CompTIA Network+®

GLOSSARY

3G

Third generation wireless data standard for cell phones and other mobile devices. 3G matured over time until Evolved High-Speed Packet Access (HSPA+) became the final wireless 3G data standard. It transferred at theoretical maximum speeds up to 168 megabits per second (Mbps), although real-world implementations rarely passed 10 Mbps.

4G

Most popularly implemented as Long Term Evolution (LTE), a wireless data standard with theoretical download speeds of 300 Mbps and upload speeds of 75 Mbps.

6in4

One of the most popular of all the IPv6 tunneling standards, and one of only two IPv6 tunneling protocols that can go through a NAT.

6to4

The dominant IPv6 tunneling protocol because it is the only IPv6 tunnel that doesn't require a tunnel broker. It is generally used to directly connect two routers because it normally requires a public IPv4 address.

10Base2

The last true bus-standard network where nodes connected to a common, shared length of coaxial cable.

10BaseFL

Fiber-optic implementation of Ethernet that runs at 10 Mbps using baseband signaling. Maximum segment length is 2 km.

10BaseT

An Ethernet LAN designed to run on UTP cabling. Runs at 10 Mbps and uses baseband signaling. Maximum length for the cabling between the NIC and the hub (or the switch, the repeater, and so forth) is 100 m.

10GBaseER/10GBaseEW

A 10 GbE standard using 1550-nm single-mode fiber. Maximum cable length up to 40 km.

10GBaseLR/10GBaseLW

A 10 GbE standard using 1310-nm single-mode fiber. Maximum cable length up to 10 km.

10GBaseSR/10GBaseSW

A 10 GbE standard using 850-nm multimode fiber. Maximum cable length up to 300 m.

10GBaseT

A 10 GbE standard designed to run on CAT 6a UTP cabling. Maximum cable length of 100 m.

10 Gigabit Ethernet (10 GbE)

Currently (2015) the fastest Ethernet designation available, with a number of fiber-optic and copper standards.

100BaseFX

An Ethernet LAN designed to run on fiber-optic cabling. Runs at 100 Mbps and uses baseband signaling. Maximum cable length is 400 m for half-duplex and 2 km for full-duplex.

100BaseT

An Ethernet LAN designed to run on UTP cabling. Runs at 100 Mbps, uses baseband signaling, and uses two pairs of wires on CAT 5 or better cabling.

100BaseT4

An Ethernet LAN designed to run on UTP cabling. Runs at 100 Mbps and uses four-pair CAT 3 or better cabling. Made obsolete by 100BaseT.

100BaseTX

The technically accurate but little-used name for 100BaseT.

110 Block

Also known as a 110-punchdown block, a connection gridwork used to link UTP and STP cables behind an RJ-45 patch panel.

110-Punchdown Block

The most common connection used on the back of an RJ-45 jack and patch panels.

110-Punchdown Tool

See Punchdown Tool.

802 Committee

The IEEE committee responsible for all Ethernet standards.

802.1X

A port-authentication network access control mechanism for networks.

802.3 (Ethernet)

See Ethernet.

802.3ab

The IEEE standard for 1000BaseT.

802.3z

The umbrella IEEE standard for all versions of Gigabit Ethernet other than 1000BaseT.

802.11

See IEEE 802.11.

802.11a

A wireless standard that operates in the frequency range of 5 GHz and offers throughput of up to 54 Mbps.

802.11a-ht

802.11a-ht, and the corresponding 802.11g-ht standard, are technical terms for mixed mode 802.11a/802.11g operation. In mixed mode, both technologies are simultaneously supported.

802.11b

The first popular wireless standard, operates in the frequency range of 2.4 GHz and offers throughput of up to 11 Mbps.

802.11g

Currently (2015) the wireless standard with the widest use, operates on the 2.4-GHz band with a maximum throughput of 54 Mbps.

802.11g-ht

802.11g-ht, and the corresponding 802.11a-ht standard, are technical terms for mixed mode 802.11a/802.11g operation. In mixed mode, both technologies are simultaneously supported.

802.11i

A wireless standard that added security features.

802.11n

An updated 802.11 standard that increases transfer speeds and adds support for multiple in/multiple out (MIMO) by using multiple antennas. 802.11n can operate on either the 2.4- or 5-GHz frequency band and has a maximum throughput of 400 Mbps.

802.16

A wireless standard (also known as WiMAX) with a range of up to 30 miles.

1000BaseCX

A Gigabit Ethernet standard using unique copper cabling, with a 25-m maximum cable distance.

1000BaseLX

A Gigabit Ethernet standard using single-mode fiber cabling, with a 5-km maximum cable distance.

1000BaseSX

A Gigabit Ethernet standard using multimode fiber cabling, with a 220- to 500-m maximum cable distance.

1000BaseT

A Gigabit Ethernet standard using CAT 5e/6 UTP cabling, with a 100-m maximum cable distance.

1000BaseTX

Short-lived gigabit-over-UTP standard from TIA/EIA. Considered a competitor to 1000BaseT, it was simpler to implement but required the use of CAT 6 cable.

1000BaseX

An umbrella Gigabit Ethernet standard. Also known as 802.3z. Comprises all Gigabit standards with the exception of 1000BaseT, which is under the 802.3ab standard.

A Records

A list of the IP addresses and names of all the systems on a DNS server domain.

AAA (Authentication, Authorization, and Accounting)

See Authentication, Authorization, and Accounting (AAA).

Acceptable Use Policy

A document that defines what a person may and may not do on an organization's computers and networks.

Access Control

All-encompassing term that defines the degree of permission granted to use a particular resource. That resource may be anything from a switch port to a particular file to a physical door within a building.

Access Control List (ACL)

A clearly defined list of permissions that specifies what actions an authenticated user may perform on a shared resource.

Access Control Server (ACS)

Cisco program/process/server that makes the decision to admit or deny a node based on posture assessment. From there, the ACS directs the edge access device to allow a connection or to implement a denial or redirect.

Access Port

Regular port in a switch that has been configured as part of a VLAN. Access ports are ports that hosts connect to. They are the opposite of a trunk port, which is only connected to a trunk port on another switch.

Active Directory

A form of directory service used in networks with Windows servers. Creates an organization of related computers that share one or more Windows domains.

Activity Light

An LED on a NIC, hub, or switch that blinks rapidly to show data transfers over the network.

Ad Hoc Mode

A wireless networking mode where each node is in direct contact with every other node in a decentralized free-for-all. Ad hoc mode is similar to the *mesh topology*.

Address Resolution Protocol (ARP)

A protocol in the TCP/IP suite used with the command-line utility of the same name to determine the MAC address that corresponds to a particular IP address.

Administrative Accounts

Specialized user accounts that have been granted sufficient access rights and authority to manage specified administrative tasks. Some administrative accounts exist as a default of the system and have all authority throughout the system. Others must be explicitly assigned the necessary powers to administer given resources.

ADSL (Asymmetric Digital Subscriber Line)

See Asymmetric Digital Subscriber Line (ADSL).

Advanced Encryption Standard (AES)

A block cipher created in the late 1990s that uses a 128-bit block size and a 128-, 192-, or 256-bit key size. Practically uncrackable.

Adware

A program that monitors the types of Web sites you frequent and uses that information to generate targeted advertisements, usually pop-up windows.

Agent

In terms of posture assessment, refers to software that runs within a client and reports the client's security characteristics to an access control server to be approved or denied entry to a system.

Agent-less

In terms of posture assessment, refers to a client that has its posture checked and presented by non-permanent software, such as a Web app program, that executes as part of the connection process. Agent-less software does not run directly within the client but is run on behalf of the client.

Aggregation

A router hierarchy in which every router underneath a higher router always uses a subnet of that router's existing routes.

Air Gap

The act of physically separating a network from every other network.

Aircrack-ng

An open source tool for penetration testing many aspects of wireless networks.

Alert

Proactive message sent from an SNMP manager as a result of a trap issued by an agent. Alerts may be sent as e-mail, SMS message, voicemail, or other avenue.

Algorithm

A set of rules for solving a problem in a given number of steps.

Allow

Permission for data or communication to pass through or to access a resource. Specific allowances through a firewall are called *exceptions*.

Amplification

The aspect of a DoS attack that makes a server do a lot of processing and responding.

Angled Physical Contact (APC)

Fiber-optic connector that makes physical contact between two fiber-optic cables. It specifies an 8-degree angle to the curved end, lowering signal loss. APC connectors have less connection degradation from multiple insertions compared to other connectors.

Anti-Malware Program

Software that attempts to block several types of threats to a client including viruses, Trojan horses, worms, and other unapproved software installation and execution.

Antivirus

Software that attempts to prevent viruses from installing or executing on a client. Some antivirus software may also attempt to remove the virus or eradicate the effects of a virus after an infection.

Anycast

A method of addressing groups of computers as though they were a single computer. Anycasting starts by giving a number of computers (or clusters of computers) the same IP address. Advanced routers then send incoming packets to the closest of the computers.

Apache HTTP Server

An open source HTTP server program that runs on a wide variety of operating systems.

Application Layer

See Open System Interconnection (OSI) Seven-Layer Model.

Application/Context Aware

Advanced feature of some stateful firewalls where the content of the data is inspected to ensure it comes from, or is destined for, an appropriate application. Context-aware firewalls look both deeply and more broadly to ensure that the data content and other aspects of the packet are appropriate to the data transfer being conducted. Packets that fall outside these awareness criteria are denied by the firewall.

Application Log

Tracks application events, such as when an application opens or closes. Different types of application logs record different events.

Application Programming Interface (API)

Shared functions, subroutines, and libraries that allow programs on a machine to communicate with the OS and other programs.

Approval Process

One or more decision makers consider a proposed change and the impact of the change, including funding. If the change, the impact, and the funding are acceptable, the change is permitted.

Archive

The creation and storage of retrievable copies of electronic data for legal and functional purposes.

Archive Bit

An attribute of a file that shows whether the file has been backed up since the last change. Each time a file is opened, changed, or saved, the archive bit is turned on. Some types of backups turn off the archive bit to indicate that a good backup of the file exists on tape.

Area ID

Address assigned to routers in an OSPF network to prevent flooding beyond the routers in that particular network. *See also* Open Shortest Path First (OSPF).

Areas

Groups of logically associated OSPF routers designed to maximize routing efficiency while keeping the amount of broadcast traffic well managed. Areas are assigned a 32-bit value that manifests as an integer between 0 and 4294967295 or can take a form similar to an IP address, for example, "0.0.0.0."

ARP

See Address Resolution Protocol (ARP).

ARP Cache Poisoning

A man-in-the-middle attack, where the attacker associates his MAC address with someone else's IP address (almost always the router), so all traffic will be sent to him first. The attacker sends out unsolicited ARPs, which can either be requests or replies.

arping

A command used to discover hosts on a network, similar to ping, but that relies on ARP rather than ICMP. The arping command won't cross any routers, so it will only work within a broadcast domain. *See also* Address Resolution Protocol (ARP) and ping.

Asset Management

Managing each aspect of a network, from documentation to performance to hardware.

Asymmetric Digital Subscriber Line (ADSL)

A fully digital, dedicated connection to the telephone system that provides download speeds of up to 9 Mbps and upload speeds of up to 1 Mbps.

Asymmetric-Key Algorithm

An encryption method in which the key used to encrypt a message and the key used to decrypt it are different, or asymmetrical.

Asynchronous Transfer Mode (ATM)

A network technology that runs at speeds between 25 and 622 Mbps using fiber-optic cabling or CAT 5 or better UTP.

Attenuation

The degradation of signal over distance for a networking cable.

Authentication

A process that proves good data traffic truly came from where it says it originated by verifying the sending and receiving users and computers.

Authentication, Authorization, and Accounting (AAA)

A security philosophy wherein a computer trying to connect to a network must first present some form of credential in order to be authenticated and then must have limitable permissions within the network. The authenticating server should also record session information about the client.

Authentication Server (AS)

In Kerberos, a system that hands out Ticket-Granting Tickets to clients after comparing the client hash to its own. *See also* Ticket-Granting Ticket (TGT).

Authoritative DNS Servers

DNS servers that hold the IP addresses and names of systems for a particular domain or domains in special storage areas called *forward lookup zones*. They also have *reverse lookup zones*.

Authoritative Name Servers

Another name for authoritative DNS servers. *See* Authoritative DNS Servers.

Authorization

A step in the AAA philosophy during which a client's permissions are decided upon. *See also* Authentication, Authorization, and Accounting (AAA).

Automatic Private IP Addressing (APIPA)

A networking feature in operating systems that enables DHCP clients to self-configure an IP address and subnet mask automatically when a DHCP server isn't available.

Autonomous System (AS)

One or more networks that are governed by a single protocol, which provides routing for the Internet backbone.

Back Up

To save important data in a secondary location as a safety precaution against the loss of the primary data.

Backup Designated Router (BDR)

A second router set to take over if the designated router fails. *See also* Designated Router (DR).

Backup Generator

An onsite generator that provides electricity if the power utility fails.

Bandwidth

A piece of the spectrum occupied by some form of signal, whether it is television, voice, fax data, and so forth. Signals require a certain size and location of bandwidth to be transmitted. The higher the bandwidth, the faster the signal transmission, thus allowing for a more complex signal such as audio or video. Because bandwidth is a limited space, when one user is occupying it, others must wait their turn. Bandwidth is also the capacity of a network to transmit a given amount of data during a given period.

Bandwidth Saturation

When the frequency of a band is filled to capacity due to the large number of devices using the same bandwidth.

Banner Grabbing

When a malicious user gains access to an open port and uses it to probe a host to gain information and access, as well as learn details about running services.

Baseband

Digital signaling that has only one signal (a single signal) on the cable at a time. The signals must be in one of three states: one, zero, or idle.

Baseline

Static image of a system's (or network's) performance when all elements are known to be working properly.

Basic NAT

A simple form of NAT that translates a computer's private or internal IP address to a global IP address on a one-to-one basis.

Basic Rate Interface (BRI)

The basic ISDN configuration, which consists of two *B* channels (which can carry voice or data at a rate of 64 Kbps) and one *D* channel (which carries setup and configuration information, as well as data, at 16 Kbps).

Basic Service Set (BSS)

In wireless networking, a single access point servicing a given area.

Basic Service Set Identifier (BSSID)

Naming scheme in wireless networks.

Baud

One analog cycle on a telephone line.

Baud Rate

The number of bauds per second. In the early days of telephone data transmission, the baud rate was often analogous to bits per second. Due to advanced modulation of baud cycles as well as data compression, this is no longer true.

Bearer Channel (B Channel)

A type of ISDN channel that carries data and voice information using standard DS0 channels at 64 Kbps.

Biometric

Human physical characteristic that can be measured and saved to be compared as authentication in granting the user access to a network or resource. Common biometrics include fingerprints, facial scans, retinal scans, voice pattern recognition, and others.

Biometric Devices

Devices that scan fingerprints, retinas, or even the sound of the user's voice to provide a foolproof replacement for both passwords and smart devices.

Bit Error Rate Test (BERT)

An end-to-end test that verifies a T-carrier connection.

Block

Access that is denied through to or from a resource. A block may be implemented in a firewall, access control server, or other secure gateway. *See also* Allow.

Blocks

Contiguous ranges of IP addresses that are assigned to organizations and end users by IANA. Also called network blocks.

Block Cipher

An encryption algorithm in which data is encrypted in "chunks" of a certain length at a time. Popular in wired networks.

BNC Connector

A connector used for 10Base2 coaxial cable. All BNC connectors have to be locked into place by turning the locking ring 90 degrees.

BNC Coupler

Passive connector used to join two segments of coaxial cables that are terminated with BNC connectors.

Bonding

Two or more NICs in a system working together to act as a single NIC to increase performance.

Bootstrap Protocol (BOOTP)

A component of TCP/IP that allows computers to discover and receive an IP address from a DHCP server prior to booting the OS. Other items that may be discovered during the BOOTP process are the IP address of the default gateway for the subnet and the IP addresses of any name servers.

Border Gateway Protocol (BGP-4)

An exterior gateway routing protocol that enables groups of routers to share routing information so that efficient, loop-free routes can be established.

Botnet

A group of computers under the control of one operator, used for malicious purposes.

Bounce

A signal sent by one device taking many different paths to get to the receiving systems.

Bps (Bits Per Second)

A measurement of how fast data is moved across a transmission medium. A Gigabit Ethernet connection moves 1,000,000,000 bps.

Bridge

A device that connects two networks and passes traffic between them based only on the node address, so that traffic between nodes on one network does not appear on the other network. For example, an Ethernet bridge only looks at the MAC address. Bridges filter and forward frames based on MAC addresses and operate at Layer 2 (Data Link layer) of the OSI seven-layer model.

Bridge Loop

A negative situation in which bridging devices (usually switches) are installed in a loop configuration, causing frames to loop continuously. Switches using Spanning Tree Protocol (STP) prevent bridge loops by automatically turning off looping ports.

Bridged Connection

An early type of DSL connection that made the DSL line function the same as if you snapped an Ethernet cable into your NIC.

Bridging Loop

A physical wiring of a circuitous path between two or more switches, causing frames to loop continuously. Implementing Spanning Tree Protocol (STP) in these devices will discover and block looped paths.

Bring Your Own Device (BYOD)

A trend wherein users bring their own network-enabled devices to the work environment. These cell phones, tablets, notebooks, and other mobile devices must be easily and securely integrated and released from corporate network environments using on-boarding and off-boarding technologies.

Broadband

Analog signaling that sends multiple signals over the cable at the same time. The best example of broadband signaling is cable television. The zero, one, and idle states exist on multiple channels on the same cable. S*ee also* Baseband.

Broadcast

A frame or packet addressed to all machines, almost always limited to a broadcast domain.

Broadcast Address

The address a NIC attaches to a frame when it wants every other NIC on the network to read it. In TCP/IP, the general broadcast address is 255.255.255.255. In Ethernet, the broadcast MAC address is FF-FF-FF-FF-FF-FF.

Broadcast Domain

A network of computers that will hear each other's broadcasts. The older term *collision domain* is the same but rarely used today.

Broadcast Storm

The result of one or more devices sending a nonstop flurry of broadcast frames on the network.

Browser

A software program specifically designed to retrieve, interpret, and display Web pages.

Brute Force

A type of attack wherein every permutation of some form of data is tried in an attempt to discover protected information. Most commonly used on password cracking.

Building Entrance

Location where all the cables from the outside world (telephone lines, cables from other buildings, and so on) come into a building.

Bus Topology

A network topology that uses a single bus cable that connects all of the computers in a line. Bus topology networks must be terminated to prevent signal reflection.

Business Continuity Planning (BCP)

The process of defining the steps to be taken in the event of a physical corporate crisis to continue operations. Includes the creation of documents to specify facilities, equipment, resources, personnel, and their roles.

Butt Set

Device that can tap into a 66- or 110-punchdown block to see if a particular line is working.

Byte

Eight contiguous bits, the fundamental data unit of personal computers. Storing the equivalent of one character, the byte is also the basic unit of measurement for computer storage. Bytes are counted in powers of two.

CAB Files

Short for "cabinet files." These files are compressed and most commonly used during Microsoft operating system installation to store many smaller files, such as device drivers.

Cable Certifier

A very powerful cable testing device used by professional installers to test the electrical characteristics of a cable and then generate a certification report, proving that cable runs pass TIA/EIA standards.

Cable Drop

Location where the cable comes out of the wall at the workstation location.

Cable Modem

A bridge device that interconnects the cable company's DOCSIS service to the user's Ethernet network. In most locations, the cable modem is the demarc.

Cable Stripper

Device that enables the creation of UTP cables.

Cable Tester

A generic name for a device that tests cables. Some common tests are continuity, electrical shorts, crossed wires, or other electrical characteristics.

Cable Tray

A device for organizing cable runs in a drop ceiling.

Cache

A special area of RAM that stores frequently accessed data. In a network there are a number of applications that take advantage of cache in some way.

Cache-Only DNS Servers (Caching-Only DNS Servers)

DNS servers that do not have any forward lookup zones. They resolve names of systems on the Internet for the network, but are not responsible for telling other DNS servers the names of any clients.

Cached Lookup

The list kept by a DNS server of IP addresses it has already resolved, so it won't have to re-resolve an FQDN it has already checked.

Caching Engine

A server dedicated to storing cache information on your network. These servers can reduce overall network traffic dramatically.

Cacti

Popular network graphing program.

Campus Area Network (CAN)

A network installed in a medium-sized space spanning multiple buildings.

Canonical Name (CNAME)

Less common type of DNS record that acts as a computer's alias.

Capture File

A file in which the collected packets from a packet sniffer program are stored.

Capturing a Printer

A process by which a printer uses a local LPT port that connects to a networked printer. This is usually only done to support older programs that are not smart enough to know how to print directly to a UNC-named printer; it's quite rare today.

Card

Generic term for anything that you can snap into an expansion slot.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

See CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

See CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

CAT 3

Category 3 wire, a TIA/EIA standard for UTP wiring that can operate at up to 16 Mbps.

CAT 4

Category 4 wire, a TIA/EIA standard for UTP wiring that can operate at up to 20 Mbps. This wire is not widely used, except in older Token Ring networks.

CAT 5

Category 5 wire, a TIA/EIA standard for UTP wiring that can operate at up to 100 Mbps.

CAT 5e

Category 5e wire, a TIA/EIA standard for UTP wiring with improved support for 100 Mbps using two pairs and support for 1000 Mbps using four pairs.

CAT 6

Category 6 wire, a TIA/EIA standard for UTP wiring with improved support for 1000 Mbps.

Category (CAT) Rating

A grade assigned to cable to help network installers get the right cable for the right network technology. CAT ratings are officially rated in megahertz (MHz), indicating the highest-frequency bandwidth the cable can handle.

CCITT (Comité Consutatif Internationale Téléphonique et Télégraphique)

European standards body that established the V standards for modems.

Central Office

Building that houses local exchanges and a location where individual voice circuits come together.

Certificate

A public encryption key signed with the digital signature from a trusted third party called a *certificate authority (CA)*. This key serves to validate the identity of its holder when that person or company sends data to other parties.

Certifier

A device that tests a cable to ensure that it can handle its rated amount of capacity.

Chain of Custody

A document used to track the collection, handling, and transfer of evidence.

Challenge Handshake Authentication Protocol (CHAP)

A remote access authentication protocol. It has the serving system challenge the remote client, which must provide an encrypted password.

Change Management

The process of initiating, approving, funding, implementing, and documenting significant changes to the network.

Change Management Documentation

A set of documents that defines procedures for changes to the network.

Change Management Team

Personnel who collect change requests, evaluate the change, work with decision makers for approval, plan and implement approved changes, and document the changes.

Change Request

A formal or informal document suggesting a modification to some aspect of the network or computing environment.

Channel

A portion of the wireless spectrum on which a particular wireless network operates. Setting wireless networks to different channels enables separation of the networks.

Channel Bonding

Wireless technology that enables wireless access points (WAPs) to use two channels for transmission.

Channel Service Unit/Digital Service Unit (CSU/DSU)

See CSU/DSU (Channel Service Unit/Data Service Unit).

Chat

A multiparty, real-time text conversation. The Internet's most popular version is known as Internet Relay Chat (IRC), which many groups use to converse in real time with each other.

Checksum

A simple error-detection method that adds a numerical value to each data packet, based on the number of data bits in the packet. The receiving node applies the same formula to the data and verifies that the numerical value is the same; if not, the data has been corrupted and must be re-sent.

Cipher

A series of complex and hard-to-reverse mathematics run on a string of ones and zeroes in order to make a new set of seemingly meaningless ones and zeroes.

Cipher Lock

A door unlocking system that uses a door handle, a latch, and a sequence of mechanical push buttons.

Ciphertext

The output when cleartext is run through a cipher algorithm using a key.

Circuit Switching

The process for connecting two phones together on one circuit.

Cisco IOS

Cisco's proprietary operating system.

Cladding

The part of a fiber-optic cable that makes the light reflect down the fiber.

Class of Service (CoS)

A prioritization value used to apply to services, ports, or whatever a quality of service (QoS) device might use.

Class License

Contiguous chunk of IP addresses passed out by the Internet Assigned Numbers Authority (IANA).

Classless Inter-Domain Routing (CIDR)

Method of categorizing IP addresses in order to distribute them. *See also* Subnetting.

Classless Subnet

A subnet that does not fall into the common categories such as Class A, Class B, and Class C.

Cleartext

See Plaintext.

Cleartext Credentials

Any login process conducted over a network where account names, passwords, or other authentication elements are sent from the client or server in an unencrypted fashion.

Client

A computer program that uses the services of another computer program; software that extracts information from a server. Your autodial phone is a client, and the phone company is its server. Also, a machine that accesses shared resources on a server.

Client-to-Site

A type of VPN connection where a single computer logs into a remote network and becomes, for all intents and purposes, a member of that network.

Client/Server

A relationship in which client software obtains services from a server on behalf of a user.

Client/Server Application

An application that performs some or all of its processing on an application server rather than on the client. The client usually only receives the result of the processing.

Client/Server Network

A network that has dedicated server machines and client machines.

Closed-Circuit Television (CCTV)

A self-contained, closed system in which video cameras feed their signal to specific, dedicated monitors and storage devices.

Cloud Computing

Using the Internet to store files and run applications. For example, Google Docs is a cloud computing application that enables you to run productivity applications over the Internet from your Web browser.

Cloud/Server Based

Remote storage and access of software, especially anti-malware software, where it can be singularly updated. This central storage allows users to access and run current versions of software easily, with the disadvantage of it not running automatically on the local client. The client must initiate access to and launching of the software.

Coaxial Cable

A type of cable that contains a central conductor wire surrounded by an insulating material, which in turn is surrounded by a braided metal shield. It is called coaxial because the center wire and the braided metal shield share a common axis or centerline.

Cold Site

A location that consists of a building, facilities, desks, toilets, parking, and everything that a business needs except computers.

Collision

The result of two nodes transmitting at the same time on a multiple access network such as Ethernet. Both frames may be lost or partial frames may result.

Collision Domain

See Broadcast Domain.

Collision Light

A light on some older NICs that flickers when a network collision is detected.

Command

A request, typed from a terminal or embedded in a file, to perform an operation or to execute a particular program.

Common Internet File System (CIFS)

The protocol that NetBIOS used to share folders and printers. Still very common, even on UNIX/Linux systems.

Community Cloud

A private cloud paid for and used by more than one organization.

Compatibility Issue

When different pieces of hardware or software don't work together correctly.

Compatibility Requirements

With respect to network installations and upgrades, requirements that deal with how well the new technology integrates with older or existing technologies.

Complete Algorithm

A cipher and the methods used to implement that cipher.

Computer Forensics

The science of gathering, preserving, and presenting evidence stored on a computer or any form of digital media that is presentable in a court of law.

Concentrator

A device that brings together at a common center connections to a particular kind of network (such as Ethernet) and implements that network internally.

Configuration Management

A set of documents, policies, and procedures designed to help you maintain and update your network in a logical, orderly fashion.

Configuration Management Documentation

Documents that define the configuration of a network. These would include wiring diagrams, network diagrams, baselines, and policy/procedure/configuration documentation.

Configurations

The settings stored in devices that define how they are to operate.

Connection

A term used to refer to communication between two computers.

Connection-Oriented

Network communication between two hosts that includes negotiation between the hosts to establish a communication session. Data segments are then transferred between hosts, with each segment being acknowledged before a subsequent segment can be sent. Orderly closure of the communication is conducted at the end of the data transfer or in the event of a communication failure. TCP is the only connection-oriented protocol in the TCP/IP suite.

Connection-Oriented Communication

A protocol that establishes a connection between two hosts before transmitting data and verifies receipt before closing the connection between the hosts. TCP is an example of a connection-oriented protocol.

Connectionless

A type of communication characterized by sending packets that are not acknowledged by the destination host. UDP is the quintessential connectionless protocol in the TCP/IP suite.

Connectionless Communication

A protocol that does not establish and verify a connection between the hosts before sending data; it just sends the data and hopes for the best. This is faster than connection-oriented protocols. UDP is an example of a connectionless protocol.

Console Port

Connection jack in a switch used exclusively to connect a computer that will manage the switch.

Content Switch

Advanced networking device that works at least at Layer 7 (Application layer) and hides servers behind a single IP.

Contingency Planning

The process of creating documents that set about how to limit damage and recover quickly from an incident.

Continuity

The physical connection of wires in a network.

Continuity Tester

Inexpensive network tester that can only test for continuity on a line.

Convergence

Point at which the routing tables for all routers in a network are updated.

Copy Backup

A type of backup similar to Normal or Full, in that all selected files on a system are backed up. This type of backup does *not* change the archive bit of the files being backed up.

Core

The central glass of the fiber-optic cable that carries the light signal.

Cost

An arbitrary metric value assigned to a network route with OSFP capable routers.

Counter

A predefined event that is recorded to a log file.

Coarse Wavelength Division Multiplexing (CWDM)

An optical multiplexing technology in which a few signals of different optical wavelength could be combined to travel a fairly short distance.

CRC (Cyclic Redundancy Check)

A mathematical method used to check for errors in long streams of transmitted data with high accuracy.

Crimper

Also called a *crimping tool*, the tool used to secure a crimp (or an RJ-

5 connector) onto the end of a cable.

Cross-Platform Support

Standards created to enable terminals (and now operating systems) from different companies to interact with one another.

Crossover Cable

A specially terminated UTP cable used to interconnect routers or switches, or to connect network cards without a switch. Crossover cables reverse the sending and receiving wire pairs from one end to the other.

Crosstalk

Electrical signal interference between two cables that are in close proximity to each other.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Access method used mainly on wireless networks. Before hosts send out data, they first listen for traffic. If the network is free, they send out a signal that reserves a certain amount of time to make sure the network is free of other signals. If data is detected on the wire, the hosts wait a random time period before trying again. If the wire is free, the data is sent out.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Access method that Ethernet systems use in wired LAN technologies, enabling frames of data to flow through the network and ultimately reach address locations. Hosts on CSMA/CD networks first listen to hear of there is any data on the wire. If there is none, they send out data. If a collision occurs, then both hosts wait a random time period before retransmitting the data.

CSU/DSU (Channel Service Unit/Data Service Unit)

A piece of equipment that connects a T-carrier leased line from the telephone company to a customer's equipment (such as a router). It performs line encoding and conditioning functions, and it often has a loopback function for testing.

Customer-Premises Equipment (CPE)

The primary distribution box and customer-owned/managed equipment that exists on the customer side of the demarc.

Cyclic Redundancy Check (CRC)

See CRC (Cyclic Redundancy Check).

Daily Backup

Also called a *daily copy backup*, makes a copy of all files that have been changed on that day without changing the archive bits of those files.

Daisy-chain

A method of connecting together several devices along a bus and managing the signals for each device.

Data Backup

The process of creating extra copies of data to be used in case the primary data source fails.

Data Encryption Standard (DES)

A symmetric-key algorithm developed by the U.S. government in the 1970s and formerly in use in a variety of TCP/IP applications. DES used a 64-bit block and a 56-bit key. Over time, the 56-bit key made DES susceptible to brute-force attacks.

Data Link Layer

See Open Systems Interconnection (OSI) Seven-Layer Model.

Data Over Cable Service Interface Specification (DOCSIS)

The unique protocol used by cable modem networks.

Datagram

A connectionless transfer unit created with User Datagram Protocol designed for quick transfers over a packet-switched network.

DB-25

A 25-pin, D-shaped subminiature connector, typically use in parallel and older serial port connections.

DB-9

A 9-pin, D-shaped subminiature connector, often used in serial port connections.

De-encapsulation

The process of stripping all the extra header information from a packet as the data moves up a protocol stack.

Dead Spot

A place that should be covered by the network signal but where devices get no signal.

Decibel (dB)

A measurement of the quality of a signal.

Dedicated Circuit

A circuit that runs from a breaker box to specific outlets.

Dedicated Line

A telephone line that is an always open, or connected, circuit. Dedicated telephone lines usually do not have telephone numbers.

Dedicated Server

A machine that does not use any client functions, only server functions.

Default

A software function or operation that occurs automatically unless the user specifies something else.

Default Gateway

In a TCP/IP network, the IP address of the router that interconnects the LAN to a wider network, usually the Internet. This router's IP address is part of the necessary TCP/IP configuration for communicating with multiple networks using IP.

Delta Channel (D Channel)

A type of ISDN line that transfers data at 16 Kbps.

Demarc

A device that marks the dividing line of responsibility for the functioning of a network between internal users and upstream service providers.

Demarc Extension

Any cabling that runs from the network interface to whatever box is used by the customer as a demarc.

Demilitarized Zone (DMZ)

A lightly protected or unprotected subnet network positioned between an outer firewall and an organization's highly protected internal network. DMZs are used mainly to host public address servers (such as Web servers).

Demultiplexer

Device that can extract and distribute individual streams of data that have been combined together to travel along a single shared network cable.

Denial of Service (DoS)

An effort to prevent users from gaining normal use of a resource. *See also* Denial of Service (DoS) Attack.

Denial of Service (DoS) Attack

An attack that floods a networked server with so many requests that it becomes overwhelmed and ceases functioning.

Dense Wavelength Division Multiplexing (DWDM)

An optical multiplexing technology in which a large number of optical signals of different optical wavelength could be combined to travel over relatively long fiber cables.

Designated Router (DR)

The main router in an OSPF network that relays information to all other routers in the area.

Destination Port

A fixed, predetermined number that defines the function or session type in a TCP/IP network.

Device Driver

A subprogram to control communications between the computer and some peripheral hardware.

Device ID

The last six digits of a MAC address, identifying the manufacturer's unique serial number for that NIC.

Device Types/Requirements

With respect to installing and upgrading networks, these determine what equipment is needed to build the network and how the network should be organized.

DHCP Lease

Created by the DHCP server to allow a system requesting DHCP IP information to use that information for a certain amount of time.

DHCP Relay

A router process that, when enabled, passes DHCP requests and responses across router interfaces. In common terms, DHCP communications can cross from one network to another within a router that has DHCP relay enabled and configured.

DHCP Scope

The pool of IP addresses that a DHCP server may allocate to clients requesting IP addresses or other IP information like DNS server addresses.

DHCP Snooping

Switch process that monitors DHCP traffic, filtering out DHCP messages from untrusted sources. Typically used to block attacks that use a rogue DHCP server.

Dial-up Lines

Telephone lines with telephone numbers; they must dial to make a connection, as opposed to a dedicated line.

Differential Backup

Similar to an incremental backup in that it backs up the files that have been changed since the last backup. This type of backup does not change the state of the archive bit.

Differentiated Services (DiffServ)

The underlying architecture that makes quality of service (QoS) work.

DIG (Domain Information Groper)

See Domain Information Groper (DIG).

Digital Signal 1 (DS1)

The signaling method used by T1 lines, which uses a relatively simple frame consisting of 25 pieces: a framing bit and 24 channels. Each DS1 channel holds a single 8-bit DS0 data sample. The framing bit and data channels combine to make 193 bits per DS1 frame. These frames are transmitted 8000 times/sec, making a total throughput of 1.544 Mbps.

Digital Signal Processor (DSP)

See DSP (Digital Signal Processor).

Digital Signature

An encrypted hash of a private encryption key that verifies a sender's identity to those who receive encrypted data or messages.

Digital Subscriber Line (DSL)

A high-speed Internet connection technology that uses a regular telephone line for connectivity. DSL comes in several varieties, including Asymmetric (ADSL) and Symmetric (SDSL), and many speeds. Typical home-user DSL connections are ADSL with a download speed of up to 9 Mbps and an upload speed of up to 1 Kbps.

Dipole Antenna

The standard straight-wire antenna that provides most omnidirectional function.

Direct Current (DC)

A type of electric circuit where the flow of electrons is in a complete circle.

Direct-Sequence Spread-Spectrum (DSSS)

A spread-spectrum broadcasting method defined in the 802.11 standard that sends data out on different frequencies at the same time.

Directional Antenna

An antenna that focuses its signal more towards a specific direction; as compared to an omnidirectional antenna that radiates its signal in all directions equally.

Disaster Recovery

The means and methods to recover primary infrastructure from a disaster. Disaster recovery starts with a plan and includes data backups.

Discretionary Access Control (DAC)

Authorization method based on the idea that there is an owner of a resource who may at his or her discretion assign access to that resource. DAC is considered much more flexible than mandatory access control (MAC).

Disk Mirroring

Process by which data is written simultaneously to two or more disk drives. Read and write speed is decreased but redundancy, in case of catastrophe, is increased. Also known as RAID level 1. *See also* Duplexing.

Disk Striping

Process by which data is spread among multiple (at least two) drives. It increases speed for both reads and writes of data, but provides no fault tolerance. Also known as RAID level 0.

Disk Striping with Parity

Process by which data is spread among multiple (at least three) drives, with parity information as well to provide fault tolerance. The most commonly implemented type is RAID 5, where the data and parity information is spread across three or more drives.

Dispersion

Diffusion over distance of light propagating down fiber cable.

Distance Vector

Set of routing protocols that calculates the total cost to get to a particular network ID and compares that cost to the total cost of all the other routes to get to that same network ID.

Distributed Control System (DCS)

A small controller added directly to a machine used to distribute the computing load.

Distributed Coordination Function (DCF)

One of two methods of collision avoidance defined by the 802.11 standard and the only one currently implemented. DCF specifies strict rules for sending data onto the network media. *See also* Point Coordination Function (PCF).

Distributed Denial of Service (DDoS)

Multicomputer assault on a network resource that attempts, with sheer overwhelming quantity of requests, to prevent regular users from receiving services from the resource.

Distributed Denial of Service (DDoS) Attack

A DoS attack that uses multiple (as in hundreds or up to hundreds of thousands) of computers under the control of a single operator to conduct a devastating attack.

DLL (Dynamic Link Library)

A file of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions, and a program accesses the functions by creating links to the DLL.

DNS Domain

A specific branch of the DNS name space. Top-level DNS domains include .com, .gov, and .edu.

DNS Resolver Cache

A cache used by Windows DNS clients to keep track of DNS information.

DNS Root Servers

The highest in the hierarchy of DNS servers running the Internet.

DNS Server

A system that runs a special DNS server program.

DNS Tree

A hierarchy of DNS domains and individual computer names organized into a tree-like structure, the top of which is the root.

Document

A medium and the data recorded on it for human use; for example, a report sheet or book. By extension, any record that has permanence and that can be read by a human or a machine.

Documentation

A collection of organized documents or the information recorded in documents. Also, instructional material specifying the inputs, operations, and outputs of a computer program or system.

Domain

A term used to describe a grouping of users, computers, and/or networks. In Microsoft networking, a domain is a group of computers and users that shares a common account database and a common security policy. For the Internet, a domain is a group of computers that shares a common element in their DNS hierarchical name.

Domain Controller

A Microsoft Windows Server system specifically configured to store user and server account information for its domain. Often abbreviated as "DC." Windows domain controllers store all account and security information in the *Active Directory* directory service.

Domain Information Groper (DIG)

Command-line tool in non-Windows systems used to diagnose DNS problems.

Domain Name System (DNS)

A TCP/IP name resolution system that resolves host names to IP addresses.

Domain Users and Groups

Users and groups that are defined across an entire network domain.

Door Access Controls

Methodology to grant permission or to deny passage through a doorway. The method may be computer-controlled, human-controlled, token-oriented, or many other means.

Dotted Decimal Notation

Shorthand method for discussing and configuring binary IP addresses.

Download

The transfer of information from a remote computer system to the user's system. Opposite of *upload*.

Drive Duplexing

See Duplexing.

Drive Mirroring

The process of writing identical data to two hard drives on the same controller at the same time to provide data redundancy.

DS0

The digital signal rate created by converting analog sound into 8-bit chunks 8000 times a second, with a data stream of 64 Kbps. This is the simplest data stream (and the slowest rate) of the digital part of the phone system.

DS1

The signaling method used by T1 lines, which uses a relatively simple frame consisting of 25 pieces: a framing bit and 24 channels. Each DS1 channel holds a single 8-bit DS0 data sample. The framing bit and data channels combine to make 193 bits per DS1 frame. These frames are transmitted 8000 times/sec, making a total throughput of 1.544 Mbps.

DSL Access Multiplexer (DSLAM)

A device located in a telephone company's central office that connects multiple customers to the Internet.

DSL Modem

A device that enables customers to connect to the Internet using a DSL connection. A DSL modem isn't really a modem—it's more like an ISDN terminal adapter—but the term stuck, and even the manufacturers of the devices now call them DSL modems.

DSP (Digital Signal Processor)

A specialized microprocessor-like device that processes digital signals at the expense of other capabilities, much as the floating-point unit (FPU) is optimized for math functions. DSPs are used in such specialized hardware as high-speed modems, multimedia sound cards, MIDI equipment, and real-time video capture and compression.

Duplexing

Also called *disk duplexing* or *drive duplexing*, similar to mirroring in that data is written to and read from two physical drives for fault tolerance. In addition, separate controllers are used for each drive, for both additional fault tolerance and additional speed. Considered RAID level 1. *See also* Disk Mirroring.

Dynamic Addressing

A way for a computer to receive IP information automatically from a server program. *See also* Dynamic Host Configuration Protocol (DHCP).

Dynamic ARP Inspection (DAI)

Cisco process that updates a database of trusted systems. DAI then watches for false or suspicious ARPs and ignores them to prevent ARP cache poisoning and other malevolent efforts.

Dynamic DNS (DDNS)

A protocol that enables DNS servers to get automatic updates of IP addresses of computers in their forward lookup zones, mainly by talking to the local DHCP server.

Dynamic Host Configuration Protocol (DHCP)

A protocol that enables a DHCP server to set TCP/IP settings automatically for a DHCP client.

Dynamic Link Library (DLL)

See DLL (Dynamic Link Library).

Dynamic NAT

Type of NAT in which many computers can share a pool of routable IP addresses that number fewer than the computers.

Dynamic Port Numbers

Port numbers 49152–65535, recommended by the IANA to be used as ephemeral port numbers.

Dynamic Routing

Process by which routers in an internetwork automatically exchange information with other routers. Requires a dynamic routing protocol, such as OSPF or RIP.

Dynamic Routing Protocol

A protocol that supports the building of automatic routing tables, such as OSPF or RIP.

E-mail (Electronic Mail)

Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses, known as a *mailing list.*

E-mail Alert

Notification sent by e-mail as a result of an event. A typical use is a notification sent from an SNMP manager as a result of an out of tolerance condition in an SNMP managed device.

E-mail Client

Program that runs on a computer and enables a user to send, receive, and organize e-mail.

E-mail Server

Also known as *mail server*, a server that accepts incoming e-mail, sorts the e-mail for recipients into mailboxes, and sends e-mail to other servers using SMTP.

E1

The European counterpart of a T1 connection that carries 32 channels at 64 Kbps for a total of 2.048 Mbps—making it slightly faster than a T1.

E3

The European counterpart of a T3 line that carries 16 E1 lines (512 channels), for a total bandwidth of 34.368 Mbps—making it a little bit slower than an American T3.

EAP-TLS (Extensible Authentication Protocol with Transport Layer Security)

A protocol that defines the use of a RADIUS server as well as mutual authentication, requiring certificates on both the server and every client.

EAP-TTLS (Extensible Authentication Protocol with Tunneled Transport Layer Security)

A protocol similar to *EAP-TLS* but only uses a single server-side certificate.

Edge

A hardware device that has been optimized to perform a task in coordination with other edge devices and controllers.

Edge Router

Router that connects one Autonomous System (AS) to another.

Effective Permissions

The permissions of all groups combined in any network operating system.

Electromagnetic Interference (EMI)

Interference from one device to another, resulting in poor performance in the device's capabilities. This is similar to having static on your TV while running a hair dryer, or placing two monitors too close together and getting a "shaky" screen.

Electronic Discovery

The process of requesting and providing electronic and stored data and evidence in a legal way.

Electrostatic Discharge (ESD)

See ESD (Electrostatic Discharge).

Emulator

Software or hardware that converts the commands to and from the host machine to an entirely different platform. For example, a program that enables you to run Nintendo games on your PC.

Encapsulation

The process of putting the packets from one protocol inside the packets of another protocol. An example of this is TCP/IP encapsulation in Ethernet, which places TCP/IP packets inside Ethernet frames.

Encryption

A method of securing messages by scrambling and encoding each packet as it is sent across an unsecured medium, such as the Internet. Each encryption level provides multiple standards and options.

End-to-End Principle

Early network concept that originally meant that applications and work should happen only at the endpoints in a network, such as in a single client and a single server.

Endpoint

In the TCP/IP world, the session information stored in RAM. *See also* Socket.

Endpoints

Correct term to use when discussing the data each computer stores about the connection between two computers' TCP/IP applications. *See also* Socket Pairs.

Enhanced Interior Gateway Routing Protocol (EIGRP)

Cisco's proprietary hybrid protocol that has elements of both distance vector and link state routing.

Environment Limitations

With respect to building and upgrading networks, refers to the degree of access to facilities and physical access to physical infrastructure. The type of building or buildings must be considered. Access to the walls and ceilings will factor in the construction of the network.

Environmental Monitor

Device used in telecommunications rooms that keeps track of humidity, temperature, and more.

Ephemeral Port

In TCP/IP communication, an arbitrary number generated by a sending computer that the receiving computer uses as a destination address when sending a return packet.

Ephemeral Port Number

See Ephemeral Port.

Equipment Limitations

With respect to installing and upgrading networks, the degree of usage of any existing equipment, applications, or cabling.

Equipment Rack

A metal structure used in equipment rooms to secure network hardware devices and patch panels. Most racks are 19" wide. Devices designed to fit in such a rack use a height measurement called *units*, or simply *U*.

ESD (Electrostatic Discharge)

The movement of electrons from one body to another. ESD is a real menace to PCs because it can cause permanent damage to semiconductors.

Ethernet

Name coined by Xerox for the first standard of network cabling and protocols. Ethernet is based on a bus topology. The IEEE 802.3 subcommittee defines the current Ethernet specifications.

Ethernet Over Power (EoP)

The IEEE 1901 standard, also known as HomePlug HD-PLC, provides high-speed home networking through the building's existing power infrastructure.

Evil Twin

An attack that lures people into logging into a rogue access point that looks similar to a legitimate access point.

Evolved High-Speed Packet Access (HSPA+)

The final wireless 3G data standard, transferring theoretical maximum speeds up to 168 Mbps, although real-world implementations rarely passed 10 Mbps.

Executable Viruses

Viruses that are literally extensions of executables and that are unable to exist by themselves. Once an infected executable file is run, the virus loads into memory, adding copies of itself to other EXEs that are subsequently run.

Exit Plan

Documents and diagrams that identify the best way out of a building in the event of an emergency. It may also define other procedures to follow.

Extended Service Set (ESS)

A single wireless access point servicing a given area that has been extended by adding more access points.

Extended Service Set Identifier (ESSID)

An SSID applied to an Extended Service Set as a network naming convention.

Extended Unique Identifier, 48-bit (EUI-48)

The IEEE term for the 48-bit MAC address assigned to a network interface. The first 24 bits of the EUI-48 are assigned by the IEEE as the organizationally unique identifier (OUI).

Extended Unique Identifier, 64-bit (EUI-64)

The last 64 bits of the IPv6 address, which are determined based on a calculation based on a device's 48-bit MAC address.

Extensible Authentication Protocol (EAP)

Authentication wrapper that EAP-compliant applications can use to accept one of many types of authentication. While EAP is a general-purpose authentication wrapper, its only substantial use is in wireless networks.

External Connections

A network's connections to the wider Internet. Also a major concern when setting up a SOHO network.

External Data Bus (EDB)

The primary data highway of all computers. Everything in your computer is tied either directly or indirectly to the EDB.

External Firewall

The firewall that sits between the perimeter network and the Internet and is responsible for bearing the brunt of the attacks from the Internet.

External Network Address

A number added to the MAC address of every computer on an IPX/SPX network that defines every computer on the network; this is often referred to as a *network number*.

External Threats

Threats to your network through external means; examples include virus attacks and the exploitation of users, security holes in the OS, or weaknesses of the network hardware itself.

F connector

A screw-on connector used to terminate small-diameter coaxial cable such as RG-6 and RG-59 cables.

Fail Close

Defines the condition of doors and locks in the event of an emergency, indicating that the doors should close and lock.

Fail Open

Defines the condition of doors and locks in the event of an emergency, indicating that the doors should be open and unlocked.

FAQ (Frequently Asked Questions)

Common abbreviation coined by BBS users and spread to Usenet and the Internet. This is a list of questions and answers that pertains to a particular topic, maintained so that users new to the group don't all bombard the group with similar questions. Examples are "What is the name of the actor who plays *X* on this show, and was he in anything else?" or "Can anyone list all of the books by this author in the order that they were published so that I can read them in that order?" The common answer to this type of question is "Read the FAQ!"

Far-End Crosstalk (FEXT)

Crosstalk on the opposite end of a cable from the signal's source.

Fast Ethernet

Nickname for the 100-Mbps Ethernet standards. Originally applied to 100BaseT.

Fault Tolerance

The capability of any system to continue functioning after some part of the system has failed. RAID is an example of a hardware device that provides fault tolerance for hard drives.

FDDI (Fiber Distributed Data Interface

See Fiber Distributed Data Interface (FDDI).

Federal Communications Commission (FCC)

In the United States, regulates public airwaves and rates PCs and other equipment according to the amount of radiation emitted.

Fiber Distributed Data Interface (FDDI)

Older technology fiber optic network used in campus-sized installations. It transfers data at 100Mbps and uses a token bus network protocol over a ring topology.

Fiber-Optic Cable

A high-speed physical medium for transmitting data that uses light rather than electricity to transmit data and is made of high-purity glass fibers sealed within a flexible opaque tube. Much faster than conventional copper wire.

Fibre Channel (FC)

A self-contained, high-speed storage environment with its own storage arrays, cables, protocols, cables, and switches. Fibre Channel is a critical part of storage addressed networking (SAN).

File Server

A computer designated to store software, courseware, administrative tools, and other data on a local or wide area network (WAN). It "serves" this information to other computers via the network when users enter their personal access codes.

File Transfer Protocol (FTP)

A set of rules that allows two computers to talk to one another as a file transfer is carried out. This is the protocol used when you transfer a file from one computer to another across the Internet.

Fire Ratings

Ratings developed by Underwriters Laboratories (UL) and the National Electrical Code (NEC) to define the risk of network cables burning and creating noxious fumes and smoke.

Firewall

A device that restricts traffic between a local network and the Internet.

FireWire

An IEEE 1394 standard to send wide-band signals over a thin connector system that plugs into TVs, VCRs, TV cameras, PCs, and so forth. This serial bus developed by Apple and Texas Instruments enables connection of 60 devices at speeds ranging from 100 to 800 Mbps.

First Responder

The person or robot whose job is to react to the notification of a possible computer crime by determining the severity of the situation, collecting information, documenting findings and actions, and providing the information to the proper authorities.

Flat Name Space

A naming convention that gives each device only one name that must be unique. NetBIOS uses a flat name space. TCP/IP's DNS uses a hierarchical name space.

Flat-surface Connector

Early fiber-optic connector that resulted in a small gap between fiber-optic junctions due to the flat grind faces of the fibers. It was replaced by Angled Physical Contact (APC) connectors.

Flow

A stream of packets from one specific place to another.

Flow Cache

Stores sets of flows for interpretation and analysis. *See also* Flow.

Forensics Report

A document that describes the details of gathering, securing, transporting, and investigating evidence.

Forward Lookup Zone

The storage area in a DNS server to store the IP addresses and names of systems for a particular domain or domains.

Forward Proxy Server

Server that acts as middleman between clients and servers, making requests to network servers on behalf of clients. Results are sent to the proxy server, which then passes them to the original client. The network servers are isolated from the clients by the forward proxy server. *See also* Reverse Proxy Server.

FQDN (Fully Qualified Domain Name)

See Fully Qualified Domain Name (FQDN).

Fractional T1 Access

A service provided by many telephone companies wherein customers can purchase a number of individual channels in a T1 line in order to save money.

Frame

A defined series of binary data that is the basic container for a discrete amount of data moving across a network. Frames are created at Layer 2 of the OSI model.

Frame Check Sequence (FCS)

A sequence of bits placed in a frame that is used to check the primary data for errors.

Frame Relay

An extremely efficient data transmission technique used to send digital information such as voice, data, LAN, and WAN traffic quickly and cost-efficiently to many destinations from one port.

FreeRADIUS

Free RADIUS server software for UNIX/Linux systems.

Freeware

Software that is distributed for free with no license fee.

Frequency Division Multiplexing (FDM)

A process of keeping individual phone calls separate by adding a different frequency multiplier to each phone call, making it possible to separate phone calls by their unique frequency range.

Frequency-Hopping Spread-Spectrum (FHSS)

A spread-spectrum broadcasting method defined in the 802.11 standard that sends data on one frequency at a time, constantly shifting (or *hopping*) frequencies.

Frequently Asked Questions (FAQ)

See FAQ (Frequently Asked Questions).

FUBAR

Fouled Up Beyond All Recognition.

Full-Duplex

Any device that can send and receive data simultaneously.

Fully Meshed Topology

A mesh network where every node is directly connected to every other node.

Fully Qualified Domain Name (FQDN)

The complete DNS name of a system, from its host name to the top-level domain name. Textual nomenclature to a domain-organized resource. It is written left to right, with the host name on the left, followed by any hierarchical subdomains within the top-level domain on the right. Each level is separated from any preceding or following layer by a dot (.).

Gain

The strengthening and focusing of radio frequency output from a wireless access point (WAP).

Gateway Router

A router that acts as a default gateway in a TCP/IP network.

General Logs

Logs that record updates to applications.

Get (SNMP)

A query from an SNMP manager sent to the agent of a managed device for the status of a management information base (MIB) object.

Giga

The prefix that generally refers to the quantity 1,073,741,824. One gigabyte is 1,073,741,824 bytes. With frequencies, in contrast, giga- often refers to one billion. One gigahertz is 1,000,000,000 hertz.

Gigabit Ethernet

See 1000BaseT.

Gigabit Interface Converter (GBIC)

Modular port that supports a standardized, wide variety of gigabit interface modules.

Gigabyte

1024 megabytes.

Global Unicast Address

A second IPv6 address that every system needs in order to get on the Internet.

Grandfather, Father, Son (GFS)

A tape rotation strategy used in data backups.

Graphing

Type of software that creates visual representations and graphs of data collected by SNMP managers.

Greenfield Mode

One of three modes used with 802.11n wireless networks wherein everything is running at higher speed.

Ground Loop

A voltage differential that exists between two different grounding points.

Group Policy

A feature of Windows Active Directory that allows an administrator to apply policy settings to network users *en masse*.

Group Policy Object (GPO)

Enables network administrators to define multiple rights and permissions to entire sets of users all at one time.

Groups

Collections of network users who share similar tasks and need similar permissions; defined to make administration tasks easier.

Guest

In terms of virtualization, an operating system running as a virtual machine inside a hypervisor.

Guest Network

A network that can contain or allow access to any resource that management deems acceptable to be used by insecure hosts that attach to the guest network.

H.320

A standard that uses multiple ISDN channels to transport video teleconferencing (VTC) over a network.

H.323

A VoIP standard that handles the initiation, setup, and delivery of VoIP sessions.

Hackers

People who break into computer systems. Those with malicious intent are sometimes considered "black hat" hackers and those who do so with a positive intent (such as vulnerability testing) are regularly referred to as "white hat" hackers. Of course, there are middle ground hackers: "gray hats."

Half-Duplex

Any device that can only send or receive data at any given moment.

Hardening

Applying security hardware, software, and processes to your network to prevent bad things from happening.

Hardware Appliance

Physical network device, typically a "box" that implements and runs software or firmware to perform one or a multitude of tasks. Could be a firewall, a switch, a router, a print server, or one of many other devices.

Hardware Tools

Tools such as cable testers, TDRs, OTDRs, certifiers, voltage event recorders, protocol analyzers, cable strippers, multimeters, tone probes/generators, butt sets, and punchdown tools used to configure and troubleshoot a network.

Hash

A mathematical function used in cryptography that is run on a string of binary digits of any length that results in a value of some fixed length.

HDMI Ethernet Channel (HEC)

Ethernet-enabled HDMI ports that combine video, audio, and data on a single cable.

Heating, Ventilation, and Air Conditioning (HVAC)

All of the equipment involved in heating and cooling the environments within a facility. These items include boilers, furnaces, air conditioners and ducts, plenums, and air passages.

Hex (Hexadecimal)

Hex symbols based on a numbering system of 16 (computer shorthand for binary numbers), using 10 digits and 6 letters to condense 0s and 1s to binary numbers. Hex is represented by digits 0 through 9 and alpha *A* through *F*, so that 09h has a value of 9, and 0Ah has a value of 10.

Hierarchical Name Space

A naming scheme where the full name of each object includes its position within the hierarchy. An example of a hierarchical name is www.totalseminars.com, which includes not only the host name, but also the domain name. DNS uses a hierarchical name space scheme for fully qualified domain names (FQDNs).

High Availability

A collection of technologies and procedures that work together to keep an application available at all times.

High-Speed WAN Internet Cards

A type of router expansion card that enables connection to two different ISPs.

History Logs

Logs that track the history of how a user or users access network resources, or how network resources are accessed throughout the network.

Home Page

Either the Web page that your browser is set to use when it starts up or the main Web page for a business, organization, or person. Also, the main page in any collection of Web pages.

Honeynet

The network created by a honeypot in order to lure in hackers.

Honeypot

An area of a network that an administrator sets up for the express purpose of attracting a computer hacker. If a hacker takes the bait, the network's important resources are unharmed and network personnel can analyze the attack to predict and protect against future attacks, making the network more secure.

Hop

The passage of a packet through a router.

Hop Count

An older metric used by RIP routers. The number of routers that a packet must cross to get from a router to a given network. Hop counts were tracked and entered into the routing table within a router so the router could decide which interface was the best one to forward a packet.

Horizontal Cabling

Cabling that connects the equipment room to the work areas.

Host

A single device (usually a computer) on a TCP/ IP network that has an IP address; any device that can be the source or destination of a data packet. Also, a computer running multiple virtualized operating systems.

Host ID

The portion of an IP address that defines a specific machine in a subnet.

Host Name

An individual computer name in the DNS naming convention.

Host-Based Anti-Malware

Anti-malware software that is installed on individual systems, as opposed to the network at large.

Host-Based Firewall

A software firewall installed on a "host" that provides firewall services for just that machine, such as Windows Firewall.

Host-to-Host

Type of VPN connection in which a single host establishes a link with a remote, single host.

Host-to-Site

Type of VPN connection where a host logs into a remote network as if it were any other local resource of that network.

hostname

Command-line tool that returns the host name of the computer it is run on.

Hosts File

The predecessor to DNS, a static text file that resides on a computer and is used to resolve DNS host names to IP addresses. The hosts file is checked before the machine sends a name resolution request to a DNS name server. The hosts file has no extension.

Hot Site

A complete backup facility to continue business operations. It is considered "hot" because it has all resources in place, including computers, network infrastructure, and current backups, so that operations can commence within hours after occupation.

Hotspot

A wireless access point that is connected to a cellular data network, typically WiMAX, 3G, or 4G. The device can route Wi-Fi to and from the Internet. Hotspots can be permanent installations or portable. Many cellular telephones have the capability to become a hotspot.

HTML (Hypertext Markup Language)

An ASCII-based script-like language for creating hypertext documents like those on the World Wide Web.

HTTP over SSL (HTTPS)

A secure form of HTTP in which hypertext is encrypted by SSL before being sent onto the network. It is commonly used for Internet business transactions or any time where a secure connection is required. *See also* Hypertext Transfer Protocol (HTTP) *and* Secure Sockets Layer (SSL).

Hub

An electronic device that sits at the center of a star topology network, providing a common point for the connection of network devices. In a 10BaseT Ethernet network, the hub contains the electronic equivalent of a properly terminated bus cable. Hubs are rare today and have been replaced by switches.

Human Machine Interface (HMI)

In a distributed control system (DCS), a computer or set of controls that exists between a controller and a human operator. The human operates the HMI, which in turn interacts with the controller.

Hybrid Cloud

A conglomeration of public and private cloud resources, connected to achieve some target result. There is no clear line that defines how much of a hybrid cloud infrastructure is private and how much is public.

Hybrid Topology

A mix or blend of two different topologies. A star-bus topology is a hybrid of the star and bus topologies.

Hypertext

A document that has been marked up to enable a user to select words or pictures within the document, click them, and connect to further information. The basis of the World Wide Web.

Hypertext Markup Language (HTML)

See HTML (Hypertext Markup Language).

Hypertext Transfer Protocol (HTTP)

Extremely fast protocol used for network file transfers on the World Wide Web.

Hypertext Transfer Protocol over SSL (HTTPS)

Protocol to transfer hypertext from a Web server to a client in a secure and encrypted fashion. SSL establishes a secure communication connection between hosts. It then encrypts the hypertext before sending it from the Web server and decrypts it when it enters the client. HTTPS uses port 443.

Hypervisor

In virtualization, a layer of programming that creates, supports, and manages virtual machine.

ICS (Internet Connection Sharing)

Also known simply as *Internet sharing*, the technique of enabling more than one computer to access the Internet simultaneously using a single Internet connection. When you use Internet sharing, you connect an entire LAN to the Internet using a single public IP address.

ICS (Industrial Control Server)

A centralized controller where the local controllers of a distributed control system (DCS) meet in order for global changes to be made.

IEEE (Institute of Electrical and Electronics Engineers)

The leading standards-setting group in the United States.

IEEE 802.2

IEEE subcommittee that defined the standards for Logical Link Control (LLC).

IEEE 802.3

IEEE subcommittee that defined the standards for CSMA/CD (a.k.a. *Ethernet*).

IEEE 802.11

IEEE subcommittee that defined the standards for wireless.

IEEE 802.14

IEEE subcommittee that defined the standards for cable modems.

IEEE 802.16

A wireless standard (also known as WiMAX) with a range of up to 30 miles.

IEEE 1284

The IEEE standard for the now obsolete parallel communication.

IEEE 1394

IEEE standard for FireWire communication.

IEEE 1905.1

Standard that integrates Ethernet, Wi-Fi, Ethernet over power lines, and Multimedia over Coax (MoCA).

IETF (Internet Engineering Task Force)

The primary standards organization for the Internet.

ifconfig

A command-line utility for Linux servers and workstations that displays the current TCP/IP configuration of the machine, similar to ipconfig for Windows systems. The newer command line utility, ip, is replacing ifconfig on most systems.

IMAP (Internet Message Access Protocol)

An alternative to POP3. Currently in its fourth revision, IMAP4 retrieves e-mail from an e-mail server like POP3, but has a number of features that make it a more popular e-mail tool. IMAP4 supports users creating folders on the e-mail server, for example, and allows multiple clients to access a single mailbox. IMAP uses TCP port 143.

Impedance

The amount of resistance to an electrical signal on a wire. It is used as a relative measure of the amount of data a cable can handle.

Implicit Deny

The blocking of access to any entity that has not been specifically granted access. May also be known as *implicit deny any*. An example might be a whitelist ACL. Any station that is not in the whitelist is implicitly denied access.

In-Band Management

Technology that enables managed devices such as a switch or router to be managed by any authorized host that is connected to that network.

Inbound Traffic

Packets coming in from outside the network.

Incident Response

Reaction to any negative situations that take place within an organization that can be stopped, contained, and remediated without outside resources.

Incremental Backup

Backs up all files that have their archive bits turned on, meaning they have been changed since the last backup. This type of backup turns the archive bits off after the files have been backed up.

Independent Basic Service Set (IBSS)

A basic unit of organization in wireless networks formed by two or more wireless nodes communicating in ad hoc mode.

Industrial Control Server (ICS)

See ICS (Industrial Control Server).

Infrastructure as a Service (IaaS)

Providing servers, switches, and routers to customers for a set rate. IaaS is commonly done by large-scale, global providers that use virtualization to minimize idle hardware, protect against data loss and downtime, and respond to spikes in demand.

Infrastructure Mode

Mode in which wireless networks use one or more wireless access points to connect the wireless network nodes centrally. This configuration is similar to the *star topology* of a wired network.

Inheritance

A method of assigning user permissions, in which folder permissions flow downward into subfolders.

Institute of Electrical and Electronics Engineers (IEEE)

See IEEE (Institute of Electrical and Electronics Engineers).

Insulating Jacket

The external plastic covering of a fiber-optic cable.

Integrated Services Digital Network (ISDN)

See ISDN (Integrated Services Digital Network).

Integrity

Network process that ensures data sent to a recipient is unchanged when it is received at the destination host.

Interface Identifier

The second half (64 bits) of an IPv6 address.

Interface Monitor

A program that tracks the bandwidth and utilization of one or more interfaces on one or more devices in order to monitor traffic on a network.

Interframe Gap (IFG)

A short, predefined silence originally defined for CSMA/CD; also used in CSMA/CA. Also known as an *interframe space (IFS)*.

Interframe Space (IFS)

See Interframe Gap (IFG).

Intermediate Distribution Frame (IDF)

The room where all the horizontal runs from all the work areas on a given floor in a building come together.

Intermediate System to Intermediate System (IS-IS)

Protocol similar to, but not as popular as, OSPF, but with support for IPv6 since inception.

Internal Connections

The connections between computers in a network.

Internal Firewall

The firewall that sits between the perimeter network and the trusted network that houses all the organization's private servers and workstations.

Internal Network

A private LAN, with a unique network ID, that resides behind a router.

Internal Threats

All the things that a network's own users do to create problems on the network. Examples include accidental deletion of files, accidental damage to hardware devices or cabling, and abuse of rights and permissions.

Internet Assigned Numbers Authority (IANA)

The organization originally responsible for assigning public IP addresses. IANA no longer directly assigns IP addresses, having delegated this to the five Regional Internet Registries. *See also* Regional Internet Registries (RIRs).

Internet Authentication Service (IAS)

Popular RADIUS server for Microsoft environments.

Internet Connection Sharing (ICS)

See ICS (Internet Connection Sharing).

Internet Control Message Protocol (ICMP)

A TCP/IP protocol used to handle many low level functions such as error reporting. ICMP messages are usually request and response pairs such as echo requests and responses, router solicitations and responses, and traceroute

requests and responses. There are also unsolicited "responses" (advertisements) which consist of single packets. ICMP messages are connectionless.

Internet Engineering Task Force (IETF)

See IETF (Internet Engineering Task Force).

Internet Group Management Protocol (IGMP)

Protocol that routers use to communicate with hosts to determine a "group" membership in order to determine which computers want to receive a multicast. Once a multicast has started, IGMP is responsible for maintaining the multicast as well as terminating at completion.

Fixed per JW. - Shannon

Internet Information Services (IIS)

Microsoft's Web server program for managing Web servers.

Internet Message Access Protocol Version 4 (IMAP4)

See IMAP (Internet Message Access Protocol).

Internet of Things (IoT)

The idea that everyday objects could be capable of communicating with each other. Although this is certainly true to an extent now, the future of this technology has much greater implications.

Internet Protocol (IP)

The Internet standard protocol that handles the logical naming for the TCP/IP protocol using IP addresses.

Internet Protocol Security (IPsec)

Network layer encryption protocol.

Internet Protocol Version 4 (IPv4)

Protocol in which addresses consist of four sets of numbers, each number being a value between 0 and 255, using a period to separate the numbers (often called *dotted decimal* format). No IPv4 address may be all 0s or all 255s. Examples include 192.168.0.1 and 64.176.19.164.

Internet Protocol Version 6 (IPv6)

Protocol in which addresses consist of eight sets of four hexadecimal numbers, each number being a value between 0000 and FFFF, using a colon to separate the numbers. No IP address may be all 0s or all FFFFs. An example is FEDC:BA98:7654:3210:0800:200C:00CF:1234.

Internet Small Computer System Interface (iSCSI)

A protocol that enables the SCSI command set to be transported over a TCP/IP network from a client to an iSCSI-based storage system. iSCSI is popular with storage area network (SAN) systems.

InterVLAN Routing

A feature on some switches to provide routing between VLANs.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

An IPv6 tunneling protocol that adds the IPv4 address to an IPv6 prefix.

Intranet

A private TCP/IP network inside a company or organization.

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

An application (often running on a dedicated IDS box) that inspects incoming packets, looking for active intrusions. The difference between an IDS and an IPS is that an IPS can react to an attack.

IP

The core routing and addressing technology that makes up the modern Internet.

IP Address

The numeric address of a computer connected to a TCP/IP network, such as the Internet. IPv4 addresses are 32 bits long, written as four octets of 8-bit binary. IPv6 addresses are 128 bits long, written as eight sets of four hexadecimal characters. IP addresses must be matched with a valid subnet mask, which identifies the part of the IP address that is the network ID and the part that is the host ID.

IP Addressing

The processes of assigning IP addresses to networks and hosts.

IP Camera

Still-frame or video camera with a network interface and TCP/IP transport protocols to send output to a network resource or destination.

IP Filtering

A method of blocking packets based on IP addresses.

IP Helper

Command used in Cisco switches and routers to enable, disable, and manage internetwork forwarding of certain protocols such as DHCP, TFTP, Time Service, TACACS, DNS, NetBIOS, and others.

ipconfig

A command-line utility for Windows that displays the current TCP/IP configuration of the machine; similar to UNIX/Linux's ifconfig.

IRC (Internet Relay Chat)

An online group discussion. Also called *chat*.

ISDN (Integrated Services Digital Network)

The CCITT (Comité Consutatif Internationale Téléphonique et Télégraphique) standard that defines a digital method for telephone communications. Originally designed to replace the current analog telephone systems. ISDN lines have telephone numbers and support up to 128-Kbps transfer rates. ISDN also allows data and voice to share a common phone line. Never very popular, ISDN is now relegated to specialized niches.

ISP (Internet Service Provider)

An institution that provides access to the Internet in some form, usually for a fee.

IT (Information Technology)

The business of computers, electronic communications, and electronic commerce.

Java

A network-oriented programming language invented by Sun Microsystems and specifically designed for writing programs that can be safely downloaded to your computer through the Internet and immediately run without fear of viruses or other harm to your computer or files. Using small Java programs (called *applets*), Web pages can include functions such as animations, calculators, and other fancy tricks.

Jumbo Frames

Usually 9000 bytes long, though technically anything over 1500 bytes qualifies, these frames make large data transfer easier and more efficient than using the standard frame size.

Just a Bunch of Disks (JBOD)

An array of hard drives that are simply connected with no RAID implementations.

K-

Most commonly used as the suffix for the binary quantity 1024. For instance, 640K means 640 × 1024 or 655,360. Just to add some extra confusion to the IT industry, *K* is often misspoken as "kilo," the metric value for 1000. For example, 10KB, spoken as "10 kilobytes," means 10,240 bytes rather than 10,000 bytes. Finally, when discussing frequencies, K means 1000. So, 1 KHz = 1000 kilohertz.

Kbps (Kilobits Per Second)

Data transfer rate.

Kerberos

An authentication standard designed to allow different operating systems and applications to authenticate each other.

Key Distribution Center (KDC)

System for granting authentication in Kerberos.

Key Fob

Small device that can be easily carried in a pocket or purse or attached to a key ring. This device is used to identify the person possessing it for the purpose of granting or denying access to resources such as electronic doors.

Key Pair

Name for the two keys generated in asymmetric-key algorithm systems.

Keypad

The device in which an alphanumeric code or password that is assigned to a specific individual for a particular asset can be entered.

Kilohertz (KHz)

A unit of measure that equals a frequency of 1000 cycles per second.

LAN (Local Area Network)

A group of PCs connected together via cabling, radio, or infrared that use this connectivity to share resources such as printers and mass storage.

Last Mile

The connection between a central office and individual users in a telephone system.

Latency

A measure of a signal's delay.

Layer

A grouping of related tasks involving the transfer of information. Also, a particular level of the OSI seven-layer model, for example, Physical layer, Data Link layer, and so forth.

Layer 2 Switch

Any device that filters and forwards frames based on the MAC addresses of the sending and receiving machines. What is normally called a "switch" is actually a "Layer 2 switch."

Layer 2 Tunneling Protocol (L2TP)

A VPN protocol developed by Cisco that can be run on almost any connection imaginable. LT2P has no authentication or encryption, but uses IPsec for all its security needs.

Layer 3 Switch

Also known as a *router,* filters and forwards data packets based on the IP addresses of the sending and receiving machines.

LC (Local Connector)

A duplex type of Small Form Factor (SFF) fiber connector, designed to accept two fiber cables. *See also* Local Connector (LC).

LED (Light Emitting Diode)

Solid-state device that vibrates at luminous frequencies when current is applied.

Leeching

Using another person's wireless connection to the Internet without that person's permission.

Legacy Mode

One of three modes used with 802.11n wireless networks where the wireless access point (WAP) sends out separate packets just for legacy devices.

Legal Hold

The process of an organization preserving and organizing data in anticipation of or in reaction to a pending legal issue.

Light Leakage

The type of interference caused by bending a piece of fiber-optic cable past its maximum bend radius. Light bleeds through the cladding, causing signal distortion and loss.

Light Meter

An optical power meter used by technicians to measure the amount of light lost through light leakage in a fiber cable.

Lights-out Management

Special "computer within a computer" features built into better servers, designed to give you access to a server even when the server itself is shut off.

Lightweight Directory Access Protocol (LDAP)

A protocol used to query and change a database used by the network. LDAP uses TCP port 389 by default**.**

Lightweight Extensible Authentication Protocol (LEAP)

A proprietary EAP authentication used almost exclusively by Cisco wireless products. LEAP is an interesting combination of MS-CHAP authentication between a wireless client and a RADIUS server.

Line Tester

A device used by technicians to check the integrity of telephone wiring. Can be used on a twisted pair line to see if it is good, dead, or reverse wired, or if there is AC voltage on the line.

Link Aggregation

Connecting multiple NICs in tandem to increase bandwidth in smaller increments. *See also* NIC teaming.

Link Aggregation Control Protocol (LACP)

IEEE specification of certain features and options to automate the negotiation, management, load balancing, and failure modes of aggregated ports.

Link Light

An LED on NICs, hubs, and switches that lights up to show good connection between the devices.

Link-Local Address

The address that a computer running IPv6 gives itself after first booting. The first 64 bits of a link-local address are always FE80::/64.

Link Segments

Segments that link other segments together but are unpopulated or have no computers directly attached to them.

Link State

Type of dynamic routing protocol that announces only changes to routing tables, as opposed to entire routing tables. Compare to distance vector routing protocols. *See also* Distance Vector.

Linux

The popular open source operating system, derived from UNIX.

List of Requirements

A list of all the things you'll need to do to set up your SOHO network, as well as the desired capabilities of the network.

Listening Port

A socket that is prepared to respond to any IP packets destined for that socket's port number.

LMHOSTS File

A static text file that resides on a computer and is used to resolve NetBIOS names to IP addresses. The LMHOSTS file is checked before the machine sends a name resolution request to a WINS name server. The LMHOSTS file has no extension.

Load Balancing

The process of taking several servers and making them look like a single server, spreading processing and to supporting bandwidth needs.

Local

Refers to the computer(s), server(s), and/or LAN that a user is physically using or that is in the same room or building.

Local Area Network (LAN)

See LAN (Local Area Network).

Local Connector (LC)

One popular type of Small Form Factor (SFF) connector, considered by many to be the predominant fiber connector. While there are several labels ascribed to the "LC" term, it is most commonly referred to as a local connector. *See also* LC (Local Connector).

Local User Accounts

The accounts unique to a single Windows system. Stored in the local system's registry.

Localhost

The hosts file alias for the loopback address of 127.0.0.1, referring to the current machine.

Log

Information about the performance of some particular aspect of a system that is stored for future reference. Logs are also called *counters* in Performance Monitor or *facilities* in syslog.

Log Management

The process of providing proper security and maintenance for log files to ensure the files are organized and safe.

Logical Address

A programmable network address, unlike a physical address that is burned into ROM.

Logical Addressing

As opposed to physical addressing, the process of assigning organized blocks of logically associated network addresses to create smaller manageable networks called subnets. IP addresses are one example of logical addressing.

Logical Link Control (LLC)

The aspect of the NIC that talks to the operating system, places outbound data coming "down" from the upper layers of software into frames, and creates the FCS on each frame. The LLC also deals with incoming frames by processing those addressed to the NIC and erasing ones addressed to other machines on the network.

Logical Network Diagram

A document that shows the broadcast domains and individual IP addresses for all devices on the network. Only critical switches and routers are shown.

Logical Topology

A network topology defined by signal paths as opposed to the physical layout of the cables. *See also* Physical Topology.

Long Term Evolution (LTE)

Better known as 4G, a wireless data standard with theoretical download speeds of 300 Mbps and upload speeds of 75 Mbps.

Looking Glass Site

Web sites that enable a technician to run various diagnostic tools from outside their network.

Loopback Address

Sometimes called the localhost, a reserved IP address used for internal testing: 127.0.0.1.

Loopback Plug

Network connector that connects back into itself, used to connect loopback tests.

Loopback Test

A special test often included in diagnostic software that sends data out of the NIC and checks to see if it comes back.

MAC-48

The unique 48-bit address assigned to a network interface card. This is also known as the MAC address or the EUI-48.

MAC (Media Access Control) Address

Unique 48-bit address assigned to each network card. IEEE assigns blocks of possible addresses to various NIC manufacturers to help ensure that each address is unique. The Data Link layer of the OSI seven-layer model uses MAC addresses for locating machines.

MAC Address Filtering

A method of limiting access to a wireless network based on the physical addresses of wireless NICs.

MAC Filtering

See MAC Address Filtering.

Macro

A specially written application macro (collection of commands) that performs the same functions as a virus. These macros normally autostart when the application is run and then make copies of themselves, often propagating across networks.

Mailbox

Special holding area on an e-mail server that separates out e-mail for each user.

Main Distribution Frame (MDF)

The room in a building that stores the demarc, telephone cross-connects, and LAN cross-connects.

Maintenance Window

The time it takes to implement and thoroughly test a network change.

Malicious User

A user who consciously attempts to access, steal, or damage resources.

Malware

Any program or code (macro, script, and so on) that's designed to do something on a system or network that you don't want to have happen.

Man in the Middle

A hacking attack where a person inserts him- or herself into a conversation between two others, covertly intercepting traffic thought to be only between those other people.

Managed Device

Networking devices, such as routers and advanced switches, that must be configured to use.

Managed Network

Network that is monitored by the SNMP protocol consisting of SNMP managed devices, Management Information Base (MIB) items, and SNMP manager(s).

Managed Switch

See Managed Device.

Management Information Base (MIB)

SNMP's version of a server. *See* Simple Network Management Protocol (SNMP).

Mandatory Access Control (MAC)

A security model in which every resource is assigned a label that defines its security level. If the user lacks that security level, they do not get access.

Mantrap

An entryway with two successive locked doors and a small space between them providing one-way entry or exit. This is a security measure taken to prevent tailgating.

Manual Tunnel

A simple point-to-point connection between two IPv6 networks. As a tunnel, it uses IPsec encryption.

Material Safety Data Sheet (MSDS)

Document that describes the safe handling procedures for any potentially hazardous, toxic, or unsafe material.

Maximum Transmission Unit (MTU)

Specifies the largest size of a data unit in a communications protocol, such as Ethernet.

MB (Megabyte)

1,048,576 bytes.

MD5 (Message-Digest Algorithm Version 5)

Arguably the most popular hashing function.

Mechanical Transfer Registered Jack (MT-RJ)

The first type of Small Form Factor (SFF) fiber connector, still in common use.

Media Access Control (MAC)

The part of a NIC that remembers the NIC's own MAC address and attaches that address to outgoing frames.

Media Converter

A device that lets you interconnect different types of Ethernet cable.

Media Gateway Control Protocol (MGCP)

A protocol that is designed to be a complete VoIP or video presentation connection and session controller. MGCP TCP uses ports 2427 and 2727.

Medianet

A network of far-flung routers and servers that provides sufficient bandwidth for video teleconferencing (VTC) via quality of service (QoS) and other tools.

Mega-

A prefix that usually stands for the binary quantity 1,048,576. One megabyte is 1,048,576 bytes. One megahertz, however, is 1,000,000 hertz. Sometimes shortened to *meg*, as in "a 286 has an address space of 16 megs."

Memorandum of Understanding (MOU)

A document that defines an agreement between two parties in situations where a legal contract is not appropriate.

Mesh Topology

Topology in which each computer has a direct or indirect connection to every other computer in a network. Any node on the network can forward traffic to other nodes. Popular in cellular and many wireless networks.

Metasploit

A unique tool that enables a penetration tester to use a massive library of attacks as well as tweak those attacks for unique penetrations.

Metric

Relative value that defines the "cost" of using a particular route.

Metro Ethernet

A metropolitan area network (MAN) based on the Ethernet standard.

Metropolitan Area Network (MAN)

Multiple computers connected via cabling, radio, leased phone lines, or infrared that are within the same city. A perfect example of a MAN is the Tennessee city Chattanooga's gigabit network available to all citizens, the Chattanooga Gig.

MHz (Megahertz)

A unit of measure that equals a frequency of 1 million cycles per second.

Microsoft Baseline Security Analyzer (MBSA)

Microsoft-designed tool to test individual Windows-based PCs for vulnerabilities.

MIME (Multipurpose Internet Mail Extensions)

A standard for attaching binary files, such as executables and images, to the Internet's text-based mail (24-Kbps packet size).

Miredo

An open source implementation of Teredo for Linux and some other UNIX-based systems. It is a NAT-traversal IPv6 tunneling protocol.

Mirroring

Also called *drive mirroring*, reading and writing data at the same time to two drives for fault-tolerance purposes. Considered RAID level 1.

Mixed Mode

Also called *high-throughput*, or *802.11a-ht/802.11g-ht*, one of three modes used with 802.11n wireless networks wherein the wireless access point (WAP) sends special packets that support older standards yet can also improve the speed of those standards via 802.

Modal Distortion

A light distortion problem unique to multimode fiber-optic cable.

Model

A simplified representation of a real object or process. In the case of networking, models represent logical tasks and subtasks that are required to perform network communication.

Modem (Modulator-Demodulator)

A device that converts both digital bit streams into analog signals (modulation) and incoming analog signals back into digital signals (demodulation). Most commonly used to interconnect telephone lines to computers.

Modulation Techniques

The various multiplexing and demultiplexing technologies and protocols, both analog and digital.

Modulator-Demodulator (Modem)

See Modem (Modulator-Demodulator).

Monlist

A query that asks the NTP server about the traffic going on between itself and peers.

Mounting Bracket

Bracket that acts as a holder for a faceplate in cable installations.

MS-CHAP

Microsoft's dominant variation of the CHAP protocol, uses a slightly more advanced encryption protocol.

MTU (Maximum Transmission Unit)

See Maximum Transmission Unit (MTU).

MTU Black Hole

When a router's firewall features block ICMP requests, making MTU worthless.

MTU Mismatch

The situation when your network's packets are so large that they must be fragmented to fit into your ISP's packets.

Multicast

Method of sending a packet in which the sending computer sends it to a group of interested computers.

Multicast Addresses

A set of reserved addresses designed to go from one system to any system using one of the reserved addresses.

Multifactor Authentication

A form of authentication where a user must use two or more factors to prove his or her identity.

Multilayer Switch

A switch that has functions that operates at multiple layers of the OSI seven-layer model.

Multilink PPP

A communications protocol that logically joins multiple PPP connections, such as a modem connection, to aggregate the throughput of the links.

Multimeter

A tool for testing voltage (AC and DC), resistance, and continuity.

Multimode

Type of fiber-optic cable with a large-diameter core that supports multiple modes of propagation. The large diameter simplifies connections, but has drawbacks related to distance.

Multimode Fiber (MMF)

Type of fiber-optic cable that uses LEDs.

Multiple In/Multiple Out (MIMO)

A feature in 802.11 WAPs that enables them to make multiple simultaneous connections.

Multiplexer

A device that merges information from multiple input channels to a single output channel.

Multiprotocol Label Switching (MPLS)

A router feature that labels certain data to use a desired connection. It works with any type of packet switching (even Ethernet) to force certain types of data to use a certain path.

Multisource Agreement (MSA)

A document that details the interoperability of network hardware from a variety of manufacturers.

MX Records

Records within DNS servers that are used by SMTP servers to determine where to send mail.

My Traceroute (mtr)

Terminal command in Linux that dynamically displays the route a packet is taking. Similar to traceroute.

Name Resolution

A method that enables one computer on the network to locate another to establish a session. All network protocols perform name resolution in one of two ways: either via *broadcast* or by providing some form of *name server*.

Name Server

A computer whose job is to know the name of every other computer on the network.

NAT (Network Address Translation)

See Network Address Translation (NAT).

NAT Translation Table

Special database in a NAT router that stores destination IP addresses and ephemeral source ports from outgoing packets and compares them against returning packets.

Native VLAN

The specified VLAN designation that will be assigned to all untagged frames entering a trunk port in a switch.

nbtstat

A command-line utility used to check the current NetBIOS name cache on a particular machine. The utility compares NetBIOS names to their corresponding IP addresses.

Near-End Crosstalk (NEXT)

Crosstalk at the same end of a cable from which the signal is being generated.

Nessus

Popular and extremely comprehensive vulnerability testing tool.

NetBEUI (NetBIOS Extended User Interface)

Microsoft's first networking protocol, designed to work with NetBIOS. NetBEUI is long obsolesced by TCP/IP. NetBEUI did not support routing.

NetBIOS (Network Basic Input/Output System)

A protocol that operates at the Session layer of the OSI seven-layer model. This protocol creates and manages connections based on the names of the computers involved.

NetBIOS Name

A computer name that identifies both the specific machine and the functions that machine performs. A NetBIOS name consists of 16 characters: the first 15 are an alphanumeric name, and the 16th is a special suffix that identifies the role the machine plays.

NetBIOS over TCP/IP (NetBT)

A Microsoft-created protocol that enabled NetBIOS naming information to be transported over TCP/IP networks. The result is that Microsoft naming services can operate on a TCP/IP network without the need for DNS services.

NetFlow

The primary tool used to monitor packet flow on a network.

NetFlow Collector

Component process of NetFlow that captures and saves data from a NetFlow-enabled device's cache for future NetFlow analysis.

netstat

A universal command-line utility used to examine the TCP/IP connections open on a given host.

Network

A collection of two or more devices interconnected by telephone lines, coaxial cables, satellite links, radio, and/or some other communication technique. A computer *network* is a group of computers that are connected together and communicate with one another for a common purpose. Computer networks support "people and organization" networks, users who also share a common purpose for communicating.

Network Access Control (NAC)

Control over information, people, access, machines, and everything in between.

Network Access Policy

Rules that define who can access the network, how it can be accessed, and what resources of the network can be used.

Network Access Server (NAS)

Systems that control the modems in a RADIUS network.

Network Address Translation (NAT)

A means of translating a system's IP address into another IP address before sending it out to a larger network. NAT manifests itself by a NAT program that runs on a system or a router. A network using NAT provides the systems on the network with private IP addresses. The system running the NAT software has two interfaces: one connected to the network and the other connected to the larger network.

The NAT program takes packets from the client systems bound for the larger network and translates their internal private IP addresses to its own public IP address, enabling many systems to share a single IP address.

Network Appliance

Feature-packed network box that incorporates numerous processes such as routing, Network Address Translation (NAT), switching, intrusion detection systems, firewall, and more.

Network as a Service (NaaS)

The act of renting virtual server space over the Internet. *See also* Cloud Computing.

Network Attached Storage (NAS)

A dedicated file server that has its own file system and typically uses hardware and software designed for serving and storing files.

Network Blocks

Also called blocks, contiguous ranges of IP addresses that are assigned to organizations and end users by IANA.

Network Closet

An equipment room that holds servers, switches, routers, and other network gear.

Network Design

The process of gathering together and planning the layout for the equipment needed to create a network.

Network Diagram

An illustration that shows devices on a network and how they connect.

Network ID

A number used in IP networks to identify the network on which a device or machine exists.

Network Interface

A device by which a system accesses a network. In most cases, this is a NIC or a modem.

Network Interface Card (NIC)

Traditionally, an expansion card that enables a PC to link physically to a network. Modern computers now use built-in NICs, no longer requiring physical cards, but the term "NIC" is still very common.

Network Interface Unit (NIU)

Another name for a demarc. *See* Demarc.

Network Layer

Layer 3 of the OSI seven-layer model. *See also* Open Systems Interconnection (OSI) Seven-Layer Model.

Network Management Software (NMS)

Tools that enable you to describe, visualize, and configure an entire network.

Network Management Station (NMS)

SNMP console computer that runs the SNMP manager software.

Network Map

A highly detailed illustration of a network, down to the individual computers. A network map will show IP addresses, ports, protocols, and more.

Network Name

Another name for the SSID.

Network Operations Center (NOC)

A centralized location for techs and administrators to manage all aspects of a network.

Network Protocol

Special software that exists in every network-capable operating system that acts to create unique identifiers for each system. It also creates a set of communication rules for issues like how to handle data chopped up into multiple packets and how to deal with routers. TCP/IP is the dominant network protocol today.

Network Share

A shared resource on a network.

Network Technology

The techniques, components, and practices involved in creating and operating computer-to-computer links.

Network Threat

Any number of things that share one essential feature: the potential to damage network data, machines, or users.

Network Time Protocol (NTP)

Protocol that gives the current time.

Network Topology

Refers to the way that cables and other pieces of hardware connect to one another.

Network-Based Anti-Malware

A single source server that holds current anti-malware software. Multiple systems can access and run the software from that server. The single site makes the software easier to update and administer than anti-malware installed on individual systems.

Network-Based Firewall

Firewall, perhaps implemented in a gateway router or as a proxy server, through which all network traffic must pass inspection to be allowed or blocked.

Newsgroup

The name for a discussion group on Usenet.

Next Hop

The next router a packet should go to at any given point.

NFS (Network File System)

A TCP/IP file system–sharing protocol that enables systems to treat files on a remote machine as though they were local files. NFS uses TCP port 2049, but many users choose alternative port numbers. Though still somewhat popular and heavily supported, NFS has been largely replaced by Samba/CIFS. *See also* Samba *and* Common Internet File System (CIFS).

NIC Teaming

Connecting multiple NICs in tandem to increase bandwidth in smaller increments. *See also* link aggregation.

Nmap

A network utility designed to scan a network and create a map. Frequently used as a vulnerability scanner.

Node

A member of a network or a point where one or more functional units interconnect transmission lines.

Noise

Undesirable signals bearing no desired information and frequently capable of introducing errors into the communication process.

Non-Discovery Mode

A setting for Bluetooth devices that effectively hides them from other Bluetooth devices.

Non-Persistent Agent

Software used in posture assessment that does not stay resident in client station memory. It is executed prior to login and may stay resident during the login session but is removed from client RAM when the login or session is complete. The agent presents the security characteristics to the access control server, which then decides to allow, deny, or redirect the connection.

Nonrepudiation

The process of making sure data came from the person or entity it was supposed to come from.

Normal Backup

A full backup of every selected file on a system. This type of backup turns off the archive bit after the backup.

Ns (Nanosecond)

A billionth of a second. Light travels a little over 11 inches in 1 ns.

NS Records

Records that list the DNS servers for a Web site.

nslookup

A once handy tool that advanced techs used to query the functions of DNS servers. Most public DNS servers now ignore all but the most basic nslookup queries.

NTFS (NT File System)

A file system for hard drives that enables object-level security, long filename support, compression, and encryption. NTFS 4.0 debuted with Windows NT 4.0. Later Windows versions continue to update NTFS.

NTFS Permissions

Groupings of what Microsoft calls special permissions that have names like Execute, Read, and Write, and that allow or disallow users certain access to files.

NTLDR

A Windows NT/2000/XP/2003 boot file. Launched by the MBR or MFT, NTLDR looks at the BOOT.INI configuration file for any installed operating systems.

ntpdc

A command that puts the NTP server into interactive mode in order to submit queries.

Object

A group of related counters used in Windows logging utilities.

OEM (Original Equipment Manufacturer)

Contrary to the name, does not create original hardware, but rather purchases components from manufacturers and puts them together in systems under its own brand name. Dell, Inc. and Gateway, Inc., for example, are for the most part OEMs. Apple, Inc., which manufactures most of the components for its own Mac-branded machines, is not an OEM. Also known as *VARs (value-added resellers).*

Offsite

The term for a virtual computer accessed and stored remotely.

Ohm Rating

Electronic measurement of a cable's or an electronic component's impedance.

Onsite

The term for a virtual computer stored at your location.

Open Port

See Listening Port.

Open Shortest Path First (OSPF)

An interior gateway routing protocol developed for IP networks based on the *shortest path first* or *link state algorithm*.

Open Source

Applications and operating systems that offer access to their source code; this enables developers to modify applications and operating systems easily to meet their specific needs.

Open Systems Interconnection (OSI)

An international standard suite of protocols defined by the International Organization for Standardization (ISO) that implements the OSI seven-layer model for network communications between computers.

Open Systems Interconnection (OSI) Seven-Layer Model

An architecture model based on the OSI protocol suite, which defines and standardizes the flow of data between computers. The following lists the seven layers:

- **Layer 1** The *Physical layer* defines hardware connections and turns binary into physical pulses (electrical or light). Repeaters and hubs operate at the Physical layer.
- **Layer 2** The *Data Link layer* identifies devices on the Physical layer. MAC addresses are part of the Data Link layer. Bridges operate at the Data Link layer.
- **Layer 3** The *Network layer* moves packets between computers on different networks. Routers operate at the Network layer. IP and IPX operate at the Network layer.
- **Layer 4** The *Transport layer* breaks data down into manageable chunks. TCP, UDP, SPX, and NetBEUI operate at the Transport layer.
- **Layer 5** The *Session layer* manages connections between machines. NetBIOS and Sockets operate at the Session layer.
- **Layer 6** The *Presentation layer*, which can also manage data encryption, hides the differences among various types of computer systems.
- **Layer 7** The *Application layer* provides tools for programs to use to access the network (and the lower layers). HTTP, FTP, SMTP, and POP3 are all examples of protocols that operate at the Application layer.

OpenSSH

A series of secure programs developed by the OpenBSD organization to fix SSH's limitation of only being able to handle one session per tunnel.

Operating System (OS)

The set of programming that enables a program to interact with the computer and provides an interface between the PC and the user. Examples are Microsoft Windows 10, Apple Mac OS X, and SUSE Linux.

Operator

In a distributed control system, the operator is a human who runs the computer-controlled resources through a human machine interface. *See also* Human Machine Interface (HMI).

Optical Carrier (OC)

Specification used to denote the optical data carrying capacity (in Mbps) of fiber-optic cables in networks conforming to the SONET standard. The OC standard is an escalating series of speeds, designed to meet the needs of medium-to-large corporations. SONET establishes OCs from 51.8 Mbps (OC-1) to 39.8 Gbps (OC-768).

Optical Power Meter

Device that measures light intensity of light pulses within or at the terminal ends of fiber-optic cables.

Optical Time Domain Reflectometer (OTDR)

Tester for fiber optic cable that determines continuity and reports the location of cable breaks.

Organizationally Unique Identifier (OUI)

The first 24 bits of a MAC address, assigned to the NIC manufacturer by the IEEE.

Orthogonal Frequency-Division Multiplexing (OFDM)

A spread-spectrum broadcasting method that combines the multiple frequencies of DSSS with FHSS's hopping capability.

OS (Operating System)

See Operating System (OS).

Oscilloscope

A device that gives a graphical/visual representation of signal levels over a period of time.

OSPF (Open Shortest Path First)

See Open Shortest Path First (OSPF).

Out-of-Band Management

Method to connect to and administer a managed device such as a switch or router that does not use a standard network-connected host as the administrative console. A computer connected to the console port of a switch is an example of out-of-band management.

Outbound Traffic

Packets leaving the network from within it.

Overlay Tunnel

Enables two IPv6 networks to connect over an IPv4 network by encapsulating the IPv6 packets within IPv4 headers, transporting them across the IPv4 network, then de-encapsulating the IPv6 data.

Packet

Basic component of communication over a network. A group of bits of fixed maximum size and well-defined format that is switched and transmitted as a complete whole through a network. It contains source and destination address, data, and control information. *See also* Frame.

Packet Analyzer

A program that reads the capture files from packet sniffers and analyzes them based on monitoring needs.

Packet Filtering

A mechanism that blocks any incoming or outgoing packet from a particular IP address or range of IP addresses. Also known as *IP filtering*.

Packet Sniffer

A tool that intercepts and logs network packets.

Pad

Extra data added to an Ethernet frame to bring the data up to the minimum required size of 64 bytes.

Partially Meshed Topology

A mesh topology in which not all of the nodes are directly connected.

Passive Optical Network (PON)

A fiber architecture that uses a single fiber to the neighborhood switch and then individual fiber runs to each final destination.

Password

A series of characters that enables a user to gain access to a file, a folder, a PC, or a program.

Password Authentication Protocol (PAP)

The oldest and most basic form of authentication and also the least safe because it sends all passwords in cleartext.

Patch Cables

Short (2 to 5 foot) UTP cables that connect patch panels to switches.

Patch Panel

A panel containing a row of female connectors (ports) that terminate the horizontal cabling in the equipment room. Patch panels facilitate cabling organization and provide protection to horizontal cabling.

Path MTU Discovery (PMTU)

A method for determining the best MTU setting that works by adding a new feature called the "Don't Fragment (DF) flag" to the IP packet.

pathping

Command-line tool that combines the features of the ping command and the tracert/traceroute commands.

Payload

The primary data that is sent from a source network device to a destination network device.

PBX (Private Branch Exchange)

A private phone system used within an organization.

Peer-to-Peer

A network in which each machine can act as either a client or a server.

Peer-to-Peer Mode

See Ad Hoc Mode.

Penetration Testing (pentest)

An authorized, network hacking process that will identify real world weaknesses in network security and document the findings.

Performance Monitor (PerfMon)

The Windows logging utility.

Peripherals

Noncomputer devices on a network; for example, fax machines, printers, or scanners.

Permanent DoS (PDoS)

An attack that damages a targeted machine, such as a router or server, and renders that machine inoperable.

Permissions

Sets of attributes that network administrators assign to users and groups that define what they can do to resources.

Persistent Connection

A connection to a shared folder or drive that the computer immediately reconnects to at logon.

Personal Area Network (PAN)

The network created among Bluetooth devices such as smartphones, tablets, printers, keyboards, mice, and so on.

Phishing

A social engineering technique where the attacker poses as a trusted source in order to obtain sensitive information.

Physical Address

An address burned into a ROM chip on a NIC. A MAC address is an example of a physical address.

Physical Contact (PC) Connector

Family of fiber-optic connectors that enforces direct physical contact between two optical fibers being connected.

Physical Layer

See Open Systems Interconnection (OSI) Seven-Layer Model.

Physical Network Diagram

A document that shows all of the physical connections on a network. Cabling type, protocol, and speed are also listed for each connection.

Physical Topology

The manner in which the physical components of a network are arranged.

ping (Packet Internet Groper)

A small network message sent by a computer to check for the presence and response of another system. A ping uses ICMP packets. *See also* Internet Control Message Protocol (ICMP).

Path MTU Discovery (PMTU)

A method for determining the best MTU setting that works by adding a new feature called the "Don't Fragment (DF) flag" to the IP packet.

ping -6

Ping is a command-line utility to check the "up/down" status of an IP addressed host. The "-6" switch included on the command-line, using the Windows version of ping, specifies that the host under test has an IPv6 address.

ping6

Linux command-line utility specifically designed to ping hosts with an IPv6 address.

Plain Old Telephone Service (POTS)

See Public Switched Telephone Network (PSTN).

Plaintext

Also called *cleartext*, unencrypted data in an accessible format that can be read without special utilities.

Platform

Hardware environment that supports the running of a computer system.

Platform as a Service (PaaS)

A complete deployment and management system that gives programmers all the tools they need to administer and maintain a Web application.

Plenum

Usually a space between a building's false ceiling and the floor above it. Most of the wiring for networks is located in this space. Plenum is also a fire rating for network cabling.

Point Coordination Function (PCF)

A method of collision avoidance defined by the 802.11 standard but has yet to be implemented. *See also* Distributed Coordination Function (DCF).

Point-to-Multipoint Topology

Topology in which one device communicates with more than one other device on a network.

Point-to-Point Topology

Network topology in which two computers are directly connected to each other without any other intervening connection components such as hubs or switches.

Point-to-Point Protocol (PPP)

A protocol that enables a computer to connect to the Internet through a dial-in connection and to enjoy most of the benefits of a direct connection. PPP is considered to be superior to SLIP because of its error detection and data compression features, which SLIP lacks, and the capability to use dynamic IP addresses.

Point-to-Point Protocol over Ethernet (PPPoE)

A protocol that was originally designed to encapsulate PPP frames into Ethernet frames. Used by DSL providers to force customers to log into their DSL connections instead of simply connecting automatically.

Point-to-Point Topology

A network of two single devices communicating with each other.

Point-to-Point Tunneling Protocol (PPTP)

A protocol that works with PPP to provide a secure data link between computers using encryption.

Pointer Record (PTR)

A record that points IP addresses to host names. *See also* Reverse Lookup Zone.

Polyvinyl Chloride (PVC)

A material used for the outside insulation and jacketing of most cables. Also a fire rating for a type of cable that has no significant fire protection.

Port (Physical Connector)

In general, the portion of a computer through which a peripheral device may communicate, such as video, USB, serial, and network ports. In the context of networking, the jacks found in computers, switches, routers, and network-enabled peripherals into which network cables are plugged.

Port (Logical Connection)

In TCP/IP, 16-bit numbers between 0 and 65535 assigned to a particular TCP/IP process or application. For example, Web servers use port 80 (HTTP) to transfer Web pages to clients. The first 1024 ports are called *well-known ports*. They have been pre-assigned and generally refer to TCP/IP processes and applications that have been around for a long time.

Port Address Translation (PAT)

The most commonly used form of Network Address Translation, where the NAT uses the outgoing IP addresses and port numbers (collectively known as a socket) to map traffic from specific machines in the network. *See also* Network Address Translation.

Port Authentication

Function of many advanced networking devices that authenticates a connecting device at the point of connection.

Port Blocking

Preventing the passage of any TCP segments or UDP datagrams through any ports other than the ones prescribed by the system administrator.

Port Bonding

The logical joining of multiple redundant ports and links between two network devices such as a switch and storage array.

Port Filtering

See Port Blocking.

Port Forwarding

Preventing the passage of any IP packets through any ports other than the ones prescribed by the system administrator.

Port Mirroring

The capability of many advanced switches to mirror data from any or all physical ports on a switch to a single physical port. Useful for any type of situation where an administrator needs to inspect packets coming to or from certain computers.

Port Number

Number used to identify the requested service (such as SMTP or FTP) when connecting to a TCP/IP host. Some example port numbers include 80 (HTTP), 20 (FTP), 69 (TFTP), 25 (SMTP), and 110 (POP3).

Port Scanner

A program that probes ports on another system, logging the state of the scanned ports.

Post Office Protocol Version 3 (POP3)

One of the two protocols that receive e-mail from SMTP servers. POP3 uses TCP port 110. While historically most e-mail clients use this protocol, the IMAP4 email protocol is now more common.

PostScript

A language defined by Adobe Systems, Inc., for describing how to create an image on a page. The description is independent of the resolution of the device that will create the image. It includes a technology for defining the shape of a font and creating a raster image at many different resolutions and sizes.

Posture Assessment

Process by which a client presents its security characteristics via an agent or agent-less interface to an access control server. The server checks the characteristics and decides whether to grant a connection, deny a connection, or redirect the connection depending on the security compliance invoked.

Power Converter

Device that changes AC power to DC power.

Power over Ethernet (PoE)

A standard that enables wireless access points (WAPs) to receive their power from the same Ethernet cables that transfer their data.

Power Redundancy

Secondary source of power in the event that primary power fails. The most common redundant power source is an uninterruptible power supply (UPS).

Power Users

A user account that has the capability to do many, but not all, of the basic administrator functions.

PPP (Point-to-Point Protocol)

See Point-to-Point Protocol (PPP).

PPPoE (PPP over Ethernet)

See Point-to-Point Protocol over Ethernet (PPPoE).

Preamble

A 64-bit series of alternating 1s and 0s, ending with 11, that begins every Ethernet frame. The preamble gives a receiving NIC time to realize a frame is coming and to know exactly where the frame starts.

Prefix Delegation

An IPv6 router configuration that enables it to request an IPv6 address block from an upstream source, then to disseminate it to local clients.

Presentation Layer

See Open Systems Interconnection (OSI) Seven-Layer Model.

Primary Lookup Zone

A *forward lookup zone* stored in a text file. *See also* Forward Lookup Zone.

Primary Zone

A *forward lookup zone* that is managed within and by the authoritative DNS server for that zone.

Primary Rate Interface (PRI)

A type of ISDN that is actually just a full T1 line carrying 23 B channels.

Private Cloud

Software, platforms, and infrastructure that are delivered via the Internet and are made available to the general public.

Private Port Numbers

See Dynamic Port Numbers.

Program

A set of actions or instructions that a machine is capable of interpreting and executing. Used as a verb, it means to design, write, and test such instructions.

Programmable Logic Controller (PLC)

A computer that controls a machine according to a set of ordered steps.

Promiscuous Mode

A mode of operation for a NIC in which the NIC processes all frames that it sees on the cable.

Prompt

A character or message provided by an operating system or program to indicate that it is ready to accept input.

Proprietary

Term used to describe technology that is unique to, and owned by, a particular vendor.

Protected Extensible Authentication Protocol (PEAP)

An authentication protocol that uses a password function based on MS-CHAPv2 with the addition of an encrypted TLS tunnel similar to *EAP-TLS*.

Protocol

An agreement that governs the procedures used to exchange information between cooperating entities; usually includes how much information is to be sent, how often it is sent, how to recover from transmission errors, and who is to receive the information.

Protocol Analyzer

A tool that monitors the different protocols running at different layers on the network and that can give Application, Session, Network, and Data Link layer information on every frame going through a network.

Protocol Data Unit (PDU)

Specialized type of command and control packet found in SNMP management systems (and others).

Protocol Stack

The actual software that implements the protocol suite on a particular operating system.

Protocol Suite

A set of protocols that are commonly used together and operate at different levels of the OSI seven-layer model.

Proximity Reader

Sensor that detects and reads a token that comes within range. The polled information is used to determine the access level of the person carrying the token.

Proxy ARP

The process of making remotely connected computers act as though they are on the same LAN as local computers.

Proxy Server

A device that fetches Internet resources for a client without exposing that client directly to the Internet. Most proxy servers accept requests for HTTP, FTP, POP3, and SMTP resources. The proxy server often caches, or stores, a copy of the requested resource for later use.

PSTN (Public Switched Telephone Network)

See Public Switched Telephone Network (PSTN).

Public-Key Cryptography

A method of encryption and decryption that uses two different keys: a public key for encryption and a private key for decryption.

Public-Key Infrastructure (PKI)

The system for creating and distributing digital certificates using sites like VeriSign, Thawte, or GoDaddy.

Public Cloud

Software, platforms, and infrastructure delivered through networks that the general public can use.

Public Switched Telephone Network (PSTN)

Also known as *Plain Old Telephone Service (POTS)*. The most common type of phone connection, which takes your sounds, translated into an analog waveform by the microphone, and transmits them to another phone.

Punchdown Tool

A specialized tool for connecting UTP wires to a 110-block.

Quality of Service (QoS)

Policies that control how much bandwidth a protocol, PC, user, VLAN, or IP address may use.

Quarantine Network

Safe network to which are directed stations that either do not require or should not have access to protected resources.

Raceway

Cable organizing device that adheres to walls, making for a much simpler, though less neat, installation than running cables in the walls.

Rack Monitoring System

Set of sensors in an equipment closet or rack-mounted gear that can monitor and alert when an out-of-tolerance condition occurs in power, temperature, and/or other environmental aspects.

Radio Frequency Interference (RFI)

The phenomenon where a Wi-Fi signal is disrupted by a radio signal from another device.

Radio Grade (RG) Ratings

Ratings developed by the U.S. military to provide a quick reference for the different types of coaxial cables.

RADIUS Server

A system that enables remote users to connect to a network service.

Real-Time Processing

The processing of transactions as they occur, rather than batching them. Pertaining to an application, processing in which response to input is fast enough to affect subsequent inputs and guide the process, and in which records are updated immediately. The lag from input time to output time must be sufficiently small for acceptable timeliness. Timeliness is a function of the total system: missile guidance requires output within a few milliseconds of input, whereas scheduling of steamships requires a response time in days. Real-time systems are those with a response time of milliseconds; interactive systems respond in seconds; and batch systems may respond in hours or days.

Real-Time Transport Protocol (RTP)

Protocol that defines the type of packets used on the Internet to move voice or data from a server to clients. The vast majority of VoIP solutions available today use RTP.

Real-Time Video

Communication that offers both audio and video via unicast messages.

Recovery Point Objective (RPO)

The state of the backup when the data is recovered. It is an evaluation of how much data is lost from the time of the last backup to the point that a recovery was required.

Recovery Time Objective (RTO)

The amount of time needed to restore full functionality from when the organization ceases to function.

Reddit Effect

The massive influx of traffic on a small or lesser-known Web site when it is suddenly made popular by a reference from the media. *See also* Slashdotting.

Redundant Array of Independent [or Inexpensive] Devices [or Disks] (RAID)

A way to create a fault-tolerant storage system. RAID has six levels. Level 0 uses byte-level striping and provides no fault tolerance. Level 1 uses mirroring or duplexing. Level 2 uses bit-level striping. Level 3 stores error-correcting information (such as parity) on a separate disk and data striping on the remaining drives. Level 4 is level 3 with block-level striping. Level 5 uses block-level and parity data striping.

Reflection

Used in DDoS attacks, requests are sent to normal servers as if they had come from the target server. The response from the normal servers are reflected to the target server, overwhelming it without identifying the true initiator.

Reflective DDoS

See Reflection.

REGEDIT.EXE

A program used to edit the Windows registry.

Regional Internet Registries (RIRs)

Entities under the oversight of the Internet Assigned Numbers Authority (IANA), which parcels out IP addresses.

Registered Ports

Port numbers from 1024 to 49151. The IANA assigns these ports for anyone to use for their applications.

Regulations

Rules of law or policy that govern behavior in the workplace, such as what to do when a particular event occurs.

Remote

Refers to the computer(s), server(s), and/or LAN that cannot be physically used due to its distance from the user.

Remote Access

The capability to access a computer from outside a building in which it is housed. Remote access requires communications hardware, software, and actual physical links.

Remote Access Server (RAS)

Refers to both the hardware component (servers built to handle the unique stresses of a large number of clients calling in) and the software component (programs that work with the operating system to allow remote access to the network) of a remote access solution.

Remote Authentication Dial-In User Service (RADIUS)

An AAA standard created to support ISPs with hundreds if not thousands of modems in hundreds of computers to connect to a single central database. RADIUS consists of three devices: the RADIUS server that has access to a database of user names and passwords, a number of network access servers (NASs) that control the modems, and a group of systems that dial into the network.

Remote Copy Protocol (RCP)

Provides the capability to copy files to and from the remote server without the need to resort to FTP or Network File System (NFS, a UNIX form of folder sharing). RCP can also be used in scripts and shares TCP port 514 with RSH.

Remote Desktop Protocol (RDP)

A Microsoft-created remote terminal protocol.

Remote Installation Services (RIS)

A tool introduced with Windows 2000 that can be used to initiate either a scripted installation or an installation of an image of an operating system onto a PC.

Remote Login (rlogin)

Program in UNIX that enables you to log into a server remotely. Unlike Telnet, rlogin can be configured to log in automatically.

Remote Shell (RSH)

Allows you to send single commands to the remote server. Whereas rlogin is designed to be used interactively, RSH can be easily integrated into a script.

Remote Terminal

A connection on a faraway computer that enables you to control that computer as if you were sitting in front of it and logged in. Remote terminal programs all require a server and a client. The server is the computer to be controlled. The client is the computer from which you do the controlling.

Remote Terminal Unit (RTU)

In a SCADA environment, has the same functions as a controller plus additional autonomy to deal with connection loss. It is also designed to take advantage of some form of long distance communication.

Repeater

A device that takes all of the frames it receives on one Ethernet segment and re-creates them on another Ethernet segment. Repeaters operate at Layer 1 (Physical) of the OSI seven-layer model. They do not check the integrity of the Layer 2 (Data Link) frame so they may repeat incorrectly formed frames. They were replaced in the early 80s by bridges which perform frame integrity checking before repeating a frame.

Replication

A process where multiple computers might share complete copies of a database and constantly update each other.

Resistance

The tendency for a physical medium to impede electron flow. It is classically measured in a unit called *ohms*. *See also* Impedance.

Resource

Anything that exists on another computer that a person wants to use without going to that computer. Also an online information set or an online interactive option. An online library catalog and the local school lunch menu are examples of information sets. Online menus or graphical user interfaces, Internet e-mail, online conferences, Telnet, FTP, and Gopher are examples of interactive options.

Response

Answer from an agent upon receiving a Get protocol data unit (PDU) from an SNMP manager.

Reverse Lookup Zone

A DNS setting that resolves IP addresses to FQDNs. In other words, it does exactly the reverse of what DNS normally accomplishes using forward lookup zones.

RF Emanation

The transmission, intended or unintended, of radio frequencies. These transmissions may come from components that are intended to transmit RF, such as a Wi-Fi network card, or something less expected, such as a motherboard or keyboard. These emanations may be detected and intercepted, posing a potential threat to security.

RG-58

A grade of small-diameter coaxial cable used in 10Base2 Ethernet networks. RG-58 has a characteristic impedance of 50 ohms.

Ring Topology

A network topology in which all the computers on the network attach to a central ring of cable.

RIP (Routing Information Protocol)

See Routing Information Protocol (RIP).

RIPv1

The first version of RIP, which had several shortcomings, such as a maximum hop count of 15 and a routing table update interval of 30 seconds, which was a problem because every router on a network would send out its table at the same time.

RIPv2

The last version of RIP. It fixed many problems of RIPv1, but the maximum hop count of 15 still applies.

Riser

Fire rating that designates the proper cabling to use for vertical runs between floors of a building.

Risk Management

The process of how organizations evaluate, protect, and recover from threats and attacks that take place on their networks.

Rivest Cipher 4 (RC4)

A popular streaming symmetric-key algorithm.

Rivest Shamir Adleman (RSA)

An improved asymmetric cryptography algorithm that enables secure digital signatures.

RJ (Registered Jack)

Connectors used for UTP cable on both telephone and network connections.

RJ-11

Type of connector with four-wire UTP connections; usually found in telephone connections.

RJ-45

Type of connector with eight-wire UTP connections; usually found in network connections and used for 10/100/1000BaseT networking.

RJ-45 Connector

Network connector that conforms to the RJ-45 standard. *See also* RJ-45.

Roaming

A process where clients seamlessly change wireless access point (WAP) connections, depending on whichever WAP has the strongest signal covered by the broadcast area.

Rogue Access Point (Rouge AP)

An unauthorized wireless access point (WAP) installed in a computer network.

Role-Based Access Control (RBAC)

The most popular authentication model used in file sharing, defines a user's access to a resource based on the roles the user plays in the network environment. This leads to the idea of creation of groups. A group in most networks is nothing more than a name that has clearly defined accesses to different resources. User accounts are placed into various groups.

ROM (Read-Only Memory)

The generic term for nonvolatile memory that can be read from but not written to. This means that code and data stored in ROM cannot be corrupted by accidental erasure. Additionally, ROM retains its data when power is removed, which makes it the perfect medium for storing BIOS data or information such as scientific constants.

Root Directory

The directory that contains all other directories.

Rootkit

A Trojan horse that takes advantage of very low-level operating system functions to hide itself from all but the most aggressive of anti-malware tools.

route

A command that enables a user to display and edit the local system's routing table.

Route Redistribution

Occurs in a multiprotocol router. A multiprotocol router learns route information using one routing protocol and disseminates that information using another routing protocol.

Router

A device that connects separate networks and forwards a packet from one network to another based only on the network address for the protocol being used. For example, an IP router looks only at the IP network number. Routers operate at Layer 3 (Network) of the OSI seven-layer model.

Routing and Remote Access Service (RRAS)

A special remote access server program, originally only available on Windows Server, on which a PPTP endpoint is placed in Microsoft networks.

Routing Information Protocol (RIP)

Distance vector routing protocol that dates from the 1980s.

Routing Loop

A situation where interconnected routers loop traffic, causing the routers to respond slowly or not respond at all.

Routing Table

A list of paths to various networks required by routers. This table can be built either manually or automatically.

RS-232

The recommended standard (RS) upon which all serial communication takes place on a PC.

Run

A single piece of installed horizontal cabling.

Samba

An application that enables UNIX systems to communicate using Server Message Blocks (SMBs). This, in turn, enables them to act as Microsoft clients and servers on the network.

SC Connector

Fiber-optic connector used to terminate single-mode and multi-mode fiber. It is characterized by its push-pull, snap mechanical coupling, known as “stick and click. Commonly referred to as Subscriber Connector, Standard Connector and sometimes, square connector.

Scalability

The capability to support network growth.

Scanner

A device that senses alterations of light and dark. It enables the user to import photographs, other physical images, and text into the computer in digital form.

Secondary Lookup Zone

A backup lookup zone stored on another DNS server. *See also* Forward Lookup Zone.

Secondary Zone

A backup of a primary zone. It is used to provide fault tolerance and load balancing. It gets its information from the primary zone and is considered authoritative. *See also* Primary Zone.

Secure Copy Protocol (SCP)

One of the first SSH-enabled programs to appear after the introduction of SSH. SCP was one of the first protocols used to transfer data securely between two hosts and thus might have replaced FTP. SCP works well but lacks features such as a directory listing.

Secure FTP (SFTP)

Designed as a replacement for FTP after many of the inadequacies of SCP (such as the inability to see the files on the other computer) were discovered.

Secure Hash Algorithm (SHA)

A popular cryptographic hash.

Secure Shell (SSH)

A terminal emulation program that looks exactly like Telnet but encrypts the data. SSH has replaced Telnet on the Internet.

Secure Sockets Layer (SSL)

A protocol developed by Netscape for transmitting private documents over the Internet. SSL works by using a public key to encrypt sensitive data. This encrypted data is sent over an SSL connection and then decrypted at the receiving end using a private key.

Security

A network's resilience against unwanted access or attack.

Security Considerations

In network design and construction, planning how to keep data protected from unapproved access. Security of physical computers and network resources is also considered.

Security Guard

Person responsible for controlling access to physical resources such as buildings, secure rooms, and other physical assets.

Security Information and Event Management (SIEM)

A two-part process consisting of security event monitoring (SEM), which performs real-time monitoring of security events, and security information management (SIM), where the monitoring log files are reviewed and analyzed by automated and human interpreters.

Security Log

A log that tracks anything that affects security, such as successful and failed logons and logoffs.

Security Policy

A set of procedures defining actions employees should perform to protect the network's security.

Segment

The bus cable to which the computers on an Ethernet network connect.

Sequential

A method of storing and retrieving information that requires data to be written and read sequentially. Accessing any portion of the data requires reading all the preceding data.

Server

A computer that shares its resources, such as printers and files, with other computers on the network. An example of this is a Network File System Server that shares its disk space with a workstation that has no disk drive of its own.

Server-Based Network

A network in which one or more systems function as dedicated file, print, or application servers, but do not function as clients.

Server Message Block (SMB)

See SMB (Server Message Block).

Service Level Agreement (SLA)

A document between a customer and a service provider that defines the scope, quality, and terms of the service to be provided.

Service Set Identifier (SSID)

A 32-bit identification string, sometimes called a *network name*, that's inserted into the header of each data packet processed by a wireless access point.

Services

Background programs in an operating system that do the behind-the-scenes grunt work that users don't need to interact with on a regular basis.

Session

A networking term used to refer to the logical stream of data flowing between two programs and being communicated over a network. Many different sessions may be emanating from any one node on a network.

Session Highjacking

The interception of a valid computer session to get authentication information.

Session Initiation Protocol (SIP)

A signaling protocol for controlling voice and video calls over IP. SIP competes with H.323 for VoIP dominance.

Session Layer

See Open Systems Interconnection (OSI) Seven-Layer Model.

Session Software

Handles the process of differentiating among various types of connections on a PC.

Set

The PDU with which a network management station commands an agent to make a change to a Management Information Base (MIB) object.

Share Level Security

A security system in which each resource has a password assigned to it; access to the resource is based on knowing the password.

Share Permissions

Permissions that only control the access of other users on the network with whom you share your resource. They have no impact on you (or anyone else) sitting at the computer whose resource is being shared.

Shareware

Software that is protected by copyright, but the copyright holder allows (encourages!) you to make and distribute copies, under the condition that those who adopt the software after preview pay a fee. Derivative works are not allowed, and you may make an archival copy.

Shell

Generally refers to the user interface of an operating system. A shell is the command processor that is the actual interface between the kernel and the user.

Shielded Twisted Pair (STP)

A cabling for networks composed of pairs of wires twisted around each other at specific intervals. The twists serve to reduce interference (also called *crosstalk*). The more twists, the less interference. The cable has metallic shielding to protect the wires from external interference. *See also* Unshielded Twisted Pair (UTP) for the more commonly used cable type in modern networks.

Short Circuit

Allows electricity to pass between two conductive elements that weren't designed to interact together. Also called a *short*.

Short Message Service (SMS) Alert

A proactive message regarding an out-of-tolerance condition of an SNMP managed device sent as an SMS text.

Shortest Path First

Networking algorithm for directing router traffic. *See also* Open Shortest Path First (OSPF).

Signal Strength

A measurement of how well your wireless device is connecting to other devices.

Signaling Topology

Another name for logical topology. *See* Logical Topology.

Signature

Specific pattern of bits or bytes that is unique to a particular virus. Virus scanning software maintains a library of signatures and compares the contents of scanned files against this library to detect infected files.

Simple Mail Transfer Protocol (SMTP)

The main protocol used to send electronic mail on the Internet.

Simple Network Management Protocol (SNMP)

A set of standards for communication with network devices (switches, routers, WAPs) connected to a TCP/IP network. Used for network management.

Single-Mode Fiber (SMF)

Fiber-optic cables that use lasers.

Single Point of Failure

One component or system that, if it fails, will bring down an entire process, workflow, or organization.

Single Sign-on

A process whereby a client performs a one-time login to a gateway system. That system, in turn, takes care of the client's authentication to any other connected systems for which the client is authorized to access.

Site Survey

A process that enables you to determine any obstacles to creating the wireless network you want.

Site-to-Site

A type of VPN connection using two Cisco VPN concentrators to connect two separate LANs permanently.

Slashdotting

The massive influx of traffic on a small or lesser-known Web site when it is suddenly made popular by a reference from the media. *See also* Reddit Effect.

Small Form Factor (SFF)

A description of later-generation, fiber-optic connectors designed to be much smaller than the first iterations of connectors. *See also* LC Connector *and* Mechanical Transfer Registered Jack (MT-RJ).

Small Form Factor Pluggable (SFP)

A Cisco module that enables you to add additional features to its routers.

Small Office/Home Office (SOHO)

See SOHO (Small Office/Home Office).

Smart Device

Device (such as a credit card, USB key, etc.) that you insert into your PC in lieu of entering a password.

Smart Jack

Type of NIU that enables ISPs or telephone companies to test for faults in a network, such as disconnections and loopbacks.

SMB (Server Message Block)

Protocol used by Microsoft clients and servers to share file and print resources.

SMTP (Simple Mail Transfer Protocol)

See Simple Mail Transfer Protocol (SMTP).

Smurf

A type of hacking attack in which an attacker floods a network with ping packets sent to the broadcast address. The trick that makes this attack special is that the return address of the pings is spoofed to that of the intended victim. When all the computers on the network respond to the initial ping, they send their response to the intended victim.

Smurf Attack

See Smurf.

Snap-Ins

Small utilities that can be used with the Microsoft Management Console.

Snapshot

A tool that enables you to save an extra copy of a virtual machine as it is exactly at the moment the snapshot is taken.

Sneakernet

Saving a file on a portable medium and walking it over to another computer.

Sniffer

Diagnostic program that can order a NIC to run in promiscuous mode. *See also* Promiscuous Mode.

Snip

See Cable Stripper.

SNMP (Simple Network Management Protocol)

See Simple Network Management Protocol (SNMP).

SNMP Manager

Software and station that communicates with SNMP agents to monitor and manage management information base (MIB) objects.

Snmpwalk

SNMP manager PDU that collects Management Information Base (MIB) information in a tree-oriented hierarchy of a MIB object and any of its subordinate objects. The snmpwalk command queries the object and then automatically queries all of the objects that are subordinated to the root object being queried.

Social Engineering

The process of using or manipulating people inside the networking environment to gain access to that network from the outside.

Socket

A combination of a port number and an IP address that uniquely identifies a connection.

Socket Pairs

See Endpoints.

Software

Programming instructions or data stored on some type of binary storage device.

Software as a Service (SaaS)

Centralized applications that are accessed over a network.

SOHO (Small Office/Home Office) Network

Refers to a classification of networking equipment, usually marketed to consumers or small businesses, which focuses on low price and ease of configuration. SOHO networks differ from enterprise networks, which focus on flexibility and maximum performance.

SOHO Firewall

Firewall, typically simple, that is built into the firmware of a SOHO router.

Solid Core

A cable that uses a single solid wire to transmit signals.

SONET (Synchronous Optical Network)

An American fiber carrier standard for connecting fiber-optic transmission systems. SONET was proposed in the mid-1980s and is now an ANSI standard. SONET defines interface standards at the Physical layer of the OSI seven-layer model.

Source Address Table (SAT)

A table stored by a switch, listing the MAC addresses and port of each connected device.

Spanning Tree Protocol (STP)

A protocol that enables switches to detect and prevent bridge loops automatically.

Speed-Test Site

A Web site used to check an Internet connection's throughput, such as www.speakeasy.net/speedtest.

Split Pair

A condition that occurs when signals on a pair of wires within a UTP cable interfere with the signals on another wire pair within that same cable.

Spoofing

A security threat where an attacker makes some data seem as though it came from somewhere else, such as sending an e-mail with someone else's e-mail address in the sender field.

Spyware

Any program that sends information about your system or your actions over the Internet.

SQL (Structured Query Language)

A language created by IBM that relies on simple English statements to perform database queries. SQL enables databases from different manufacturers to be queried using a standard syntax.

SSID Broadcast

A wireless access point feature that announces the WAP's SSID to make it easy for wireless clients to locate and connect to it. By default, most WAPs regularly announce their SSID. For security purposes, some entities propose disabling this broadcast.

SSL (Secure Sockets Layer)

See Secure Sockets Layer (SSL).

SSL VPN

A type of VPN that uses SSL encryption. Clients connect to the VPN server using a standard Web browser, with the traffic secured using SSL. The two most common types of SSL VPNs are SSL portal VPNs and SSL tunnel VPNs.

ST Connector

Fiber-optic connector used primarily with 2.5mm, single-mode fiber. It uses a push on, then twist-to-lock mechanical connection commonly called stick-and-twist although ST actually stands for Straight Tip.

Star Topology

A network topology in which all computers in the network connect to a central wiring point.

Star-Bus Topology

A hybrid of the star and bus topologies that uses a physical star, where all nodes connect to a single wiring point such as a hub and a logical bus that maintains the Ethernet standards. One benefit of a star-bus topology is *fault tolerance.*

Stateful (DHCP)

Describes a DHCPv6 server that works very similarly to an IPv4 DHCP server, passing out IPv6 addresses, subnet masks, and default gateways as well as optional items like DNS server addresses.

Stateful Filtering/Stateful Inspection

A method of filtering in which all packets are examined as a stream. Stateful devices can do more than allow or block; they can track when a stream is disrupted or packets get corrupted and act accordingly.

Stateless (DHCP)

Describes a DHCPv6 server that only passes out optional information.

Stateless Filtering/Stateless Inspection

A method of filtering where the device that does the filtering looks at each IP packet individually, checking the packet for IP addresses and port numbers and blocking or allowing accordingly.

Statement of Work (SOW)

A contract that defines the services, products, and time frames for the vendor to achieve.

Static Addressing

The process of assigning IP addresses by manually typing them into client computers.

Static NAT (SNAT)

A type of NAT that maps a single routable IP address to a single machine, allowing you to access that machine from outside the network.

Static Routes

Entries in a router's routing table that are not updated by any automatic route discovery protocols. Static routes must be added, deleted, or changed by a router administrator. Static routes are the opposite of dynamic routes.

Static Routing

A process by which routers in an internetwork obtain information about paths to other routers. This information must be supplied manually.

Storage

A device or medium that can retain data for subsequent retrieval.

Storage Area Network (SAN)

A server that can take a pool of hard disks and present them over the network as any number of logical disks.

STP (Spanning Tree Protocol)

See Spanning Tree Protocol (STP).

Straight-through Cable

UTP or STP cable segment that has the wire and pin assignments at one end of the cable match the wire and same pin assignments at the other end. Straight-through cables are used to connect hosts to switches and are the connective opposite of crossover cables.

Stranded Core

A cable that uses a bundle of tiny wire strands to transmit signals. Stranded core is not quite as good a conductor as solid core, but it will stand up to substantial handling without breaking.

Stream Cipher

An encryption method that encrypts a single bit at a time. Popular when data comes in long streams (such as with older wireless networks or cell phones).

Stripe Set

Two or more drives in a group that are used for a striped volume.

Structured Cabling

Standards defined by the Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA) that define methods of organizing the cables in a network for ease of repair and replacement.

STS Overhead

Carries the signaling and protocol information in Synchronous Transport Signal (STS).

STS Payload

Carries data in STS.

Subnet

Each independent network in a TCP/IP internetwork.

Subnet Mask

The value used in TCP/IP settings to divide the IP address of a host into its component parts: network ID and host ID.

Subnetting

Taking a single class of IP addresses and chopping it into multiple smaller groups.

Succession Planning

The process of identifying people who can take over certain positions (usually on a temporary basis) in case the people holding those critical positions are incapacitated or lost in an incident.

Supervisory Control and Data Acquisition (SCADA)

A system that has the basic components of a distributed control system (DCS), yet is designed for large-scale, distributed processes and functions with the idea that remote devices may or may not have ongoing communication with the central control.

Supplicant

A client computer in a RADIUS network.

Switch

A Layer 2 (Data Link) multiport device that filters and forwards frames based on MAC addresses.

Switching Loop

When you connect multiple switches together in a circuit causing a loop to appear. Better switches use spanning tree protocol (STP) to prevent this.

Symmetric DSL (SDSL)

Type of DSL connection that provides equal upload and download speed and, in theory, provides speeds up to 15 Mbps, although the vast majority of ISPs provide packages ranging from 192 Kbps to 9 Mbps.

Symmetric-Key Algorithm

Any encryption method that uses the same key for both encryption and decryption.

Synchronous

Describes a connection between two electronic devices where neither must acknowledge (ACK) when receiving data.

Synchronous Digital Hierarchy (SDH)

European fiber carrier standard equivalent to SONET.

Synchronous Optical Network (SONET)

See SONET (Synchronous Optical Network).

Synchronous Transport Signal (STS)

Signal method used by SONET. It consists of the STS payload and the STS overhead. A number is appended to the end of STS to designate signal speed.

System Log

A log file that records issues dealing with the overall system, such as system services, device drivers, or configuration changes.

System Restore

A Windows utility that enables you to return your PC to a recent working configuration when something goes wrong. System Restore returns your computer's system settings to the way they were the last time you remember your system working correctly—all without affecting your personal files or e-mail.

T Connector

A three-sided, tubular connector found in 10Base2 Ethernet networking. The connector is in the shape of a *T* with the "arms" of the *T* ending with a female BNC connector and the "leg" having a male BNC connector. The T connector is used to attach a BNC connector on a host between two cable segments.

T1

A leased-line connection capable of carrying data at 1,544,000 bps.

T1 Line

The specific, shielded, two-pair cabling that connects the two ends of a T1 connection.

T3 Line

A leased-line connection capable of carrying data at 44,736,000 bps.

Tailgating

When an unauthorized person attempts to enter through an already opened door.

TCP Segment

The connection-oriented payload of an IP packet. A TCP segment works on the Transport layer.

TCP/IP Model

An architecture model based on the TCP/IP protocol suite, which defines and standardizes the flow of data between computers. The following lists the four layers:

- **Layer 1** The *Link layer (Network Interface layer)* is similar to OSI's Data Link and Physical layers. The Link layer consists of any part of the network that deals with frames.
- **Layer 2** The *Internet layer* is the same as OSI's Network layer. Any part of the network that deals with pure IP packets—getting a packet to its destination—is on the Internet layer.
- **Layer 3** The *Transport layer* combines the features of OSI's Transport and Session layers. It is concerned with the assembly and disassembly of data, as well as connection-oriented and connectionless communication.
- **Layer 4** The *Application layer* combines the features of the top three layers of the OSI model. It consists of the processes that applications use to initiate, control, and disconnect from a remote system.

TCP/IP Suite

The collection of all the protocols and processes that make TCP over IP communication over a network possible.

TCP Three-way Handshake

A three-packet conversation between TCP hosts to establish and start a data transfer session. The conversation begins with a SYN request by the initiator. The target responds with a SYN response and an ACK to the SYN request. The initiator confirms receipt of the SYN AC with an ACK. Once this handshake is complete, data transfer can begin.

Telecommunications Room

A central location for computer or telephone equipment and, most importantly, centralized cabling. All cables usually run to the telecommunications room from the rest of the installation.

Telephony

The science of converting sound into electrical signals, moving those signals from one location to another, and then converting those signals back into sounds. This includes modems, telephone lines, the telephone system, and any products used to create a remote access link between a remote access client and server.

Telnet

A program that enables users on the Internet to log onto remote systems from their own host systems.

Temperature Monitor

Device for keeping a telecommunications room at an optimal temperature.

TEMPEST

The NSA's security standard that is used to combat RF emanation by using enclosures, shielding, and even paint.

Temporal Key Integrity Protocol (TKIP)

The extra layer of security that Wi-Fi Protected Access (WPA) adds on top of Wired Equivalent Privacy (WEP).

Teredo

A NAT-traversal IPv6 tunneling protocol, built into Microsoft Windows.

Terminal Access Controller Access Control System Plus (TACACS+)

A proprietary protocol developed by Cisco to support AAA in a network with many routers and switches. It is similar to RADIUS in function, but uses TCP port 49 by default and separates authorization, authentication, and accounting into different parts.

Terminal Adapter (TA)

The most common interface used to connect a computer to an ISDN line.

Terminal Emulation

Software that enables a PC to communicate with another computer or network as if it were a specific type of hardware terminal.

TFTP (Trivial File Transfer Protocol)

See Trivial File Transfer Protocol (TFTP).

Thick Client

A wireless access point that is completely self-contained with a full set of management programs and administrative access ways. Each thick client is individually managed by an administrator who logs into the WAP, configures it, and logs out.

Thin Client

A wireless access point with minimal configuration tools installed. Instead, it is managed by a central controller. An administrator can manage a large number of thin clients by logging into the central controller and performing management tasks on any thin client routers from there.

Thinnet

Trade name for 10Base2 Ethernet technology. Thinnet is characterized by the use of RG-58 coaxial cable segments and BNC T connectors to attach stations to the segments.

Threat

Any form of potential attack against a network.

TIA/EIA (Telecommunications Industry Association/Electronics Industry Association)

The standards body that defines most of the standards for computer network cabling. Many of these standards are defined under the TIA/EIA 568 standard.

TIA/EIA 568A

One of two four-pair UTP crimping standards for 10/100/1000BaseT networks. Often shortened to T568A. The other standard is TIA/EIA 568B.

TIA/EIA 568B

One of two four-pair UTP crimping standards for 10/100/1000BaseT networks. Often shortened to T568B. The other standard is TIA/EIA 568A.

TIA/EIA 606

Official methodology for labeling patch panels.

Ticket-Granting Ticket (TGT)

Sent by an Authentication Server in a Kerberos setup if a client's hash matches its own, signaling that the client is authenticated but not yet authorized.

Time Division Multiplexing (TDM)

The process of having frames that carry a bit of every channel in every frame sent at a regular interval in a T1 connection.

Time Domain Reflectometer (TDR)

Advanced cable tester that tests the length of cables and their continuity or discontinuity, and identifies the location of any discontinuity due to a bend, break, unwanted crimp, and so on.

TLS (Transport Layer Security)

See Transport Layer Security (TLS).

Tone Generator

See Toners.

Tone Probe

See Toners.

Toners

Generic term for two devices used together—a tone generator and a tone locator (probe)—to trace cables by sending an electrical signal along a wire at a particular frequency. The tone locator then emits a sound when it distinguishes that frequency. Also referred to as *Fox and Hound*.

Top Listener

Host that receives the most data on a network.

Top Talker

Host that sends the most data on a network.

Top-Level Domain Servers

A set of DNS servers—just below the root servers—that handle the top-level domain names, such as .com, .org, .net, and so on.

Topology

The pattern of interconnections in a communications system among devices, nodes, and associated input and output stations. Also describes how computers connect to each other without regard to how they actually communicate.

tracert (also traceroute)

A command-line utility used to follow the path a packet takes between two hosts.

tracert –6 (also traceroute6)

A command-line utility that checks a path from the station running the command to a destination host. Adding the –6 switch to the command line specifies that the target host uses an IPv6 address. tracerout6 is a Linux command that performs a traceroute to an IPv6 addressed host.

Traffic Analysis

Tools that chart a network's traffic usage.

Traffic Shaping

Controlling the flow of packets into or out of the network according to the type of packet or other rules.

Traffic Spike

Unusual and usually dramatic increase in the amount of network traffic. Traffic spikes may be the result of normal operations within the organization or may be an indication of something more sinister.

Transceiver

The device that transmits and receives signals on a cable.

Transmission Control Protocol (TCP)

Part of the TCP/IP protocol suite, operates at Layer 4 (Transport) of the OSI seven-layer model. TCP is a connection-oriented protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A set of communication protocols developed by the U.S. Department of Defense that enables dissimilar computers to share information over a network.

Transmit Beamforming

A multiple-antenna technology in 802.11n WAPs that helps get rid of dead spots.

Transport Layer

See Open System Interconnection (OSI) Seven-Layer Model.

Transport Layer Security (TLS)

A robust update to SSL that works with almost any TCP application.

Trap

Out-of-tolerance condition in an SNMP managed device.

Trivial File Transfer Protocol (TFTP)

A protocol that transfers files between servers and clients. Unlike FTP, TFTP requires no user login. Devices that need an operating system, but have no local hard disk (for example, diskless workstations and routers), often use TFTP to download their operating systems.

Trojan Horse

A virus that masquerades as a file with a legitimate purpose, so that a user will run it intentionally. The classic example is a file that runs a game, but also causes some type of damage to the player's system.

Trunk Port

A port on a switch configured to carry all data, regardless of VLAN number, between all switches in a LAN.

Trunking

The process of transferring VLAN data between two or more switches.

Trusted User

An account that has been granted specific authority to perform certain or all administrative tasks.

Tunnel

An encrypted link between two programs on two separate computers.

Tunnel Broker

In IPv6, a service that creates the actual tunnel and (usually) offers a custom-made endpoint client for you to use, although more advanced users can often make a manual connection.

Tunnel Information and Control Protocol (TIC)

One of the protocols that set up IPv6 tunnels and handle configuration as well as login.

Tunnel Setup Protocol (TSP)

One of the protocols that set up IPv6 tunnels and handle configuration as well as login.

Twisted Pair

Twisted pairs of cables, the most overwhelmingly common type of cabling used in networks. The two types of twisted pair cabling are UTP (unshielded twisted pair) and STP (shielded twisted pair). The twists serve to reduce interference, called *crosstalk*; the more twists, the less crosstalk.

Two-Factor Authentication

A method of security authentication that requires two separate means of authentication; for example, some sort of physical token that, when inserted, prompts for a password.

U (Units)

The unique height measurement used with equipment racks; 1 U equals 1.75 inches.

UART (Universal Asynchronous Receiver/Transmitter)

A device that turns serial data into parallel data. The cornerstone of serial ports and modems.

UC Device

One of three components of a UC network, it is used to handle voice, video, and more.

UC Gateway

One of three components of a UC network, it is an edge device used to add extra services to an edge router.

UC Server

One of three components of a UC network, it is typically a dedicated box that supports any UC-provided service.

UDP (User Datagram Protocol)

See User Datagram Protocol (UDP).

UDP Datagram

A connectionless networking container used in UDP communication.

Ultra Physical Contact (UPC) Connector

Fiber-optic connector that makes physical contact between to fiber-optic cables. The fibers within a UPC are polished extensively for a superior finish and better junction integrity.

UNC (Universal Naming Convention)

Describes any shared resource in a network using the convention \\<*server name*>\<*name of shared resource*>.

Unencrypted Channel

Unsecure communication between a two hosts that pass data between them using cleartext. A Telnet connection is a common unencrypted channel.

Unicast

A message sent from one computer to one other computer.

Unicast Address

A unique IP address that is exclusive to a single system.

Unidirectional Antenna

Unidirectional antennas focus all of their transmission energy in a single, relatively narrow direction. Similarly, their design limits their ability to receive signals that are not aligned with the focused direction.

Unified Communication (UC)

A system that rolls many different network services into one, for example, instant messaging (IM), telephone service, video conferencing, and more.

Unified Threat Management (UTM)

Firewall that is also packaged with a collection of other processes and utilities to detect and prevent a wide variety of threats. These protections include intrusion detection systems, intrusion prevention systems, VPN portals, load balancers, and other threat mitigation apparatus.

Unified Voice Services

Complete self-contained Internet services that rely on nothing more than software installed on computers and the computers' microphone/speakers to provide voice telecommunication over the Internet. All of the interconnections to the PSTN are handled in the cloud.

Uninterruptible Power Supply (UPS)

A device that supplies continuous clean power to a computer system the whole time the computer is on. Protects against power outages and sags. The term *UPS* is often used mistakenly when people mean stand-by power supply or system (SPS).

Unit (U)

The unique height measurement used with equipment racks; 1 U equals 1.75 inches.

Universal Asynchronous Receiver Transmitter (UART)

A device inside a modem that takes the 8-bit-wide digital data and converts it into 1-bit-wide digital data and hands it to the modem for conversion to analog data. The process is reversed for incoming data.

UNIX

A popular computer software operating system used on many Internet host systems.

Unsecure Protocol

Also known as an insecure protocol, transfers data between hosts in an unencrypted, clear text format. If these packets are intercepted between the communicating hosts, their data is completely exposed and readable.

Unshielded Twisted Pair (UTP)

A popular cabling for telephone and networks composed of pairs of wires twisted around each other at specific intervals. The twists serve to reduce interference (also called *crosstalk*). The more twists, the less interference. The cable has *no* metallic shielding to protect the wires from external interference, unlike its cousin, *STP*. 10BaseT uses UTP, as do many other networking technologies. UTP is available in a variety of grades, called categories, as defined in the following:

- **Category 1 UTP** Regular analog phone lines, not used for data communications
- **Category 2 UTP** Supports speeds up to 4 Mbps
- **Category 3 UTP** Supports speeds up to 16 Mbps
- **Category 4 UTP** Supports speeds up to 20 Mbps
- **Category 5 UTP** Supports speeds up to 100 Mbps
- **Category 5e UTP** Supports speeds up to 100 Mbps with two pairs and up to 1000 Mbps with four pairs
- **Category 6 UTP** Improved support for speeds up to 10 Gbps
- **Category 6a UTP** Extends the length of 10-Gbps communication to the full 100 meters commonly associated with UTP cabling.

Untrusted User

An account that has been granted no administrative powers.

Uplink Port

Port on a switch that enables you to connect two switches together using a straight-through cable.

Upload

The transfer of information from a user's system to a remote computer system. Opposite of download. *See also* Download.

URL (Uniform Resource Locator)

An address that defines the type and the location of a resource on the Internet. URLs are used in almost every TCP/IP application. A typical HTTP URL is http://www.totalsem.com.

Usenet

The network of UNIX users, generally perceived as informal and made up of loosely coupled nodes, that exchanges mail and messages. Started by Duke University and UNC-Chapel Hill. An information cooperative linking around 16,000 computer sites and millions of people. Usenet provides a series of "news groups" analogous to online conferences.

User

Anyone who uses a computer. You.

User Account

A container that identifies a user to the application, operating system, or network, including name, password, user name, groups to which the user belongs, and other information based on the user and the OS or NOS being used. Usually defines the rights and roles a user plays on a system.

User Datagram Protocol (UDP)

A protocol used by some older applications, most prominently TFTP (Trivial FTP), to transfer files. UDP datagrams are both simpler and smaller than TCP segments, and they do most of the behind-the-scenes work in a TCP/IP network.

User-Level Security

A security system in which each user has an account, and access to resources is based on user identity.

User Profiles

A collection of settings that corresponds to a specific user account and may follow the user, regardless of the computer at which he or she logs on. These settings enable the user to have customized environment and security settings.

UTP Coupler

A simple, passive, double-ended connector with female connectors on both ends. UTP couplers are used to connect two UTP cable segments together to achieve longer length when it is deemed unnecessary or inappropriate to use a single, long cable.

V Standards

Standards established by CCITT for modem manufacturers to follow (voluntarily) to ensure compatible speeds, compression, and error correction.

V.92 Standard

The current modem standard, which has a download speed of 57,600 bps and an upload speed of 48 Kbps. V.92 modems have several interesting features, such as Quick Connect and Modem on Hold.

Variable

Value of an SNMP Management Information Base (MIB) object. That value can be read with a Get PDU or changed with a Set PDU.

Vertical Cross-Connect

Main patch panel in a telecommunications room. *See also* Patch Panel.

Very High Bitrate DSL (VDSL)

The latest form of DSL with download and upload speeds of up to 100 Mbps. VDSL was designed to run on copper phone lines, but many VDSL suppliers use fiber-optic cabling to increase effective distances.

Video Monitoring

Security measures that use remotely monitored visual systems that include IP cameras and closed-circuit televisions.

Video Teleconferencing

The classic, multicast-based presentation where one presenter pushes out a stream of video to any number of properly configured and properly authorized multicast clients.

View

The different displays found in Performance Monitor.

Virtual Firewall

A firewall that is implemented in software within a virtual machine in cases where it would be difficult, costly, or impossible to install a traditional physical firewall.

Virtual IP

A single IP address shared by multiple systems. This is commonly the single IP address assigned to a home or organization that uses NAT to have multiple IP stations on the private side of the NAT router.

Virtual Local Area Network (VLAN)

A common feature among managed switches that enables a single switch to support multiple logical broadcast domains. Not only is VLAN support a common feature of managed switches but VLAN installations take advantage of this feature and are very common today.

Virtual Machine (VM)

A virtual computer accessed through a class of program called a hypervisor or virtual machine manager. A virtual machine runs *inside* your actual operating system, essentially enabling you to run two or more operating systems at once.

Virtual Machine Manager (VMM)

See Hypervisor.

Virtual PBX

Software that functionally replaces a physical PBX telephone system.

Virtual Private Network (VPN)

A network configuration that enables a remote user to access a private network via the Internet. VPNs employ an encryption methodology called *tunneling*, which protects the data from interception.

Virtual Router

A router that is implemented in software within a virtual machine. The scalability of a virtual machine makes it easy to add capacity to the router when it is needed. Virtual routers are easily managed and are highly scalable without requiring the purchase of additional network hardware.

Virtual Switch

Special software that enables VMs to communicate with each other without going outside of the host system.

Virtual Trunk Protocol (VTP)

A proprietary Cisco protocol to automate the updating of multiple VLAN switches.

Virus

A program that can make a copy of itself without your necessarily being aware of it. All viruses carry some payload that may or may not do something malicious.

Virus Definition or Data Files

Enables the virus protection software to recognize the viruses on your system and clean them. These files should be updated often. Also called *signature files*, depending on the virus protection software in use.

Virus Shield

Anti-malware program that passively monitors a computer's activity, checking for viruses only when certain events occur, such as a program executing or a file being downloaded.

VLAN Hopping

Older technique to hack a switch to change a normal switch port from an access port to a trunk port. This allows the station attached to the newly created trunk port to access different VLANs. Modern switches have preventative measures to stop this type of abuse.

VLAN Pooling

Used in wireless networking, a setup where multiple VLANs share a common domain. The multiple VLANs are used to keep broadcast traffic to manageable levels. Wireless clients are randomly assigned to different VLANs. Their common domain enables them all to be centrally managed.

VLAN Trunking Protocol (VTP)

Cisco proprietary protocol to automate the updating of multiple VLAN switches.

Voice over IP (VoIP)

Using an IP network to conduct voice calls.

Voltage

The pressure of the electrons passing through a wire.

Voltage Event Recorder

Tracks voltage over time by plugging into a power outlet.

Volts (V)

Units of measurement for voltage.

VPN Concentrator

The new endpoint of the local LAN in L2TP.

Vulnerability

A potential weakness in an infrastructure that a threat might exploit.

Vulnerability Scanner

A tool that scans a network for potential attack vectors.

WAN (Wide Area Network)

A geographically dispersed network created by linking various computers and LANs over long distances, generally using leased phone lines. There is no firm dividing line between a WAN and a LAN.

Warm Boot

A system restart performed after the system has been powered and operating. This clears and resets the memory, but does not stop and start the hard drive.

Warm Site

Facility with all of the physical resources, computers, and network infrastructure to recover from a primary site disaster. A warm site does not have current backup data and it may take a day or more to recover and install backups before business operations can recommence.

Wattage (Watts or W)

The amount of amps and volts needed by a particular device to function.

Wavelength

In the context of laser pulses, the distance the signal has to travel before it completes its cyclical oscillation and starts to repeat. Measured in nanometers, wavelength can be loosely associated with colors.

Web Server

A server that enables access to HTML documents by remote users.

Web Services

Applications and processes that can be accessed over a network, rather than being accessed locally on the client machine. Web services include things such as Web-based e-mail, network-shareable documents, spreadsheets and databases, and many other types of cloud-based applications.

Well-Known Port Numbers

Port numbers from 0 to 1204 that are used primarily by client applications to talk to server applications in TCP/IP networks.

Wi-Fi

The most widely adopted wireless networking type in use today. Technically, only wireless devices that conform to the extended versions of the 802.11 standard—802.11a, b, g, n, and ac—are Wi-Fi certified.

Wi-Fi Analyzer

Any device that finds and documents all wireless networks in the area. Also known as a wireless analyzer.

Wi-Fi Protected Access (WPA)

A wireless security protocol that addresses the weaknesses and acts as a sort of upgrade to WEP. WPA offers security enhancements such as dynamic encryption key generation (keys are issued on a per-user and per-session

basis), an encryption key integrity-checking feature, user authentication through the industry-standard Extensible Authentication Protocol (EAP), and other advanced features that WEP lacks.

Wi-Fi Protected Access 2 (WPA2)

An update to the WPA protocol that uses the Advanced Encryption Standard algorithm, making it much harder to crack.

Wi-Fi Protected Setup (WPS)

Automated and semi-automated process to connect a wireless device to a WAP. The process can be as simple as pressing a button on the device or pressing the button and then entering a PIN code.

Wide Area Network (WAN)

See WAN (Wide Area Network).

WiMAX

See 802.16.

Windows Domain

A group of computers controlled by a computer running Windows Server, which is configured as a domain controller.

Windows Firewall

The firewall that has been included in Windows operating systems since Windows XP; originally named Internet Connection Firewall (ICF) but renamed in XP Service Pack 2.

Windows Internet Name Service (WINS)

A name resolution service that resolves NetBIOS names to IP addresses.

WINS Proxy Agent

A WINS relay agent that forwards WINS broadcasts to a WINS server on the other side of a router to keep older systems from broadcasting in place of registering with the server.

Wire Scheme

See Wiring Diagram.

Wired Equivalent Privacy (WEP)

A wireless security protocol that uses a 64-bit encryption algorithm to scramble data packets.

Wired/Wireless Considerations

The planning of structured cabling, determining any wireless requirements, and planning access to the Internet when building or upgrading networks.

Wireless Access Point (WAP)

Connects wireless network nodes to wireless or wired networks. Many WAPs are combination devices that act as high-speed hubs, switches, bridges, and routers, all rolled into one.

Wireless Analyzer

Any device that finds and documents all wireless networks in the area. Also known as a Wi-Fi analyzer.

Wireless Bridge

Device used to connect two wireless network segments together, or to join wireless and wired networks together in the same way that wired bridge devices do.

Wireless Controller

Central controlling device for thin client WAPs.

Wireless LAN (WLAN)

A complete wireless network infrastructure serving a single physical locale under a single administration.

Wireless Network

See Wi-Fi.

Wireless Survey Tool

A tool used to discover wireless networks in an area that also notes signal interferences.

Wiremap

Term that techs use to refer to the proper connectivity of wires in a network.

Wireshark

A popular packet sniffer.

Wiring Diagram

A document, also known as a *wiring schematic*, that usually consists of multiple pages and that shows the following: how the wires in a network connect to switches and other nodes, what types of cables are used, and how patch panels are configured. It usually includes details about each cable run.

Wiring Schematic

See Wiring Diagram.

Work Area

In a basic structured cabling network, often simply an office or cubicle that potentially contains a PC attached to the network.

Workgroup

A convenient method of organizing computers under Network/My Network Places in Windows operating systems.

Workstation

A general-purpose computer that is small enough and inexpensive enough to reside at a person's work area for his or her exclusive use.

Worm

A very special form of virus. Unlike other viruses, a worm does not infect other files on the computer. Instead, it replicates by making copies of itself on other systems on a network by taking advantage of security weaknesses in networking protocols.

WPA2-Enterprise

A version of WPA2 that uses a RADIUS server for authentication.

WWW (World Wide Web)

The (graphical) Internet that can be accessed using Gopher, FTP, HTTP, Telnet, Usenet, WAIS, and some other tools.

X.25

The first generation of packet-switching technology, enables remote devices to communicate with each other across high-speed digital links without the expense of individual leased lines.

Yost Cable

Cable used to interface with a Cisco device.

Zero-Day Attack

New attack that uses a vulnerability that has yet to be identified.

Zombie

A single computer under the control of an operator that is used in a botnet attack. *See also* Botnet.