Glossary

A

access link
A port on a switch that is used to link to an individual device. Most ports on switches are access links.

ad hoc wireless network
Offers equal sharing between devices without the use of a wireless access point (WAP).

Address Resolution Protocol (ARP)
Resolves IP addresses to Media Access Control (MAC) addresses. MAC addresses are also known as physical addresses. The `arp -a` command (issued at the command prompt) can retrieve the contents of the ARP cache.

Application layer
Layer 7 of the OSI Model and the top layer of the TCP/IP Model. Protocols such as DNS, DHCP, and SMTP operate on the Application layer. Proxy servers and advanced firewalls operate on the Application layer.

Automatic Private Internet Protocol Addressing (APIPA)
DHCP clients automatically assign themselves an APIPA address if they are unable to get an IP address from a DHCP server. An APIPA address always starts with 169.254 in the IP address. It can be any address in the range of 169.254.0.1 to 169.254.255.254.

B

basic service set (BSS)
A group of computers connected with a WAP and share the same SSID.

broadband cable
A method of connecting to the Internet. It uses the same cable used by cable TV and splits the TV and Internet signals. The computer is connected to a cable modem to provide Internet access.

broadcast
Network traffic from one network device to all other network devices on a subnet.

broadcast domain
A group of devices on a network that can receive broadcast traffic from each other. Routers create separate broadcast domains.

C

Classless Inter-Domain Routing (CIDR)
An upgrade of classful IP addressing. IP addresses are accompanied with a subnet mask, and the subnet mask doesn’t have to comply with conventional classful IP addressing rules. CIDR notation identifies the subnet mask with a slash (/) and the number of 1s in the subnet mask such as 192.168.1.20/26 to represent a subnet mask of 255.255.255.192.
**collision domain**
A group of devices on the same segment that are subject to collisions. Switches create separate collision domains.

**command prompt**
A text-based command window. Users can enter commands in this window such as ping, ipconfig, netstat, and more.

**crossover cable**
A twisted-pair cable with specific wires swapped or crossed over on one of the two cable connections. Crossover cables connect similar networking devices such as a switch to a switch, a switch to a router, or a cable modem to a router.

**crosstalk**
A potential problem that occurs when copper cables (such as twisted pair) are close to each other. Data from one cable crosses over to the other cable causing collisions or resulting in loss of confidentiality.

**CSMA/CA**
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is the transmission type used with wireless networks. CSMA/CA prevents collisions, whereas CSMA/CD contends with the collision after it happens.

**CSMA/CD**
Carrier Sense Multiple Access/Collision Detection (CSMA/CD) defines the rules for network communication on an Ethernet LAN. It detects collisions and dictates how data is resent after a collision.

**Data Link layer**
Layer 2 of the OSI Model. It has two sublayers: Logical Link Control (LLC) and Media Access Control (MAC).

**default gateway**
The IP address on the near side of the router in a subnet. The default gateway usually provides a path to the Internet.

**dial-up**
A method of connecting to the Internet. Dial-up uses regular phone lines and an analog modem. The modem modulates and demodulates the signals. Dial-up is also a method used for remote access servers where the user dials the remote access server instead of using a VPN.

**digital subscriber line (DSL)**
A method of connecting to the Internet in urban areas using digital signals over standard telephone lines. Users must be relatively close to the telephone company’s central office. The central office can be as far away as 2 miles, but some equipment requires users to be closer.

**directly connected route**
A path to a subnet that is directly connected to a router. Routers automatically know the patch for any directly connected subnets as directly connected routes.
**domain**
A LAN with a domain controller hosting Active Directory Domain Services (AD DS). AD DS includes user and computer accounts for all users and computers that are granted access on the LAN.

**Domain Naming System (DNS)**
A service that runs on a server to resolve host names. DNS servers are used on the Internet and on internal networks.

**Dynamic Host Configuration Protocol (DHCP)**
A protocol used to dynamically assign TCP/IP configuration information such as the IP address, subnet mask, default gateway, and address of a DNS server. Windows Server 2008 servers can be configured as DHCP servers.

**dynamic routing**
Routers can have the routing table updated manually or dynamically. Dynamic routing means that a routing protocol automatically updates the routing table. Common routing protocols used in internal networks include RIPv2 and OSPF.

**Ethernet**
A group of technologies used to connect networks using media such as twisted-pair and fiber-optic connections. Ethernet is defined by IEEE 802.3.

**extended service set (ESS)**
An ESS is an extension of a basic service set (BSS). It connects multiple BSSs together using more than one WAP as wireless repeaters.

**extranet**
An area between the Internet and an intranet hosting resources for trusted entities. Trusted entities are able to access these resources through the Internet.

**fiber-optic cable**
A cable type that uses light pulses instead of electrical signals to send data down a glass or plastic core cable. Fiber is immune to EMI, RFI, and crosstalk.

**File Transfer Protocol (FTP)**
A protocol used to transfer files over the Internet using TCP. Many operating systems such as Windows 7 include an FTP command-line tool. FTP uses ports 20 and 21.

**firewall**
A host-based or network-based device that filters inbound and outbound traffic. Firewalls use rules to define the filters.

**electromagnetic interference (EMI)**
EMI is interference caused by machinery and electrical devices.
**frame**
The name of data traveling on the Data Link layer of the OSI Model. Packets travel on the Network layer, and segments travel on the Transport layer.

**global unicast address**
An IPv6 address used on the Internet similar to IPv4 public IP addresses. Global unicast addresses start with the first three bits as 001 or as 2 with the first number. Most have a prefix of 2001, but others are also in use.

**host cache**
An area of memory on any computer that stores previously resolved host names and their IP addresses. It’s also called the DNS resolver cache since many of the entries are created when DNS is queried to resolve a host name. You can view the host cache with `ipconfig /displaydns` and flush the cache with `ipconfig /flushdns`.

**host name**
A user-friendly name for a computer or other network device. Host names are on the Internet and most internal networks. The primary name resolution method for host names is DNS.

**hosts file**
A text file in the `c:\windows\system32\drivers\etc` folder by default. The hosts file maps the names of computers to IP addresses.

**hub**
A hub is a layer 1 device that connects multiple devices in an Ethernet environment. Data sent in one port goes out all other ports, creating a single collision domain for all connected devices.

**Hypertext Markup Language (HTML)**
A language used to define how web pages are formatted. HTML pages are transferred over the Internet using HTTP. HTML pages are displayed in web browsers.

**Hypertext Transfer Protocol (HTTP)**
The primary protocol used to transfer web pages and web elements such as pictures and audio files over the Internet. HTTP commonly transfers HTML files that are displayed in web browsers. HTTP uses port 80. HTTPS is a secure version of HTTP using port 443.

**IEEE 802.1a**
A wireless standard that uses a frequency of 5 GHz and supports speeds as high as 54 Mbps.

**IEEE 802.1b**
A wireless standard that uses a frequency of 2.4 GHz and supports speeds as high as 11 Mbps.
IEEE 802.1g
A wireless standard that uses a frequency of 2.4 GHz and supports speeds as high as 54 Mbps.

IEEE 802.1n
A wireless standard that uses frequencies of 2.4 GHz and 5 GHz and supports speeds as high as 300 Mbps.

IEEE 802.1x
A group of technologies that increases security with a network. It ensures that clients are authenticated before granting access to a network. WPA2 Enterprise mode uses an 802.1x server for authentication.

Institute of Electrical and Electronics Engineers (IEEE)
A professional association that creates standards for networking. It created the IEEE 802.3 standard used for Ethernet and the IEEE 802.11 standard used for wireless.

Integrated Services Digital Network (ISDN)
A group of standards used for transmission of voice, data, and video and can be used as a WAN link. ISDN is commonly bundled as a BRI with two B channels and one D channel or as a PRI with 23 B channels and one D channel.

interception
Eavesdropping, or capturing traffic as it crosses a network. Protocol analyzers or sniffers, such as Microsoft’s Network Monitor, can capture the traffic.

International Telecommunication Union (ITU)
A United Nations agency that focuses on information and communication technology issues on a global scale.

Internet Assigned Numbers Authority (IANA)
An organization that assigns port numbers to protocols including the well-known ports from 0 to 1023. IANA also manages the public IP address assignments.

Internet Control Message Protocol (ICMP)
A protocol used to carry error messages and messages about the availability of services. Troubleshooting tools such as Ping, PathPing, and TraceRt use ICMP. ICMP uses IP directly and doesn’t use either TCP or UDP.

Internet Engineering Task Force (IETF)
An organization that defines Internet communication standards known as RFCs.

Internet Group Management Protocol (IGMP)
A protocol used to multicast data to a group of computers. This is in contrast to unicast, which sends data from one computer to one computer, and broadcast, which sends data from one computer to all other computers in a subnet.

Internet layer
One of the layers on the TCP/IP Model that maps to the Network layer of the OSI Model. Routers operate on this layer.
Internet Message Access Protocol (IMAP)
A mail protocol used to store email messages and download them to clients when requested. Users can view email message headers and choose whether to download the email messages or not. This differs from POP servers which download the messages as soon as the client connects. Clients use SMTP to send email. IMAP4 uses port 143.

Internet Protocol (IP)
IP is a logical addressing scheme used with networking. IPv4 has been around since the 1980s, and IPv6 is the newer version. Both are currently being used on the Internet and in internal networks. Eventually, IPv6 will replace IPv4.

Internet Protocol Security (IPSec)
An encryption protocol that includes an Authentication Header (AH) for authentication and Encapsulating Security Payload (ESP) for encryption. IPSec is used with L2TP/IPSec for VPNs.

intranet
An internal network using the same TCP/IP protocols used on the Internet.

ipconfig
A command-line tool that can display TCP/IP configuration information for a system. It can also change some of the configuration settings.

IPv6 prefix
The first numbers in an IPv6 address that identify the type of IPv6 address. For example, it can be a global unicast address (prefix of 2), a link-local address (prefix of fe80), a unique local address (prefix of fd), or a Teredo address (prefix of 2001:000).

K

Kerberos

L

Layer 2 Tunneling Protocol (L2TP)
A tunneling protocol used for VPNs. L2TP is commonly used with IPSec (as L2TP/IPSec) when used in a VPN. L2TP uses port 1723.

layer 3 switch
An advanced switch that can operate on layer 3 similar to a router. Layer 3 switches function just like a router but perform routing using internal hardware instead of software.

leased line
A WAN link circuited contracted through a communications provider for an organization’s use. The organization pays to lease the line instead of running an independent cable between two offices.
Lightweight Directory Access Protocol (LDAP)
A protocol used to query directories such as Microsoft’s Active Directory Domain Services. LDAP uses port 389. LDAP can be secured with either SSL or TLS. Secure LDAP uses port 636.

link aggregation control protocol (LACP)
LACP is defined by IEEE 802.3ax and is responsible for allowing bundled links on switches to linked devices. Bundled links allows higher throughput between devices.

Link layer
The lowest layer of the TCP/IP Model. It maps to the Data Link and Physical layers of the OSI Model.

link-local addresses
Automatically created IPv6 addresses used on local subnets. These are similar to the APIPA addresses used in IPv4. Link-local addresses start with a prefix of fe80.

Local area network (LAN)
A LAN is a group of computers and/or other devices that are connected in a network.

MAC address
The MAC address is a 48-bit hardware address that is required by every device on a LAN to communicate on that segment. The switch uses the MAC address in the MAC table.

MAC table
The MAC table is a table created within a switch that maps device MAC addresses to switch ports. The MAC table is normally built after the switch is first turned on. Managed switches support static entries in the MAC table created by an administrator. As traffic is sent through a switch, the MAC address is recorded, and the port is noted in the table.

managed switch
A configurable switch. It can be configured to create VLANs, to modify specific settings on individual ports, to send alerts via SNMP, and much more.

multicast
Network traffic from one network device to multiple other network devices on a network.

multimode fiber
Multimode fiber (MMF) uses a plastic core and can transfer data at up to 100 Mbps and as far as 2 km, or up to 10 Gbps for shorter distances. MMF supports a wider variety of light sources than SMF.

neighbor discovery
An IPv6 protocol that uses ICMPv6 to discover details about the network. It can discover routers and other IPv6 parameters used on the local network.
NetBIOS name
A user-friendly name for a computer or other device. NetBIOS names are used on internal networks but never on the Internet. The primary name resolution method for NetBIOS names is WINS.

netstat
A command-line tool that measures network statistics for a computer. It can also show all open ports and identify applications that are using the ports.

Network Address Translation (NAT)
A service that translates public IP addresses to private IP addresses and translates private IP addresses back to public. NAT can run on routers and proxy servers.

Network layer
Layer 3 of the OSI Model. It maps to the Internet layer of the TCP/IP Model. The Network layer of the OSI is responsible for routing and selecting the best path to another network. Routers and layer 3 switches operate on this layer. IPv4, IPv6, ARP, and ICMP operate on this layer.

Network Monitor
Microsoft’s version of a protocol analyzer. It captures frames of data going across a network so that the data can be analyzed. Protocol analyzers are also known as sniffers.

nonpromiscuous mode
A mode of a protocol analyzer that allows it only to capture traffic going to or coming from the system. Promiscuous mode allows it to capture any traffic that reaches its network interface card, no matter what the source or destination IP address is.

octet
An octet is 8 bits. An IPv4 address includes 32 bits that can be represented as four decimals in dotted decimal format. Each decimal can also be represented as an octet of eight bits, with four octets giving a total of 32 bits.

Open Shortest Path First (OSPF)
A routing protocol added to a router. Routing protocols allow routers to exchange routing information between each other. OSPF is used in place of RIPv2 on many hardware routers.

Open Systems Interconnect (OSI) model
The Open Systems Interconnection (OSI) model is a framework for network communication. It includes seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical.

packet
The name of data traveling on the Network layer of the OSI Model. Frames travel on the Data Link layer, and segments travel on the Transport layer.
**pathping**
A command-line tool that combines the features of ping and tracert. It measures packet loss for each router between the source and destination.

**perimeter network**
An area between the Internet and an intranet hosting resources available to any Internet users.

**Physical layer**
Layer 1 of the OSI Model. Hubs and repeaters are examples of devices at this layer. Ethernet and Token Rink are examples of protocols on this layer.

**ping**
A command-line tool that checks connectivity with a remote system. It sends out four packets, and if the target computer is up, it can send back four echo packets back, indicating it's up. Ping uses ICMP, which is often blocked.

**plenum safe**
A rating for cable indicating that is safe to use within a plenum (an open space between walls, below floors, or above ceilings). Nonplenum safe cable can release toxic fumes if it catches fire.

**point-to-point (P2P) wireless**
Technology used to bridge wired networks in two buildings with wireless methods. A P2P bridge is useful when a wired connection is not feasible or affordable.

**Point-to-Point Tunneling Protocol (PPTP)**
A tunneling protocol used with VPNs. PPTP uses Microsoft Point-to-Point Encryption (MPPE) for security. It is largely replaced with L2TP/IPSec or SSL as a tunneling protocol. PPTP uses port 1701.

**port**
Ports can be logical or physical. A port is a logical connection point that is associated with a protocol or an application. Physical ports are the connections to devices such as the port on a switch.

**Post Office Protocol version 3 (POP3)**
An email protocol used to download email to clients as soon as the client connects to the email server. Clients use SMTP to send email. POP3 uses port 110.

**Presentation layer**
Layer 6 of OSI Model. It is responsible for translation between different formats, encryption, decryption, compression, and decompression.

**promiscuous mode**
A mode of a protocol analyzer that allows it to capture any traffic that reaches its network interface card. Nonpromiscuous mode only allows the system to capture traffic going to or coming from the system.

**protocol**
Protocols provide the rules that computers and other devices use to communicate with others on networks.
**protocol data unit (PDU)**
The name of data traveling at layers 5, 6, and 7 of the OSI Model. Data is called a segment on the Transport layer (layer 4), packets are on the Network layer (layer 3), and frames are on the Data Link layer (layer 2).

**proxy server**
A server that acts as on behalf of private clients to retrieve web pages from the Internet. Proxy servers include NAT, can cache requests, filter requests, and check some of the retrieved web page’s content. A reverse proxy isolates web servers from direct access on the Internet by receiving requests from Internet clients and forwarding them to the web server.

**radio frequency interference (RFI)**
RFI is interference caused by radio signals broadcasted over the air.

**remote access**
A technology used to allow remote users to access private networks using either dial-up or VPN remote access servers.

**Remote Desktop Services (RDS)**
A group of Microsoft technologies previously known as Terminal Services. RDS uses the Remote Desktop Protocol and allows users to access desktops of remote computers over the network. RDS uses port 3389.

**requests for comments (RFCs)**
Documents created by the IETF to define Internet communications standards. Published RFCs go through a standards track before actually being considered a standard.

**router**
A network device that connects networks and routes traffic between the networks. A router creates separate broadcast domains.

**Routing and Remote Access Services (RRAS)**
A server role available in Windows Server 2008. When added, you can configure the server as a router or a remote access server.

**Routing Information Protocol**
A routing protocol added to a router. Routing protocols allow routers to exchange routing information between each other. RIPv2 is the current version and has replaced RIPv1 in most applications.

**routing protocols**
Protocols added to routers that allow the router to communicate with other routers on a network. Information exchanged between routers with these protocols update the routers routing tables without administrator intervention.

**routing table**
A logical table maintained in router memory that. The routing table lists all known routes and the paths to these routes. Routing tables consume memory and can be updated either manually (static) or automatically (dynamic).
Secure Shell (SSH)
An encryption protocol that transfers data over a secure channel. SSH is a recommended replacement for Telnet and is also used to encrypt other protocols such as FTP. SSH uses port 22.

Secure Sockets Layer (SSL)
An encryption protocol used to encrypt other protocols such as HTTP and LDAP. SSL uses port 443 with HTTPS. It uses port 636 with Secure LDAP.

Session layer
Layer 5 of the OSI Model. The Session layer establishes, maintains, and terminates the session between two devices.

Simple Mail Transfer Protocol (SMTP)
A primary protocol used to send email on the Internet and internal networks. Clients use SMTP to send email to email servers. Email servers use SMTP to send and receive email between other email servers. SMTP uses port 25.

Simple Network Management Protocol (SNMP)
A management protocol used to query and manage network devices such as routers and switches. SNMP uses ports 161 and 162.

Single mode fiber
Single-mode fiber (SMF) uses a glass core and can transfer data at up to 10 Gbps and as far as 40 km. SMF doesn’t support as many light sources as MMF.

Single sign-on (SSO)
SSO allows a user to sign on once, and then all user access is granted using this single account.

Small office and home office (SOHO)
A network used in a small office of one to ten workers. SOHOs typically have up to 10 workers but may have more.
**static routing**
Routers can have the routing table updated manually or dynamically. Static routing means that an administrator manually updates the routing table.

**straight-through cable**
A twisted-pair Ethernet cable with all the wires going to the same pins on both connections of the cable. Straight-through cables connect computers to networking devices such as switches.

**subnet**
A subnet is a group of computers separated from other computers by one or more routers.

**subnet mask**
The subnet mask is used with the IP address to determine which portion of the IP address is the network ID and which portion is the host ID.

**switch**
A network device that connects computers and keeps track of computers connected to the switch. A switch creates separate collision domains. A traditional switch is a layer 2 device that tracks the location of computers based on their MAC addresses. It uses this information to internally switch traffic to only the destination device instead of all devices connected to the switch. Advanced switches can also operate on layer 3.

**T**

**T1**
A data transmission line used for WAN links in the United States. A T1 includes 24 DS0 channels for a total of 1.544 Mbps. It is connected with Channel Service Unit/Data Service Unit (CSU/DSU) at each end. E1 lines are used in Europe, and they are 2.048 Mbps.

**T3**
A data transmission line used for WAN links similar to a T3. A T3 includes 28 DS1 channels for a total of 44.736 Mbps. E3 lines are used in Europe, and they are 34.368 Mbps.

**TCP/IP**
A suite of protocols used on the Internet and Microsoft networks. It includes TCP, IP, and many other protocols.

**TCP/IP Model**
The TCP/IP Model describes a virtual networking model that was created by the U.S. Department of Defense in the 1970s. It includes four layers known as Application, Transport, Internet, and Link.

**Telnet**
A command-line interface that allows bidirectional communication with network devices.

**Teredo**
A tunneling protocol used to encapsulate IPv6 packets within IPv4 datagrams. It allows IPv6 packets to transit through devices that aren’t IPv6 capable.
**tracert**
A command-line tool that identifies all the routers between a source computer and a destination computer.

**Transmission Control Protocol (TCP)**
A connection-oriented protocol that provides guaranteed delivery. TCP uses a three-way handshake to begin a session, uses sequence numbers to track packets, and includes regular acknowledgments. The alternative is UDP, which is a connectionless protocol that provides best-effort delivery.

**Transport layer**
Layer 4 of the OSI Model and one of the layers of the TCP/IP Model. The Transport layer is responsible for flow control, reliability, and error checking. TCP and UDP protocols operate here.

**Transport Layer Security (TLS)**
An encryption that is the designated replacement for Secure Socket Layer protocol (SSL) protocol and currently coexists with SSL.

**Trivial File Transfer Protocol (TFTP)**
A scaled-down version of File Transfer Protocol (FTP). TFTP uses UDP as the transport protocol and can’t be used on the Internet.

**twisted pair**
A commonly used transmission media type. Current versions include four twisted pair within a single cable.

**U**

**unicast**
Network traffic from one device on a network to one other device on a network.

**unique local address**
IPv6 addresses assigned to hosts in internal networks. This is similar to private IPv4 addresses. Unique local IPv6 addresses start with fd.

**unmanaged switch**
A basic Layer 2 switch. This will work simply by plugging it in and connecting it. It is not configurable.

**uplink port**
An uplink port is used between two devices so that they may share in the communication process on the LAN. Uplink ports may be utilized by either hubs or switches.

**User Datagram Protocol (UDP)**
A connectionless protocol that provides a best-effort delivery. The alternative is TCP, which is a connection-oriented protocol that provides guaranteed delivery.

**V**

**Virtual Private Network (VPN)**
A VPN provides access to a private internal network over a public network such as the Internet. It uses tunneling protocols such as PPTP, L2TP, or SSTP.
**VLAN**

A VLAN is a LAN environment that is created on managed switches. VLANs offer improved security, increased performance, and the ability to add clients to a network segment regardless of their physical location.

**war driving**

The act of driving a car through an area and scanning for wireless networks. Attackers war drive to locate wireless networks and tap into wireless networks with weak security.

**wide area network (WAN)**

A network spanning a large physical area. Typically it is a group of two or more LANs connected from separate geographical locations. The connection between the LANs is almost always slower than the speed within the LANs themselves.

**Wi-Fi Protected Access (WPA)**

WPA was introduced as an interim replacement for WEP until WPA2 could be finalized. WPA offers significantly improved security over WEP without requiring additional hardware. WPA can be used in WPA Personal mode with a preshared key or WPA2 Enterprise mode with an 802.1x server.

**Wi-Fi Protected Access version 2 (WPA2)**

WPA2 provides a permanent fix for the security problems of WEP and is standardized as IEEE 802.11i. WPA2 requires different hardware than that used by WEP and uses the Advanced Encrypted Standard (AES) encryption method. WPA2 can be used in WPA Personal mode with a preshared key or WPA2 Enterprise mode with an 802.1x server.

**Windows Internet Naming Service (WINS)**

A service that runs on a server to resolve NetBIOS names. WINS servers are used on internal Microsoft networks.

**Wired Equivalent Privacy (WEP)**

WEP was the first encryption model offered for wireless network. It is insecure and should be used only in current wireless networks as a last resort.

**Wireless Access Point (WAP)**

A WAP is a device that is located between a wired LAN and a group of wireless clients. It bridges the wireless devices to the wired LAN.

**wireless router**

A WAP with additional components. It provides connectivity for wireless devices using a switch component and includes routing components to route traffic between networks.

**workgroup**

A workgroup is a group of networked computers where user accounts are located on each individual computer.

**World Wide Web Consortium (W3C)**

An organization that defines standards for the World Wide Web (WWW).