[Previous] [Next]

Chapter 1

Designing a Windows 2000 Network

About This Chapter

In this chapter, you will learn how to plan a Windows 2000 network. In addition, you will learn about important considerations when developing an implementation plan. You will also learn about various network protocols used by Microsoft Windows 2000, and how they relate to network services.

Before You Begin

To complete this chapter, you must have

- There are no prerequisites for this chapter.

[Previous] [Next]

Lesson 1: Network Services Overview

Microsoft Windows 2000 provides many network features and services that can be used by your organization to meet your business objectives. Windows 2000 includes key technologies that add value to both new and existing networks. Some technologies must be implemented on your network in order to use certain services. For example, Transmission Control Protocol/Internet Protocol (TCP/IP) must be installed in order to implement the Windows 2000 Active Directory service.

This lesson introduces the following Windows 2000 network services:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Windows Internet Name Service (WINS)

You will also learn about remote networking with the Routing and Remote Access feature of Windows 2000 service. This includes features such as network address translators (NATs). You will also learn how security is implemented using Microsoft Certificate Services.

> **After this lesson, you will be able to**
>
> - Explain the purpose of DNS, DHCP, and WINS
> - Describe the Routing and Remote Access Service

- Describe the benefit of a network address translator (NAT)
- Identify the features of Microsoft Certificate Services

Estimated lesson time: 40 minutes

TCP/IP

There are many networking protocols supported in Windows 2000; however, TCP/IP is the core protocol used in Windows 2000, and is the default networking protocol installed by Windows 2000 Setup. Many networking services in Windows 2000 use TCP/IP, and some services, such as Internet Information Server (IIS) and Active Directory, require it to be installed. TCP/IP is a routable protocol used by many wide area networks (WANs) and the Internet. Other protocols, such as NetBEUI (NetBIOS Enhanced User Interface), are designed only for local area networks (LANs) and thus do not support Internet connectivity. This issue is important to consider when planning your network.

Domain Name System

Although TCP/IP uses Internet Protocol (IP) to locate and connect to hosts (computers and other TCP/IP network devices), users typically prefer to use friendly names. For example, users prefer the name ftp.microsoft.com, instead of its IP address, 172.16.23.55. Domain Name System (DNS) enables you to use hierarchical, friendly names to easily locate computers and other resources on an IP network.

DNS is used on the Internet to provide a standard naming convention for locating IP-based computers. Before the implementation of DNS, a Hosts file was used to locate resources on TCP/IP networks including the Internet. Network administrators entered names and IP addresses into the Hosts file, and computers used the file for name resolution.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) simplifies administrating and managing IP addresses on a TCP/IP network by automating address configuration for network clients. A DHCP server is defined as any computer running the DHCP service. Windows 2000 Server provides the DHCP Server service, which enables a computer to function as a DHCP server and configure DHCP-enabled client computers on your network. This architecture is illustrated in Figure 1.1.

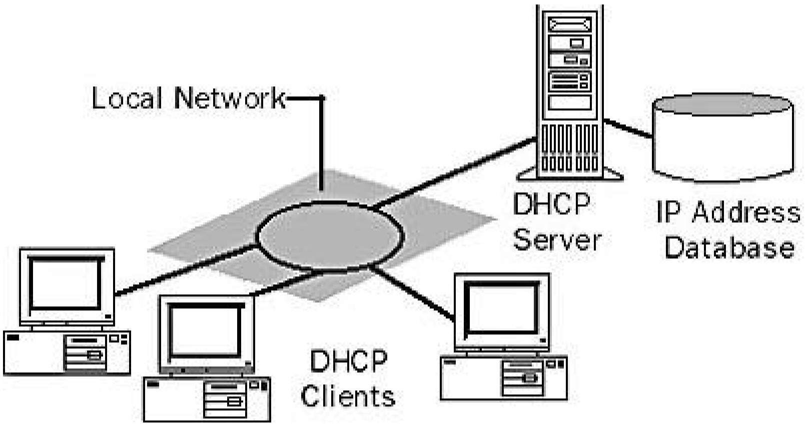


Figure 1.1 *The basic DHCP model*

The DHCP Server service for Windows 2000 also provides

- Integration with the Microsoft Active Directory directory service and DNS
- Enhanced monitoring and statistical reporting
- Vendor-specific options and user-class support
- Multicast address allocation
- Rogue DHCP server detection

Every computer on a TCP/IP-based network must have a unique IP address in order to access the network and its resources. Without DHCP, IP configuration must be done manually for new computers, computers moving from one subnet to another, and computers removed from the network. By deploying DHCP in a network, this entire process is automated and centrally managed.

The DHCP implementation is so closely linked to the Windows Internet Name Service (WINS) and DNS that network administrators will benefit from combining all three when planning deployment. If you use DHCP servers for Microsoft network clients, you must use a name resolution service. Windows 2000 networks use the DNS service to support Active Directory, in addition to general name resolution. Networks supporting Windows NT 4.0 and earlier clients must use WINS servers. Networks supporting a combination of Windows 2000 and Windows NT 4.0 clients should implement both WINS and DNS.

Windows Internet Name Service

Windows Internet Name Service (WINS) is the name resolution system used for Windows NT Server 4.0 and earlier operating systems. WINS provides a distributed database for registering and querying a computer name (which is the same as the NetBIOS name) to IP address mapping in a routed network environment. If you are administering a routed network, WINS is your best choice for NetBIOS name resolution. WINS reduces the use of local broadcasts for name resolution and allows users to easily locate systems on remote networks. In a dynamic DHCP environment, the IP addresses of the hosts can change frequently; WINS provides a way to dynamically register the changes for computer names-to-IP addresses mapping. This feature is necessary for the name-to-IP address resolution to work properly in a DHCP environment.

Name Resolution

Whether your network uses DNS or WINS, name resolution is an essential part of network administration. Although Windows 2000 primarily uses DNS to match host names to IP addresses, Windows 2000 still supports WINS for this purpose.

Name resolution allows you to search your network and connect to resources using names such as "printer1" or "fileserver1" rather than memorizing a host's IP address. Remembering IP addresses would be even more impractical when using DHCP for address assignment because the assignments can change over time. WINS is tightly integrated with DHCP services. Because of this integration, whenever the computer you named "fileserver1" is dynamically assigned a new IP address, the change is transparent. When you connect to fileserver1 from another node, you can use the name fileserver1 rather than the new IP address because WINS keeps track of the changing IP addresses associated with that name.

Remote Access Overview

With the Windows 2000 Routing and Remote Access feature, remote clients are transparently connected to the remote server, known as point-to-point remote access connectivity. Clients can also be transparently connected to the network to which the routing and remote access server is attached. This is known as point-to-LAN remote access connectivity. This transparent connection allows clients to dial in from remote locations and access resources as if they were physically attached to the network. Windows 2000 remote access provides two different types of remote access connectivity:

- **Dial-up remote access.** With dial-up remote access, a remote access client uses the telecommunications infrastructure to create a temporary physical circuit or a virtual circuit to a port on a remote access server. Once the physical or virtual circuit is created, the rest of the connection parameters can be negotiated.

- **Virtual private network remote access.** With virtual private network (VPN) remote access, a VPN client uses an IP internetwork to create a virtual point-to-point connection with a remote access server acting as the VPN server. Once the virtual point-to-point connection is created, the rest of the connection parameters can be negotiated.

Elements of a Dial-Up Remote Access Connection

The Windows 2000 Routing and Remote Access Service accepts dial-up connections and forwards packets between remote access clients and the network to which the remote access server is attached. A remote connection consists of a remote access client, a WAN infrastructure, and a remote access server, as illustrated in Figure 1.2.

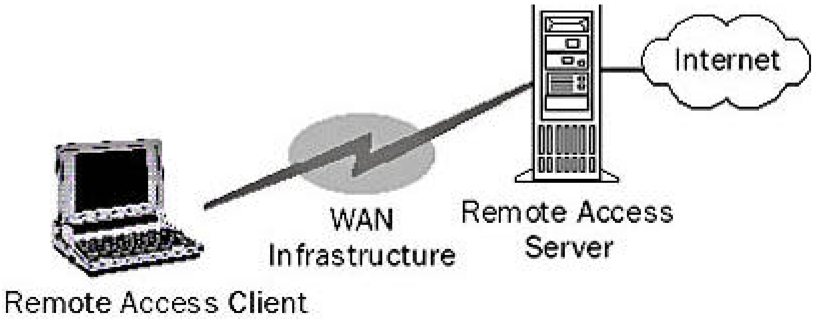


Figure 1.2 *Elements of a dial-up remote access connection*

Remote Access Protocols

Remote access protocols control the connection establishment and transmission of data over WAN links. The operating system and LAN protocols used on remote access clients and servers dictate which remote access protocol your clients can use.

There are three types of remote access protocols supported by Windows 2000 Routing and Remote Access:

1. Point-to-Point Protocol (PPP) is an industry-standard set of protocols providing the best security, multiprotocol support, and interoperability.

2. Serial Line Internet Protocol (SLIP) is used by legacy remote access servers.

3. Microsoft remote access service protocol, also known as Asynchronous NetBEUI (AsyBEUI), is a remote access protocol used by legacy remote access clients running Microsoft operating systems, such as Windows NT 3.1, Windows for Workgroups, MS-DOS, and LAN Manager.

LAN protocols are the protocols used by the remote access client to access resources on the network connected to the remote access server. Windows 2000 remote access supports TCP/IP, IPX, AppleTalk, and NetBEUI.

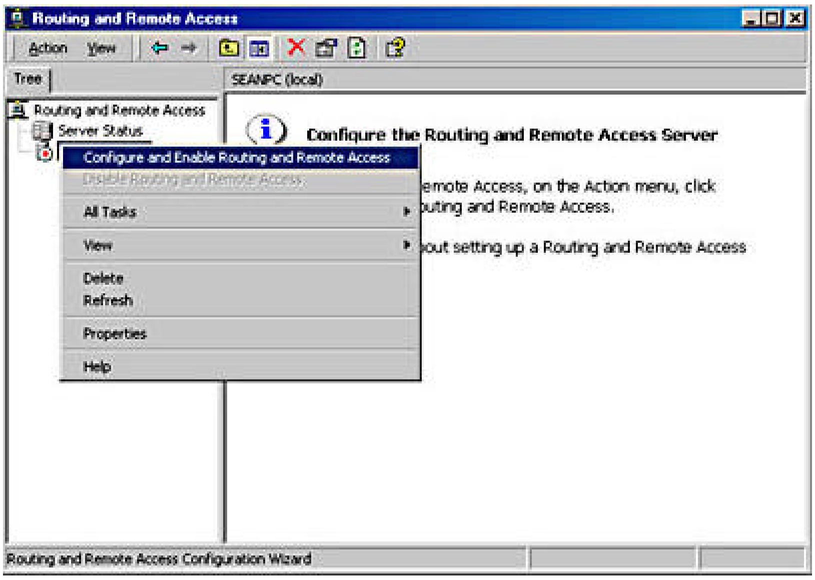
- **To configure a routing and remote access server**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing And Remote Access.

   The Routing and Remote Access management tools appear in the Microsoft Management Console.

2. Right-click the server in the left pane, and then click Configure And Enable Routing And Remote Access, as illustrated in Figure 1.3.

   The Routing and Remote Access Server Setup Wizard appears allowing you to specify server configuration information.



Routing and Remote Access
Action
View
Tree
SEANPC (local)
Routing and Remote Access
Server Status
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help

Configure the Routing and Remote Access Server

emote Access, on the Action menu, click
outing and Remote Access.

out setting up a Routing and Remote Access

Routing and Remote Access Configuration Wizard

Figure 1.3 *Creating a routing and remote access server*

Network Address Translator

There are two types of IP addresses: public and private. Public addresses are assigned to you by the Internet service provider (ISP) you use to connect to the Internet. For the hosts within the organization that do not require direct access to the Internet, IP addresses that do not duplicate already assigned public addresses are required. To solve this addressing problem, designers of the Internet reserved a portion of the IP address space and named this space the private address space. An IP address in the private address space is never assigned as a public address. IP addresses within the private address space are known as private addresses. Using private IP addresses, you can provide protection from network hacking.

Because the IP addresses in the private address space will never be assigned by the Internet Network Information Center (InterNIC) as public addresses, routes in the Internet routers for private addresses will never exist. Private addresses are not reachable on the Internet. Therefore, when using private IP addresses, you need some type of proxy or server to convert the private IP address range(s) on your local network to a public IP address that can be routed. Another option is to have private addresses translated into valid public addresses by a network address translator (NAT) before it is sent on the Internet. Support for network address translation to translate private and public addresses to allow the connection of small office or home office networks to the Internet is illustrated in Figure 1.4.

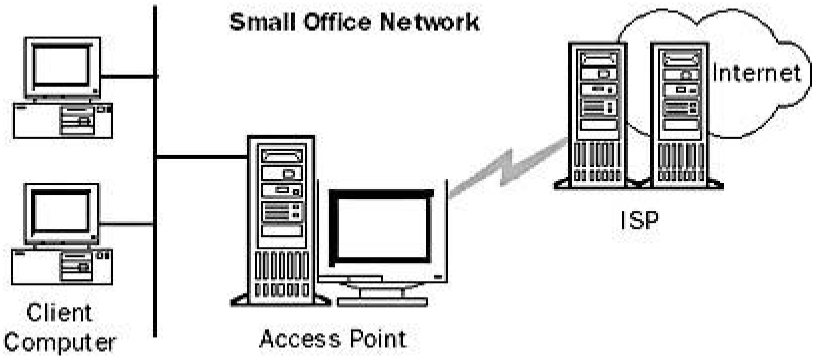


Figure 1.4 *Connecting a small office network to the Internet*

An NAT hides internally managed IP addresses from external networks by translating the private internal address to a public external address. This reduces IP address registration costs by letting customers use unregistered IP addresses internally, with translation to a small number of registered IP addresses externally. It also hides the internal network structure, reducing risks of denial of service attacks against internal systems.

Certificate Services

Designing an appropriate security system to protect your organization's confidential and proprietary information requires developing a set of appropriate solutions for specific risk scenarios. Windows 2000 provides a range of technologies from which to choose in developing your security plan. One of these technologies is Microsoft Certificate Services. You can deploy Microsoft Certificate Services to create and manage Certificate Authorities (CAs) that issue digital certificates.

Digital certificates are electronic credentials that certify the online identities of individuals, organizations, and computers. Certificates function similarly to identification cards, such as passports and driver's licenses. When an identification card is presented to others, they can verify the identify of its owner because the card provides the following security benefits:

- It contains personal information to help identify and trace the owner.
- It contains the signature of the rightful owner to enable positive identification.
- It contains the information that is required to identify and contact the issuing authority.
- It is designed to be tamper resistant and difficult to counterfeit.
- It is issued by an authority that can revoke the identification card at any time (for example, if the card is misused or stolen).
- It can be checked for revocation by contacting the issuing authority.

Digital certificates can be used in the same way to provide a variety of security functions. Some common security functions of digital certificates include the following:

- Secure e-mail
- Secure communications between Web clients and servers
- Code signing for executable code for distribution on public networks
- Local network and remote access logon authentication
- IPSec authentication

Certificate Services provides a means for an enterprise to easily establish CAs in support of their business needs. Certificate Services includes a default policy module suitable for issuing certificates to enterprise entities such as users, machines, or services.

Lesson Summary

Windows 2000 includes key technologies that add value to both new and existing TCP/IP-based networks. Although TCP/IP uses IP to locate and connect to hosts, users typically prefer to use friendly names. DNS enables you to use hierarchical, friendly names to easily locate computers and other resources on an IP network. DHCP simplifies administrating and managing IP addresses on a TCP/IP network by automating address configuration for network clients. WINS provides a distributed database for registering and querying a computer name (which is the same as the NetBIOS name) to IP address mapping in a routed network environment. With Windows 2000 Routing and Remote Access Service, clients are transparently connected to the remote access server. Clients can also be transparently connected to the network to which the routing and remote access server is attached.

[Previous] [Next]

Lesson 2: Developing a Network Implementation Plan

Implementing new technologies in an enterprise network environment requires research, planning, approval, and funding. To obtain the greatest benefit from Windows 2000, you need to plan your deployment carefully. As you begin your Windows 2000 operating system deployment planning, you should understand its features so you can utilize them to your advantage. This will help people in your organization to increase productivity and will reduce total cost of ownership (TCO). In this lesson, you will learn how to plan your Windows 2000 network implementation.

After this lesson, you will be able to

- Describe the various Windows 2000 operating systems
- Describe the phases of a network deployment project life cycle
- Identify hardware and software considerations when designing a network
- Identify network protocol and legacy system integration issues on a network

Estimated lesson time: 40 minutes

Operating System Considerations

When planning your Windows 2000 network, you should consider operating systems based on the needs of your users and business requirements. For example, if your network servers run demanding memory- and processor-intensive applications, implementing a Windows 2000 Advanced Server is your best choice. You should review specific Windows 2000 technology features to determine which technologies are most important for your organization, while considering your organization's short-term, mid-term, and long-term objectives. The following sections describe the different Windows 2000 operating systems.

Windows 2000 Professional

Windows 2000 Professional is a desktop operating system that provides advanced features of Windows NT, including security and fault tolerance, with the easy- to-use features of Windows 98, including plug and play and device support. Windows 2000 Professional can be upgraded from Windows NT Workstation 3.51 and greater, or Windows 98. The minimum system requirements for running Windows 2000 Professional include:

- **133 MHz or higher Pentium-compatible CPU.** Windows 2000 Professional supports single and dual CPU systems.
- **64 megabytes (MB) of RAM.** More memory generally improves responsiveness.
- **2 GB hard disk.** Your hard disk must have a minimum of 650 MB of free space to install Windows 2000 Professional.

Windows 2000 Server

Windows 2000 Server builds on the powerful features of the Windows NT Server 4.0 operating system. Windows 2000 Server integrates standards-based directory, Web, application, communications, file, and print services with high reliability, efficient management, and support for the latest advances in networking hardware to provide the best foundation for integrating your business with the Internet. These features include:

- Information Services 5.0 (IIS)
- Active Server Pages (ASP) programming environment
- XML parser
- Windows DNA 2000
- Component Object Model + (COM+)
- Multimedia platform
- Directory-enabled applications
- Web folders
- Internet printing

Windows 2000 minimum hardware requirements are

- **133 MHz or higher Pentium-compatible CPU.** Windows 2000 Server supports up to four CPUs on one computer.

- **128 MB of RAM.** 256 MB of RAM is recommended. More memory generally improves responsiveness, and Windows 2000 Server supports a maximum 4 gigabytes (GB) of RAM.

- **2 GB hard disk.** You must have a minimum of 1 GB free disk space to install Windows 2000 Server. Additional free hard disk space is required if you are installing over a network.

Windows 2000 Advanced Server

Windows 2000 Advanced Server is the new version of Windows NT Server 4.0, Enterprise Edition. Windows 2000 Advanced Server is ideal for line-of-business and e-commerce applications, where scalability and high availability demands are most critical. While the hardware requirements for Windows 2000 Advanced Server are the same, Advanced Server includes

- All Windows 2000 Server features

- Network (TCP/IP) Load Balancing

- Up to 8 GB main memory on Intel Page Address Extension (PAE) systems

- Support of up to eight processors

NOTE

Be sure to schedule enough time to install a Windows 2000 server, as it can take several hours.

Windows 2000 Datacenter Server

Another Windows 2000 operating system that builds upon the features of Windows 2000 Advanced Server is the Windows 2000 Datacenter Server, which supports 32 processors and more RAM than the other Windows 2000 Server operating systems. Physical memory support includes

- 32 GB of RAM on Alpha-based computers

- 64 GB of RAM on Intel-based computers

Consider installing Windows 2000 Datacenter Server if you must support intensive online transaction processing (OLTP), large data warehouses, and large Internet and application service providers (ISPs and ASPs).

Phases of Deployment

The purpose of your Windows 2000 network planning process is to ensure that your network performs the required activities. When planning your Windows 2000 network deployment, you should follow a process, or life cycle. The phases of this project life cycle should include the following:

1. **Analysis.** During the analysis phase, determine IT goals and objectives. This will help you to design a network to support bandwidth, meet security needs, measure

cost versus benefits, and provide deliverables appropriate to your organization.

2. **Design.** During the design phase, evaluate the Windows 2000 Infrastructure design. This includes features such as DNS, WINS, DHCP, and network protocols. Your design will be based on your analysis, interoperability issues, and desired features.

3. **Testing.** During the testing phase, conduct a pilot project to test the Windows 2000 network you designed in a production environment with a low number of users. You might have to adjust your designs based upon pilot-testing results to achieve a completely functional and stable network environment.

4. **Production.** The production phase is the final phase of Windows 2000 deployment. The network has been tested using the pilot program based on your designs, and you are ready to deploy Windows 2000 throughout your enterprise. During this phase, create a disaster recovery plan and provide training material for user and helpdesk personnel.

Hardware Considerations

Compatibility issues with devices and programs can compromise reliability and quality. You can check hardware and software compatibility with Windows 2000 at *http://www.microsoft.com/windows2000/default.asp*.

Before deploying Windows 2000, you should record hardware and software inventories of all servers and client computers in use on your network, and include basic input/output system (BIOS) settings. You should also record the configuration of peripheral devices, driver versions, service packs, and other software and firmware information. In addition, establish standard configurations for your clients and servers. This includes guidelines for minimum and recommended values for CPU, RAM, hard disks, and accessories such as CD-ROM drives and uninterruptible power supplies.

Make sure that network devices, such as hubs and cabling, are fast enough for your needs. If your organization transfers voice and video over your network, the cabling and switches must be capable of handling the bandwidth demand of those services. Some remote users do not generate much network traffic. For example, a remote user who works with Microsoft Word or Microsoft Excel files does not generate as much network traffic to a routing and remote access server as databases and accounting systems. Therefore, a Category 3 10-Mbps cable matched with the same speed hubs might be acceptable for some situations, whereas Category 5 100-Mbps devices and cabling might be required for applications generating considerably more network traffic. Try to record available bandwidth during the course of low, normal, and high network utilization.

Interaction with Legacy Systems

Many networks are heterogeneous, which means that there are a mix of operating systems and network protocols. For example, your Windows 2000 computers might interact with mainframe hosts, UNIX systems, or other network operating systems. You should concentrate on the interoperability issues that are most important to your organization during planning.

In addition, Windows 2000 Server offers gateway services to other operating systems allowing you to access network resources. Gateway Service for NetWare, for example, allows your Windows 2000 network clients to navigate Novell Directory Services (NDS) hierarchies, use Novell version 4.2 or later logon scripts, and authenticate with a Novell server.

Network Protocol Considerations

Some networks use a variety of protocols based on their needs. For example, a small Ethernet network could use NetBEUI as the LAN protocol, while using TCP/IP for Internet connectivity. In addition, networks that include both Novell NetWare and Windows NT servers might use both IPX/SPX and TCP/IP. Always identify the protocols in use on your current network, and consider whether any of these protocols can be replaced or eliminated by Windows 2000. For example, if you upgrade clients that use IPX/SPX with Windows 2000 Professional, it's possibe to eliminate the use of IPX/SPX on your network.

Windows 2000 contains a TCP/IP protocol suite with more functionality than previous versions of Windows. You must use TCP/IP to use Active Directory and to utilize advanced features of Windows 2000; therefore, you should consider simplifying your network by using only TCP/IP.

You can obtain network settings and protocol information in Windows NT by right-clicking on the My Network Places icon on your desktop and choosing Properties.

Lesson Summary

You should plan your deployment carefully to obtain the greatest benefit from Windows 2000, and be aware of the different Windows 2000 operating systems. An enterprise network deployment consists of different phases of a project life cycle: analysis, design, testing, and production. Before deploying Windows 2000, record hardware and software inventories of all servers and client computers in use on your network. Additionally, consider interoperability issues and decide which protocols best meet your needs.

[Previous] [Next]

Lesson 3: Common Protocols Supported by Windows 2000

When planning your network, consider the connectivity requirements of your users. Network protocols are similar to languages in the sense that languages haves different words, word patterns, and punctuation. A network protocol serves a similar role for computers attempting to communicate. The network protocol used on a network determines how packets (units of data) are configured and sent over the network cable. Consider the following questions:

- **Do network users connect to Novell NetWare servers?** Clients that connect to NetWare servers must use the NWLink protocol. Even if the NetWare servers are configured to use TCP/IP, Windows-based clients must use NWLink to communicate with them.

- **Is your network connected by routers?** NetBEUI is not routable. For computers across routers to communicate, they must use a routable network protocol such as TCP/IP or NWLink.

- **Are you connected to the Internet?** For clients to connect to the Internet, they must use the TCP/IP protocol.

Additionally, some features require that particular protocols be installed. If you want to implement Active Directory, use IIS, or provide clients with access to the Internet, you will need to install TCP/IP. This lesson describes the TCP/IP protocol and other protocols that you can use with Windows 2000.

After this lesson, you will be able to

- Identify different network architectures

- Identify various network protocols used in Windows 2000

Estimated lesson time: 30 minutes

Transmission Control Protocol/Internet Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard suite of protocols designed for large networks. TCP/IP is routable, which means that data packets can be switched (routed to a different subnet) by use of the packet's destination address. TCP/IP's ability to be routed provides fault tolerance, which is the ability of a computer or an operating system to respond to a catastrophic event or fault, such as a power outage or a hardware failure, to ensure that data is not lost or corrupted. If a network failure occurs, TCP/IP packets are transported on a different route.

Although the original purpose of TCP/IP was to provide connection between disparate networks, TCP/IP now provides high-speed communication network links between networks. Microsoft has implemented TCP/IP as a standard network transport for Windows 2000. You will learn more about the architecture, installation, and configuration of TCP/IP in Chapter 2, "Implementing TCP/IP."

Benefits of Implementing TCP/IP

TCP/IP in Windows 2000 includes many performance improvements for high-bandwidth networks. These features are described in the following sections.

Large Window Support

The window size in TCP-based communication is the maximum number of packets that can be sent before the first packet must be acknowledged. Window size is typically fixed and established at the beginning of a session between sending and receiving hosts. With large window support, window size is dynamically recalculated and increased if a large number of packets is exchanged during a lengthy session. This increases bandwidth and allows more data packets to be in transit on the network at one time.

Selective Acknowledgments

With selective acknowledgments, the receiver can notify and request specific packets that were missing or corrupted during delivery from the sender. This allows networks to recover quickly from a state of temporary congestion or interference, because only corrupted packets are re-sent. In previous TCP/IP implementations, if a receiving host failed to receive a single TCP packet, the sender was forced to retransmit all packets transmitted following the negatively acknowledged packet. Using selective acknowledgments, fewer packets are re-sent, providing better network utilization and performance.

Round Trip Time Estimation

Round Trip Time (RTT) is the amount of time it takes for a round-trip communication between a sender and receiver on a TCP-based connection. RTT estimation is a technique of estimating packet transit times and adjusting for the optimum retransmission time for packets. Because performance depends on knowing how long to wait for a missing packet, improving the accuracy of RTT estimation results in better time-out values being set on each host, so that a host cannot request a packet to be retransmitted until the requisite time interval expires. Better timing improves performance over long round-trip network links, such as WANs, that span large distances (for example, continent-to-continent) or use either wireless or satellite links.

IP Security (IPSec) Support

IPSec provides the ideal platform for safeguarding intranet and Internet communications. IPSec can secure paths between two computers, two security gateways, or a host and a security gateway. Windows 2000 Server tightly integrates IPSec with system policy management to enforce encryption between systems. Customers can have encryption-secured communications managed by group policy—a safeguard that protects information sent over networks. Because IPSec is integrated into the operating system, it is easier to configure and manage than add-on solutions.

The services available and required for traffic are configured using IPSec policy. IPSec policy can be configured locally on a computer, or can be assigned through Windows 2000 Group Policy mechanisms using the Active Directory directory service, as illustrated in Figure 1.5. When using Active Directory, hosts detect policy assignment at startup, retrieve the policy, and periodically check for policy updates. The IPSec policy specifies the trust relationship among computers. The easiest trust relationship to use is the Windows 2000 domain trust based on the Kerberos version 5 protocol. Predefined IPSec policies are configured to trust computers in the same or other trusted Windows 2000 domains.

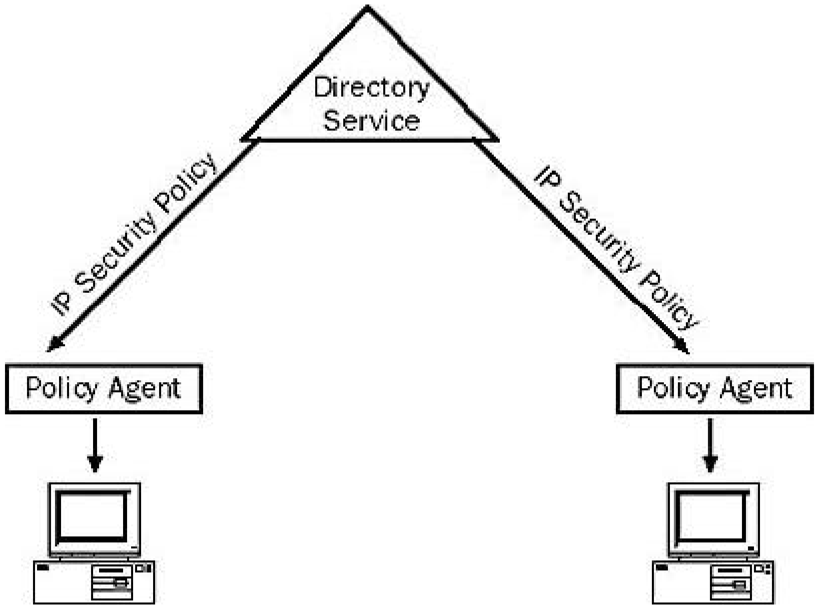


Figure 1.5 *Windows 2000 Group Policy using Active Directory*

At the IP (network) layer, each incoming or outgoing packet is referred to as a datagram. Each IP datagram bears the source IP address of the sender and the destination IP address of the intended recipient. Each IP datagram processed at the IP layer is compared against a set of filters that are provided by the security policy, which is maintained by an administrator for a computer, user, group, or an entire domain. The IP layer can perform one of the following actions with a datagram:

- Provide IPSec services to the datagram
- Allow the datagram to pass unmodified
- Discard the datagram

Because IPSec typically encrypts the entire IP packet, capturing an IPSec datagram sent after the security association (SA) is established reveals very little of what is actually in the datagram. The only parts of the packet that can be parsed or read by a network sniffer such as Network Monitor are the Ethernet and IP headers. This lends greater security to IP transactions. IPSec is covered in more detail in Chapter 5, "Implementing IPSec."

Generic Quality of Service

Generic Quality of Service (GQoS) is a method by which a TCP/IP network can offer Quality of Service guarantees for multimedia applications. Generic Quality of Service allocates different bandwidths for each connection on an as-needed basis.

Quality of Service (QoS) allows network administrators to use their existing resources efficiently and to guarantee that critical applications receive high-quality service without having to expand as quickly or upgrade their networks. Deploying QoS means that network administrators can have better control over their networks, reduce costs, and improve customer satisfaction. The suite of QoS components included in Windows 2000 works with the different QoS mechanisms that can exist in network elements such as routers and switches. These host mechanisms give administrators an idea of which applications are in use and what their resource requirements are without having to calculate the mappings between actual users, network ports, and addresses. When the host and the network operate cooperatively, resources can be utilized easily and more knowledgeably.

The following QoS components are currently included with the Windows 2000 operating system:

- **The Generic Quality of Service (GQoS) application programming interface (API).** The GQoS API is a subset of the WinSock 2 API that allows applications to invoke QoS services from the operating system without needing to understand the underlying mechanisms.

- **The QoS service provider.** This responds to requests from the GQoS API. It provides Resource Reservation Protocol (RSVP) signaling and QoS policy support with Kerberos. It also invokes the traffic control mechanisms.

- **The Admission Control Service (ACS) service and Subnet Bandwidth Manager (SBM) protocol.** This provides management of shared network resources over a standardized signaling protocol.

- **A traffic control infrastructure.** This infrastructure includes a packet scheduler and marker for providing traffic control over drivers and network cards that have no packet scheduling features of their own. It also marks packets for diffserv and 802.1p. Windows 2000 traffic control also includes additional mechanisms such as Integrated Services over Slow Links (ISSLOW) and Asynchronous Transfer Mode (ATM).

Microsoft is working closely with Cisco on the delivery of qualitative QoS services, and is working along with Cisco, Extreme Networks, Intel, Sun, 3Com, and others on the continuing development of the Internet Engineering Task Force (IETF) RSVP standard.

NWLink

NWLink is a Microsoft-compatible IPX/SPX protocol for Windows 2000. NWLink is useful if there are Novell NetWare client/server programs running that use WinSock or NetBIOS over IPX/SPX protocols. WinSock is an API that allows Windows-based applications to access the transport protocols. NWLink can be run on a computer running Windows 2000 Server or Windows 2000 Professional to access a NetWare server.

NWLink alone does not allow a computer running Windows 2000 to access files or printers shared on a NetWare server, or to act as a file or print server to a NetWare client. To access files or printers on a NetWare server, a redirector must be used, such as Client Service for NetWare on Windows 2000 Professional, or Gateway Service for NetWare on Microsoft Windows 2000 Server. NWLink is included with both Windows 2000 Server and Windows 2000 Professional, and installs automatically during Client Service for NetWare or Gateway Service for NetWare installation. Both Client Service for NetWare and Gateway Service for NetWare depend on the NWLink protocol. NWLink is covered in more detail in Chapter 3, "Implementing NWLink."

Gateway Service for NetWare

Gateway Service for NetWare works with NWLink to provide access to NetWare file, print, and directory services by acting as a gateway through which multiple clients can access NetWare resources. With Gateway Service for NetWare, you can connect a computer running Windows 2000 Server to NetWare bindery-based servers and Novell NDS servers. Multiple Windows-based clients can then use Gateway Service for NetWare as a common gateway to access NetWare file, print, and directory services, without requiring special client software.

Gateway Service for NetWare supports direct access to NetWare services from the computer running Windows 2000 Server in the same way that Client Service for NetWare supports direct access from the client computer. Additionally, Gateway Service for NetWare supports NetWare login scripts.

> **NOTE**
>
> Gateway Service for NetWare is included only with Windows 2000 Server and Windows 2000 Advanced Server.

Client Service for NetWare

Similar to Gateway Service for NetWare, Client Service for NetWare works with NWLink to provide access to NetWare file, print, and directory services. However, rather than acting as a gateway for clients, Client Service for NetWare enables clients to connect directly to file and print services on NetWare bindery-based servers and NetWare servers running NDS. Client Service for NetWare also supports NetWare login scripts. Client Service for NetWare is included only with Windows 2000 Professional.

NetBEUI

NetBIOS Enhanced User Interface (NetBEUI) was originally developed as a protocol for small departmental LANs of 20 to 200 computers. NetBEUI is not routable because it does not have a network layer. NetBEUI is included with Windows 2000 Server and Windows 2000 Professional, and is primarily a legacy protocol to support existing workstations that have not been upgraded to Windows 2000.

AppleTalk

AppleTalk is a protocol suite developed by Apple Computer, Inc. for communication between Apple Macintosh computers. Windows 2000 includes support for AppleTalk, which allows Windows 2000 to function as a router and a dial-up server. Support is natively provided as a service for file sharing and printer sharing.

Windows 2000 supports an AppleTalk protocol stack and AppleTalk routing software so that the Windows 2000 server can connect to and provide routing for AppleTalk-based Macintosh networks.

Data Link Control

Data Link Control (DLC) was originally developed for IBM mainframe communications. The protocol was not designed to be a primary protocol for network use between personal computers. The other use of DLC is to print to Hewlett-Packard printers connected directly to networks. Network-attached printers use the DLC protocol because the received frames are easy to disassemble and DLC functionality can easily be coded into read-only memory (ROM). DLC's usefulness is limited because it does not directly interface with the Transport Driver Interface layer. DLC needs to be installed only on those network computers that perform these two tasks, such as a print server sending data to a network Hewlett-Packard printer. Clients sending print jobs to a network printer do not need the DLC protocol installed on their computers. Only the print server communicating directly with the printer needs the DLC protocol installed.

Infrared Data Association

Infrared Data Association (IrDA) has defined a group of short-range, high-speed, bidirectional wireless infrared protocols, generically referred to as IrDA. IrDA allows a variety of devices to communicate with each other. Cameras, printers, portable computers, desktop computers, and personal digital assistants (PDAs) can communicate with compatible devices using this technology.

Lesson Summary

TCP/IP is an industry-standard suite of protocols designed for large networks. TCP/IP is routable, which means that data packets can be switched by use of the packet's destination address. TCP/IP's ability to be routed provides fault tolerance. Other protocols supported by Windows 2000 include

- NWLink
- NetBEUI
- AppleTalk
- Data Link Control
- Infrared Data Association

[Previous] [Next]

Review

Answering the following questions will reinforce key information presented in this chapter. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. You are currently configuring TCP/IP manually for new computers and computers moving from one subnet to another. You want to simplify management of TCP/IP addresses and assign them automatically. Which Windows 2000 network service should you use?

2. You have an Alpha server with 8 GB of RAM and 8 CPUs. You want to provide file services to over 400 people in your company. Which Windows 2000 operating system would be most appropriate to deploy, and why?

3. You want a Windows 2000 server to connect to and provide routing for AppleTalk-based Macintosh networks. What protocol should you install?

Answers