. A network interface can have only one active default
gateway at a time, although multiple gateways can be configured in Windows
2000 for fault tolerance purposes. Be aware that the term “gateway” is also
used to refer to software that translates between protocols and connects
networks of different types, such as connecting a Windows PC network to an
IBM mainframe (SNA gateway) or to a NetWare network (Gateway Services
for NetWare).

Be aware for exam purposes that there are two basic types of routing: static
and dynamic.

**Static Routing**  Static routing requires that an administrator manually construct
a routing table, which contains the pathways to outside networks.

You should know how to use the ROUTE utility at the command line to view
the routing table and manually add, delete, and modify routing table entries. Be
familiar with the switches shown in Table 1-1.

<table>
<thead>
<tr>
<th>Switch or Command</th>
<th>Action</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>Clears all gateway entries from the routing table.</td>
<td>Can be used with other commands to clear the table before invoking the action of the other command.</td>
</tr>
<tr>
<td>-p</td>
<td>Creates a persistent route.</td>
<td>Is used with the ADD command. Causes the entry to stay in the table when the computer is restarted.</td>
</tr>
</tbody>
</table>
Dynamic Routing

Dynamic routing uses routing protocols such as the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) to allow routers to communicate with one another and automatically, dynamically update their routing tables without human intervention.

You should know that Windows 2000 supports the following routing protocols:

- **RIPv1**
- **RIPv2**
- **OSPF**

RIP is known as a *distance vector protocol*. This means that it has a maximum path length of 15 hops. If a packet must pass through more than 15 routers (gateways) to reach its destination, RIP considers the destination “unreachable.” Another drawback of these protocols is that they are vulnerable to routing loops. RIP and the other distance vector protocols were designed for use in moderately sized networks, not for huge internetworks. However, RIP is a well-established standard and offers many...
advantages over static routing. Link state protocols are more efficient, and scale better than distance vector protocols, but they are also more complex.

OSPF belongs to a different group, the link state protocols. This type of protocol maps the network and updates the mapping database (called the link state database) whenever any changes are made to the network. Link state protocols are more efficient but more complex than distance vector protocols.

The Microsoft exams will expect you to know the differences between these protocol types, and how to add and configure the protocols. This is done through the Routing and Remote Access management console, as shown in Figure 1-5.

Configuring both static routing tables and the dynamic routing protocols will be covered in more detail in chapter 9, “Installing, Configuring, Managing, Monitoring, and Troubleshooting IP Routing.”

The Security Infrastructure

Network security is a big concern to almost all network administrators today, in light of the growing popularity of “hack attacks” from outsiders, the increasing computer savvy of employees at all levels, and the amount and types of data that are stored on networked systems. Trade secrets, confidential client information, and other sensitive
information lives on the hard disks of company networks and must be protected from both malicious and accidental access by unauthorized persons.

Microsoft has made many improvements to the security components in Windows 2000. In fact, security is such an integral factor in many of the new features, such as Active Directory and RRAS, that it is difficult to define it separately.

Windows 2000 security features include the following:

- Kerberos authentication
- IP Security (IPSec)
- Much improved policy management (Group Policy)
- Enhanced certificate services
- Encrypting File System (EFS)
- Secondary Logon
- Security Configuration Toolset
- Smart card support

Although the security-related topics will be covered in depth in the elective Exam 70-220, Designing Security for a Microsoft Windows 2000 Network, you will be expected to know about some of the basic security options for the Networking Infrastructure exam.

Exam 70-216 specifically covers topics pertaining to Certificate Services and installation and configuration of Certification Authority. You should get hands-on practice in setting up CA and issuing and revoking certificates prior to taking this exam.

CERTIFICATION OBJECTIVE 1.02

Overview of Exam 70-216

For a list of the learning objectives for Exam 70-216, see the Microsoft Web site at www.microsoft.com/mcp/exam/stat/SP70-216.htm. The objectives are somewhat broad, and you’ll note that they are performance-based. This does not mean that you don’t need to know any of the theory behind the concepts being tested. It does
mean that *only* knowing the theory, without having ever put it into practice by working with the operating system, will make it difficult or even impossible for you to pass the exam.

The objectives are divided into logical categories that include all the general topics discussed earlier. More specifically:

- **DNS** For the DNS exam objective, you will need to be familiar with the installation procedure, how to configure the service, best practices for managing DNS/DDNS in a Windows 2000 network, how to monitor DNS performance, and basic troubleshooting of common DNS problems. Specifically, you’ll need to know what a root server is and how to configure one, the function of zones and how they are configured (including for dynamic updates), how to set up the DNS client computer, and how to configure a DNS server to be caching-only. You’ll also need to know how to implement a delegated DNS zone and how to manually create resource records.

- **DHCP** In relation to DHCP, you must be familiar with installation, configuration, management, monitoring, and troubleshooting principles. You should pay particular attention to installing the DHCP Server Service, and practice creating and managing scopes, superscopes, and multicast scopes. You will need to know how DHCP is integrated with DNS and be able to authorize a DHCP server in Active Directory.

- **RAS** For the Remote Access Services (RAS) portion of the exam, you’ll need to know how to configure inbound connections and how to set remote access policies and configure profiles. You should also focus on configuring multilink connections and how to set up a virtual private network (VPN). Finally, you should know how DHCP is integrated with RRAS.

- **Network Protocols** Expect TCP/IP to be an important part of this exam, now that there is no separate exam on the topic. You should know how to install and configure it, how to configure TCP/IP packet filtering, and how to manage and monitor network traffic using Network Monitor and other tools. Be sure you understand the fundamentals of protocol security and have hands-on practice in enabling IPSec and configuring it for both transport and tunnel modes, as well as customizing IPSec policies and rules and managing and monitoring it. Also in relation to networking protocols, familiarize yourself with the installation and configuration of NWLink (IPX/SPX).
Even though WINS may be “on the way out,” it is still very much alive and well in the first release of Windows 2000, and likely to be the subject of at least a few exam questions. So be sure you know how to install, configure, and troubleshoot WINS, and pay particular attention to WINS replication, management, and monitoring.

Routing Windows 2000 can function as an IP router, and for the exam, you’ll need to know how to configure static routes as well as the dynamic routing protocols in RRAS. Know how to implement demand-dial routing, and how to monitor and manage both border routing and internal routing.

ICS and NAT Internet Connection Sharing and Network Address Translation are new features in Windows 2000 that are sure to come up in exam questions. You should know the difference between ICS (built into both Windows 2000 Professional and Server) and NAT (available only with the Server products), and how to install and configure both.

Security Security is a major concern and has been the focus of many new Windows 2000 features. In fact, there is an elective exam that deals exclusively with security issues. For the Networking Infrastructure exam, you need to be familiar with the Windows 2000 Certificate services, and know how to install and configure Certificate Authority (CA), issue and revoke certificates, and remove the Encrypting File System (EFS) recovery keys.

Although much of the knowledge and skill you may have gained from working with NT in the past is transferable to Windows 2000, it is imperative that you not make assumptions that similar tasks are accomplished in the same way in Windows 2000. Nothing substitutes for hands-on experience using the operating system.
Chapter 1: Introduction to Implementing and Administering a Windows 2000 Network

certification objectives are written almost exclusively as performance-based statements. We know that in order to really understand what you’re doing, you need to know the theory behind it. If you have many long years of on-the-job experience working with NT, and have worked a great deal with extra add-on software and third-party products, you may already be familiar with the concepts behind these task-oriented objectives. Otherwise, it will benefit you to read the explanatory text carefully as well as performing the exercises in each chapter.

Knowledge

In the beginning of each chapter, we will try to provide you with a foundation of knowledge upon which conceptual comprehension and practices skills can be built. This includes definitions of new terms, explanations of processes, and discussion of relationships between components.

Topic Tie-ins

We will cross reference subjects that appear elsewhere in the book that tie in to the topic of the chapter and/or that will aid you in understanding the material to be presented in the chapter.

Concepts

In addition to basic knowledge-based information such as definitions and relationships, we will provide an overview of the concepts behind the skills-based exercises. For example, setting up a WINS server involves a skill set. The concept of WINS—resolution of NetBIOS names to IP addresses and why this needs to be done—is not absolutely necessary in order to perform the task, but will certainly be helpful to you in making configuration decisions.

The authors will attempt to make all abstract concepts as easy to understand as possible, using analogies and graphical illustrations.

Practical Skills

The heart of Windows 2000 exam preparation is development of practical skills—the ability not just to know about the operating system, but also to use it to perform
common network administration tasks. The exams are performance-based, as is obvious from the wording of the exam objectives, almost all of which use action verbs such as “configure, install, monitor, troubleshoot, manage, create, remove, implement” and the like.

More so than with the NT exams, it is imperative that you do the practical exercises in each chapter, experiment with various settings and options, and get hands-on experience in performing the tasks about which you read.

Many of the exam questions will be relatively simple for those who have worked with the product, and almost impossible to answer for someone who hasn’t gone through the processes themselves. In this book, we attempt to simulate the Windows 2000 working environment as much as possible by liberal use of screenshots and detailed descriptions of what to expect in response to particular actions or commands; however, there is no substitute for doing it yourself.

CERTIFICATION OBJECTIVE 1.04

Networking Terminology

For those who are beginning their study of Windows 2000 with little exposure to real-life networking, one of the most important (and perhaps most tedious) tasks is to “learn the language” of computer networking. At times, as you read through the study material, you may feel as if you’re floating in a sea of acronyms and unfamiliar words.

In this book, our policy is to spell out all acronyms in full the first time they appear, and to define new terms within the text whenever possible. However, what’s a well-known term to a networking professional may be “new” to you, and in a book this size, trying to flip back through the pages to find the first occurrence of a word could be a time-consuming process.

We suggest that you make liberal use of the Glossary. If you run across a word or term whose meaning you’re not sure of, and that’s not obvious from the context, don’t just skim over it and hope it will be clarified later. Taking the time to look it up may seem to slow down your study, but it’s one of the best ways to ensure that you remember the meaning later.
“Double Meanings”

Don’t despair if you find that definitions are not always absolutely consistent from one source to the next. Within the computer industry and even within the more narrowly defined networking world, there are many subspecialty areas that have their own brand of jargon.

For example, you may hear the word “segment” used to describe a length of cable, or the parts of the network connected to a length of backbone cable. You will hear the same word used, in discussions of TCP/IP, to describe the “chunks” into which data is broken down to be transmitted across the network. Likewise, “cell” means one thing in the context of wireless communications, and something else when discussing ATM technology.

The following scenario and solution lists some of these more confusing “double meanings” that you are likely to encounter in your studies of networking infrastructure fundamentals.

SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>What is a segment?</th>
<th>In discussions of the physical networking infrastructure, “segment” usually refers to a length of cable, or the portion of the network connected to a length of backbone cable between repeaters. In TCP/IP terminology, “segment” is the term used to describe the chunk of data sent by TCP over the network (roughly equivalent to the usage of “packet” or “frame”).</th>
</tr>
</thead>
<tbody>
<tr>
<td>I see the acronyms DN, DNM, DNS, and DDNS? What does it all mean and what, if any, is the relationship between them?</td>
<td>DN, in Active Directory parlance, stands for Distinguished Name, an LDAP way of uniquely identifying an object. A DNM is a Domain Naming Master, one of the operations master roles played by domain controllers in a Windows 2000 network. DNS is Domain Name System, used to map fully qualified domain names to IP addresses. Dynamic DNS is the enhanced version used in Windows 2000. In the Networking Infrastructure exam, this last is the one you are more likely to encounter. The only relationship is their common status as components of Windows 2000. DNS will be familiar to NT 4.0 administrators; the others may not be.</td>
</tr>
<tr>
<td>What does PVC mean?</td>
<td>In discussing the physical networking infrastructure, PVC refers to polyvinyl chloride, the material out of which standard Ethernet cable is made. In discussions of networking concepts, PVC is used to mean Permanent Virtual Circuit, referring to a network pathway in which all packets follow the same route (as opposed to a switched virtual circuit).</td>
</tr>
</tbody>
</table>
CERTIFICATION OBJECTIVE 1.05

For “Newbies” and “Old Pros”

For those who are new to the world of networking, this chapter will contain a section that provides background information that, although not specifically covered by the Windows 2000 exam objectives, is essential to understanding the chapter topic(s). And for experienced administrators, there will be special tips for NT pros, pointing out the areas in which Windows 2000 differs (subtly or drastically) from its predecessor, and warning you of common pitfalls that you may encounter in making the transition to Microsoft’s new way of doing things.

For Networking Newbies

If you are new to computer networking, we recommend that you take a course or study a good book in basic networking concepts. Even if you are following the Windows 2000 MCSE certification track, it would benefit you to study one of the NT 4.0 Networking Essentials study guides and/or take the Windows 2000 Network and Operating Systems Essentials course.

SCENARIO & SOLUTION

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why does the word “gateway” seem to have two different meanings?</td>
<td>“Gateway” is used in networking to refer to a router or a computer functioning as one, the “way out” of the network or subnet, to get to another network. The word “gateway” is also used in regard to software that connects a system using one protocol to a system using a different protocol, such as the Systems Network Architecture (SNA) software that allows a PC LAN to connect to an IBM mainframe, or the Gateway Services for NetWare used to provide a way for Microsoft clients to go through a Windows NT or Windows 2000 server to access files on a Novell file server.</td>
</tr>
<tr>
<td>What’s the difference between OSI, ISO, and IOS?</td>
<td>OSI stands for Open Systems Interconnection and is used in all standard basic networking texts and classes in regard to the OSI layered networking model. The ISO is the organization that created this and other international standards; its name is the International Organization for Standardization and its short form, ISO, is not really an acronym but a derivative of a Greek word. IOS is the dedicated operating system used by Cisco routers.</td>
</tr>
</tbody>
</table>

Why does the word “gateway” seem to have two different meanings?

“Gateway” is used in networking to refer to a router or a computer functioning as one, the “way out” of the network or subnet, to get to another network. The word “gateway” is also used in regard to software that connects a system using one protocol to a system using a different protocol, such as the Systems Network Architecture (SNA) software that allows a PC LAN to connect to an IBM mainframe, or the Gateway Services for NetWare used to provide a way for Microsoft clients to go through a Windows NT or Windows 2000 server to access files on a Novell file server.

What’s the difference between OSI, ISO, and IOS?

OSI stands for Open Systems Interconnection and is used in all standard basic networking texts and classes in regard to the OSI layered networking model. The ISO is the organization that created this and other international standards; its name is the International Organization for Standardization and its short form, ISO, is not really an acronym but a derivative of a Greek word. IOS is the dedicated operating system used by Cisco routers.
You will find that familiarizing yourself with basic networking concepts—such as physical topologies, characteristics of different cable and other media types, the popular networking architectures such as Ethernet, AppleTalk, and Token Ring, and often-referenced networking standards and models such as the OSI, DoD, and Windows models and the IEEE 802 specifications—will benefit you in many ways. Not only will the knowledge provide a solid foundation for the material you will be studying in the process of obtaining Microsoft certification, but most employers will expect you, as an MCP or MCSE, to recognize these fundamental concepts.

The very best investment a networking neophyte can make, though, is that of building your own network from the ground up. Even a simple two-computer thinnet network will give you a taste of the challenges faced by Enterprise pros in the field, and many of the setup, maintenance, and troubleshooting scenarios associated with large production networks can be simulated on a smaller scale with a small home network.

There are a number of excellent books, as well as numerous Web resources, available to guide you through the challenging experience of getting those first two computers to “talk” to one another.

For NT Pros

If you are already certified and/or experienced in NT 4.0, you may be able to skip some parts of this book that provide basic information about protocols and services with which you are already familiar. But don’t skip too much! Windows 2000 is built on the NT kernel and you will find much in the new operating system that feels like “home”—but you will also discover, as you delve deeper, that there are many fundamental changes, even to “old friends” like DNS and WINS.

NT professionals will need to guard against the possibility that your experience and mastery of the earlier operating system will be your biggest enemy on the Windows 2000 certification exams. Expect questions that try to “trick” you by providing solutions that would have been correct if you were using NT, which measure whether you’re aware of the differences between the two operating systems (just as there were traditionally questions on the NT certification exams that used a test-taker’s experience with Windows 9x against him in the same way).

We certainly don’t advise NT pros to “forget everything you ever knew” about network operating systems, but we do encourage you not only to study Windows 2000, but to actually use it on a day-to-day basis. If possible, upgrade your primary
workstation to Windows 2000 Professional so that the slightly different ways of performing routine tasks, the subtle differences in the interface, become second nature to you. And work with Windows 2000 Server or Advanced Server—on the job, at home, or in the classroom. It’s in the server products that the real differences between NT and Windows 2000 show themselves.

Your NT experience can put you a step ahead of the networking newcomers—if you remember not to make too many assumptions (generally a good policy to follow in all areas of life).

CERTIFICATION SUMMARY

This chapter has provided a brief introduction to the Windows 2000 certification exam process in general and an overview of the objectives of Exam 70-216, Implementing and Administering a Microsoft Windows 2000 Networking Infrastructure, in particular.

We have discussed some very fundamental concepts of Microsoft networking, such as IP addressing, name resolution, remote access, and security. We have also discussed those specific topics that are the focus of the Networking Infrastructure exam, such as DNS/DDNS, WINS, IP routing, TCP/IP, DHCP, NAT, and Windows 2000 certificate services.

We briefly touched on the importance of mastering common networking terminology, and provided examples of a few common cases of acronyms or terms that may have unclear or dual meanings.

In closing, we addressed the special needs of the two very different audiences who are likely to use this book: the networking novice who is beginning his or her career with the study of Windows 2000, and the networking professional who has experience working in the field with, and may already be certified in, other network operating systems.
TWO-MINUTE DRILL

What Is a Network Infrastructure?

- Microsoft’s “target audience” for the Windows 2000 exams consists of networking professionals with at least one year’s experience; this does not mean you can’t pass the exams without that experience, but it does mean you will need to do more hands-on practice with the operating system.

- The Windows 2000 exams will involve questions that require a higher cognitive level to arrive at the correct solution; most questions will be performance-based rather than purely knowledge-based.

- A computer network has both a physical and a logical infrastructure. The former consists of hardware components; the latter is software-based and includes protocols and services upon which network communications depend. Exam 70-216 focuses on the components of the logical infrastructure.

- The TCP/IP protocol suite, on which most of today’s medium-to-large networks (including the Internet) run, is an important component of the logical networking infrastructure, and a good understanding of how it works will be essential to passing the exam.

- Name resolution is an important component of the infrastructure because it allows “friendly” host names or NetBIOS names to be mapped to IP addresses (and the latter is used by the networking protocol for one computer to communicate with another).

- The Domain Name Service, DNS, maps fully qualified domain names to IP addresses. The Windows 2000 implementation, Dynamic DNS (DDNS) is an essential component of Windows 2000 networks and is likely to be the subject of one or more questions on Exam 70-216.

- The Windows Internet Naming Service (WINS) resolves NetBIOS names to IP addresses. Although WINS plays a lesser role in Windows 2000 networks, Microsoft has made several significant improvements to the service, and the exam will require that you know how to install, configure, manage, monitor, and troubleshoot the service, with a focus on WINS replication issues.
The Dynamic Host Configuration Protocol (DHCP) is used for automatic assignment of IP addresses. Windows 2000’s implementation of DHCP is integrated with DNS, and the ability to install, configure, monitor, and troubleshoot DHCP will be essential skills for passing the Networking Infrastructure exam.

Remote access services in Windows 2000 include the ability to act as both a remote client (using PPP or SLIP) and a remote server (supporting PPP only). Connections can be dial-up or via virtual private networking (VPN), and you should know how to create and configure inbound connections, set up policies and profiles, and utilize multilink capabilities.

IPSec is a new security feature in Windows 2000 that provides end-to-end security of IP packets (including over a VPN connection, if the L2TP tunneling protocol is used). You will need to know how to configure, customize, and monitor IPSec for the exam.

IP routing is fundamental to any medium to large networking environment, and you will need to know, for Exam 70-216, how to install and configure dynamic routing protocols, as well as how to enter static routes in the routing table. You also need to understand the difference between border and internal routers.

Network Address Translation (NAT), a new feature to Windows 2000, allows for the sharing of one Internet connection (or other WAN connection) with other computers on the LAN by mapping private IP addresses to one or more public registered address(es). The exam will expect you to be familiar with installation and configuration of both Internet Connection Sharing (ICS) that is included in both Windows 2000 Professional and Server, and the more full-featured form, called simply NAT, available only in the server products.

One of many security features included in Windows 2000 is its certificate services. For the exam, you will need to know how to install and configure Certificate Authority and how to issue and revoke certificates.
SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all of the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

What Is a Network Infrastructure?

1. Which of the following is the network/transport protocol stack used on most medium and large networks today?
   A. IPX/SPX
   B. NetBEUI/NetBIOS
   C. TCP/IP
   D. DNS/DDNS

2. Which of the following is true of the Dynamic Host Configuration Protocol? (Select all that apply.)
   A. It has been replaced by APIPA in Windows 2000.
   B. It is used to automatically assign IP addresses.
   C. It is derived from BOOTP.
   D. It is a name resolution service.

3. Which of the following is the term used to refer to the IP address of the router or computer functioning as a router?
   A. The Subnet Mask
   B. The Default Gateway
   C. The Network ID
   D. The host ID

4. “A set of rules, or a standardized order of procedures, that the networking components of the systems follow when they transmit data over the network” is the definition of which of the following?
   A. Protocol
   B. Media
   C. Standards
   D. Models
5. Which of the following is a sublayer of the Data Link layer of the OSI networking model? 
(Select all that apply.)
A. Presentation sublayer
B. Media Access Control sublayer
C. Network interface sublayer
D. Logical Link Control sublayer

6. Which of the following pieces of information is required to manually configure the TCP/IP properties of a Windows 2000 client computer’s network interface on a routed network? 
(Select all that apply.)
A. The IP address assigned to the NIC
B. The IP address of the Windows 2000 domain controller
C. The default gateway address
D. The subnet mask

7. Which of the following is the correct default subnet mask for a Class B network?
A. 255.255.255.255
B. 255.255.255.0
C. 255.255.0.0
D. 255.0.0.0

8. Which of the following is a “connectionless” protocol that operates at the Transport layer of the OSI model?
A. UDP
B. TCP
C. IP
D. FTP

9. Which of the following is a dynamic routing protocol supported by Windows 2000? (Select all that apply.)
A. OSPF
B. IOS
C. RRAS
D. RIP
10. Which of the following is a reason to have a secondary DNS server? (Select all that apply.)
   A. DNS servers work only in pairs.
   B. It provides fault tolerance.
   C. It is used for load balancing.
   D. You cannot have a secondary DNS server.

11. Which of the following is a “connection-oriented” protocol that operates at the Transport layer of the OSI model?
   A. UDP
   B. FTP
   C. IP
   D. TCP

12. The term “gateway” is used to refer to which of the following? (Select all that apply.)
   A. A router
   B. A bridge
   C. Software that translates between different protocols
   D. A device that connects different cable types

13. Which of the following is the TCP/IP utility that is used to display the local NetBIOS name table, a table of NetBIOS names registered by local applications, and the NetBIOS name cache, a local cache listing of NetBIOS computer names that have been resolved to IP addresses?
   A. NETSTAT
   B. NBTSTAT
   C. IPCONFIG
   D. TRACERT

14. Which of the following is true of the binary numbering system? (Select all that apply.)
   A. It uses both alpha and numeric characters.
   B. It is a base ten system.
   C. It is a base two system.
   D. It uses 0s and 1s, which are referred to as “bits.”
15. Which of the following is a TCP/IP-based service that allows users to log on to, run character-mode applications, and view files on a remote computer?

A. FTP
B. Telnet
C. HTTP
D. RAS
SELF TEST ANSWERS

What Is a Network Infrastructure?

1. ✓ C. TCP/IP is the protocol of the global Internet and is used by most medium and large (and many small) LANS.
   ✗ A, B, and D are incorrect. IPX/SPX is the protocol stack traditionally used with Novell NetWare networks (although NetWare version 5.0 can run on pure IP). NetBEUI is a protocol used in small workgroups that do not need routing capabilities. NetBIOS is the API on which NetBEUI is based. The Domain Name System, DNS, and its Dynamic version as implemented in Windows 2000, DDNS, are name resolution services, not network/transport protocols.

2. ✓ B, C. DHCP is used to automatically assign IP addresses to computers configured as DHCP clients.
   ✗ A is incorrect. APIPA works in conjunction with DHCP, to allow DHCP clients who can’t find a DHCP server to assign themselves addresses. D is incorrect because DHCP does not resolve names.

3. ✓ B. The address of the router that is used as the “way out” of the network (to send packets to remote networks) is referred to as the default gateway.
   ✗ A is incorrect because a subnet mask is a 32-bit number that identifies which part of an IP address indicates the network ID. C is incorrect because the network ID is that part of an IP address that identifies the network or subnet. D is incorrect because the host ID is that part of the IP address that identifies the individual computer, or host, on the network.

4. ✓ A. This is the definition of “protocol” in the context of computer networking.
   ✗ B is incorrect because media refers to the cable, airwaves, or other way in which messages are transmitted. C is incorrect because standards refer to established criteria followed by vendors, programmers, etc. to ensure compatibility between systems, programs, and components. D is incorrect because models, in networking context, are representations (usually graphical) of a process based on a set of standards.

5. ✓ B, D. The MAC and LLC sublayers make up the Data Link layer of the OSI model.
   ✗ A is incorrect because the Presentation layer is an independent layer in the OSI model, not a sublayer. C is incorrect because the Network Interface layer is a part of the Department of Defense (DoD) model, not part of the OSI model.

6. ✓ A, C, D. The IP address of the NIC whose TCP/IP properties are being configured and the subnet mask are always required for manual configuration. A default gateway address is required if the network is routed.
B is incorrect because you do not need to enter the IP address of the domain controller when you configure a client computer’s TCP/IP properties.

7. C. In a Class B network that is not subnetted, two octets are “masked” to represent the network ID, and the other two are unmasked to represent the Host ID.

A is incorrect because 255.255.255.255 does not represent a valid default subnet mask for any of the network classes. B is incorrect because 255.255.255.0 is the default subnet mask for a Class C network. D is incorrect because 255.0.0.0 is the default subnet mask for a Class A network.

8. A. The User Datagram Protocol (UDP) is the TCP/IP stack’s connectionless transport protocol, which is faster (but less reliable) than TCP.

B is incorrect because although TCP operates at the Transport layer, it is a connection-oriented protocol. C is incorrect because although IP is connectionless, it operates at the Network layer of the OSI model. D is incorrect because FTP is an application layer protocol.


B is incorrect because IOS is the Cisco Systems operating system used by Cisco routers. C is incorrect because RRAS is the Routing and Remote Access Service.

10. B, C. A secondary DNS server has a copy of the zone file, which provides fault tolerance in case the primary DNS server goes down. It also is used for load balancing to take some of the burden of queries off the primary server.

A is incorrect because a single DNS server can work by itself. D is incorrect because you can—but are not required to—have a secondary DNS server.

11. D. TCP, the Transmission Control Protocol, operates at the Transport layer of the OSI networking model and is “connection-oriented.”

A is incorrect because although the User Datagram Protocol operates at the Transport layer, it is a “connectionless” protocol. B is incorrect because FTP is an application layer protocol, and C is incorrect because IP operates at the Network layer.

12. A, C. Routers are referred to as “gateways,” and the router to which packets going outside the local subnet are sent is referred to as the “default gateway.” Software programs such as SNA and GSNW that translate between protocols to connect different types of networks are also called gateways.

B is incorrect because a bridge does not offer a “way out” of the network and is not called a gateway. D is incorrect because a device that merely connects different cable types does not subnet the network and is not referred to as a gateway.
13.  ✔  B. NBTSTAT displays NetBIOS information; the “NBT” stands for “NetBIOS over TCP/IP.
    ✗  A is incorrect because NETSTAT is used to display protocol statistics and current TCP/IP
        connections. C is incorrect because IPCONFIG is used to display general information about
        the TCP/IP configuration, such as IP address, subnet mask, and default gateway. D is incorrect
        because TRACERT is used to trace the route of a packet.

14.  ✔  C, D. Binary is a base two system that uses the two digits 0 and 1 for all calculations. The
        digits are referred to as “bits.”
    ✗  A is incorrect because it is the hexadecimal system that uses alpha and numeric characters.
        B is incorrect because it is the decimal system that is a base ten system.

15.  ✔  B. Telnet is the TCP/IP Application layer protocol that allows users to view files and run
        programs on a remote computer (but does not allow uploading or downloading of files).
    ✗  A is incorrect because FTP is a service that allows users to upload files to or download files
        from an FTP server using FTP client software. C is incorrect because HTTP is the Hypertext
        Transfer Protocol used to access pages on the World Wide Web. D is incorrect because Remote
        Access Service (RAS) is used to establish a dial-up or VPN connection to another computer.