Communication network security

**OSI MODEL**

A protocol is a set of rules and restrictions that define how data is transmitted over a network medium (e.g., twisted-pair cable, wireless transmission. International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) Reference Model for protocols in the early 1980’s (Specifically, ISO 7498 defines the OSI Reference Model (more commonly called the OSI model) TCP/IP (which is based on the DARPA model, also known now as the TCP/IP model), was developed in the early 1970s. The OSI model was not developed until the late 1970s.

**Encapsulation/Deencapsulation**

**Protocols based on the OSI model employ a mechanism called encapsulation. *Encapsulation* is the addition of a header, and possibly a footer, to the data received by each layer from the layer above before it’s handed off to the layer below**. As the message is encapsulated at each layer, the previous layer’s header and payload combine to become the payload of the current layer. **Encapsulation occurs as the data moves down through the OSI model layers from Application to Physical. The inverse action occurring as data moves up through the OSI model layers from Physical to Application is known as deencapsulation**. The encapsulation/deencapsulation process is as follows:

1.The Application layer creates a message.

**2.** The Application layer passes the message to the Presentation layer.

**3.** The Presentation layer encapsulates the message by adding information to it. Information is usually added only at the beginning of the message (called a header); however, some layers also add material at the end of the message (called a footer.

4.The process of passing the message down and adding layer-specific information continues until the message reaches the Physical layer.

**5.** At the Physical layer, the message is converted into electrical impulses that represent bits and is transmitted over the physical connection.

**6.** The receiving computer captures the bits from the physical connection and re-creates the message in the Physical layer.

**7.** The Physical layer converts the message from bits into a Data Link frame and sends the message up to the Data Link layer.

**8.** The Data Link layer strips its information and sends the message up to the Network layer.

**9.** This process of deencapsulation is performed until the message reaches the Application layer.

**10.** When the message reaches the Application layer, the data in the message is sent to the intended software recipient.

The information removed by each layer contains instructions, checksums, and so on that can be understood only by the peer layer that originally added or created the information.

**The message sent to the protocol stack at the application layer is called the data stream**. It retains the label of data stream **until it reaches** the **Transport layer (layer 4), where it is called a segment** (TCP protocols) or a datagram (UDP protocols). **In the Network layer (layer 3), it is called a packet**. In the **Data Link layer (layer 2), it is called a frame**. In the **Physical layer (layer 1), the data has been converted into bits** for transmission over the physical connection medium.

**Physical layer**

The Physical layer (layer 1) accepts the frame from the Data Link layer and converts the frame into bits for transmission over the physical connection medium. The Physical layer is also responsible for receiving bits from the physical connection medium and converting them into a frame to be used by the Data Link layer.

**Located within the Physical layer are electrical specifications, protocols, and interface standards.**

**EIA/TIA-232 and EIA/TIA-449■ X.21■ High-Speed Serial Interface (HSSI), Synchronous Optical Network (SONET)■ V.24 and V.35**

**Network hardware devices that function at layer 1, the Physical layer, are network interface cards (NICs), hubs, repeaters, concentrators, and amplifiers. These devices perform hardware-based signal operations, such as sending a signal from one connection port out on all other ports (a hub) or amplifying the signal to support greater transmission distances (a repeater).**

**Data Link Layer**

The Data Link layer (layer 2) is responsible for formatting the packet from the Network layer into the proper format for transmission. The proper format is determined by the hardware and the technology of the network. There are numerous possibilities, such **as Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), asynchronous transfer mode (ATM), Fiber Distributed Data Interface (FDDI), and Copper DDI (CDDI).** However, only Ethernet remains a common Data Link layer technology in use in modern networks. Within the Data Link layer resides the technology-specific protocols that convert the packet into a properly formatted frame. Once the frame is formatted, it is sent to the Physical layer for transmission.

Serial Line Internet Protocol (SLIP)

■ Point-to-Point Protocol (PPP)

■ Address Resolution Protocol (ARP)

■ Reverse Address Resolution Protocol (RARP)

■ Layer 2 Forwarding (L2F)

■ Layer 2 Tunneling Protocol (L2TP)

■ Point-to-Point Tunneling Protocol (PPTP)

■ Integrated Services Digital Network (ISDN)

Part of the processing performed on the data within the Data Link layer includes adding the hardware source and destination addresses to the frame. The hardware address is the Media Access Control (MAC) address, **which is a 6-byte (48-bit) binary address** written in hexadecimal notation (for example, 00-13-02-1F-58-F5). The first 3 bytes (24 bits) of the address denote the vendor or manufacturer of the physical network interface. This is known as the **Organizationally Unique Identifier (OUI). OUIs are registered with IEEE, which controls their issuance**. The OUI can be used to discover the manufacturer of a NIC through the IEEE.

**MAC addresses typically are used to identify network hardware, while EUI is used to identity other types of hardware as well as software.**

ARP is used to resolve IP addresses into MAC addresses. Traffic on a network segment (for example, cables across a hub) is directed from its source system to its destination system using MAC addresses. RARP is used to resolve MAC addresses into IP addresses.

The Data Link layer contains two sublayers: **the Logical Link Control (LLC) sublayer and the MAC sublayer**

Network hardware devices that function at layer 2, the Data Link layer, are **switches and bridges**. These devices support MAC-based traffic routing. Switches receive a frame on one port and send it out another port based on the destination MAC address. MAC address destinations are used to determine whether a frame is transferred over the bridge from one network to another.

**Network Layer**

The Network layer (layer 3) is responsible for adding routing and addressing information to the data. The Network layer accepts the segment from the Transport layer and adds information to it to create a packet. The packet includes the source and destination IP addresses. The routing protocols are located at this layer and include the following:

■ Internet Control Message Protocol (ICMP)

■ Routing Information Protocol (RIP)

■ Open Shortest Path First (OSPF)

■ Border Gateway Protocol (BGP)

■ Internet Group Management Protocol (IGMP)

■ Internet Protocol (IP)

■ Internet Protocol Security (IPSec)

■ Internetwork Packet Exchange (IPX)

■ Network Address Translation (NAT)

■ Simple Key Management for Internet Protocols (SKIP)

The Network layer is responsible for providing routing or delivery information, but it is not responsible for verifying guaranteed delivery (that is the responsibility of the Transport layer). The Network layer also manages error detection and node data traffic (in other words, traffic control).

Non-IP protocols are protocols that serve as an alternative to IP at the OSI Network layer (3). In the past, non-IP protocols were widely used. However, with the dominance and success of TCP/IP, non-IP protocols have become the purview of special-purpose networks. **The three most recognized non-IP protocols are IPX, AppleTalk, and NetBEUI**

Routers and bridge routers (brouters) are among the network hardware devices that function at layer 3. Routers determine the best logical path for the transmission of packets based on speed, hops, preference, and so on.

There are two broad categories of routing protocols: **distance vector and link state**. ***Distance vector* routing protocols maintain a list of destination networks along with metrics of direction and distance as measured in hops (in other words, the number of routers to cross to reach the destination**). ***Link state* routing protocols maintain a topography map of all connected networks and use this map to determine the shortest** path to the destination. Common examples of distance vector routing protocols are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), and Border Gateway Protocol (BGP), while a common example of **a link state routing protocol is Open Shortest Path First (OSPF).**

Transport Layer

The Transport layer establishes a logical connection between two devices and provides end-to-end transport services to ensure data delivery. **This layer includes mechanisms for segmentation, sequencing, error checking, controlling the flow of data, error correction, multiplexing, and network service optimization**. The following protocols operate within the Transport layer:

■ Transmission Control Protocol (TCP)

■ User Datagram Protocol (UDP)

■ Sequenced Packet Exchange (SPX)

■ Secure Sockets Layer (SSL)

■ Transport Layer Security (TLS)

**Session Layer**

The Session layer (layer 5) is responsible for **establishing, maintaining, and terminating communication sessions between two computers.** It manages dialogue discipline or dialogue control (simplex, half-duplex, full-duplex), establishes checkpoints for grouping and recovery, and retransmits PDUs that have failed or been lost since the last verified checkpoint. The following protocols operate within the Session layer:

■ Network File System (NFS)

■ Structured Query Language (SQL)

■ Remote Procedure Call (RPC)

Communication sessions can operate in one of three different discipline or control modes:

**Simplex** One-way direction communication

**Half-Duplex** Two-way communication, but only one direction can send data at a time

**Full-Duplex** Two-way communication, in which data can be sent in both directions

Simultaneously

**Presentation Layer**

The Presentation layer (layer 6) is responsible for transforming data received from the Application layer into a format that any system following the OSI model can understand. It imposes common or standardized structure and formatting rules onto the data. **The Presentation layer is also responsible for encryption and compression. Thus, it acts as an interface between the network and applications**. This layer is what allows various applications to interact over a network, and it does so by ensuring that the data formats are supported by both systems. Most file or data formats operate within this layer. This includes formats for images, video, sound, documents, email, web pages, control sessions,

American Standard Code for Information Interchange (ASCII)

■ Extended Binary-Coded Decimal Interchange Mode (EBCDICM)

■ Tagged Image File Format (TIFF)

■ Joint Photographic Experts Group (JPEG)

■ Moving Picture Experts Group (MPEG)

■ Musical Instrument Digital Interface (MIDI)

**Application Layer**

The Application layer (layer 7) is responsible for interfacing user applications, network services, or the operating system with the protocol stack. It allows applications to communicate with the protocol stack.

Hypertext Transfer Protocol (HTTP) ■ File Transfer Protocol (FTP) ■ Line Print Daemon (LPD)

■ Simple Mail Transfer Protocol (SMTP) ■ Telnet ■ Trivial File Transfer Protocol (TFTP)

■ Electronic Data Interchange (EDI) Post Office Protocol version 3 (POP3) ■ Internet Message Access Protocol (IMAP)

■ Simple Network Management Protocol (SNMP) ■ Network News Transport Protocol (NNTP) ■ Secure Remote Procedure Call (S-RPC) ■ Secure Electronic Transaction (SET).

There is a network device (or service) that works at the Application layer, namely, the gateway. However, an Application layer gateway is a specific type of component. Application layer firewalls also operate at this layer. Other networking devices or filtering software may observe or modify traffic at this layer.

TCP/IP Model

The TCP/IP model (**also called the DARPA or the DOD model**) consists of only four layers,

The TCP/IP model’s Application layer corresponds to layers 5, 6, and 7 of the OSI model. The TCP/IP model’s Transport layer corresponds to layer 4 from the OSI model. The TCP/IP model’s Internet layer corresponds to layer 3 from the OSI model. The TCP/IP model’s Link layer corresponds to layers 1 and 2 from the OSI model.

TCP/IP is a platform-independent protocol based on open standards. However, this is both a benefit and a drawback. TCP/IP can be found in just about every available operating system, but it consumes a significant amount of resources and is relatively easy to hack into because it was designed for ease of use rather than for security

**TCP/IP can be secured using VPN links between systems. VPN links are encrypted to add privacy, confidentiality, and authentication and to maintain data integrity. Protocols used to establish VPNs are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPSec). Another method to provide protocol-level security is to employ TCP wrappers. A *TCP wrapper* is an application that can serve as a basic firewall by restricting access to ports and resources based on user IDs or system IDs. Using TCP wrappers is a form of port-based access control.**

**Transport Layer Protocols**

The two primary Transport layer protocols of TCP/IP are TCP and UDP. **TCP is a fullduplex connection-oriented protocol, whereas UDP is a simplex connectionless protocol.** When a communication connection is established between two systems, it is done using ports**. TCP and UDP each have 65,536 ports**. Since port numbers are 16-digit binary numbers, the total number of ports is 216, or 65,536, numbered from 0 through 65,535. **A port (also called a socket)**

Berkeley Software Distribution (BSD) uses ports 1024 through 4999.

■ Many Linux kernels use 32768 to 61000.

■ Microsoft, up to and including Windows Server 2003, uses the range 1025 to 5000.

■ Windows Vista, Windows 7, and Windows Server 2008 use the IANA range.

■ FreeBSD, since version 4.6, has used the IANA suggested port range.

**The three-way handshake process follows:**

**1. The client sends a SYN (synchronize) flagged packet to the server.**

**2. The server responds with a SYN/ACK (synchronize and acknowledge) flagged packet back to the client.**

**3. The client responds with an ACK (acknowledge) flagged packet back to the server.**

When a communication session is complete, there are two methods to disconnect the TCP session. First, and most common, is the use of FIN (finish) flagged packets instead of SYN flagged packets. Each side of a conversation will transmit a **FIN flagged packet** once all its data is transmitted, triggering the opposing side to confirm with an ACK flagged packet. Thus, it takes four packets to gracefully tear down a TCP session. Second is the use of an **RST (reset) flagged** packet, **which causes an immediate and abrupt session termination.**

The segments of a TCP transmission are tagged with a sequence number. This allows the receiver to rebuild the original communication by reordering received segments back into their proper arrangement despite the order in which they were received. The TCP header is relatively complex when compared to its sister protocol UDP. A **TCP header is 20 to 60 bytes long**. This header is divided into several sections.

**Data flow is controlled through a mechanism called sliding windows**. TCP can use different sizes of windows (in other words, a different number of transmitted packets) before sending an acknowledgment. Larger windows allow for faster data transmission. **TCP value in the header is 6, ICMP -1 ; 51 for AH ; 88 for EIGRP; 89 for OSPF**

**User Datagram Protocol (UDP) also operates at layer 4** (the Transport layer) of the OSI model. It is a connectionless “**best-effort” communications protocol**. It **offers no error detection or correction, does not use sequencing, does not use flow control mechanisms, does not use a preestablished session, and is considered unreliable. UDP has very low overhead and thus can transmit data quickly**. However, UDP should be used only when the delivery of data is not essential. UDP is often employed by real-time or streaming communications for audio and/or video. **The IP header protocol field value for UDP is 17**

**A UDP header is 8 bytes and This header is divided into four sections**, or fields (**each 16 bits long):**

■ Source port

■ Destination port

■ Message length

■ Checksum

Another important protocol in the TCP/IP protocol suite operates at the Network layer of the OSI model, namely**, Internet Protocol (IP).** IP provides route addressing for data packets. **It is this route addressing that is the foundation of global Internet communications because it provides a means of identity and prescribes transmission paths**. **Like UDP, IP is connectionless and is an unreliable datagram service.** IP does not offer guarantees that packets will be delivered or that packets will be delivered in the correct order, and it does not guarantee that packets will be delivered only once. Thus, you must employ TCP on IP to gain reliable and controlled communication sessions.

**IPv4 uses a 32-bit addressing scheme, while IPv6 uses 128 bits for addressing**

**Class First Binary Digits Decimal Range of First Octet Default Subnet Mask CIDR Equivalent**

A 0 1–126 255.0.0.0 /8

B 10 128–191 255.255.0.0 /16

C 110 192–223 255.255.255.0 /24

D 1110 224–239

E 1111 240–255

**Another option for subnetting is to use Classless Inter-Domain Routing (CIDR) notation. CIDR uses mask bits rather than a full dotted-decimal notation subnet mask. Thus, instead of 255.255.0.0, a CIDR is added to the IP address after a slash, as in 172.16.1.1/16, One significant benefit of CIDR over traditional subnet-masking techniques is the ability to combine multiple noncontiguous sets of addresses into a single subnet. For example, it is possible to combine several Class C subnets into a single larger subnet grouping.**

**Private IP range 10.0.0.0 or 172.16.0.0 or 192.168.0.0**

**ICMP** Internet Control Message Protocol (ICMP) is used to determine the health of a network or a specific link. ICMP is **utilized by ping, traceroute, pathing, and** other network management tools. The ping utility employs ICMP echo packets and bounces them off remote systems. Thus, you can use ping to determine whether the remote system is online, whether the remote system is responding promptly, whether the intermediary systems are supporting communications, and the level of performance efficiency at which the intermediary systems are communicating. The ping utility includes a redirect function that allows the echo responses to be sent to a different destination than the system of origin.

the features of ICMP were often exploited in various forms of bandwidth-based denial of service attacks, such as ping of death, smurf attacks, and ping floods. This fact has shaped how networks handle ICMP traffic today, resulting in many networks limiting the use of ICMP or at least limiting its throughput rates**. Ping of death sends a malformed ping larger than 65,535 bytes. Smurf attacks generate enormous amounts of traffic on a target network by spoofing broadcast pings, and ping floods are a basic denial of service (DoS) attack relying on consuming all the bandwidth that a target has available**.

ICMP

Type Function

0 Echo reply

3 Destination unreachable

5 Redirect

8 Echo request

9 Router advertisements

10 Router solicitation

11 Time exceeded

**IGMP** Internet Group **Management Protocol (IGMP) allows systems** to **support multicasting**. **Multicasting is the transmission of data to multiple specific recipients**. (RFC1112 discusses the requirements to perform IGMP multicasting.) IGMP is used by IP hosts to register their dynamic multicast group membership. It is also used by connected routers to discover these groups. Using IGMP multicasting, a server can initially transmit a single data signal for the entire group rather than a separate initial data signal for each intended recipient. With IGMP, the single initial signal is multiplied at the router if divergent pathways exist to the intended recipients. The IP header **protocol field value for IGMP is 2** (0x02).

**ARP and Reverse ARP** Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) are essential to the interoperability of logical and physical addressing schemes. **ARP is used to resolve IP addresses (32-bit binary number for logical addressing) into** **Media Access Control (MAC) addresses** (48-bit binary number for physical addressing)—or EUI-48 or even EUI-64. Traffic on a network segment (for example, cables across a hub) is directed from its source system to its destination system using MAC addresses. **RARP is used to resolve MAC addresses into IP addresses**.

**Both ARP and RARP function using caching and broadcasting**. The first step in resolving an IP address into a MAC address, or vice versa, is to check the local ARP cache**. If the needed information is already present in the ARP cache, it is used. This activity is sometimes abused using a technique called ARP cache poisoning**, g where an attacker inserts bogus information into the ARP cache. If the ARP cache does not contain the necessary information, an ARP request in the form of a broadcast is transmitted. If the owner of the queried address is in the local subnet, it can respond with the necessary information. If not, the system will default to using its default gateway to transmit its communications. Then, the default gateway (in other words, a router) will need to perform its own ARP or RARP process.

**Telnet, TCP Port 23** This is a terminal emulation network application that supports remote connectivity for executing commands and running applications but does not support transfer of files.

**File Transfer Protocol (FTP), TCP Ports 20 and 21** This is a network application that supports an exchange of files that requires **anonymous or specific authentication.**

**Trivial File Transfer Protocol (TFTP), UDP Port 69** This is a network application that supports an exchange of files that **does not require authentication.**

**Simple Mail Transfer Protocol (SMTP), TCP Port 25** This is a protocol used to transmit email messages from a client to an email server and from one email server to another.

**Post Office Protocol (POP3), TCP Port 110** This is a protocol used to pull email messages from an inbox on an email server down to an email client.

**Internet Message Access Protocol (IMAP), TCP Port 143** This is a protocol used to pull email messages from an inbox on an email server down to an email client**. IMAP is more secure than POP3** and offers the ability to pull headers down from the email server as well as to delete messages directly off the email server without having to download to the local client first.

**Dynamic Host Configuration Protocol (DHCP), UDP Ports 67 and 68** DHCP uses **port 67 for server point-to-point response and port 68 for client request broadcasts**. It is used to assign TCP/IP configuration settings to systems upon bootup. DHCP enables centralized control of network addressing.

**Hypertext Transport Protocol (HTTP), TCP Port 80** This is the protocol used to transmit web page elements from a web server to web browsers.

**Secure Sockets Layer (SSL), TCP Port 443 (for HTTP Encryption)** This is a VPN-like security protocol that operates at the Transport layer. SSL was originally designed to support secured web communications (HTTPS) but is capable of securing any Application layer protocol communications.

**Line Print Daemon (LPD), TCP Port 515** This is a network service that is used to spool print jobs and to send print jobs to printers.

**X Window, TCP Ports 6000–6063** This is a GUI API for command-line operating systems.

**Bootstrap Protocol (BootP)/Dynamic Host Configuration Protocol (DHCP), UDP Ports 67 and 68** This is a protocol used to connect diskless workstations to a network through auto assignment of IP configuration and download of basic OS elements. BootP is the forerunner to Dynamic Host Configuration Protocol (DHCP).

**Network File System (NFS), TCP Port 2049** This is a network service used to support file sharing between dissimilar systems.

**Simple Network Management Protocol (SNMP), UDP Port 161 (UDP Port 162 for Trap Messages**) This is a network service used to collect network health and status information by polling monitoring devices from a central monitoring station.

**TCP/IP is therefore a multilayer protocol.** when communicating between a web server and a web browser over a typical network connection, HTTP is encapsulated in TCP, which in turn is encapsulated in IP, which is in turn encapsulated in Ethernet.

Another area of concern caused by unbounded encapsulation support is the ability to jump between VLANs. VLANs are networks segments that are logically separated by tags. This attack, known as VLAN hopping, is performed by creating a double-encapsulated IEEE 802.1Q VLAN tag:

[ Ethernet [ VLAN1 [ VLAN2 [ IP [ TCP [ HTTP]] ] ] ] ]

DNP3 is primarily used in the electric and water utility and management industries. It is used to support communications between data acquisition systems and the system control equipment. DNP3 is a multilayer protocol that functions similarly to that of TCP/IP, in that it has link, transport, and transportation layers.

TCP/IP’s vulnerabilities are numerous. Improperly implemented TCP/IP stacks in various operating systems are vulnerable to **buffer overflows, SYN flood attacks, various DoS attacks, fragment attacks, oversized packet attacks, spoofing attacks, man-in-the-middle attacks, hijack attacks, and coding error attacks.**

DNS

The third, or bottom, layer is the MAC address. The MAC address, or hardware address, is a “permanent” physical address.

■ The second, or middle, layer is the IP address. The IP address is a “temporary” logical address assigned over or onto the MAC address.

■ The top layer is the domain name. The domain name or computer name is a “temporary” human-friendly convention assigned over or onto the IP address

Converged Protocols

Converged protocols are the merging of specialty or proprietary protocols with standard protocols, such as those from the TCP/IP suite. The primary benefit of converged protocols is the ability to use existing TCP/IP supporting network infrastructure to host special or proprietary services without the need for unique deployments of alternate networking hardware. This can result in significant cost savings. However, not all converged protocols provide the same level of throughput or reliability as their proprietary implementations

**Fibre Channel over Ethernet (FCoE)** Fibre Channel is a form of **network data-storage solution** (storage area network [SAN]) or network-attached storage [NAS]) that allows for high-speed fi le transfers at upward of 16 Gbps. It was designed to be operated over fiber-optic cables; support for copper cables was added later to offer less-expensive options. Fibre Channel typically requires its own dedicated infrastructure (separate cables). However, Fibre Channel over Ethernet (FCoE) can be used to support it over the existing network infrastructure. **FCoE is used to encapsulate Fibre Channel communications over Ethernet networks**. It **typically requires 10 Gbps Ethernet** in order to support the Fibre Channel protocol. With this technology, **Fibre Channel operates as a Network layer or OSI layer 3 protocol, replacing IP as the payload of a standard Ethernet network.**

**MPLS (Multiprotocol Label Switching)** MPLS (Multiprotocol Label Switching) is a high-throughput high-performance network technology that directs data across a network based on short path labels rather than longer network addresses. This technique saves significant time over traditional IP-based routing processes, which can be quite complex. Furthermore, MPLS is designed to handle a wide range of protocols through encapsulation. Thus, the network is not limited to TCP/IP and compatible protocols. This enables the use of many other networking technologies, including T1/E1, ATM, Frame Relay, SONET, and DSL.

**Internet Small Computer System Interface (iSCSI)** Internet Small Computer System Interface (iSCSI) is a networking storage standard based on IP. This technology can be used to enable location-independent fi le storage, transmission, and retrieval over LAN, WAN, or public Internet connections. **iSCSI is often viewed as** a **low-cost alternative to Fibre Channel**.

**Voice over IP (VoIP)** Voice over IP (VoIP) is a tunneling mechanism used to transport voice and/or data over a TCP/IP network. VoIP has the potential to replace or supplant PSTN because it’s often less expensive and offers a wider variety of options and features. VoIP can be used as a direct telephone replacement on computer networks as well as mobile devices. VoIP-to-VoIP calls are free.

**Software-Defined Networking (SDN)** Software-Defined Networking (SDN) is a unique approach to network operation, design, and management. The concept is **based on the theory that the complexities of a traditional** network with on-device configuration (i.e., routers and switches) often force an organization to stick with a single device vendor, such as Cisco, and limit the flexibility of the network to respond to changing physical and business conditions. SDN aims at separating the infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management). Furthermore, this also removes the traditional networking concepts of IP addressing**, subnets, routing, and so on from needing to be programmed into or be deciphered by hosted applications. SDN offers a new network design that is directly programmable from a central location, is flexible, is vendor neutral, and is open-standards based.**

**Another way of thinking about SDN is that it is effectively network virtualization.**

**Content Distribution Networks**

**A content distribution network (CDN), or content delivery network, is a collection of resource services deployed in numerous data centers across the Internet in order to provide low latency, high performance, and high availability of the hosted content**. CDNs provide the desired multimedia performance quality demanded by customers through the concept of distributed data hosts. Rather than having media content stored in a single location to be transmitted to all parts of the Internet, **the media is distributed to numerous** locations across the Internet. This results in a type of geographic and logical load-balancing. No one server or cluster of servers will be strained under the load of all resource requests, and the hosting servers are located closer to the requesting customers. **The overall result is lower latency and higher-quality throughput**. There are many CDN service providers, including CloudFlare**, Akamai, Amazon** CloudFront, CacheFly, and Level 3 Communications.

**While most CDNs focus on the physical distribution of servers, client-based CDN is also possible. This is often referred to by the term P2P (peer-to-peer). The most widely recognized P2P CDN is BitTorrent.**

Wireless Networks

**Wireless networking is a popular method of connecting corporate and home systems because of the ease of deployment and relatively low cost.**

***Data emanation***is the transmission of data across electromagnetic signals. Almost all activities within a computer or across a network are performed using some form of data emanation. However, this term is often used to focus on emanations that are unwanted or on data that is at risk due to the emanations.

**Emanations occur whenever electrons move**. Movement of electrons creates a magnetic field. If you can read that magnetic field, you could re-create it elsewhere to reproduce the electron stream. If the original electron stream was used to communicate data, then the re-created electron stream is also a re-creation of the original data. This form of electronic eavesdropping sounds like science fiction, but it is scientific fact. The **U.S. government has been researching emanation security since the 1950s under the TEMPEST project**. Protecting against eavesdropping and data theft requires a multipronged effort. First, you must maintain **physical access control over all electronic equipment**. Second, where physical access or proximity is still possible for unauthorized personnel, you must **use shielded devices and media. Third, you should always transmit any sensitive data using secure encryption protocols.**

**Securing Wireless Access Points**

*Wireless cells* are the areas within a physical environment where a wireless device can connect to a wireless access point. Wireless cells can leak outside the secured environment and allow intruders easy access to the wireless network. You should adjust the strength of the wireless access point to maximize authorized user access and minimize intruder access. Doing so may require unique placement of wireless access points, shielding, and noise transmission.

***802.11* is the IEEE standard** **for wireless network communications**. 802.11a, 802.11b, 802.11g, and 802.11n.

The 802.11 standard also defines **Wired Equivalent Privacy (WEP), which provides eavesdropping protection for wireless communications.** The b, g, and n amendments all use the same frequency; thus, they maintain backward compatibility

**Amendment Speed Frequency**

802.11 2 Mbps 2.4 GHz

802.11a 54 Mbps 5 GHz

802.11b 11 Mbps 2.4 GHz

802.11g 54 Mbps 2.4 GHz

802.11n 200+ Mbps 2.4 GHz or 5 GHz

802.11ac 1 Gbps 5 GHz

When you’re deploying wireless networks, you should deploy wireless access points configured to use ***infrastructure mode* rather than *ad hoc mode.* Ad hoc mode means that any two wireless networking devices, including two wireless network interface cards (NICs), can communicate without a centralized control authority. Infrastructure mode means that a wireless access point is required, wireless NICs on systems can’t interact directly, and the restrictions of the wireless access point for wireless network access are enforced**

Within the infrastructure mode concept are several variations, **including stand-alone, wired extension**, **enterprise extended, and bridge**. **A *stand-alone* mode infrastructure occurs when there is a wireless access point connecting wireless clients to each other but not to any wired resources**. The wireless access point serves as a wireless hub exclusively. **A *wired extension* mode infrastructure occurs when the wireless access point acts as a connection point to link the wireless clients to the wired network**. **An *enterprise extended* mode infrastructure occurs when multiple wireless access points (WAPs) are used to connect a large physical area to the same wired network**. Each wireless access point will use the same extended service set identifier (ESSID) so clients can roam the area while maintaining network connectivity, even while their wireless NICs change associations from one wireless access point to another**. A *bridge* mode infrastructure occurs when a wireless connection is used to link two wired networks.**

Technically there are two types of SSIDs, namely extended service set identifier (**ESSID)** and basic service set identifier **(BSSID).**

**An ESSID is the name of a wireless network when a wireless base station or WAP is used (i.e., infrastructure mode.**

**A BSSID is the name of a wireless network when in ad hoc or peer-to-peer mode (**(i.e., when a base station or WAP is not used).

**However, when operating in infrastructure mode, the BSSID is the MAC address of the base station hosting the ESSID to differentiate multiple base stations supporting a single extended wireless network.**

Within the assigned frequency of the wireless signal are subdivisions of that frequency known as *channels*

**Securing the SSID**

If a wireless client knows the SSID, they can configure their wireless NIC to communicate with the associated WAP. SSIDs are defined by default by vendors, and since these default SSIDs are well known, standard security practice dictates that the SSID should be changed to something unique before deployment.

**The SSID is broadcast by the WAP via a special transmission called a *beacon frame.***

**Thus, disabling SSID broadcasting is not a true mechanism of security. Instead, use WPA2 as a reliable authentication and encryption solution rather than trying to hide the existence of the wireless network.**

**A *site survey***is the process of investigating the presence, strength, and reach of wireless access points deployed in an environment. This task usually involves walking around with a portable wireless device, taking note of the wireless signal strength, and mapping this on a plot or schematic of the building.

**Using Secure Encryption Protocols**

**The IEEE 802.11 standard defines two methods** that wireless clients can use to authenticate to WAPs before normal network communications can occur across the wireless link. These two methods are **open system authentication (OSA) and shared key authentication (SKA**). **OSA means there is no real authentication** required. If a radio signal can be transmitted between the client and WAP, communications are allowed. It is also the case that wireless networks using OSA typically transmit everything in clear text, thus providing no secrecy or security. **SKA means that some form of authentication must take place before network communications can occur. The 802.11 standard defines one optional technique for SKA known as Wired Equivalent Privacy (WEP).** **Later amendments to the original 802.11 standard added WPA, WPA2, and other technologies.**

**WEP**

***Wired Equivalent Privacy* is defined by the IEEE 802.11 standard**. It was **designed to provide the same level of security and encryption on wireless networks** as is found on wired or cabled networks. **WEP provides protection from packet sniffing and eavesdropping against wireless transmissions**. A secondary benefit of WEP is that it can be configured to **prevent unauthorized access to the wireless network**. **WEP uses a predefined shared secret key; however, rather than being a typical dynamic symmetric cryptography solution,** the shared key is static and shared among all wireless access points and device interfaces

there are alternatives to WEP, namely WPA and WPA2. WPA is an improvement over WEP in that **it does not use the same static key to encrypt all communications.** Instead, **it negotiates a unique key** set with each host. However, a single passphrase is used to authorized the association with the base station (i.e., allow a new client to set up a connection). If the passphrase is not long enough, it could be guessed. **Usually 14 characters or more for the passphrase is recommended. WEP encryption employs Rivest Cipher 4 (RC4), a symmetric stream cipher.**

**WPA**

WPA (Wi-Fi Protected Access) was designed as the replacement for WEP; it was a temporary fix until the new 802.11i amendment was completed. The process of crafting the new amendment took years, and thus WPA established a foothold in the marketplace and is still widely used today. Additionally, WPA can be used on most devices, whereas the features of 802.11i exclude some lower-end hardware.

802.11i is the amendment that defines a cryptographic solution to replace WEP. However, when 802.11i was finalized, the WPA solution was already widely used, so they could not use the WPA name as originally planned; thus it was branded WPA2. But this does not indicate that 802.11i is the second version of WPA. In fact, **they are two completely different sets of technologies. 802.11i, or WPA2,** implements concepts like **IPSec to bring the best-to-date encryption and security to wireless communications. Wi-Fi Protected Access is based on the LEAP and TKIP cryptosystems and often employs a secret passphrase for a**uthentication.

**WPA no longer provides long-term reliable security.**

**WPA2**

Eventually, a new method of securing wireless was developed that is still considered secure. This is the amendment known as 802.11i or WPA2. It is a new encryption scheme known as the **Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP**), which is based on the AES encryption scheme. To date, **no real-world attack has compromised** the encryption of a properly configured WPA2 wireless network.

**802.1X/EAP**

Both WPA and WPA2 support the enterprise authentication known as 802.1X/EAP, a standard port-based network access control that ensures clients cannot communicate with a resource until proper authentication has taken place. Effectively, 802.1X is a hand-off system that allows the wireless network to leverage the existing network infrastructure’s authentication services. **Using 802.1X, other techniques and solutions such as RADIUS, TACACS, certificates, smart cards, token devices, and biometrics can be integrated into wireless networks providing techniques for both mutual and multi-factor authentication**.

**EAP (Extensible Authentication Protocol) is not a specific mechanism of authentication; rather it is an authentication framework.** Effectively, EAP allows for new authentication technologies to be compatible with existing wireless or point-to-point connection technologies. **More than 40 different EAP methods of authentication are widely supported. These include the wireless methods of LEAP, EAP-TLS, EAP-SIM, EAP-AKA, and EAP-TTLS.** **Not all EAP methods are secure. For example, EAP-MD5 and a pre-release EAP known as LEAP are also crackable**

**PEAP**

**PEAP (Protected Extensible Authentication Protocol) encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption**. **Since EAP was originally designed for use over physically isolated channels and hence assumed secured pathways ,EAP is usually not encrypted**. So, **PEAP can provide encryption for EAP methods.**

**LEAP**

**LEAP (Lightweight Extensible Authentication Protocol) is a Cisco proprietary alternative to TKIP for WPA**. This was developed to address deficiencies in TKIP before the 802.11i/ WPA2 system was ratified as a standard. An attack tool known as Asleap was released in 2004 that could exploit the ultimately weak protection provided by LEAP. LEAP should be avoided when possible; use **of EAP-TLS as an alternative is recommended, but if LEAP is used, a complex password is strongly recommended.**

**MAC Filter**

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a wireless access point **to block access to all non-authorized devices**. While a useful feature to implement, it can be difficult to manage, and tends to be used only in small, static environments. Additionally, a hacker with basic wireless hacking tools can discover the MAC address of a valid client and then spoof that address onto their attack wireless client.

**TKIP**

**TKIP (Temporal Key Integrity Protocol) was designed as the replacement for WEP without requiring replacement of legacy wireless hardware. TKIP was implemented into 802.11 wireless networking under the name WPA (Wi-Fi Protected Access). TKIP improvements include a key-mixing function that combines the initialization vector (IV) (i.e., a random number) with the secret root key before using that key with RC4 to perform encryption;** a sequence counter is used to prevent packet replay attacks; and a strong integrity check named Michael is used. TKIP and WPA were officially replaced by WPA2 in 2004. Additionally, attacks specific to WPA and TKIP (i.e., coWPAtty and a GPU-based cracking tool) have rendered WPA’s security unreliable.

**CCMP**

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) was created to replace WEP and TKIP/WPA. CCMP uses AES (Advanced Encryption Standard) with a 128-bit key. CCMP is the preferred standard security protocol of 802.11 wireless networking indicated by 802.11i. To date, no attacks have yet been successful against the AES/CCMP encryption.

**Antenna types**

**The standard straight or pole antenna** is an omnidirectional antenna that can send and receive signals in all directions perpendicular to the line of the antenna itself. This is the type of antenna found on most base stations and some client devices. **This type of antenna is sometimes also called a base antenna or a rubber duck antenna (since most are covered in a flexible rubber coating).**

**Most other types of antennas are directional, meaning they focus their sending and receiving capabilities in one primary direction**. Some examples of directional antennas include Yagi, cantenna, panel, and parabolic. A Yagi antenna is similar in structure to that of traditional roof TV antennas. Yagi antennas are crafted from a straight bar with cross sections to catch specific radio frequencies in the direction of the main bar. Cantennas are constructed from tubes with one sealed end. They focus along the direction of the open end of the tube. **Some of the first cantennas were crafted from Pringles cans**. Panel antennas are flat devices that focus from only one side of the panel. Parabolic antennas are used to focus signals from very long distances or weak sources

**Using Captive Portals**

**A captive portal is an authentication technique that redirects a newly connected wireless Web client to a portal access control page**. The portal page may require the user to input payment information, provide logon credentials, or input an access code. A captive portal is also used to display an accessible use policy, privacy policy, and tracking policy to the user, who must consent to the policies before being able to communicate across the network. **Captive portals are most often located on wireless networks implemented for public use, such as at hotels, restaurants, bars, airports, libraries, and so on. However, they can be used on cabled Ethernet connections as well**.

**there is a collection of techniques, commonly called *wardriving****,* **to discover that a wireless network is present**. This activity involves using a wireless interface or a wireless detector to locate wireless network signals. Once an attacker knows a wireless network is present, they can use sniffers to gather wireless packets for investigation. With the right tools, an attacker can discover hidden SSIDs, active IP addresses, valid MAC addresses, and even the authentication mechanism in use by the wireless clients. From there, attackers can grab dedicated cracking tools to attempt to break into the connection or attempt to conduct man-in-the-middle attacks. The older and weaker your protections, the faster and more successful such attacks are likely to be.

**Network Access Control**

Network Access Control (NAC) is a concept of controlling access to an environment through strict adherence to and implementation of security policy. The goals of NAC are as follows:

■ Prevent/reduce zero-day attacks

■ Enforce security policy throughout the network

■ Use identities to perform access control

**Originally, 802.1X (which provides port-based NAC) was thought to embody NAC**, but most supporters believe that 802.1X is only a simple form of NAC or just one component in a complete NAC solution. NAC can be implemented with a preadmission philosophy or a postadmission philosophy, or aspects of both: The **preadmission philosophy requires a system to meet all current security requirements** (such as patch application and antivirus updates) before it can communicate with the network. **The postadmission philosophy allows and denies access based on user activity, which is based on a predefined authorization** **matrix.**

**Firewall**

**There are four basic types of firewalls: static packet-filtering firewalls, application-level gateway firewalls, circuit-level gateway firewalls, and stateful inspection firewalls.**

**Static Packet-Filtering Firewalls A *static packet-filtering firewall l* filters traffic by examining data from a message header. Usually, the rules are concerned with source, destination, and port addresses. Using static filtering, a firewall is unable to provide user authentication or to tell whether a packet originated from inside or outside the private network, and it is easily fooled with spoofed packets. Static packet-filtering firewalls are known as first generation firewalls; they operate at layer 3 (the Network layer) of the OSI model. They can also be called *screening routers* or *common routers* .**

**Application-Level Gateway Firewalls An application-level gateway firewall is also called a proxy firewall. A *proxy* is a mechanism that copies packets from one network into another; the copy process also changes the source and destination addresses to protect the identity of the internal or private network. An application-level gateway firewall filters traffic based on the Internet service (in other words, the application) used to transmit or receive the data. Each type of application must have its own unique proxy server. Thus, an application-level gateway firewall comprises numerous individual proxy servers. This type of firewall negatively affects network performance because each packet must be examined and processed as it passes through the firewall. Application-level gateways are known as second-generation firewalls, and they operate at the Application layer (layer 7) of the OSI model**.

**Circuit-Level Gateway Firewalls *Circuit-level gateway firewalls* are used to establish communication sessions between trusted partners. They operate at the Session layer (layer 5) of the OSI model. SOCKS (from *Socket Secure* , as in TCP/IP ports) is a common implementation of a circuit-level gateway firewall. Circuit-level gateway firewalls, also known as *circuit proxies* , manage communications based on the circuit, not the content of traffic. They permit or deny forwarding decisions based solely on the endpoint designations of the communication circuit (in other words, the source and destination address and service port numbers).**

**Stateful Inspection Firewalls *Stateful inspection firewalls* (also known as *dynamic packet filtering firewalls* ) evaluate the state or the context of network traffic. By examining source and destination addresses, application usage, source of origin, and relationship between current packets and the previous packets of the same session, stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users and activities. Stateful inspection firewalls generally operate more efficiently than application-level gateway firewalls. They are known as third-generation firewalls, and they operate at the Network and Transport layers (layers 3 and 4) of the OSI model.**

**Multihomed Firewalls**

Some firewall systems have more than one interface. For instance, a multihomed firewall must have at least two interfaces to filter traffic (they’re also known as dual-homed firewalls). All multihomed firewalls should have IP forwarding, which automatically sends traffic to another interface, disabled. This will force the filtering rules to control all traffic rather than allowing a software-supported shortcut between one interface and another. A bastion host or a screened host is just a firewall system logically positioned between a private network and an untrusted network. Usually, the bastion host is located behind the router that connects the private network to the untrusted network. All inbound traffic is routed to the bastion host, which in turn acts as a proxy for all the trusted systems within the private network. It is responsible for filtering traffic coming into the private network as well as for protecting the identity of the internal client.

**Firewall Deployment Architectures**

There are three commonly recognized firewall deployment architectures: **single tier, two tier, and three tier (also known as multitier).**

**A collision occurs when two systems transmit data at the same time onto a connection medium that supports only a single transmission path**. A broadcast occurs when a single system transmits data to all possible recipients. Generally, collisions are something to avoid and prevent, while broadcasts have useful purposes from time to time. The management of collisions and broadcasts introduces a new term known as *domains****.* A collision domain is a group of networked systems that could cause a collision** if any two (or more) of the systems in that group transmitted simultaneously. Any system outside the collision domain cannot cause a collision with any member of that collision domain.

A *broadcast domain* is a group of networked systems in which all other members receive a broadcast signal when one of the members of the group transmits it. Any system outside a broadcast domain would not receive a broadcast from that broadcast domain.

Collision domains are divided by using any layer 2 or higher device, and broadcast domains are divided by using any layer 3 or higher device. When a domain is divided, it means that systems on opposite sides of the deployed device are members of different domains.

**Repeaters, Concentrators, and Amplifiers** Repeaters, concentrators, and amplifiers are used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol. These devices can be used to extend the maximum length of a specific cable type by deploying one or more repeaters along a lengthy cable run. Repeaters, concentrators, and amplifiers operate at OSI layer 1. Systems on either side of a repeater, concentrator, or amplifier are part of the same collision domain and broadcast domain.

**Hubs** are used to connect multiple systems and connect network segments that use the same protocol. They repeat inbound traffic cover all outbound ports. This ensures that the traffic will reach its intended host. A hub is a multiport repeater. Hubs operate at OSI layer 1. Systems on either side of a hub are part of the same collision and broadcast domains. Most organizations have a no-hub security policy to limit or reduce the risk of sniffing attacks since they are an outmoded technology and switches are preferred.

**Modems** A traditional land-line modem (modulator-demodulator) is a communications device that covers or modulates between an analog carrier signal and digital information to support computer communications of public switched telephone network (PSTN) lines. From about 1960 until the mid-1990s, modems were a common means of WAN communications. Modems have generally been replaced by digital broadband technologies including ISDN, cable modems, DSL modems, 802.11 wireless, and various forms of wireless modems.

**Bridges** A bridge is used to connect two networks together—even networks of different topologies, cabling types, and speeds—to connect network segments that use the same protocol. A bridge forwards traffic from one network to another. Bridges that connect networks using different transmission speeds may have a buffer to store packets until they can be forwarded to the slower network. This is known as a *store-and-forward* device. Bridges operate at OSI layer 2. Systems on either side of a bridge are part of the same broadcast domain but are in different collision domains.

**Switches** Rather than using a hub, you might consider using a switch, or intelligent hub. Switches know the addresses of the systems connected on each outbound port. Instead of repeating traffic on every outbound port, a switch repeats traffic only out of the port on which the destination is known to exist. Switches offer greater efficiency for traffic delivery, create separate collision domains, and improve the overall throughput of data. Switches can also create separate broadcast domains when used to create VLANs. In such configurations, broadcasts are allowed within a single VLAN but not allowed to cross unhindered from one VLAN to another. Switches operate primarily at OSI layer 2. When switches have additional features, such as routing, they can operate at OSI layer 3 as well (such as when routing between VLANs). Systems on either side of a switch operating at layer 2 are part of the same broadcast domain but are in different collision domains. Systems on either side of a switch operating at layer 3 are part of different broadcast domains and different collision domains. Switches are used to connect network segments that use the same protocol.

**Routers** are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between the two. They can function using statically defined routing tables, or they can employ a dynamic routing system. There are numerous dynamic routing protocols, such as RIP, OSPF, and BGP. Routers operate at OSI layer 3. Systems on either side of a router are part of different broadcast domains and different collision domains. Routers are used to connect network segments that use the same protocol.

**Brouters**  are combination devices comprising a router and a bridge. A brouter attempts to route first, but if that fails, it defaults to bridging. Thus, a brouter operates primarily at layer 3 but can operate at layer 2 when necessary. Systems on either side of a brouter operating at layer 3 are part of different broadcast domains and different collision domains. Systems on either side of a brouter operating at layer 2 are part of the same broadcast domain but are in different collision domains. Brouters are used to connect network segments that use the same protocol.

**Gateways A gateway connects networks that are using different network protocols. A gateway is responsible for transferring traffic from one network to another by transforming the format of that traffic into a form compatible with the protocol or transport method used by each network. Gateways, also known as *protocol translators*, can be stand-alone hardware devices or a software service (for example, an IP-to-IPX gateway).** Systems on either side of a gateway are part of different broadcast domains and different collision domains. Gateways are used to connect network segments that use different protocols. There are many types of gateways, including data, mail, application, secure, and Internet. **Gateways typically operate at OSI layer 7.**

**Proxies** A proxy is a form of gateway that does not translate across protocols. Instead, proxies serve as mediators, filters, caching servers, and even NAT/PAT servers for a network. A proxy performs a function or requests a service on behalf of another system and connects network segments that use the same protocol. Proxies are most often used in the context of providing clients on a private network with Internet access while protecting the identity of the clients. A proxy accepts requests from clients, alters the source address of the requester, maintains a mapping of requests to clients, and sends the altered request packets out. This mechanism is commonly known as Network Address Translation (NAT). Once a reply is received, the proxy server determines which client it is destined for by reviewing its mappings and then sends the packets on to the client. Systems on either side of a proxy are part of different broadcast domains and different collision domains.

Cabling, Wireless, Topology, and Communications Technology

There are two basic types of networks: **LANs and WANs. A *local area network (LAN)* is a network typically spanning a single floor or building. This is commonly a limited geographical area. *Wide area network (WAN)* is the term usually assigned to the long-distance connections between geographically remote networks.**

WAN connections and communication links can include **private circuit technologies and packet-switching technologies**. Common **private circuit technologies include dedicated or leased lines and PPP, SLIP, ISDN, and DSL connections**. **Packet-switching technologies include X.25, Frame Relay, asynchronous transfer mode (ATM), Synchronous Data Link Control (SDLC), and High-Level Data Link Control (HD**LC). Packet-switching technologies use virtual circuits instead of dedicated physical circuits. A virtual circuit is created only when needed, which makes for efficient use of the transmission medium and is extremely cost-effective.

**Coaxial Cable**

Coaxial cable, also called coax, was a popular networking cable type used throughout the 1970s and 1980s. In the early 1990s, its use quickly declined because of the popularity and capabilities of twisted-pair wiring (explained in more detail later). Coaxial cable has a center core of copper wire surrounded by a layer of insulation, which is in turn surrounded by a conductive braided shielding and encased in a final insulation sheath. The design of coaxial cable makes it fairly resistant to electromagnetic interference (EMI) and makes it able to support high bandwidths.

There are two main types of coaxial cable: **thinnet and thicknet. Thinnet, also known as 10Base2, was commonly used to connect systems to backbone trunks of thicknet cabling. Thinnet can span distances of 185 meters and provide throughput up to 10 Mbps. Thicknet**, also known as 10Base5, can span 500 meters and provide throughput up to 10 Mbps (megabits per second).

The most common problems with coax cable are as follows:

■ Bending the coax cable past its maximum arc radius and thus breaking the center conductor

■ Deploying the coax cable in a length greater than its maximum recommended length(which is 185 meters for 10Base2 or 500 meters for 10Base5)

■ Not properly terminating the ends of the coax cable with a 50-ohm resistor.

**Baseband and Broadband Cables**

The naming convention used to label most network cable technologies follows the syntax XXyyyyZZ. XX represents the maximum speed the cable type offers, such as 10 Mbps for a 10Base2 cable. The next series of letters, yyyy, represents the baseband or broadband aspect of the cable, such as baseband for a 10Base2 cable. Baseband cables can transmit only a single signal at a time, and broadband cables can transmit multiple signals simultaneously. Most networking cables are baseband cables. However, when used in specific configurations, coaxial cable can be used as a broadband connection, such as with cable modems. ZZ either represents the maximum distance the cable can be used or acts as shorthand to represent the technology of the cable, such as the approximately 200 meters for 10Base2 cable (actually 185 meters, but it’s rounded up to 200) or T or TX for twisted-pair in 10Base-T or 100Base-TX. (Note that 100Base-TX is implemented using two Cat 5 UTP or STP cables—one issued for receiving, the other for transmitting.)

**Type Max Speed Distance Difficulty of Installation Susceptibility to EMI Cost**

10Base2 10 Mbps 185 meters Medium Medium Medium

10Base5 10 Mbps 500 meters High Low High

10Base-T (UTP) 10 Mbps 100 meters Low High Very low

STP 155 Mbps 100 meters Medium Medium High

100Base-T/100Base-TX 100 Mbps 100 meters Low High Low

1000Base-T 1 Gbps 100 meters Low High Medium

Fiber-optic 2+ Gbps 2+ kilometers Very high None Very high

**Twisted-Pair**

Twisted-pair cabling is extremely thin and flexible compared to coaxial cable. It consists of four pairs of wires that are twisted around each other and then sheathed in a PVC insulator. If there is a metal foil wrapper around the wires underneath the external sheath, the wire is known as shielded twisted-pair (STP). The foil provides additional protection from external EMI. Twisted-pair cabling without the foil is known as unshielded twisted-pair (UTP). UTP is most often used to refer to 10Base-T, 100Base-T, or 1000Base-T, which are now considered outdated references mostly outdated technology.

The wires that make up UTP and STP are small, thin copper wires that are twisted in pairs. The twisting of the wires provides protection from external radio frequencies and electric and magnetic interference and reduces crosstalk between pairs. Crosstalk occurs when data transmitted over one set of wires is picked up by another set of wires due to radiating electromagnetic fields produced by the electrical current. Each wire pair within the cable is twisted at a different rate (in other words, twists per inch); thus, the signals traveling over one pair of wires cannot cross over onto another pair of wires (at least within the same cable). The tighter the twist (the more twists per inch), the more resistant the cable is to internal and external interference and crosstalk, and thus the capacity for throughput (that is, higher bandwidth) is greater.

**UTP Category Throughput Notes**

Cat 1 Voice only Not suitable for networks but usable by modems

Cat 2 4 Mbps Not suitable for most networks; often employed for host-to-terminal connections on mainframes

Cat 3 10 Mbps Primarily used in 10Base-T Ethernet networks (offers only 4 Mbps when used on Token Ring networks) and as telephone cables

Cat 4 16 Mbps Primarily used in Token Ring networks

Cat 5 100 Mbps Used in 100Base-TX, FDDI, and ATM networks

Cat 6 1,000 Mbps Used in high-speed networks

Cat 7 10 Gbps Used on 10 gigabit-speed networks.

The following problems are the most common with twisted-pair cabling:

■ Using the wrong category of twisted-pair cable for high-throughput networking

■ Deploying a twisted-pair cable longer than its maximum recommended length (in other words, 100 meters)

■ Using UTP in environments with significant interference

**Conductors**

The distance limitations of conductor-based network cabling stem from the resistance of the metal used as a conductor. Copper, the most popular conductor, is one of the best and least expensive room-temperature conductors available. However, it is still resistant to the flow of electrons. This resistance results in a degradation of signal strength and quality over the length of the cable.

The maximum length defined for each cable type indicates the point at which the level of degradation could begin to interfere with the efficient transmission of data**. This degradation of the signal is known as attenuation.** Attenuation is more pronounced as the speed of the transmission increases. It is recommended

that you use shorter cable lengths as the speed of the transmission increases.

Long cable lengths can often be supplemented through the use of repeaters or concentrators. A repeater is a signal amplification device, much like the amplifier for your car or home stereo. The repeater boosts the signal strength of an incoming data stream and rebroadcasts it through its second port. A concentrator does the same thing except it has more than two ports. However, using more than four repeaters (or hubs) in a row is discouraged.

An alternative to conductor-based network cabling is fiber-optic cable. Fiber-optic cables transmit pulses of light rather than electricity. This gives fiber-optic cable the advantage of being extremely fast and nearly impervious to tapping and interference. However, it is difficult to install and expensive; thus, the security and performance it offers come at a steep price.

**Ring Topology** A ring topology connects each system as points on a circle .The connection medium acts as a unidirectional transmission loop. Only one system can transmit data at a time. Traffic management is performed by a token. A token is a digital hall pass that travels around the ring until a system grabs it. A system in possession of the token can transmit data. Data and the token are transmitted to a specific destination. As the data travels around the loop, each system checks to see whether it is the intended recipient of the data. If not, it passes the token on. If so, it reads the data. Once the data is received, the token is released and returns to traveling around the loop until another system grabs it. **If any one segment of the loop is broken, all communication around the loop ceases.** Some implementations of ring topologies employ a fault tolerance mechanism, such as dual loops running in opposite directions, to prevent single points of failure.

**Bus Topology** A bus topology connects each system to a trunk or backbone cable. All systems on the bus can transmit data simultaneously, which can result in collisions. A collision occurs when two systems transmit data at the same time; the signals interfere with each other. To avoid this, the systems employ a collision avoidance mechanism that basically “listens” for any other currently occurring traffic. If traffic is heard, the system waits a few moments and listens again. If no traffic is heard, the system transmits its data. When data is transmitted on a bus topology, all systems on the network hear the data. If the data is not addressed to a specific system, that system just ignores the data. The benefit of a bus topology is that if a single segment fails, communications on all other segments continue uninterrupted. However, the central trunk line remains a single point of failure. **There are two types of bus topologies: linear and tree. A linear bus topology employs a single trunk line with all systems directly connected to it. A tree topology employs a single trunk line with branches that can support multiple systems.**

**Star Topology** A star topology employs a centralized connection device. This device can be a simple hub or switch. Each system is connected to the central hub by a dedicated segment. If any one segment fails, the other segments can continue to function. However, the central hub is a single point of failure. Generally, the star topology uses less cabling than other topologies and makes the identification of damaged cables easier

**Mesh Topology** A mesh topology connects systems to other systems using numerous paths. A full mesh topology connects each system to all other systems on the network. A partial mesh topology connects many systems to many other systems. Mesh topologies provide redundant connections to systems, allowing multiple segment failures without seriously affecting connectivity.

**General wireless concepts**

Spread spectrum means that communication occurs over multiples frequencies at the same time. Thus, a message is broken into pieces, and each piece is sent at the same time but using a different frequency. Effectively this is a parallel communication rather than a serial communication.

**Frequency Hopping Spread Spectrum (FHSS)** was an early implementation of the spread spectrum concept. However, instead of sending data in a parallel fashion, **it transmits data in a series while** constantly changing the frequency in use. The entire range of available frequencies is employed, but only one frequency at a time is used. As the sender changes from one frequency to the next, the receiver has to follow the same hopping pattern to pick up the signal. FHSS was designed to help minimize interference by not using only a single frequency that could be affected. Instead, by constantly shifting frequencies, it minimizes interference.

**Direct Sequence Spread Spectrum (DSSS)** employs all the available frequencies simultaneously in parallel. This provides a higher rate of data throughput than FHSS. **DSSS also uses a special encoding mechanism known as chipping code to allow a receiver to reconstruct data even if parts of the signal were distorted because of interference. This occurs in much** the same way that the parity of RAID-5 allows the data on a missing drive to be re-created.

**Orthogonal Frequency-Division Multiplexing (OFDM**) is yet another variation on frequency use. OFDM **employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission**. The modulated signals are perpendicular (orthogonal) and thus do not cause interference with each other. Ultimately, OFDM requires a smaller frequency set (aka channel bands) but can offer greater data throughput.

**Cell phones**

Technology Generation

NMT 1G

AMPS 1G

TACS 1G

GSM 2G

iDEN 2G

TDMA 2G

CDMA 2G

PDC 2G

HSCSD 2.5G

GPRS 2.5G

W-CDMA 3G

TD-CDMA 3G

UWC 3G

EDGE 3G

DECT 3G

UMTS 3G

HSPDA 3.5G

WiMax – IEEE 802.16 4G

XOHM (Brand name of WiMax) 4G

Mobile Broadband – IEEE 802.20 4G

LTE (Long Term Evolution) 4G

One important cell phone technology to discuss is **Wireless Application Protocol (WAP**). WAP is not a standard; instead, it is a functioning industry-driven protocol stack. Via WAP-capable devices. **One of these protocols is Wireless Transport Layer Security (WTLS), which provides security connectivity services similar to those of SSL or TLS.**

A secure link is established **between the mobile device and the telco’s main server** using **WAP/WTLS**. The data is converted into its clear form before being reencapsulated in SSL, TLS, IPSec, and so on for its continued transmission.

**Bluetooth (802.15) -Personal area network.**

**LAN Technologies**

T**here are three main types of LAN technologies: Ethernet, Token Ring, and FDDI.**

**Ethernet**

Ethernet is a shared-media LAN technology (also known as a broadcast technology). That means it allows numerous devices to communicate over the same medium but requires that the devices take turns communicating and performing collision detection and avoidance**. Ethernet employs broadcast and collision domains**. A broadcast domain is a physical grouping of systems in which all the systems in the group receive a broadcast sent by a single system in the group. A broadcast is a message transmitted to a specific address that indicates that all systems are the intended recipients.

A collision domain consists of groupings of systems within which a data collision occurs if two systems transmit simultaneously. A data collision takes place when two transmitted messages attempt to use the network medium at the same time. It causes one or both of the messages to be corrupted.

Ethernet can support full-duplex communications (in other words, full two-way) and usually employs twisted-pair cabling. (Coaxial cabling was originally used.) Ethernet is most often deployed on star or bus topologies. Ethernet is based on the IEEE 802.3 standard. Individual units of Ethernet data are called frames. Fast Ethernet supports 100 Mbps throughput. Gigabit Ethernet supports 1,000 Mbps (1 Gbps) throughput. 10 Gigabit Ethernet support 10,000 Mbps (10 Gbps) throughput.

**Token Ring**

Token Ring employs a token-passing mechanism to control which systems can transmit data over the network medium. The token travels in a logical loop among all members of the LAN. Token Ring can be **employed on ring or star network topologies**. It is rarely used today because of its performance limitations, **higher cost compared to Ethernet**, and increased difficulty in deployment and management. Token Ring can be deployed as a physical star using a multi station access unit (MAU). A MAU allows for the cable segments to be deployed as a star while internally the device makes logical ring connections.

**Fiber Distributed Data Interface (FDDI)**

**Fiber Distributed Data Interface is a high-speed token-passing technology that employs two rings with traffic flowing in opposite directions. FDDI is often used as a backbone for large enterprise networks**. Its dual-ring design allows for self-healing by removing the failed segment from the loop and creating a single loop out of the remaining inner and outer ring portions. **FDDI is expensive but was often used in campus environments before Fast Ethernet and Gigabit Ethernet were developed. A less-expensive, distance-limited, and slower version known as Copper Distributed Data Interface (CDDI) uses twisted-pair cables. CDDI is also more vulnerable to interference and eavesdropping.**

**Analog and Digital**

One sub technology common to many forms of network communications is the mechanism used to actually transmit signals over a physical medium, such as a cable. There are two types: analog and digital.

Analog communications occur with a continuous signal that varies in frequency, amplitude, phase, voltage, and so on. The variances in the continuous signal produce a wave shape (as opposed to the square shape of a digital signal). The actual communication occurs by variances in the constant signal.

Digital communications occur through the use of a discontinuous electrical signal and a state change or on-off pulses.

**Synchronous and Asynchronous**

Some communications are synchronized with some sort of clock or timing activity. Communications are either synchronous or asynchronous:

■ **Synchronous communications rely on a timing or clocking mechanism based on either an independent clock or a time stamp embedded in the data stream. Synchronous communications are typically able to support very high rates of data transfer.**

■ Asynchronous communications rely **on a stop and start delimiter** bit to manage the transmission of data. Because of the use of delimiter bits and the stop and start nature of its transmission, asynchronous communication is best suited for smaller amounts of data. **Public switched telephone network (PSTN) modems are good examples of asynchronous communication devices**.

**Baseband and Broadband**

How many communications can occur simultaneously over a cable segment depends on whether you use baseband technology or broadband technology:

■ **Baseband technology can support only a single communication channel**. It uses a direct current applied to the cable. A current that **is at a higher level represents the binary signal of 1, and a current that is at a lower level represents the binary signal of** 0. **Baseband is a form of digital signal**. **Ethernet is a baseband technology.**

■ Broadband technology can support multiple simultaneous signals. **Broadband uses frequency modulation to support numerous channels, each supporting a distinct communication session**. Broadband is suitable for high throughput rates, especially when several channels are multiplexed**. Broadband is a form of analog signal. Cable television and cable modems, ISDN, DSL, T1, and T3 are examples of broadband technologies.**

**Broadcast, Multicast, and Unicast**

Broadcast, multicast, and unicast technologies determine how many destinations a single transmission can reach

■ Broadcast technology supports communications to all possible recipients.

■ Multicast technology supports communications to multiple specific recipients.

■ Unicast technology supports only a single communication to a specific recipient.

**Carrier-Sense Multiple Access (CSMA)** This is the LAN media access technology that performs communications using the following steps:

1. The host listens to the LAN media to determine whether it is in use.

2. If the LAN media is not being used, the host transmits its communication.

3. The host waits for an acknowledgment.

4. If no acknowledgment is received after a time-out period, the host starts over at step 1.

CSMA does not directly address collisions. If a collision occurs, the communication would not have been successful, and thus an acknowledgment would not be received. This causes the sending system to retransmit the data and perform the CSMA process again.

**Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)** This is the LAN media access technology that performs communications using the following steps:

**1.** The host has two connections to the LAN media: inbound and outbound. The host listens on the inbound connection to determine whether the LAN media is in use.

**2.** If the LAN media is not being used, the host requests permission to transmit.

**3.** If permission is not granted after a time-out period, the host starts over at step 1.

**4.** If permission is granted, the host transmits its communication over the outbound connection.

**5.** The host waits for an acknowledgment.

**6.** If no acknowledgment is received after a time-out period, the host starts over at step 1.

**AppleTalk and 802.11 wireless networking** are examples of networks **that employ CSMA/ CA technologies**. CSMA/CA attempts to avoid collisions by granting only a single permission to communicate at any given time. This system requires designation of a master or primary system, which responds to the requests and grants permission to send data transmissions.

**Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)** This is the LAN media access technology that performs communications using the following steps:

1. The host listens to the LAN media to determine whether it is in use.

2. If the LAN media is not being used, the host transmits its communication.

3. While transmitting, the host listens for collisions (in other words, two or more hosts transmitting simultaneously).

4. If a collision is detected, the host transmits a jam signal.

5. If a jam signal is received, all hosts stop transmitting. Each host waits a random period of time and then starts over at step 1.

**Ethernet networks employ the CSMA/CD technology.** CSMA/CD responds to collisions by having each member of the collision domain wait for a short but random period of time before starting the process over. Unfortunately, allowing collisions to occur and then responding or reacting to collisions causes delays in transmissions as well as a required repetition of transmissions. This results in about 40 percent loss in potential throughput.

**Token Passing** This is the LAN media access technology that performs communications using a digital token. Possession of the token allows a host to transmit data. Once its transmission is complete, it releases the token to the next system. **Token passing is used by Token Ring networks, such as FDDI. Token Ring prevents collisions since only the system possessing the token is allowed to transmit data**.

**Polling** This is the LAN media access technology **that performs communications using a master-slave**

**configuration. One system is labeled as the primary system. All other systems are labeled as secondary**. The primary system polls or inquires of each secondary system in turn whether they have a need to transmit data. If a secondary system indicates a need, it is granted permission to transmit. Once its transmission is complete, the primary system moves on to poll the next secondary system. Synchronous Data Link Control (SDLC) uses polling.

Polling addresses collisions by attempting to prevent them from using a permission system. Polling is an inverse of the CSMA/CA method. Both use masters and slaves (or primary and secondary), but while CSMA/CA allows the slaves to request permissions, polling has the master offer permission. Polling can be configured to grant one (or more) system priority over other systems…