Network+ Terminology

66 block Traditionally used in corporate environments for cross-connecting phone system cabling. As 10-Mbps LANs started to grow in popularity in the late 1980s and early 1990s, these termination blocks were used to cross-connect Category 3 UTP cabling. The electrical characteristics (specifically, crosstalk) of a 66 block, however, do not support higher-speed LAN technologies, such as 100-Mbps Ethernet networks.

110 block Because 66 blocks are subject to too much crosstalk for higher-speed LAN connections, 110 blocks can be used to terminate a cable (such as a Category 5 cable) being used for those higher-speed LANs.

802.11a Ratified in 1999, this standard supports speeds as high as 54 Mbps. Other supported data rates (which can be used if conditions are not suitable for the 54-Mbps rate) include 6, 9, 12, 18, 24, 36, and 48 Mbps. The 802.11a standard uses the 5-GHz band and the OFDM transmission method.

802.11ac An IEEE wireless networking standard operating in the 5GHz range, with increased throughput compared to previous WiFi IEEE standards.

802.11b Ratified in 1999, this standard supports speeds as high as 11 Mbps. However, 5.5 Mbps is another supported data rate. The 802.11b standard uses the 2.4-GHz band and the DSSS transmission method.

802.11g Ratified in 2003, this standard supports speeds as high as 54 Mbps. Like 802.11a, other supported data rates include 6, 9, 12, 18, 24, 36, and 48 Mbps. However, like 802.11b, 802.11g operates in the 2.4-GHz band, which allows it to offer backward compatibility to 802.11b devices. 802.11g can use either the OFDM or DSSS transmission method.

802.11n Ratified in 2009, this standard supports a variety of speeds, depending on its implementation. Although the speed of an 802.11n network could approach 300 Mbps (through the use of channel bonding), many 802.11n devices on the market have speed ratings in the 130 to 150-Mbps range. Interestingly, an 802.11n WLAN can operate in the 2.4-GHz band, the 5-GHz band, or both simultaneously. 802.11n uses the OFDM transmission method.

acceptable use policy (AUP) Identifies what users of a network are and are not allowed to do on that network. For example, retrieving sports scores during working hours via an organization's Internet connection might be deemed inappropriate by an AUP.

access control list (ACL) Rules typically applied to router interfaces, which specify permitted and denied traffic.

Address Resolution Protocol (ARP) An ARP request is a broadcast asking for the MAC address corresponding to a known IP address. An ARP reply contains the requested MAC address.

administrative distance (AD) A routing protocol's index of believability. Routing protocols with a smaller AD are considered more believable than routing protocols with a higher AD.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

Advanced Encryption Standard (AES) Released in 2001, AES is typically considered the preferred symmetric encryption algorithm. AES is available in 128-bit key, 192-bit key, and 256-bit key versions.

anycast An anycast communication flow is a one-to-nearest (from the perspective of a router's routing table) flow.

application layer (OSI model) Layer 7 of the OSI model, it provides application services to a network. An important, and an often-misunderstood concept, is that end-user applications do not reside at the application layer. Instead, the application layer supports services used by end-user applications. Another function of the application layer is advertising available services.

application layer (TCP/ IP stack) Addresses concepts described by Layers 5, 6, and 7 (that is, the session, presentation, and application layers) of the OSI model.

arp command Can be used in either the Microsoft Windows or the UNIX environment to see what a Layer 2 MAC address corresponds to in a Layer 3 IP address.

asset management As related to networks, this is a formalized system of tracking network components and managing the lifecycle of those components.

asymmetric encryption With asymmetric encryption, the sender and receiver of a packet use different keys.

Asynchronous Transfer Mode (ATM) A Layer 2 WAN technology that interconnects sites using virtual circuits. These virtual circuits are identified by a pair of numbers, called the VPI/ VCI pair.

A virtual path identifier (VPI) identifies a logical path, which can contain multiple virtual circuits.

A virtual circuit identifier (VCI) identifies the unique logical circuit within a virtual path.

Authentication Header (AH) An IPsec protocol that provides authentication and integrity services. However, it does not provide encryption services.

authentication server In a network using 802.1X user authentication, an authentication server (typically, a RADIUS server) checks a supplicant's credentials. If the credentials are acceptable, the authentication server notifies the authenticator that the supplicant is allowed to communicate on a network. The authentication server also gives the authenticator a key that can be used to securely transmit data during the authenticator's session with the supplicant.

authenticator In a network using 802.1X user authentication, an authenticator forwards a supplicant's authentication request on to an authentication server. After the authentication server authenticates the supplicant, the authenticator receives a key that is used to communicate securely during a session with the supplicant.

Automatic Private IP Addressing (APIPA) Allows a networked device to self-assign an IP address from the 169.254.0.0/ 16 network. Note that this address is only usable on the device's local subnet (meaning that the IP address is not routable).

availability The measure of a network's uptime.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

baseline A collection of data portraying the characteristics of a network under normal operating conditions. Data collected while troubleshooting can then be contrasted against baseline data.

Basic Rate Interface (BRI) A BRI circuit contains two 64-kbps B channels and one 16-Kbps D channel. Although such a circuit can carry two simultaneous voice conversations, the two B channels can be logically bonded together into a single virtual circuit (by using PPP's multilink interface feature) to offer a 128-kbps data path.

basic service set (BSS) WLANs that have just one AP are called BSS WLANs. BSS WLANs are said to run in infrastructure mode because wireless clients connect to an AP, which is typically connected to a wired network infrastructure. A BSS network is often used in residential and SOHO locations, where the signal strength provided by a single AP is sufficient to service all of the WLAN's wireless clients.

bit-error rate tester (BERT) When troubleshooting a link where you suspect a high bit-error rate (BER), you can use a piece of test equipment called a bit-error rate tester (BERT), which contains both a pattern generator (which can generate a variety of bit patterns) and an error detector (which is synchronized with the pattern generator and can determine the number of bit errors) and can calculate a BER for the tested transmission link.

black-hole router A router that drops packets that cannot be fragmented and are exceeding the MTU size of an interface without notifying the sender.

block size The number of IP addresses in a subnet, including the subnet's address and the subnet's directed broadcast address.

Bootstrap Protocol (BOOTP) A legacy broadcast-based protocol used by networked devices to obtain IP address information.

Border Gateway Protocol (BGP) The only EGP in widespread use today. In fact, BGP is considered to be the routing protocol that runs the Internet, which is an interconnection of multiple autonomous systems. BGP is a path-vector routing protocol, meaning that it can use as its metric the number of autonomous system hops that must be transited to reach a destination network, as opposed to the number of required router hops.

borrowed bits Bits added to a classful subnet mask.

buffer overflow This attack occurs when an attacker leverages a vulnerability in an application, causing data to be written to a memory area (that is, a buffer) that's being used by a different application.

bus topology Typically, it uses a cable running through the area requiring connectivity, and devices to be networked can tap into that cable.

butt set A piece of test equipment typically used by telephone technicians. The clips on a butt set can connect to the tip and ring wires on a punch-down block (for example, a 66 block or a 110 block) connecting to a telephone. This allows the technician to check the line (for example, to determine whether a dial tone is present on the line and determine whether a call can be placed from the line).

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

cable certifier If you are working with existing cable and want to determine its category, or if you simply want to test the supported frequency range (and therefore data throughput) of the cable, you can use a cable certifier.

cable modem Attaches to the same coaxial cable (typically in a residence) that provides television programming. A cable modem can use predetermined frequency ranges to transmit and receive data over that coaxial cable.

cable tester A cable tester can test the conductors in an Ethernet cable. It contains two parts. By connecting these parts of the cable tester to each end of a cable under test, you can check the wires in the cable for continuity (that is, check to make sure that there are no opens, or breaks, in a conductor). In addition, you can verify an RJ-45 connector's pinouts (which are wires connected to the appropriate pins on an RJ-45 connector).

campus-area network (CAN) An interconnection of networks located in nearby buildings (for example, buildings on a college campus).

carrier sense multiple access collision avoidance (CSMA/ CA) Just as CSMA/ CD is needed for half-duplex Ethernet connections, CSMA/ CA is needed for WLAN connections because of their half-duplex operation. Similar to how an Ethernet device listens to an Ethernet segment to determine whether a frame exists on the segment, a WLAN device listens for a transmission on a wireless channel to determine whether it is safe to transmit. In addition, the collision-avoidance part of the CSMA/ CA algorithm causes wireless devices to wait for a random backoff time before transmitting.

carrier sense multiple access collision detect (CSMA/ CD) Used on an Ethernet network to help prevent a collision from occurring and to recover if a collision does occur. CSMA/ CD is only needed on half-duplex connections.

central office (CO) A building containing a telephone company's telephone-switching equipment. COs are categorized into five hierarchical classes. A Class 1 CO is a long-distance office serving a regional area. A Class 2 CO is a second-level long-distance office; that is, it is subordinate to a Class 1 office. A Class 3 CO is a third-level long-distance office. A Class 4 CO is a fourth-level long-distance office, which provides telephone subscribers access to a live operator. A Class 5 CO is at the bottom of the five-layer hierarchy and physically connects to customer devices in a local area.

Challenge Handshake Authentication Protocol (CHAP) Like PAP, CHAP performs one-way authentication. However, authentication is performed through a three-way handshake (challenge, response, and acceptance messages) between a server and a client. The three-way handshake allows a client to be authenticated

Challenge-Response Authentication Mechanism Message Digest 5 (CRAM-MD5) A common variant of HMAC frequently used in e-mail systems. Like CHAP, CRAM-MD5 only performs one-way authentication (the server authenticates the client).

channel bonding With channel bonding, two wireless bands can be logically bonded together, forming a band with twice the bandwidth of an individual band. Some literature refers to channel bonding as 40-MHz mode, which refers to the bonding of two adjacent 20-MHz bands into a 40-MHz band.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

channel service unit/ data service unit (CSU/ DSU) Acts as a digital modem that terminates a digital circuit (for example, a T1 or an E1 circuit).

circuit-switched connection A connection that is brought up on an as-needed basis. A circuit-switched connection is analogous to a phone call, where you pick up a phone, dial a number, and a connection is established based on the number you dial.

classful mask A classful mask is the default subnet mask applied to Class A, B, and C IPv4 networks. Specifically, Class A networks have a classful mask of 255.0.0.0. Class B networks have a classful mask of 255.255.0.0, and Class C networks have a classful mask of 255.255.255.0.

classification Classification is the process of placing traffic into different categories.

Classless interdomain routing (CIDR) Shortens a classful subnet mask by removing right-justified 1s from a classful mask. As a result, CIDR allows contiguous classful networks to be aggregated. This process is sometimes called route aggregation.

client Defines the device an end user uses to access a network. This device might be a workstation, laptop, smartphone with wireless capabilities, tablet, or variety of other end-user terminal devices.

client/ server network In a client/ server network, a dedicated server (for example, a file server or a print server) provides shared access to a resource (for example, files or a printer). Clients (for example, PCs) on the network with appropriate privilege levels can gain access to those shared resources.

client-to-site VPN Also known as a remote-access VPN, a client-to-site VPN interconnects a remote user with a site, as an alternative to dial-up or ISDN connectivity, at a reduced cost.

coaxial cable Also known as coax, a coaxial cable is composed of two conductors. One of the conductors is an inner insulated conductor. This inner conductor is surrounded by another conductor. This second conductor is sometimes made of a metallic foil or woven wire.

collision A collision occurs when two devices on an Ethernet network simultaneously transmit a frame. Because an Ethernet segment cannot handle more than one frame at a time, both frames become corrupted.

committed information rate (CIR) The CIR of an interface is the average traffic rate over the period of a second.

Common Address Redundancy Protocol (CARP) An open standard variant of HSRP, which provides first-hop router redundancy.

congestion avoidance If an interface's output queue fills to capacity, newly arriving packets are discarded (or tail dropped). Congestion avoidance can prevent this behavior. RED is an example of a congestion-avoidance mechanism.

congestion management When a device, such as a switch or a router, receives traffic faster than it can be transmitted, the device attempts to buffer (or store) the extra traffic until bandwidth becomes available. This buffering process is called queuing or congestion management.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

content engine A dedicated appliance whose role is to locally cache content received from a remote network (for example, a destination on the Internet). Subsequent requests for that content can be serviced locally, from the content engine, thus reducing bandwidth demand on a WAN.

content switch Can be used to load balance requests for content across a group of servers containing that content. If one of the servers in the group needed to have maintenance performed, that server could be administratively removed from the group, as defined on the content switch. As a result, the content switch can help maximize uptime when performing server maintenance. It minimizes the load on individual servers by distributing its load across multiple identical servers. A content switch also allows a network to scale because one or more additional servers could be added to the server group defined on the content switch if the load on existing servers increases.

crimper Used to attach a connector (for example, an RJ-45 connector) to the end of an unshielded twisted-pair (UTP) cable.

current state modulation One way to electrically or optically represent a binary 1 or 0 is to use current state modulation, which represents a binary 1 with the presence of voltage (on a copper cable) or the presence of light (on a fiber-optic cable). Similarly, the absence of light or voltage represents a binary 0.

customer premise equipment (CPE) This device resides at a customer site. A router, as an example, can be a CPE that connects a customer with an MPLS service provider.

cyclic redundancy check (CRC) A mathematical algorithm that is executed on a data string by both the sender and the receiver of the data string. If the calculated CRC values match, the receiver can conclude that the data string was not corrupted during transmission.

data link layer As Layer 2 of the OSI model, this layer is concerned with the packaging of data into frames and transmitting those frames on a network, performing error detection/ correction, uniquely identifying network devices with an address, and handling flow control.

decibel (dB) A ratio of radiated power to a reference value. In the case of dBi, the reference value is the signal strength (that is, the power) radiated from an isotropic antenna, which represents a theoretical antenna that radiates an equal amount of power in all directions (in a spherical pattern). An isotropic antenna is considered to have gain of 0 dBi.

decibel (dB) loss A loss of signal power. If a transmission's dB loss is too great, the transmission cannot be properly interpreted by the intended recipient.

dedicated leased line A logical connection interconnecting two sites. This logical connection might physically connect through a service provider's facility or a telephone company's central office. The expense of a dedicated leased line is typically higher than other WAN technologies offering similar data rates, because with a dedicated leased line, a customer does not have to share bandwidth with other customers.

default gateway The IP address of a router (or multilayer switch) to which a networked device sends traffic destined for a subnet other than the device's local subnet.

default static route A default static route is an administratively configured entry in a router's routing table that specifies where traffic for all unknown networks should be sent.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

demarc Also known as a demarcation point or a demarc extension, this is the point in a telephone network where the maintenance responsibility passes from a telephone company to a subscriber (unless the subscriber purchased an inside wiring plan). This demarc is typically a box mounted to the outside of a customer's building (for example, a residence).

demilitarized zone (DMZ) Often contains servers that should be accessible from the Internet. This approach would, for example, allow users on the Internet to initiate an e-mail or a web session coming into an organization's e-mail or web server. However, other protocols would be blocked.

denial of service (DoS) A DoS attack floods a system with an excessive amount of traffic or requests, which consumes the system's processing resources and prevents the system from responding to many legitimate requests.

designated port In a STP topology, every network segment has a single designated port, which is the port on that segment that is closest to the root bridge, in terms of cost. Therefore, all ports on a root bridge are designated ports.

differentiated services (DiffServ) As its name suggests, DiffServ differentiates between multiple traffic flows. Specifically, packets are marked, and routers and switches can then make decisions (for example, dropping or forwarding decisions) based on those markings.

dig command Can resolve a FQDN to an IP address on UNIX hosts.

digital subscriber line (DSL) A group of technologies that provide high-speed data transmission over existing telephone wiring. DSL has several variants, which vary in data rates and distance limitations. Three of the more popular DSL variants include asymmetric DSL (ADSL), symmetric DSL (DSL), and very high bit-rate DSL (VDSL).

Direct-sequence spread spectrum (DSSS) Modulates data over an entire range of frequencies using a series of symbols called chips. A chip is shorter in duration than a bit, meaning that chips are transmitted at a higher rate than the actual data. These chips not only represent encoded data to be transmitted, but also what appears to be random data. Because both parties involved in a DSSS communication know which chips represent actual data and which chips do not, if a third-party intercepted a DSSS transmission, it would be difficult for that party to eavesdrop on the data because he would not easily know which chips represented valid bits. DSSS is more subject to environmental factors, as opposed to FHSS and OFDN, because it uses an entire frequency spectrum.

distance vector A category of routing protocol that sends a full copy of its routing table to its directly attached neighbors.

distributed denial of service (DDoS) These attacks can increase the amount of traffic flooded to a target system. Specifically, an attacker compromises multiple systems, and those compromised systems, called zombies, can be instructed by the attacker to simultaneously launch a DDoS attack against a target system.

Domain Name System (DNS) server Performs the task of taking a domain name (for example, www.ciscopress.com) and resolving that name into a corresponding IP address (for example, 10.1.2.3).

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

dotted-decimal notation A method of writing an IPv4 address or subnet mask, where groups of 8 bits (called octets) are separated by periods.

Dynamic Host Configuration Protocol (DHCP) Dynamically assigns IP address information (for example, IP address, subnet mask, DNS server's IP address, and default gateway's IP address) to network devices.

Dynamic NAT (DNAT) A variant of NAT in which inside local addresses are automatically assigned an inside global address from a pool of available addresses.

E1 An E1 circuit contains 32 channels, in contrast to the 24 channels on a T1 circuit. Only 30 of those 32 channels, however, can transmit data (or voice or video). Specifically, the first of those 32 channels is reserved for framing and synchronization, and the 17th channel is reserved for signaling (that is, to set up, maintain, and tear down a session).

E3 A digital circuit in the same E-carrier family of standards as an E1. An E3 circuit's available bandwidth is 34.4 Mbps.

edge label switch router (ELSR) Resides at the edge of an MPLS service provider's cloud and interconnects a service provider to one or more customers.

electromagnetic interference (EMI) An electromagnetic waveform that can be received by network cable (possibly corrupting data traveling on the cable) or radiated from a network cable (possibly interfering with data traveling on another cable).

electrostatic discharge (ESD) wrist strap To prevent static electricity in your body from damaging electrical components on a circuit board, you can wear an ESD wrist strap. The strap is equipped with a clip that you can attach to something with a ground potential (for example, a large metal desk). While wearing the wrist strap, if you have any static buildup in your body, the static flows to the object with a ground potential to which your strap is clipped, thus avoiding damage to any electrical components that you might touch.

Encapsulating Security Payload (ESP) An IPsec protocol that provides authentication, integrity, and encryption services.

Enhanced Interior Gateway Routing Protocol (EIGRP) A Cisco proprietary protocol. So, although EIGRP is popular in Cisco-only networks, it is less popular in mixed-vendor networks. Like OSPF, EIGRP is an IGP with very fast convergence and high scalability. EIGRP is considered to be an advanced distance vector or a hybrid routing protocol.

Enterprise mode In the context of wireless networking, this refers to using a centralized authentication server such as RADIUS for authentication, instead of a pre-shared key (PSK).

Ethernet Ethernet is a Layer 1 technology developed by Xerox and encompasses a variety of standards, which specify various media types, speeds, and distance limitations.

extended service set (ESS) WLANs containing more than one AP are called ESS WLANs. Like BSS WLANs, ESS WLANs operate in infrastructure mode. When you have more than one AP, take care to

prevent one AP from interfering with another. Specifically, nonoverlapping channels (that is, channels 1, 6, and 11 for the 2.4-GHz band) should be selected for adjacent wireless coverage areas.

Exterior Gateway Protocol (EGP) A routing protocol that operates between autonomous systems, which are networks under different administrative control. Border Gateway Protocol (BGP) is the only EGP in widespread use today.

firewall Primarily a network security appliance, a firewall can protect a trusted network (for example, a corporate LAN) from an untrusted network (for example, the Internet) by allowing the trusted network to send traffic into the untrusted network and receive the return traffic from the untrusted network, while blocking traffic for sessions that were initiated on the untrusted network.

fox and hound See toner probe.

Frame Relay A Layer 2 WAN technology that interconnects sites using virtual circuits. These virtual circuits are identified by locally significant data-link connection identifiers (DLCI).

frequency-hopping spread spectrum (FHSS) Allows the participants in a communication to hop between predetermined frequencies. Security is enhanced because the participants can predict the next frequency to be used but a third party cannot easily predict the next frequency. FHSS can also provision extra bandwidth by simultaneously using more than one frequency.

FTP bounce An FTP bounce attack uses the FTP PORT command to covertly open a connection with a remote system. Specifically, an attacker connects to an FTP server and uses the PORT command to cause the FTP server to open a communications channel with the intended victim, which might allow a connection from the FTP server, while a connection directly from the attacker might be denied.

full duplex This connection allows a device to simultaneously transmit and receive data.

full-mesh topology Directly connects every site to every other site.

GNU privacy guard (GPC) A free variant of pretty good privacy (PGP), which is an asymmetric encryption algorithm.

half duplex A half-duplex connection allows a device to either receive or transmit data at any one time. However, a half-duplex device cannot simultaneously transmit and receive.

hardware firewall A network appliance dedicated to the purpose of acting as a firewall. This appliance can have multiple interfaces for connecting to areas of a network requiring varying levels of security.

hold-down timers Can speed the convergence process of a routing protocol. After a router makes a change to a route entry, the hold-down timer prevents subsequent updates for a specified period of time. This approach can help stop flapping routes (which are routes that oscillate between being available and unavailable) from preventing convergence.

honey net A network containing more than one honey pot.

honey pot Acts as a distracter. Specifically, a system designated as a honey pot appears to be an attractive attack target. One school of thought on the use of a honey pot is to place one or more honey-

pot systems in a network to entice attackers into thinking the system is real. The attackers then use their resources attacking the honey pot, resulting in their leaving the real servers alone.

host-based IPS (HIPS) A HIPS system is a computer running intrusion prevention software for the purpose of protecting the computer from attacks.

host command Can resolve a FQDN to an IP address on hosts.

hub An Ethernet hub is an older technology used to interconnect network components, such as clients and servers. Hubs vary in their number of available ports. A hub does not perform an inspection of the traffic it passes. Rather, a hub simply receives traffic in a port and repeats that traffic out all of its other ports.

hub-and-spoke topology When interconnecting multiple sites (for example, multiple corporate locations) via WAN links, a hub-and-spoke topology has a WAN link from each remote site (a spoke site) to the main site (the hub site).

independent basic service set (IBSS) A WLAN can be created without the use of an AP. Such a configuration, called an IBSS, is said to work in an ad-hoc fashion. An ad hoc WLAN is useful for temporary connections between wireless devices. For example, you might temporarily interconnect two laptop computers to transfer a few files.

integrated services (IntServ) Often referred to as hard QoS because IntServ can make strict bandwidth reservations. IntServ uses signaling among network devices to provide bandwidth reservations.

Resource Reservation Protocol (RSVP) is an example of an IntServ approach to QoS. Because IntServ must be configured on every router along a packet's path, a primary drawback of IntServ is its lack of scalability.

Integrated Services Digital Network (ISDN) A digital telephony technology that supports multiple 64-kbps channels (known as bearer channels or B channels) on a single connection. ISDN was popular back in the 1980s for connecting PBXs, which are telephone switches owned and operated by a company, to a telephone company's central office. ISDN has the ability to carry voice, video, or data over its B channels. ISDN also offers a robust set of signaling protocols: Q. 921 for Layer 2 signaling and Q. 931 for Layer 3 signaling. These signaling protocols run on a separate channel in an ISDN circuit (known as the delta channel, data channel, or D channel).

Interior Gateway Protocol (IGP) A routing protocol that operates within an autonomous system, which is a network under a single administrative control. OSPF and EIGRP are popular examples of IGPs.

Intermediate System-to-Intermediate System (IS-IS) A link-state routing protocol similar in its operation to OSPF. IS-IS uses a configurable, yet dimensionless, metric associated with an interface and runs Dijkstra's shortest path first algorithm. Although using IS-IS as an IGP offers the scalability, fast convergence, and vendor-interoperability benefits of OSPF, it has not been deployed as widely as OSPF.

Internet Group Management Protocol (IGMP) A multicast protocol used between clients and routers to let routers know which of their interfaces has a multicast receiver attached.

Internet Key Exchange (IKE) A protocol used to set up an IPsec session.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

Internet layer This layer of the TCP/ IP stack maps to Layer 3 (network layer) of the OSI model. Although multiple routed protocols (for example, IPv4 and IPv6) may reside at the OSI model's network layer, the Internet layer of the TCP/ IP stack focuses on IP as the protocol to be routed through a network.

Internet Security Association and Key Management Protocol (ISAKMP) Negotiates parameters for an IPsec session.

intrusion detection system (IDS) IDS devices can recognize the signature of a well-known attack and respond to stop the attack. However, an IDS sensor does not reside in-line with the traffic flow. Therefore, one or more malicious packets might reach an intended victim before the traffic flow is stopped by an IDS sensor.

intrusion prevention system (IPS) IPS devices can recognize the signature of a well-known attack and respond to stop the attack. An IPS device resides in-line with the traffic flow, unlike an IDS sensor.

IP Security (IPsec) A type of VPN that provides confidentiality, integrity, and authentication.

ipconfig command A Microsoft Windows command that can be used to display IP address configuration parameters on a PC. In addition, if DHCP is used by the PC, the ipconfig command can be used to release and renew a DHCP lease, which is often useful during troubleshooting.

jitter The uneven arrival of packets.

Kerberos A client-server authentication protocol that supports mutual authentication between a client and a server. Kerberos uses the concept of a trusted third party (a key distribution center) that hands out tickets to be used instead of a username and password combination.

label switch router (LSR) Resides inside a service provider's MPLS cloud and makes frame forwarding decisions based on labels applied to frames.

latency The measure of delay in a network.

Layer 2 Forwarding (L2F) A VPN protocol designed (by Cisco Systems) with the intent of providing a tunneling protocol for PPP. Like L2TP, L2F lacks native security features.

Layer 2 Tunneling Protocol (L2TP) A VPN protocol that lacks security features, such as encryption. However, L2TP can still be used for a secure VPN connection if it is combined with another protocol that provides encryption.

link aggregation As defined by the IEEE 802.3ad standard, link aggregation allows multiple physical connections to be logically bundled into a single logical connection.

link efficiency To make the most of the limited bandwidth available on slower speed links, you might choose to implement compression or link fragmentation and interleaving (LFI). These QoS mechanisms are examples of link efficiency mechanisms.

link-local IP address A link-local IP address is a nonroutable IP address usable only on a local subnet.

link state A category of routing protocol that maintains a topology of a network and uses an algorithm to determine the shortest path to a destination network.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

link-state advertisement (LSA) Sent by routers in a network to advertise the networks the routers know how to reach. Routers use those LSAs to construct a topological map of a network. The algorithm run against this topological map is Dijkstra's shortest path first algorithm.

local-area network (LAN) Interconnects network components within a local region (for example, within a building).

local loop A connection between a customer premise and a local telephone company's central office.

logical topology The actual traffic flow of a network determines the network's logical topology.

marking Alters bits within a frame, cell, or packet to indicate how a network should treat that traffic. Marking alone does not change how a network treats a packet. Other tools (such as queuing tools) can, however, reference markings and make decisions (for example, forwarding decisions or dropping decisions) based on those markings.

maximum transmission unit (MTU) The largest packet size supported on an interface.

media Devices need to be interconnected via some sort of media. This media could be copper cabling. Alternatively, it could be a fiber-optic cable. Media might not even be a cable, as is the case with wireless networks, where radio waves travel through the media of air.

metric A value assigned to a route. Lower metrics are preferred over higher metrics.

metropolitan-area network (MAN) Interconnects locations scattered throughout a metropolitan area.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) A Microsoft-enhanced version of CHAP, offering a collection of additional features not present with PAP or CHAP, including two-way authentication. Microsoft Routing and Remote Access Server (RRAS) A Microsoft Windows server feature that allows Microsoft Windows clients to remotely access a Microsoft Windows network.

multicast A multicast communication flow is a one-to-many flow.

multifactor authentication Similar to two-factor authentication, multifactor authentication requires two or more types of successful authentication before granting access to a network.

multilayer switch Like a router, a multilayer switch can make traffic forwarding decisions based on Layer 3 information. Although multilayer switches more closely approach wire-speed throughput than most routers, routers tend to have a greater feature set and are capable of supporting more interface types than a multilayer switch.

multimode fiber (MMF) Multimode fiber-optic cabling has a core with a diameter large enough to permit the injection of light into the core at multiple angles. The different paths (that is, modes) that light travels can lead to multimode delay distortion, which causes bits to be received out of order because the pulses of light representing the bits traveled different paths (and therefore, different distances).

multiple input multiple output (MIMO) MIMO uses multiple antennas for transmission and reception. These antennas do not interfere with one another, thanks to MIMO's use of spatial multiplexing, which encodes data based on the antenna from which the data will be transmitted. Both reliability and throughput can be increased with MIMO's simultaneous use of multiple antennas.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

Multiprotocol Label Switching (MPLS) A WAN technology popular among service providers. MPLS performs labels switching to forward traffic within an MPLS cloud by inserting a 32-bit header (which contains a 20-bit label) between a frame's Layer 2 and Layer 3 headers and making forwarding decisions based on the label within an MPLS header.

nbtstat command Displays NetBIOS information for IP-based networks. The nbt prefix of the nbtstat command refers to NetBIOS over TCP/ IP, which is called NBT (or NetBT). This command can, for example, display a listing of NetBIOS device names learned by a Microsoft Windows-based PC.

Nessus A network-vulnerability scanner available from Tenable Network Security.

netstat command Can display a variety of information about IP-based connections on a Windows or UNIX host.

Network Address Translation (NAT) Allows private IP addresses (as defined in RFC 1918) to be translated into Internet-routable IP addresses (public IP addresses).

network as a service (NaaS) A service provider offering where clients can purchase data services (for example, e-mail, LDAP, and DNS services) traditionally hosted in a corporate data center.

network interface layer The network interface layer of the TCP/ IP stack (also known as the network access layer) encompasses the technologies addressed by Layers 1 and 2 (that is, the physical and data link layers) of the OSI model.

network layer Layer 3 of the OSI model, it is primarily concerned with forwarding data based on logical addresses.

network-based IDS (NIDS) A NIDS device is a network appliance dedicated to the purpose of acting as an IDS sensor.

network-based IPS (NIPS) A NIPS device is a network appliance dedicated to the purpose of acting as an IPS sensor.

next hop An IP address on the next router to which traffic should be forwarded.

Nmap A network-vulnerability scanner.

nondesignated port In STP terms, nondesignated ports block traffic to create a loop-free topology.

nslookup command Can resolve a FQDN to an IP address on Microsoft Windows and UNIX hosts.

octet A grouping of 8 bits. An IPv4 address consists of four octets (that is, a total of 32 bits).

offsite The term offsite in the context of virtualization technologies refers to hosting virtual devices on hardware physically located in a service provider's data center.

omnidirectional antenna Radiates power at relatively equal power levels in all directions (somewhat similar to the theoretical isotropic antenna). Omnidirectional antennas are popular in residential WLANs and SOHO locations.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

onsite The term onsite in the context of virtualization technologies refers to hosting virtual devices on hardware physically located in a corporate data center.

open A broken strand of copper that prevents current from flowing through a circuit.

Open Shortest Path First (OSPF) A link-state routing protocol that uses a metric of cost, which is based on the link speed between two routers. OSPF is a popular IGP because of its scalability, fast convergence, and vendor interoperability.

Open Systems Interconnection (OSI) reference model Commonly referred to as the OSI model or the OSI stack. This seven-layer model categorizes various network technologies.

optical carrier (OC) Optical networks often use OC levels to indicate bandwidth. As a base reference point, the speed of an OC-1 link is 51.84 Mbps. Other OC levels are multiples of an OC-1. For example, an OC-3 link has three times the bandwidth of an OC-1 link (that is, 3 * 51.84 Mbps = 155.52 Mbps).

optical time domain reflectometer (OTDR) Detects the location of a fault in a fiber cable by sending light down the fiber-optic cable and measuring the time required for the light to bounce back from the cable fault. The OTDM can then mathematically calculate the location of the fault.

orthogonal frequency-division multiplexing (OFDM) Whereas DSSS uses a high modulation rate for the symbols it sends, OFDM uses a relatively slow modulation rate for symbols. This slower modulation rate, combined with the simultaneous transmission of data over 52 data streams, helps OFDM support high data rates while resisting crosstalk between the various data streams.

packet-switched connection Similar to a dedicated leased line, because most packet-switched networks are always on. However, unlike a dedicated leased line, packet-switched connections allow multiple customers to share a service provider's bandwidth.

partial-mesh topology A hybrid of a hub-and-spoke topology and a full-mesh topology. A partial-mesh topology can be designed to provide an optimal route between selected sites, while avoiding the expense of interconnecting every site to every other site.

Password Authentication Protocol (PAP) Performs one-way authentication (that is, a client authenticates with a server). However, a significant drawback to PPP, other than its unidirectional authentication, is its clear-text transmission of credentials, which could permit an eavesdropper to learn authentication credentials.

peer-to-peer network Allows interconnected devices (for example, PCs) to share their resources with one another. These resources could be, for example, files or printers.

personal-area network (PAN) A network whose scale is smaller than a LAN. As an example, a connection between a PC and a digital camera via a USB cable is considered to be a PAN.

Personal mode In the context of wireless networking, this refers to using a pre-shared key (PSK) instead of a centralized server, such as RADIUS, for authentication.

physical layer Layer 1 of the OSI model, it is concerned with the transmission of bits on a network.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

physical topology The way a network's components are physically interconnected determines the network's physical topology.

ping command One of the most commonly used command-line commands. It can check IP connectivity between two network devices. Multiple platforms (for example, routers, switches, and hosts) support the ping command.

plain old telephone service (POTS) A POTS connection connects a customer device (such as a telephone) to the public switched telephone network (PSTN).

plenum Plenum cabling is fire retardant and minimizes toxic fumes released by network cabling if that cable were to catch on fire. As a result, plenum cabling is often a requirement of local fire codes for cable in raised flooring or in other open-air return ducts.

Point-to-Point Protocol (PPP) A common Layer 2 protocol offering features such as multilink interface, looped link detection, error detection, and authentication.

Point-to-Point Protocol over Ethernet (PPPoE) Commonly used between a DSL modem in a home (or business) and a service provider. Specifically, PPPoE encapsulates PPP frames within Ethernet frames. PPP is used to leverage its features, such as authentication.

Point-to-Point Tunneling Protocol (PPTP) An older VPN protocol (that supported the dial-up networking feature in older versions of Microsoft Windows). Like L2TP and L2F, PPTP lacks native security features. However, Microsoft's versions of PPTP bundled with various versions of Microsoft Windows were enhanced to offer security features.

poison reverse This feature of a distance-vector routing protocol causes a route received on one interface to be advertised back out of that same interface with a metric considered to be infinite.

policing Instead of making a minimum amount of bandwidth available for specific traffic types, you might want to limit available bandwidth. Both policing and traffic-shaping tools can accomplish this objective. Collectively, these tools are called traffic conditioners. Policing can drop exceeding traffic, as opposed to buffering it.

Port Address Translation (PAT) A variant of NAT in which multiple inside local IP addresses share a single inside global IP address. PAT can distinguish between different flows based on port numbers.

Power over Ethernet (PoE) Defined by the IEEE 802.3af and 802.3at standards, PoE allows an Ethernet switch to provide power to an attached device (for example, a wireless access point, security camera, or IP phone) by applying power to the same wires in a UTP cable that are used to transmit and receive data.

prefix notation A method of indicating how many bits are in a subnet mask. For example, /24 is prefix notation for a 24-bit subnet mask. Prefix notation is also known as slash notation.

presentation layer Layer 6 of the OSI model, it is responsible for the formatting of data being exchanged and securing the data with encryption.

pretty good privacy (PGP) PGP is a widely deployed asymmetric encryption algorithm and is often used to encrypt e-mail traffic.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

primary rate interface (PRI) A PRI circuit is an ISDN circuit built on a T1 or E1 circuit. Recall that a T1 circuit has 24 channels. Therefore, if a PRI circuit is built on a T1 circuit, the ISDN circuit has 23 B channels and 1 64-Kbps D channel. The 24th channel in the T1 circuit serves as the ISDN D channel (that is, the channel used to carry the Q. 921 and Q. 931 signaling protocols, which set up, maintain, and tear down connections).

private IP addresses Specific Class A, B, and C networks have been designed for private use. Although these networks are routable (with the exception of the 169.254.0.0– 169.254.255.255 address range), within the organization, service providers do not route these private networks over the public Internet.

protocol data unit (PDU) The name given to data at different layers of the OSI model. Specifically, the PDU for Layer 4 is segment. The Layer 3 PDU is packet, the Layer 2 PDU is frame, and the Layer 1 PDU is bit.

Protocol Independent Multicast (PIM) A multicast protocol used between multicast-enabled routers to construct a multicast distribution tree.

proxy server Intercepts requests being sent from a client and forwards those requests on to their intended destination. The proxy server then sends any return traffic to the client that initiated the session. This provides address hiding for the client. Also, some proxy servers conserve WAN bandwidth by offering a content caching function. In addition, some proxy servers offer URL filtering to, for example, block users from accessing social networking sites during working hours.

public key infrastructure (PKI) A PKI system uses digital certificates and a certificate authority to allow secure communication across a public network.

public switched telephone network (PSTN) The worldwide telephony network consisting of multiple telephone carriers.

punch-down tool When terminating wires on a punch-down block (for example, a 110 block), you should use a punch-down tool, which is designed to properly insert an insulated wire between two contact blades in a punch-down block, without damaging the blades.

Real-time Transport Protocol (RTP) A Layer 4 protocol that carries voice (and interactive video). reliability The measure of how error-free a network transmits packets.

remote-access VPN See client-to-site VPN.

Remote Authentication Dial-In User Service (RADIUS) A UDP-based protocol used to communicate with a AAA server. Unlike TACACS +, RADIUS does not encrypt an entire authentication packet, but only the password. However, RADIUS offers more robust accounting features than TACACS +. Also, RADIUS is a standards-based protocol, whereas TACACS + is a Cisco proprietary protocol.

ring topology In a ring topology, traffic flows in a circular fashion around a closed network loop (that is, a ring). Typically, a ring topology sends data, in a single direction, to each connected device in turn, until the intended destination receives the data.

root port In a STP topology, every nonroot bridge has a single root port, which is the port on that switch that is closest to the root bridge, in terms of cost.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

route command Can add, modify, or delete routes in the IP routing table of Microsoft Windows and UNIX hosts. In addition, the route command can be used to view the IP routing table of Microsoft Windows hosts.

route redistribution Allows routes learned by one routing protocol to be injected into the routing process of another routing protocol.

routed protocol A protocol with an addressing scheme (for example, IP) that defines different network addresses.

router A router is considered a Layer 3 device, meaning that it makes its forwarding decisions based on logical network addresses. Most modern networks use IP addressing.

Routing Information Protocol (RIP) A distance-vector routing protocol that uses a metric of hop count. The maximum number of hops between two routers in an RIP-based network is 15. Therefore, a hop count of 16 is considered to be infinite. RIP is considered to be an IGP.

routing protocol A routing protocol (for example, RIP, OSPF, or EIGRP) that advertises route information between routers, which describes how to reach specified destination networks.

RSA A popular and widely deployed asymmetric encryption algorithm.

satellite (WAN technology) Provides WAN access to sites where terrestrial WAN solutions are unavailable. Satellite WAN connections can suffer from long round-trip delay (which can be unacceptable for latency-sensitive applications) and are susceptible to poor weather conditions.

Secure Sockets Layer (SSL) Provides cryptography and reliability for upper layers (Layers 5– 7) of the OSI model. SSL, which was introduced in 1995, has largely been replaced by Transport Layer Security (TLS). However, recent versions of SSL (for example, SSL 3.3) have been enhanced to be more comparable with TLS. Both SSL and TLS are able to provide secure web browsing via HTTPS.

security association (SA) An agreement between the two IPsec peers about the cryptographic parameters to be used in an ISAKMP session.

security policy A continually changing document that dictates a set of guidelines for network use. These guidelines complement organizational objectives by specifying rules for how a network is used.

server As its name suggests, a server serves up resources to a network. These resources might include e-mail access as provided by an e-mail server, web pages as provided by a web server, or files available on a file server.

service set identifier (SSID) A string of characters that identifies a WLAN. APs participating in the same WLAN can be configured with identical SSIDs. An SSID shared among multiple APs is called an extended service set identifier (ESSID).

Session Initiation Protocol (SIP) A VoIP signaling protocol used to set up, maintain, and tear down VoIP phone calls.

session layer As Layer 5 of the OSI model, it's responsible for setting up, maintaining, and tearing down sessions.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

shielded twisted-pair (STP) cable STP cabling prevents wires in a cable from acting as an antenna, which might receive or transmit EMI. STP cable might have a metallic shielding, similar to the braided wire that acts as an outer conductor in a coaxial cable.

short A short occurs when two copper connectors touch each other, resulting in current flowing through that short rather than the attached electrical circuit, because the short has lower resistance.

Simple Network Management Protocol (SNMP) A protocol used to monitor and manage network devices, such as routers, switches, and servers.

single-mode fiber (SMF) SMF cabling has a core with a diameter large enough to permit only a single path for light pulses (that is, only one mode of propagation). By having a single path for light to travel, SMF eliminates the concern of multimode delay distortion.

single sign-on (SSO) Allows a user to authenticate once to gain access to multiple systems, without requiring the user to independently authenticate with each system.

site-to-site VPN Interconnects two sites, as an alternative to a leased line, at a reduced cost.

slash notation See prefix notation.

social engineering Attackers sometimes use social techniques (which often leverage people's desire to be helpful) to obtain confidential information. For example, an attacker might pose as a member of an IT department and ask a company employ for her login credentials in order for the "IT staff to test the connection." This type of attack is called social engineering.

software firewall A computer running firewall software. For example, the software firewall could protect the computer itself (for example, preventing incoming connections to the computer). Alternatively, a software firewall could be a computer with more than one network interface card that runs firewall software to filter traffic flowing through the computer.

Spanning Tree Protocol (STP) Defined by the IEEE 802.1D standard, it allows a network to have redundant Layer 2 connections, while logical preventing a loop, which could lead to symptoms such as broadcast storms and MAC address table corruption.

split horizon This feature of a distance-vector routing protocol prevents a route learned on one interface from being advertised back out of that same interface.

star topology In a star topology, a network has a central point (for example, a switch) from which all attached devices radiate.

state transition modulation One way to electrically or optically represent a binary 1 or 0 is to use the transition between a voltage level (for example, going from a state of no voltage to a state of voltage, or vice versa, on a copper cable) or the transition of having light or no light on a fiber optic cable to represent a binary 1. Similarly, a binary 0 is represented by having no transition in a voltage level or light level from one time period to the next. This approach of representing binary digits is called state transition modulation.

stateful firewall Inspects traffic leaving the inside network as it goes out to the Internet. Then, when returning traffic from the same session (as identified by source and destination IP addresses and port

numbers) attempts to enter the inside network, the stateful firewall permits that traffic. The process of inspecting traffic to identify unique sessions is called stateful inspection.

Static NAT (SNAT) A variant of NAT in which an inside local IP address is statically mapped to an inside global IP address. SNAT is useful for servers inside a network that need to be accessible from an outside network.

Supervisory Control and Data Acquisition (SCADA) network Specialized network that provides control of remote equipment for monitoring and control of that equipment. A power plant or gas refinery would have a SCADA network.

supplicant In a network using 802.1X user authentication, a supplicant is the device that wants to gain access to a network.

switch Like an Ethernet hub, an Ethernet switch interconnects network components. Like a hub, switches are available with a variety of port densities. However, unlike a hub, a switch doesn't simply take traffic in on one port and forward copies of that traffic out all other ports. Rather, a switch learns which devices reside off of which ports. As a result, when traffic comes in a switch port, the switch interrogates the traffic to see where it's destined. Then, based on what the switch has learned, the switch forwards the traffic out of the appropriate port and not out all of the other ports.

symmetric encryption With symmetric encryption, both the sender and the receiver of a packet use the same key (a shared key) for encryption and decryption.

Synchronous Optical Network (SONET) A Layer 1 technology that uses fiber-optic cabling as its media. Because SONET is a Layer 1 technology, it can be used to transport various Layer 2 encapsulation types, such as ATM. Also, because SONET uses fiber-optic cabling, it offers high data rates, typically in the 155-Mbps to 10-Gbps range, and long-distance limitations, typically in the 20-km to 250-km range.

syslog A syslog-logging solution consists of two primary components: syslog servers, which receive and store log messages sent from syslog clients; and syslog clients, which can be a variety of network devices that send logging information to a syslog server.

T1 T1 circuits were originally used in telephony networks, with the intent of one voice conversation being carried in a single channel (that is, a single DS0). A T1 circuit consists of 24 DS0s, and the bandwidth of a T1 circuit is 1.544 Mbps.

T3 In the same T-carrier family of standards as a T1, a T3 circuit offers an increased bandwidth capacity. Although a T1 circuit combines 24 DS0s into a single physical connection to offer 1.544 Mbps of bandwidth, a T3 circuit combines 672 DS0s into a single physical connection, with a resulting bandwidth capacity of 44.7 Mbps. TCP/ IP stack Also known as the DoD model, this four-layer model (as opposed to the seven-layer OSI model) targets the suite of TCP/ IP protocols.

telco A telephone company. Some countries have government-maintained telcos, and other countries have multiple telcos that compete with one another.

Terminal Access Controller Access-Control System Plus (TACACS +) A TCP-based protocol used to communicate with a AAA server. Unlike RADIUS, TACACS + encrypts an entire authentication packet

rather than just the password. TACACS + offers authentication features, but they are not as robust as the accounting features found in RADIUS. Also, unlike RADIUS, TACACS + is a Cisco-proprietary protocol.

time-division multiplexing (TDM) Supports different communication sessions (for example, different telephone conversations in a telephony network) on the same physical medium by allowing sessions to take turns. For a brief period of time, defined as a time slot, data from the first session is sent, followed by data from the second sessions. This continues until all sessions have had a turn, and the process repeats itself.

time domain reflectometer (TDR) Detects the location of a fault in a copper cable by sending an electric signal down the copper cable and measuring the time required for the signal to bounce back from the cable fault. A TDM can then mathematically calculate the location of the fault.

Time To Live (TTL) The TTL field in an IP header is decremented once for each router hop. Therefore, if the value in a TTL field is reduced to 0, a router discards the frame and sends a time exceeded ICMP message back to the source.

tip and ring The red and green wires found in an RJ-11 wall jacks, which carry voice, ringing voltage, and signaling information between an analog device (for example, a phone or a modem) and an RJ-11 wall jack.

toner probe Sometimes called a fox and hound, a toner probe allows you to place a tone generator at one end of the connection (for example, in someone's office) and use a probe on the punch-down block to audibly detect to which pair of wires the tone generator is connected.

traceroute command A UNIX command that displays every router hop along the path from a source host destination host on an IP network. Information about the router hop can include the IP address of the router hop and the round-trip delay of that router hop.

tracert command A Microsoft Windows-based command that displays every router hop along the path from a source host to a destination host on an IP network. Information about a router hop can include such information as the IP address of the router hop and the round-trip delay of that router hop.

traffic shaping Instead of making a minimum amount of bandwidth available for specific traffic types, you might want to limit available bandwidth. Both policing and shaping tools can accomplish this objective. Collectively, these tools are called traffic conditioners. Traffic shaping delays excess traffic by buffering it as opposed to dropping the excess traffic.

Transmission Control Protocol (TCP) A connection-oriented transport protocol. Connection-oriented transport protocols provide reliable transport, in that if a segment is dropped, the sender can detect that drop and retransmit that dropped segment. Specifically, a receiver acknowledges segments that it receives. Based on those acknowledgments, a sender can determine which segments were successfully received.

transport layer (OSI model) As Layer 4 of the OSI model, it acts as a dividing line between the upper layers and the lower layers. Specifically, messages are taken from the upper layers (Layers 5– 7) and encapsulated into segments for transmission to the lower layers (Layers 1– 3). Similarly, data streams

coming from lower layers are decapsulated and sent to Layer 5 (the session layer) or some other upper layer, depending on the protocol.

transport layer (TCP/ IP stack) The transport layer of the TCP/ IP stack maps to Layer 4 (transport layer) of the OSI model. The two primary protocols found at the TCP/ IP stack's transport layer are TCP and UDP.

trouble ticket A problem report explaining the details of an issue being experienced in a network.

trunk In the context of an Ethernet network, this is a single physical or logical connection that simultaneously carries traffic for multiple VLANs. However, a trunk also refers to an interconnection between telephone switches, in the context of telephony.

twisted-pair cable Today's most popular media type is twisted-pair cable, where individually insulated copper strands are intertwined into a twisted-pair cable. Two categories of twisted-pair cable include shielded twisted pair (STP) and unshielded twisted pair (UTP).

two-factor authentication (TFA) Requires two types of authentication from a user seeking admission to a network. For example, a user might need to know something (for example, a password) and have something (for example, a specific fingerprint that can be checked with a biometric authentication device).

unicast A unicast communication flow is a one-to-one flow.

unidirectional antenna Unidirectional antennas can focus their power in a specific direction, thus avoiding potential interference with other wireless devices and perhaps reaching greater distances than those possible with omnidirectional antennas. One application for unidirectional antennas is interconnecting two nearby buildings.

unified threat management (UTM) A firewall or gateway that attempts to bundle multiple security functions into a single physical or logical device.

uninterruptible power supply (UPS) An appliance that provides power to networking equipment in the event of a power outage.

unshielded twisted-pair (UTP) cable Blocks EMI from the copper strands making up a twisted-pair cable by twisting the strands more tightly (that is, more twists per centimeter [cm]). By wrapping these strands around each other, the wires insulate each other from EMI.

User Datagram Protocol (UDP) A connectionless transport protocol. Connectionless transport protocols provide unreliable transport, in that if a segment is dropped, the sender is unaware of the drop, and no retransmission occurs.

virtual desktop A virtual desktop solution allows a user to store data in a centralized data center, as opposed to the hard drive of his local computer. Then, with appropriate authentication credentials, that user can access his data from various remote devices (for example, his smartphone or another computer).

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.

virtual LAN (VLAN) A single broadcast domain, representing a single subnet. Typically, a group of ports on a switch is assigned to a single VLAN. For traffic to travel between two VLANs, that traffic needs to be routed.

virtual PBX Usually a VoIP telephony solution hosted by a service provider, which interconnects with a company's existing telephone system.

virtual private network (VPN) Some VPNs can support secure communication between two sites over an untrusted network (for example, the Internet).

virtual server Allows a single physical server to host multiple virtual instances of various operating systems. This allows, for example, a single physical server to simultaneously host multiple Microsoft Windows servers and multiple Linux servers.

virtual switch Performs Layer 2 functions (for example, VLAN separation and filtering) between various server instances running on a single physical server.

warchalking If an open WLAN (or a WLAN whose SSID and authentication credentials are known) is found in a public place, a user might write a symbol on a wall (or some other nearby structure) to let others know the characteristics of the discovered network. This practice, which is a variant of the decades-old practice of hobos leaving symbols as messages to fellow hobos, is called warchalking.

wide-area network (WAN) Interconnects network components that are geographically separated.

wide-area network (WAN) link An interconnection between two devices in a WAN.

Wi-Fi Protected Access (WPA) The Wi-Fi Alliance (a nonprofit organization formed to certify interoperability of wireless devices) developed its own security standard to address the weaknesses of Wired Equivalent Privacy (WEP). This new security standard was called Wi-Fi Protected Access (WPA) Version 1. Wi-Fi Protected Access Version 2 (WPA2) Uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. These algorithms enhance the security offered by WPA.

Wired Equivalent Privacy (WEP) A security standard for WLANs. With WEP, an AP is configured with a static WEP key. Wireless clients needing to associate with an AP are configured with an identical key (making this a preshared key [PSK] approach to security). The IEEE 802.11 standard specifies a 40-bit WEP key, which is considered to be a relatively weak security measure.

wireless access point (AP) A device that connects to a wired network and provides access to that wired network for clients that wirelessly attach to the AP.

wireless router Attaches to a wired network and provides access to that wired network for wirelessly attached clients, like a wireless AP. However, a wireless router is configured such that the wired interface that connects to the rest of the network (or to the Internet) is on a different IP network than the wireless clients. Typically, a wireless router performs NATing between these two IP address spaces.

Zeroconf A technology that performs three basic functions: assigning link-local IP addresses, resolving computer names to IP addresses, and locating network services.

Barker, Keith and Kevin Wallace. *CompTIA® Network+ N10-006 Cert Guide.* Indianapolis, IN: Pearson Certification, 2015. Print.