#

#DOM	A predefined keyword that is prefixed with a #. The #DOM is an LMHOSTS keyword and facilitates domain activity such as logon validation over a router or account sychronization and browsing.
#PRE	An LMHOSTS file keyword that defines which entries should be initially preloaded as permanent entries in the name cache. The preloaded entries can reduce network broadcasts, because the names will be resolved from cache rather than making a broadcast. Any entries with a #PRE tag get loaded automatically during initialization.
16-bit Application	An application that has been written using the 16 bit length for communicating data.
32-bit Application	An application that has been written using the 32 bit length for communicating data.
64-bit Application	An application that has been written using the 64 bit length for communicating data.
802.1x	802.1x is a networking protocol that defines how to support EAP (Extensible Authentication Protocol) over a wired or wireless LAN.

A

.ADM file	Template files that Internet Explorer and its Profile Manager use to create system policy files that control the IE options that are available to network users.
Accepted domains	Accepted domains identify the domains for which the organization is solely responsible and the SMTP domains from which the server will accept messages. There are three types of accepted domains in Exchange 2007: • Authoritative is the domain over which the Exchange server has sole responsibility. In a typical environment, the organization will have an e-mail domain of "company.com" which is hosted by the company's e-mail server. If another e-mail system or domain exists in the environment, internal and external relays are employed. • An internal relay is an e-mail domain that is hosted by another Active Directory Forest within the Exchange organization. This system uses different e-mail addresses, but all incoming mail goes through the Exchange organization. • An external relay accepts e-mail for an external organization and then delivers it to an external entity such as the Internet via the Edge Transport server.
Access Control List (ACL)	A list that contains information on allowed and denied access to folders and files.
Access token	A grouping of information used to control a user's access to network resources. After the logon process, the access token is used to control

	access to all secured objects. An access token includes the user's SID (security ID), ID of users' group memberships, and rights assigned to the user. The access token is generated during the logon process and is not updated while the user is logged on.
Account lockout	A mechanism to lock out accounts after multiple failed logon attempts. This reduces the chance of an unauthorized person gaining access to the network.
Account Operator	A specific user who has been designated an Account Operator can create, delete, and modify user accounts, global and local groups, and set account policies.
Account policy	Determines the characteristics of passwords for user accounts. The policy sets requirements for password age, length, and uniqueness.
ACL (Access Control List)	A list that contains information on allowed and denied access to folders and files.
Active Desktop	A feature of Microsoft Internet Explorer that lets you display content from Web pages on the computer desktop, using Dynamic HTML, Webcasting, and active channels.
Active Directory	The new Windows 2000 directory service. It stores information about all the network resources such as user accounts, computers, printers, servers, and so on. Active Directory makes it easy for administrators to manage the network resources, and makes it easy for users to locate and use the resources.
Active Directory Sites and Services Snap-In	A Microsoft Management Console (MMC) snap-in that lets you create and work with the configuration partition of an Active Directory database.
Active Server Pages (ASP)	Microsoft's answer to the slower and more limited performance of CGI scripts written in Perl. They combine HTML pages, scripts, programming objects, and ActiveX components to create dynamic Web pages.
ActiveX	A set of programming tools based on the Component Object Model (COM), which provides the low-level services that allow programming objects to communicate with each other. ActiveX is used for Internet applications that need to be optimized for speed and size.
AD (Advertised Distance)	The Advertised Distance (AD) is the cost to the destination network as reported by the neighbor router. The AD is also called the reported distance (RD).
Ad hoc	A wireless networking architecture topology that does the following: • Works in peer-to-peer mode without a WAP (the wireless NICs in each host communicate directly with one another) • Uses a physical mesh topology • Cheap and easy to set up but cannot handle more than four hosts • Requires special modifications to reach wired networks

Adapter card	The physical interface between the computer and the network cable. An adapter card communicates with the computer's hardware, firmware, and software to allow the computer to communicate with the local area network. Also called a network adapter card, network card, or NIC.
Adapter teaming	Adapter teaming is the use of two or more adapter cards in a system to eliminate a network adapter as a single point of failure. In adapter teaming: • Up to four adapter teams can be supported with two to four adapters in each team. • Each adapter is connected to the same network segment via a network switch or hub.
Address family	An address family is a group of network protocols whose network addresses share a common format.
Address Resolution Protocol (ARP)	A protocol that maps an IP address to the Media Access Control (MAC) address of a computer on a network.
Adjacency	An adjacency is the connection that is established when neighboring routers transfer packets.
ADMD (Administration Management Domain)	An ADMD is a public operating agency that controls an X.400 management domain. These domains are the backbone for transferring electronic messages. ADMDs handle messages sent between PRMDs.
Administration Management Domain (ADMD)	An ADMD is a public operating agency that controls an X.400 management domain. These domains are the backbone for transferring electronic messages. ADMDs handle messages sent between PRMDs.
Administrative distance	The administrative distance is a metric used to show how trustworthy a router deems information from a specific protocol. Administrative distances are as follows: • 0= Connected interface • 0= Static route out of an interface • 1= Static route to a next-hop address • 5= EIGRP summary route • 20= External BGP • 90= Internal EIGRP • 100= IGRP • 110= OSPF • 115= IS-IS • 120= RIPv1 and RIPv2 • 140= EGP • 160= ODR • 170= External EIGRP • 200= Internal EIGRP • 255= Unknown

	Protocols with lower administrative distances are considered more trustworthy.
Administrative share	Windows 2000 provides share names that are used for administration. These names are C$, D$, E$, etc. and Admin$.The $ hides the shared folder from a user who browses the computer. Administrative shares are used to remotely connect to a computer to perform administrative tasks.
Administrative template	A group of registry settings stored in a file (Registry.pol). Adminstrative templates can be distributed using Active Directory-based Group Policy Objects (GPOs).
Administrator	A user who is granted rights to create, delete, or modify user accounts. They also have rights to create user policies, move folders, add and remove hardware from the computer, and access the file system.
Administrators	A built-in group in Windows 2000. Members of the Administrators group have full administrative capabilities (see Administrator).
ADSI Edit	A graphical Windows 2000 support tool that lets you view, edit, and create objects and attributes in the Active Directory database.
Advanced Research Projects Agency (ARPA)	The first group to conduct packet-switching network experiments.
Advanced Research Projects Agency Network (ARPANET)	In the late 1960s and early 1970s, the United States Department of Defense sponsored this project to create a network between government and research institutions. The project became the foundation for what is now known as the Internet.
Advanced RISC Computing (ARC) naming convention	The syntax used for recovering data in a secondary partition. ARC paths specify the hardware adapter and disk controller, the numbers of the hardware adapter, the SCSI bus, the disk, and the partition.
Advertised Distance (AD)	The Advertised Distance (AD) is the cost to the destination network as reported by the neighbor router. The AD is also called the reported distance (RD).
AH (Authentication Header)	Authentication Header (AH) is one of two services comprising IPSec, Encapsulating Security Payload (ESP) being the other. AH is used primarily for authenticating the two communication partners of an IPSec link. The AH provides message integrity through authentication, verifying that data are received unaltered from the trusted destination. AH provides no privacy however, and is often combined with ESP to achieve integrity and confidentiality.
Alert	An action, defined by an administrator, that takes place in response to an administrator-specified event. The action can be the execution of a job, or e-mailing/paging a particular operator.

American National Standards Institute (ANSI)	A standards body that provides computing standards. It is a voluntary organization comprised of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the IEC and the ISO.
American Wire Gauge (AWG)	A U.S. standard set of wire sizes that apply to copper wires, including household electrical wiring and telephone lines. The higher the number, the thinner the wire.
ANDing process	The internal process used by TCP/IP to determine whether a packet is destined for a host on a local or remote network. TCP/IP performs the function of ANDing the host's IP address with its subnet mask. When a packet is sent on the network, the destination IP address is ANDed with the same subnet mask.
Anonymous authentication	An authentication method that does not require the user to enter a username and password to gain access to resources such as Web sites. Some anonymous access methods (like FTP) require an e-mail address as a username, but this is not a secure solution because a fake e-mail address can be used.
ANSI (American National Standards Institute)	A standards body that provides computing standards. It is a voluntary organization comprised of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the IEC and the ISO.
Answer file	A script file that you use to automate Windows installations by supplying answers to questions that you would normally have to answer yourself. You can modify the sample Unattend.txt file or use Setup Manager to create a new answer file.
API (Application Programming Interface)	The API can be provided by any vendor to provide functionality to an application or operating system. Each vendor publishes its API's so that developers can code to that application's APIs.
APIPA (Automatic Private IP Addressing)	APIPA is a Microsoft implementation of automatic IP address assignment without a DHCP server. Using APIPA, hosts assign themselves an IP address on the 169.254.0.0 network (mask of 255.255.0.0). With APIPA: • The host is configured to obtain IP information from a DHCP server (this is the default configuration). • If a DHCP server can't be contacted, the host uses APIPA to assign itself an IP address. • The host only configures the IP address and mask. It does not assign itself the default gateway and DNS server addresses. For this reason, APIPA can only be used on a single subnet.

Apple MacOS	The proprietary Macintosh operating system used by Apple computers.
Applet	A small application built into another application or an operating system. The programs in the Windows Control Panel are applets. Also called programs in Microsoft documentation.
AppleTalk	The set of network protocols native to Apple computers.
Application	A software program that performs a specific function for the user or another program. For example, word processors, database programs, spreadsheets, and graphics packages are applications.
Application files	Files necessary for an application to run, such as .EXE, .DLL, and other files.
Application Layer (OSI model)	Layer 7 of the OSI reference model. This layer provides services to application processes (such as electronic mail, file transfer, and terminal emulation) that are outside of the OSI model. The application layer identifies and establishes the availability of intended communication partners (and the resources required to connect with them), synchronizes cooperating applications, and establishes agreement on procedures for error recovery and control of data integrity. Corresponds roughly with the transaction services layer in the SNA model. See also data link layer, network layer, physical layer, presentation layer, session layer, and transport layer.
Application log	An Event Viewer file containing application events such as file errors. Application developers determine the events that their applications write to the application log.
Application Programming Interface (API)	The API can be provided by any vendor to provide functionality to an application or operating system. Each vendor publishes its API's so that developers can code to that application's APIs.
Application Server	Application servers run certain software applications that can be accessed by users.
ARC (Advanced RISC Computing) naming convention	The syntax used for recovering data in a secondary partition. ARC paths specify the hardware adapter and disk controller, the numbers of the hardware adapter, the SCSI bus, the disk, and the partition.
Archive Bit	An archive bit is a file attribute that indicates whether a file was backed up since it was modified.
ARIN	A Windows Socket specification using Visual Basic.
ARP (Address Resolution Protocol)	A protocol that maps an IP address to the Media Access Control (MAC) address of a computer on a network.
ARP cache	A portion of memory that is used to store a hardware address and IP address. The ARP cache is always checked for an IP address/hardware address mapping before an ARP request broadcast is initiated.
ARPA (Advanced Research Projects Agency)	The first group to conduct packet-switching network experiments.

ARPANET (Advanced Research Projects Agency Network)	In the late 1960s and early 1970s, the United States Department of Defense sponsored this project to create a network between government and research institutions. The project became the foundation for what is now known as the Internet.
AS (Autonomous System)	An Autonomous System (AS) is a set of routers under a common administration and with common routing policies. Each Autonomous System (AS) in BGP appears to other autonomous systems to have a single coherent interior routing plan.
AS path	The AS path (type code 2) is a well-known mandatory BGP attribute that lists the different autonomous systems to reach a network.
ASBR (Autonomous System Boundary Router)	An Autonomous System Boundary Router (ASBR) is a router that has an interface to an external autonomous system (e.g. RIP or EIGRP). ASBRs can import and export non-OSPF network information to and from the OSPF network.
ASP (Active Server Pages)	Microsoft's answer to the slower and more limited performance of CGI scripts written in Perl. They combine HTML pages, scripts, programming objects, and ActiveX components to create dynamic Web pages.
Attenuation	The loss of signal strength over distance.
Attribute version number	A counter that identifies how many times the value for an Active Directory attribute has changed. During replication, attribute values with higher version numbers override values of the same attribute with lower version numbers.
Audit log	A file containing information about events you have chosen to monitor, such as logging on and logging off, accessing files and objects, and system shutdowns. You may want to save auditing logs to help you track trends. Tracking trends helps you plan for growth and detect unauthorized use of resources. For more accurate trend information, it is better to view logs that are kept over a few months.
Authentication	The process of supplying a valid user name and password in order to access resources on a network or computer.
Authentication Header (AH)	Authentication Header (AH) is one of two services comprising IPSec, Encapsulating Security Payload (ESP) being the other. AH is used primarily for authenticating the two communication partners of an IPSec link. The AH provides message integrity through authentication, verifying that data are received unaltered from the trusted destination. AH provides no privacy however, and is often combined with ESP to achieve integrity and confidentiality.
Authoritative domain	A domain is considered authoritative if your organization hosts mailboxes for recipients within the domain.

Authoritative restore	A restoration method which uses the Backup utility to return Active Directory database to the state it was in before the backup, then uses NTDSUTIL to mark an object as the most current. Most current objects will not be overwritten with the data from the server's replication partners during Windows 2000 replication. Use the authoritative restore when an object is deleted after the last backup. Restore the database with the last backup file, then update all the data modified after the last backup, except the one you marked with NTDSUTIL.
Authoritative Server	An authoritative server is a DNS server that has a full, complete copy of all the records for a particular domain.
Autodiscover service	The Autodiscover service in Exchange 2007 is designed to make it easier for users to set up their profiles in Outlook or for their Exchange Active Sync devices. The Autodiscover service automatically adds the following information to a user's profile: • The server on which the user's mailbox resides • The user's display name • Separate connection settings for internal and external connectivity • The URLs for Exchange features associated with the user • Outlook Anywhere server settings
Automatic Private IP Addressing (APIPA)	APIPA is a Microsoft implementation of automatic IP address assignment without a DHCP server. Using APIPA, hosts assign themselves an IP address on the 169.254.0.0 network (mask of 255.255.0.0). With APIPA: • The host is configured to obtain IP information from a DHCP server (this is the default configuration). • If a DHCP server can't be contacted, the host uses APIPA to assign itself an IP address. • The host only configures the IP address and mask. It does not assign itself the default gateway and DNS server addresses. For this reason, APIPA can only be used on a single subnet.
Autonomous System (AS)	An Autonomous System (AS) is a set of routers under a common administration and with common routing policies. Each Autonomous System (AS) in BGP appears to other autonomous systems to have a single coherent interior routing plan.
Autonomous System Boundary Router (ASBR)	An Autonomous System Boundary Router (ASBR) is a router that has an interface to an external autonomous system (e.g. RIP or EIGRP). ASBRs can import and export non-OSPF network information to and from the OSPF network.
Autosummarization	Autosummarization transpires when a router that uses a classful routing protocol sends and update about a subnet of a classful network across an interface belonging to a different classful network and assumes that the remote router will use the default subnet mask for that class of IP

	address. The following protocols use autosummarization: • RIP • EIGRP • BGP
AWG (American Wire Gauge)	A U.S. standard set of wire sizes that apply to copper wires, including household electrical wiring and telephone lines. The higher the number, the thinner the wire.

B

Back end	The server where database operations occur. The back end fulfills client requests by receiving structured requests from the client, processing the requests, and returning the results. It is usually more powerful than the client.
Backbone area	A backbone area acts as a hub for inter-area transit traffic and the distribution of routing information between areas. All OSPF networks have at least one backbone area, also known as an *area 0*.
Backbone router	A backbone router is located in the perimeter of the backbone area. Backbone routers: • Maintain OSPF routing information using the same procedures and algorithms as internal routers. • Have at least one interface that is connected to area 0.
Backup Designated Router (BDR)	On each subnet, a single OSPF router is identified as the Backup Designated Router (BDR). The BDR becomes the Designated Router (DR) if the DR becomes unavailable.
Backup Domain Controller (BDC)	A server containing a replicated copy of the domain database. Each Windows NT domain will have one PDC (Primary Domain Controller) with zero or more BDCs (backup domain controllers).
Backup log	A text file that records backup operations. The log is helpful when restoring data. You can print it or read it in a text editor.
Backup marker	Windows Backup can set a backup marker, also known as the archive attribute, indicating that the file has been backed up.
Backup Operators	A group that has permission to perform backups on a system. This group should have only sufficient rights to perform a backup. They typically use the Windows backup software.
Backup set	A term used to describe a group of files or folders on a single volume from a single backup operation. A group of tapes is called a family set.
Baseband	Baseband signalling allows one signal at a time on the network medium (cabling).

Baseline	A server baseline is a snapshot of the performance statistics of your server that is used as a logical basis for future comparison. Server baselines enable you to effectively monitor the performance of your system to determine when changes negatively impact performance or when systems need upgrading or replacing.
Baselining	Documenting a network's average performance statistics over time.
Basic authentication	An authentication method that requires the user to enter a valid username and password for a Windows user account. This information passes between the server and client in clear text.
Basic disk	A physical disk containing primary partitions, extended partitions, or logical drives. Using Windows NT 4.0 or earlier, you can create RAID-5 volumes for basic disks; they can also be spanned, mirrored, or part of a stripe set. MS-DOS can access basic disks. Compare dynamic disk.
Basic multicast	Basic multicast supports multicast applications within an enterprise campus. It is an interactive, intra-domain form of multicast that provides integrity within a network when combined with a reliable multicast transport such as PGM.
Batch file	A set of commands used to perform a specific operation on a computer.
Baud rate	The number of bits per second that are physically signaled over a communication medium. The term "baud" originally referred to the number of dots per second that could be signaled using Morse code over particular telegraph systems. The unit of measure was named after J.M.E. Baudot, the developer of the first printer for telegraph systems.
BDC (Backup Domain Controller)	A server containing a replicated copy of the domain database. Each Windows NT domain will have one PDC (Primary Domain Controller) with zero or more BDCs (backup domain controllers).
BDR (Backup Designated Router)	On each subnet, a single OSPF router is identified as the Backup Designated Router (BDR). The BDR becomes the Designated Router (DR) if the DR becomes unavailable.
Best information	Using the split horizon method (also called best information), routers keep track of where the information about a route came from. Routers do not report route information to the routers on that path. In other words, routers do not report information back to the router from which their information originated.
BGP (Border Gateway Protocol)	Border Gateway Protocol (BGP) is a policy-based, interautonomous system routing protocol that exchanges reachability information with other BGP systems.
BGP Address Family Identifier (AFI)	The Cisco BGP Address Family Identifier (AFI) model was introduced with multiprotocol BGP. It is designed to be scalable and modular, and to support multiple AFI and Subsequent Address Family Identifier (SAFI) configurations.
BGP attributes	BGP attributes are used to select the best path to be entered into the routing table and propagated to the BGP neighbors. BGP attributes can

	be well-known mandatory, well-known discretionary, optional transitive, or optional nontransitive. The following definitions are used to define BGP attributes:
	
	• Well-known attributes are standard. All implementations of BGP support standard attributes.
	  ▪ Well-known mandatory attributes have to be present in all implementations of BGP.
	  ▪ Well-known discretionary attributes are implemented according to the needs of individual implementations of BGP.
	• Optional attributes are non-standard, meaning they are specific to particular implementations of BGP.
	  ▪ Optional transitive attributes are transmitted between two or more autonomous systems.
	  ▪ Optional nontransitive attributes remain in a single autonomous system.

BGP peer	A BGP peer (also called a neighbor) is a BGP speaker that is configured to form a neighbor relationship with another BGP speaker. Neighbor relationships allow BGP speakers to directly exchange BGP routing information with one another.
BGP peer group	A BGP peer group consists of the neighbors of a router that is being configured. All routers in a BGP peer group have the same update policies; thus allowing updates to be generated only once for the entire peer group.
BGP speaker	A BGP speaker is any router that runs BGP.
BGP synchronization rule	The BGP synchronization rule states that a BGP router cannot use or advertise a route that it has learned from internal BGP (iBGP) to an external neighbor unless it has also been established through an internal gateway protocol, such as RIP or OSPF.
Bidirectional PIM	Bidirectional PIM explicitly builds shared bi-directional trees. Bidirectional PDM: • Never builds a shortest path tree. • May have longer end-to-end delays than PIM-SM. • Is scalable because it needs no source-specific state.
Binary compatible	An application that runs on any Windows-supported platform, not only on the hardware for which it was originally compiled.
Binary Synchronous Communications Protocol (BISYNC)	A Data Link layer protocol for synchronous communication devices.
Bindery	The system that networks running Novell NetWare use to validate user accounts and passwords. It is the equivalent of the directory database in Windows NT.

Binding	The process of assigning services to network components.
BISYNC (Binary Synchronous Communications Protocol)	A Data Link layer protocol for synchronous communication devices.
Bit	The smallest unit of data a computer uses. A bit is a binary value, either a 0 or a 1.
Bluetooth	A proposed standard of the IEEE 802.15 committee, designed to allow people to connect in PAN (personal area network) configurations using cell phones, PDAs (personal digital assistants), printers, mice, keyboards and other Bluetooth equipped devices.
B-node	A type of broadcast used by NetBIOS over TCP/IP. The B-node uses UDP datagrams to broadcast for name registration and resolution. B-node broadcasts are usually not forwarded by routers, and only computers on the local network can respond.
Body parts	Body parts are the codes for the text, data, and other information included in an e-mail message.
Boot disk	A floppy disk containing an operating system that is used to boot up a PC in the absence of the PC's operating system.
Boot partition	The partition on a hard drive where the Windows operating system files reside.
Boot.ini	A file that builds the Boot Loader Operating System Selection menu. The screen that is displayed is known as the boot loader screen and allows a user to select an operating system from the screen. If no selection is made, NTLDR loads the operating system specified by the default parameter in the Boot.ini file. To change the default entry, you must edit the Boot.ini file.
BootP (Bootstrap Protocol)	BootP is used to discover the IP address of a device with a known MAC address. BootP is an enhancement to RARP, and is more commonly implemented than RARP. As its name implies, BootP is used by computers as they boot to receive an IP address from a BootP server. The BootP address request packet sent by the host is answered by the server.
Bootstrap Protocol (BootP)	BootP is used to discover the IP address of a device with a known MAC address. BootP is an enhancement to RARP, and is more commonly implemented than RARP. As its name implies, BootP is used by computers as they boot to receive an IP address from a BootP server. The BootP address request packet sent by the host is answered by the server.
Bootstrap Router (BSR)	A Bootstrap Router (BSR) is a capability that was added in PIM version 2 to automate and simplify the Auto-RP process. It is enabled by default in Cisco IOS releases supporting PIMv2.
Border Gateway Protocol (BGP)	Border Gateway Protocol (BGP) is a policy-based, interautonomous system routing protocol that exchanges reachability information with other BGP systems.

Bottleneck	A bottleneck is a point in a system of processes that does not have the capacity to perform the functions required of it. This lack of processing capacity impedes overall information flow and negatively impacts the performance of the whole system. Changes in the system, including increased volume, can cause bottlenecks.
Bounce	The longest acceptable round-trip time for a test message to travel between the monitor's home server and the target server.
Boundary layer	Parts of the network architecture that provide a common programming interface. Programmers can use these components to create independently-coded drivers and other programs which extend the operating system's abilities. Boundary layers in Windows include the Transport Driver Interface (TDI) and the Network Device Interface Specification (NDIS) 4.0.
Bridge	A data forwarding device that provides data transfer at the data link layer in the OSI model. A bridge is not used as much in networks because routers have assumed the responsibility for routing data at the network layer of the OSI model.
Bridgehead server	A domain controller that participates in intersite replication.
Broadband	Broadband signalling divides the network medium (cabling) into multiple channels, allowing several signals to traverse the medium at the same time.
Broadcast	In broadcast transmission, a single device transits a message to all of the other devices in a given address range. Broadcast messages can be received by all hosts on the subnet, all subnets, or all hosts on all subnets.
Broadcast domain	The portion of the network that can receive a broadcast. Not all routers have the capability to forward broadcasts. Those that do usually disable this feature and keep the broadcast on the local network.
Broadcast storm	A broadcast storm occurs when so many messages are broadcast across the network at the same time that they exceed the network's bandwidth.
Broadcasts	A request from the source host for a name query request on the local network. Each computer on the local network receives the broadcast and checks its local NetBIOS table to see if it owns the requested name.
Brouter	A device that combines the features of a bridge and a router. For data packets that use a non-routable network/transport protocol, a brouter acts like a bridge. For data packets that use a routable network/transport protocol, a brouter acts like a router.
Browser	A software application you use to display pages from the World Wide Web.
BSR (Bootstrap Router)	A Bootstrap Router (BSR) is a capability that was added in PIM version 2 to automate and simplify the Auto-RP process. It is enabled by default in Cisco IOS releases supporting PIMv2.

Built-in account	A built-in account is an account already created by Windows. The Guest account and the Administrator account are built-in accounts.
Built-in capabilities	Built-in groups are predefined groups that have predetermined set of user rights.
Bus	Bus is a network topology that consists of a trunk cable with nodes either inserted directly into the trunk, or nodes tapping into the trunk using offshoot cables called drop cables.
Byte	A unit of information made up of eight bits. Usually, a byte represents a character.

C

.CDF file	Channel Definition Format files. Text files that contain a personalized index for a Web site, so you can download only the content that interests you. Using a .CDF converts a Web site into a channel.
.CHK file	Exchange 2007's database engine is referred to as the Extensible Storage Engine (ESE). ESE is a transactional database that writes information into RAM memory and into a log file. Once it is in the log file, it will be written to disk. There are a number of files used to store information: • An .edb file is located in the actual database itself. All of a user's messages, folders, public folders, contacts, appointment information, etc. is all stored on the .edb file. An .edb file size can exceed multiple GB. • A .log file is an ESE transaction log file. All .log files are 1 MB. • A .jrs file is a reserve log file which is used to commit any transactions that are still in memory in the event of the server running out of disk space. All .jrs files are 1 MB. • A .chk file is used to identify which log files have been committed to the database. The size of .chk file varies from 2-3 KB. The ESE takes the following steps to write information into database files: 1. The ESE writes a message into memory RAM when it arrives at the server. 2. At the same time that information is written to RAM, it's written into the current .log file. All current log files are named E00.log. The information is written in a sequential format until the log file is full. When the log file is full, it will be renamed. 3. Once it has been committed to the log file, the information is written to the .edb file. 4. The checkpoint file is updated to indicate that the transaction log that has been committed to the database.
.CSV file	A comma-delimited text file.

Cache	A file that contains host information needed to resolve names outside of authoritative domains. It also contains names and addresses of root name servers.
Cache Manager	A part of the I/O Manager that improves a computer's performance by temporarily storing files in memory instead of reading and writing them to the hard disk. The Cache Manager uses virtual address space to cache data.
CAL (Client Access License)	A client access license permits a client to connect to a Windows 2000 server.
Callback	A remote access server configuration that provides network security by restricting network access to a specified list of phone numbers. When a client calls the server, the server hangs up, then calls the client back at the appropriate phone number.
Canonical Name (CNAME) record	Enables you to associate more than one host name with an IP address. This concept is also referred to as aliasing.
Carrier Sense Media Access/Collision Avoidance (CSMA/CA)	CSMA/CA is the technology used by Ethernet and wireless networks to control media access and avoid (rather than detect) collisions. CSMA/CD works as follows: • If a host detects traffic on the network, it experiences a longer back-off time than hosts on a wired network before attempting to transmit again. • Every transmission must be acknowledged. As every frame is acknowledged by the receiving host, other hosts receive a message indicating that they must wait to transmit.
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	CSMA/CD is the technology used by Ethernet. CSMA/CD works as follows: 1. The system listens for traffic, if the line is clear it begins transmitting. 2. During the transmission, the system listens for collisions. 3. If no collisions are detected, the communication succeeds. If collisions are detected, an interrupt jam signal is broadcast to stop all transmissions. Each system waits a random amount of time before starting over at step 1.
CAS (Client Access server)	Client Access server role is required in every Exchange 2007 organization because it supports the client applications Outlook Web Access and Exchange ActiveSync and also the Post Office Protocol version 3 (POP3), and Internet Message Access Protocol version 4rev1 (IMAP4) protocols.
Cascading physical star	A logical ring topology created with the FDDI standard. In this topology, single-attachment hubs connect single-attachment stations to a network.

Case sensitive	All capital and lower-case characters must be typed exactly as they appear. For example, if the password was "Himalayas" and you typed "himalayas," you would not be allowed to log on.
CCR (Local Continuous Replication)	Cluster Continuous Replication (CCR) combines the asynchronous log shipping and replay technology of Exchange 2007 with the failover and management features provided by the Microsoft Windows Cluster service. CCR does not have a single point of failure and provides high availability by replicating data on a passive node, so the clustered Mailbox server can operate on either node at any time.
CD File System (CDFS)	A read-only file system for CD-ROMs, supported by Windows 2000.
CDFS (CD File System)	A read-only file system for CD-ROMs, supported by Windows 2000.
Central Processing Unit (CPU)	The logic circuitry that responds to instructions and runs the computer. Also called a processor.
Centralized computing	A configuration in which all the data and applications are stored and executed on a mainframe computer. The terminals act only to accept keystrokes on the keyboard and display data from the mainframe computer.
Centralized network administration	The ability to manage network resources from a centralized database location. The Windows 2000 directory service provides the capability to manage resources centrally.
Certificate	A digitally signed statement issued by a Certification Authority (CA). It contains a public key and certifies that a specific person, organization, device, or service is the only holder of the corresponding private key. Certificates commonly use the ITU-T X.509 international standard.
Certificate authority	A certificate authority (CA) is the component of the public key infrastructure entrusted to issue, store, and revoke certificates. A certificate authority accepts certificate requests, verifies the information provided by the requester, creates and digitally signs the certificate, and issues the certificate to the requester. It also revokes certificates and publishes a certificate revocation list (CRL).
Certificate Revocation List (CRL)	Digital certificates usually expire after one year, but CAs can revoke certificates earlier for various reasons. All revoked certificates are stored in the certification revocation list, which is open to all users. This allows users to check the list to verify whether a given certificate is valid.
Certificate Services	The Microsoft Windows 2000 component that lets a system administrator create a certificate authority to issue, revoke, and manage digital certificates as part of a public key infrastructure.
Certification Authority server	A Certification Authority server creates new encryption keys for clients and publishes public keys for users. The Exchange KM Server is a Certification Authority server.
CGI (Common Gateway Interface)	A software program that allows Web servers to send data to an application and receive information back from the application, regardless of the operating system the application is running under.

CGMP(Cisco Group Management Protocol)	Cisco Group Management Protocol (CGMP) is a Cisco proprietary protocol that works between the router and the switch. In CGMP, the switch only allows multicast traffic to flow through specific ports according to client data from the router instead of flooding data across all ports. CGMP: • Enables routers to inform each of their directly-connected switches of IGMP registrations from hosts accessible through the switch. • Forwards multicast traffic only to ports on which the requesting routers are located. • Is the most common multicast switching solution. • Is based on a client/server model in which the router acts as a server and the switch acts as a client.
Challenge Handshake Authentication Protocol (CHAP)	CHAP is an authentication encryption protocol designed to protect passwords while in transit from a client to the logon server. CHAP periodically verifies the identity of a peer using a three-way handshake. CHAP ensures that the same client or system exists throughout a communication session by repeatedly and randomly re-testing the validated system. This test involves the security server sending a challenge message to the client. The client then performs a one-way hash function on the challenge and returns the result to the security server. The security server performs its own function on the challenge and compares its result with that received from the client. If they don't match the session is terminated.
Channel Service Unit/Data Service Unit (CSU/DSU)	A hardware device that converts a digital data frame from a LAN format into a WAN format and vice versa.
Channels	Web sites that you can customize with a .CDF file to give you only the information that you want to see. When you subscribe to a channel, Internet Explorer monitors the Web sites included in the channel and downloads only the information that fits the channel's parameters.
CHAP (Challenge Handshake Authentication Protocol)	CHAP is an authentication encryption protocol designed to protect passwords while in transit from a client to the logon server. CHAP periodically verifies the identity of a peer using a three-way handshake. CHAP ensures that the same client or system exists throughout a communication session by repeatedly and randomly re-testing the validated system. This test involves the security server sending a challenge message to the client. The client then performs a one-way hash function on the challenge and returns the result to the security server. The security server performs its own function on the challenge and compares its result with that received from the client. If they don't match the session is terminated.
Character set	A set of 256 letters, digits, and symbols specific to a country or language. The character set selected during SQL installation specifies the characters SQL Server will recognize in the various data types. The first

	128 values are called printable characters, and the last 128 values are called extended characters. Printable characters are the same for each set; extended characters vary from set to set. See also Unicode characters.
Checkpoint	A marked point in a SQL transaction log. It represents a point at which completed transactions and modified database pages were written to disk.
Chkdsk	An MS-DOS utility you can use to scan and repair both FAT and Windows NT NTFS volumes.
CIDR (Classless Inter-Domain Routing)	A technique used to collapse Class C entries into a single entry corresponding to all the Class IDs that are being used by that organization. This allows companies to use many Class C addresses rather than requesting a Class B address, since the availability of IP addresses is scarce.
Circuit Switching	A circuit switched network uses a dedicated connection between sites. Circuit switching is ideal for transmitting data that must arrive quickly in the order it is sent, as is the case with real-time audio and video.
Circuit-level Gateway	A circuit-level gateway monitors traffic between trusted hosts and un-trusted hosts via virtual circuits or sessions. A circuit-level gateway: • Verifies sequencing of session packets. • Hides the private network from the public network. • Does not filter packets. Rather it allows or denies sessions.
Circular logging	Circular logging is a logging method in which older logs are overwritten with new logging information. This method saves disk space but does not provide as much fault tolerance.
Cisco Group Management Protocol (CGMP)	Cisco Group Management Protocol (CGMP) is a Cisco proprietary protocol that works between the router and the switch. In CGMP, the switch only allows multicast traffic to flow through specific ports according to client data from the router instead of flooding data across all ports. CGMP: • Enables routers to inform each of their directly-connected switches of IGMP registrations from hosts accessible through the switch. • Forwards multicast traffic only to ports on which the requesting routers are located. • Is the most common multicast switching solution. • Is based on a client/server model in which the router acts as a server and the switch acts as a client.
Class A address	An IP address range that is assigned to networks with very large numbers of hosts. The Class A address assigns the high order bit to zero. The next seven bits complete the network ID portion of the address. The

	remaining 24 bits make up the host ID. The address range for the first octet (8 bits) is 1-126.
Class B address	An IP address range that is assigned to networks with medium to large networks. The Class B address assigns the two high order bits to binary 1 0 . The next 14 bits complete the network ID. The last 16 bits are used for the host ID. The address range for the first octet (8 bits) is 128 B 191.
Class C address	An IP address range that is used for small local area networks. The Class C address assigns the three high order bits to binary 1 1 0. The next 21 bits are used to complete the network ID. The last 8 bits are used to represent the network ID. The address range for the first octet (8 bits) is 192 B223.
Classful IP addresses	Classful addresses are IP addresses that use the default subnet mask.
Classful routing protocols	Classful routing protocols do not include default subnet mask information in routing updates. The default subnet mask is used to identify the network and host portions of the address. Classful routing protocols are: • Interior Gateway Routing Protocol (IGRP) • Routing Information Protocol version 1(RIPv1)
Classless Inter-Domain Routing (CIDR)	A technique used to collapse Class C entries into a single entry corresponding to all the Class IDs that are being used by that organization. This allows companies to use many Class C addresses rather than requesting a Class B address, since the availability of IP addresses is scarce.
Classless IP addresses	Classless addresses are IP addresses that use a custom mask value to separate network and host portions of the IP address.
Classless routing protocols	Classless routing protocols use a custom mask value to separate network and host portions of the IP address. They are considered to be second-generation protocols because they improve on the limitations of classful protocols. The most common routing protocols are: • Enhanced Interior gateway Routing Protocol (EIGRP) • Intermediate System-to-Intermediate System (IS-IS) • Open Shortest Path First (OSPF) • Routing Information Protocol version 2 (RIPv2)
Client	A computer that uses files and resources from another computer on a network. Also called a workstation.
Client Access License (CAL)	A client access license permits a client to connect to a Windows 2000 server.
Client Access server (CAS)	Client Access server role is required in every Exchange 2007 organization because it supports the client applications Outlook Web Access and Exchange ActiveSync and also the Post Office Protocol

	version 3 (POP3), and Internet Message Access Protocol version 4rev1 (IMAP4) protocols.
Client Service for NetWare (CSNW)	A service included with Windows 2000 that allows a Windows workstation to use file and print resources residing on NetWare servers.
Client-based administration tools	Tools that allow you to perform several network administration tasks from a Windows 95/98 or Windows 2000 Professional workstation, such as creating users and groups, sharing folders, and assigning permissions to access resources.
ClipBook Viewer	A Windows shared resource that uses OLE to store up to 127 pieces of information, each called a ClipBook Viewer Page. Users can create and share these pages for use in OLE applications.
CLNS (Connectionless Network Service)	Connectionless Network Service (CLNS) is an address family that is used to identify routing sessions for protocols that use standard network service access point (NSAP) address prefixes, such as BGP.
Cluster Continuous Replication (CCR)	Cluster Continuous Replication (CCR) combines the asynchronous log shipping and replay technology of Exchange 2007 with the failover and management features provided by the Microsoft Windows Cluster service. CCR does not have a single point of failure and provides high availability by replicating data on a passive node, so the clustered Mailbox server can operate on either node at any time.
Clustering	A situation in which groups of independent computers work together as a single system.
CNAME (Canonical Name) record)	Enables you to associate more than one host name with an IP address. This concept is also referred to as aliasing.
Coaxial Cable	Coaxial cable is a type of network transmission media. It is an older technology that is usually implemented with a bus topology. It is not suitable for ring or star topologies because the ends of the cable must be terminated. It is composed of two conductors, which share a common axis, within a single cable.
Cold Site	A cold site is a fault tolerant strategy which provides a redundant work location. If a disaster renders a work site unusable, the effected organization may have a cold site in which to relocate. Cold sites have the following characteristics: • This is the least ready of alternative site types, but it is probably the most common. • The site is ready for equipment to be brought in during an emergency because there is no hardware on site. • The site might have electrical power and HVAC, but it may or may not have communication links. • A cold site is low cost, and may be better than nothing. • A cold site often offers a false sense of security. The actual amount of work involved in getting a cold site up and running

	might be more than expected and might take too long to adequately keep the business running.
Cold Spare	A cold spare is a component that sits on the shelf until there is a failure. Cold spares obviously need more time to implement recovery, but they don't have the maintenance requirements of hot spares.
COM (Component Object Model)	A method that allows objects to communicate with each other. It is the basis for both OLE and ActiveX.
Command line switches	Codes you can use at the command prompt when starting an application or installation program to customize the way the program runs.
Command prompt	The 32-bit Windows command-line interface similar to the MS-DOS prompt. You can use it to start programs and type Windows commands.
Common Gateway Interface (CGI)	A software program that allows Web servers to send data to an application and receive information back from the application, regardless of the operating system the application is running under.
Community	A community is a group that contains hosts that are running the SNMP service. These communities are identified by a community name and provide the first level of security and context checking for agents.
Community attribute	The community (type code 8) is an optional BGP transitive attribute that filters incoming or outgoing routes. BGP communities are routes that share some common properties and policies, which allows routers to act on the community as a whole rather than on individual routes.
Complete trust domain model	In this Windows NT network model, every domain on the network trusts every other domain. No single domain has control over the other domains. The complete trust model distributes administration of users, groups, domains, and resources among different departments rather than using a centralized approach.
Component Object Model (COM)	A method that allows objects to communicate with each other. It is the basis for both OLE and ActiveX.
Computer account	An account entry in the local SAM database or the Active Directory domain database that identifies a computer (workstation) as part of a domain.
Configuration container	The configuration container is used to store information about the configuration of the Active Directory environment in Exchange 2007, such as site configuration and areas of optimal connectivity. When AD is employed over a WAN, a site for each end of the WAN link is defined along with the site link that represents the WAN connection. Exchange 2007 uses this site information to route messages within the environment. The configuration container also contains additional Exchange configuration such as the definition of the connectors within the environment, the accepted domains, and which servers hold which roles.

Configuration partition	An Active Directory partition that stores the domain, site, and replication structure of a Windows 2000 network.
Connection object	An Active Directory object that represents a uni-directional connection between a source and target replication partner over which Active Directory data is replicated.
Connectionless communication	Connectionless communications assume an existing link between devices and allow transmission without extensive session establishment. Connectionless communications use no error checking, session establishment, or acknowledgements. Connectionless protocols allow quick, efficient communication at the risk of data errors and packet loss. Connectionless protocols are a good choice where speed is important and smaller chunks of data are being sent.
Connectionless Network Service (CLNS)	Connectionless Network Service (CLNS) is an address family that is used to identify routing sessions for protocols that use standard network service access point (NSAP) address prefixes, such as BGP.
Connection-oriented communication	Connection-oriented communication does not assume that there is an existing link between devices. Connection-oriented communications use error detection/correction, session establishment, or acknowledgements, and, if necessary, retransmission. Connection-oriented communication provides a more reliable communication when are delivery is more important than speed and is a good method to use when larger chunks of data are being sent.
Console	The Microsoft Management Console (MMC) is a graphical interface for the administration of Windows 2000 and some earlier Microsoft operating systems. It accommodates various "snap-in" tools.
Console tree	The left pane of the Microsoft Management Console (MMC). It shows a hierarchical structure of functions and/or objects.
Control Panel	A Windows utility that displays other utilities that are used to manage the local computer.
Convergence	A routing metric is a value used by routing protocols to determine the length of paths within a network. Different routing protocols use various measurements to calculate metrics, such as: • Bandwidth • Network delay • Hop count • Interface speed • Path cost • Load • MTU • Reliability • Communication cost
Cookie	Marker downloaded from Internet servers and stored on the hard drives of client computers. Cookies store information about your preferences,

	browser settings, location, and so on. They identify you (or your browser) to Web sites.
Cooperative multitasking	A system in which each application currently running a process voluntarily passes control of the CPU to another application between processes. It is also called non-preemptive multitasking.
Copy backup	A specific type of backup that backs up selected files and folders but does not mark their archive attributes.
CPU (Central Processing Unit)	The logic circuitry that responds to instructions and runs the computer. Also called a processor.
CRC (Cyclic Redundancy Checking)	Cyclic redundancy checking is a method used to verify correct transmission and reception of data that has been sent across a network.
Creator Owner	A built-in group that is used for network administration. It includes the user that created or took ownership of a resource.
CRL (Certificate Revocation List)	Digital certificates usually expire after one year, but CAs can revoke certificates earlier for various reasons. All revoked certificates are stored in the certification revocation list, which is open to all users. This allows users to check the list to verify whether a given certificate is valid.
Crossover cable	A cable connecting one hub with another hub or with a repeater in a network.
CSMA/CA (Carrier Sense Media Access/Collision Avoidance)	CSMA/CA is the technology used by Ethernet and wireless networks to control media access and avoid (rather than detect) collisions. CSMA/CD works as follows: • If a host detects traffic on the network, it experiences a longer back-off time than hosts on a wired network before attempting to transmit again. • Every transmission must be acknowledged. As every frame is acknowledged by the receiving host, other hosts receive a message indicating that they must wait to transmit.
CSMA/CD (Carrier Sense Multiple Access with Collision Detection)	CSMA/CD is the technology used by Ethernet. CSMA/CD works as follows: 1. The system listens for traffic, if the line is clear it begins transmitting. 2. During the transmission, the system listens for collisions. 3. If no collisions are detected, the communication succeeds. If collisions are detected, an interrupt jam signal is broadcast to stop all transmissions. Each system waits a random amount of time before starting over at step 1.
CSNW (Client Service for NetWare)	A service included with Windows 2000 that allows a Windows workstation to use file and print resources residing on NetWare servers.

CSR subsystem	The Windows subsystem that supports 32- and 16-bit Windows and MS-DOS applications within Windows 2000. Also called the Win32 subsystem, client/server subsystem, or CSRSS.
CSU/DSU (Channel Service Unit/Data Service Unit)	A hardware device that converts a digital data frame from a LAN format into a WAN format and vice versa.
Custom subnet mask	A subnet mask that is defined by a network administrator. Each host on a TCP/IP network requires a subnet mask. If a custom subnet mask is not used, then a default subnet mask is automatically used.
Cyclic Redundancy Checking (CRC)	Cyclic redundancy checking is a method used to verify correct transmission and reception of data that has been sent across a network.

D

Daily copy backup	A specific backup type that copies only files and folders that have changed during that day. It does not mark their archive attributes.
DARPA (Department of Defense Advanced Research Projects Agency)	The agency of the U.S. Department of Defense which created the industry-standard TCP/IP suite of protocols based on packet-switching network experiments conducted in the late 1960's and 1970's.
Data definition	The process of creating a database and associated objects, such as tables, indexes, constraints, defaults, rules, procedures, triggers, and views.
Data Encryption Standard (DES)	Data Encryption Standard is a common symmetric cryptography method. It was created in 1972 and re-certified in 1993. DES has a limitation of 56-bit keys and offers little encryption security since it can be easily broken.
Data Link Control (DLC)	A non-routable protocol. Windows NT computers use DLC to connect to IBM mainframes via 3270 terminal emulators and to connect to IBM AS/400 computers via 5250 emulators. Microsoft SNA Server for Windows NT uses DLC to communicate with mainframes on a token ring network. DLC is also used with some HP print devices that are attached to the network through a built-in adapter card.
Data Link Layer (OSI model)	Layer 2 of the OSI reference model. This layer provides reliable transit of data across a physical link. The data link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE has divided this layer into two sublayers: the MAC sublayer and the LLC sublayer. Sometimes simply called link layer. Roughly corresponds to the data link control layer of the SNA model. See also application layer, MAC address, network layer, physical layer, presentation layer, session layer, and transport layer.
Data redundancy	Creating and maintaining multiple copies of the same data.
Database	A collection of information, tables, and other objects organized and presented to serve a specific purpose, such as facilitating searching, sorting, and recombining data. Databases are stored in files.

Database replication	The process by which a WINS server can resolve NetBIOS names of hosts registered with another WINS server. For example, if a host on subnet A is registered with a local WINS server, but wants to communicate with a host on subnet B where the host is registered with a different WINS server, the NetBIOS name cannot be resolved unless the two WINS servers have replicated their databases with each other.
Datagram	Another term used to describe a packet. The term is also used to describe the Internet protocol known as the User Datagram Protocol, a connectionless protocol that does not guarantee delivery of datagrams.
DCOM (Distributed Component Object Model)	A method of configuring a client/server application so that several computers can use it at the same time. DCOM uses remote procedure calls (RPCs) to allow applications to interoperate and communicate with each other.
DDE (Dynamic Data Exchange)	A system by which applications can share data and commands. Both applications must support DDE.
DDS (Digital Data Service)	Digital lines to which a computer can connect using a channel service unit/digital service unit (CSU/DSU). These kinds of lines carry 99 percent error-free digital signals at speeds ranging from 2.4 to 56 kilobits per second. DDS lines are normally leased lines rather than on-demand. An exception is Switched 56, which is a system of on-demand (dial-up) 56 Kbps DDS lines.
DEC (Digital Equipment Corporation)	A computer manufacturing company that makes RISC-based processors such as Alpha.
Default	An action that a system performs, or a characteristic that it displays unless explicitly instructed otherwise.
Default gateway	The gateway you always want to use to communicate with a host on a different network. It receives packets from the local network and transfers them to another gateway on the other network. You specify a default gateway when you configure TCP/IP.
Default route	If a default route is configured, the router will send packets via that route in cases where a dynamic route is not provided. This can be used to create sufficient reachability, especially for route between an edge and the core. Default routes also reduce the burden on network resources caused by dynamic routing.
Default subnet mask	A subnet mask that is used on TCP/IP networks that are not divided into subnets. All TCP/IP hosts require a subnet mask even if the network is a single segment.
Demand paging	A Windows process that moves data between the computer's RAM and a paging file on the hard drive.
Demilitarized Zone (DMZ)	DMZ (Demilitarized Zone) is a buffer subnet. A DMZ should only contain servers that are to be accessed by external visitors. Often it is assumed that any server placed in the DMZ will be compromised. Thus, no mission critical or sensitive systems are located in a DMZ.

	A domain controller may appear in a DMZ when the DMZ is an entire isolated domain, however this is not common. User workstations are never located in a DMZ. Backup servers, unless specifically deployed for just the DMZ, are never located in a DMZ.
Department of Defense Advanced Research Projects Agency (DARPA)	The agency of the U.S. Department of Defense which created the industry-standard TCP/IP suite of protocols based on packet-switching network experiments conducted in the late 1960's and 1970's.
DES (Data Encryption Standard)	Data Encryption Standard is a common symmetric cryptography method. It was created in 1972 and re-certified in 1993. DES has a limitation of 56-bit keys and offers little encryption security since it can be easily broken.
Designated Router (DR)	A Designated Router (DR) is a router in a PIM-Sparse Mode tree that initiates the Join/Prune message cascade upstream in response to the IGMP membership information that is received from IGMP hosts.
Destination replication partner	A replication partner that receives updates from a source replication partner. Also called a target replication partner.
Device driver	A software component that allows a hardware device to communicate with the operating system of a computer.
DFS (Distributed File System)	A file management system that lets users and administrators create a virtual file structure such that a folder or hierarchy of folders appear to contain a collection of files that are, if fact, located on multiple computers or drives connected at various physical locations on the network. A Dfs directory tree helps users to browse through, search for, and access data on the network.
DHCP (Dynamic Host Configuration Protocol)	A protocol that dynamically assigns IP addresses to each computer on a network.
DHCP discover	A message that makes a request for an IP lease. The message contains the client's hardware address and computer name, so that DHCP servers know which client sent the request.
DHCP Manager	A Microsoft utility used to manage DHCP servers.
DHCP offer	All DHCP servers that have valid IP addressing information available send a DHCP offer to the client when the client makes a request.
DHCP request	The client will initialize TCP/IP and broadcasts a request for the location of a DHCP server and IP addressing information.
DHCP scope	The ability to set a start and end range for the assignment of IP addresses using DHCP. Addresses can also be excluded from the available addresses as well. The scope is set using the DHCP Console.
Dial-up Networking	A software program that allows a client computer to connect to an external or remote network via modem. It is the client version of RAS. Examples of dial-up networking include connecting from home to a computer at work over the phone lines or connecting with an internet service provider by modem.

Differential backup	A backup process that copies to tape only those files that have not been marked by previous backups. A differential backup does not mark the files after backing them up.
Diffuse Mode (Scatter Mode)	One mode that an infrared device operates in is diffuse mode (also called *scatter mode*), which operates by broadcasting a large beam of light rather than a narrow beam. It does not require line-of-sight connections.
Diffusing Update Algorithm Link-state (DUAL)	Diffusing Update Algorithm Link-state (DUAL) technology makes decisions concerning EIGRP routing computations and guarantees freedom from routing loops. DUAL tracks all routes advertised by neighbors, and uses metrics (also called *cost*) to select the best path and a second best path to reach a destination.
Dig	Dig is the Linux preferred tool for testing name resolution. Dig resolves (looks up) the IP address of a host name. Displays other name resolution-related information such as the DNS server used for the lookup request.
Digital certificates	Encoded computer information that provides verification of the identity of a client or server. These certificates include encoded information that identifies a particular person, company, or computer, and are often used to distribute public encryption keys to recipients.
Digital Data Service (DDS)	Digital lines to which a computer can connect using a channel service unit/digital service unit (CSU/DSU). These kinds of lines carry 99 percent error-free digital signals at speeds ranging from 2.4 to 56 kilobits per second. DDS lines are normally leased lines rather than on-demand. An exception is Switched 56, which is a system of on-demand (dial-up) 56 Kbps DDS lines.
Digital envelope	A method of hiding the content of a message from anyone but the recipient. The sender uses the recipient's public key to encrypt the contents of the message. The recipient uses her own private key to decrypt and read the message.
Digital Equipment Corporation (DEC)	A computer manufacturing company that makes RISC-based processors such as Alpha.
Digital Network Architecture (DNA)	In the mid-1970s, Digital Equipment Corporation developed a protocol suite known as Digital Network Architecture (DNA). It is also known as DECnet. The Physical and Data Link layers of DNA were the predecessors of the Ethernet IEEE 802.3 standard.
Digital signature	A method of verifying the sender of a message, but does not encrypt the message itself. The sender uses his own private key to encrypt a digital signature attached to a message. The recipient uses the sender's public key to decrypt the signature and verify the sender's identity.
Digital Subscriber Line (DSL)	DSL or Digital Subscriber Line is a form of high-speed dial-up connection used to connect remote systems to the Internet. DSL operates over existing copper phone lines and is an economical choice for homes and small businesses.

Digital Volt Meter (DVM)	An electrical device that you can use to diagnose cable problems. A DVM can determine if there is a break or short in the cable by testing the resistance (measured in ohms) of the network cable.
Direct Memory Access (DMA)	Direct Memory Access (DMA) channels are conduits used by high-speed devices to communicate directly with RAM, bypassing the CPU.
Directory replication	Directory replication is the process of sharing directory information between servers inside and between sites.
Directory Service Agent (DSA)	A process that runs on a domain controller and provides access to the Active Directory database.
Directory Services Restore Mode	A special safe mode you use to restore the system state data on a domain controller.
Direct-Sequence Spread Spectrum (DSSS)	A type of signalling method, used by a wireless networking architecture, where the transmitter breaks data into pieces and sends the pieces across multiple frequencies in a defined range. DSSS is more susceptible to interference and less secure then other forms of signalling, such as Frequency Hopping Spread Spectrum (FHSS).
DirectX APIs	A low-level API that provides fast response to user input. Microsoft designed DirectX specifically to run graphically-intensive computer games. DirectX components are Microsoft DirectDraw, Microsoft DirectPlay, and Microsoft DirectSound.
Disk partition	Also called a partition. A portion of the free space on a hard disk that you format with a file system. Partitions can be either primary or extended.
Distance Vector Multicast Routing Protocol (DVMRP)	Distance Vector Multicast Routing Protocol (DVMRP) is a protocol that shares information between routers to transport IP Multicast packets among networks.
Distance vector routing protocol	Class of routing algorithms that iterate on the number of hops in a route to find a shortest-path spanning tree. Distance vector routing algorithms call for each router to send its entire routing table in each update, but only to its neighbors. Distance vector routing algorithms can be prone to routing loops, but are computationally simpler than link state routing algorithms. Also called Bellman-Ford routing algorithm. See also link state routing algorithm.
Distribute list	A distribute list is a type of access list that is applied to routing updates. Unlike normal access lists, distribute lists can control routing updates no matter their origin.
Distributed applications	Applications that split processing tasks between a client (front-end) and a server (back-end).
Distributed Component Object Model (DCOM)	A method of configuring a client/server application so that several computers can use it at the same time. DCOM uses remote procedure calls (RPCs) to allow applications to interoperate and communicate with each other.

Distributed File System (DFS)	A file management system that lets users and administrators create a virtual file structure such that a folder or hierarchy of folders appear to contain a collection of files that are, if fact, located on multiple computers or drives connected at various physical locations on the network. A Dfs directory tree helps users to browse through, search for, and access data on the network.
Distributed Management Interface (DMI)	The Distributed Management Interface (DMI) is a standard for organizing information about desktop, notebook, and server computers. DMI is part of the System Management BIOS (SMBIOS) specification which allows data about a system to be stored in the individual system's BIOS. Management software interfaces with the BIOS on a monitored system to gather this information and assemble it into an administrator-specified format such as a report or a database.
Distributed Parity	Distributed parity is a method of data protection used in a RAID 5 configuration. Duplicate data (parity) is placed on multiple disks (distributed) to protect against data loss in the event of a storage disk failure.
Distributed processing	A technique of using both the client and server's processors to complete a task. The client or "front end" accepts input and runs simple calculations, while the server or "back end" handles processes that require more processing power.
Distribution group	A distribution group is a universal group that has been mail-enabled, such as a security group. A distribution group can be used to send an e-mail to a large number of people in an Exchange organization, such as entire departments or groups.
Distribution list	A distribution list contains addresses for individual users, public folders, and other distribution lists. They allow each member to receive a copy of a message sent to the entire list. Applications use distribution lists.
Distribution tree	A distribution tree shows the source of multicast information and the path that multicast traffic use across the network infrastructure.
DLC (Data Link Control)	A non-routable protocol. Windows NT computers use DLC to connect to IBM mainframes via 3270 terminal emulators and to connect to IBM AS/400 computers via 5250 emulators. Microsoft SNA Server for Windows NT uses DLC to communicate with mainframes on a token ring network. DLC is also used with some HP print devices that are attached to the network through a built-in adapter card.
DMA (Direct Memory Access)	Direct Memory Access (DMA) channels are conduits used by high-speed devices to communicate directly with RAM, bypassing the CPU.
DMI (Distributed Management Interface)	The Distributed Management Interface (DMI) is a standard for organizing information about desktop, notebook, and server computers. DMI is part of the System Management BIOS (SMBIOS) specification which allows data about a system to be stored in the individual system's BIOS. Management software interfaces with the BIOS on a monitored system to gather this information and assemble it into an administrator-specified format such as a report or a database.

DMZ (Demilitarized Zone)	DMZ (Demilitarized Zone) is a buffer subnet. A DMZ should only contain servers that are to be accessed by external visitors. Often it is assumed that any server placed in the DMZ will be compromised. Thus, no mission critical or sensitive systems are located in a DMZ. A domain controller may appear in a DMZ when the DMZ is an entire isolated domain, however this is not common. User workstations are never located in a DMZ. Backup servers, unless specifically deployed for just the DMZ, are never located in a DMZ.
DNA (Digital Network Architecture)	In the mid-1970s, Digital Equipment Corporation developed a protocol suite known as Digital Network Architecture (DNA). It is also known as DECnet. The Physical and Data Link layers of DNA were the predecessors of the Ethernet IEEE 802.3 standard.
DNS (Domain Name Server)	A server that maintains a database of IP address/computer name mappings. A DNS server can run on Windows NT, Unix, or NetWare (5). The DNS has the responsibility to resolve fully qualified domain names and other host names to IP addresses. In DNS, the clients are called resolvers and the servers are called name servers.
DNS (Domain Name System)	A hierarchical client/server-based database management system that translates computer names into IP addresses. DNS maps to the application layer and uses UDP and TCP as the underlying protocols. Clients, known as resolvers, contact name servers for the IP address they are seeking.
DNS Domain	A domain that defines different levels of authority in a hierarchical structure. The highest level is called the root domain. The other levels of domains are currently defined as com, edu, org, net, gov, mil, num, and arpa. Second level domains are any domains defined by companies such as Microsoft.com or Novell.com.
DNS Service Discovery (DNS-SD)	A service location feature used in Zeroconf networking implementation. DNS-SD allows IP hosts to automatically find available services, such as file servers, printers, and routers. DNS-SD is a Mac OS related feature.
DNS-SD (DNS Service Discovery)	A service location feature used in Zeroconf networking implementation. DNS-SD allows IP hosts to automatically find available services, such as file servers, printers, and routers. DNS-SD is a Mac OS related feature.
Domain	A logical grouping of computers and users. In a domain, all users have access to a central directory database that stores security and user account information for the domain.
Domain Admins	A built-in global group that is added automatically to the Administrators local group, making all members of Domain Admins group domain administrators.
Domain controller	Windows 2000 domain controllers contain copies of the Active Directory database. They provide a centralized approach to administration and account maintenance.
Domain Dfs	A configuration of Dfs in which Active Directory stores the information about the virtual file structure. Advantages include fault-tolerance.

Domain Guests	A built-in global group in which the Guest user account is a member.
Domain Name	A domain name locates entities (for example, websites) on the Internet. Domain names are managed within a domain name system (DNS), which is a hierarchy that is made up of the following components: • . (dot) domain (also called the *root* domain) • Top Level Domains (TLDs) such as .com, .edu, .gov • Additional domains such as yahoo.com, microsoft.com, etc.
Domain Name Server (DNS)	A server that maintains a database of IP address/computer name mappings. A DNS server can run on Windows NT, Unix, or NetWare (5). The DNS has the responsibility to resolve fully qualified domain names and other host names to IP addresses. In DNS, the clients are called resolvers and the servers are called name servers.
Domain Name System (DNS)	A hierarchical client/server-based database management system that translates computer names into IP addresses. DNS maps to the application layer and uses UDP and TCP as the underlying protocols. Clients, known as resolvers, contact name servers for the IP address they are seeking.
Domain partition	An Active Directory partition that stores objects, attribute, and attribute values for a particular domain. Each domain in Active Directory has its own domain partition.
Domain user accounts	User name and password information stored in the Active Directory database on the domain controllers.
Domain Users	Any user account created in a Windows domain is a domain user. Domain Users is a global group.
DOS	See MS-DOS.
DR (Designated Router)	A Designated Router (DR) is a router in a PIM-Sparse Mode tree that initiates the Join/Prune message cascade upstream in response to the IGMP membership information that is received from IGMP hosts.
Drive mapping	A specific letter used to map a drive or volume on a workstation or server.
DROTHER	Any other router that is not a DR or a BDR is called a DROTHER. This is simply a term used to describe a non-DR or non-BDR router. It is not technically an OSPF router role.
DSA (Directory Service Agent)	A process that runs on a domain controller and provides access to the Active Directory database.
DSL (Digital Subscriber Line)	DSL or Digital Subscriber Line is a form of high-speed dial-up connection used to connect remote systems to the Internet. DSL operates over existing copper phone lines and is an economical choice for homes and small businesses.

DSSS (Direct-Sequence Spread Spectrum)	A type of signalling method, used by a wireless networking architecture, where the transmitter breaks data into pieces and sends the pieces across multiple frequencies in a defined range. DSSS is more susceptible to interference and less secure then other forms of signalling, such as Frequency Hopping Spread Spectrum (FHSS).
DUAL (Diffusing Update Algorithm Link-state)	Diffusing Update Algorithm Link-state (DUAL) technology makes decisions concerning EIGRP routing computations and guarantees freedom from routing loops. DUAL tracks all routes advertised by neighbors, and uses metrics (also called *cost*) to select the best path and a second best path to reach a destination.
Dual Ring	A dual ring is an enhanced version of the ring networking topology. A dual ring network includes two rings; the primary and secondary rings, which increase performance and fault tolerance. A break in one ring in a dual ring configuration has no effect on communications. A decrease in bandwidth might result, but data can be sent on the other ring.
Dual Stack	A method used to allow concurrent support for both IPv4 and IPv6 within the same network.
Dual-boot	The ability to boot a computer with either one of two operating systems. Both operating systems must be loaded on the computer. At bootup a menu prompts the user to load the operating system the computer should use.
Duplex (Simplex)	Simplex and duplex are methods of communication transmission. Simplex is the one-way transmission of a signal across a medium. Duplex is the two-way transmission of a signals across a medium. There are two types of duplex transmission; half-duplex and full-duplex. Half-duplex allows transmission of signals, one party at a time. Full-duplex allows transmission and reception of signals to occur concurrently.
DVM (Digital Volt Meter)	An electrical device that you can use to diagnose cable problems. A DVM can determine if there is a break or short in the cable by testing the resistance (measured in ohms) of the network cable.
DVMRP (Distance Vector Multicast Routing Protocol)	Distance Vector Multicast Routing Protocol (DVMRP) is a protocol that shares information between routers to transport IP Multicast packets among networks.
Dynamic Data Exchange (DDE)	A system by which applications can share data and commands. Both applications must support DDE.
Dynamic disk	A disk device managed by Windows 2000 Disk Management. Dynamic disks do not contain partitions or logical drives. They can contain only dynamic volumes created with Disk Management. They cannot be accessed by earlier version of Windows or by MS-DOS.
Dynamic distribution group	A dynamic distribution group is an Exchange distribution group whose membership is defined by the results of a query which is executed every time a message is sent to the group. This is optimal for environments in

	which people move groups or buildings often and e-mail groups need to be able to accommodate changes as they occur.
Dynamic Host Configuration Protocol (DHCP)	A protocol that dynamically assigns IP addresses to each computer on a network.
Dynamic routing	Dynamic routing is an addressing method that senses changes in the network topology and responds accordingly without administrator involvement. Dynamic routers: • Propagate changes and shifts in the network topology to each router in the network, causing the routing tables on each router to always be up to date. • Are responsible for all networks to which they are connected. • Employ additional processes or services to exchange routing information between routers.

E

.EDB file	Exchange 2007's database engine is referred to as the Extensible Storage Engine (ESE). ESE is a transactional database that writes information into RAM memory and into a log file. Once it is in the log file, it will be written to disk. There are a number of files used to store information: • An .edb file is located in the actual database itself. All of a user's messages, folders, public folders, contacts, appointment information, etc. is all stored on the .edb file. An .edb file size can exceed multiple GB. • A .log file is an ESE transaction log file. All .log files are 1 MB. • A .jrs file is a reserve log file which is used to commit any transactions that are still in memory in the event of the server running out of disk space. All .jrs files are 1 MB. • A .chk file is used to identify which log files have been committed to the database. The size of .chk file varies from 2-3 KB. The ESE takes the following steps to write information into database files: 1. The ESE writes a message into memory RAM when it arrives at the server. 2. At the same time that information is written to RAM, it's written into the current .log file. All current log files are named E00.log. The information is written in a sequential format until the log file is full. When the log file is full, it will be renamed. 3. Once it has been committed to the log file, the information is written to the .edb file. 4. The checkpoint file is updated to indicate that the transaction log that has been committed to the database.

EAP (Extensible Authentication Protocol)	EAP is an authentication protocol (an extension of PPP). It is a set of interface standards that provide various authentication methods (smartcards, biometrics, and digital certificates), define access definitions, providing protection mechanisms and custom solutions, and does not maintain a database of user accounts and passwords.
EAPoL (Extensible Authentication Protocol over LAN)	The Extensible Authentication Protocol over LAN is used for authentication of 802.1X port access control over either wired or wireless LANs.
Eavesdropping	Eavesdropping is the act of capturing and examining traffic on a network cable. Eavesdropping is the primary security vulnerability of networking systems using 802.11 technology. On wireless networks, eavesdropping is made more difficult by using WEP keys. Fiber optic cable is the most resistant to tapping and eavesdropping. Fiber optic cable transmits light pulses rather than electricity to communicate. Thus, it is not susceptible to most forms of interference or wire tapping technologies. ThickNet (10Base5 coax), 10Base2 (ThinNet coax), and 10BaseT (STP and UTP) are very susceptible to tapping and eavesdropping.
EBGP (External BGP)	External BGP (EBGP) is used by BGP to route information between autonomous systems.
Edge Rules agent	Transport policy agents apply transport policies to e-mails within an Exchange organization. There are two types of transport policy agents in Exchange 2007: • A Transport Rules agent runs on a Hub Transport server and implements policies set by administrators to all e-mail that travels in and out of an Exchange organization. • An Edge Rules agent runs on an Edge Transport server and helps control spam and unwanted mail flow within an organization.
Edge Transport server	The Edge Transport server handles all Internet-facing mail flow and provides Simple Mail Transfer Protocol (SMTP) relay and smart host services for the Exchange 2007 organization.
EDirectory	NetWare 4.*x* and higher uses a directory service called *eDirectory* (formerly called Novell Directory Services (NDS)). User accounts are configured in the directory. eDirectory can also run on other servers such as Windows and Linux.
Effective permission	The combined rights a user has to perform specific network functions and access network resources.
EGP (Exterior Gateway Protocol)	Exterior Gateway Protocol (EGP) is a routing protocol that exchanges routing information between autonomous systems. BGP is the most common EGP protocol.

EIDE (Enhanced Integrated Drive Electronics)	A standard electronic interface that allows a computer to communicate with a storage device such as the hard drive or a CD-ROM drive.
EISA (Extended Industry Standard Architecture)	A 32-bit I/O bus slot providing compatibility with 386 through Pentium machines. EISA buses: • Have a maximum throughput rate of 33 MB/s. • Offer *bus mastering* which is a mini-processor on the expansion card. The mini-processor assumes the task from the CPU of transferring data to and from memory. • Offer a second row of pins to a standard ISA bus. • Provide backward compatibility with ISA cards. • Allow EISA cards to take advantage of both rows of pins (the 32-bit data path) to improve transfer rates and increase addressable memory. • Allow for automatic configuration of system resources (addresses, DMA channels and IRQs). • Support sharing of system resources. • Allow multiple EISA cards to share the same interrupt. • EISA supports multiprocessing by allowing more than one CPU to share the bus. • Are usually black, though they are sometimes white.
Electromagnetic Interference (EMI)	The disruption of one electronic device, caused by an electromagnetic field (in the radio frequency spectrum) generated by another electronic device.
E-mail Address policies	E-mail Address policies are used to generate e-mail addresses for Exchange recipients within an Exchange 2007 organization. Policies can be used to generate e-mail addresses for a number of environments, such as SMTP, X400, Lotus Notes, or Novell GroupWise.
E-mail client	An e-mail client is a software application that supports specific protocols and provides the user with an interface to a server.
Emergency Repair Disk (ERD)	A backup disk that can provide the necessary files to bring back the Windows operating system in the case of a disk disaster running the Windows operating system. You create an ERD using Windows 2000.
EMI (Electromagnetic Interference)	The disruption of one electronic device, caused by an electromagnetic field (in the radio frequency spectrum) generated by another electronic device.
Encapsulating Security Payload (ESP)	Encapsulating Security Payload (ESP) is one of two services comprising IPSec. ESP supports both authentication of the sender and is used primarily to encrypt and secure the data transferred between IPSec partners.
Encapsulation	The process of adding an additional header to a packet before transporting the packet onto the network. For example, NetBIOS can be encapsulated with an IP header.

Encryption	A security technique that uses a cryptographic algorithm to encode information so that only someone with the proper key can unencode it.
Enhanced Integrated Drive Electronics (EIDE)	A standard electronic interface that allows a computer to communicate with a storage device such as the hard drive or a CD-ROM drive.
Enhanced Small Device Interface (ESDI)	A type of hard disk that uses CHS addressing and has a 1024 cylinder limitation. ESDI hard disks are predecessors of the newer IDE disks.
ERD (Emergency Repair Disk)	A backup disk that can provide the necessary files to bring back the Windows operating system in the case of a disk disaster running the Windows operating system. You create an ERD using Windows 2000.
ErrorControl levels	The values Windows uses to determine what to do in case of an error in loading or initializing drivers. The levels are 0x0 (ignore the error), 0x1 (display an error message then ignore the error), 0x2 (use the LastKnownGood control set and restart), 0x3 (stop the boot sequence and display an error message).
ESDI (Enhanced Small Device Interface)	A type of hard disk that uses CHS addressing and has a 1024 cylinder limitation. ESDI hard disks are predecessors of the newer IDE disks.
ESE (Extensible Storage Engine)	Exchange 2007's database engine is referred to as the Extensible Storage Engine (ESE). ESE is a transactional database that writes information into RAM memory and into a log file. Once it is in the log file, it will be written to disk. There are a number of files used to store information: • An .edb file is located in the actual database itself. All of a user's messages, folders, public folders, contacts, appointment information, etc. is all stored on the .edb file. An .edb file size can exceed multiple GB. • A .log file is an ESE transaction log file. All .log files are 1 MB. • A .jrs file is a reserve log file which is used to commit any transactions that are still in memory in the event of the server running out of disk space. All .jrs files are 1 MB. • A .chk file is used to identify which log files have been committed to the database. The size of .chk file varies from 2-3 KB. The ESE takes the following steps to write information into database files: 1. The ESE writes a message into memory RAM when it arrives at the server. 2. At the same time that information is written to RAM, it's written into the current .log file. All current log files are named E00.log. The information is written in a sequential format until the log file is full. When the log file is full, it will be renamed. 3. Once it has been committed to the log file, the information is written to the .edb file. 4. The checkpoint file is updated to indicate that the transaction log that has been committed to the database.

ESP (Encapsulating Security Payload)	Encapsulating Security Payload (ESP) is one of two services comprising IPSec. ESP supports both authentication of the sender and is used primarily to encrypt and secure the data transferred between IPSec partners.
Ethernet	One of the major families of network architectures. The structure of all Ethernet networks is based on the bus topology. Most Ethernet networks use baseband signaling and CSMA/CD as a media access method.
Event ID	The identification for the event that displays in the Event Detail window in the Event Viewer.
Event log	Any of three log files in which Windows records monitored events such as errors, warnings, and the success or failure of tasks. Event logs include the system, security, and application logs. You can view these logs in the Event Viewer.
Event Viewer	An administration tool that provides information about such events as errors, warnings, and the success or failure of tasks.
Everyone	A special group or identity that includes all users and can be used to assign permissions that all users in a domain hold in common, including guests and users from other domains.
Exchange 2007 Management Console	The Exchange 2007 Management Console is a graphic interface used to manage an Exchange environment. It has been simplified from previous versions of Exchange so it now focuses only on the most commonly executed tasks. Additional tasks that could traditionally only be performed in REGEDIT or ADSIEDIT were also added to the Exchange Management Console to improve ease of use. In Exchange 2003, the information shown in the tree-pane was dependent on the configuration of your Exchange Server. This pane is now static in Exchange 2007 Management Console so no matter how many servers you have, what options have been chosen, or what has been installed, the tree-pane will always be the same.
Exchange ActiveSync	Exchange ActiveSync is a protocol used by Internet-enabled mobile devices to send and retrieve Exchange data.
Exchange Management Console	The Exchange Management Console is the graphical administration tool. It is comprised of a three-paned view that includes a tree view, results, and an actions pane. It cannot perform many of the administrative tasks that can be performed in the Exchange Management Shell.
Exchange Management PowerShell	The Exchange 2007 Management Shell environment allows administrators to perform all of their tasks from a command line environment, thus making it easier to automate tasks. The PowerShell must be installed before Exchange 2007 is fully installed, then extensions are installed to the PowerShell during Exchange 2007 installation to create the Exchange 2007 PowerShell environment. The PowerShell uses with verb/noun-based syntax and is the primary platform for all administration; the graphical interface is simply running atop of the command shell.

Exchange Management Shell	The Exchange 2007 Management Shell environment allows administrators to perform all of their tasks from a command line environment, thus making it easier to automate tasks. The PowerShell must be installed before Exchange 2007 is fully installed, then extensions are installed to the PowerShell during Exchange 2007 installation to create the Exchange 2007 PowerShell environment. The PowerShell uses with verb/noun-based syntax and is the primary platform for all administration; the graphical interface is simply running atop of the command shell.
Exchange PowerShell	Microsoft Exchange Management Shell (Windows PowerShell) is a command line environment designed for automating administration and maintenance. The Exchange Management Shell is the primary management interface of 2007.
Exchange storage group	A Microsoft Exchange storage group is a collection of Exchange stores (databases). A Recovery Storage Group (RSG) is a special storage group used for recovering Mailbox stores.
Executive Services	The central component of Windows network architecture. It includes the managers and device drivers that run in kernel mode.
Extended Industry Standard Architecture (EISA)	A 32-bit I/O bus slot providing compatibility with 386 through Pentium machines. EISA buses: • Have a maximum throughput rate of 33 MB/s. • Offer *bus mastering* which is a mini-processor on the expansion card. The mini-processor assumes the task from the CPU of transferring data to and from memory. • Offer a second row of pins to a standard ISA bus. • Provide backward compatibility with ISA cards. • Allow EISA cards to take advantage of both rows of pins (the 32-bit data path) to improve transfer rates and increase addressable memory. • Allow for automatic configuration of system resources (addresses, DMA channels and IRQs). • Support sharing of system resources. • Allow multiple EISA cards to share the same interrupt. • EISA supports multiprocessing by allowing more than one CPU to share the bus. • Are usually black, though they are sometimes white.
Extended partition	A partition you create from free space on a hard disk and can be subdivided into logical drives. You can have only one extended partition on a single hard disk.
Extensible Authentication Protocol (EAP)	EAP is an authentication protocol (an extension of PPP). It is a set of interface standards that provide various authentication methods (smartcards, biometrics, and digital certificates), define access definitions, providing protection mechanisms and custom solutions, and does not maintain a database of user accounts and passwords.

Extensible Authentication Protocol over LAN (EAPoL)	The Extensible Authentication Protocol over LAN is used for authentication of 802.1X port access control over either wired or wireless LANs.
Extensible Storage Engine (ESE)	Exchange 2007's database engine is referred to as the Extensible Storage Engine (ESE). ESE is a transactional database that writes information into RAM memory and into a log file. Once it is in the log file, it will be written to disk. There are a number of files used to store information: • An .edb file is located in the actual database itself. All of a user's messages, folders, public folders, contacts, appointment information, etc. is all stored on the .edb file. An .edb file size can exceed multiple GB. • A .log file is an ESE transaction log file. All .log files are 1 MB. • A .jrs file is a reserve log file which is used to commit any transactions that are still in memory in the event of the server running out of disk space. All .jrs files are 1 MB. • A .chk file is used to identify which log files have been committed to the database. The size of .chk file varies from 2-3 KB. The ESE takes the following steps to write information into database files: 1. The ESE writes a message into memory RAM when it arrives at the server. 2. At the same time that information is written to RAM, it's written into the current .log file. All current log files are named E00.log. The information is written in a sequential format until the log file is full. When the log file is full, it will be renamed. 3. Once it has been committed to the log file, the information is written to the .edb file. 4. The checkpoint file is updated to indicate that the transaction log that has been committed to the database.
Exterior Gateway Protocol (EGP)	Exterior Gateway Protocol (EGP) is a routing protocol that exchanges routing information between autonomous systems. BGP is the most common EGP protocol.
External BGP (EBGP)	External BGP (EBGP) is used by BGP to route information between autonomous systems.
External relay	Accepted domains identify the domains for which the organization is solely responsible and the SMTP domains from which the server will accept messages. There are three types of accepted domains in Exchange 2007: • Authoritative is the domain over which the Exchange server has sole responsibility. In a typical environment, the organization will have an e-mail domain of "company.com" which is hosted by the company's e-mail server. If another e-mail system or

	domain exists in the environment, internal and external relays are employed. • An internal relay is an e-mail domain that is hosted by another Active Directory Forest within the Exchange organization. This system uses different e-mail addresses, but all incoming mail goes through the Exchange organization. • An external relay accepts e-mail for an external organization and then delivers it to an external entity such as the Internet via the Edge Transport server.
Extranet	An extranet is a division of a private network that is accessible to a limited number of external users, such as business partners, suppliers, and certain customers.

F

Failback	Failback is the process of moving services back to the original server when it comes back online.
Failover	Failover is the process of moving services from a failed server to another available server.
FAT (File Allocation Table)	A file system that is required for Windows 95 and MS-DOS based computers.
FAT32	A 32-bit file allocation table which was first shipped with Windows 95. FAT32 supports large volumes and is more efficient than the 16-bit FAT system.
FC (Fibre Channel)	Fibre Channel (FC) is an integrated set of standards developed to provide a reliable method for quickly transferring large amounts of data. FC is the recommended method of implementing a shared disk array because of its high bandwidth and high capacity. FC communication can also be used to link workstations, mainframes, and other peripherals.
FCIP	Fibre Channel over IP (FCIP) is an IP-based storage networking technology developed by the Internet Engineering Task Force (IETF). FCIP enables the transmission of data to and from FC storage devices over standard Ethernet copper cabling and switches.
FD (Feasible Distance)	The Feasible Distance (FD) is the lowest total cost to a destination network.
FDDI (Fiber Distributed Data Interface)	A standard produced by the American National Standards Committee for transmitting data on fiber optic lines. FDDI is based on token ring topology and can support a large network over large geographic areas.
FDISK	An MS-DOS utility you can use to create a primary partition or logical drive on a hard disk.
Feasible Distance (FD)	The Feasible Distance (FD) is the lowest total cost to a destination network.

FHSS (Frequency Hopping Spread Spectrum)	A type of signalling method, used by a wireless networking architecture, where a narrow frequency band 'hops' data signals in a predictable sequence from frequency to frequency over a wide band of frequencies. Because FHSS hops between frequencies, it can avoid interference on one cable as it shifts to another. Hopping between frequencies increases transmission security by making eavesdropping and data capture more difficult. Because FHSS shifts automatically between frequencies, it can avoid interference that may be on a single frequency.
Fiber Distributed Data Interface (FDDI)	A standard produced by the American National Standards Committee for transmitting data on fiber optic lines. FDDI is based on token ring topology and can support a large network over large geographic areas.
Fiber optic cable	Fiber optic cable uses glass strands to transmit light pulses rather than electricity to communicate. Thus, it is not susceptible to most forms of interference or wire taping technologies. The biggest disadvantage to fiber optic cable is the high cost of the cable, its components and installation.
Fibre Channel (FC)	Fibre Channel (FC) is an integrated set of standards developed to provide a reliable method for quickly transferring large amounts of data. FC is the recommended method of implementing a shared disk array because of its high bandwidth and high capacity. FC communication can also be used to link workstations, mainframes, and other peripherals.
Fibre Channel over IP (FCIP)	Fibre Channel over IP (FCIP) is an IP-based storage networking technology developed by the Internet Engineering Task Force (IETF). FCIP enables the transmission of data to and from FC storage devices over standard Ethernet copper cabling and switches.
File Allocation Table (FAT)	A file system that is required for Windows 95 and MS-DOS based computers.
File and Print Services for NetWare (FPNW)	A software component that allows NetWare clients to access file and print services on a Windows 2000 server.
File transfer protocol (FTP)	This protocol provides bi-directional file transfers between two TCP/IP hosts. These hosts must be running FTP software.
File-level security	Security that is applied to individual files and folders on a local computer.
Final partition	The final partition is the domain naming context partition in Exchange 2007. This is used to hold all of the user accounts, groups, and computer accounts. If mail-enabled context is used, then it is stored in the final partition. The domain naming context stores the largest amount of information in a typical employment.
Finger service	A TCP/IP service that allows you to gather system information from a remote computer.
Firewall	A firewall is the best device to deploy to protect your private network from a public untrusted network. Firewalls are used to control traffic entering and leaving your trusted network environment. Firewalls can manage traffic based on source or destination IP address, port number,

	service protocol, application or service type, user account, and even traffic content.
Firewire	Firewire is a type of media (cable and connectors) that interface between computers to create a network.
Firmware	Computer instructions contained in programmable read-only memory (PROM). Firmware comes as part of a hardware device such as a printer or modem.
Flash updates	With the triggered update method (also known as a flash updates), routers that receive updated (changed) information broadcast those changes immediately rather than waiting for the next reporting interval. With this method, routers broadcast their routing tables periodically, punctuated by special broadcasts if conditions have changed. This method reduces the convergence time.
Floating static route	A floating static route is a static route whose administrative distance has been manually configured to be greater than the administrative distance of dynamic routes; thus making it less desirable than the dynamic route it supports.
Foreign connector	A Foreign connector is a logical object that controls the sending of messages to non-SMTP mail systems or to fax systems.
Forest	In Windows 2000, a forest is collection of one or more domains linked with two-way transitive trusts and sharing a common schema, configuration, and global catalog.
Format	To set up partitions and volumes on a hard disk that will use file system such as FAT or NTFS.
Forward lookup	The query process in which DNS domain names are resolved to IP addresses. In contrast, reverse lookup is the query process in which IP addresses are resolved to domain names.
Forwarder	Forwarders are designated DNS servers that accept and resolve recursively all queries regarding external or off-site addresses. Other servers are configured to send all such queries to the forwarder.
FPNW (File and Print Services for NetWare)	A software component that allows NetWare clients to access file and print services on a Windows 2000 server.
FQDN (Fully Qualified Domain Names)	Host names inside domains that are added to the beginning of the domain name. For example, any name given that is placed in front of Microsoft.com, such as support.Microsoft.com, is a fully qualified domain name.
Frame type	A setting that controls how a network adapter card formats the data you want to send over the network. Ethernet network can operate using various frame types. Ethernet frames are between 64 and 1518 bytes in length. For two computers to communicate, they must use the same frame type. These are the four Ethernet frame types: Ethernet 802.3, Ethernet 802.2, Ethernet II, and Ethernet SNAP.

Frequency Hopping Spread Spectrum (FHSS)	A type of signalling method, used by a wireless networking architecture, where a narrow frequency band 'hops' data signals in a predictable sequence from frequency to frequency over a wide band of frequencies. Because FHSS hops between frequencies, it can avoid interference on one cable as it shifts to another. Hopping between frequencies increases transmission security by making eavesdropping and data capture more difficult. Because FHSS shifts automatically between frequencies, it can avoid interference that may be on a single frequency.
Front end	The client in the client/server computing model. It provides an interface for the user to enter requests, formats user requests so that the server understands them, and displays data from the server.
FTP (File transfer protocol)	This protocol provides bi-directional file transfers between two TCP/IP hosts. These hosts must be running FTP software.
Full Mesh	A mesh topology exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. A full Mesh topology connects every node in a point-to-point connection with every other node. Full mesh topologies are usually impractical because the number of connections increases dramatically with every new node added to the network. However, a full mesh topology becomes more practical through the implementation of an ad-hoc wireless network.
Full-mesh iBGP	Full-mesh iBGP is an iBGP network in which each BGP speaker has a neighbor statement containing updated information for all other iBGP speakers in the AS.
Fully Qualified Domain Names (FQDN)	Host names inside domains that are added to the beginning of the domain name. For example, any name given that is placed in front of Microsoft.com, such as support.Microsoft.com, is a fully qualified domain name.

G

Gateway	A gateway is a generic term used to describe any device that connects one administratively managed network with another. For example, a gateway connects a business network to the Internet. The gateway device controls the flow of data between the two networks. In addition, the term *gateway* is often used to describe a specialized device that translates data sent between two networks using different protocols.
Gateway Services for NetWare (GSNW)	A Windows 2000 service that allows a Windows 2000 server to use file and print resources on a NetWare server.
Global catalog server	A Windows 2000 domain controller that stores at least partial replicas of each partition in the forest. The partial replicas are read-only and make it possible to search the Active Directory database on a forest-wide basis.
Gopher	A protocol that makes it easier to browse resources on the Internet by displaying Internet resources in a menu structure.
GPC (Group Policy Container)	The portion of a Group Policy Object (GPO) that is stored in Active Directory.

GPO (Group Policy Object)	An Active Directory object that contains user-specific and/or computer-specific settings that Windows 2000 must enforce.
Gpotool.exe	A command-line Windows 2000 Server Resource Kit tool that lets you check replication status of Group Policy Objects (GPOs) on a computer.
Gpresult.exe	A command-line Windows 2000 Server Resource Kit tool that lists the group policy settings applied to a particular user or computer.
GPT (Group Policy Template)	The portion of a Group Policy Object (GPO) that is stored on the domain controller's file system.
Group account	A group of users that have common privileges only in the domain which they were created. Local groups can contain both users and global groups. Global groups are lists of user accounts from within a single domain. A global group can include user accounts from only the domain in which the global group was created.
Group Policy	The primary Windows 2000 desktop administration feature. Use Group Policy to create Group Policy objects to control and manage users' computing environments. This includes desktop features such as Start menu options, shortcuts, and available applications, as well as security settings, home folder assignments, auditing, and more.
Group Policy Container (GPC)	The portion of a Group Policy Object (GPO) that is stored in Active Directory.
Group Policy Creator Owners Group	A domain global group that lets members create Group Policy Objects (GPOs) within the domain.
Group Policy Object (GPO)	An Active Directory object that contains user-specific and/or computer-specific settings that Windows 2000 must enforce.
Group Policy Snap-In	A Microsoft Management Console (MMC) snap-in that lets you view and edit settings for a Group Policy Object (GPO). Also called the Group Policy Editor.
Group Policy Template (GPT)	The portion of a Group Policy Object (GPO) that is stored on the domain controller's file system.
GSNW (Gateway Services for NetWare)	A Windows 2000 service that allows a Windows 2000 server to use file and print resources on a NetWare server.
Guest	A built-in account that is used to give occasional users the ability to log on and access limited resources.
Guests	Members of the local Guest group on workstations and servers have limited rights. They can maintain a profile on a Windows 2000 workstation, but they cannot manage local groups.

H

HAL (Hardware Abstraction Layer)	Software that makes it easy for operating systems to interact with different types of hardware.

Hard disk	A magnetic storage device used to store computer data. Workstation computers and servers both have hard disks.
Hardware Abstraction Layer (HAL)	Software that makes it easy for operating systems to interact with different types of hardware.
Hardware Compatibility List (HCL)	A list of hardware devices that have been tested by Microsoft and are known to be compatible with Windows 2000.
Hardware profile	A registry entry that lists the physical devices and services on your computer that Windows 2000 should enable on startup. Profiles can be created for computers that alternate between two or more hardware configurations.
Hashing algorithms	Hashing algorithms are used to create a message digest to ensure that data integrity is maintained. A sender creates a message digest by performing the hash function on the data files to be transmitted. The receiver performs the same action on the data received and compares the two message digests. If they are the same then the data was not altered.
HCL (Hardware Compatibility List)	A list of hardware devices that have been tested by Microsoft and are known to be compatible with Windows 2000.
Header	The header is the initial section of an IPM which contains addressing and routing information for the e-mail message.
Hello PDU	A Hello PDU; such as End System Hello (ESH), Intermediate System Hello (ISH), or IS to IS Hello (IIH); establishes and maintain adjacencies.
Heterogenous	A network that consists of many foreign TCP/IP-based hosts is known as a heterogeneous environment. TCP/IP provides the protocol to connect many foreign computer systems, because each system uses the same protocol.
Hierarchical Storage Management (HSM)	Hierarchical Storage Management (HSM) monitors the way data is used, then automatically moves data between high- and low-cost storage media in a way that will maximize storage utilization. The bulk of an organization's data is kept on slower devices, then a copy of that data is transferred to faster disk drives when needed. This process optimizes utilization by allowing the high-speed disk drives to act as caches for the slower mass storage devices.
High-level formatting	A logical formatting process that prepares the disk to be used by a specific file system. It scans the disk and marks bad sectors, creates the partition boot sector, modifies the partition table on the hard disk, creates the File Allocation Table for FAT volumes, and creates the Master File Table for NTFS volumes.
High-water mark	A server's highest local USN value for which another server has received updates. For example, if Server2 has received updates from Server1 up to Server1's local USN value 4653, then 4653 is Server2's high-water mark for Server1.

Hives	Sections of the Registry made up of keys, subkeys, and values, which are saved as files on your hard disk.
H-node	A protocol used to support NetBIOS over TCP/IP. It is a combination of the p-node and b-node. The default function of an h-node is a P-node. If it cannot resolve a name through the NetBIOS name server, it uses a broadcast to resolve the name.
Hold time	The hold time is the amount of time that a neighbor is considered to be functioning properly without a router receiving a packet from the neighbor.
Hold-down method	With the hold-down method, routers will, for a period of time, "hold" an update that reinstates an expired link. The time period typically reflects the time required to attain convergence on the network. The hold-down timer is reset when the timer runs out or when a network change occurs.
Home directory	A designated folder that is accessible to the user and can contain his or her files and programs. The home directory is assigned in Active Directory Users and Computers or Local Users and Groups and can be assigned to one user or shared by many.
Hop	A hop is a stage on an electronic message's journey from sender to receiver.
Host headers	Alternative names that differentiate multiple Web sites hosted on the same Microsoft Internet Information Server computer. You can allow Web sites to use the same IP address and port number by configuring a unique host header for each site.
Host IDs	An identifier of a workstation, server, router, or other TCP/IP host within a segment. The network ID must be unique to the network ID.
Host name	An alias assigned to a computer by an administrator to identify a TCP/IP host. The host name can be any 256-character string. Multiple host names can be assigned to the same host. Many utilities can use host names rather than the TCP/IP address. A host name always corresponds to an IP address that is stored in a HOSTS file or in a database on a DNS or NetBIOS name server.
Host name resolution	The process of mapping TCP/IP host names to IP addresses.
HOSTS file	A local text file in the same format as the 4.3 Berkeley Software Distribution (BSD) UNIX\etc\host file that maps host names to IP addresses. This file is used to resolve host names for TCP/IP utilities.
Hot Site	A hot site is a fault tolerant strategy which provides a redundant work location. If a disaster renders a work site unusable, the effected organization may have a hot site in which to relocate. Hot sites have the following characteristics: • This is a fully configured facility with power, A/C, etc., fully functional servers and clients that are up-to-date mirroring the production system. • A hot site is immediately available in the event of a disaster.

	• The site is expensive to maintain; requires constant maintenance of the hardware, software, data, and applications; and presents a security risk. • This facility is necessary when an organization cannot tolerate any downtime.
Hot Spare	A hot spare is a component that is connected to a system. A hot spare can take over automatically when another component fails.
Hot Swap	A component that is *hot-swappable* can be removed and replaced while the system is still running.
HSM (Hierarchical Storage Management)	Hierarchical Storage Management (HSM) monitors the way data is used, then automatically moves data between high- and low-cost storage media in a way that will maximize storage utilization. The bulk of an organization's data is kept on slower devices, then a copy of that data is transferred to faster disk drives when needed. This process optimizes utilization by allowing the high-speed disk drives to act as caches for the slower mass storage devices.
HTML (Hypertext Markup Language)	A series of rules for formatting documents that you can transfer between platforms. It is the language used to format ASCII text files as pages for the World Wide Web.
HTTP (Hypertext Transfer Protocol)	The standard protocol for Internet browsing. Using the Hypertext Transfer Protocol (HTTP) with Exchange lets both users and anonymous users access mailboxes, public folders, and address lists by typing the Exchange server's URL into an Internet browser.
HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)	HTTPS is a secure form of HTTP that uses SSL as a sublayer for security.
Hub	A network device that ties multiple workstations (or other devices) together for communication on a network. A hub can come with 5 ports or more and is basically a repeater of data. Also called a multi-port repeater.
Hub Transport server	The Hub Transport server is responsible for handling all message delivery in Exchange 2007.
Hyperlink	A word, phrase, or graphic formatted so that clicking it allows you to display data from another file on your computer, the network, or the Internet.
Hypertext Markup Language (HTML)	A series of rules for formatting documents that you can transfer between platforms. It is the language used to format ASCII text files as pages for the World Wide Web.
Hypertext Transfer Protocol (HTTP)	The standard protocol for Internet browsing. Using the Hypertext Transfer Protocol (HTTP) with Exchange lets both users and anonymous users access mailboxes, public folders, and address lists by typing the Exchange server's URL into an Internet browser.

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)	HTTPS is a secure form of HTTP that uses SSL as a sublayer for security.

I

.INF file	Files that contain the necessary Registry keys for specific policy settings. You use the System Preparation Tool and the Setup Manager Wizard to create .INF files for Windows 2000.
IAB (Internet Architecture Board)	A technical advisory group of the Internet Society responsible for setting Internet standards including publishing RFC's and overseeing the standards process. This organization governs the Internet Engineering Task Force (IETF), Internet Assigned Number Authority (IANA), and the Internet Research Task Force (IRTF).
IAS (Internet Authentication Service)	Software services that furnish authentication and security for dial-in users.
IBGP (Internal BGP)	Internal BGP (IBGP) is used by BGP to exchange information within the autonomous system.
ICANN (Internet Corporation for Assigned Names and Numbers)	ICANN, or the Internet Corporation for Assigned Names and Numbers, is a private non-profit corporation tasked with IP address space allocation, protocol assignment, and domain name system management.
ICMP (Internet Control Message Protocol)	An Internet protocol used to report errors and control messages on behalf of IP. ICMP reports errors and provides feedback on specific conditions. ICMP messages are carried as IP datagrams and therefore are not reliable.
IDE (Integrated Device Electronics)	A standard electronic interface that allows a computer to communicate with a storage device such as the hard drive or a CD-ROM drive.
IEEE (Institute of Electrical and Electronics Engineers)	A technical professional group that, among other contributions, develops standards (such as the 802.x series of standards) that often become national and international standards.
IETF (Internet Engineering Task Force)	This organization works to develop solutions to technical problems as they occur on the Internet. They also work to develop Internet standards and protocols.
IGMP (Internet Group Management Protocol)	Informs routers that hosts of a certain multicast group are available on a given network. This information is then passed to other routers so that each router that supports multicasting is aware of which host groups are on a particular network. IGMP packets are transported using IP datagrams, and are considered unreliable.
IGMP message	IGMP messages to exchange information, such as routing diagrams, with other routers.
IGMP snooping	IGMP snooping enables a switch to detect multicast patterns and multicast traffic in the overall traffic flow on a network; thus making a switch aware of Layer 3. IGMP Snooping listens to multicast join and remove messages to:

	• Restrict unwanted traffic flow. • Allow traffic to flow to the optimal ports.
IGP (Interior Gateway Protocol)	Interior Gateway Protocol (IGP) is a routing protocol that exchanges information within an autonomous system and can be controlled by the system in which they operate. The most common examples of IGPs are Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-Intermediate System (IS-IS), and Enhanced Interior Gateway Routing Protocol (EIGRP).
IIS (Internet Information Server)	A network server that allows you to send HTML documents using HTTP. IIS installs with Windows 2000 Server. Peer Web Services (PWS) installs with Windows 2000 Professional.
IMAP4 (Internet Message Access Protocol Version 4)	Like POP3, IMAP4 is a protocol that allows a client to download messages from a server. (It does not allow you to send messages.) IMAP4 is much more powerful than POP3. For example, with IMAP4, you can open all folders in your mailbox, not just the Inbox, as well as public folders on the server.
IN record	A type of name service record that can be defined by using the DNS Console utility.
In-band management	In-band management uses a normal network connection with the server for performing management tasks. Tools such as Telnet, Remote Desktop, or SNMP provide in-band server management.
Incremental backup	A backup method that copies to tape only those files that have not been marked by the previous normal or incremental backups. After backing the files to tape, an incremental backup marks each file as having been backed up.
Individual NTFS permissions (special access permissions)	The NTFS file system provides the ability to assign individual users access rights to files and folders.
Industry Standard Architecture (ISA)	A 16-bit I/O bus slot found on 286 through Pentium machines. ISA buses: • Have DIP switches and jumpers. • Have 98 pins. • Are backwards compatible with earlier 8-bit designs. • Are more likely to be paired with PCI buses rather than being replaced by EISA. • Are normally black plastic.
Infrared (IR)	Infrared (IR) wireless networking employs light waves that are outside of the visible light spectrum. IR networks are very insecure because the signals are not encrypted, and they can be easily intercepted.
Initialization aid	A hardware device that lets you reset the relays on a multi-station access unit.

Institute of Electrical and Electronics Engineers (IEEE)	A technical professional group that, among other contributions, develops standards (such as the 802.x series of standards) that often become national and international standards.
Integrated Device Electronics (IDE)	A standard electronic interface that allows a computer to communicate with a storage device such as the hard drive or a CD-ROM drive.
Integrated Services Digital Network (ISDN)	ISDN is another alternative to traditional dial-up that can be used to connect to the Internet or to directly communicate with another computer connected to the ISDN network. ISDN is more common in Europe than in the U.S. ISDN can use regular telephone wiring, but must be connected to a special ISDN network. Levels of ISDN service include: • BRI (Basic Rate Interface): ▪ 2 64-Kbps bearer (B) channels can transfer data up to 128 Kbps. Only one B channel is used during phone use. ▪ 1 16-Kbps delta (D) channel for connection control. • PRI (Primary Rate Interface): ▪ 23 B channels (each at 64 Kbps) for data transmission. ▪ 1 D channel (at 64 Kbps) for connection control.
Intel x86 machines	A computer containing an IBM-compatible processor built by Intel, Cyrix, or AMD.
Intelligent Platform Management Interface (IPMI)	The Intelligent Platform Management Interface (IPMI) is a specification for monitoring physical information about a computer. IPMI is an embedded chip on the motherboard, referred to as the baseboard management controller, which provides system information that allows the network administrator to monitor and manage a remote system, even if the remote system is not powered on.
Interactive	A system group that is not used for network administration but automatically includes a user who logs on to the computer locally. Interactive members access resources on the computer at which they are physically sitting by logging on and interacting with that computer.
Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP) is a routing protocol that exchanges information within an autonomous system and can be controlled by the system in which they operate. The most common examples of IGPs are Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-Intermediate System (IS-IS), and Enhanced Interior Gateway Routing Protocol (EIGRP).
Interleave ratio	Sectors on a hard disk are not consecutively numbered. Instead, they are interleaved. this gives the hard disk drive interface time to process the data before the subsequently-numbered sector passes beneath the read/write head. An interleave ratio of 1:1 has no interleave at all, a 1:2 ratio means the subsequently-numbered sector is the second sector from the current one, a 1:3 ratio means the next sector is three sectors from the current one, and so on.

Interleaving	Interleaving increases the rate at which data can be written to or read from a memory module by grouping data into contiguous blocks instead of dispersing data intermittently. The following components must be interleaving-enabled in order for interleaving to work: • Motherboard • BIOS • Memory Module
Intermediate System to Intermediate System (IS-IS)	Intermediate System to Intermediate System (IS-IS) is an OSI-based link-state routing protocol.
Internal BGP (IBGP)	Internal BGP (IBGP) is used by BGP to exchange information within the autonomous system.
Internal relay	Accepted domains identify the domains for which the organization is solely responsible and the SMTP domains from which the server will accept messages. There are three types of accepted domains in Exchange 2007: • Authoritative is the domain over which the Exchange server has sole responsibility. In a typical environment, the organization will have an e-mail domain of "company.com" which is hosted by the company's e-mail server. If another e-mail system or domain exists in the environment, internal and external relays are employed. • An internal relay is an e-mail domain that is hosted by another Active Directory Forest within the Exchange organization. This system uses different e-mail addresses, but all incoming mail goes through the Exchange organization. • An external relay accepts e-mail for an external organization and then delivers it to an external entity such as the Internet via the Edge Transport server.
Internal router	An internal router is located in the same area as all other interfaces. All internal routers with an area have the same are have identical LSDBs.
International Telecommunications Union (ITU)	A committee that has set most standards related to modems since the late 1980s.
Internet	A general name for the informal system of connected computers all around the world. These computers (and therefore their users) use telephone lines to send and receive data from other computers. In order to send and receive data accurately, the networking software inside the computers uses a set of commonly agreed upon protocols and computer languages.
Internet Architecture Board (IAB)	A technical advisory group of the Internet Society responsible for setting Internet standards including publishing RFC's and overseeing the standards process. This organization governs the Internet Engineering

	Task Force (IETF), Internet Assigned Number Authority (IANA), and the Internet Research Task Force (IRTF).
Internet Authentication Service (IAS)	Software services that furnish authentication and security for dial-in users.
Internet clients	A client computer using SMTP, POP3, IMAP4, HTTP, LDAP, MIME, and/or NNTP protocols to connect to Web sites and receive and send Internet mail.
Internet Control Message Protocol (ICMP)	An Internet protocol used to report errors and control messages on behalf of IP. ICMP reports errors and provides feedback on specific conditions. ICMP messages are carried as IP datagrams and therefore are not reliable.
Internet Corporation for Assigned Names and Numbers (ICANN)	ICANN, or the Internet Corporation for Assigned Names and Numbers, is a private non-profit corporation tasked with IP address space allocation, protocol assignment, and domain name system management.
Internet Engineering Task Force (IETF)	This organization works to develop solutions to technical problems as they occur on the Internet. They also work to develop Internet standards and protocols.
Internet Group Management Protocol (IGMP)	Informs routers that hosts of a certain multicast group are available on a given network. This information is then passed to other routers so that each router that supports multicasting is aware of which host groups are on a particular network. IGMP packets are transported using IP datagrams, and are considered unreliable.
Internet Information Server (IIS)	A network server that allows you to send HTML documents using HTTP. IIS installs with Windows 2000 Server. Peer Web Services (PWS) installs with Windows 2000 Professional.
Internet Layer	The layer in the TCP/IP protocol suite that includes four Internet protocols. They are Internet Protocol, Address Resolution Protocol, Internet Control Message Protocol, and Internet Group Management Protocol.
Internet Message Access Protocol Version 4 (IMAP4)	Like POP3, IMAP4 is a protocol that allows a client to download messages from a server. (It does not allow you to send messages.) IMAP4 is much more powerful than POP3. For example, with IMAP4, you can open all folders in your mailbox, not just the Inbox, as well as public folders on the server.
Internet Protocol (IP)	The protocol in TCP/IP that addresses and sends TCP packets on a network.
Internet Protocol Security (IPSec)	IPSec is a security mechanism that can be used as its own VPN protocol for network to network links or it can serve as the data encryption mechanism for other VPN protocols, such as L2TP. IPSec (Internet Protocol Security) can be used to encrypt any traffic supported by the IP protocol. This includes Web, e-mail, telnet, file transfer, and SNMP traffic as well as countless others. IPSec is fully

	capable of providing a secure means to communicate for any LAN or Internet based system using TCP/IP. IPSec is the most widely deployed VPN technology used for network to network VPN links. IPSec can be used to connect two individual systems, a system to a network, or two networks together. VPNs are used to connect trusted systems together over an untrusted network. The Internet is a common untrusted network used to connect distant networks together. Use IPSec to encrypt data in a VPN tunnel as it passes between two communication partners. Even if someone intercepts the traffic, they will be unable to extract the contents of the messages because they are encrypted.
Internet Protocol version 4 (IPv4)	Internet Protocol version 4 (IPv4) is an address family that is used to identify routing sessions for protocols that use standard IP version 4 address prefixes, such as BGP. In the IPv4 address family: • Unicast or multicast address prefixes can be specified. • Unicast routing information is advertised by default when a BGP peer is configured unless the advertisement of unicast IPv4 information is explicitly turned off.
Internet Research Task Force (IRTF)	This organization has the responsibility to coordinate all TCP/IP-related research projects.
Internet service provider (ISP)	An ISP (Internet service provider) is a company that provides Internet access and other web related services.
Internet Society (ISOC)	A global organization created in 1992. Responsible for the internetworking technologies and applications of the Internet. It is also responsible for the further development of the standards and protocols that allow the Internet to function.
Internetwork	A network that consists of multiple network segments. Each segment is defined by a separate network address. Internetworks are connected by routers that maintain tables with the addresses of each segment on the network.
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)	IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) is an older communication protocol used to interconnect clients and servers on a Novell NetWare operating system environment. IPX is a connectionless packet protocol that operates at the Network layer of communication. SPX is a transport layer protocol that sits on top of the IPX layer providing connection-oriented services between network nodes.
InterNIC	The Internet organization that has the responsibility to allocate all IP addresses.

Interprocess communications mechanisms	The methods by which tasks and processes to exchange data under a multitasking operating system. Mailboxes, queues, semaphores, shared memory, and signals are all IPC mechanisms.
Interrupt Request Line (IRQ)	A physical line that devices use to send signals to the processor when they want to send or receive information.
Intersite connection object	A connection object whose source and target replication partners exist in different sites.
Intersite replication	Replication between sites.
Intersite Topology Generator (ISTG)	A domain controller whose Knowledge Consistency Checker (KCC) establishes inbound intersite Connection objects for all bridgehead servers in a site.
Intranet	An intranet is a private network that happens to employ Internet information services.
Intrasite connection object	A connection object whose source and target replication partners exist in the same site.
Intrasite replication	Replication within a site.
Inverse lookup	The process used to resolve the host name associated with a known IP address when a host resolver sends a request to a name server.
IP (Internet Protocol)	The protocol in TCP/IP that addresses and sends TCP packets on a network.
IP Address	A unique address assigned to each computer (workstation or server) on an IP network so they can communicate with each other. IP addresses are usually written in dotted-decimal notation. Each address is made up of four 'octets' separated by periods. A typical IP address is written in decimal format. An IP address can be assigned permanently to a single computer (static) or assigned on a session basis by a service such as DHCP (dynamic).
IP multicasting	IP multicasting is a very efficient and effective tool for transmitting large amounts of data to multiple destinations.
Ipconfig	A TCP/IP utility. Type "ipconfig" at the command prompt to display the TCP/IP information for the computer.
IPMI (Intelligent Platform Management Interface)	The Intelligent Platform Management Interface (IPMI) is a specification for monitoring physical information about a computer. IPMI is an embedded chip on the motherboard, referred to as the baseboard management controller, which provides system information that allows the network administrator to monitor and manage a remote system, even if the remote system is not powered on.
IPSec (Internet Protocol Security)	IPSec is a security mechanism that can be used as its own VPN protocol for network to network links or it can serve as the data encryption mechanism for other VPN protocols, such as L2TP.

	IPSec (Internet Protocol Security) can be used to encrypt any traffic supported by the IP protocol. This includes Web, e-mail, telnet, file transfer, and SNMP traffic as well as countless others. IPSec is fully capable of providing a secure means to communicate for any LAN or Internet based system using TCP/IP. IPSec is the most widely deployed VPN technology used for network to network VPN links. IPSec can be used to connect two individual systems, a system to a network, or two networks together. VPNs are used to connect trusted systems together over an untrusted network. The Internet is a common untrusted network used to connect distant networks together. Use IPSec to encrypt data in a VPN tunnel as it passes between two communication partners. Even if someone intercepts the traffic, they will be unable to extract the contents of the messages because they are encrypted.
IPv4 (Internet Protocol version 4)	Internet Protocol version 4 (IPv4) is an address family that is used to identify routing sessions for protocols that use standard IP version 4 address prefixes, such as BGP. In the IPv4 address family: • Unicast or multicast address prefixes can be specified. • Unicast routing information is advertised by default when a BGP peer is configured unless the advertisement of unicast IPv4 information is explicitly turned off.
IPv6	A new packet structure that has 128-bit source and destination IP addresses, which are four times larger than the current Ipv4. Ipv6 also provides for a simplified header format and supports time-dependent traffic for use with voice and video that require specified bandwidth. Ipv6 is also extensible to provide for additional headers if needed.
IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)	IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) is an older communication protocol used to interconnect clients and servers on a Novell NetWare operating system environment. IPX is a connectionless packet protocol that operates at the Network layer of communication. SPX is a transport layer protocol that sits on top of the IPX layer providing connection-oriented services between network nodes.
IRQ (Interrupt Request Line)	A physical line that devices use to send signals to the processor when they want to send or receive information.
IRTF (Internet Research Task Force)	This organization has the responsibility to coordinate all TCP/IP-related research projects.
ISA (Industry Standard Architecture)	A 16-bit I/O bus slot found on 286 through Pentium machines. ISA buses: • Have DIP switches and jumpers. • Have 98 pins.

	• Are backwards compatible with earlier 8-bit designs. • Are more likely to be paired with PCI buses rather than being replaced by EISA. • Are normally black plastic.
ISCSI	iSCSI is a network protocol that encapsulates storage device communication data into IP packets for transmission over an Ethernet connection allowing IP-connected hosts to access a Storage Area Network (SAN). iSCSI provides the benefits of a FC SAN without the cost of fibre channel hardware. Using Ethernet and iSCSI, you can create a very powerful, very fast SAN using off-the-shelf, commodity-grade Ethernet hardware such as Cat5/5e cabling and Ethernet switches.
ISDN (Integrated Services Digital Network)	ISDN is another alternative to traditional dial-up that can be used to connect to the Internet or to directly communicate with another computer connected to the ISDN network. ISDN is more common in Europe than in the U.S. ISDN can use regular telephone wiring, but must be connected to a special ISDN network. Levels of ISDN service include: • BRI (Basic Rate Interface): ▪ 2 64-Kbps bearer (B) channels can transfer data up to 128 Kbps. Only one B channel is used during phone use. ▪ 1 16-Kbps delta (D) channel for connection control. • PRI (Primary Rate Interface): ▪ 23 B channels (each at 64 Kbps) for data transmission. ▪ 1 D channel (at 64 Kbps) for connection control.
IS-IS (Intermediate System to Intermediate System)	Intermediate System to Intermediate System (IS-IS) is an OSI-based link-state routing protocol.
ISOC (Internet Society)	A global organization created in 1992. Responsible for the internetworking technologies and applications of the Internet. It is also responsible for the further development of the standards and protocols that allow the Internet to function.
ISP (Internet service provider)	An ISP (Internet service provider) is a company that provides Internet access and other web related services.
ISTG (Intersite Topology Generator)	A domain controller whose Knowledge Consistency Checker (KCC) establishes inbound intersite Connection objects for all bridgehead servers in a site.
ITU (International Telecommunications Union)	A committee that has set most standards related to modems since the late 1980s.
IUSR_computername	The standard Internet guest account that the server uses to allow anonymous connections to your Windows Internet server. When you install IIS or PWS, this file is automatically created.

J

.JRS file	Exchange 2007's database engine is referred to as the Extensible Storage Engine (ESE). ESE is a transactional database that writes information into RAM memory and into a log file. Once it is in the log file, it will be written to disk. There are a number of files used to store information: • An .edb file is located in the actual database itself. All of a user's messages, folders, public folders, contacts, appointment information, etc. is all stored on the .edb file. An .edb file size can exceed multiple GB. • A .log file is an ESE transaction log file. All .log files are 1 MB. • A .jrs file is a reserve log file which is used to commit any transactions that are still in memory in the event of the server running out of disk space. All .jrs files are 1 MB. • A .chk file is used to identify which log files have been committed to the database. The size of .chk file varies from 2-3 KB. The ESE takes the following steps to write information into database files: 1. The ESE writes a message into memory RAM when it arrives at the server. 2. At the same time that information is written to RAM, it's written into the current .log file. All current log files are named E00.log. The information is written in a sequential format until the log file is full. When the log file is full, it will be renamed. 3. Once it has been committed to the log file, the information is written to the .edb file. 4. The checkpoint file is updated to indicate that the transaction log that has been committed to the database.
Java	A programming language designed to let programmers create applications for the Internet. Java applications do not depend on a particular operating system or hardware platform to run.
Journaling	Journaling is the ability to record and retain all communications in an organization.

K

KCC (Knowledge Consistency Checker)	A process that runs on each domain controller and creates inbound Connection objects (almost always intrasite Connection objects).
Keepalive messages	Keepalive messages act as hello packets to ensure that routers are still responsive.
Kerberos	Kerberos is an authentication encryption protocol designed to provide security for the initial logon process and service requests. Kerberos uses symmetric key cryptography, employs DES, and provides end-to-end security.

Kernel mode	A privileged operating mode for the operating system files and processes that interact directly with the computer's hardware.
Key	A part of the Registry. Keys appear as folders in the Registry window and can contain subkeys and values.
Knowledge Consistency Checker (KCC)	A process that runs on each domain controller and creates inbound Connection objects (almost always intrasite Connection objects).

L

.LOG file	Exchange 2007's database engine is referred to as the Extensible Storage Engine (ESE). ESE is a transactional database that writes information into RAM memory and into a log file. Once it is in the log file, it will be written to disk. There are a number of files used to store information: • An .edb file is located in the actual database itself. All of a user's messages, folders, public folders, contacts, appointment information, etc. is all stored on the .edb file. An .edb file size can exceed multiple GB. • A .log file is an ESE transaction log file. All .log files are 1 MB. • A .jrs file is a reserve log file which is used to commit any transactions that are still in memory in the event of the server running out of disk space. All .jrs files are 1 MB. • A .chk file is used to identify which log files have been committed to the database. The size of .chk file varies from 2-3 KB. The ESE takes the following steps to write information into database files: 1. The ESE writes a message into memory RAM when it arrives at the server. 2. At the same time that information is written to RAM, it's written into the current .log file. All current log files are named E00.log. The information is written in a sequential format until the log file is full. When the log file is full, it will be renamed. 3. Once it has been committed to the log file, the information is written to the .edb file. 4. The checkpoint file is updated to indicate that the transaction log that has been committed to the database.
L2F (Layer 2 Forwarding Protocol)	L2F is a VPN protocol which offers no data encryption. L2F was combined with PPTP, creating L2TP. Support for IPSec was added, and the result is a very versatile, nearly universally interoperable VPN protocol that provides solid authentication and reliable data encryption.

L2TP (Layer Two Tunneling Protocol)	L2TP (Layer 2 Tunneling Protocol) is the VPN protocol that typically employs IPSec as its data encryption mechanism. L2TP is the recommended VPN protocol to use on dial-up VPN connections. L2TP was created by combining PPTP and L2F and adding in support for IPSec. The result is a very versatile, nearly universally interoperable VPN protocol that provides solid authentication and reliable data encryption.
LAN (Local area network)	A group of closely located computers or peripherals connected so that they can interact with each other as a network.
LAPM (Link Access Procedure for Modems)	A Data Link layer protocol called Link Access Procedure for Modems (LAPM) used by newer modems for error detection. LAPM is implemented in the modem hardware. LAPM is described by ITU's V.42 standard.
Layer 2 Forwarding Protocol (L2F)	L2F is a VPN protocol which offers no data encryption. L2F was combined with PPTP, creating L2TP. Support for IPSec was added, and the result is a very versatile, nearly universally interoperable VPN protocol that provides solid authentication and reliable data encryption.
Layer 3 switch	A layer 3 switch operates at the Network layer reading the logical address and making forwarding and receiving decisions. Contrast this with most switches that operate at the Data Link layer which read the MAC address.
Layer Two Tunneling Protocol (L2TP)	L2TP (Layer 2 Tunneling Protocol) is the VPN protocol that typically employs IPSec as its data encryption mechanism. L2TP is the recommended VPN protocol to use on dial-up VPN connections. L2TP was created by combining PPTP and L2F and adding in support for IPSec. The result is a very versatile, nearly universally interoperable VPN protocol that provides solid authentication and reliable data encryption.
Layered Service Provider (LSP)	A Layered Service Provider (LSP) distributes link-state information and defines the characteristics of an IS-IS router.
LCR (Local Continuous Replication)	Local Continuous Replication (LCR) is a cluster implementation which maintains a copy of the production storage group on a second set of disks that are connected to the same server using built-in asynchronous log shipping and log replay technology.
LDAP (Lightweight Directory Access Protocol)	A lightweight protocol that clients such as Outlook Express use to look up and search for addresses in an online directory. It also allows a user to add, edit, and delete information from the directory.
Lease	The period of time for which a dynamically assigned IP address remains valid for a DHCP client. Before the end of the lease, the client has to renew the lease or be assigned a new lease by DHCP.

Legacy streaming	Legacy streaming is the traditional method of backup for Exchange environments. When a legacy streaming backup is initiated: 1. The backup application will notify the database engine that a backup is being started. 2. The database engine creates a file that will be used as a marker that the backup is occurring. 3. The backup application freezes the database. 4. The backup application backs up the database. 5. The backup application copies the marker file which contains any additional transactions and log files which took place during the backup.
Licensing mode	The way you pay to use an application or operating system. You can choose Per Server or Per Seat licensing for Windows 2000.
Lightweight Directory Access Protocol (LDAP)	A lightweight protocol that clients such as Outlook Express use to look up and search for addresses in an online directory. It also allows a user to add, edit, and delete information from the directory.
Line Printer Daemon (LPD)	A service residing on a UNIX print server that receives print jobs from clients using the LPR utility.
Line Printer Daemon/Line Print Remote (LPD/LPR)	LPD/LPR is the most widely-used cross platform print protocol. LPD/LPR establishes connection between printing devices and workstations. LPD is usually loaded on the printing device. LPR is usually loaded onto the client workstation.
Line Printer Queue (LPQ)	This utility obtains the status of a print queue on a host running the Line Printing Daemon (LPD) service.
Line Printer Remote (LPR)	A utility on a client that allows it to send print jobs to the Line Printer Daemon on the server.
Link Access Procedure for Modems (LAPM)	A Data Link layer protocol called Link Access Procedure for Modems (LAPM) used by newer modems for error detection. LAPM is implemented in the modem hardware. LAPM is described by ITU's V.42 standard.
Link state routing protocol	Routing algorithm in which each router broadcasts or multicasts information regarding the cost of reaching each of its neighbors to all nodes in the internetwork. Link state algorithms create a consistent view of the network and are therefore not prone to routing loops, but they achieve this at the cost of relatively greater computational difficulty and more widespread traffic (compared with distance vector routing algorithms). Compare with distance vector routing algorithm.
Linked mailbox	Linked mailboxes are used in environments in which there are multiple forests (known as resource forests). When a linked mailbox is created, a mailbox and a disabled user account are created in the forest which hosts the Exchange organization. Once the mailbox has been created, it is then linked or associated with a user account that resides in the second forest. In order to assign an account from the second forest to the mailbox, a

	trust relationship must exist between the domain that contains the Exchange server and the domain in which the user account resides.
Link-local Multicast Name Resolution (LLMNR)	Link-local Multicast Name Resolution (LLMNR) enables IP hosts to perform IP address-to-host name resolution without a DNS server. LLMNR is feature used in Zeroconf networking and is being developed by Microsoft.
Linux	A popular (freely-distributable open source) operating system that runs on multiple hardware platforms.
LLC (Logical Link Control)	In the OSI model, the Logical Link Control (LLC) layer is one of two sublayers of the Data-Link layer. The LLC manages traffic (flow and error control) over the physical medium.
LLMNR (Link-local Multicast Name Resolution)	Link-local Multicast Name Resolution (LLMNR) enables IP hosts to perform IP address-to-host name resolution without a DNS server. LLMNR is feature used in Zeroconf networking and is being developed by Microsoft.
LMHOSTS file	An ASCII text file that associates IP addresses to computer names outside the local subnet. In Windows 2000, the Lmhost file is located in systemroot \System32\Drivers\Etc. You must manually update the LMHOSTS file.
Load balancing	Load balancing is the capability of a router to distribute traffic over all of its network ports that are the same metric from the destination address.
Local area network (LAN)	A group of closely located computers or peripherals connected so that they can interact with each other as a network.
Local Continuous Replication (LCR)	Local Continuous Replication (LCR) is a cluster implementation which maintains a copy of the production storage group on a second set of disks that are connected to the same server using built-in asynchronous log shipping and log replay technology.
Local GPO	A Group Policy Object (GPO) stored on the local computer. Every Windows 2000 computer has exactly one local GPO.
Local group	Groups used to provide users with permissions to access a network resource and to provide rights to perform system tasks.
Local Host	Addresses in the 127.0.0.0 range are reserved to refer to the local host (in other words "this" host or the host you're currently working at).
Local preference attribute	The local preference (type code 5) is a well-known discretionary BGP attribute that describes the preferred exit path from an AS. Local preferences are configured by assigning a number between 1 and 100; higher values representing higher preference over lower values.
Local routing table	A neighbor table contains a list of neighbors with which it has a BGP connection.
Local update sequence number	The USN of the local domain controller when an Active Directory update is made.

Local user accounts	User name and password information stored in the directory database of the local computer.
Local user profile	A profile stored on a user's local workstation.
Log file	A text file that contains detailed information about the backup procedures you perform with Windows Backup. Other processes, such as the Performance Monitor, also generate log files.
Log off	The process by which a user disconnects from a network and closes connections to mapped drives and printers.
Log on	The process by which a user gains access to a network by providing security credentials (usually a user name and password).
Logical Link Control (LLC)	In the OSI model, the Logical Link Control (LLC) layer is one of two sublayers of the Data-Link layer. The LLC manages traffic (flow and error control) over the physical medium.
Logoff script	A script that executes when a user logs off.
Logon script	A script that executes when a user logs on.
Long file name	A name for a file or folder that includes more characters than the standard MS-DOS 8.3 filename convention.
Loopback address	A reserved IP address, 127.0.0.1, that is used to perform loopback functions.
Loopback Processing Mode	A mode of processing Active Directory-based Group Policy Objects (GPOs) in which computer-specific settings replace or take precedence over user-specific settings.
LostAndFound container	An Active Directory container that holds objects that no longer have a valid parent container. For example, this could happen if an object is created on one domain controller while simultaneously the object's container is deleted or renamed on another domain controller.
Low-level disk formatting	A hard disk formatting process, usually performed by the disk manufacturer, that defines the basic physical structure of the disk. It runs a surface analysis to test the disk heads, defines sectors and assigns sector IDs, temporarily fills each sector, identifies bad sectors on the drive, and defines the interleave ratio.
LPD (Line Printer Daemon)	A service residing on a UNIX print server that receives print jobs from clients using the LPR utility.
LPD/LPR (Line Printer Daemon/Line Print Remote)	LPD/LPR is the most widely-used cross platform print protocol. LPD/LPR establishes connection between printing devices and workstations. LPD is usually loaded on the printing device. LPR is usually loaded onto the client workstation.
LPQ (Line Printer Queue)	This utility obtains the status of a print queue on a host running the Line Printing Daemon (LPD) service.

LPR (Line Printer Remote)	A utility on a client that allows it to send print jobs to the Line Printer Daemon on the server.
LSP (Layered Service Provider)	A Layered Service Provider (LSP) distributes link-state information and defines the characteristics of an IS-IS router.

M

.MSI file	A file with extension MSI that contains software installation instructions and data for use with the Windows Installer service.
.MST file	A file with the .MST extension that can be applied to a Windows Installer package (.MSI file) to customize it. Also called a software modification file.
MAC (Media Access Control) Address	A unique hardware address that is assigned to each device by the vendor. For example, a LAN adapter has a unique MAC address that is permanent to the adapter card.
MADCAP (multicast addressing server)	MADCAP is a multicast addressing server, which provides multicast address allocation.
MADMAN MIB	Madman.mib is the Management Information Base (MIB) for Simple Network Management Protocol (SNMP) Mail and Directory Management (MADMAN). Windows NT Performance Monitor counters are made available as MIB objects that can be monitored through SNMP.
Mail Exchanger (MX) record	A DNS resource record that you can define in DNS. The MX records specify a mail exchanger for a domain name: a host that will either process or forward mail for the domain name.
Mailbox delivery queue	Mailbox delivery queues only exist on Hub Transport servers in Exchange 2007. They hold messages for recipients whose mailbox data is stored on a Mailbox server within the same site as the Hub Transport server. More than one mailbox delivery queue can exist on a Hub Transport server.
Mailbox server	The Mailbox server in Exchange 2007 contains the mailbox and public folder databases. The Mailbox server role in Exchange 2007 supports multiple storage groups and multiple stores, making it possible to have up to 50 storage groups and up to 5 stores (databases) per storage group. The maximum number of stores on a single Exchange server is limited to 50.
Mailbox-enabled user	A mailbox-enabled user is an Active Directory user that has a mailbox that is hosted on one of the mailbox servers within an Exchange organization. A mailbox-enabled user can logon to the domain and access resources on the network according to the permissions and groups to which they are assigned. Mailbox-enabled users are the most common type of Exchange recipient.
Mail-enabled contacts	Mail-enabled contacts are used to make it easier for users within an Exchange organization to locate the contact details of people outside of your organization.

Mail-enabled user	A mail-enabled user is an Active Directory user the has an e-mail address associated with their account, but whose mailbox is stored on an external mail system. For example, a contractor who is working for the organization but is using their own e-mail address.
Malware	Another name for virus, which is a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found.
Management domains	Management domains are the network subdivisions specified in the X.400 international messaging standard. Management domains include Administration Management Domains (ADMDs) and Private Management Domains (PRMDs).
Management Information Base (MIB)	A database containing the data gathered by SNMP agents which monitor network traffic and components.
Management Information Bases (MIBs)	A set of manageable objects representing various types of information about a network device, such as the number of active sessions or the version of the network operating system software that is running on a host.
Mandatory user profile	A pre-configured user profile that the user cannot change, including desktop arrangement, screen saver, printer connections, and so on. One mandatory profile can be assigned to many users.
MAPI (Messaging Application Programming Interface)	A set of standard commands developed by Microsoft. Messaging services use these commands to communicate with other MAPI-compliant applications.
Mapping	Making an association between two different elements, such as computer names and IP addresses, drives and drive letters, and so on.
Master Boot Record (MBR)	The area of the hard disk containing the partition table for the drive and the specialized executable code necessary to boot the computer.
MAU (Multistation Access Unit)	The central connecting point for a token ring network.
MAU (Multi-station Access Unit)	A hub or concentrator that connects a group of computers to a local area network in token ring topology.
MBR (Master Boot Record)	The area of the hard disk containing the partition table for the drive and the specialized executable code necessary to boot the computer.
MD5 (Message-Digest algorithm 5)	Message-Digest algorithm 5 (MD5) is a cryptographic authentication method that prevents unauthorized routing messages from unapproved sources in EIGRP.
MDBEF (Message Database Encoding Format)	MDBEF is the internal format for e-mail messages in Exchange. The Exchange directory database (Dir.edb) is based on (but not entirely identical to) the International Telecommunications Union's X.500 directory recommendations.
MED attribute	The MultiExist-Discriminator (MED) (type code 4) is an optional, nontransitive BGP attribute (also known as a metric) that communicates to neighbors the preferred path for information to be sent to them.

Media (Transmission Media)	In the realm of information technology, transmission media refers to the cables and wires through which signals (such as electric current or light impulse) are transmitted through a network.
Media Access Control (MAC) Address	A unique hardware address that is assigned to each device by the vendor. For example, a LAN adapter has a unique MAC address that is permanent to the adapter card.
Media tester	Use a media tester to make sure that a cable is unbroken and that all cables are connected to the correct pins inside the connector.
Member server	An Windows 2000 Server computer that is not a domain controller. Member servers provide file and print services for the network.
Memory Interleaving	Interleaving increases the rate at which data can be written to or read from a memory module by grouping data into contiguous blocks instead of dispersing data intermittently. The following components must be interleaving-enabled in order for interleaving to work: • Motherboard • BIOS • Memory Module
Mesh	Mesh is a network topology that exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. This increases the network's fault tolerance because alternate paths can be used when one path fails. Two variations of mesh topologies exist: • Partial Mesh--Some redundant paths exist. • Full Mesh--Every node has a point-to-point connection with every other node.
Message Database Encoding Format (MDBEF)	MDBEF is the internal format for e-mail messages in Exchange. The Exchange directory database (Dir.edb) is based on (but not entirely identical to) the International Telecommunications Union's X.500 directory recommendations.
Message queue	In the Exchange 2007 messaging environment, messages are placed in queues as they wait to be sent. Queues are stored in an Extensible Storage Engine (ESE) databases which reside on Hub Transport servers. Exchange 2007 queues can hold up to a million messages, so in the event of a Hub Transport server failure, the database can be retrieved and mounted onto another Hub Transport server, at which point the queued messages will be sent to their recipients.
Message-Digest algorithm 5 (MD5)	Message-Digest algorithm 5 (MD5) is a cryptographic authentication method that prevents unauthorized routing messages from unapproved sources in EIGRP.

Messaging Application Programming Interface (MAPI)	A client access specification that enables clients to communicate with a messaging system. It is implemented as a subsystem in the Windows operating system. Microsoft and many other vendors support this standard.
MIB (Management Information Base)	A database containing the data gathered by SNMP agents which monitor network traffic and components.
MIBs (Management Information Bases)	A set of manageable objects representing various types of information about a network device, such as the number of active sessions or the version of the network operating system software that is running on a host.
Microcom Network Protocol (MNP)	A company called Microcom introduced a series of standards for early modems that described error detection techniques. The standards were called MNP Class 2, Class 3, and Class 4. This standard became popular with several modem manufacturers
Microkernel	The part of the operating system that handles vital low-level processes. These include deferred procedure calls, first-level interrupt handling, thread scheduling, and so on.
Microsoft Certificate Server	A certificate server for issuing and administering in-house digital certificates that let you authenticate the identity of visitors to your Web sites. It also lets you enable SSL encryption.
Microsoft Cluster Servers	Microsoft Cluster servers are fault-tolerant servers that use two separate nodes.
Microsoft Download Service (MSDN)	A bulletin board sponsored by Microsoft. Check the MSDN for support information and downloadable code.
Microsoft Exchange Mailbox store	A store is a database of Microsoft Exchange information. There are two types of Exchange stores: • A Mailbox store holds the information that comprise mailboxes in Exchange 2007, such as data, data definitions, indexes, checksums, and flags. Sent and received e-mails are held in the mailbox store. • A Public Folder store holds information that can be shared by users. Messages posted to public folders are held in the public folder store.
Microsoft Exchange Management Console	The Exchange Management Console is the graphical administration tool. It is comprised of a three-paned view that includes a tree view, results, and an actions pane. It cannot perform many of the administrative tasks that can be performed in the Exchange Management Shell.
Microsoft Exchange Management Shell	Microsoft Exchange Management Shell (Windows PowerShell) is a command line environment designed for automating administration and maintenance. The Exchange Management Shell is the primary management interface of 2007.

Microsoft Exchange PowerShell	Microsoft Exchange Management Shell (Windows PowerShell) is a command line environment designed for automating administration and maintenance. The Exchange Management Shell is the primary management interface of 2007.
Microsoft Exchange Public store	A store is a database of Microsoft Exchange information. There are two types of Exchange stores: • A Mailbox store holds the information that comprise mailboxes in Exchange 2007, such as data, data definitions, indexes, checksums, and flags. Sent and received e-mails are held in the mailbox store. • A Public Folder store holds information that can be shared by users. Messages posted to public folders are held in the public folder store.
Microsoft Exchange recovery storage group	A Microsoft Exchange storage group is a collection of Exchange stores (databases). A Recovery Storage Group (RSG) is a special storage group used for recovering Mailbox stores.
Microsoft Exchange storage group	A Microsoft Exchange storage group is a collection of Exchange stores (databases). A Recovery Storage Group (RSG) is a special storage group used for recovering Mailbox stores.
Microsoft Exchange store	A store is a database of Microsoft Exchange information. There are two types of Exchange stores: • A Mailbox store holds the information that comprise mailboxes in Exchange 2007, such as data, data definitions, indexes, checksums, and flags. Sent and received e-mails are held in the mailbox store. • A Public Folder store holds information that can be shared by users. Messages posted to public folders are held in the public folder store.
Microsoft Internet Explorer	An application that includes not only a Web browser but also a set of tools that integrates it with Microsoft Windows 95/98, NT, and 2000.
Microsoft Internet Information Server	A Windows NT Server file and application server designed to host Internet sites. IIS is integrated with Windows 2000 Server.
Microsoft Management Console (MMC)	A common framework for a variety of Windows 2000 administrative tools. It provides no functionality of its own.
Microsoft Technet	A compact disc from Microsoft that contains information to help you administer and troubleshoot networks.
Microsoft Transaction Server (MTS)	A processing system for creating and distributing Web applications using Active Server Pages. It tracks unique transactions, and ensures that each component of a process must be completed in order for the transaction to succeed.

Microsoft Web site	The Internet site that you can use to read information about Microsoft products or reach Microsoft support.
Migration	The process of transferring files, folders, and account information from a NetWare server to a Windows 2000 server.
Millions of Instructions Per Second (MIPS)	A measure of performance. Many computer companies use MIPS to measure the cost of computing. MIPS is also the name of a company that makes RISC processors.
MIME (Multipurpose Internet Mail Extensions)	MIME's primary purpose is allowing users to send attachments along with e-mail messages through the Internet. With MIME, you can use several different character sets, as well as binary data.
MIPS (Millions of Instructions Per Second)	A measure of performance. Many computer companies use MIPS to measure the cost of computing. MIPS is also the name of a company that makes RISC processors.
Mirrored volume	A mirrored volume stores data to two duplicate disks simultaneously. It provides fault tolerance because if one disk fails, data is preserved on the other disk, and the system switches immediately from the failed disk to the functioning disk to maintain service. Mirrored volumes: • Provide fault tolerance. Data is available even if one disk in the set fails. • Do not increase performance. • Require two disks. • Have a 50% overhead. Data is written twice, meaning that half of the disk space is used to store the second copy of the data.
Mirroring	Mirroring is a data protection method. To mirror data is to duplicate and store it in a separate location.
MMC (Microsoft Management Console)	A common framework for a variety of Windows 2000 administrative tools. It provides no functionality of its own.
M-node	A NetBIOS node that provides support over TCP/IP. The M-node is a combination of B-nodes and P-Nodes. The default is to function as a B-node.
MNP (Microcom Network Protocol)	A company called Microcom introduced a series of standards for early modems that described error detection techniques. The standards were called MNP Class 2, Class 3, and Class 4. This standard became popular with several modem manufacturers
Modem	A modem is a device that modulates and demodulates signals being sent and received across transmission media (telephone wire). For example, computer data is in digital form, which must be converted to analog. To receive data, the modem reconverts the signal back to digital form.
MPR (Multiple Provider Router)	A component that allows computers to use file and print resources on the network by routing requests to the correct redirector or provider.

MSAU (Multistation Access Unit)	The central connecting point for a token ring network.
MSDN (Microsoft Download Service)	A bulletin board sponsored by Microsoft. Check the MSDN for support information and downloadable code.
MSDP (Multicast Source Discovery Protocol)	Multicast Source Discovery Protocol (MSDP) is a mechanism that connects multiple PIM-SM domains; allowing the discovery of multicast sources in other domains.
MSN (The Microsoft Network)	An online network sponsored by Microsoft. You can find answers to technical questions, read articles about Microsoft products, chat with other users, and much more.
MTS (Microsoft Transaction Server)	A processing system for creating and distributing Web applications using Active Server Pages. It tracks unique transactions, and ensures that each component of a process must be completed in order for the transaction to succeed.
Multicast	Multicast is a transmission method that transmits packets from a single device to a specific set of hosts. It is optimal for transmitting voice and video applications and streaming video.
Multicast addressing server (MADCAP)	MADCAP is a multicast addressing server, which provides multicast address allocation.
Multicast scope	A range of multicast group IP addresses available to be leased to multicast clients by DHCP. Addresses are in the Class D address range -- 224.0.0.0 to 239.255.255.255 -- are reserved for use in IP multicasting.
Multicast Source Discovery Protocol (MSDP)	Multicast Source Discovery Protocol (MSDP) is a mechanism that connects multiple PIM-SM domains; allowing the discovery of multicast sources in other domains.
Multi-homed	The ability of a router to function using both static and dynamic routing. For example, you can configure a Windows 2000 computer with multiple network adapters and route between the two cards. Computers configured in this fashion are known as multihomed computers.
Multihoming	Multihoming is the term used to describe an AS that has more than one connection to the Internet. If an organization performs multihoming with BGP, it is accomplished in one of the following ways: • Each ISP only passes a default route to the AS. • Each ISP only passes a default route and provider-owned specific routes to the AS. • Each ISP passes all routes to the AS.
Multi-master replication model	A replication model in which updates can be made to any of several domain controllers (masters). The master that receives the update then replicates its updates to other domain controllers. Windows 2000 uses this replication model.

Multiple master domain model	In this Windows NT domain model, user accounts are distributed among more than one master domain and the domains communicate via trust relationships. In this model a user can log on from any domain because pass-through authentication sends the request to the user's home domain. This model is typically used for large companies that want centralized administration. Each network user account is created in one of the master domains. Other domains in the network are resource domains, which are usually created at the department level.
Multiple Provider Router (MPR)	A component that allows computers to use file and print resources on the network by routing requests to the correct redirector or provider.
Multiple Universal Naming Convention Provider (MUP)	A component that allows a remote computer to accept paths and filenames written in UNC format. The MUP keeps the UNC list so that the client computer does not have to rewrite the UNC names for each redirector on the network.
Multiplexer	A communications device that combines signals for transmission over a single transmission medium. A multiplexer is sometimes called a mux.
Multiprotocol BGP	Multiprotocol BGP is an enhanced extension of BGP that has the ability to carry IP multicast routes.
Multipurpose Internet Mail Extensions (MIME)	MIME's primary purpose is allowing users to send attachments along with e-mail messages through the Internet. With MIME, you can use several different character sets, as well as binary data.
Multistation Access Unit (MAU)	The central connecting point for a token ring network.
Multi-station Access Unit (MAU)	A hub or concentrator that connects a group of computers to a local area network in token ring topology.
Multistation Access Unit (MSAU)	The central connecting point for a token ring network.
Multitasking	In multitasking operating systems, the processor is time-sliced across tasks, devoting a certain amount of processing time to each task. The processor then alternates between tasks until they have all been completed. This process occurs so rapidly that the computer appears to be working on multiple tasks at one time.
Multithreading	An operating system feature that allows more than one process to work at the same time. For example, Winnt32.exe can decompress and copy files at the same time, since each task is a separate thread.
MUP (Multiple Universal Naming Convention Provider)	A component that allows a remote computer to accept paths and filenames written in UNC format. The MUP keeps the UNC list so that the client computer does not have to rewrite the UNC names for each redirector on the network.
MX (Mail Exchanger) record	A DNS resource record that you can define in DNS. The MX records specify a mail exchanger for a domain name: a host that will either process or forward mail for the domain name.

N

Name resolution	The process by which host names (such as Computer1) are translated to numerical IP addresses (such as 192.168.35.2). The principle means of name resolution in Windows 2000 is DNS. WINS may be used for some name resolution when earlier versions of Windows are still part of the network..
Name Service (NS) record	A name service record that is placed in a DNS server.
Named pipes	A mechanism that processes use to communicate with each other locally or remotely.
Namespace	A group of unique labels for objects in a shared computing environment. For example, the DNS database is a a tree structure called the domain namespace. Each domain (node) is named and can contain subdomains. The domain name identifies the position of the domain in relation to its parent domain. A group of contiguous names in such a structure constitutes a namespace.
NAS (Network-Attached Storage)	Network-Attached Storage (NAS) is another method of adding storage capacity to a network. A NAS system plugs directly into the network in the same way that workstations and other peripherals do. A NAS device is typically a pared down file server consisting of: • A RAID array with terabytes of storage space. • A motherboard (logic board). • One or more network interface cards. Multiple interface cards allow you to perform adapter teaming. • A minimal network operating system.
NAT (Network Address Translation)	The process of converting the IP addresses used in private network (such as an intranet) to Internet IP addresses. This increases the number addresses available within the the intranet without reducing the number of available Internet addresses.
NBMA (NonBroadcast MultiAccess)	An NonBroadcast MultiAccess (NBMA) network is a network that interconnects multiple routers but does not have broadcast capabilities (examples are Frame Relay, X.25, and ATM).
NBTSTAT	A Microsoft utility that checks the state of current NetBIOS over TCP/IP connections. It also updates the LMHOSTS cache, and determines your registered name and scope ID. The utility is also used for troubleshooting and pre-loading the NetBIOS name cache.
NDIS (Network Device Interface Specification) 4.0	A set of software rules that specify how protocols communicate with device drivers. All NDIS-compatible cards and drivers can communicate with each other without needing to use specifically tailored protocols.
NDS (NetWare Directory Services)	NDS lets you display a list of shared objects and servers in a NetWare network. The NDS tree shows the available resources as a hierarchical list.

Neighbor discovery/recovery	Neighbor discovery/recovery is a mechanism that enables routers to dynamically learn about the other routers on their directly attached networks. Neighbor discovery/recovery: • Allows routers to know when neighbors become unreachable or inoperative. • Has low overhead. • Periodically sends and receives small hello packets to and from neighboring routers. If hello packets start to not be received from a particular router, neighbor discovery/recovery will assume that the router is not functioning.
NET command	This command accepts several command arguments that control functions such as logon, logoff, and resource connections.
NetBEUI (NetBIOS Extended User Interface)	A protocol supported by all Microsoft products. It has a small stack size, excellent data transfer rates, and is compatible with all Microsoft networks. It cannot be routed, and it is not compatible with non-Microsoft networks.
NetBIOS (Network Basic Input/Output System)	A program that allows computers to share resources on a network. Each computer has a unique NetBIOS name that provides applications with a common set of commands for requesting the lower-level network services that are necessary to transmit information between network resources.
NetBIOS applications	A utility that checks the state of current NetBIOS over TCP/IP connections. It is also used to update the LMHOSTS cache and determine your registered name and scope ID.
NetBIOS Extended User Interface (NetBEUI)	A protocol supported by all Microsoft products. It has a small stack size, excellent data transfer rates, and is compatible with all Microsoft networks. It cannot be routed, and it is not compatible with non-Microsoft networks.
NetBIOS name cache	A local cache containing the NetBIOS names that the local computer has recently resolved. Having the IP address in cache eliminates the need for extraneous broadcasts on the network.
NetBIOS name resolution	The process of successfully mapping a computer's NetBIOS name to an IP address. Before an IP address can be resolved to a hardware address, a computer's NetBIOS computer name must be resolved to an IP address.
NetBIOS scope	The NetBIOS scope parameter is configured on the remote host. The scope ID must match the scope ID on your Microsoft clients or they will not be able to communicate with NetBIOS.
NetDDE (Network Dynamic Share)	A Win32 service that can share processes with other Win32 services. It is a service registered under the Services subkey in the Registry.
NetShow Player	Software that runs on the client computer and lets you play, start, and stop audio, illustrated audio (slide show), and full-motion video files.

Netstat	A Microsoft utility that displays the protocol statistics and the current state of TCP/IP connections.
NetWare	Networking software from Novell.
NetWare Directory Services (NDS)	NDS lets you display a list of shared objects and servers in a NetWare network. The NDS tree shows the available resources as a hierarchical list.
Network	A system group that is not used for network administration. It includes any user who is currently connected from another computer on the network to a shared resource on your computer.
Network Address Translation (NAT)	The process of converting the IP addresses used in private network (such as an intranet) to Internet IP addresses. This increases the number addresses available within the the intranet without reducing the number of available Internet addresses.
Network architecture	A standardized set of physical and data link layer protocols that serve as the network's foundation upon which other protocol layers can function.
Network Basic Input/Output System (NetBIOS)	A program that allows computers to share resources on a network. Each computer has a unique NetBIOS name that provides applications with a common set of commands for requesting the lower-level network services that are necessary to transmit information between network resources.
Network Device Interface Specification (NDIS) 4.0	A set of software rules that specify how protocols communicate with device drivers. All NDIS-compatible cards and drivers can communicate with each other without needing to use specifically tailored protocols.
Network Dynamic Share (NetDDE)	A Win32 service that can share processes with other Win32 services. It is a service registered under the Services subkey in the Registry.
Network ID	The network ID identifies the TCP/IP hosts that are located on the same physical network. Any hosts that are on the same physical network must be assigned the same network ID in order to communicate.
Network Interface Layer	The base of the Department of Defense (DOD) model. This layer has the responsibility to place frames on the wire and retrieve frames from the wire.
Network Layer	Layer 3 of the OSI reference model. This layer provides connectivity and path selection between two end systems. The network layer is the layer at which routing occurs. Corresponds roughly with the path control layer of the SNA model. See also application layer, data link layer, physical layer, presentation layer, session layer, and transport layer.
Network Monitor	A Windows troubleshooting tool. It monitors the information in frames which are transferred over the network to or from the local computer.
Network News Transfer Protocol (NNTP)	A protocol that provides access to Internet newsgroups. It allows a client to read messages sent to newsgroups and makes it possible for hosts to replicate articles back and forth.

Network number	The unique number that the NWLink IPX/SPX protocol uses to identify a specific part of the network. Also called an external network number.
Network printer	A printer connected to the network and registered as a shared resource.
Network protocols	Protocols that allow computers to communicate with each other over a network. For example, AppleTalk and NetBEUI are network protocols.
Network Service Access Point (NSAP)	A Network Service Access Point (NSAP) is used to identify routers and build the topology table in IS-IS.
Network Time Protocol (NTP)	NTP is used to communicate time synchronization information between systems on a network.
Network-Attached Storage (NAS)	Network-Attached Storage (NAS) is another method of adding storage capacity to a network. A NAS system plugs directly into the network in the same way that workstations and other peripherals do. A NAS device is typically a pared down file server consisting of: • A RAID array with terabytes of storage space. • A motherboard (logic board). • One or more network interface cards. Multiple interface cards allow you to perform adapter teaming. • A minimal network operating system.
New Technology File System (NTFS)	A Windows NT file system that provides secure and robust file access. File and folder names can be up to 255 characters (long file names). Permissions can be assigned to individual files and folders. Windows 2000 updates NTFS with new features.
Newsreader	A client that uses NNTP to read postings in Internet newsgroups.
Next-hop attribute	The next-hop (type code 3) is a well-known mandatory BGP attribute that indicates the next-hop IP address that can be used to reach a destination.
NNTP (Network News Transfer Protocol)	A protocol that provides access to Internet newsgroups. It allows a client to read messages sent to newsgroups and makes it possible for hosts to replicate articles back and forth.
Node	A node is a device that acts as a connection point within a network. Nodes can be used for redistributing or forwarding data or providing services to other devices or programs. Node and host, in the network context, are often used interchangeably.
Node prioritization	The priority assigned to each computer (values between 0 and 8) in a token ring. Computers with higher priority levels get first rights to the token. Computers that perform critical network functions may need higher priority.
Nonauthoritative restore	A restoration method which uses the Backup utility to return the Active Directory database to the state it was in before the back up. Windows 2000 automatically performs a consistency check on and re-indexes the Active Directory database. It then updates Active Directory and File

	Replication service (FRS) with data from the server's replication partners.
Nonbackbone area	A regular area (also known as nonbackbone area)does not allow traffic to pass through it. The regular area's primary function is to connect users and resources.
NonBroadcast MultiAccess (NBMA)	An NonBroadcast MultiAccess (NBMA) network is a network that interconnects multiple routers but does not have broadcast capabilities (examples are Frame Relay, X.25, and ATM).
Non-local GPO	A Group Policy Object (GPO) stored in Active Directory. Settings in a non-local GPO can be applied to users and computers throughout the network. Also called an Active Directory-based (GPO).
Non-paged pool system memory	The part of operating system memory that remains in physical memory instead of being swapped into virtual memory.
Non-preemptive multitasking	A system in which each application currently running a process voluntarily passes control of the CPU to another application between processes. Also called cooperative multitasking.
Nontransit AS peering	Nontransit AS peering provides access to a single EBGP peer; excluding all other EBGP peers. This is optimal for scenarios in which a customer is connected to two ISP's networks and wishes to have each ISP's customers use their own connections for communication.
Normal backup	A backup method that backs up selected files and folders, and marks their archive attributes.
Not So Stubby Area (NSSA)	A Not So Stubby Area (NSSA) is similar to a stub area because it does not allow external ASBR routes, but it does allow ASBR routes that originate from within the area. These ASBR routes are flagged as Type 7 LSA packets (NSSA type LSA packets).
Notification messages	Notification messages are transmitted when errors have been detected.
NS (Name Service) record	A name service record that is placed in a DNS server.
NSAP (Network Service Access Point)	A Network Service Access Point (NSAP) is used to identify routers and build the topology table in IS-IS.
NSLOOKUP	A Microsoft utility used to diagnose problems with DNS. Users can interact with the DNS server, and this utility can be used to display resource records on DNS servers, including UNIX DNS servers.
NSSA (Not So Stubby Area)	A Not So Stubby Area (NSSA) is similar to a stub area because it does not allow external ASBR routes, but it does allow ASBR routes that originate from within the area. These ASBR routes are flagged as Type 7 LSA packets (NSSA type LSA packets).
NT Hardware Qualifier (NTHQ)	A Windows NT utility which checks the hardware installed on an Intel x86 computer before you begin installing Windows NT. This helps you prevent problems during installation.

NT Virtual DOS Machine (NTVDM)	A specialized environment that allows MS-DOS and Win16 applications to run under Windows NT.
Ntdetect.com	This program has the responsibility to pass hardware configuration information to the NTLDR program.
Ntdos.sys	The NTVDM equivalent of the MSDOS.SYS in MS-DOS.
NTDS Performance Object	An object in System Monitor which represents Directory Services and can be monitored to observe the performance of Active Directory.
NTFS (New Technology File System)	A Windows NT file system that provides secure and robust file access. File and folder names can be up to 255 characters (long file names). Permissions can be assigned to individual files and folders. Windows 2000 updates NTFS with new features.
NTFS partition	A partition formatted with the NTFS file system.
NTHQ (NT Hardware Qualifier)	A Windows NT utility which checks the hardware installed on an Intel x86 computer before you begin installing Windows NT. This helps you prevent problems during installation.
Ntio.sys	The NTVDM equivalent to the IO.SYS in MS-DOS.
Ntldr	The Windows NT operating system loader. During the startup phase, the pre-boot sequence locates the boot partition of the hard disk. NTLDR (the boot loader) is then loaded and initialized from the boot sector. This program switches the processor to the 32-bit flat memory mode, starts the appropriate minifile system, and reads the Boot.ini file.
NTP (Network Time Protocol)	NTP is used to communicate time synchronization information between systems on a network.
NTVDM (NT Virtual DOS Machine)	A specialized environment that allows MS-DOS and Win16 applications to run under Windows NT.
Ntvdm.exe	The executable that emulates MS-DOS and manages an NTVDM. It runs in kernel mode.
NWLink	The Microsoft implementation of Novell's IPX/SPX protocol. It is a communications protocol that helps Windows 2000 and NetWare operate in a single environment. Client Services for NetWare is also needed to complete the connection.

O

Object	A discrete piece of information, such as a graphic, chart, or paragraph of text, that you can create in one application and link or embed into a file created in another application.
Object Linking and Embedding (OLE)	A standard for embedding objects and text in electronic documents.
Octet	A term used to describe 8 bits in an IP address. An IP address consists of a 4 octet address. An octet is separated by periods. The octet represents a decimal number in the range of 0-255 known as dotted decimal notation.

ODR (On-Demand Routing)	On-Demand Routing (ODR) uses the Cisco Discovery Protocol (CDP) to transfer network information between routers. ODR makes it possible to find the following types of characteristics about neighboring devices: • Device type • IP address • Cisco IOS version being run • Network capabilities
OEM (Original Equipment Manufacturer)	A company that uses parts of other company's products to create its own products.
Offline defragmentation	A defragmentation method you perform manually using NTDSUTIL when the computer is not connected to the network. It rearranges the data in the Active Directory database, compresses the file, and creates a compact, new file.
Off-site storage	Backup tapes stored at a location different from the business location.
OLE (Object Linking and Embedding)	A standard for embedding objects and text in electronic documents.
OLE DB	An application programming interface (API) that lets COM applications access data from an OLE DB provider without regard to the data storage format of the provider. For example, the provider could be a database, a spreadsheet, or text files.
Omni-directional Antenna	Wireless networks require antennas for sending and receiving transmitted signals. An omni-directional antenna disperses a radio frequency wave in an equal 360-degree pattern. This type of antenna is used to provide access to many clients in a radius.
On-Demand Routing (ODR)	On-Demand Routing (ODR) uses the Cisco Discovery Protocol (CDP) to transfer network information between routers. ODR makes it possible to find the following types of characteristics about neighboring devices: • Device type • IP address • Cisco IOS version being run • Network capabilities
Online defragmentation	A defragmentation method that the Extensible Storage engine performs automatically at regular intervals, following the garbage collection process. It rearranges the data in the Active Directory database, but does not compress the data or reduce the size of the database file.
On-site storage	Backup tapes stored at the business location.
Open Graphics Language (OpenGL)	The standard software interface you can use on any hardware or software platform to create high-quality graphics.

Open message	The first message sent by each side of an established TCP session is an open message. Open messages exchange information on how to set up a session
Open Shortest Path First (OSPF)	A routing protocol like RIP. This routing protocol periodically exchanges routes to known networks among dynamic routers. If a route changes, other routers are automatically informed of the change. Dynamic routing requires a protocol such as Open Shortest Path First.
Open Systems Interconnection (OSI) model	It includes the Application, Presentation, Session, Transport, Network, Data Link, and Physical layers, which correspond to the model created by the International Standards Organization (ISO).
OpenGL (Open Graphics Language)	The standard software interface you can use on any hardware or software platform to create high-quality graphics.
Origin attribute	The origin (type code 1) is a well-known mandatory BGP attribute used to describe the origination of information in transit.
Original Equipment Manufacturer (OEM)	A company that uses parts of other company's products to create its own products.
Originating domain controller	The domain controller on which an Active Directory update was originally made.
Originating update	An update to the Active Directory update that is made directly rather than through replication. For example, if BSmith's password is changed on Server1 then replicated to Server2, the originating update was made on Server1.
Originating update sequence number	The local USN of the domain controller on which an Active Directory update was originally made.
Oscilloscope	An electronic device that displays signal voltage information. You can use an oscilloscope to detect shorts, breaks, bends, or crimps in a network cable. Oscilloscopes can also indicate attenuation problems (loss of signal power).
OSI (Open Systems Interconnection) model	It includes the Application, Presentation, Session, Transport, Network, Data Link, and Physical layers, which correspond to the model created by the International Standards Organization (ISO).
OSPF (Open Shortest Path First)	A routing protocol like RIP. This routing protocol periodically exchanges routes to known networks among dynamic routers. If a route changes, other routers are automatically informed of the change. Dynamic routing requires a protocol such as Open Shortest Path First.
Outlook Anywhere	Outlook Web Access (OWA) provides browser access to e-mail.
Out-of-band management	Out-of-band management uses communication channels and methods that are different from those used by the server to communicate with normal network clients. With out-of-band management, you separate server management traffic from normal network traffic. You might also use unique tools that allow you to communicate with a server before the operating system loads or if the server is unresponsive to normal network communications.

P

Packet	The term used to describe information that is compartmentalized for transport across the network. For example, the IP protocol has a packet structure that contains the Source IP address, Destination IP Address, Protocol type, Checksum, data, and so on.
Packet filtering firewall	A packet filtering firewall filters packets based on source and destination addresses, ports, and service protocols. This type of firewall uses ACLs or filter rules to control traffic. It operates at OSI layer 3 (Network layer), Offers high performance because it only examines addressing information in the packet header and it is subject to DoS and buffer overflow attacks.
Packet InterNet Groper (PING)	A TCP/IP utility that verifies TCP/IP is configured correctly and that another host is available.
Packet Switching	A packet switched network allows data to be broken up into packets. Packets are transmitted along the most efficient route to the destination. Packet switching is ideal for transmitting data that can handle transmission delays, as is often the case with Web pages and e-mail.
Page	A contiguous, fixed-length block of virtual addresses. It is copied from memory to disk and back during paging operations. Windows 2000 uses 4 KB blocks to map physical and virtual memory addresses. SQL Server allocates database space in 8K pages.
Page Description Languages (PDL)	A program that tells a printer how printed output should appear on a page. PostScript and TrueType are two different PDLs.
Paging file	Pagefile.sys. A file on a hard disk that Windows 2000 uses to transfer information in and out of RAM and virtual memory. Also called a swap file or a virtual memory page file.
PAN (Personal Area Network)	A personal area network is the interconnection of components, such as laptops, personal digital assistants, printers, mice, keyboards, and other Bluetooth equipped devices, using some form of wireless technology within a personal range (typically 10 meters).
PAP (Password Authentication Protocol)	One of the less-secure protocols, where the username and password are sent in clear text for authentication increasing the chance of interception. PAP should be used only when no other form of authentication is supported. PAP protocols are supported by multiple platforms, including Microsoft and Linux.
Partial Mesh	A mesh topology exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. In a partial mesh topology, some redundant paths exist.
Partial replica	A replica that contains only selected attributes of objects on which a searches are likely to be performed. Partial replicas are read-only.
Partition	A portion of the free space on a hard disk that you format with a file system. Partitions can be either primary or extended.

	A partition can also refer to a division (part) of the Active Directory database. In this case, it is called an Active Directory partition or directory partition.
Passive interface	Passive interfaces stop the routing process from participating out of a particular interface. The interface still listens and receives network traffic, but the interface does not participate, advertise, or generate any traffic for a given protocol. Passive interfaces are often used with protocol migration or redistribution.
Pass-through authentication	The process by which users log on to the network from computers or domains in which they have no account. Pass-through authentication allows a user with an account on one domain to access the entire network. Pass-through authentication can occur when a user logs on to a trusted domain or connects to a resource in a trusting domain.
Password	A credential used to verify a user's request to log on to the network. A password is associated with a user account name and both are used during the authentication process.
Password Authentication Protocol (PAP)	One of the less-secure protocols, where the username and password are sent in clear text for authentication increasing the chance of interception. PAP should be used only when no other form of authentication is supported. PAP protocols are supported by multiple platforms, including Microsoft and Linux.
PCI (Peripheral Component Interconnect)	A 32 or 64-bit bus providing compatibility with both 486 and Pentium machines. PCI buses: • Have a maximum throughput rate of 133 MB/s. • Are processor independent (the CPU and the PCI bus can process concurrently). • Use a divisor to synchronize the system bus speed and the PCI bus speed. • Are most commonly 5V, but specifications provide for 3V and dual-voltage cards. • Can support ISA and EISA; however if PCI and ISA share a bus, then the use of one disables the other. • Are plug-and-play. • Are normally white plastic. • Are available in 64-bit as well as 32-bit. 64-bit PCI cards are often backwards compatible with 32-bit PCI slots.
PCIe	PCI Express is the latest expansion bus standard, replacing AGP in newer systems. • PCI Express has a maximum throughput rate of 8 GB/s. • Rather than a shared bus, each PCIe slot links to a switch which prioritizes and routes data through a point-to-point dedicated connection and provides a serial full-duplex method of transmission.

	• Data is transferred in packets, allowing data to be transferred more quickly. • PCI Express is a serial communications channel made up of two differential wire pairs that provide 2.5 GB/s in each direction. Up to 32 of these lanes may be combined in x2, x4, x8, x16 and x32 configurations, creating a parallel interface of independently controlled serial links, providing up to 4GB/s transfer speeds. • The slots are different lengths because of the different lane configurations. • PCI Express offers greatly increased speed and higher quality service. • The bandwidth of the switch backplane determines the total capacity of a PCI Express implementation. • Each device on the bus can create a point-to-point connection with another device. • PCI Express is backwards compatible and allows legacy PCI technology to be run in the same system. • Originally called "Third Generation I/O" (3GIO), PCI Express is software compatible with PCI, but not plug compatible. • PCI Express is most commonly used for video cards in modern computer systems. • PCI Express supports Scalable Link Interface (SLI) video. SLI allows two instances of the same graphics card to be linked together to provide amazing graphic performance.
PCI-X	The PCI-X specification is a high-performance enhancement to the conventional PCI bus specification. • PCI-X has a maximum throughput rate of 1.06 GB/s. • PCI-X provides maximum clock frequencies of 266 MHz and 533 MHz increasing transfer rates up to 4.3 GB/s. • PCI-X 1.0 improved the efficiency of the PCI bus itself and the devices attached to it by providing new features such as split transactions and transaction byte counts. • PCI-X 2.0 adds additional features for systems reliability to minimize errors at high speeds and keep up with other advances made to such as RAID, Fiber Channel, and iSCSI architectures. • PCI-X is used primarily in server systems.
PCONSOLE	A GSNW or CSNW utility that allows you to manage NetWare print servers from a Windows 2000 client computer.
PDA (Personal Digital Assistant)	Any portable hand-held device used for computing.
PDC (Primary Domain Controller)	A PDC holds all security and account information for a Windows NT domain and is responsible to communicate all changes to the BDCs.
PDL (Page Description Languages)	A program that tells a printer how printed output should appear on a page. PostScript and TrueType are two different PDLs.

PDM (Protocol-Dependent Modules)	A Protocol-Dependent Module (PDM) is used by EIGRP to carry out the requirements specific to independent protocols. PDMs: • Operate completely independent of one another. • Learn from other sources to make decisions about adding routes. • Offer support for various routed protocols (e.g. IP, IPX, and AppleTalk). • Carry information from the routing table to the topology table.
PEAP (Protected Extensible Authentication Protocol)	PEAP (an extension of EAP) is one of the most effective wireless security solutions. PEAP provides authentication, including passwords. PEAP, provides the following two options: • PEAP-EAP-TLS. This method uses certificates (either on the local system or on a smart card). • PEAP-MS-CHAP v2. This method uses certificates on the server, but passwords on the client. Use this method when the client does not have a certificate.
Peer-to-peer network	A network in which every computer on the network is equal in providing and requesting resources. These networks have no central administration and only share-level security.
Per seat licensing	A licensing mode that requires you to buy a license for every client computer that will connect to resources on the server running Windows 2000.
Per server licensing	A licensing mode that requires you to buy a license for each server that will be running Windows 2000.
Peripheral Component Interconnect (PCI)	A 32 or 64-bit bus providing compatibility with both 486 and Pentium machines. PCI buses: • Have a maximum throughput rate of 133 MB/s. • Are processor independent (the CPU and the PCI bus can process concurrently). • Use a divisor to synchronize the system bus speed and the PCI bus speed. • Are most commonly 5V, but specifications provide for 3V and dual-voltage cards. • Can support ISA and EISA; however if PCI and ISA share a bus, then the use of one disables the other. • Are plug-and-play. • Are normally white plastic. • Are available in 64-bit as well as 32-bit. 64-bit PCI cards are often backwards compatible with 32-bit PCI slots.

PERL (Practical Extraction and Report Language)	An interpreted script language that includes UNIX facilities with C. It is faster and easier to code than other languages, but works best for small, limited applications.
Permanent Virtual Circuit (PVC)	A virtual circuit that provides permanent access to the network like a permanent physical connection. Leasing a PVC is cheaper than leasing a permanent physical connection because the physical circuit is not dedicated to a single PVC and can be used to carry data from other virtual circuits.
Permissions	The rights granted to a user or group to access files and folders on a Windows 2000 computer or a network. These permissions may reside in the local computer's security database or in the Active Directory database of a domain controller on the network.
Persistent route	A static route entry or entry in a router that is stored in the registry. Static routes are stored in memory unless you specify through the Bp parameter that the route is persistent. When you restart a Windows 2000 computer, you will need to re-create all non-persistent routes.
Personal Area Network (PAN)	A personal area network is the interconnection of components, such as laptops, personal digital assistants, printers, mice, keyboards, and other Bluetooth equipped devices, using some form of wireless technology within a personal range (typically 10 meters).
Personal Digital Assistant (PDA)	Any portable hand-held device used for computing.
Personal Web Server (PWS)	If you install Microsoft Internet Information Server on a computer running Windows 2000 Professional, it installs as Microsoft Personal Web Server (PWS). PWS is not a full Internet server, but you can use it to publish content on your local LAN, or to remotely administer an IIS server.
Phonebook entry	A list of the settings Dial-Up Networking uses to connect a client to a remote computer. The entry includes information such as the country code, area code, phone number, name of the remote computer, and so on.
Physical Layer	The lowest layer in the seven-layer OSI model that represents the hardware on a network. The physical layer is the adapter card and the physical media that transport protocols across the network.
PIF (Program Information File)	A text file that contains the information Windows needs to run MS-DOS applications, such as the path and filename of the executable file.
Piggyback attack	Entering a secured building immediately behind another employee without authenticating yourself is a piggyback attack.
PIM (Protocol Independent Multicast)	Protocol Independent Multicast (PIM) is a very important multicast routing protocol that tells the router to ignore any Layer 3 protocol when making multicast-routing decisions (e.g. OSPF and EIGRP). PIM: • Uses the routing table that is populated by the unicast routing protocol in its multicast routing calculations. • Does not send routing updates between PIM routers.

PIM Dense Mode (PIM-DM)	PIM Dense Mode (PIM-DM) is a push method controlled by the source to push multicast information. PIM-DM: • Is used when there are many clients requesting the same multicast information. • Builds shortest-path trees by flooding multicast traffic domain wide, then prunes back the branches of the tree where no receivers are present. • Generally has poor scaling properties.
PIM Source Specific Multicast (PIM-SSM)	PIM Source Specific Multicast (PIM-SSM) builds trees that are rooted in just one source. PIM-SSM: • Sources (S) transmit an IP datagram to an SSM destination address (G). • Receivers can receive data by subscribing to channel (S,G).
PIM Sparse Mode (PIM-SM)	PIM Sparse Mode (PIM-SM) is a client-initiated pull method to get multicast information. PIM-SM: • Is used when there are few sources of information. • Uses a shared tree. • Requires an RP to be defined. • Requires multicast sources and receivers to register with their local RP.
PIM-DM (PIM Dense Mode)	PIM Dense Mode (PIM-DM) is a push method controlled by the source to push multicast information. PIM-DM: • Is used when there are many clients requesting the same multicast information. • Builds shortest-path trees by flooding multicast traffic domain wide, then prunes back the branches of the tree where no receivers are present. • Generally has poor scaling properties.
PIM-SM (PIM Sparse Mode)	PIM Sparse Mode (PIM-SM) is a client-initiated pull method to get multicast information. PIM-SM: • Is used when there are few sources of information. • Uses a shared tree. • Requires an RP to be defined. • Requires multicast sources and receivers to register with their local RP.

PIM-SSM (PIM Source Specific Multicast)	PIM Source Specific Multicast (PIM-SSM) builds trees that are rooted in just one source. PIM-SSM: • Sources (S) transmit an IP datagram to an SSM destination address (G). • Receivers can receive data by subscribing to channel (S,G).
PING (Packet Internet Groper)	A TCP/IP utility that verifies TCP/IP is configured correctly and that another host is available.
Plain Old Telephone Service (POTS)	POTS refers to the telephone system. Early on, Internet connectivity was accomplished with a modem converting digital signals into analog for transmission via POTS. Newer, better, and faster methods are quickly replacing POTS as a signal transport medium.
P-node	A peer to peer protocol that uses NetBIOS over TCP/IP. The P-node uses a NetBIOS name server (NBNS) such as WINS to resolve NetBIOS names and does not use broadcasts. It will query the name server directly. All computers using P-node must be configured with the IP address of the NBNS. Computers can communicate as long as the NBNS is working.
Point to Point Protocol (PPP)	A protocol designed as an enhancement to the original SLIP specification. PPP is a data link protocol that provides a standard protocol for sending packets across a point to point network link.
Pointer (PTR) record	A special resource record that is added to DNS to associate the IP addresses and the corresponding host name. Part of the administration of a DNS name server is ensuring that pointer records are created for hosts.
Point-to-Point Protocol over Ethernet (PPPoE)	PPPoE is a variation of Point-to-Point Protocol (PPP) that sends PPP packets over an Ethernet network and an "always on" WAN link (DSL or cable modem, for example) rather than over a dial-up connection. In this way, Internet service providers can install PPP-based remote access servers and require remote clients to establish a connection before being granted access to the Internet. This lets Internet usage be better tracked and regulated. PPP over Ethernet automatically discovers the remote access server using broadcast messages.
Point-to-Point Tunneling Protocol (PPTP)	A protocol that allows a remote user to connect to the network over the Internet so that a company does not have to lease dedicated lines.
Poison message queue	Poison message queues are used to isolate messages that contain potentially harmful errors caused by an Exchange 2007 system failure. This queue is only viewable in the case that such messages have been directed to the poison message queue. Delivery of all messages within the poison message queue is suspended. If a message is deemed unharmful, it will be passed to the submission queue. All other messages within the poison message queue are deleted.
Poison reverse	Using the split horizon with poison reverse method (also called poison reverse or route poisoning), routers continue to send information about routes back to the next hop router, but advertise the path as unreachable.

	If the next hop router notices that the route is still reachable, it ignores the information. If, however, the path timeout has been reached, the route is immediately set to unreachable (16 hops for RIP).
POP3 (Post Office Protocol Version 3)	A mail-drop protocol designed to work with clients that are not always connected to the network. It allows a mail server to receive mail messages and store them on a server until the client comes back on line and requests them.
Port	Network ports are logical connections, provided by the TCP or UDP protocols at the Transport layer, for use by protocols in the upper layers of the OSI model. The TCP/IP protocol stack uses port numbers to determine what protocol incoming traffic should be directed to. Some ICANN specified categories for ports are listed below: • Well Known -- Port numbers range from 0 to 1023 and are assigned for specific protocols and services. • Registered -- Port numbers range from 1024 to 49151 and are specifically assigned, by ICANN, for newly created network services. • Dynamic, Private, or High -- Port numbers range from 49,152 to 65,535 and are assigned when a network service establishes contact and released when the session ends.
POSIX	A standard for versions of UNIX and UNIX-like operating systems. POSIX allows developers to create applications that meet certain US Federal standards.
POST (Power On Self-Test)	The first stage in the Windows NT boot process, during which the system checks to make sure all necessary hardware components and memory are in place and functioning correctly.
Post Office Protocol Version 3 (POP3)	A mail-drop protocol designed to work with clients that are not always connected to the network. It allows a mail server to receive mail messages and store them on a server until the client comes back on line and requests them.
PostScript	A programming language developed by Adobe that determines how a page will look when you print it.
POTS (Plain Old Telephone Service)	POTS refers to the telephone system. Early on, Internet connectivity was accomplished with a modem converting digital signals into analog for transmission via POTS. Newer, better, and faster methods are quickly replacing POTS as a signal transport medium.
Power On Self-Test (POST)	The first stage in the Windows NT boot process, during which the system checks to make sure all necessary hardware components and memory are in place and functioning correctly.
Power Users	Users that can perform user functions on workstations and servers. They can also create user accounts and modify the accounts they have created. Power users can also add user accounts to the built-in groups Users, Guests, and Power Users.

PowerPC	An open-standard microprocessor architecture that uses RISC instead of Intel x86 processors. IBM, Motorola, and Apple worked together to develop the PowerPC.
PPP (Point to Point Protocol)	A protocol designed as an enhancement to the original SLIP specification. PPP is a data link protocol that provides a standard protocol for sending packets across a point to point network link.
PPPoE (Point-to-Point Protocol over Ethernet)	PPPoE is a variation of Point-to-Point Protocol (PPP) that sends PPP packets over an Ethernet network and an "always on" WAN link (DSL or cable modem, for example) rather than over a dial-up connection. In this way, Internet service providers can install PPP-based remote access servers and require remote clients to establish a connection before being granted access to the Internet. This lets Internet usage be better tracked and regulated. PPP over Ethernet automatically discovers the remote access server using broadcast messages.
PPTP (Point-to-Point Tunneling Protocol)	A protocol that allows a remote user to connect to the network over the Internet so that a company does not have to lease dedicated lines.
Practical Extraction and Report Language (PERL)	An interpreted script language that includes UNIX facilities with C. It is faster and easier to code than other languages, but works best for small, limited applications.
Preemptive multitasking	The ability of the Windows 2000 operating system to service multiple requests of the CPU by preempting a task to execute another task.
Preferred bridgehead server	A domain controller that can potentially be chosen as a bridgehead server.
Presentation Layer	Layer 6 of the OSI reference model. This layer ensures that information sent by the application layer of one system will be readable by the application layer of another. The presentation layer is also concerned with the data structures used by programs, and therefore negotiates data transfer syntax for the application layer. Corresponds roughly with the presentation services layer of the SNA model. See also application layer, data link layer, network layer, physical layer, session layer, and transport layer.
Primary Domain Controller (PDC)	A PDC holds all security and account information for a Windows NT domain and is responsible to communicate all changes to the BDCs.
Primary Domain Controller (PDC) Emulator operations master	An operations master that simulates a Windows NT 4.0 Primary Domain Controller (PDC). Also called a PDC Emulator master.
Primary ID	The ID assigned to a specific user for auditing purposes. With the impersonation (or client) ID, this information tells a system administrator who is using which network functions.
Primary partition	The partition of a hard disk that the operating system uses. One basic hard disk can have up to four primary partitions.
Print audit policy	A list of the types of print events you want to record in your auditing logs. Print audit policies should include both file and object access.

Print device	In the Windows 2000 environment, the hardware that produces printed output (what the rest of the world calls a printer). When the term "printer" is used, it refers to the software interface between the operating system and the print device. The print devices are connected to print servers or client computers that have the correct printing software installed on it.
Print driver	A piece of software that translates the graphics commands in documents into a language the print device can understand.
Print forms	A description of and location for a specific size of paper in a particular tray in the print device.
Print monitor	A component of the print spooler that controls access to and monitors the status of a specific print device.
Print Operators	A special group of users that have been given the necessary rights to manage a printer or printers.
Print permissions	Specific printing-related rights you assign to users. There are four levels of printer permissions that can be assigned, including Print, Manage Documents, and Manage Printers.
Print processor	A component of the print spooler that works in conjunction with a print driver to despool the spooled print jobs. Despooling is the process of reading the contents from a spool file and converting the print data into a format the print device can understand.
Print queue	In the Windows 2000 environment, a list of print jobs waiting to be processed by the printer and printed by the print device. This terminology is a little different from other operating systems such as NetWare. In NetWare, the print queue is a directory on a server that holds print jobs waiting to be printed and has configurable properties and settings.
Print router	A component of the print spooler that receives print jobs from the remote print provider and routes them to the appropriate print processor.
Print services	Software components that reside on the print server. They receive print jobs from clients and send them on to the spooler.
Print spooler	A collection of DLLs that receive, process, schedule, and distribute print jobs. Every print job goes through the print spooler.
Printer	In the Windows 2000 environment, the "printer" is the software interface between the operating system and the print device. The printer determines how a print job travels to the print devices. A single printer can send print jobs to multiple print devices. Multiple printers can send jobs to a single print device.
Printer port	An I/O port through which the printer and computer communicate.
Printing pool	A technique that helps you use the available resources more efficiently in a high traffic printing environment. In a printing pool, the print server directs new print jobs to the print device with the lightest load.

Private key	The private (secret) member of a cryptographic key pair associated with a public key algorithm. The private key can be used to decrypt data that has been encrypted using the public key.
Private Management Domain (PRMD)	A PRMD is a private company that controls an X.400 management domain. These domains are the backbone for transferring electronic messages. PRMDs handle internal messages and communicate with each other through ADMDs.
Private Network	A LAN or WAN for private individual or group use which may or may not be secure. Examples include home and organization (small business, corporate, institute, government) networks. *Intranets* and *extranets*, although related to the Internet, are private networks. Both an extranet and intranet are tightly controlled, and made available only to select organizations. An extranet is made available to the public and an intranet is made available internally.
PRMD (Private Management Domain)	A PRMD is a private company that controls an X.400 management domain. These domains are the backbone for transferring electronic messages. PRMDs handle internal messages and communicate with each other through ADMDs.
Process isolation	Lets you run each application separately. This means that if one application fails, it can't affect the other applications running on your server.
Processor	The logic circuitry that responds to instructions and runs the computer. Also called a CPU (central processing unit).
Processor queue length	How long the processor queue is. A counter measures how many threads are requesting processor time at once.
Program Information File (PIF)	A text file that contains the information Windows needs to run MS-DOS applications, such as the path and filename of the executable file.
Promiscuous mode	The ability for an adapter card to view packets travelling across the network. A LAN adapter must support promiscuous mode if it is used to monitor network traffic.
Promote	The process of changing a Windows 2000 member server into a domain controller. The process transfers an up-to-date copy of the Active Directory database from a current domain controller to the new domain controller.
Protected Extensible Authentication Protocol (PEAP)	PEAP (an extension of EAP) is one of the most effective wireless security solutions. PEAP provides authentication, including passwords. PEAP, provides the following two options: • PEAP-EAP-TLS. This method uses certificates (either on the local system or on a smart card). • PEAP-MS-CHAP v2. This method uses certificates on the server, but passwords on the client. Use this method when the client does not have a certificate.

Protocol	Conventions or rules for sending data across a network. These conventions may deal with content, format, timing, sequencing, and error control.
Protocol Independent Multicast (PIM)	Protocol Independent Multicast (PIM) is a very important multicast routing protocol that tells the router to ignore any Layer 3 protocol when making multicast-routing decisions (e.g. OSPF and EIGRP). PIM: • Uses the routing table that is populated by the unicast routing protocol in its multicast routing calculations. • Does not send routing updates between PIM routers.
Protocol stacks	Protocol stacks are installed and configured versions of protocols that connectors use to communicate. For example, the X.400 Connector uses TCP/IP, TP4/CLNP, and/or X.25.
Protocol-Dependent Modules (PDM)	A Protocol-Dependent Module (PDM) is used by EIGRP to carry out the requirements specific to independent protocols. PDMs: • Operate completely independent of one another. • Learn from other sources to make decisions about adding routes. • Offer support for various routed protocols (e.g. IP, IPX, and AppleTalk). • Carry information from the routing table to the topology table.
Proxy	A computer on the network that keeps a cache of resolved names and responds to queries for names outside the local subnet.
Proxy server	A computer on the network that keeps a cache of resolved names and responds to queries for names outside the local subnet.
PSTN (Public Switched Telephone Network)	The network you use when you make a typical telephone call. It is a worldwide, circuit-switched, analog network. Computers connect to the PSTN through a modem. The PSTN can be used on an on-demand (dial-up) basis or a circuit can be leased permanently as a dedicated line.
PTR (Pointer) record	A special resource record that is added to DNS to associate the IP addresses and the corresponding host name. Part of the administration of a DNS name server is ensuring that pointer records are created for hosts.
Public folder	Public folders provide a simple and efficient way to collect, organize, and share Exchange 2007 collaborative applications such as calendars, contact lists, task lists, and message lists.
Public key	The public (non-secret) member of a cryptographic key pair associated with public key algorithm. When the public key is used to encrypt data, the corresponding private key is necessary to decrypt it.
Public key infrastructure	Also called PKI. The policies and software relating to digital certificates and public and private keys. It includes digital certificates and

	certification authorities the guarantee the identity the parties involved in an electronic transaction.
Public Network	A large collection of unrelated computers, with each node on the network having a unique address. The Internet, for example, is a public network. Because computers are unrelated and many companies and individuals share the same communication media, the public network is by nature insecure.
Public Switched Telephone Network (PSTN)	The network you use when you make a typical telephone call. It is a worldwide, circuit-switched, analog network. Computers connect to the PSTN through a modem. The PSTN can be used on an on-demand (dial-up) basis or a circuit can be leased permanently as a dedicated line.
Pull feed	In a pull feed, a computer connects to a host at scheduled times and requests any new information.
Pull partners	A WINS server that pulls (requests) WINS database entries from its push partners. The pull partner pulls new WINS database entries by requesting entries with a higher version number than the last entry it received during the last replication from that push partner.
Punch-down block	A punch-down block is typically used in telephone wiring cabinets to connect individual strands of twisted pair wires. For example, the punch-down block connects the outside phone lines to inside extensions or phone plugs at the demark (where the local network ends and the telephone company's network begins). You use a punch-down tool to attach wires to the punch down block.
Push feed	In a push feed, the computer containing replicated information connects to its partners at specified intervals and uploads new information.
PVC (Permanent Virtual Circuit)	A virtual circuit that provides permanent access to the network like a permanent physical connection. Leasing a PVC is cheaper than leasing a permanent physical connection because the physical circuit is not dedicated to a single PVC and can be used to carry data from other virtual circuits.
PWS (Personal Web Server)	If you install Microsoft Internet Information Server on a computer running Windows 2000 Professional, it installs as Microsoft Personal Web Server (PWS). PWS is not a full Internet server, but you can use it to publish content on your local LAN, or to remotely administer an IIS server.

R

RADIUS (Remote Authentication Dial-in User Service)	RADIUS (Remote Authentication Dial-In User Service) is primarily used for pre-authenticating remote clients before access to the network is granted. RADIUS maintains client profiles in a centralized database. It offloads the authentication burden for dial-in users from the normal authentication of local network clients. For environments with a large number of dial-in clients, RADIUS provides improved security, easier administration, improved logging, and less-performance impact on LAN security systems.

	The primary benefit of RADIUS (Remote Authentication Dial-In User Service) can be summarized as *centralized*. RADIUS is a centralized database of user access profiles. User access profiles determine the rules and restrictions dial-in users must comply with to establish a dial-up link to the network. Only after satisfying the criteria enforced by RADIUS is a remote client granted access to the network.
RAID (Redundant Array of Inexpensive Disks)	A method of categorizing the use of multiple disks to provide performance enhancement and/or fault tolerance.
RARP (Reverse Address Resolution Protocol)	With a given host name, the RARP request will discover the IP address on a network.
RAS (Remote Access Service)	A Windows NT service that you install on one of your network's servers to allow clients to access your network remotely. The RAS software can manage up to 256 simultaneous remote connections.
RCONSOLE	A GSNW or CSNW utility that allows you to view and perform console functions on a remote NetWare system console.
RDISK	A Windows utility that you can use to restore the hard disk configuration and to update a Emergency Repair Disk.
Reciprocal replication	The process of a domain controller pulling updates from its replication partner as well as pushing updates to its replication partner. In comparison, each replication partner typically pulls updates from its partner.
Recomputation	Recomputation is the process of a router comparing routes in search for a new successor route. Recomputation occurs when a successor route to a destination goes down and there are no feasible successors for the destination.
Record	An entry in a DNS name server is known as a record. In SQL Server, a record is a set of related fields (columns) of data joined as a unit. In a SQL database, it is more common to talk about rows and columns than records and fields.
Recursive query	In a recursive query, a name server uses its own resources to resolve the request. A client sends a name resolution request to a server. If it has the information, it sends the results back to the client. If it does not have the information, it passes the request to another server. A server can answer a recursive request with either the requested information or an error message. It cannot refer the client to another server.
Redirector	A file system driver that receives I/O requests for network resources and send the requests into the network. For example, a redirector redirects print jobs away from the client computer's printer port and out to the network.
Reduced Instruction Set Computing (RISC)	A RISC computer has a microprocessor that performs a small subset of instructions. This lets it process data more quickly.

Redundancy	Redundancy is the implementation of one or more backup components that perform duplicate functions. Redundancy: • Improves system performance. • Allows a system to keep functioning normally in the event of a component failure. • Increases fault tolerance.
Redundant Array of Inexpensive Disks (RAID)	A method of categorizing the use of multiple disks to provide performance enhancement and/or fault tolerance.
REG_	Prefix for Registry data types REG_BINARY, REG_DWORD, REG_EXPAND_SZ, REG_MULTI_SZ, AND REG_SZ.
Registry	A unified database in which Windows 2000 stores all hardware and software configuration information for the local computers.
Registry Editor	A Windows utility you can use to display, troubleshoot, and manually edit the contents of the registry.
Regular area	A regular area (also known as nonbackbone area)does not allow traffic to pass through it. The regular area's primary function is to connect users and resources.
Rehoming	Rehoming is the process of moving a public folder from one server to another.
Relational database	A collection of units of data stored in tables that represent a group of objects (for example, Empoyees, Products, or Customers). Columns in a table represent an attribute of the object (for example, an attribute of an Employee might be LastName, or an attribute of a Product might be shipping weight). Each row in a table represents a single instance of that kind of object (for example, the employee name Jane Smith or the part number 3Y557). Data from one table can be used to find related data in another.
Relational database management system (RDBMS)	Software used to store, update, and retrieve data. It has a client/server architecture, stores data in tables with rows (records) and columns (fields), defines and enforces relationships among data items, and uses some version of Structured Query Language (SQL).
Relay domain	A relay domain is a domain for which a server accepts mail but is not authoritative.
Reliable Transport Protocol (RTP)	Reliable Transport Protocol (RTP) is used by EIGRP to deliver packets to neighboring routers in a guaranteed, ordered manner. RTP: • Supports intermixed transmission of unicast or multicast packets. • Only reliably sends certain EIGRP packets. • Sends hello packets that contain an indicator as to whether or not the packet needs to be acknowledged by the recipient.

	• Ensures low convergence time by sending packets even when unacknowledged packets are pending.
Remote access	In a broad sense, remote access is access to a local area network from home or some other place that is not directly connected to the LAN. More specifically, remote access is remote networking for mobile workers or system administrators who manage servers at multiple location. Windows 2000 and Network and Dial-up Connections let users access networks remotely for such services as file and printer sharing, electronic mail, and database access. Remote access is part of the integrated Routing and Remote Access service.
Remote Access Admin	An Windows NT utility used to configure a RAS server. This utility can also be used to start a RAS server.
Remote Access Service (RAS)	A Windows NT service that you install on one of your network's servers to allow clients to access your network remotely. The RAS software can manage up to 256 simultaneous remote connections.
Remote Authentication Dial-in User Service (RADIUS)	RADIUS (Remote Authentication Dial-In User Service) is primarily used for pre-authenticating remote clients before access to the network is granted. RADIUS maintains client profiles in a centralized database. It offloads the authentication burden for dial-in users from the normal authentication of local network clients. For environments with a large number of dial-in clients, RADIUS provides improved security, easier administration, improved logging, and less-performance impact on LAN security systems. The primary benefit of RADIUS (Remote Authentication Dial-In User Service) can be summarized as *centralized*. RADIUS is a centralized database of user access profiles. User access profiles determine the rules and restrictions dial-in users must comply with to establish a dial-up link to the network. Only after satisfying the criteria enforced by RADIUS is a remote client granted access to the network.
Remote delivery queue	Remote delivery queues hold messages that will be delivered using SMTP to recipient mailboxes that reside on remote servers in Exchange 2007. Each remote delivery queue holds messages that are routed to recipients with the same delivery destination. Each time multiple recipients have the same delivery destination, a remote delivery queue is dynamically created. Once the messages have been successfully delivered, the queue expires and is automatically deleted three minutes later.
Remote Execution (REXEC)	A Windows utility that lets you run a process on a remote computer.
Remote network backup	A backup method that uses a tape drive installed on a single server or workstation to back up data other servers and computers connected to the network. This method backs up the registry on the computer attached to the tape drive, but not the registries of the other computers.
Remote Procedure Call (RPC)	Remote Procedure Calls are based on a client/server model in which one server runs processes on another server. Both servers assume the calls

	are local, when in reality they run over LAN connections and through software libraries on both servers.
Remote Shell (RSH)	A Windows NT utility that lets you run commands on a UNIX host.
Rendezvous Point (RP)	A Rendezvous Point (RP) is a temporary connection between a multicast receiver and an existing shared multicast tree. When a volume of traffic crosses a threshold, the receiver is joined to a source-specific tree, and the feed through the RP is dropped.
Repadmin.exe	A command-line Windows 2000 support tool that lets you perform replication-related tasks.
Repeater	A device that reamplifies packets sent on a network. A repeater provides additional distance on a network by reamplifying packets and sending them on.
Replica	A copy of the data in a directory partition or shared folder.
Replicated update	An update to the Active Directory update that is made through replication. For example, if BSmith's password is changed on Server1 then replicated to Server2, the replicated update was made on Server1.
Replication	A process by which a collection data is copied to one or more computers in order to create synchronized sets of data. Changes to Active Directory, for example, are regularly replicated to all domain controllers in a forest.
Replication latency	The time period between when a change is made to a server's directory and when that change appears on other servers in the same site. It is usually 5 minutes.
Replication Monitor	Replmon.exe. A graphical Windows 2000 support tool that lets you monitor the replication process and perform replication-related tasks.
Replication partner	One of two domain controllers that exchange updated information.
Replication topology	The series of connections over which replication takes place.
Replicator	A local group used by the Directory Replicator service. This group is not used for administration.
Request for Comment (RFC)	A series of documents regarding TCP/IP standards. RFCs describe the internal workings and processes of the Internet. TCP/IP standards, however, are developed by consensus. Member of the Internet Society can submit a document to be published as an RFC. After submittal, the document is reviewed for technical accuracy and assigned a classification. There are five classifications of RFCs, including Required, Recommended, Elective, Limited Use, Not Recommended. If a document is being considered as a standard, it goes through stages known as maturity levels. These levels include proposed standard, draft standard, and Internet standard.
Reservation	A specific IP address permanently set aside for use by a specific DHCP client. Addresses are reserved in the DHCP database by using DHCP Manager. Each reserved address is associated with a unique client device identifier.

Resolver	A client computer running DNS that queries a DNS server on the network for name resolution.
Resource	Any network service, such as file and print are resources. Microsoft provides many resource types, including DHCP server, file shares, print spooler, and so on.
Resource mailboxes	Resource mailboxes are used to manage meeting rooms, projectors, and additional facilities in Exchange 2007. When a resource mailbox is created, a disabled user account is created for the mailbox. Rights are then designated to a user who will manage the resource mailbox, or rules are created for the mailbox so it can manage itself.
Resource records	A DNS record that is to be placed in the name service. Using the DNS Manager, you can configure new host records and new resource records.
Retransmit Time-Out (RTO)	Retransmit Time-Out (RTO) is the amount of time in milliseconds that a router will wait for an acknowledgement before sending a reliable packet to a neighbor from the retransmission queue.
Reverse Address Resolution Protocol (RARP)	With a given host name, the RARP request will discover the IP address on a network.
Reverse lookup	A lookup capability provided by DNS that allows a resolver to provide an IP address and request a matching host name. Some applications provide the ability to implement security based on connecting host names. When a request is made to access a particular application, the application can contact the DNS server and do a reverse lookup on the client's IP address. If the host name returned by the DNS server is not in the access list for the NFS volume, or if the host name was not found in DNS, then the request would be denied.
Reverse Path Forwarding (RPF)	Reverse Path Forwarding (RPF) routes traffic away from the source rather than to the receiver.
REXEC (Remote Execution)	A Windows utility that lets you run a process on a remote computer.
RFC (Request for Comment)	A series of documents regarding TCP/IP standards. RFCs describe the internal workings and processes of the Internet. TCP/IP standards, however, are developed by consensus. Member of the Internet Society can submit a document to be published as an RFC. After submittal, the document is reviewed for technical accuracy and assigned a classification. There are five classifications of RFCs, including Required, Recommended, Elective, Limited Use, Not Recommended. If a document is being considered as a standard, it goes through stages known as maturity levels. These levels include proposed standard, draft standard, and Internet standard.
RFC editor	A person who has the responsibility to review an RFC submitted for publication and assign a classification to the document. See RFC for information on classifications and maturity levels for RFCs.
Rights	Rights allow you to carry out specific tasks in Windows 2000. For example, with Backup Operator, you can back up and restore user and system state data on a Windows 2000 computer.

Ring	A ring topology connects neighboring nodes until they form a ring. Signals travel in one direction around the ring. In ring topologies, each device on the network acts as a repeater to send the signal to the next device. With a ring: • Installation requires careful planning to create a continuous ring. • Isolating problems can require going to several physical locations along the ring. • A malfunctioning node or cable break can prevent signals from reaching nodes further along on the ring.
Ring wrapping	A technique for rerouting data on an FDDI ring network to a secondary ring to prevent a break in the network from interrupting network service. Also referred to as dual counter-rotating rings.
RIP (Routing Information Protocol)	A protocol that allows a router to communicate routing information to another router on the network.
RIPX (Routing Information Protocol over IPX)	A protocol that routers use to exchange information between other routers on an IPX network and that hosts use to decide on the best route when forwarding remote IPX traffic.
RISC (Reduced Instruction Set Computing)	A RISC computer has a microprocessor that performs a small subset of instructions. This lets it process data more quickly.
Roaming user profile	A user profile located on the server but downloaded to the local computer when the user logs on. Changes to the profile are saved both locally and on the server when the user logs off. Roaming user profiles are convenient for users that move from location to location and use different computers, but want to keep the same desktop. The profile defines their desktop and will be downloaded to the computer when the user logs in.
Robot	A program that explores links inside and outside a Web site. Also called a spider.
Rogue DHCP Server	A rogue DHCP server is an unauthorized DHCP server on the network.
Root authority	A certification authority that has no higher authority to vouch for it. The root authority is at the top of a certification hierarchy.
Root certificate	A certificate that is digitally signed by the authority that issued it. This occurs when the issuing authority is the root authority and there is no higher authority to verify the certificate.
Root directory	The first-level directory on a hard disk or partition.
ROUTE	A Microsoft utility that views or modifies the local routing table in a TCP/IP network.

Route aggregation	Route aggregation allows the aggregation of specific routes into a single route in BGP. When route aggregation is implemented without any modifiers, granularity is lost because there is no inheritance of the individual route attributes (such as AS_PATH or community).
Route convergence	The process by which routers exchange route information between themselves. Each routing table entry learned through RIP is given a time-out value of three minutes past the last time it was last received in a RIP advertisement.
Route map	A route map is an access list that has the ability to apply logic and make modifications to parameters by using route map statements. Route maps are best used in: • PBR • NAT • BGP • Route filtering during redistribution
Route poisoning	Using the split horizon with poison reverse method (also called poison reverse or route poisoning), routers continue to send information about routes back to the next hop router, but advertise the path as unreachable. If the next hop router notices that the route is still reachable, it ignores the information. If, however, the path timeout has been reached, the route is immediately set to unreachable (16 hops for RIP).
Route redistribution	Route redistribution is the capability of boundary routers connecting different routing domains to exchange and advertise routing information.
Route summarization	Route summarization is the consolidation of multiple routes into a single advertisement.
Router	A device that receives packets, reads their headers to find addressing information, and sends them on to their correct destination on the network or Internet.
Routing Information Protocol (RIP)	A protocol that allows a router to communicate routing information to another router on the network.
Routing Information Protocol over IPX (RIPX)	A protocol that routers use to exchange information between other routers on an IPX network and that hosts use to decide on the best route when forwarding remote IPX traffic.
Routing table	A table that gives network bridges and routers the information needed to forward data packets to locations on other networks. Routing tables must be updated frequently as changes to machines and connections occur. Routing tables include network addresses, the subnet mask, and the gateway addresses. They may also include the subnet broadcast address, network broadcast address, local loopback address, local network address, and the local host address.

RP (Rendezvous Point)	A Rendezvous Point (RP) is a temporary connection between a multicast receiver and an existing shared multicast tree. When a volume of traffic crosses a threshold, the receiver is joined to a source-specific tree, and the feed through the RP is dropped.
RPC (Remote Procedure Call)	Remote Procedure Calls are based on a client/server model in which one server runs processes on another server. Both servers assume the calls are local, when in reality they run over LAN connections and through software libraries on both servers.
RPF (Reverse Path Forwarding)	Reverse Path Forwarding (RPF) routes traffic away from the source rather than to the receiver.
RSH (Remote Shell)	A Windows NT utility that lets you run commands on a UNIX host.
RTO (Retransmit Time-Out)	Retransmit Time-Out (RTO) is the amount of time in milliseconds that a router will wait for an acknowledgement before sending a reliable packet to a neighbor from the retransmission queue.
RTP (Reliable Transport Protocol)	Reliable Transport Protocol (RTP) is used by EIGRP to deliver packets to neighboring routers in a guaranteed, ordered manner. RTP: • Supports intermixed transmission of unicast or multicast packets. • Only reliably sends certain EIGRP packets. • Sends hello packets that contain an indicator as to whether or not the packet needs to be acknowledged by the recipient. • Ensures low convergence time by sending packets even when unacknowledged packets are pending.
Run	A Windows utility that is used to start applications.

S

SAM (Security Accounts Manager)	A database hive in the Registry that includes the directory database for a Windows NT computer.
Samba	Samba is an open source file sharing protocol that provides file and print services. Samba (based on SMB) allows non-Windows servers to communicate with Windows based applications and networks.
SAN (Storage Area Network)	A Storage Area Network (SAN) is an out-of-the-computer storage option for large systems. Instead of storage devices being connected inside of a server (known as Direct Attached Storage (DAS)), storage devices are instead connected to the network and then associated with one or more servers. SANs allow for greater capacity storage than is possible with DAS, and support high data transfer rates and clustering to provide high availability.
Scalability	The capacity of a single computer or an entire network to function well as you add or remove components (hardware or software).

Scatter Mode (Diffuse Mode)	One mode that an infrared device operates in is diffuse mode (also called *scatter mode*), which operates by broadcasting a large beam of light rather than a narrow beam. It does not require line-of-sight connections.
SCC (Single Copy Cluster)	Single Copy Cluster (SCC) uses shared storage in a failover cluster configuration which allows multiple servers to manage a single copy of storage groups. Because nothing in a single copy cluster is shared between the nodes, nodes have access to shared data, but cannot access it at the same time.
Schema	The schema is used to hold the blueprint for Active Directory in Exchange 2007. It defines all of the valid object types and attributes that can be associated with each object type on the Active Directory. If you try to create an object on an Active Directory domain controller that has not been defined within the schema, the domain controller will contact the schema master to make sure it has the latest copy of the schema. If the object is not defined, then the attempt to create the new object will fail.
Schema partition	An Active Directory partition that stores which types objects and attributes can be created in the Active Directory database.
Scope	A Microsoft term for a range of IP addresses that have been configured on a DHCP server awaiting assignment to a host.
Script	A file that lists actions to be executed when the script is run.
SCSI (Small Computer System Interface)	An interface used to connect microcomputers to physical devices (hard disks, scanners, and so on). The American National Standards Institute (ANSI) defines SCSI as a standard high-speed parallel interface.
SDR (Session Description Protocol)	Session Description Protocol (SDR) is an application tool that is commonly used to find multicast traffic by querying directories or listening to announcements. SDR encapsulates the following protocols: • Session Directory Protocol (SDP) • Session Announcement Protocol (SAP)
Sector sparing	A fault-tolerant feature that detects bad sectors of a hard disk, moves data from bad sectors to good sectors, and maps out bad sectors to prevent future use.
Secure File Transfer Protocol (SFTP)	SFTP is a file transfer protocol that uses Secure Shell (SSH) to secure data transfers. SSH ensures that SFTP transmissions use encrypted commands and data which prevent data from being transmitted over the network in clear text.
Secure Hypertext Transfer Protocol (SHTTP)	SHTTP (Secure Hypertext Transfer Protocol) is a proposed standard for security enhanced HTTP. It is used only for Web traffic. SHTTP is an alternative to SSL for Web traffic, but it does not employ SSL. SHTTP should not be confused with HTTPS (Hypertext Transfer Protocol over Secure Socket Layer), which uses a URL of https://.

Secure Shell (SSH)	SSH (Secure Shell) is a secure and acceptable alternative to remote control systems such as Telnet. SSH allows for secure interactive control of remote systems. SSH uses RSA public key cryptography for both connection and authentication. SSH uses the IDEA algorithm for encryption by default, but is able to use Blowfish and DES. SSH is comprised of slogin, ssh, and scp.
Secure Socket Layer over Hypertext Transfer Protocol (SHTTPS)	HTTPS is a secure form of HTTP that uses SSL as a sublayer for security.
Secure Sockets Layer (SSL)	A protocol that provides encryption for communication between the Internet servers and browser clients. It uses public/private key cryptography and digital certificates to verify users' identities.
Security Accounts Manager (SAM)	A database hive in the Registry that includes the directory database for a Windows NT computer.
Security Analysis and Configuration Snap-In	A Microsoft Management Console (MMC) snap-in that lets you compare a computer's current security settings with an existing security template. You can also save security settings as a new security templates.
Security Identifier (SID)	A unique ID used to identify everything in the domain.
Security log	A text file containing records of events you have chosen to audit. For example, if you chose to monitor unsuccessful attempts to log on to your system, you would look at the security log to find the results of that audit.
Security Subsystem	The Windows subsystem that handles the process of logging on to a domain. It works with the Security Accounts Manager to validate the given user name and password, generates an access token, and returns it to the user.
Security template	A group of security-related settings stored in a file. Security templates can be imported into a Group Policy Object (GPO).
Seed metric	The seed metric is the default metric or cost for a redistributed route. • In OSPF, the seed metric is based on the interface's bandwidth. • In IS-IS, the default seed metric is 10. • In EIGRP and IGRP, the default seed metric is based on the interface bandwidth and delay. • In RIP, the seed metric starts with a hop count of 0 and increases from router to router in increments.
Segmentation	Segmentation is a Transport layer process of breaking large packets of information from higher layers into smaller packets called segments. Segmentation is necessary to enable the data to meet network size and format restrictions. The other function of segmentation happens when

	the receiving Transport layer uses packet sequence numbers to reassemble segments into the original message.
Separator page file	A page you can print between each print job sent to a printer. Also called a banner.
Serial Line Internet Protocol (SLIP)	An industry-standard protocol developed in 1984 to support TCP/IP over low-speed serial interfaces. Windows 2000 supports SLIP client functionality, but not server functionality. Also, Windows NT RAS Servers do not accept SLIP client connections.
Serial port	A serial port transmits and receives data one bit at a time. The modem and mouse connect to a computer through a serial port.
Server	A computer that runs a server program (or the server program itself) providing services to users and other computer programs on a network.
Server Management Services (SMS)	A Microsoft management utility that provides management for Windows NT servers.
Server Message Block (SMB)	The file-sharing protocol used on all MS Net products. A workstation communicates with an SMB server process at the remote host.
Server object	An Active Directory object that represents the physical location of a server (usually a domain controller) on a Windows 2000 network.
Server Operators	A built-in local group on domain controllers only. Server Operators share disk resources and can back up and restore the server.
Server-only backup	A backup technique that backs up the data stored on the server. This requires fewer backup devices and storage media, but requires all users to store critical files on the server.
Service	A computing process that performs a specific task in the system. It may also provide a programming interface for other processes.
Service packs	Updates to the Windows 2000 operating system that Microsoft periodically issues. They include bug fixes and other improvements and are available at no cost from the Microsoft web site.
Service provider	The organization that provides a WAN service to an individual or company. A service provider might be the same organization that owns the WAN, or it might be a separate organization that purchases network access from a WAN carrier and then resells network access to the general public.
Service Set Identification (SSID)	A type of wireless security feature used to group several wireless devices and access points as part of the same network and to distinguish these devices from other adjacent wireless networks. The SSID is also commonly referred to as the network name. Most WAPs come with a default SSID, which you should change as part of your security

	implementation. Even after you change the SSID, it is still only a minimal security feature. There are two type of SSIDs: • BSSID (Basic Service Set Identification) is used by an ad-hoc wireless network with no access points. • ESSID (Extended Service Set Identification), or ESS Identifier, is used in an infrastructure wireless network that has access points.
Session	A session refers to a communication between two end points (usually between client and service) that occur during a single connection. The session begins when the connection is established at both ends and terminates when the connection is ended.
Session Description Protocol (SDR)	Session Description Protocol (SDR) is an application tool that is commonly used to find multicast traffic by querying directories or listening to announcements. SDR encapsulates the following protocols: • Session Directory Protocol (SDP) • Session Announcement Protocol (SAP)
Session Layer	Layer 5 of the OSI reference model. This layer establishes, manages, and terminates sessions between applications. It also manages data exchange between presentation layer entities. It corresponds to the data flow control layer of the SNA model. See also application layer, data link layer, network layer, physical layer, presentation layer, and transport layer.
SFTP (Secure File Transfer Protocol)	SFTP is a file transfer protocol that uses Secure Shell (SSH) to secure data transfers. SSH ensures that SFTP transmissions use encrypted commands and data which prevent data from being transmitted over the network in clear text.
Share name	The name of a folder that many users will access on a network. Use intuitive share names so that your users can easily identify resources.
Share permissions	Security to control how users access a shared folder.
Shared folder	A folder that is used by a group of people on the network. Shared folders give access to users of applications, data, and home folders.
Shared printer	A printer that is connected to the network so many users can access it.
Shared-file messaging system	A messaging system based on a server/client relationship in which the client takes the active role in delivering and processing messages. The server is simply a repository of shared files. Microsoft Mail 3.x and Lotus cc:Mail are shared-file messaging systems.
Shielded Twisted Pair (STP)	Twisted pair cables support a wide variety of fast, modern network standards. Twisted pair cabling is composed of two wires that carry the data signals. PVC plastic insulation surrounds each wire. Two wires are

	twisted to reduce the effects of electromagnetic interference and crosstalk. Because the wires are twisted, EMI should affect both wires equally and can be cancelled out. Multiple wire pairs are bundled together in an outer sheath. Twisted pair cable can be classified according to the makeup of the outer sheath. Shielded Twisted Pair (STP) has a grounded outer copper shield around the bundle of twisted pairs or around each pair. This provides added protection against EMI.
Shiva Password Authentication Protocol (SPAP)	The SPAP protocol is a more secure version of PAP. SPAP uses an encrypted password for authentication. Password encryption is easily reversible. SPAP is required to be connected to a Shiva LAN Rover (proprietary).
SHTTP (Secure Hypertext Transfer Protocol)	SHTTP (Secure Hypertext Transfer Protocol) is a proposed standard for security enhanced HTTP. It is used only for Web traffic. SHTTP is an alternative to SSL for Web traffic, but it does not employ SSL. SHTTP should not be confused with HTTPS (Hypertext Transfer Protocol over Secure Socket Layer), which uses a URL of https://.
SHTTPS (Secure Socket Layer over Hypertext Transfer Protocol)	HTTPS is a secure form of HTTP that uses SSL as a sublayer for security.
Shutdown script	A script that executes when a computer shuts down.
SID (Security Identifier)	A unique ID used to identify everything in the domain.
Simple Mail Transfer Protocol (SMTP)	The Internet standard protocol for transferring e-mail messages between hosts. SMTP assumes that both host and client are constantly connected, but you can use both permanent and dial-up connections to an SMTP host.
Simple Network Management Protocol (SNMP)	A simple protocol for managing TCP/IP networks. It is used to report the status of a host on a Windows TCP/IP network. Network equipment vendors developed SNMP to let management software monitor network components. Using SNMP, programs called agents are loaded on to each network component. The agents monitor network traffic and other network components and compile the information in a management information base (MIB). Windows 2000 uses SNMP to check the status of another computer on a TCP/IP network.
Simple Password Authentication Protocol	Simple Password Authentication Protocol is used to authenticate a user to a network access server. Simple password authentication protocol: • Allows a password (key) to be configured per area. Routers in the same area that want to participate in the routing domain will have to be configured with the same key. • Is commonly used by internet service providers. • Is a Point to Point Protocol.

	• Is supported by almost all network operating system remote servers.
Simplex (Duplex)	Simplex and duplex are methods of communication transmission. Simplex is the one-way transmission of a signal across a medium. Duplex is the two-way transmission of a signals across a medium. There are two types of duplex transmission; half-duplex and full-duplex. Half-duplex allows transmission of signals, one party at a time. Full-duplex allows transmission and reception of signals to occur concurrently.
Single Copy Cluster (SCC)	Single Copy Cluster (SCC) uses shared storage in a failover cluster configuration which allows multiple servers to manage a single copy of storage groups. Because nothing in a single copy cluster is shared between the nodes, nodes have access to shared data, but cannot access it at the same time.
Single domain model	A Windows NT domain model in which all users and groups reside in one domain, with a single PDC and one or more BDCs. This model does not use trust relationships because there is only a single domain. Typically used for centralized administration of accounts and resources.
Single master domain model	A Windows NT domain model consisting of at least two domains. Each of the domains has its own domain controller, but all account information is kept on the master domain's controllers. The single master domain model is used when a company has divisions and departments where each entity has its own resource management, but there is still centralized account management.
Single-master replication model	A replication model in which updates can only be made to one domain controller (master). The master then replicates its updates to other domain controllers. Windows NT 4.0 used this replication model.
Site	A TCP/IP subnet or group of well connected subnets. If subnets are well connected the connection is very reliable and fast. Sites make it easier to configure Active Directory access and replication to best utilize the physical network. In Windows 2000, a site is a physical unit that defines replication for Active Directory informatioon. Each site includes one or more servers within an organization. To be in the same site, servers need permanent, high-speed LAN or WAN connections to each other.
Site link bridge object	An Active Directory object that models which site links should be bridged (in other words, over which site links IP packets can be routed).
Site link object	An Active Directory object that represents a non-permanent or low-bandwidth link between multiple sites.
Site object	An Active Directory object that represents a group of permanent, high-bandwidth TCP/IP subnets.

Sliding windows	A sliding window is used to buffer data transmission between two hosts. Each TCP/IP host maintains two sliding windows: one for receiving and the other for transmitting data. The size of the window is the amount of data that can be buffered on a computer.
SLIP (Serial Line Internet Protocol)	An industry-standard protocol developed in 1984 to support TCP/IP over low-speed serial interfaces. Windows 2000 supports SLIP client functionality, but not server functionality. Also, Windows NT RAS Servers do not accept SLIP client connections.
Small Computer System Interface (SCSI)	An interface used to connect microcomputers to physical devices (hard disks, scanners, and so on). The American National Standards Institute (ANSI) defines SCSI as a standard high-speed parallel interface.
SMB (Server Message Block)	The file-sharing protocol used on all MS Net products. A workstation communicates with an SMB server process at the remote host.
Smooth Round Trip Time (SRTT)	The Smooth Round Trip Time (SRTT) is the average time in milliseconds between the transmission of a packet to a neighbor and the receipt of an acknowledgement.
SMP (Symmetric Multiprocessing)	Using multiple processors that share the same operating system and memory to process programs more quickly.
SMS (Server Management Services)	A Microsoft management utility that provides management for Windows NT servers.
SMTP (Simple Mail Transfer Protocol)	The Internet standard protocol for transferring e-mail messages between hosts. SMTP assumes that both host and client are constantly connected, but you can use both permanent and dial-up connections to an SMTP host.
SMTP service domains	A method of organizing e-mail messages. The default domain and local domains include e-mail addresses hosted on the local Microsoft Internet Information Server computer. Remote domains include e-mail addresses hosted on other SMTP computers.
SNA (Systems Network Architecture)	A protocol suite that is a complete networking system, including proprietary hardware. SNA enables communication between IBM mainframes and terminals. It also interfaces with IBM Token Ring local area networks.
Snap-in	A tool used through Microsoft Management Console (MMC). Snap-ins can be stand-alone (can be added to MMC by itself) or extension (can be added to MMC only to extend the function some other snap-in).
SNMP (Simple Network Management Protocol)	A simple protocol for managing TCP/IP networks. It is used to report the status of a host on a Windows TCP/IP network. Network equipment vendors developed SNMP to let management software monitor network components. Using SNMP, programs called agents are loaded on to each network component. The agents monitor network traffic and other network components and compile the information in a management information base (MIB). Windows 2000 uses SNMP to check the status of another computer on a TCP/IP network.

SNMP agent	An SNMP agent performs get, get-next, and set operations requested by a management system. An agent can be any computer running the SNMP agent software, usually a server or router.
SNMP trap	An SNMP agent performs a trap, which is an alert that is sent to management systems for some event that has occurred with that device. This event could be excess traffic, password violations, or a hardware failure.
Snmputil	A utility that verifies whether the SNMP Service has been correctly configured to communicate with SNMP management stations. For example, you can use the utility to determine the number of DHCP Server addresses leased by a DHCP server in the Public Community.
SNPA (Subnetwork Point of Attachment)	A Subnetwork Point of Attachment (SNPA) is a point in a network that provides subnetwork services; comparable to the layer 2 address corresponding to the NET or NSAP address. The SNPA is assigned by using one of the following: • The MAC address on a LAN interface. • The virtual circuit ID from X.25 or ATM connections. • The Data-Link Connection Identifier (DLCI) from Frame Relay connections.
Social engineering	Social engineering is an attack where someone claims to be someone other than who they are. Attackers can assume any role within your organization or of anyone outside of your organization. Their goal is to get you to disclose confidential or sensitive information verbally or to perform some action on the computer system that would grant the attacker access, such as changing a password based on a verbal request over the phone by someone claiming to be an offsite manager. Some common social engineering attacks are: • Dumpster diving -- Going through someone's trash to find private information. • Keyboard surfing -- Observing sensitive information by looking over one's shoulder. • Piggybacking -- Gaining access into a secure facility by slipping in as an authorized visitor enters. • Phishing -- Sending legitimate-looking e-mails designed to trick the recipient into divulging private information (often identity theft related activities). The primary countermeasure to social engineering is awareness. If users are unaware of the necessity for security in your organization and they are not properly trained to support and provide security, they are vulnerable to numerous social engineering exploits. Awareness training focused on preventing social engineering should include methods to authenticate personnel over the phone, assigning classification levels to information and activities, and educating your personnel on what information should not be distributed over the phone.

Sockets	A socket is much like a file handle and functions as an endpoint for network communication. Each application creates a socket by specifying the IP address of the host, the type of service (connection oriented, connectionless), and the port that the application is using.
Software distribution point	A network share that stores software installation programs and/or data and from which software can be installed.
Software modification file	A file with the .MST extension that can be applied to a Windows Installer package (.MSI file) to customize it. Also called a transform file (.MST).
Software package	A Windows Installer package (.MSI file) or ZAP file that is distributed to network users using an Active Directory-based Group Policy Object (GPO).
Source compatible	An application that can run only on the hardware platform for which it was originally compiled.
Source replication partner	A replication partner that sends updates to a target replication partner.
Spanned volume	A volume on a dynamic disk that spans multiple physical drives. Spanned volumes are not fault tolerant and nor can you mirror spanned volume. In Windows NT 4.0, a spanned volume was called a volume set.
SPAP (Shiva Password Authentication Protocol)	The SPAP protocol is a more secure version of PAP. SPAP uses an encrypted password for authentication. Password encryption is easily reversible. SPAP is required to be connected to a Shiva LAN Rover (proprietary).
Spider	A program that explores links inside and outside a Web site. Also called a robot.
Split horizon	Using the split horizon method (also called best information), routers keep track of where the information about a route came from. Routers do not report route information to the routers on that path. In other words, routers do not report information back to the router from which their information originated.
Split horizon with poison reverse	Using the split horizon with poison reverse method (also called poison reverse or route poisoning), routers continue to send information about routes back to the next hop router, but advertise the path as unreachable. If the next hop router notices that the route is still reachable, it ignores the information. If, however, the path timeout has been reached, the route is immediately set to unreachable (16 hops for RIP).
SQL (Structured Query Language)	A query and programming language for databases, widely used with relational database systems. SQL translates what the user sees on the display to commands that the server can understand. IBM originally developed SQL as an English-like query language for entering, editing, and retrieving data in mainframes. There is now an ANSI-standard SQL definition.

SRTT (Smooth Round Trip Time)	The Smooth Round Trip Time (SRTT) is the average time in milliseconds between the transmission of a packet to a neighbor and the receipt of an acknowledgement.
SSH (Secure Shell)	SSH (Secure Shell) is a secure and acceptable alternative to remote control systems such as Telnet. SSH allows for secure interactive control of remote systems. SSH uses RSA public key cryptography for both connection and authentication. SSH uses the IDEA algorithm for encryption by default, but is able to use Blowfish and DES. SSH is comprised of slogin, ssh, and scp.
SSID (Service Set Identification)	A type of wireless security feature used to group several wireless devices and access points as part of the same network and to distinguish these devices from other adjacent wireless networks. The SSID is also commonly referred to as the network name. Most WAPs come with a default SSID, which you should change as part of your security implementation. Even after you change the SSID, it is still only a minimal security feature. There are two type of SSIDs: • BSSID (Basic Service Set Identification) is used by an ad-hoc wireless network with no access points. • ESSID (Extended Service Set Identification), or ESS Identifier, is used in an infrastructure wireless network that has access points.
SSL (Secure Sockets Layer)	A protocol that provides encryption for communication between the Internet servers and browser clients. It uses public/private key cryptography and digital certificates to verify users' identities.
Standard area	A standard area allows any type of route information to enter or leave the area.
Standard primary zone	An authoritative DNS server for a zone that contains a read-write copy of the zone file and can be updated directly. The updated zone information can then be replicated to secondary zones.
Standard secondary zone	An DNS server that contains a read-only copy of the zone file. The zone information is updated by replication from other servers. Its zone file can then be replicated to other secondary zones.
Standby server	A standby server is a Windows 2000 server that you have configured as an emergency backup server. It has Windows 2000 and all necessary components installed, but has not joined a domain.
Star	Star is a network topology that uses a hub (or switch) to concentrate all network connections to a single physical location. Today it is the most popular type of topology for a LAN.
Startup script	A script that executes when a computer starts up.

Static mapping	A router that is configured to communicate only with networks to which it has a configured interface. To route IP packets to other networks, each static router must be configured with either an entry in each router's routing for each network in the internetwork or a default gateway address of another router's local interface.
Static route	A static route is a route that is manually configured to a remote destination. They can be used to reduce overall traffic because they do not require information to be generated. Static routes are most commonly used to: • Define specific routes to use when routing information must be exchanged between two autonomous systems. This eliminates the need for entire routing tables to be exchanged. • Define routes to destinations over a WAN link. This eliminates the need for a dynamic routing protocol.
Static routing	Static routing is an addressing method in which IP configuration information must be built and updated manually on each host by an administrator.
Storage Area Network (SAN)	A Storage Area Network (SAN) is an out-of-the-computer storage option for large systems. Instead of storage devices being connected inside of a server (known as Direct Attached Storage (DAS)), storage devices are instead connected to the network and then associated with one or more servers. SANs allow for greater capacity storage than is possible with DAS, and support high data transfer rates and clustering to provide high availability.
STP (Shielded Twisted Pair)	Twisted pair cables support a wide variety of fast, modern network standards. Twisted pair cabling is composed of two wires that carry the data signals. PVC plastic insulation surrounds each wire. Two wires are twisted to reduce the effects of electromagnetic interference and crosstalk. Because the wires are twisted, EMI should affect both wires equally and can be cancelled out. Multiple wire pairs are bundled together in an outer sheath. Twisted pair cable can be classified according to the makeup of the outer sheath. Shielded Twisted Pair (STP) has a grounded outer copper shield around the bundle of twisted pairs or around each pair. This provides added protection against EMI.
Stripe sets	A method of saving data by writing it in stripes across several different hard disks at once.
Striped volume	A striped volume breaks data into units and stores the units across a series of disks (as opposed to a spanned volume that fills the first area with data, then the second area, and so on). Striped volumes: • Do not provide fault tolerance. A failure of one disk in the set means all data is lost. • Provide an increase in performance.

	• Use two or more disks. • Have no overhead--all disk space is available for storing data.
Striping	Striping is a data protection method. Striping divides data into units and stores the units across a series of disks. Distributing the data removes the threat of losing all of the data in event of a single disk failure.
Structured Query Language (SQL)	A query and programming language for databases, widely used with relational database systems. SQL translates what the user sees on the display to commands that the server can understand. IBM originally developed SQL as an English-like query language for entering, editing, and retrieving data in mainframes. There is now an ANSI-standard SQL definition.
Stub area	A stub area does not allow ASBR routes, so routes that are external to the OSPF routing process are not transmitted.
Stub routing	*Stub routing* is a topology in which the remote router forwards all traffic that is not local to a hub router.
Subkeys	A key inside another key in the Registry. Subkeys can contain more subkeys or values.
Subnet	A physical segment in a TCP/IP environment that uses IP addresses created from a single network ID. The subnet is created by partitioning the bits in the host ID into two parts. The first part is used to identify the segment as a unique network, and the other part is used to identify the hosts. Companies typically used subnetting because they exceeded the maximum number of hosts per segment with their IP address.
Subnet mask	The concept of blocking out a portion of the IP address so that TCP/IP can determine the network ID from the host ID. TCP/IP hosts use the subnet mask to determine whether the destination host is located on a local or remote network. Typically the subnet mask is 255.255.255.0.
Subnet object	An Active Directory object that represents a TCP/IP subnet.
Subnetting	Subnetting is the division of a network address into multiple smaller subnets. For example, this allows a single Class B or Class C addresses to be divided and used by multiple organizations.
Subnetwork Point of Attachment (SNPA)	A Subnetwork Point of Attachment (SNPA) is a point in a network that provides subnetwork services; comparable to the layer 2 address corresponding to the NET or NSAP address. The SNPA is assigned by using one of the following: • The MAC address on a LAN interface. • The virtual circuit ID from X.25 or ATM connections. • The Data-Link Connection Identifier (DLCI) from Frame Relay connections.

Subtree	The folders and subfolders contained inside the export directory you use for directory replication.
Successor route	A successor route is the best route to a destination.
Supernetting	Supernetting, combining multiple network addresses into a single larger subnet. For example, this allows multiple Class C addresses to be combined into a single network.
Superscope	In Windows 2000 Server, a grouping of multiple DHCP scopes into a single unit. A superscope makes it possible to have multiple logical subnets on a single physical subnet. The individual scopes are called member scopes or child scopes.
SVC (Switched Virtual Circuit)	An on-demand virtual circuit that is maintained for the length of a conversation. When the conversation ends, the connection is released.
Switch	A network device that works at the data link layer and allows each device to have higher bandwidth on the network. A switch can offer speeds of 10 to 100 megabits to the desktop.
Switched 56	A system of Digital Data Service (DDS) lines that are on-demand (dial-up) instead of leased and transfer data at a rate of 56 Kbps.
Switched Virtual Circuit (SVC)	An on-demand virtual circuit that is maintained for the length of a conversation. When the conversation ends, the connection is released.
Switches	Codes you can use at the command prompt when starting an application or installation program to customize the way the program runs. Also called command line switches.
Symmetric Multiprocessing (SMP)	Using multiple processors that share the same operating system and memory to process programs more quickly.
Synchronization	The mechanism by which domain controllers share directory changes and ensure that their information is accurate.
SYSCON	A GSNW or CSNW utility that lets you set up user accounts, define policies, and grant user permissions on a NetWare network from a Windows NT computer.
Sysdiff.exe	An executable file you can use during an unattended installation of Windows NT if you need to install an application that does not support scripted installations.
System groups	Built-in groups that organize users for system use. You do not assign users to a system group; these groups are automatically updated by Windows 2000. Users become members of system groups by default or as a result of network activity. The the four main system groups are Everyone, Creator Owner, Network, and Interactive.
System hive	A hive in the Registry which includes information about the devices and services installed on the computer.

System log	A text file containing the events that Windows 2000 components log, such as driver failures. You can use the Event Viewer to display the system log.
System Monitor	A Windows 2000 tool that is used to monitor real-time and historical system performance, trends, bottlenecks, and the effects of system configuration changes.
System partition	The partition on the hard disk containing the boot files and hardware-specific files for the operating system.
System policy	A set of registry settings that controls what users can see and do on their Windows NT computers. System policies are used to control and manage desktop computers. You can use system policies to provide all users or computers with a uniform system policy, or customize settings for specific users, groups, and computers. Windows 2000 computers use Group Policy instead.
System Policy Editor	Poledit.exe. A graphical front-end to the registry included with Windows NT Server that allows you to make registry changes without using the registry editor.
System policy files	The files containing the rules governing how a Windows NT client computer will display the desktop, use Control Panel options, access the network, and so on. Ntconfig.pol is a default system policy file. Windows 2000 computer use Group Policy Objects (GPOs) instead.
System state data	System state data includes all the Windows 2000 system components and distributed services that Active Directory depends on.
Systemroot	The directory in which you installed the Windows 2000 operating system files.
Systems Network Architecture (SNA)	A protocol suite that is a complete networking system, including proprietary hardware. SNA enables communication between IBM mainframes and terminals. It also interfaces with IBM Token Ring local area networks.

T

Tape catalog	A graphical representation of the contents of a backup tape. Windows 2000 automatically creates catalogs during backup and stores them on the tape. The tape catalog shows all the backup sets on a tape.
Tape device	A tape drive which can reads a magnetic storage tape, write data to it, and position it to receive data.
TAPI (Telephony Application Programming Interface)	An API that Windows 2000 communication applications use when they make calls over the telephone line. These calls can include data, fax, and voice.
Target replication partner	A replication partner that receives updates from a source replication partner. Also called a destination replication partner.
T-Carriers	Digital lines that carry data, digitized voice, and digitized video signals. A T-Carrier line multiplexes several channels on to a single physical

	communication medium. Each channel operates at 64 kilobits per second.
TCP (Transmission Control Protocol)	A reliable protocol that divides data into packets, which the IP protocol then sends to other computers on the network.
TCP/IP	TCP/IP is the protocol suite used on the Internet and on most networks. Nearly all computers today use TCP/IP for communication because it is highly scalable and routable.
TDI (Transport Driver Interface)	A Windows NT boundary layer that gives file system drivers a common programming interface so that they do not have to be tied to specific protocols.
TDR (Time-Domain Reflectometer)	A device you can use to examine the breaks and shorts in a network and identify their locations within a few feet. TDRs work by sending a sonar-like pulse down the cable. The pulse looks for shorts or breaks in the cable and reports their location.
Telecommuter	An employee who works outside the office, at home or on the road, and uses a network or the Internet to communicate with the office.
Telephony Application Programming Interface (TAPI)	An API that Windows 2000 communication applications use when they make calls over the telephone line. These calls can include data, fax, and voice.
Telnet	A protocol that emulates a terminal so you can log on to a remote computer. Also called Virtual Terminal Protocol.
Template	A user account template is a standard user account that you create to simplify creating accounts for other users with similar needs.
Terminal	A terminal with no processor. It accepts keystrokes and displays data from a mainframe computer. Also called a dumb terminal.
TFTP (Trivial File Transfer Protocol)	This data transfer utility provides bi-directional file transfers between two TCP/IP hosts, where one is running the TFTP server software. No user authentication is required.
The Microsoft Network (MSN)	An online network sponsored by Microsoft. You can find answers to technical questions, read articles about Microsoft products, chat with other users, and much more.
Thicknet	Thicknet (sometimes called ThickWire) is a term for the larger size of coaxial cable used in Ethernet local area networks.
Thinnet	Thinnet (sometimes called ThinWire) is a term for the smaller size of coaxial cable used in Ethernet local area networks.
Thrashing	Thrashing is excessive paging. It occurs when the computer spends too much time passing pages between physical memory and the paging file on a hard drive. A symptom of thrashing is that the CPU is under-used but the I/O system is working exceptionally hard.

Thread	An object inside a process that runs program instructions. If an operating system allows it, multiple threads can run on different processors at the same time.
Three-way handshake	A process by which a TCP session is initialized. The purpose of the handshake is to synchronize the sending and receiving of segments, and to communicate to the other host the window size and segment size of data it is capable of receiving.
THT (Token Holding Timer)	A timer in which determines how long each station of an FDDI network can keep the token. Each station has a THT.
Thunking	The process by which Win16 on Win32 (WOW) converts calls from 16-bit applications into 32-bit calls for Win32 functions.
Time to Live (TTL)	A name server caches all of the information that it receives during a process known as iterative queries. The amount of time that the data is stored in cache is referred to as Time to Live. The name server administrator of the zone that contains the data determines the TTL for the data. This parameter can be adjusted. The TTL is a maximum hop count.
Time-Domain Reflectometer (TDR)	A device you can use to examine the breaks and shorts in a network and identify their locations within a few feet. TDRs work by sending a sonar-like pulse down the cable. The pulse looks for shorts or breaks in the cable and reports their location.
Token	In computer networking, a token can be either a physical or a virtual object (often used to authenticate users). Security tokens can be in the form of code, PIN number, or devices like smartcards.
Token Holding Timer (THT)	A timer in which determines how long each station of an FDDI network can keep the token. Each station has a THT.
Token passing	Token passing is a mechanism that uses a digital pass card. Only the system holding the token is allowed to communicate.
Token Ring	A network topology in which computers are connected in a closed ring. Tokens passed from one computer to another allow each computer to use the network.
Tombstone	A tombstone marks the fact that someone deleted an object in the directory. When you delete an object in the directory, that item is no longer part of directory replication. Instead, tombstones are replicated to servers to notify them to delete these objects.
Tombstone lifetime	The tombstone lifetime specifies how long a tombstone will exist before the garbage collection process deletes it as well. A tombstone lifetime should be long enough for directory replication to reach every server in your organization.
Tone generator	A tone generator sends an electronic signal on a wire or cable. Use a tone generator to locate the other end of a specific cable. Generate the tone on one end of the cable, then test the other ends of many cables until you detect the tone.

Topology	The physical layout of a network. Topology describes how the network's computers are connected to each other. Common topologies include buses and rings.
Topology table	A topology table is a record of the updates sent between neighboring routers when a new router is discovered.
Totally stubby area	A totally stubby area does not allow ASBR routes or inter-area routes; only routes within its own specific area are allowed.
Traceroute	Traceroute is a Linux diagnostic utility that tests connectivity between devices, but as it does so it shows the path between the two devices. Responses from each hop on the route are measured three times to provide an accurate representation of how long the packet takes to reach, and be returned by that host.
TRACERT	A Microsoft diagnostic utility that verifies the route used from the local host to a remote host.
Transaction	An entire operation consisting of multiple steps that must all be completed properly, or the entire transaction fails.
Transact-SQL	The standard language for communicating between applications and SQL Server. It is an implementation of ANSI-standard Structured Query Language (SQL) that includes extensions such as stored procedures that make Transact-SQL a full programming language. Sometimes referred to as T-SQL.
Transceiver	A transceiver is responsible for transmitting and receiving network communications. To send signals to the network, the transceiver converts digital data from a PC to digital signals. To receive signals, the transceiver converts digital signals from the network to digital data for the PC. Many transceivers are attached to network interface cards.
Transform file	A file with the .MST extension that can be applied to a Windows Installer package (.MSI file) to customize it. Also called a software modification file.
Transit area	A transit area is an area that has more than one way into itself.
Transit AS peering	Transit AS peering is the communication of information between all EBGP peers. This is optimal for scenarios in which an ISP allows their customers using BGP to access all their other customers using BGP.
Transmission Control Protocol (TCP)	A reliable protocol that divides data into packets, which the IP protocol then sends to other computers on the network.
Transmission Media (Media)	In the realm of information technology, transmission media refers to the cables and wires through which signals (such as electric current or light impulse) are transmitted through a network.

Transport Driver Interface (TDI)	A Windows NT boundary layer that gives file system drivers a common programming interface so that they do not have to be tied to specific protocols.
Transport Layer (OSI Model)	Layer 4 of the OSI reference model. This layer is responsible for reliable network communication between end nodes. The transport layer provides mechanisms for the establishment, maintenance, and termination of virtual circuits, transport fault detection and recovery, and information flow control. Corresponds to the transmission control layer of the SNA model. See also application layer, data link layer, network layer, physical layer, presentation layer, and session layer.
Transport policies	Transport policies (also referred to as transport rules) provide an easy, flexible way for administrators to process, filter, store, and modify all e-mail messages within an Exchange organization. Transport rules allow you to: • Apply corporate policies • Apply compliance policies • Apply content restraints • Manage message routing Each transport rule consists of three components: • Conditions identify the e-mail messages to which a transport policy action are applied. • Exceptions identify the e-mail messages which are excluded from a policy, even if the message matches a transport policy condition. • Actions modify some aspect of message content or the delivery for e-mail messages that match all the conditions and none of the exceptions of a transport policy.
Transport policy actions	Transport policies (also referred to as transport rules) provide an easy, flexible way for administrators to process, filter, store, and modify all e-mail messages within an Exchange organization. Transport rules allow you to: • Apply corporate policies • Apply compliance policies • Apply content restraints • Manage message routing Each transport rule consists of three components: • Conditions identify the e-mail messages to which a transport policy action are applied. • Exceptions identify the e-mail messages which are excluded from a policy, even if the message matches a transport policy condition.

	• Actions modify some aspect of message content or the delivery for e-mail messages that match all the conditions and none of the exceptions of a transport policy.
Transport policy agents	Transport policy agents apply transport policies to e-mails within an Exchange organization. There are two types of transport policy agents in Exchange 2007: • A Transport Rules agent runs on a Hub Transport server and implements policies set by administrators to all e-mail that travels in and out of an Exchange organization. • An Edge Rules agent runs on an Edge Transport server and helps control spam and unwanted mail flow within an organization.
Transport policy conditions	Transport policies (also referred to as transport rules) provide an easy, flexible way for administrators to process, filter, store, and modify all e-mail messages within an Exchange organization. Transport rules allow you to: • Apply corporate policies • Apply compliance policies • Apply content restraints • Manage message routing Each transport rule consists of three components: • Conditions identify the e-mail messages to which a transport policy action are applied. • Exceptions identify the e-mail messages which are excluded from a policy, even if the message matches a transport policy condition. • Actions modify some aspect of message content or the delivery for e-mail messages that match all the conditions and none of the exceptions of a transport policy.
Transport policy exceptions	Transport policies (also referred to as transport rules) provide an easy, flexible way for administrators to process, filter, store, and modify all e-mail messages within an Exchange organization. Transport rules allow you to: • Apply corporate policies • Apply compliance policies • Apply content restraints • Manage message routing Each transport rule consists of three components:

	• Conditions identify the e-mail messages to which a transport policy action are applied. • Exceptions identify the e-mail messages which are excluded from a policy, even if the message matches a transport policy condition. • Actions modify some aspect of message content or the delivery for e-mail messages that match all the conditions and none of the exceptions of a transport policy.
Transport protocol	A type of protocol that allows two computers to communicate with each other. For example, TCP/IP and IPX/SPX are both transport protocols.
Transport rules	Transport policies (also referred to as transport rules) provide an easy, flexible way for administrators to process, filter, store, and modify all e-mail messages within an Exchange organization. Transport rules allow you to: • Apply corporate policies • Apply compliance policies • Apply content restraints • Manage message routing Each transport rule consists of three components: • Conditions identify the e-mail messages to which a transport policy action are applied. • Exceptions identify the e-mail messages which are excluded from a policy, even if the message matches a transport policy condition. • Actions modify some aspect of message content or the delivery for e-mail messages that match all the conditions and none of the exceptions of a transport policy.
Transport Rules agent	Transport policy agents apply transport policies to e-mails within an Exchange organization. There are two types of transport policy agents in Exchange 2007: • A Transport Rules agent runs on a Hub Transport server and implements policies set by administrators to all e-mail that travels in and out of an Exchange organization. • An Edge Rules agent runs on an Edge Transport server and helps control spam and unwanted mail flow within an organization.
Triggered update	With the triggered update method (also known as a flash updates), routers that receive updated (changed) information broadcast those changes immediately rather than waiting for the next reporting interval. With this method, routers broadcast their routing tables periodically,

	punctuated by special broadcasts if conditions have changed. This method reduces the convergence time.
Trivial File Transfer Protocol (TFTP)	This data transfer utility provides bi-directional file transfers between two TCP/IP hosts, where one is running the TFTP server software. No user authentication is required.
Trojan horses	Pieces of software code written expressly to cause problems with servers and workstations. A Trojan horse conceals harmful code inside what looks like a harmless data string or program. Once it is inside a computer, however, it damages data or systems. A Trojan horse is a type of computer virus.
Trunk Cable	The central cable connecting all of the nodes, either inserted directly into the trunk, or nodes tapping into the trunk using offshoot cables called drop cables. Commonly used in the physical bus topology.
Trusts	In a one-way trust, accounts in one domain can be given permission to access resources in another domain. In a two-way, trust, permission is given to each domain to access resources in the other domain.
TTL (Time to Live)	A name server caches all of the information that it receives during a process known as iterative queries. The amount of time that the data is stored in cache is referred to as Time to Live. The name server administrator of the zone that contains the data determines the TTL for the data. This parameter can be adjusted. The TTL is a maximum hop count.
Tunnel	A logical connection that carries encapsulated and possibly encrypted data. Encapsulation and encryption make the tunnel a secure and private link for users across a public network such as the internet.
Tunneling	Tunneling is used primarily to support private traffic through a public communication medium. The most widely known form of tunneling is VPN (Virtual Private Networking). A VPN establishes a secured communications tunnel through an insecure network connecting two systems. Tunnels provide secure communications, they usually provide less than optimal throughput due to the additional overhead of encryption and maintaining the communications link. Tunnels are not directly associated with password theft or protection. L2TP, PPTP, and IPSec are all VPN tunnel protocols.

U

UDF (Uniqueness Database File)	A database containing supplementary information for a Windows 2000 answer file. For example, a UDF may contain the unique IDs, user data, and other information that varies for each installation.
UDP (User Datagram Protocol)	The is a connectionless communications service that does not guarantee delivery of packets. Applications using UDP typically deliver small

	amounts of data and the application has the responsibility for reliable delivery.
Unattended installation	A method of installing Windows 2000 using an answer file that automates the installation so you do not have to be physically present at the computer during the installation.
UNC (Universal Naming Convention)	A standardized convention used for describing network servers. UNC names start with two backslashes followed by the server computer name, and then the shared folder name. For example, \\server_name\users\%username%
Unicast	Unicast is a transmission method in which packets are sent from a single host to a single host.
Unicode characters	The set of letters, numbers, and symbols that SQL Server recognizes in the nchar, nvarchar, and ntext data types. It includes characters for most languages. Unicode is related to character sets, but is not the same thing, having some 200 times as many possible values and requiring twice the storage space.
Unified Messaging server	The Unified Messaging server automates and integrates voice, e-mail, and fax communications in a single store within the Exchange environment which is accessible through either telephone or the computer. The Unified Messaging server communicates with an IP-based phone system which directs all voicemails to the Unified Messaging server. All voicemails are converted to windows media audio files which are then sent to the user's Mailbox server and stored as attachments in an e-mail. The Unified Messaging server also supports voice-prompt calendar and planning services.
Uniform Resource Locator (URL)	The address of a World Wide Web page, graphic file, or program file on the Internet. Each resource has an exclusive address (URL) that allows your computer to find and display it. The URL includes the code for the transfer protocol, plus the unique name of the Web server containing the page. For example, http://www.universal.com/widgets uses the Hypertext Transfer Protocol (http://) to connect to a specific server (www.universal.com) and display a specific Web page (/widgets).
Uninterruptible Power Supply (UPS)	A power supply that is typically used on file servers to provide battery backup power in case of a power failure. The UPS provides power to a server until an emergency shutdown of the system can occur.
Uniqueness Database File (UDF)	A database containing supplementary information for a Windows 2000 answer file. For example, a UDF may contain the unique IDs, user data, and other information that varies for each installation.
Universal Naming Convention (UNC)	A standardized convention used for describing network servers. UNC names start with two backslashes followed by the server computer name, and then the shared folder name. For example, \\server_name\users\%username%
Universal Serial Bus (USB)	A Universal Serial Bus (USB) is a type of media (cable and connectors) that interface between computer and external devices (hubs, audio players, joysticks, keyboards, telephones, scanners, and printers). A

	network can be created by linking USB cables between multiple computers.
UNIX	An operating system invented at Bell Labs in 1969. UNIX is a non-proprietary operating system, so there are many independently-produced versions of UNIX, called "flavors."
UNIX LPD print server	A server running the line printer daemon (LPD) service, which allows you to print documents from a remote computer.
Unreachable queue	Unreachable queues hold messages that cannot be routed to their destination due to configuration changes or modified routing paths in Exchange 2007. Each transport server can have only one unreachable queue.
Unshielded Twisted Pair (UTP)	Twisted pair cables support a wide variety of fast, modern network standards. Twisted pair cabling is composed of two wires that carry the data signals. PVC plastic insulation surrounds each wire. Two wires are twisted to reduce the effects of electromagnetic interference and crosstalk. Because the wires are twisted, EMI should affect both wires equally and can be cancelled out. Multiple wire pairs are bundled together in an outer sheath. Twisted pair cable can be classified according to the makeup of the outer sheath. Unshielded Twisted Pair (UTP) does not have a grounded outer copper shield. UTP cables are easier to work with and are less expensive than shielded cables.
Update messages	Update messages notify all routers in a network of any updates that have been made within the network.
Update Sequence Number (USN)	Servers track directory changes using Update Sequence Numbers (USNs). Each server keeps track of the changes it has already received or made. When a server requests changes from another server, they compare USNs. If the numbers are the same, neither server makes any changes. If one server's number is higher than another, the server with the lower number requests the changes corresponding to the higher numbers. In Windows 2000, a USN is a server-specific 64-bit counter that increases each time that domain controller's Active Directory database is updated. See also local update sequence number and originating update sequence number.
UPS (Uninterruptible Power Supply)	A power supply that is typically used on file servers to provide battery backup power in case of a power failure. The UPS provides power to a server until an emergency shutdown of the system can occur.
Up-to-date vector	A server's highest originating USN received from a particular originating domain controller. For example, if Server1 has received originating updates from Server6 corresponding to Server6's local USN value 4653, then Server1's up-to-date vector for Server6 is Server6-4653.
URL (Uniform Resource Locator)	The address of a World Wide Web page, graphic file, or program file on the Internet. Each resource has an exclusive address (URL) that allows your computer to find and display it. The URL includes the code for the

	transfer protocol, plus the unique name of the Web server containing the page. For example, http://www.universal.com/widgets uses the Hypertext Transfer Protocol (http://) to connect to a specific server (www.universal.com) and display a specific Web page (/widgets).
USB (Universal Serial Bus)	A Universal Serial Bus (USB) is a type of media (cable and connectors) that interface between computer and external devices (hubs, audio players, joysticks, keyboards, telephones, scanners, and printers). A network can be created by linking USB cables between multiple computers.
User account	A user name and password that allows a user to log on to a domain or a local computer and gain access to resources.
User Datagram Protocol (UDP)	The is a connectionless communications service that does not guarantee delivery of packets. Applications using UDP typically deliver small amounts of data and the application has the responsibility for reliable delivery.
User Manager for Domains	The Windows NT tool used to manage the security for domains, member servers, and workstations. If the computer is not configured as a domain controller, User Manager is installed. Windows 2000 uses Active Directory Users and Computers instead.
User mode	A mode in which applications run. User mode confines each application to its own address space and does not allow any application to access the computer's hardware directly.
User profile	A file that specifies which Windows 2000 elements are loaded by the system when a user logs on. Included are program items, screen colors, network connections, printer connections, mouse settings, window size, and window position. When a user logs on for the first time from a Windows-based client, the operating system creates a default profile for that user. A user profile can also be customized to restrict what users see in their interface and have available when they log on.
User rights	The rights that a user has been granted to access files, printers, and applications in a Windows environment.
User rights policy	An account policy in Windows NT that manages the assignment of rights to groups and user accounts.
Username	A the name given to a user's account in a Windows environment. Each user account must have a username and password.
Users	A user in a local group is someone who has been given permission to access a network resource such as access to a folder, file, or printer.
USN (Update Sequence Number)	Servers track directory changes using Update Sequence Numbers (USNs). Each server keeps track of the changes it has already received or made. When a server requests changes from another server, they compare USNs. If the numbers are the same, neither server makes any changes. If one server's number is higher than another, the server with

	the lower number requests the changes corresponding to the higher numbers. In Windows 2000, a USN is a server-specific 64-bit counter that increases each time that domain controller's Active Directory database is updated. See also local update sequence number and originating update sequence number.
UTP (Unshielded Twisted Pair)	Twisted pair cables support a wide variety of fast, modern network standards. Twisted pair cabling is composed of two wires that carry the data signals. PVC plastic insulation surrounds each wire. Two wires are twisted to reduce the effects of electromagnetic interference and crosstalk. Because the wires are twisted, EMI should affect both wires equally and can be cancelled out. Multiple wire pairs are bundled together in an outer sheath. Twisted pair cable can be classified according to the makeup of the outer sheath. Unshielded Twisted Pair (UTP) does not have a grounded outer copper shield. UTP cables are easier to work with and are less expensive than shielded cables.
UUENCODE	UUENCODE was the first widely-used format for binary attachments. It is still an alternative to MIME. It comes in several different flavors, due to different implementations, but it characteristically sends attachments as encoded 7-bit text strings.

V

Values	In the Registry, values contain the value name, the type of data the value uses, and the value. Both keys and subkeys can contain values. In Active Directory, properties common to all objects contain values that correspond to a single user, computer, and so on.
VDD (Virtual Device Driver)	Component that an NTVDM uses to intercept the calls an MS-DOS application makes to the computer's hardware and send them to the Win32 system instead. The application behaves as if it interacts directly with the hardware device.
Vector-based routing protocol	A routing protocol that uses a vector of nearest routers to create a routing table.
VGA (Video Graphics Array)	A display system that is the standard for PC computers.
Video Graphics Array (VGA)	A display system that is the standard for PC computers.
Virtual Device Driver (VDD)	Component that an NTVDM uses to intercept the calls an MS-DOS application makes to the computer's hardware and send them to the Win32 system instead. The application behaves as if it interacts directly with the hardware device.
Virtual directory	A feature of Microsoft Internet Information Server that lets you include information from other folders (besides the designated home directory) in your Web, FTP, and other sites without physically copying the material.

Virtual LAN (VLAN)	Use a switch to create virtual LANs (VLANs). The various ports on a switch can be assigned to a specific VLAN to create logically distinct networks on the same physical network topology. VLANs reduce the likelihood of traffic interception because the switch creating the VLANs transmits traffic only over the specific port hosting the intended recipient of a message. Thus, eavesdropping on any given segment will reveal only the traffic occurring on that specific segment rather than from the entire network. VLANs decrease broadcast traffic and allow the connection of geographically separate systems into the same network. VLANs usually reduce collisions. Routers, gateways, and hubs do not support the creation of VLANs.
Virtual link	A virtual link is a link that allows for discontinuous area 0s to be connected. Virtual links also all disconnected areas to be connected to area 0.
Virtual memory	A Windows technique of using hard disk space like RAM. Windows uses a paging file to store information that would otherwise be stored in RAM. Virtual memory allows you to run more applications simultaneously than your system's RAM would normally allow.
Virtual Memory Manager (VMM)	A component of the virtual memory architecture in Windows NT. It intercepts data storage requests from an application, figures out how much space is needed for the data, then gives the data an unused memory address in either virtual or physical memory. With the VMM, an application does not have to keep track of how the physical memory is organized.
Virtual memory page file	Pagefile.sys. A file on a hard disk that Windows uses to transfer information in and out of RAM and virtual memory. Also called a swap file or a paging file.
Virtual private network	Sometimes called a VPN. A VPN is the extension of a private network over a shared or public network such as the Internet. It makes use of encrypted and authenticated links that provide remote access and routed connections between private networks or computers.
Virtual Private Network (VPN)	Sometimes called a VPN. A VPN is the extension of a private network over a shared or public network such as the Internet. It makes use of encrypted and authenticated links that provide remote access and routed connections between private networks or computers.
Virtual server	An independent Web, FTP, or other site hosted on a Microsoft Internet Information Server. You can configure each virtual server independently, as if it were a physically separate server.
Virus	A virus is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found. Viruses are a serious threat to computer systems, especially if they are connected to the Internet. It is

	often a minimal requirement to have an anti-virus scanner installed on every machine of a secured network to protect against viruses. E-mail is the most common means of virus distribution. Often viruses will employ self-contained SMTP servers to facilitate self-replication and distribution over the Internet. Viruses are able to spread quickly and broadly by exploiting the communication infrastructure of Internet e-mail. For this reason, it is important to keep your anti-virus software updated so as to block any possible attempt of viruses to infect your systems or to spread to other systems from your system. Floppy disks, downloaded music files, and commercial software CDs all have the potential to spread viruses, but they are not as common as e-mail.
VLAN (Virtual LAN)	Use a switch to create virtual LANs (VLANs). The various ports on a switch can be assigned to a specific VLAN to create logically distinct networks on the same physical network topology. VLANs reduce the likelihood of traffic interception because the switch creating the VLANs transmits traffic only over the specific port hosting the intended recipient of a message. Thus, eavesdropping on any given segment will reveal only the traffic occurring on that specific segment rather than from the entire network. VLANs decrease broadcast traffic and allow the connection of geographically separate systems into the same network. VLANs usually reduce collisions. Routers, gateways, and hubs do not support the creation of VLANs.
VMM (Virtual Memory Manager)	A component of the virtual memory architecture in Windows NT. It intercepts data storage requests from an application, figures out how much space is needed for the data, then gives the data an unused memory address in either virtual or physical memory. With the VMM, an application does not have to keep track of how the physical memory is organized.
Volume	A partition or several partitions you have formatted to use a file system such as FAT or NTFS.
Volume set	A method of combining areas on different hard drives into a single volume. Data fills each part of the volume before filling the next.
Volume Shadow Copy Service (VSS)	Volume Shadow Copy Service (VSS) is a component of Windows Server 2003 that takes a point-in-time snapshot of files on the disk. By enabling VSS, you can quickly back up and restore files.
VPN (Virtual Private Network)	Sometimes called a VPN. A VPN is the extension of a private network over a shared or public network such as the Internet. It makes use of encrypted and authenticated links that provide remote access and routed connections between private networks or computers.

VSS (Volume Shadow Copy Service)	Volume Shadow Copy Service (VSS) is a component of Windows Server 2003 that takes a point-in-time snapshot of files on the disk. By enabling VSS, you can quickly back up and restore files.

W

WAN (Wide Area Network)	A network whose computers and servers are geographically far apart but still connected.
WAP (Wireless Application Protocol)	WAP (Wireless Application Protocol) access points privacy, integrity, and authentication to wireless client devices and using WTLS (Wireless Transport Layer Security). WTLS is a wireless security services protocol. It protects data between the wireless hub/router/access point and all wireless NICs.
Warm Site	A warm site is a fault tolerant strategy which provides a redundant work location. If a disaster renders a work site unusable, the effected organization may have a warm site in which to relocate. Warm sites have the following characteristics: • This is a facility readily available with power, A/C, and computers, but the applications may not be installed or configured. • Extra communications links and other data elements that commonly take a long time to order and install will be present. • The warm site is considerably cheaper than a hot (fully operational) site. • Lower administrative and maintenance resources consumed.
Weight attribute	The weight is a mandatory, optional (Cisco-proprietary) BGP attribute that allows a preferred path from a router to a specific network to be configured on a local router only.
Well-known discretionary attribute	The well-known discretionary attribute is understood by all BGP implementations, but its presence is not mandatory.
Well-known ports	Also called commonly-used ports. Ports numbers below 256 are defined as commonly used ports. Some of these ports are 21 (FTP), 23 (Telnet), and 53 (Domain Name Service).
WEP (Wired Equivalent Privacy)	WEP (Wired Equivalent Privacy) was designed to provide wireless networks the same type of protection that cables provide on a wired network. WEP requires that authorized users have a valid WEP key to communicate with the access point. Likewise, cables provide this type of protection in that a client can only communicate with a hub or router if they have an active network cable connected to them. On a wireless network that is employing WEP (Wired Equivalent Privacy), only users with the correct WEP key are allowed to

	authenticate through the WAP (Wireless Application Protocol) access points. That's the whole point of WEP, to prevent unauthorized users by employing a wireless session key for access.
Wide Area Network (WAN)	A network whose computers and servers are geographically far apart but still connected.
Windows 95	An operating system that runs on client computers. It is not a networking operating system.
Windows 98	An operating system that runs on client computers. It is not a networking operating system.
Windows Backup	A backup solution for Windows that allows you to transfer files to and from tape. You can either perform backups manually or schedule an unattended backup.
Windows for Workgroups	An operating system that runs on client computers. It is not a networking operating system.
Windows Installer package	A file with the .MSI extension that contains software installation instructions and data for use with the Windows Installer service.
Windows Installer Service	A Windows 2000 service that uses Windows Installer packages (MSI files) to automate software installation and re-installation.
Windows Internet Naming Service (WINS)	A component of Microsoft Windows NT Server that resolves NetBIOS names into IP addresses for computers and resources on the network using a dynamically-updated database.
Windows Media Player	An application that lets you use streaming audio, illustrated audio, and video to download real-time content from the Internet.
Windows NT	An operating system from Microsoft that you can use for both client and server computers. The two types of Windows NT are Windows NT Server and Windows NT Workstation.
Windows NT Diagnostics	A program that provides a graphical interface to view computer hardware and operating system information. It is used to gather information to help troubleshoot hardware and memory problems.
Windows NT Executive	The collective name for the Windows NT subsystems and components that run in kernel mode. These include the Executive Services, Microkernel, and HAL.
Windows NT Server	A file and application server product from Microsoft that allows applications and files to be stored on it. The latest Windows NT server version is 4.0.
Windows NT Workstation	A desktop operating system that can function alone or also be part of a network in a workgroup or Windows NT Server domain environment.
Windows Scripting Host (WSH)	A scripting host that lets you run scripts, batch files, and command files from the command prompt or the Windows desktop.

Windows socket service (Winsock)	Winsock provides a standard application programming interface to transport protocols such as TCP/IP and IPX. Network applications can use this interface to use the services of the TCP/IP protocol stack.
Windows Sockets	An NWLink API that provides an interface for communication between NetWare Loadable Modules (IPX/SPX sockets) and TCP/IP protocols.
Windows Sockets applications	The Windows Sockets service provides a standard application programming interface (API) to different transport protocols such as IPX and TCP/IP. Applications that take advantage of this service are known as Windows Sockets applications.
Windows-on-Windows (WOW)	Win16 on Win32. A 32-bit program inside Windows NT that lets you run Win16 applications. WOW works inside an NTVDM.
Winipcfg	A Microsoft Windows NT utility that is used to verify a TCP/IP configuration. For Windows 2000, use the IPCONFIG utility.
Winnt.exe	The executable you use to install Windows 2000 on a computer that does not have a previous version of Windows 95, 98, or NT installed.
Winnt32.exe	The executable you use to re-install or upgrade Windows 2000 on a computer that already has Windows 95, 98, or NT installed.
WINS (Windows Internet Naming Service)	A component of Microsoft Windows NT Server that resolves NetBIOS names into IP addresses for computers and resources on the network using a dynamically-updated database.
WINS Manager	A Microsoft utility that is used to manage the Microsoft Windows Internet Name Service. With this utility, you can make configuration changes to your WINS server such as disabling logging or configuring static mappings.
Winsock (Windows socket service)	Winsock provides a standard application programming interface to transport protocols such as TCP/IP and IPX. Network applications can use this interface to use the services of the TCP/IP protocol stack.
Wire crimper	A tool used to attach cable connectors to bare wires (by crimping), such as when you are making your own cables.
Wired Equivalent Privacy (WEP)	WEP (Wired Equivalent Privacy) was designed to provide wireless networks the same type of protection that cables provide on a wired network. WEP requires that authorized users have a valid WEP key to communicate with the access point. Likewise, cables provide this type of protection in that a client can only communicate with a hub or router if they have an active network cable connected to them. On a wireless network that is employing WEP (Wired Equivalent Privacy), only users with the correct WEP key are allowed to authenticate through the WAP (Wireless Application Protocol) access points. That's the whole point of WEP, to prevent unauthorized users by employing a wireless session key for access.
Wireless	Wireless networking uses radio waves or infrared light (with the air as the transmission medium) to send data between hosts. Wireless networks

	are common in homes, businesses, airports, and hotels. Most wireless networks connect into larger wired networks (such as LANs) which are in turn connected to the Internet.
Wireless Application Protocol (WAP)	WAP (Wireless Application Protocol) access points privacy, integrity, and authentication to wireless client devices and using WTLS (Wireless Transport Layer Security). WTLS is a wireless security services protocol. It protects data between the wireless hub/router/access point and all wireless NICs.
Workgroup	A peer-to-peer network where each Windows 2000 workstation is a member of a logical grouping of computers. The workgroup model has no central user account database or computer that validates a logon. Each Windows 2000 workstation in a workgroup must contain accounts for every person who needs to gain access to resources on that workstation. Workgroups are convenient for very small networks, but because there is no central database for maintaining accounts, administration is difficult.
Workstation-only backup	A backup technique that allows users to back up the critical information they store on their own local computer. Each computer needs its own backup device and storage media.
World Wide Web	A graphically-based and user-friendly part of the Internet. You need a software application called an Internet browser (to view the information on the World Wide Web. The World Wide Web uses the Hypertext Transfer Protocol (HTTP) to connect a system of graphical pages, called Web sites, formatted using Hypertext Markup Language (HTML).
Worms	Pieces of software code written expressly to cause problems with servers and workstations by "tunneling" through the data and code on the hard drive. Worms are a type of computer virus.
WOW (Windows-on-Windows)	Win16 on Win32. A 32-bit program inside Windows NT that lets you run Win16 applications. WOW works inside an NTVDM.
Write-ahead log	A method of logging transactions. Using this method, the log is always written to disk before the data.
WSH (Windows Scripting Host)	A scripting host that lets you run scripts, batch files, and command files from the command prompt or the Windows desktop.

X

X.400 standard	The X.400 standard contains guidelines for exchanging messages electronically. It includes rules for addressing messages as well as an addressing scheme that uses management domains, originator/recipient names, and other information to uniquely identify users within the hierarchy of the organization.
X.500	X.500 is a set of recommendations from the International Telecommunications Union. It lays out the rules that allow combining local directory services into one global directory.

Z

ZAP File	A text file that references a conventional setup program. The ZAP file can be distributed to network users using Active Directory-based Group Policy Objects (GPOs).
Zeroconf	Zero Configuration Networking (Zeroconf) is a standards-based initiative of an IETF working groups whose goals are to: • Make current computer network administration easier by performing configuration tasks automatically without the need for network services such as DNS or DHCP • Enable the creation and implementation of a new generation of network related products • Accomplish all of this without disrupting the existing network infrastructure of large networks With Zeroconf, you should be able to connect two computers and automatically have them be able to communicate. You should also be able to set up a small network (even a network with multiple subnets or connected to the Internet) by simply connecting devices and without performing any additional configuration tasks.
Zone	A portion of the DNS namespace made up of a single domain or of a domain and subdomains that are administered as a single, separate entity. A particular name server is responsible for each zone. The name server stores all address mappings for the domain name space with the zone. It also answers client queries for those names.
Zone transfer	The process of replicating updates to the zone information among multiple DNS servers. Regular zone transfers are necessary because as computers and other devices are added to or removed from a network, host names and IP addresses change.