Part 1

Standards and Terminology

Chapter 1

Networking Terms and Concepts

As one of the required exams in the Microsoft MCSE program, the test for Networking Essentials is intended to challenge your knowledge of computer networking components, theory, and implementation. This chapter covers mostly theory and acquaints you with some of the basic terms and concepts used in networking. Study this chapter carefully—you will use these terms and concepts often throughout the rest of this book. Realize also that the topics covered in this chapter are generally applicable to all networking models. In addition, although most of the examples are given in terms of Microsoft solutions, all other successful networking models must accomplish the same tasks.

Chapter 1 targets the following objectives in the Standards and Terminology section of the Networking Essentials exam:

Test Objectives

- Define common networking terms for LANs and WANs
- Compare a file-and-print server with an application server
- Compare user-level security with access permission assigned to a shared directory on a server
- Compare a client/server network with a peer-to-peer network

Test Yourself

Stop! Before reading this chapter, test yourself to determine how much study time you will need to devote to this section.

1. Which two of the following are indicative of the server-based network model?
   - A. The model is better for smaller networks (fewer than 10 users).
   - B. The model has single point of failure.
   - C. The model relies on centralized administration.
   - D. The model makes it harder to implement RAID.

2. The size limit for a WAN is ________.
   - A. 100 kilometers
   - B. 1,000 kilometers
   - C. 10,000 kilometers
   - D. worldwide (no limit)

3. The _________ routes I/O requests from the local machine to the network.
   - A. router
   - B. redirector
   - C. network driver
   - D. none of the above

4. A ________ network typically demands more knowledgeable users.
   - A. server-based
   - B. peer-to-peer
   - C. local area
   - D. wide area

In the 1980s, the desktop computer emerged as a low-cost alternative to terminals connected to a high-priced mainframe. Each desktop computer was capable of integrating peripherals and software to accomplish certain tasks, but data transfer between systems all too often required the cumbersome intervention of a human with a floppy disk. As the computer industry grew, PC managers, marketers, users, and designers began to see the advantages of sharing data and hardware among a group of individual, but cooperating, PCs. The first PC network operating systems (such as Novell NetWare and Microsoft LAN Manager) were designed as add-ons to existing desktop operating systems. A new breed of PC operating systems, such as Microsoft Windows 95 and Windows NT, now include a fully-integrated system of network services. The integration of network services within personal desktop operating systems and the public emergence of the worldwide network—the Internet—has generated incredible momentum in the movement to "get connected." Networks have become the primary means of disseminating information in most modern offices.

Networking Concepts and Components

A *network* is a group of interconnected systems sharing services and interacting by means of a shared communications link (see fig. 1.1). A network, therefore, requires two or more individual systems with something to share (data). The individual systems must be connected through a physical pathway (called the *transmission mediu*m). All systems on the physical pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules that govern computer communication are called *protocols.*

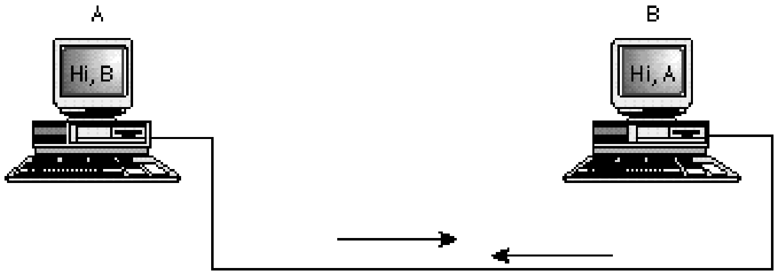


Figure 1.1

At its simplest, a computer network is two or more computers sharing information across a common transmission medium.

In summary, all networks must have the following:

- Something to share (data)
- A physical pathway (transmission medium)
- Rules of communication (protocols)

Merely having a transmission pathway does not produce communication. When two entities communicate, they do not merely exchange data; rather, they understand the data they receive from each other. The goal of computer networking, therefore, is not simply to exchange data, but to be able to understand and use data received from other entities on the network.

Because all computers are different, are used in different ways, and can be located at different distances from each other, enabling computers to communicate is often a daunting task that draws on a wide variety of technologies.

note

Remembering that the term *network* can be applied to human communication can be useful. When you are in a classroom, for example, the people in that class form a human information network (see fig. 1.2). In computer terms, the instructor is the server, and the students are network clients. When the instructor speaks, the language he uses is equivalent to a computer protocol. If the instructor speaks French, and the student understands only English, the lack of a common protocol makes productive communication difficult. Likewise, air is the transmission medium for human communication. Sound is really nothing more than wave vibrations transmitted across the air to our eardrums, which receive and interpret the signals. In a vacuum, we cannot communicate via speech because our transmission pathway is gone.

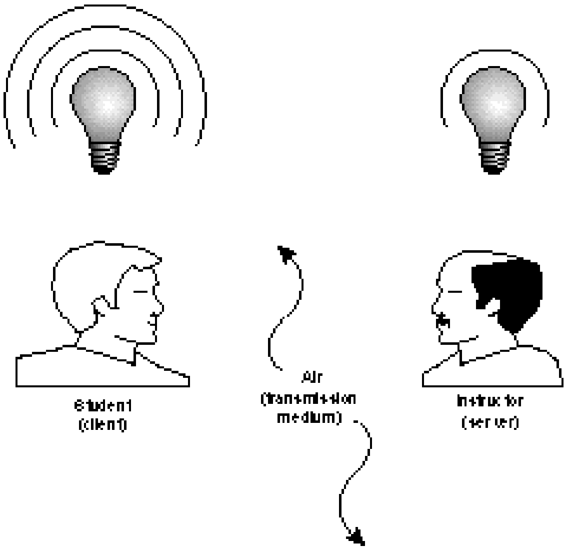


Figure 1.2

Human communication is a kind of network.

The goals of computer networking are to provide services and to reduce equipment costs. Networks enable computers to share their resources by offering services to other computers. Some of the primary reasons for networking PCs are as follows:

- Sharing files
- Sharing printers and other devices
- Enabling common administration and security
- Supporting network applications such as electronic mail and database services

You learn more about these important network functions later in this chapter.

Models of Network Computing

After you have the necessary prerequisites for network communication, a structure must be put in place that organizes the way communication and sharing occur. Three methods of organization, or *models*, are generally recognized. The three models for network computing are as follows:

- Centralized computing
- Distributed computing
- Collaborative or cooperative computing

These three models are the basis for the various types of computer networks you learn about in this book. The following sections discuss the three models for network computing.

Centralized Computing

The earliest computers were large, expensive, and difficult to manage. Originally, these large mainframe computers were not networked in the sense you are familiar with today. Jobs were entered into the system by reading commands from card decks. The computer would execute one job at a time and generate a printout when the job was complete. Terminals, which came later, enabled users to interact with the centralized computer, but terminals were merely input/output devices that had no independent processing power. All processing still took place on the mainframe, hence the name *centralized computing*. Networks, therefore, served little purpose other than to deliver commands to and results from the powerful centralized processing device. Large IBM and Digital (DEC) networks often still operate on this model, but Microsoft has largely ignored it.

In summary, the centralized computing model involves the following:

- All processing takes place in the central, mainframe computer.
- Terminals are connected to the central computer and function only as input/output devices.
- Networks may be employed to interconnect two or more mainframe computers. Terminals connect only to the mainframe, never to each other.

This early computing model worked well in large organizations, but was not flexible and did not scale down to meet the needs of smaller organizations. As such, new ways of sharing information were needed to allow computing power to be shared efficiently on smaller networks.

Distributed Computing

As personal computers were introduced to organizations, a new model of *distributed computing* emerged. Instead of concentrating computing to a central device, PCs made it possible to give each worker an independent, individual computer. Each of these PCs can process and store data locally, without assistance from another machine. This meant that groups who previously had found the cost of a mainframe environment prohibitive were able to gain the benefits of networking at a far reduced cost. Under the distributed computing model, networking has evolved to enable the many distributed computers to exchange data and share resources and services among themselves. Note that these machines need not be considered equals. A Windows NT file server, for instance, is considered to be a part of a distributed network. This server stores and retrieves files for other machines, but does not do the thinking for these machines as a mainframe would have done in the centralized computing model.

note

> The term PC initially referred to a specific device, the IBM PC computer. Over time, though, *PC* has become a generic term referring to any IBM-compatible workstation computer.

In summary, distributed computing involves the following:

- Multiple computers are capable of operating independently.
- Tasks are completed locally on various computers.
- Networks enable the computers to exchange data and services but do not provide processing assistance.

Distributed computing was a major step forward in the way that businesses could leverage their hardware resources. However, it largely dealt with the sharing of data and printers. Processing was left to be done at each machine separately, without any specialization or assistance.

Collaborative Computing

Also called cooperative computing, *collaborative computing* enables computers in a distributed computing environment to share processing power in addition to data, resources, and services. In a collaborative computing environment, one computer might “borrow” processing power by running a program on other computers on the network. Or, processes might be designed so that they can run on two or more computers. Obviously, collaborative computing cannot take place without a network to enable the various computers to communicate.

Collaborative computing is exemplified in Microsoft networks by server-based products such as Exchange Server or SQL Server.

With both of these products, requests originate from intelligent client software (which uses the processor power of the workstation it is running on) but then are serviced from server software running on an NT Server. The server processes the request using its own resources and then passes the results back to the client. Processor and memory resources on both the client and the server are utilized in the completion of the task.

In summary, collaborative computing involves the following:

- Multiple computers cooperating to perform a task
- A network that enables the computers to exchange data and services
- Software designed to take advantage of the collaborative environment.

Now that we have looked at these three organizational models, you should realize that Microsoft networks are generally based on the distributed computing model and that many higher-end NT options incorporate collaborative computing elements as well. The next decision an administrator needs to make is what type of server the network will have.

Network Models: Comparing Server-Based and Peer-to-Peer Configurations

PC networks generally fall within one of these two network types:

- **Server-based.** A server-based network consists of a group of user-oriented PCs (called *clients*) that request and receive network services from specialized computers called *servers*. Servers are generally higher-performance systems, optimized to provide network services to other PCs. (Some common server types include file servers, mail servers, print servers, fax servers, and application servers.)

- **Peer-to-peer.** A peer-to-peer network is a group of user-oriented PCs that basically operate as equals. Each PC is called a *peer*. The peers share resources, such as files and printers, but no specialized servers exist. Each peer is responsible for its own security, and, in a sense, each peer is both a client (because it requests services from the other peers) and a server (because it offers services to the other peers). Small networks—usually under 10 machines—may work well in this configuration.

Many network environments are a combination of server-based and peer-to-peer networking models. For example, an organization may concurrently use Novell's server-based network operating system, NetWare, and Microsoft's peer-to-peer operating system, Windows for Workgroups. New desktop operating systems, such as Microsoft Windows 95, integrate easily into either network model.

Windows NT Server and Workstation

The two flavors of Windows NT—Windows NT Server and Windows NT Workstation—embody the different orientations of the server-based and peer-to-peer networking models (see fig. 1.3). Under the hood, the two operating systems are quite similar, yet they are outfitted and optimized for very different roles.

Windows NT Server—is optimized to act as a file, print, and application server and is designed to function as a server in server-based networks. NT Server can support unlimited concurrent incoming sessions (depending on the licensing agreement) and up to 256 inbound RAS connections. Windows NT Server can also act as a domain controller, maintaining a user account database for an entire domain. (See the section titled "Network Security" later in this chapter.)

Windows NT Workstation—is optimized for desktop performance. Windows NT Workstation can serve as a high-security, industrial strength desktop operating system and, therefore, is designed to function as a client in a server-based network or as a peer in a peer-to-peer network.

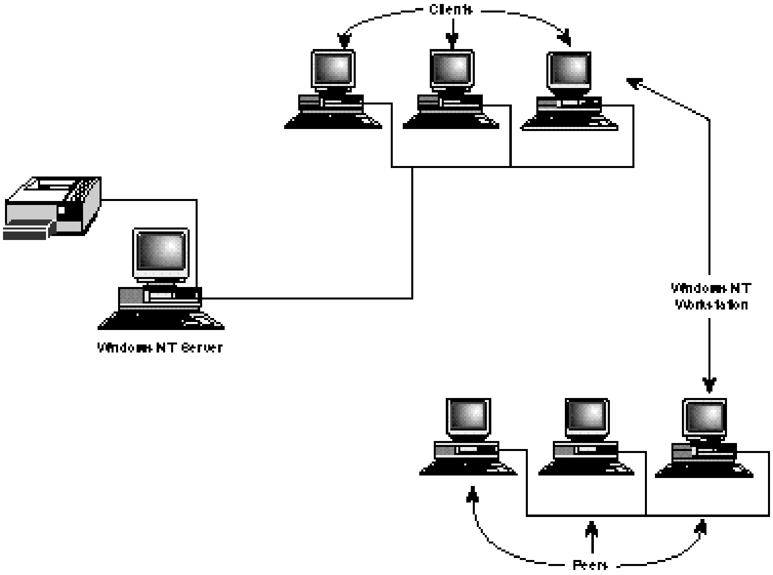


Figure 1.3

Windows NT Server is optimized for file, print, and application services. Windows NT Workstation is optimized for desktop performance, either as a network client or as a peer.

Server-Based Networking

In a *server-based* network environment, resources are located on a central server or group of servers. A *server* is a computer that is specifically designated to provide services for the other computers on the network. A *network client* is a computer that accesses the resources available on the server.

The server-based network model is more efficient for all but the smallest networks because hardware resources can be concentrated on relatively few highly-utilized network servers; client computers can be designed with minimal hardware configurations. A basic network client machine, for instance, might have a 486 processor and 8–16 megabytes of RAM. A typical server might have 32 megabytes of RAM (or more) and many gigabytes of file storage capacity.

note

Humans often specialize so that they become very good at one type of task. This approach has benefits for network servers as well. By dedicating a server to providing a specific set of services, it becomes possible to carefully tailor the computer to the requirements for that service, which results in optimal performance, simpler troubleshooting, and enhanced scalability. Both Exchange Server and SQL Server, for instance, are very resource-intensive services, and running these on a server that also provides file and print services often can result in decreased performance. Dedicating a single server to SQL Server, while expensive, greatly improves overall access to both the SQL databases and normal file and print requests.

A *file server* is a server that stores files on the network for users (see fig. 1.4). A user at a client machine can save a file to a hard drive located on the file server. If the user wants to access the file later, she can access the file from the client machine through a network connection to the file server. Maintaining a central location for file storage on the server makes it easier to provide a backup copy of important files and implement a fault-tolerance system, such as the RAID (Redundant Array of Inexpensive Disks) systems you learn about in Chapter 9, “Disaster Recovery.”

A print server manages access to network printing resources, thus enabling several client machines to use the same printer (see fig. 1.5). Because files and printers are so basic and so important to most networks, file and print services are very basic components of most network operating systems, and a single machine commonly acts (or is able to act) as both a file server and a print server.

note

For licensing purposes, Microsoft uses the term *file-and-print server* to refer to a machine that provides either file or print service functions because the use of either a printer or hard drive space on the server is considered a client connection. Licensing compliance is an important and often confusing part of network administration, which is covered in Chapter 8, “Managing and Securing a Microsoft Network.”

Figure 1.4

A file server stores files for users on other network machines.

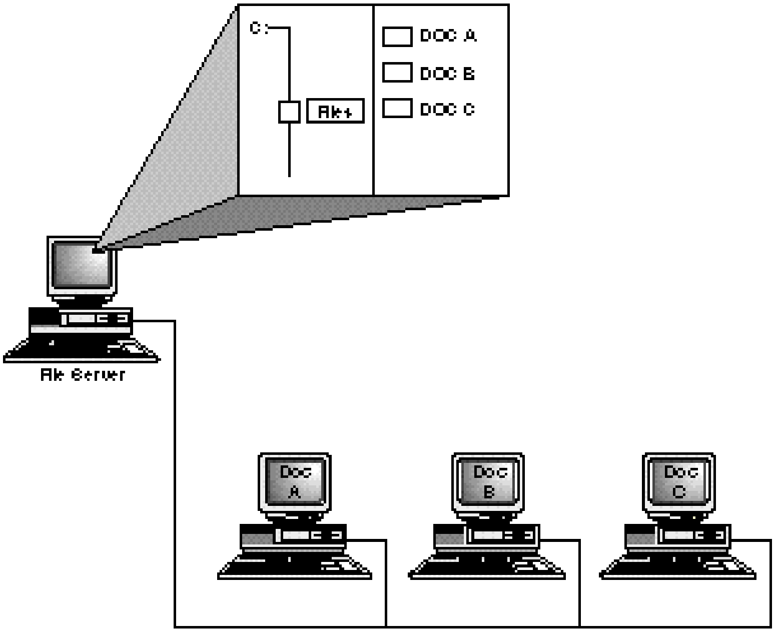
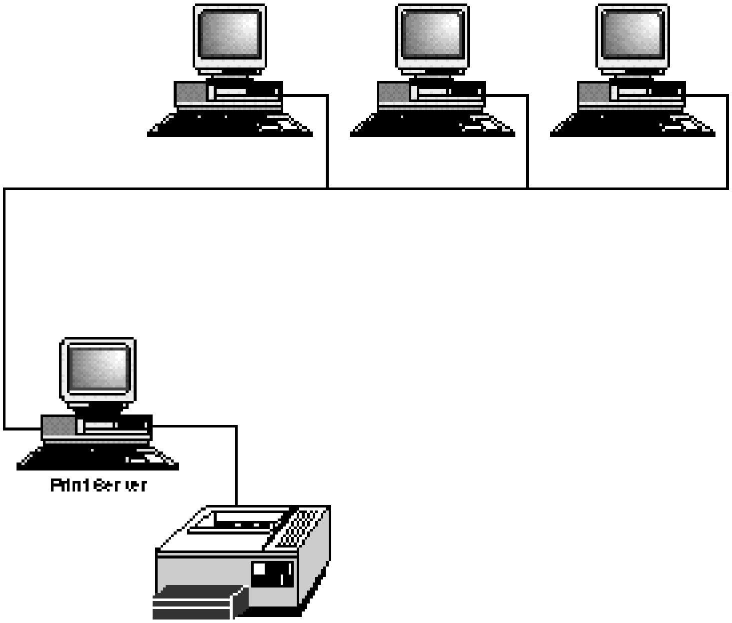


Figure 1.5

A print server manages access to a shared printer, making it accessible to users at other network machines.



An *application server* is a server that actually runs an application (or part of an application) for the client (see fig. 1.6). Whereas a file server simply holds data (in the form of a file) that then is retrieved and processed at the client, an application server performs all or part of the processing on the server end. An application server might search through a large database to provide a requested record for a client. Or, an application server might be part of a client/server application, in which both the client and the server perform some of the processing.

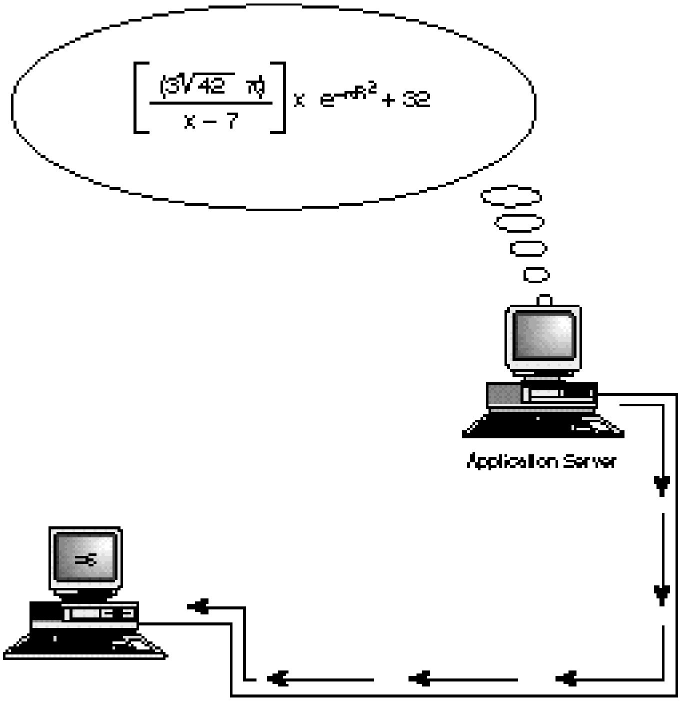

$\left[\frac{(3\sqrt{42}\ \pi)}{x-7}\right] x\ e^{-\pi R^2} + 32$
Application Server

Figure 1.6

An application server runs all or part of an application on behalf of the client and then transmits the result to the client for further processing.

note

The distinction between a file-and-print server and an application server is very important. Remember that a file-and-print server stores files, but it does not actually provide any processing. An application server provides processing and downloads the result to the client. A file-and-print server, therefore, generally requires a great deal of RAM, but is easy on the processor. An application server can be RAM intensive as well, but it definitely needs a more powerful processor.

Under the server-based model, a network administrator can easily control access to network resources. Through the network operating system, the network administrator can give or withhold permission for a user to access files, printers, and other resources located on the server.

The following network operating systems are designed to implement LANs based on server-based models:

- Novell NetWare
- Banyan VINES
- OpenVMS
- IBM OS/2 LAN Server
- Microsoft Windows NT Server

Peer-to-Peer Networking

In the *peer-to-peer* network environment, resources are distributed throughout the network on computer systems that may act as both service requesters and service providers. In a peer-to-peer network, the user of each PC is responsible for the administration and sharing of resources for his PC, which is known as distributed or workgroup administration.

A peer-to-peer network sometimes is called a *workgroup*. Peer-to-peer networks are ideal for small organizations (fewer than ten users) where security is not of concern. Peer-to-peer networks also provide a decentralized alternative for situations in which server administration would be too large or complex a task.

Because a peer-to-peer network does not attempt to centralize security, and because peer-to-peer networks are generally much smaller and simpler than server-based networks, the software required to operate a peer-to-peer network can be much simpler. Several desktop operating systems, including the Microsoft operating systems Windows for Workgroups, Windows 95, and Windows NT Workstation, come with built-in peer-to-peer networking functionality.

> note
>
> When deciding whether to build a peer-to-peer network around NT Workstation or a server-based network around NT Server, remember that a key difference between the two is that NT Workstation supports a *maximum* of ten concurrent, logged-on users. This means that no more than ten other computers can access resources on a Workstation at one time. NT Server, however, has no such limitation and is capable of supporting dozens, even hundreds, of connections at once by the addition of more access licenses.

Aside from Microsoft's NT Workstation, Windows 95, and Windows for Workgroups, numerous other operating systems, including the following, are designed to implement peer-to-peer networking models:

- Novell Personal NetWare
- AppleTalk (the networking system for Apple Macintosh computers)
- Artisoft LANtastic

Remember that many of these peer-to-peer products can be integrated with networks that are primarily managed in a server-based environment. Macintosh computers, for example, can access resources on an NT Server system that is configured to receive them.

Network Security

Because the purpose of a network is to make accessing resources easy, network administrators and designers are constantly concerned with how to protect network resources so that unauthorized users can't gain access to them. All commercial network operating systems provide some form of security system that limits access to shared files, printers and other resources, and the system itself. Chapter 8 describes how to secure resources in Microsoft networks. The following are the elements of network security:

- **Authentication.** A user must provide a username and password to gain access to the system. The logon process is like a front door to the system, and the user's credentials (a username and a password) are the key. If you have the key, you can go inside. Otherwise, you are "out" of the system.

- **Access permissions.** Specific resources (such as files, directories, or printers) have their own access lists. The operating system checks the access list to determine whether a user has permission to access the resource. Some kind of authentication method (see preceding bullet) must accompany the access permission system—the operating system has to know the identity of the user to determine whether the user has the required permissions.

- **Password-protected shares.** Specific resources (such as files, directories, or printers) are protected with passwords. To access the resource, the user must type the correct password. This method does not require an initial authentication procedure. The operating system does not have to verify the identity of the user—it just checks to see whether the user knows the password.

On Windows NT networks, a *domain* is a collection of computers with a common account database. The account database resides on special Windows NT Server systems called domain controllers. When a user logs on to the domain from a client machine (attempts to gain access to the domain), the user's credentials are forwarded via the network to the domain controller for authentication.

Windows NT enables you to directly set access permissions for files, directories, printers, and other resources (see the following sidebar). To simplify the task of assigning access permissions to users, Windows NT uses a concept called a *group.* A group is a predefined collection of access permissions and rights assigned to a collection of users. Permissions are initially assigned to the group, and any user who becomes a member of the group assumes those permissions. Rather than configuring an individual set of permissions for each user, add the user to a group that possesses the permissions you want the user to have.

Some of the Windows NT access permissions are as follows:

- **Read.** Grants permission to read and copy files.
- **Write.** Grants permission to create new files.
- **Execute.** Grants permission to execute files.
- **Delete.** Grants permission to delete files.
- **No Access.** Denies all access to the resource.

When using Windows NT, you can set user-level security for a file or directory only if the file directory is on a partition that uses the NTFS files system (New Technology File System or NT File System). The permissions then become part of the access control list for the file or directory. The older FAT (File Allocation Table) file system doesn't support access permissions for file or directory objects; however, Windows NT enables you to define access permissions for a directory share whether or not the share is on a FAT or an NTFS partition. (See Chapter 8.)

note

A *share* is an object that has been made available for network access. You learn more about shares and permissions in Chapter 8.

Share permissions in NT are known as ATS (Access through Share) permissions. ATS permissions are independent of any local NTFS file- or directory-level permissions (see fig. 1.7). Think of a share as an object that is distinct from the object you are sharing. The available access types for an ATS share are more limited than the access types available through directory permissions for an NTFS directory. (Your choices are No Access, Read, Change, and Full Control. NTFS directory permissions offer several other access types, such as List, Add, Add & Read, and Special Access.) If you have directly specified permissions for an NTFS file or directory and also specified ATS permissions for that file or directory through a directory share, the most restrictive permissions apply.

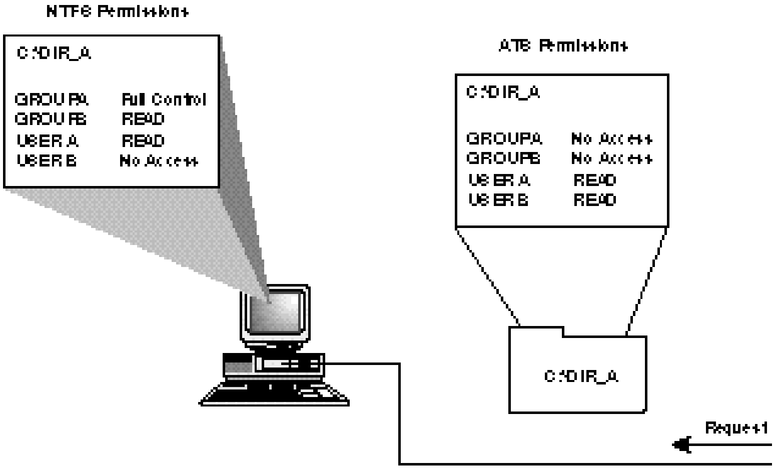


Figure 1.7

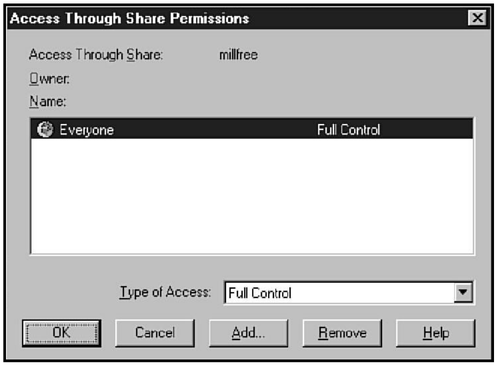
Access through ATS permissions applies to the share, while NTFS file or directory permissions apply to the actual file or directory.

ATS permissions apply only to access via the network. Set ATS permissions through the Sharing tab of the directory Properties dialog box (see the following sidebar). Set file- or directory-level access permissions through the Security tab of the file/directory Properties dialog box.

Windows NT Permissions

You can set permissions for a Windows NT 4.0 object (such as a file, directory, printer, drive, or network share) by using the object's Security tab. You can find the Security tab in the Properties dialog box for the object (right-click on an icon for the object and choose Properties). Clicking on the Permissions button in the Security tab invokes a Permissions dialog box that enables you to specify the level of access you want to extend to specific groups and users.

The FAT file system doesn't support file-level access permissions, so if your partition is formatted for the FAT file system, you won't find a Security tab in the Properties dialog box. If you share the file or directory, however, you can still define permissions for the share. Select the Sharing tab and click on the Permissions button to invoke a Permissions dialog box similar to the one shown in figure 1.8.



Access Through Share Permissions

Access Through Share: millfree

Owner:

Name:

Everyone	Full Control

Type of Access: Full Control

Figure 1.8

The Access Through Share Permissions dialog box.

A Windows 95 machine can share its resources either through user-level permissions or through password-protected shares. If you choose to assign permissions using user-level security, you must tell Windows 95 where to obtain a list of users because Windows 95 does not support its own user account database. Requests to access the resource then are passed to a security provider (a Windows NT computer or a NetWare server) on the network.

tip

Another major advantage of a server-based Windows NT domain over a Windows peer-to-peer workgroup is the capability to share user information. If you have nine machines in a peer-to-peer workgroup with NT Workstation, and you need to add a user to a group that has access to them all, for example, you need to go to each individual machine and create an account for the user. You then add this new user to the appropriate group on each machine. If you have eight workstations and an NT Server acting as a domain controller in a properly constructed domain, things are far easier. You create the user on the server, add the user to the proper Global group (also on the server), and add this Global group into Local groups on each machine. The user then has rights on all nine machines. You can find more on this in Chapter 8.

Local and Wide Area Networks

Networks come in all shapes and sizes. Network administrators often classify networks according to geographical size. Networks of similar size have many similar characteristics, as you learn in later chapters. The most common size classifications are the following:

- Local area networks (LANs)
- Wide area networks (WANs)

Each of these size classifications is described in the following sections.

Local Area Networks (LANs)

A *local area network (LAN)* is a group of computers and network communication devices interconnected within a geographically limited area, such as a building or campus. A LAN tends to use only one type of transmission medium—cabling.

LANs are characterized by the following:

- They transfer data at high speeds.
- They exist in a limited geographical area.
- Their technology is generally less expensive.

Wide Area Networks (WANs)

A *wide area network (WAN)* interconnects LANs. A WAN may be located entirely within a state or country, or it may be interconnected around the world.

WANs are characterized by the following:

- They exist in an unlimited geographical area.
- They are more susceptible to errors due to the distances data travels.
- They interconnect multiple LANs.

- They are more sophisticated and complex than LANs.
- Their technology is expensive.

WANs can be further classified into two categories: enterprise WANs and global WANs. An *enterprise WAN* is a WAN that connects the widely separated computer resources of a single organization. An organization with computer operations at several distant sites can employ an enterprise WAN to interconnect the sites. An enterprise WAN can use a combination of private and commercial network services but is dedicated to the needs of a particular organization. A *global WAN* interconnects networks of several corporations or organizations. An example of a global WAN is the Internet.

WANs are often a natural outgrowth of the need to connect geographically separate LANs into a single network. For instance, a company might have several branch offices in different cities. Every branch would have its own LAN so that branch employees could share files and other resources, and all the branches together would be part of a WAN, a greater network that enables the exchange of files, messages, and application services between cities.

Much of the complexity and expense of operating a WAN is caused by the great distances that the signal must travel to reach the interconnected segments. WAN links are often slower and typically depend on a public transmission medium leased from a communications service provider.

Network Operating Systems

The PCs in a network must have special system software that enables them to function in a networking environment. The early network operating systems were really add-on packages that supplied the networking software for existing operating systems, such as MS-DOS or OS/2. More recent operating systems, such as Windows 95 and Windows NT, come with the networking components built in.

Client and server machines require specific software components. A computer that is in a peer-to-peer network is functioning as both a client and a server and thus requires both client and server software. Operating systems, such as Windows NT, include dozens of services and utilities that facilitate networking. You learn about some of those components in other chapters, and some are beyond the scope of the Networking Essentials exam. (You'll get to know them when you study for the Windows NT Server or Windows NT Workstation exam.) This section introduces you to a pair of key network services —the redirector and the server— that are at the core of all networking functions.

A network client must have a software component called a *redirector*. In a typical stand-alone PC, I/O requests pass along the local bus to the local CPU. The redirector intercepts I/O requests within the client machine and checks whether the request is directed toward a service on another computer. If it is, the redirector directs the request toward the appropriate network entity. The redirector enables the client machine to perform the following tasks:

- Log on to a network
- Access shared resources
- Access and participate in distributed applications

note

In some operating environments, the redirector is called the *requester.* The Workstation service acts as a redirector on Windows NT systems.

A network server machine must have a component that accepts I/O requests from clients on the network and fulfills those requests by routing the requested data back across the network to the client machine. In Windows NT, the Server service performs the role of fulfilling client requests.

File Services

File services enable networked computers to share files. This capability was one of the primary reasons networking personal computers initially came about. File services include all network functions centering on the storage, retrieval, or movement of data files. A common feature of file services is access control and transaction logging. File services enable users to read, write, and manage files and data, but they also should restrict users to authorized file operations so that files aren't accidentally overwritten or deleted. In addition, file services should track unauthorized actions.

File services are an important part of server-based and peer-to-peer networks. Two types of servers exist: dedicated and non-dedicated. Dedicated servers do nothing but fulfill requests to network clients. These are commonly found in client-server environments. Non-dedicated servers do double duty by requesting and providing services, and they are the backbone of the peer-to-peer structure. (A Windows 95 machine used to access files on the network and to provide access to a shared printer is an example of a non-dedicated server.)

Dedicated file servers have the following benefits:

- Files are in a specific place where they can be reliably archived.
- Central file servers can be managed more efficiently, with user and security data located in a single database.
- Central file servers can contain expensive, high-performance hardware that expedites file services and makes the file servers more reliable.
- The cost of specialized file server technology is shared by a large number of users.
- Centralized networks are more scaleable.

The following drawbacks, however, should be considered with regard to centralized file services:

- When all data is stored on a single server, a single point of failure exists. If the server fails, all data becomes unavailable, making proper design, management, and backup of the server essential.
- Because all clients contend for file services from a single source, average file-access times might be slower with a centralized file server than when files are stored on individual, local hard drives.

Centralized file services generally are chosen for organizations that want to achieve the highest levels of protection for their data files.

note

> Take care when discussing the words "centralized" and "distributed." These terms describe the utilization method of processor resources, file resources, or administrative tasks. For instance, a single administrator can watch over a network with a single file server and many PC clients. This network utilizes centralized administration and provides for centralized file access, but because the clients do their own processing, the network itself fits under the distributed computing model.

In a peer-to-peer network environment, any computer can share its files and applications with any other computer. The sharing of services must be established for each individual computer, and each user must have the skills required to manage the networking services on her PC. Because services are provided by many different computers, users must become aware of which computers are providing which services. Clearly, the skills and responsibility required of users are greater than for centralized file services.

Some advantages of distributed file storage include the following:

- No single point of failure exists. When a computer fails, only the files stored on that computer become unavailable.
- Individuals typically experience faster access for files located on local hard drives than for files on centralized file servers.

- No specialized server hardware is required. File services can be provided with standard PCs.

Some negative issues related to distributed file storage include the following:

- It's more difficult to manage the file service and to protect the integrity of files. File backup is more difficult when files are distributed across many PCs.
- Individual PCs generally don't have high-reliability hardware, such as uninterruptible power supplies and disk mirroring.
- File services provided by peers typically are not as fast or as flexible as file services provided by a central file server that is specifically designed for the purpose.
- Instead of upgrading one central file server when higher performance is required, you must upgrade each computer.

Organizations tend to choose peer-to-peer networking for two primary reasons. One is a desire to network with their current stock of PCs without the expense of a centralized server. Another is that peer-to-peer is an informal networking approach that fits the working style of many organizations. Microsoft implements peer-to-peer networking components into Windows for Workgroups, Windows 95, and Windows NT Workstation. Any of these operating systems is capable of sharing and accessing network resources without the aid of a centralized server. These systems are not optimized for file and printer sharing, however, and this sort of network structure is only recommended for smaller networks with limited security concerns.

Some key file services include:

- File transfer
- File storage
- Data migration

- File archiving
- File-update synchronization

Each of these services is discussed in the following sections.

File Transfer

Without a network, the options for transferring data between computers are limited. You can, of course, exchange files on floppy disks. This process came to be called “sneaker-net” because it consisted of networking by physically running around and hand-delivering floppy disks from desk to desk. Otherwise, you can use communication software to dial another computer and transfer files via a modem or a direct serial connection. With a network, users have constant access to high-speed data transfer without leaving their desks or dialing anywhere. Moving a file is as easy as depositing it in a shared directory.

When users transfer confidential files, the need for network security rises. You might need to limit file transfers to authorized users who are using password-controlled security systems, to assign file attributes that restrict the operations that may be performed with a file, or to encrypt files so they may be read only by authorized users. Each of these options is possible with networking.

Another important file-management task of the NOS is to provide and regulate access to programs and data stored on the file server’s hard drive, which is known as *file sharing*. File sharing is another main reason companies invest in a network. Companies save money by purchasing a single network version of an application rather than many single-user versions. Placing data files created by employees on a file server also serves several other purposes, such as security, document control, and backup.

note

One of the most difficult facts to convince your network users of is that their data is actually far more secure on the network file server than on their own workstation. The reasons for this are numerous, but they center on the fact that network servers are backed up more regularly and have more sophisticated authentication and permission structures than most workstations. Perhaps most important, servers generally are locked away and are not as vulnerable to physical damage or theft.

Centralized document control can be critical in a company where a document might need to be revised several times. In an architectural firm, for example, the design of a building might be created by using a drafting program, such as AutoCAD. The architects might produce several versions of the building plan as the client comes to a decision. If the plan is stored on the individual computers of each architect, the firm might not know which is the most recent version of the plan. The wrong version might have a more recent date (because of a backup, for example). If the plan is saved on a file server, however, each architect can work on the same file. The file sharing is regulated by the operating system.

A tape backup should always be installed on the network, forming the heart of a centralized backup strategy. All files located on the network can be backed up regularly. This strategy is much safer than relying on individual users to back up their workstations and can be more easily managed and controlled by the administrator.

File Storage

Most networks have some form of centralized file storage. For many years, companies have used the *online storage* approach to file storage. In the online storage scenario, data is stored on hard disks that are accessible on demand. The files that can be accessed on a server are limited to the amount of available hard drive space. Hard drives are fast, but even with drive prices decreasing in recent years, the cost to store a megabyte of data this way is still fairly high. Hard drives have another disadvantage; that is, generally, they cannot be removed for off-site storage or exchange or simply to build a library of files that are seldom required but must be fairly readily available.

Almost all companies have large amounts of infrequently used data. For example, there is usually no need to keep all the financial reports from the previous year online. However, those reports must be stored somewhere in case questions arise or an audit occurs.

Another common approach to file storage, therefore, is *offline storage*, which consists of removable media that is managed manually. After data is written to a tape or optical disk, the storage medium can be removed from the server and shelved. Users who require offline data might need to know which tape or optical disk to request. Some systems provide indexes or other aids that make requesting the proper offline storage element automatic. A system operator still has to retrieve the tape or disk and mount it on the server, however.

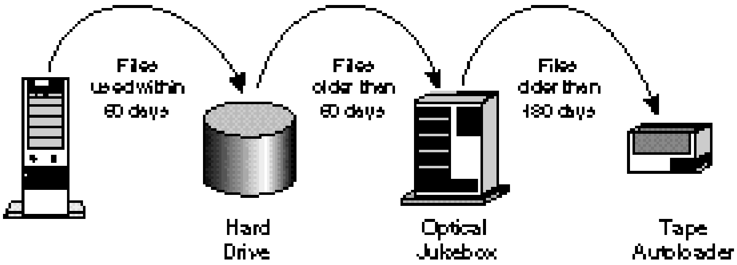
When the slow response of offline storage is unacceptable, a *near-line storage* approach may be selected. Near-line storage employs a machine, often called a *jukebox*, to manage large numbers of tapes or optical disks automatically. The proper tape or disk is retrieved and mounted by the jukebox without human intervention. With near-line storage, huge amounts of data can be made available with only slight delays, but at a much lower cost than would be required to store the data on hard drives.

Data Migration

Data migration is a technology that automatically moves less-used data from online storage to near-line or offline storage. The criteria for moving files can depend on when the files were last used, the owner of the files, file size, or a variety of other factors. An efficient data-migration facility makes locating migrated files easier for users. Figure 1.9 illustrates one approach to data migration.

Figure 1.9

Data migration.



File Archiving

File archiving (also known as backup) is basically offline storage that is primarily geared to creating duplicate copies of online files. These backup copies serve as insurance against minor or major system failures by creating a redundant copy of important system and data files.

Generally, network administrators enable file archiving from a centralized location. A single site, for example, can back up all the servers on a network. Many current backup systems also offer the capability to back up various client workstations, making it feasible to archive all files on the network to a central facility, whether the files are located on network servers or clients. This archive then is stored in a safe location, and a duplicate often is made and placed off the premises in case of disaster.

File-Update Synchronization

In its simplest form, *file-update synchronization* is a means of ensuring that all users have the latest copy of a file. File-update synchronization services can manage files by monitoring the date and time stamps on files to determine which files were saved most recently. By tracking the users who access the file, along with the date and time stamps, the service can update all the copies of the file with the most recent version.

File-update synchronization, however, can be considerably more involved. In a modern computing environment, it is not always feasible for all users to access all files in real time. A salesman, for example, might carry a notebook computer on which to enter orders. Dialing the central LAN every time an order was to be entered would be impractical, so the salesman would enter orders offline (while disconnected from the network) and store them in the laptop. That evening, he would call the central LAN, log in, and transmit all the day's orders at once.

During this process, files on the LAN must be updated to reflect new data in the salesman's portable computer. In addition, the salesman's PC might need to be updated, for example, with order confirmations or new pricing information. The process of bringing the local and remote files into agreement is also known as file-update synchronization.

File-update synchronization becomes considerably more challenging when additional users are sharing data files simultaneously. Complex mechanisms must be in place to ensure that users do not accidentally overwrite each other's data. In some cases, the system simply flags files that have multiple, conflicting updates and require a human to reconcile the differences. In Windows 95 and NT 4.0, the My Briefcase program provides this service.

Network Printing

After file services, printing is the second biggest incentive for installing a LAN. The following are just some of the advantages of network print services:

- Many users can share the same printers—a capability that is especially useful with expensive devices, such as color printers and plotters.
- Printers can be located anywhere, not just next to a user's PC.
- Queue-based network printing is more efficient than direct printing because the workstation can begin working again as soon as a job is queued to the network.
- Modern printing services can enable users to send facsimile (fax) transmissions through the network to a fax server.

In this book, print services are defined as network applications that control and manage access to printers, network fax, and other similar devices.

Network Applications

Application services enable applications to leverage the computing power and specialized capabilities of other computers on a network.

For example, business applications often must perform complex statistical calculations beyond the scope of most desktop PCs. Statistical software with the required capabilities might need to run on a mainframe computer or on a minicomputer. The statistical package, however, can make its capabilities available to applications on users' PCs by providing an application service.

The client PC sends the request for a calculation to the statistics server. After the results become available, they are returned to the client. This way, only one computer in an organization requires the expensive software license and processing power required to produce the statistics, but all client PCs can benefit.

Application services enable organizations to install servers that are specialized for specific functions. Currently, the most common application servers are database servers, which are discussed in the next section. Other application services, however, are beginning to emerge, such as fax and e-mail messaging services.

Application servers are an effective strategy for making a network more scaleable. Additional application servers can be added as new types of application needs emerge. If more power is needed for the application, only the application server needs to be upgraded. A database server, for example, might grow from a PC to a multiprocessor RISC system running Unix or Windows NT without requiring many (or even any) changes to the client PCs.

If demand for a server-based application begins to affect a server's performance, it's easy to move the application to a different server or even to dedicate a server specifically to that application.

This isolates the application and enables it and applications remaining on the other server to run more efficiently This scalability is one of the advantages of a LAN architecture.

Some common forms of network applications are as follows:

- Database services
- Electronic mail
- Groupware

Each of these applications is discussed in the following sections.

Database Services

Database servers are the most common examples of application servers. Because database services enable applications to be designed in separate client and server components, such applications are frequently called client/server databases.

With a client/server database, the client and server applications are designed to take advantage of the specialized capabilities of client and database systems, as follows:

- The client application manages data input from the user, generation of screen displays, some of the reporting, and data-retrieval requests that are sent to the database server.
- The database server manages the database files; adds, deletes, and modifies records in the database; queries the database and generates the results required by the client; and transmits results back to the client. The database server can service requests for multiple clients more or less at the same time.

Database services relieve clients of most responsibilities for managing data. A modern database server is a sophisticated piece of software that can perform the following functions:

- Provide database security
- Optimize the performance of database operations

- Determine optimal locations for storing data without requiring clients to know where the data is located
- Service large numbers of clients by reducing the time any one client is accessing the database
- Distribute data across multiple database servers.

note

Microsoft SQL Server and Exchange are two examples of applications that run at the server but are able to perform tasks requested by clients. Because of the way in which these applications are designed, both of these require a "back-end," or server, component and a "front-end," or client, component.

Distributed databases are becoming increasingly popular. They enable portions of databases to be stored on separate server computers, which may be in different geographic locations. This technique, known as *distributed data*, looks like a single logical database to users, but places the data users need in the most accessible location. East Coast sales data, for example, might be located on a database server in Boston, whereas West Coast sales data is on a server in San Diego. Special database mechanisms must be in place to keep the data in the copies of the database synchronized.

More simply, databases can be replicated. Complete copies of the database can be stored in various locations, which provides a redundancy factor because disaster is unlikely to strike all copies at once. Additionally, database replication improves application response time over low-bandwidth connections because users can access the database on the LAN rather than over a comparatively slow WAN link.

As shown in figure 1.10, the most popular strategies for replication databases are the following:

- **Master driven updates.** A single master server receives all updates and, in turn, updates all replicas.

- **Locally driven updates.** Any local server can receive an update and is responsible for distributing the change to other replicas.

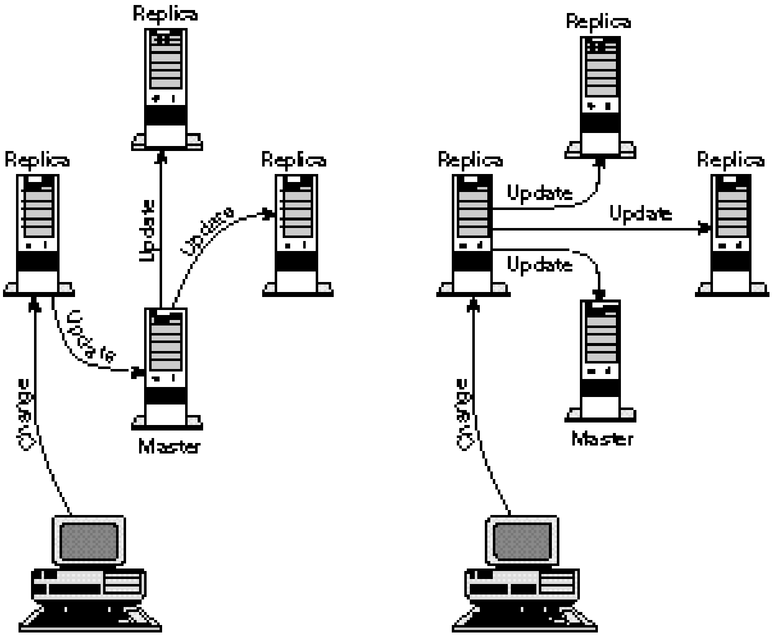


Figure 1.10

Master driven and locally driven database replications.

Electronic Mail

Electronic mail (e-mail) is technology for electronically transferring messages between networked computers. A LAN is an excellent platform for e-mail because it provides reliable, high-speed service at a low cost.

E-mail systems can service anything from a local workgroup, to a corporation, to the world. By installing e-mail routing devices, you can transfer mail smoothly and efficiently among several LANs. Moreover, e-mail also can be routed to and received from the Internet, which enables users in dozens of countries throughout the world to exchange electronic messages.

Early text-based e-mail has given way to elaborate systems that support embedded sound, graphics, and even video data.

The preferred e-mail system for Microsoft networks is Exchange, which is an advanced e-mail server included in Microsoft's BackOffice. Other major e-mail packages include Novell's Groupwise and Lotus Notes.

note

BackOffice is a suite of Microsoft products that are designed to run only on NT Server. These products include Exchange, Systems Management Server, Internet Information Server, SQL Server, and SNA Server.

Groupware

Groupware is a recent technology that enables several network users to communicate and cooperate on solving a problem through real-time document management. Interactive conferencing, screen sharing, and bulletin boards are examples of groupware applications. Examples of applications with groupware features are Microsoft Exchange, Novell's Groupwise and Lotus Notes.

Summary

This chapter has introduced you to a number of terms that are commonly used in computer networking and has examined many of the basic networking structures you need to understand as an administrator. Use the following exercises to put this information to use and then use the quiz to see how well you remember.

Exercises

Exercise 1.1: Logging on as a Peer

Objective: Explore the distinction between logging on locally and logging on to a domain from Windows NT Workstation.

Estimated time: 15 minutes

1. Boot a domain-based Windows NT Workstation computer. Press Ctrl+Alt+Del to reach the Logon Information dialog box.
2. The box labeled Domain should display the name of the Windows NT domain to which the Windows NT Workstation belongs. This option logs you in by using the domain account database located on a domain controller. Click the down arrow to the right of the Domain box. At least one other option—the name of the workstation itself—should appear in the domain list. This option logs you in by using the workstation's local account database. The local account database is completely separate from the domain database, and it gives you access only to the local computer.

note

If the workstation were a member of a peer-to-peer workgroup instead of a domain, the local logon option would be the only option. In fact, if a Windows NT workstation is a member of a workgroup, the Domain box doesn't even appear in the Logon Information dialog box—you automatically log on to the local account database.

3. Select the computer name in the Domain box. Type in a username and password for the local account.

note

> If you rarely or never use the local logon option, you may not even remember a username or password for a local account. If you can't remember a local username and password, log on to the domain from the workstation and find a local account by using the workstation's User Manager application (in the Administrative Tools group). Double-click on an account name to check the properties. Reset the password if necessary.

4. After you have successfully logged on to the local workstation account, you are operating as a peer in a peer-to-peer network would operate. Your credentials will carry you no farther than the local system. Try to access another network computer using Network Neighborhood. Windows NT will display a dialog box asking for a username and password. The computer you are accessing will validate your credentials separately.

Exercise 1.2: Windows NT Access Permissions

Objective: Explore Windows NT access permissions.

Estimated time: 10 minutes

1. Log on to a Windows NT system as an Administrator.
2. Right-click the Start button and choose Explore to start Explorer. (This exercise assumes you are using a Windows NT 4.0 system. If you are using Windows NT 3.x, start File Manager. The remaining steps are similar.)
3. Right-click on a directory in Explorer. The Directory Properties dialog box appears. Click on the Sharing tab.
4. In the Directory Properties Sharing tab, click on the Share As button and then click the Permissions button.
5. The Access Through Share Permissions dialog box appears. Through this dialog box, you can define which users or groups can access the share. Click Add to add users and groups to the permissions list.

continues

Exercise 1.2: Continued

6. If the directory is on an NTFS partition, you also see a Security tab in the Directory Properties dialog box. Click on the Security tab. From the Security tab, click on the Permissions button. The subsequent Directory Permissions dialog box enables you to set permissions for the directory itself (as opposed to the share).

note

A hard drive partition must be formatted for a specific file system. Windows NT uses the FAT and NTFS file systems. NTFS is a disk file system designed to make use of Windows NT's finest features, including file-level access permissions.

Exercise 1.3: Exploring the NT Workstation Service

Objective: Examine the effect of stopping Windows NT's redirector: the Workstation service.

Estimated time: 15 minutes

1. Log on to a Windows NT Workstation system as an Administrator.

2. Browse a shared directory on another computer by using Network Neighborhood or the Network Neighborhood icon in Explorer. You should see a list of the files on the shared directory.

3. From the Start menu, click Settings and choose Control Panel. Double-click the Services icon to start the Control Panel Services application.

4. From the Control Panel Services application, scroll down to the Workstation service and click the Stop button. This stops the Workstation service on your computer. Windows NT asks if you want to stop some other dependent services also. Click Yes.

5. Now try to access the shared directory by using Network Neighborhood. Without the redirector (the Workstation service) you will be unable to access the other computers on the network.

Review Questions

The following questions test your knowledge of the information in this chapter. For additional exam help, visit Microsoft's site at www.microsoft.com/train_cert/cert/Mcpsteps.htm.

1. You have a small office network of Windows NT and Windows 95 machines. One Windows NT machine will maintain a user account database for the network. Your network is a _________.

   A. workgroup

   B. domain

   C. coterie

   D. none of the above

2. _________ is a common fault-tolerance method.

   A. Remote access

   B. File service

   C. RAIN

   D. RAID

3. Your client computer isn't able to access services on other network PCs. It could be a problem with the ________ on your client computer.

   A. reflector

   B. redirector

   C. server service

   D. none of the above

4. You need to add a server to your domain that will compensate for the shortage of disk space on many of the older machines. You will be adding _________.

A. a peer

B. an application server

C. a file-and-print server

D. both A and C

5. You have a small office of Windows NT and Windows 95 computers. Each machine is responsible for its own security. Your network is a ________.

A. workgroup

B. domain

C. WAN

D. none of the above.

6. You need to add a server to your domain that will provide services designed to alleviate the problems caused by slow processor speeds on many of the older machines. You will be adding ________.

A. a peer

B. an application server

C. a file-and-print server

D. both A and C

7. You are designing a small network for a single office. The network will have nine users, each operating from one of nine networked PCs. The users are all accustomed to working with computers. The best solution is to use the ________ networking model.

A. server-based

B. peer-to-peer

C. a combination of A and B

D. any of the above

8. You are designing a small network for a single office. The network will have approximately 19 users who will roam freely among the 14 participating PCs. The best solution is to use the ________ networking model.

   A. server-based

   B. peer-to-peer

   C. a combination of A and B

   D. any of the above

9. Which type of network is most likely confined to a building or a campus?

   A. Local area

   B. Metropolitan area

   C. Wide area

   D. Departmental

10. Which of the following can concurrently provide and request services?

   A. Server

   B. Client

   C. Peer

   D. None of the above

11. The rules that govern computer communication are called ______.

   A. protocols

   B. media

   C. services

   D. network operating systems

12. Which file service is responsible for creating duplicate copies of files to protect against file damage?

    A. File transfer

    B. File-update synchronization

    C. File archiving

    D. Remote file access

13. Which two of the following are file services?

    A. Archiving

    B. Remote file access

    C. Update synchronization

    D. Data integrity

14. Which three statements are true regarding application services?

    A. Clients request services.

    B. Application services lack scalability.

    C. Application servers can be optimized to specialize in a service.

    D. Multiple services can be offered by the same server PC.

15. Which three statements are true regarding database services?

    A. A database server improves data security.

    B. All data must be located on the main database server.

    C. Database performance may be optimized.

    D. Database services enable multiple clients to share a database.

16. Which are the two most popular strategies for replication databases?

    A. Remote file access

    B. File-update synchronization

    C. Locally driven update

    D. Master server update

17. Which three are advantages of a centralized approach to providing file services?

    A. Centralized files may be readily archived.

    B. It provides the best possible performance.

    C. Management is efficient.

    D. The cost of high-performance, high-reliability servers can be spread across many users.

18. Which two are advantages of a distributed approach to providing file services?

    A. There is no central point of failure.

    B. It's less difficult to manage than a complex, centralized server.

    C. It's easily scaled to improve performance for all users.

    D. Specialized equipment is not required.