Figure 14-4

Attenuation

Background noise can merge with an electronic signal and alter the signal’s integrity.

Noise The term line noise refers to random fluctuations in electrical-magnetic impulses that are carried along a physical medium. Noise on a line is usually caused by surrounding devices or by characteristics of the wiring’s environment. Noise can be caused by motors, computers, copy machines, fluorescent lighting, and microwave ovens, to name a few.

This background noise can combine with the data being transmitted over the cable and distort the signal, as shown in Figure 14-4. The more noise there is interacting with the cable, the more likely the receiving end will not receive the data in the form originally transmitted.

Attenuation Attenuation is the loss of signal strength as it travels. This is akin to rolling a ball down the floor; as it travels, air causes resistance that slows it down and eventually stops it. In the case of electricity, the metal in the wire also offers resistance to the flow of electricity. Though some materials such as copper and gold offer very little resistance, it is still there. The longer a wire, the more attenuation occurs, which causes the signal carrying the data to deteriorate. This is why standards include suggested cablerun lengths.

The effects of attenuation increase with higher frequencies; thus, 100Base-TX at 80 MHz has a higher attenuation rate than 10Base-T at 10 MHz. This means that cables used to transmit data at higher frequencies should have shorter cable runs to ensure attenuation does not become an issue.

If a networking cable is too long, attenuation will become a problem. Basically, the data is in the form of electrons, and these electrons have to “swim” through a copper wire. However, this is more like swimming upstream, because there is a lot of resistance on the electrons working in this media. After a certain distance, the electrons start to slow down and their encoding format loses form. If the form gets too degraded, the receiving system cannot interpret the electrons any longer. If a network administrator needs to run a cable longer than its recommended segment length, she needs to insert a repeater or some type of device that amplifies the signal and ensures that it gets to its destination in the right encoding format.

Attenuation can also be caused by cable breaks and malfunctions. This is why cables should be tested. If a cable is suspected of attenuation problems, cable testers can inject signals into the cable and read the results at the end of the cable.

EXAM TIP Most implementations of Ethernet over UTP have a maximum cable length of 100 meters, partly to deal with attenuation.

Crosstalk Crosstalk is a phenomenon that occurs when electrical signals of one wire spill over to the signals of another wire. When electricity flows through a wire, it generates a magnetic field around it. If another wire is close enough, the second wire acts as an antenna that turns this magnetic field into an electric current. When the different electrical signals mix, their integrity degrades and data corruption can occur. UTP mitigates crosstalk by twisting the wires around each other. Because crosstalk is greatest wherever wires are parallel to each other, this twisting makes it harder for this condition to exist. Still, UTP is much more vulnerable to crosstalk than STP or coaxial because it does not have extra layers of shielding to help protect against it.

NOTE While a lot of the world’s infrastructure is wired and thus uses one of these types of cables, remember that a growing percentage of our infrastructure is not wired, but rather uses some form of wireless technology (Bluetooth, Wi-Fi, satellite, etc.), particularly to reach end devices.

Fire Rating of Cables Just as buildings must meet certain fire codes, so must wiring schemes. A lot of organizations string their network wires in drop ceilings—the space between the ceiling and the next floor—or under raised floors. This hides the cables and prevents people from tripping over them. However, when wires are strung in places like this, they are more likely to catch on fire without anyone knowing about it. Some cables produce hazardous gases when on fire that would spread throughout the building quickly.

Network cabling that is placed in these types of areas, called plenum space, must meet a specific fire rating to ensure the cable will not produce and release harmful chemicals in case of a fire. A ventilation system's components are usually located in this plenum space, so if toxic chemicals were to get into that area, they could easily spread throughout the building in minutes.

Nonplenum cables usually have a polyvinyl chloride (PVC) jacket covering, whereas plenum-rated cables have jacket covers made of fluoropolymers. When setting up a network or extending an existing network, it is important that you know which wire types are required in which situation.

Cables should be installed in unexposed areas so they are not easily tripped over, damaged, or eavesdropped upon. The cables should be strung behind walls and in the protected spaces, such as in dropped ceilings. In environments that require extensive security, wires can be encapsulated within pressurized conduits so if someone attempts to access a wire, the pressure of the conduit changes, causing an alarm to sound and a message to be sent to the security staff. A better approach to high-security requirements is probably to use fiber-optic cable, which is much more difficult to covertly tap.

Bandwidth and Throughput

Whatever type of transmission you use over any given cable, there is a limit to how much information you can encode within it. In computer networks, we use two different but related terms to measure this limit. Bandwidth is the amount of information that theoretically can be transmitted over a link within a second. In a perfect world, this is the data transfer capability of a connection and is commonly associated with the number of available frequencies and speed of a link. Data throughput is the actual amount of data that can be carried over a real link. Throughput is always less than or equal to a link's bandwidth. In fact, it is most often the case that throughput is notably less than bandwidth. Why?

As mentioned, bandwidth is a theoretical limit determined by analyzing a medium (e.g., category 5 UTP cable) and a physical layer protocol (e.g., 100BaseT Ethernet) and then doing the math to calculate the maximum possible amount of data we could push through it. Now, of course, when you put that medium and protocol into a real environment, a multitude of issues come into play and make it hard to achieve that optimal data rate.

The throughput of our networks is affected by many factors. There could be EMI (or line noise) in the medium, as previously discussed. However, in a well-engineered facility and network, this should not be a big problem. Typically, you'll be more concerned about packet delays and losses. Latency is the amount of time it takes a packet to get from its source to its destination. This could be measured as either time to first byte (TTFB) or round-trip time (RTT). Latency can be caused by multiple factors, including

- Transmission medium Even though electricity and light move at the speed of light, it still takes time to get from one place to another. If your links are very long, or if the cables have too many imperfections, the medium itself will cause latency.
- Network devices Routers and firewalls take some time to examine packets, even if they're just deciding which outbound interface to use. If you have too many rules in your routing or security devices, this is invariably going to introduce delays.

To reduce latency, you should keep your physical links as short as possible. You should also look at how many hops your packets must take to get to their destinations. Virtual LANs (VLANs) can help keep devices that communicate frequently "closer" to each other. For international organizations, using a content distribution network (CDN), which we address later in this chapter, keeps most data close to where it is needed. Finally, the use of proxies can reduce latency by bringing frequently requested data closer to your users.

Another issue that negatively impacts your data throughputs (compared to a link's rated bandwidth) is congestion. Since some links in your network are shared, if you have too many packets moving around, it will inevitably bog things down. You may have a 1-GBps (bandwidth) connection to your home, but if every house in your neighborhood has one too and you all share a 1-GBps link from the local switch to the first router, your throughput will be way lower than advertised unless you log on when everyone else is sleeping. The best way to prevent congestion is through careful design and implementation of your network. Keep your broadcast domains as small as possible, ensure that your shared links are able to support peak traffic rates, and consider prioritizing certain types of traffic so that if your staff decides to livestream news, that doesn’t slow down your ability to get real work done.

Network Devices

Several types of devices are used in LANs, MANs, and WANs to provide intercommunication among computers and networks. We need to have physical devices throughout the network to actually use all the protocols and services we have covered up to this point.

The different network devices vary according to their functionality, capabilities, intelligence, and network placement. We will look at the following devices:

The typical network has a bunch of these devices, and their purposes and operation can get confusing really quickly. Therefore, we will also look at network diagram techniques that can help us create different (simpler) views into complex environments. We’ll also consider operational issues like power requirements, warranties, and support agreements.

Repeaters

A repeater provides the simplest type of connectivity because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.

A hub is a multiport repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

- Repeaters
- Bridges
- Switches
- Routers
- Gateways
- Proxy servers
- PBXs
- Network access control devices

NOTE Hubs are exceptionally rare nowadays but you may still come across them.

Bridges

A bridge is a LAN device used to connect LAN segments (or VLAN segments) and thus extends the range of a LAN. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If it is not, the bridge forwards the frame to the necessary network segment. A bridge amplifies the electrical signal, as does a repeater, but it has more intelligence than a repeater and is used to extend a LAN and enable the administrator to filter frames to control which frames go where.

When using bridges, you have to watch carefully for broadcast storms. While bridges break up a collision domain by port (i.e., computers on the same bridge port are in the same collision domain), all ports are on the same broadcast domain. Because bridges can forward all traffic, they forward all broadcast packets as well. This can overwhelm the network and result in a broadcast storm, which degrades the network bandwidth and performance.

The international standard for bridges on Ethernet networks is IEEE 802.1Q. It describes the principal elements of bridge operation as follows:

- Relaying and filtering frames (based on MAC addresses and port numbers)
- Maintenance of the information required to make frame filtering and relaying decisions (i.e., the forwarding tables)
- Management of the elements listed (e.g., aging off forwarding table entries)

EXAM TIP Do not confuse routers with bridges. Routers work at the network layer and filter packets based on IP addresses, whereas bridges work at the data link layer and filter frames based on MAC addresses. Routers usually do not pass broadcast information, but bridges do pass broadcast information.

Forwarding Tables

A bridge must know how to get a frame to its destination—that is, it must know to which port the frame must be sent and where the destination host is located. Years ago, network administrators had to type route paths into bridges so the bridges had static paths indicating where to pass frames that were headed for different destinations. This was a tedious task and prone to errors. Today, most bridges use transparent bridging.

In transparent bridging, a bridge starts to learn about the network's environment as soon as it is powered on and continues to learn as the network changes. It does this by examining frames and making entries in its forwarding tables. When a bridge receives a frame from a new source computer, the bridge associates this new source address and the

Connecting Two LANS: Bridge vs. Router

What is the difference between two LANs connected via a bridge versus two LANs connected via a router? If two LANs are connected with a bridge, the LANs have been extended because they are both in the same broadcast domain. A router separates broadcast domains, so if two LANs are connected with a router, an internetwork results. An internetwork is a group of networks connected in a way that enables any node on any network to communicate with any other node. The Internet is an example of an internetwork.

Switches

Switches are, essentially, multiport bridges that typically have additional management features. Because bridges are intended to connect and extend LANs (and not necessarily individual hosts), they tend to have few ports. However, if you take the exact same functionality and add a bunch of ports to it, you could use the ports to connect to each individual host or to other switches. Figure 14-5 illustrates a typical, hierarchical network configuration in which computers are directly connected to access switches within close proximity (100 m or less). Access switches are, in turn, connected to distribution switches, which usually connect different departments or floors in a building. This distribution layer is a great place to implement access control lists (ACLs) and filtering to provide security. Finally, the upper tier of core switches provides a high-speed switching and routing backbone for the organization and is designed to pass network traffic as fast as possible. In this layer, only switches are connected to each other (i.e., there are no computers directly connected to them).

On Ethernet networks, computers have to compete for the same shared network medium. Each computer must listen for activity on the network and transmit its data when it thinks the coast is clear. This contention and the resulting collisions cause

port on which it arrived. It does this for all computers that send frames on the network.

Eventually, the bridge knows the address of each computer on the various network segments and to which port each is connected. If the bridge receives a request to send a frame to a destination that is not in its forwarding table, it sends out a query frame on each network segment except for the source segment. The destination host is the only one that replies to this query. The bridge updates its table with this computer address and the port to which it is connected and forwards the frame.

Many bridges use the Spanning Tree Protocol (STP), which adds more intelligence to the bridges. STP ensures that frames do not circle networks forever, provides redundant paths in case a bridge goes down, assigns unique identifiers to each bridge, assigns priority values to these bridges, and calculates path costs. This creates much more efficient frame-forwarding processes by each bridge. STP also enables an administrator to indicate whether he wants traffic to travel certain paths instead of others. Newer bridges implement the Shortest Path Bridging (SPB) protocol, which is defined in IEEE 802.1aq and is more efficient and scalable than STP.

Core

Distribution

Access

Figure 14-5

Hierarchical model of a switched network traffic delays and use up precious bandwidth. When switches are used, contention and collisions are not issues, which results in more efficient use of the network’s bandwidth and decreased latency. Switches reduce or remove the sharing of the network medium and the problems that come with it.

Since a switch is a multiport bridging device where each port is connected to exactly one other device, each port provides dedicated bandwidth to the device attached to it. A port is bridged to another port so the two devices have an end-to-end private link. The switch employs full-duplex communication, so one wire pair is used for sending and another pair is used for receiving. This ensures the two connected devices do not compete for the same bandwidth.

Basic switches work at the data link layer and forward traffic based on MAC addresses. However, today’s layer 3, layer 4, and other layer switches have more enhanced functionality than layer 2 switches. These higher-level switches offer routing functionality, packet inspection, traffic prioritization, and QoS functionality. These switches are referred to as multilayered switches because they combine data link layer, network layer, and other layer functionalities.

Multilayered switches use hardware-based processing power, which enables them to look deeper within the frame, to make more decisions based on the information encapsulated within the frame, and then to provide forwarding and traffic management tasks. Usually this amount of work creates a lot of overhead and traffic delay, but multilayered switches perform these activities within an application-specific integrated circuit (ASIC). This means that most of the functions of the switch are performed at the hardware and chip level rather than at the software level, making it much faster than routers.

CAUTION While it is harder for attackers to sniff traffic on switched networks, they should not be considered safe just because switches are involved. Attackers commonly poison cache memory used on switches to divert traffic to their desired location.

Layer 3 and 4 Switches

In Address

Tag Prefix

Out Out
I/F Tag

In In
Tag I/F

Address
Prefix

Out Out
I/F Tag

128.89

1

128.89

0

171.69

1

171.69

1

Tag request
for 128.89

2

Out Out
I/F Tag

128.89

1

0
3
1

Tag request
for 128.89

Tag request
for 128.89

Tag request
for 171.69

Tag request
for 128.89

Figure 14-6

Address
Prefix

1

1
Tag request
for 171.69

In In
Tag I/F

MPLS uses tags and tables for routing functions.

0

PART IV

Layer 2 switches only have the intelligence to forward a frame based on its MAC address and do not have a higher understanding of the network as a whole. A layer 3 switch has the intelligence of a router. It not only can route packets based on their IP addresses but also can choose routes based on availability and performance. A layer 3 switch is basically a router on steroids, because it moves the route lookup functionality to the more efficient switching hardware level.

The basic distinction between layer 2, 3, and 4 switches is the header information the device looks at to make forwarding or routing decisions (data link, network, or transport OSI layers). But layer 3 and 4 switches can use tags, which are assigned to each destination network or subnet. When a packet reaches the switch, the switch compares the destination address with its tag information base, which is a list of all the subnets and their corresponding tag numbers. The switch appends the tag to the packet and sends it to the next switch. All the switches in between this first switch and the destination host just review this tag information to determine which route it needs to take, instead of analyzing the full header. Once the packet reaches the last switch, this tag is removed and the packet is sent to the destination. This process increases the speed of routing of packets from one location to another.

The use of these types of tags, referred to as Multiprotocol Label Switching (MPLS), not only allows for faster routing but also addresses service requirements for the different packet types. Some time-sensitive traffic (such as video conferencing) requires a certain level of service (QoS) that guarantees a minimum rate of data delivery to meet the requirements of a user or application. When MPLS is used, different priority information is placed into the tags to help ensure that time-sensitive traffic has a higher priority than less sensitive traffic, as shown in Figure 14-6.

Because security requires control over who can access specific resources, more intelligent devices can provide a higher level of protection because they can make more detail-oriented decisions regarding who can access resources. When devices can look deeper into the packets, they have access to more information to make access decisions, which provides more granular access control.

As previously stated, switching makes it more difficult for intruders to sniff and monitor network traffic because no broadcast and collision information is continually traveling throughout the network. Switches provide a security service that other devices cannot provide. VLANs (described in depth in Chapter 13) are an important part of switching networks, because they enable administrators to have more control over their environment and they can isolate users and groups into logical and manageable entities.

Routers

We are going up the chain of the OSI layers while discussing various network devices. Repeaters work at the physical layer, bridges and switches work at the data link layer, and routers work at the network layer. As we go up each layer, each corresponding device has more intelligence and functionality because it can look deeper into the frame. A repeater looks at the electrical signal. The switch can look at the MAC address within the header. The router can peel back the first header information and look farther into the frame and find out the IP address and other routing information. The farther a device can look into a frame, the more decisions it can make based on the information within the frame.

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Frame Relay link.) A router is a device that has two or more interfaces and a routing table, so it knows how to get packets to their destinations. It can filter traffic based on an access control list (ACL), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

A router discovers information about routes and changes that take place in a network through its routing protocols (RIP, BGP, OSPF, and others, as discussed in Chapter 11). These protocols tell routers if a link has gone down, if a route is congested, and if another route is more economical. They also update routing tables and indicate if a router is having problems or has gone down.

The router may be a dedicated appliance or a computer running a networking operating system that is dual-homed. When packets arrive at one of the interfaces, the router compares those packets to its ACL. This list indicates what packets are allowed in and what packets are denied. Access decisions are based on source and destination IP addresses, protocol type, and source and destination ports. An administrator may block all packets coming from the 10.10.12.0 network, any FTP requests, or any packets headed toward a specific port on a specific host, for example. This type of control is provided by the ACL, which the administrator must program and update as necessary.

What actually happens inside the router when it receives a packet? Let’s follow the steps:

1. A packet is received on one of the interfaces of a router. The router views the routing data.
2. The router retrieves the destination IP network address from the packet.
3. The router looks at its routing table to see which port matches the requested destination IP network address.
4. If the router does not have information in its table about the destination address, it sends out an ICMP error message to the sending computer indicating that the

message could not reach its destination.

5. If the router does have a route in its routing table for this destination, it decrements the TTL value and sees whether the maximum transmission unit (MTU) is different for the destination network. If the destination network requires a smaller MTU, the router fragments the packet.

7. The router sends the packet to its output queue for the necessary interface.

Table 14-3 provides a quick review of how routers differ from bridges and switches.

When is it best to use a repeater, bridge, or router? A repeater is used if an administrator needs to expand a network and amplify signals so they do not weaken on longer cables. However, a repeater also extends collision and broadcast domains.

Bridges and switches work at the data link layer and have a bit more intelligence than a repeater. Bridges can do simple filtering and separate collision domains, but not broadcast domains. A switch should be used when an administrator wants to connect multiple computers in a way that reduces traffic congestion and excessive collisions.

A router splits up a network into collision domains and broadcast domains. A router gives more of a clear-cut division between network segments than repeaters or bridges.

Bridge/Switch

Router

Reads header information but does not alter it

Creates a new header for each packet

Builds forwarding tables based on MAC addresses

Builds routing tables based on IP addresses

Has no concept of network addresses

Assigns a different network address per port

Filters traffic based on MAC addresses

Filters traffic based on IP addresses

Forwards broadcast traffic

Does not forward broadcast traffic

Forwards traffic if a destination address is unknown to the bridge

Does not forward traffic that contains a destination address unknown to the router

Table 14-3

Main Differences Between Bridges/Switches and Routers

6. The router changes header information in the packet so that the packet can go to the next correct router, or if the destination computer is on a connecting network, the changes made enable the packet to go directly to the destination computer.

A router should be used if an administrator wants to have more defined control of where the traffic goes, because more sophisticated filtering is available with routers, and when a router is used to segment a network, the result is more controllable sections.

Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate mail from one type of mail server and format it so that another type of mail server can accept and understand it, or it can connect and translate different data link technologies such as Fiber Distributed Data Interface (FDDI) to Ethernet (both of which are discussed in Chapter 11).

Gateways perform much more complex tasks than connection devices such as routers and bridges. However, some people refer to routers as gateways when they connect two unlike networks (Token Ring and Ethernet) because the router has to translate between the data link technologies. Figure 14-7 shows how a network access server (NAS) functions as a gateway between telecommunications and network connections.

When networks connect to a backbone, a gateway can translate the different technologies and frame formats used on the backbone network versus the connecting LAN protocol frame formats. If a bridge were set up between an FDDI backbone and an Ethernet LAN, the computers on the LAN would not understand the FDDI protocols and frame formats. In this case, a LAN gateway would be needed to translate the protocols used between the different networks.

NAS

Figure 14-7

Several types of gateways can be used in a network. A NAS is one example.

A popular type of gateway is an e-mail gateway. Because several e-mail vendors have their own syntax, message format, and way of dealing with message transmission, e-mail gateways are needed to convert messages between e-mail server software. For example, suppose that David, whose corporate network uses Sendmail, writes an e-mail message to Dan, whose corporate network uses Microsoft Exchange. The e-mail gateway converts the message into a standard that all mail servers understand—usually X.400—and passes it on to Dan's mail server.

Proxy Servers

Figure 14-8
Proxy servers
control traffic
between clients
and servers.

Computer A

Computer B

Computer C

Proxy
server

Web
server

Proxy servers act as an intermediary between the clients that want access to certain services and the servers that provide those services. As a security professional, you do not want internal systems to directly connect to external servers without some type of control taking place. For example, if users on your network could connect directly to websites without some type of filtering and rules in place, the users could allow malicious traffic into the network or could surf websites your organization deems inappropriate. To prevent this situation, all internal web browsers should be configured to send their web requests to a web proxy server. The proxy server validates that the request is safe and then sends an independent request to the website on behalf of the user. A very basic proxy server architecture is shown in Figure 14-8.

The proxy server may cache the response it receives from the server so that when other clients make the same request, the proxy server doesn’t have to make a connection out to the actual web server again but rather can serve up the necessary data directly. This drastically reduces latency and allows the clients to get the data they need much more quickly.

There are different types of proxies that provide specific services. A forwarding proxy is one that allows the client to specify the server it wants to communicate with, as in our scenario earlier. An open proxy is a forwarding proxy that is open for anyone to use. An anonymous open proxy allows users to conceal their IP address while browsing websites

or using other Internet services. A reverse proxy appears to the clients as the original server. The client sends a request to what it thinks is the original server, but in reality this reverse proxy makes a request to the actual server and provides the client with the response. The forwarding and reverse proxy functionality seems similar, but as Figure 14-9 illustrates, a forwarding proxy server is commonly on an internal network controlling traffic that is exiting the network. A reverse proxy server is commonly on the network that fulfills clients’ requests; thus, it is handling traffic that is entering its network. The reverse proxy can carry out load balancing, encryption acceleration, security, and caching.

Web proxy servers are commonly used to carry out content filtering to ensure that Internet use conforms to the organization’s acceptable use policy (AUP). These types of proxies can block unacceptable web traffic, provide logs with detailed information pertaining to the websites specific users visited, monitor bandwidth usage statistics, block restricted website usage, and screen traffic for specific keywords (e.g., porn, confidential, Social Security numbers). The proxy servers can be configured to act mainly as caching servers, which keep local copies of frequently requested resources, allowing organizations to significantly reduce their upstream bandwidth usage and costs while significantly increasing performance.

While the most common use of proxy servers is for web-based traffic, they can be used for other network functionality and capabilities, as in DNS proxy servers. Proxy servers are a critical component of almost every network today. They need to be properly placed, configured, and monitored.

NOTE The use of proxy servers to allow for online anonymity has increased over the years. Some people use a proxy server to protect their browsing behaviors from others, with the goal of providing personal freedom and privacy. Attackers use the same functionality to help ensure their activities cannot be tracked back to their local systems.

Figure 14-9
Forward vs.
reverse proxy
services
User

Proxy

Internet

Internal network

Internet

Proxy

Web server

Internal network

The Tor Network

Tor (originally known as The Onion Router) is a volunteer-operated network of computers around the world that work together to route encrypted web traffic. The goal of Tor is to keep your identity private online, or at least as close to private as is possible. (Misconfigurations or exploitable software on your local machine can still reveal your identity.) Every computer (or node) in Tor receives data from another node and passes it on to the next. Each node only knows where the encrypted data came from and where it’s going next. After several hops, someone at the destination has no way of knowing who initiated the connection when you pop back up in the open Internet. Tor can also provide access to so-called “hidden services” in the deep web that run only inside Tor. The infamous drug marketplace The Silk Road was an example of this. Tor is very popular among privacy advocates and people who live in countries that have strong censorship laws. However, Tor also is commonly used by criminal and even nation-state actors who want to protect their source location. Therefore, you should be extremely suspicious if you see Tor traffic in any enterprise network.

Telephone companies use switching technologies to transmit phone calls to their destinations. A telephone company’s central office houses the switches that connect towns, cities, and metropolitan areas through the use of optical fiber rings. So, for example, when

Putting It All Together: Network Devices

The network devices we’ve covered so far are the building blocks of almost any network architecture. Table 14-4 lists them and points out their important characteristics.

Device	OSI Layer	Functionality
Repeater	Physical	Amplifies the signal and extends networks
Bridge	Data link	Forwards packets and filters based on MAC addresses; forwards broadcast traffic, but not collision traffic
Switch	Data link	Provides a private virtual link between communicating devices; allows for VLANs; reduces collisions; impedes network sniffing
Router	Network	

		Separates and connects LANs creating internetworks; filters based on IP addresses
Gateway	Application	Connects different types of networks; performs protocol and format translations
Web proxy	Application	Acts as an intermediary between clients and servers, typically to improve security and/or performance

Table 14-4 Main Differences Between Network Devices

PBXs

Dusty makes a landline phone call from his house, the call first hits the local central office of the telephone company that provides service to Dusty, and then the switch within that office decides whether it is a local or long-distance call and where it needs to go from there. A Private Branch Exchange (PBX) is a private telephone switch that is located on an organization’s property. This switch performs some of the same switching tasks that take place at the telephone company’s central office. The PBX has a dedicated connection to its local telephone company’s central office, where more intelligent switching takes place.

A PBX can interface with several types of devices and provides a number of telephone services. The voice data is multiplexed onto a dedicated line connected to the telephone company’s central office. Figure 14-10 shows how data from different data sources can be placed on one line at the PBX and sent to the telephone company’s switching facility.

PBXs use digital switching devices that can control analog and digital signals. While these modern exchanges are more secure than their analog predecessors, that in no way means PBX systems are free from vulnerabilities. Many PBX systems have system administrator passwords that are hardly ever changed. These passwords are set by default; therefore, if 100 companies purchase and implement 100 PBX systems from the PBX vendor ABC and they do not reset the password, a phreaker (a phone hacker) who knows this default password now has access to 100 PBX systems. Once a phreaker breaks into a PBX system, she can cause mayhem by rerouting calls, reconfiguring switches, or configuring the system to provide her and her friends with free long-distance calls. This type of fraud happens more often than most organizations realize because many of them do not closely audit their phone bills. Though the term is not used as much nowadays, phreakers are very much an issue to our telecommunications systems. Toll fraud (as most of their activities are called) associated with PBX systems are estimated to cost over $3 billion in annual losses worldwide, according to the Communications Fraud Control Association’s (CFCA) 2019 Fraud Loss Survey.

Analog
voice
interface

Digital
voice
interface

Digital
switch

Data
interface

Figure 14-10 A PBX combines different types of data on the same lines.

TI

Network Access Control Devices

Network access control (NAC) is any set of policies and controls that we use to, well, control access to our networks. The term implies that we will verify that a device satisfies certain requirements before we let it in. At its simplest level, this could just be user authentication, which was the theme of our discussion of the IEEE 802.1X standard when we were covering wireless network security in Chapter 12. The 802.1X protocol allows devices to connect in a very limited manner (i.e., only to the network authenticator) until we can verify the user credentials it presents.

To fully leverage the power of NAC, however, we should do much more. For starters, we can (and should) authenticate a device. Endpoint/device authentication should be familiar to you because you already use it whenever you establish an HTTPS connection to a web server. When a client requests a secure connection, the server responds with its certificate, which contains its public key issued by a trusted certificate authority (CA). The client then encrypts a secret session key using the server’s public key, so only the server can decrypt it and then establish a symmetrically encrypted secure link. It is possible to configure a NAC device to authenticate itself in a similar manner, but also require the client device to do the same. Obviously, we’d need a certificate (and matching private key) installed on the client device for this to work. An alternative approach to using certificates is to use a hardware Trusted Platform Module (TPM) if the endpoint has one. We discussed TPMs in Chapter 9.

PART IV

PBX systems are also vulnerable to brute force and other types of attacks, in which phreakers use scripts and dictionaries to guess the necessary credentials to gain access to the system. In some cases, phreakers have listened to and changed people’s voice messages. So, for example, when people call Bob and reach his voicemail, they might hear not his usual boring message but a new message that is screaming obscenities and insults.

Unfortunately, many security people do not even think about a PBX when they are assessing a network’s vulnerabilities and security level. This is because telecommunication devices have historically been managed by service providers and/or by someone on the staff who understands telephony. The network administrator is usually not the person who manages the PBX, so the PBX system commonly does not even get assessed. The PBX is just a type of switch and it is directly connected to the organization’s infrastructure; thus, it is a doorway for the bad guys to exploit and enter. These systems need to be assessed and monitored just like any other network device.

So, what should we do to secure PBX systems? Since many of these systems nowadays ride on IP networks, some of the basic security measures will sound familiar. Start by ensuring you know all accounts on the system and that their passwords are strong. Then, ensure that your PBX is updated regularly and that it sits behind your firewall with the appropriate ACLs in place. Other security measures are more specific to a PBX. For example, consider separating your voice and data traffic through these systems by placing them on different VLANs. If one of the VLANs is penetrated, the other could remain secure. Also, limiting the rate of traffic to IP telephony VLANs can slow down an outside attack.

A common use of NAC is to ensure the endpoint is properly configured prior to it being allowed to connect to the network. For example, it is pretty common to check the version of the OS as well as the signatures for the antimalware software. If either of these is not current, the device may be placed in an untrusted LAN segment from which it can download and install the required updates. Once the device meets the access policy requirements, it is allowed to connect to the protected network.

Network Diagramming

In many cases, you cannot capture a full network in a diagram because of the complexity of most organizations' networks. Sometimes we have a false sense of security when we have a pretty network diagram that we can all look at and be proud of, but let's dig deeper into why this can be deceiving. From what perspective should you look at a network? Many possibilities exist:

- A cabling diagram that shows how everything is physically connected (coaxial, UTP, fiber) and a wireless portion that describes the WLAN structure
- A network diagram that illustrates the network in infrastructure layers of access, aggregation, edge, and core
- A diagram that illustrates how the various networking routing takes place (VLANs, MPLS connections, OSPF, IGRP, and BGP links)
- A diagram that shows how different data flows take place (FTP, IPSec, HTTP, TLS, L2TP, PPP, Ethernet, FDDI, ATM, etc.)
- A diagram that separates workstations and the core server types that almost

every network uses (DNS, DHCP, web farm, storage, print, SQL, PKI, mail, domain controllers, RADIUS, etc.)

- A view of a network based upon trust zones, which are enforced by filtering routers, firewalls, and DMZ structures
- A view of a network based upon its IP subnet structure

But what if you look at a network diagram from a Microsoft perspective, which illustrates many of these things but in forest, tree, domain, and OU containers? Then you need to show remote access connections, VPN concentrators, extranets, and the various MAN and WAN connections. How do we illustrate our IP telephony structure? How do we integrate our mobile device administration servers into the diagram? How do we document our new cloud computing infrastructure? How do we show the layers of virtualization within our database? How are redundant lines and fault-tolerance solutions marked? How does this network correlate and interact with our offsite location that carries out parallel processing? And we have not even gotten to our security components (firewalls, IDS, IPS, DLP, antimalware, content filters, etc.). And in the real world,

whatever network diagrams an organization does have are usually out of date because they take a lot of effort to create and maintain.

Application platform
Network Service Control

VOD

MS

IM

Presence

Location
Info

Security
SOC
platform

SIP-AS

Service
platform

NOC

FW
Operation
platform

MGW
PSTN

HSSP-CSCF

I-CSCF

RACS

NASS

Operation

SBC
Core Network

CR
ADM

WDM

Metro
ER

WDM

Metro
Edge

Edge

Optical
access

Internet

CR

Copper
access

ADM

PSTN

ER

Other IP
network
Wireless access

AGW
BS

OLT

BTS

SS
HGW
Enterprise
GW

Outdoors

STB

Enterprise Network

Home Network

The point is that a network is a complex beast that cannot really be captured on one piece of paper. Compare it to a human body. When you go into the doctor’s office, you see posters on the wall. One poster shows the circulatory system, one shows the muscles, one shows bones, another shows organs, and another shows tendons and ligaments; a dentist’s office has a bunch of posters on teeth; if you are at an acupuncture clinic, there will be a poster on acupuncture and reflexology points. And then there is a ton of stuff no one makes posters for—hair follicles, skin, toenails, eyebrows—but these are all part of one system.

Access Network

OLT

OXC
Core

So what does this mean to the security professional? You have to understand a network from many different aspects if you are actually going to secure it. You start by learning all this network stuff in a modular fashion, but you need to quickly understand how it all works together under the covers. You can be a complete genius on how everything works within your current environment but not fully understand that when an employee connects her iPhone to her company laptop that is connected to the corporate network and uses it as a modem, this is an unmonitored WAN connection that can be used as a doorway by an attacker. Security is complex and demanding, so do not ever get too cocky, and always remember that a diagram is just showing a perspective of a network, not the whole network.

Operation of Hardware

Once you have your network designed and implemented, you need to ensure it remains operational. Keep in mind that one of the aspects of security is availability, which can be compromised not only by adversaries but also by power outages, equipment defects, and human error. Remember that all risks, not just the ones that come from human actors, should be addressed by your risk management program. This ensures that you can select cost-effective controls to mitigate those risks. In the sections that follow, we discuss three specific types of controls that protect the availability of your network components. These control types are redundant electrical power, equipment warranties, and support agreements on the operation of our network components.

Electrical Power

Electrical power is essential to operating IT hardware, which, in turn, runs the software that provides IT services to our organizations. We already discussed this topic generally in Chapter 10, but we now return to it in terms of ensuring our critical systems have redundant power. To understand these power requirements, we need to first become familiar with three key terms that describe electricity:

- Voltage Measured in volts, this tells us what the potential electric force between two points in a circuit could be. You can think of volts as the water pressure inside a pipe.
- Current Measured in amps, this is the actual electric flow through the circuit. If you think of volts as the pressure inside a water pipe, you can think of current

as the diameter of a valve attached to it; the bigger the valve, the faster the water can come out.

- Power There are two ways to measure power. We measure electrical power in watts, which we calculate by multiplying voltage by amperage. In other words, if your server rack is running on 240 volts and drawing 9 amps of current, it is consuming 2,160 watts or 2.16 kilowatts (kW). Another related term is kilowatthours (kWh), which is simply the amount of power consumed during a 1-hour period. So, that same server rack would draw 2.16 kWh in one hour, or 51.84 kWh in a day (assuming the current draw is constant).

What we actually care about is whether or not we have enough electric power to run our equipment. There are two ways to measure power: apparent and real. You can think of apparent power as the maximum amount of electricity that could get through a circuit in a perfect case. This value is simply the product of the voltage and current of a system, and is measured in volt-amps (VA). So, if you have a 120-volt computer that can draw up to 3 amps, its apparent power would be 360 VA.

Typically, however, the real power drawn by a system is less than its apparent power. This is because of certain complexities of alternating current (AC) circuits that we won’t dive into. Suffice it to say that AC, which is the type of current produced from virtually every power outlet, is constantly changing. This variance means that the real power drawn by a server will be some value, measured in watts, equal to or (much more frequently) lower than the apparent power. Thankfully, we don’t have to calculate this value; most computing equipment is labeled with the real power value in watts (or kilowatts).

Why should you care? Because real power (watts) determines the actual power you purchase from the utility company, the size of any backup generators you might need, and the heat generated by the equipment. Apparent power (VA) is used for sizing wiring and circuit breakers, so the former don’t melt (or worse, catch fire) and the latter don’t trip. The ratio of real power to apparent power is called the work factor, which can never be greater than one (since the denominator is the ideal apparent power).

With all this discussion under our belts, we can now (finally) talk about redundant power, which typically comes in the two forms presented in Chapter 10: uninterruptable power supplies (UPSs) and backup power sources. Suppose one of your organization’s facilities has (what will eventually turn out to be) an extended power outage lasting multiple days. Your business continuity plan (BCP; covered in Chapter 2) should identify your mission-critical systems and determine how long they can remain unavailable before your organizational losses are intolerable. You would have addressed this in your facility planning (Chapter 10) by implementing a backup power source. Typically, there is a period between the start of a power outage and when the backup power source comes online and is usable. This is the amount of time during which your UPS systems will have to keep your critical assets running.

To determine how much power you need from your backup power source, you simply add up the power consumption of your critical assets (in kW), keeping in mind the need for cooling and any other supporting systems. Let’s say this comes out to be 6 kW and your backup source is a generator. Since generators run optimally at 75 percent to 80 percent of their rated loads, you’d need an 8-kW generator or greater. You also want to factor in room for growth, which should be no less than 25 percent, so you end up getting a 10-kW generator. Now, suppose you also get an automatic transfer switch that will start the generator and transfer the load from critical circuits 60 seconds after the outage is detected. How much UPS capacity do you need?

Whereas the real power consumption that you used to estimate your generator needs probably came from actual readings of how many kilowatts your critical servers drew, your apparent power needs are probably higher because they capture peaks in consumption that are averaged out by real power readings. Remember that apparent power is at least as much as (and usually higher than) your real power. If you look at your equipment’s technical descriptions (or labels) you may see a value measured in volt-ampere (VA or kVA), and all you have to do is add up these values and get a UPS that is rated for that value. Alternatively, a good rule of thumb is to multiply your real power by 1.4 kWA (kilowatt-ampere) per kVA. The resulting number of kVAs should give you sufficient UPS capacity until the generator kicks in.

Equipment Warranty

Of course, many other things can go wrong with our assets with or without power outages. Equipment failures due to manufacturing defects are, unfortunately, unavoidable in the long run. The good news is that most original equipment manufacturers (OEMs) provide a three-year warranty against such defects. However, you have to read the fine print and may want to upgrade the protections. Suppose that you have a critical server fail and you can only afford to have it down for 24 hours. The standard warranty includes next-day replacement delivery, so you’re covered, right? Well, not if you factor in the time it’ll take you to reconfigure the server, load up all the data it needs, and put it back into production. Since it is difficult and expensive to get better than next-day support, you may want to build in the cost of having a spare server (or two) in addition to the warranty to ensure you meet your maximum tolerable downtime (MTD).

Most OEMs also offer extended warranties at an additional cost. Depending on your hardware refresh cycle (i.e., how long you will operate equipment before replacing it with new systems), you may want to add one, two, or three more years to the base three-year warranty. This is usually cheaper to purchase when you buy the hardware, as opposed to purchasing it a year or two later. Seven to eight years after the initial purchase, however, warranty offers tend to expire, as the hardware will be too old for the OEM to continue supporting it.

Support Agreements

Even if your hardware doesn’t fail, it could become unavailable (or insufficiently available) with regard to supporting your organizational processes. For example, suppose that a server slows down to the point where your users sit around for several seconds (or even minutes) waiting for a response. This would not only be frustrating but also lead to a loss of productivity that could add up to significant financial losses. If you have a large and well-staffed organization, you probably have a resident expert who can troubleshoot the server and get it back to peak performance. If you don’t have such an expert, what do you do?

Many organizations use support agreements with third parties to deal with issues that are outside the expertise of their IT or security staff. Sometimes this support can be provided by the OEM as part of the purchase of a system. Other times, organizations hire a managed services provider (MSP), who not only responds when things go badly but continuously monitors the systems’ performance to detect and fix problems as early as possible. Most MSPs charge flat monthly fees per device and include 24/7 remote monitoring, maintenance, and, when needed, onsite support. Think of this as an insurance policy against loss of availability.

Endpoint Security

Securing Endpoints

Endpoint security really boils down to a handful of best practices. Sure, you should thoroughly analyze risks to your endpoints and implement cost-effective controls as part of a broader risk management program, but if you don’t take care of the basic “tackling and blocking,” then whatever else you do won’t really make much of a difference. Here’s a short list to get you started:

- Know what every single endpoint is, where it is, who uses it, and what it should (and should not) be doing.
- Strictly enforce least privilege (i.e., no regular users with local admin rights).
- Keep everything updated (ideally, do this automatically).
- Use endpoint protection and response (EDR) solutions.
- Back up everything (ideally in a way that is difficult for an attacker to compromise).
- Export endpoint logs to a security information and event management (SIEM) solution.

An endpoint is any computing device that communicates through a network and whose principal function is not to mediate communications for other devices on that network. In other words, if a device is connected to a network but is not part of the routing, relaying, or managing of traffic on that network, then it is an endpoint. That definition leaves out all of the network devices we’ve discussed in the preceding sections. Endpoints include devices that you would expect, such as desktops, laptops, servers, smartphones, and tablets. However, they also include other devices that many of us don’t normally think of, such as point of sale (POS) terminals at retail stores, building automation devices like smart thermostats and other Internet of Things (IoT) devices, and sensors and actuators in industrial control systems (ICS).

One of the greatest challenges in dealing with (and securing) endpoints is knowing they are present in the first place. While it would be extremely unusual (not to say frightening) for your routers and switches to unexpectedly drop in and out of the network, this is what mobile devices do by their very nature. The intermittent connectivity of mobile devices is also a problem when it comes to ensuring that they are properly configured and running the correct firmware, OS, and software versions. An approach to dealing with some of these issues is to use network access control (NAC), as discussed earlier in this chapter.

But mobile devices are not the only problem. Our increasing reliance on embedded systems like IoT and ICS devices poses additional challenges. For starters, embedded devices normally have lesser computing capabilities than other endpoints. You usually can’t install security software on them, which means that many organizations simply create security perimeters or bubbles around them and hope for the best. Just to make things even more interesting, IoT and ICS devices oftentimes control physical processes like heating, ventilation, and air conditioning (HVAC) that can have effects on the health and safety of the people in our organizations.

Content Distribution Networks

So far, our discussion of networking has sort of implied that there is a (singular) web server, a (singular) database server, and so on. While this simplifies our discussion of network foundations, protocols, and services, we all know that this is a very rare scenario in all but the smallest networks. Instead, we tend to implement multiples of each service, whether to segment systems, provide redundancy, or both. We may have a couple of web servers connected by a load balancer and interfacing with multiple backend database servers. This sort of redundant deployment can improve performance, but all clients still have to reach the same physical location regardless of where in the world they may be. Wouldn’t it be nice if users in Europe did not have to ride transatlantic cables or satellite links to reach a server in the United States and instead could use one closer to them?

A content distribution network (CDN) consists of multiple servers distributed across a large region, each of which provides content that is optimized for users closest to it. This optimization can come in many flavors. For example, if you were a large streaming video distribution entity like Netflix, you would want to keep your movie files from having to traverse multiple links between routers, since each hop would incur a delay and potential loss of packets (which could cause jitter in the video). Reducing the number of network hops for your video packets would also usually mean having a server geographically closer to the other node, offering you the opportunity to tailor the content for users in that part of the world. Building on our video example, you could keep movies dubbed in Chinese on servers that are in or closer to Asia and those dubbed in French closer to Europe. So when we talk about optimizing content, we can mean many things.

Another benefit of using CDNs is that they make your Internet presence more resistant to distributed denial-of-service (DDoS) attacks. These attacks rely on having a large number of computers flood a server until it becomes unresponsive to legitimate requests. If an attacker can muster a DDoS attack that can send a million packets per second (admittedly fairly small by today’s standards) and aim it at a single server, then it could very well be effective. However, if the attacker tries that against a server that is part of a CDN, the clients will simply start sending their requests to other servers in the network. If the attacker then directs a portion of his attack stream to each server on the CDN in hopes of bringing the whole thing down, the attack will obviously be diffused and would likely require many times more packets. Unsurprisingly, using CDNs is how many organizations protect themselves against DDoS attacks.

Chapter Review

The physical components that make up our networks are foundational to our information systems. Without these cables and switches and routers, nothing else would work.

This may seem obvious, but when was the last time you inspected any of them to ensure that they are secure, in good condition, properly configured, and well supported by appropriate third parties? The two classes of threat actors with which we should concern ourselves in this context are attackers and nature. We take care of the first by applying the principles of secure design we’ve discussed throughout the book and, particularly, by physically securing these cables and devices as discussed in Chapter 10. As far as natural threats, we need to be on the lookout for the wear and tear that is natural over time and that can exacerbate small product defects that may not have been apparent during our initial inspections of new products. This boils down to having qualified staff that is augmented, as necessary, by third parties that provide warranty and support services.

Quick Review

- Analog signals represent data as continuously changing wave values, while digital signals encode data in discrete voltage values.
- Digital signals are more reliable than analog signals over a long distance and provide a clear-cut and efficient signaling method because the voltage is either on (1) or not on (0), compared to interpreting the waves of an analog signal.
- Synchronous communications require a timing component but ensure reliability and higher speeds; asynchronous communications require no timing component and are simpler to implement.
- A baseband technology uses the entire communication channel for its transmission, whereas a broadband technology divides the communication channel into individual and independent subchannels so that different types of data can be transmitted simultaneously.
- Coaxial cable has a copper core that is surrounded by a shielding layer and grounding wire, which makes it more resistant to electromagnetic interference (EMI), provides a higher bandwidth, and supports the use of longer cable lengths.
- With twisted-pair cable, the twisting of the wires, the type of insulation used, the quality of the conductive material, and the shielding of the wire determine the

rate at which data can be transmitted.

- Fiber-optic cabling carries data as light waves, is expensive, can transmit data at high speeds, is difficult to tap into, and is resistant to EMI and RFI. If security is extremely important, fiber-optic cabling should be used.
- Because it uses glass, fiber-optic cabling has higher transmission speeds that allow signals to travel over longer distances.
- Depending on the material used, network cables may be susceptible to noise, attenuation, and crosstalk.
- Line noise refers to random fluctuations in electrical-magnetic impulses that are carried along a physical medium.
- Attenuation is the loss of signal strength as it travels.
- Crosstalk is a phenomenon that occurs when electrical signals of one wire spill over to the signals of another wire.

- Bandwidth is the amount of information that can theoretically be transmitted over a link within a second.
- Data throughput is the actual amount of data that can actually be carried over a real link.
- A repeater provides the simplest type of connectivity because it only repeats electrical signals between cable segments, which enables it to extend a network.
- A bridge is a LAN device used to connect LAN segments (or VLAN segments) and thus extends the range of a LAN.
- A transparent bridge starts to learn about the network's environment as soon as it is powered on and continues to learn as the network changes by examining frames and making entries in its forwarding tables.
- Spanning Tree Protocol (STP) ensures that forwarded frames do not circle networks forever, provides redundant paths in case a bridge goes down, assigns unique identifiers to each bridge, assigns priority values to these bridges, and calculates path costs.
- The Shortest Path Bridging (SPB) protocol is defined in IEEE 802.1aq and is more efficient and scalable than STP; it is used in newer bridges.
- Switches are multiport bridges that typically have additional management features.
- Routers are layer 3, or network layer, devices that are used to connect similar or different networks.
- Routers link two or more network segments, where each segment can function as an independent network. A router works at the network layer, works with IP addresses, and has more network knowledge than bridges, switches, or repeaters.
- Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions.
- A Private Branch Exchange (PBX) is a private telephone switch that is located on

an organization’s property and performs some of the same switching tasks that take place at the telephone company’s central office.

- Proxy servers act as an intermediary between the clients that want access to certain services and the servers that provide those services.
- Network access control (NAC) is any set of policies and controls that restrict access to our networks.
- An endpoint is any computing device that communicates through a network and whose principal function is not to mediate communications for other devices on that network.
- A content distribution network (CDN) consists of multiple servers distributed across a large region, each of which provides content that is optimized for users closest to it.

⮉Chapter 14: Network Components

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. Which of the following is true of asynchronous transmission signals?
A. Used for high-speed, high-volume transmissions
B. Robust error checking
C. Used for irregular transmission patterns
D. More complex, costly implementation

2. Which of the following technologies divides a communication channel into individual and independent subchannels?
A. Baseband
B. Broadband
D. Crosstalk

3. What type of cabling would you use if you needed inexpensive networking in an environment prone to electromagnetic interference?
A. Fiber-optic
B. Unshielded twisted pair (UTP)
C. Plenum
D. Coaxial

4. Which of the following issues would be likeliest to cause problems in a cable tray where large numbers of cables run in parallel and close proximity?
A. Thermal noise
B. Line noise
C. Crosstalk
D. Attenuation

5. What problem is inevitable as the length of a cable run increases?
A. Thermal noise
B. Line noise
C. Crosstalk
D. Attenuation

C. Circuit-switched

6. What is the term for the maximum amount of data that actually traverses a given network link?
A. Latency
B. Bandwidth
C. Throughput
D. Maximum transmission unit (MTU)

7. Which protocol ensures that frames being forwarded by switches do not circle networks forever?
A. Open Shortest Path First (OSPF)
B. Border Gateway Protocol (BGP)
C. Intermediate System-to-Intermediate System (IS-IS)
D. Spanning Tree Protocol (STP)

8. Which standard specifically addresses issues in network access control?
A. IEEE 802.1Q
B. IEEE 802.1aq
C. IEEE 802.AE
D. IEEE 802.1X

9. Which of the following would not be considered an endpoint?
A. Point of sale (POS) terminal
B. Industrial control system (ICS)
C. Internet of Things (IoT) device
D. Multiprotocol Label Switching (MPLS) system

10. All of the following are good reasons to implement a content distribution network except for which one?
A. Reduced latency
B. Reduced total cost of ownership (TCO)
C. Protection against distributed denial-of-service (DDoS) attacks
D. Tailoring content to users around the world

Answers

1. C. Asynchronous communications are typically used when data transfers happen at lower volumes and with unpredictable intervals. All other answers describe synchronous signaling, which is best suited for regular, high-volume traffic.

2. B. A broadband technology divides the communication channel into individual and independent subchannels so that different types of data can be transmitted simultaneously. A baseband technology, on the other hand, uses the entire communication channel for its transmission.

3. D. Coaxial cable has a copper core that is surrounded by a shielding layer and grounding wire, which makes it more resistant to electromagnetic interference (EMI). It is significantly cheaper than fiber-optic cable, which is the other EMI-resistant answer listed, while still allowing higher bandwidths.

4. C. Crosstalk is a phenomenon that occurs when electrical signals of one wire spill over to the signals of another wire. The more cables you have in close proximity, the worse this issue can be unless you use shielded cables.

5. D. Attenuation is the loss of signal strength as it travels. Regardless of which type of cabling is used, attenuation is inevitable given a long enough distance, which is why repeaters were invented.

6. C. Data throughput is the actual amount of data that can be carried over a real link. Bandwidth, on the other hand, is the amount of information that can theoretically be transmitted over a link within a second.

8. D. The 802.1X protocol allows devices to connect in a very limited manner (i.e., only to the network authenticator) until the device and/or user can be authenticated. The other standards listed all pertain to layer 2 bridging and security.

9. D. An endpoint is any computing device that communicates through a network and whose principal function is not to mediate communications for other devices on that network. MPLS functionality is built into networking devices to help them move packets between endpoints more efficiently.

10. B. A content distribution network (CDN) consists of multiple servers distributed across a large region, each of which provides content that is optimized for users closest to it. This improves latency and localization. The very distributed nature of the CDN also provides DDoS protections. It all comes at significant costs and increases the complexity of deploying systems and content, which may require additional organizational resources apart from the service itself.

7. D. Spanning Tree Protocol (STP) ensures that forwarded frames do not circle networks forever, provides redundant paths in case a bridge goes down, assigns unique identifiers to each bridge, assigns priority values to these bridges, and calculates path costs. The other answers are all routing (layer 3) protocols.

🡅This page intentionally left blank

🡅15

CHAPTER

Secure Communications Channels

This chapter presents the following:

- Voice communications
- Multimedia collaboration
- Remote access
- Data communications
- Virtualized networks
- Third-party connectivity

Mr. Watson—come here—I want to see you.
—Alexander Graham Bell

Up to this point, we've treated all the data as if it were equal. While it is true that a packet is a packet regardless of its contents, there are a number of common cases in which the purpose of a communication matters a lot. If we're downloading a file from a server, we normally don't care (or even know about) the variation in delay times between consecutive packets. This variation, known as packet jitter, could mean that some packets follow each other closely (no variance) while others take a lot longer (or shorter) time to arrive.

While packet jitter is largely inconsequential to our file download, it could be very problematic for voice, video, or interactive collaboration communications channels.

Implementing secure communications channels has always been important to most organizations. However, the sudden shift to remote working brought on by COVID-19 has made the security of these channels critical due to the convergence of increased demand by legitimate users and increased targeting by threat actors. In this chapter, we look at some of the most prevalent communications channels that ride on our networks. These include voice, multimedia collaboration, remote access, and third-party channels.

Let's start with the one we're most accustomed to: voice communications.

Voice Communications

Voice communications have come a long way since Alexander Graham Bell made that first call in 1876. It is estimated that 95 percent of the global population has access to telephone service, with most of those being cellular systems. What ties global voice networks together is a collection of technologies, some of which we’ve discussed before (e.g., ATM in Chapter 11 and LTE in Chapter 12), and some to which we now turn our attention.

Public Switched Telephone Network

The traditional telephone system is based on a circuit-switched, voice-centric network called the public switched telephone network (PSTN). The PSTN uses circuit switching instead of packet switching. When a phone call is made, the call is placed at the PSTN interface, which is the user’s telephone. This telephone is connected to the telephone company’s local loop via electric wires, optical fibers, or a radio channel. Once the signals for this phone call reach the telephone company’s central office (the end of the local loop), they are part of the telephone company’s circuit-switching world. A connection is made between the source and the destination, and as long as the call is in session, the data flows through the same switches.

When a phone call is made, the phone numbers have to be translated, the connection has to be set up, signaling has to be controlled, and the session has to be torn down. This takes place through the Signaling System 7 (SS7) protocol. Figure 15-1 illustrates how calls are made in the PSTN using SS7. Suppose Meeta calls Carlos. Meeta’s phone is directly connected to a signal switching point (SSP) belonging to the telephone company (telco) that provides her service. Her telco’s SSP finds the SSP of the telco providing Carlos’s phone service and they negotiate the call setup. The call itself is routed over

Nancy
Signal
transfer
point

Service
control
point
Signal
transfer
point
Signal
switching
point

PSTN
Signal
transfer
point
Signal
switching
point

Carlos

Meeta

Figure 15-1

Base station

Major components of a public switched telephone network

the two signal transfer points (STPs) that interconnect the two SSPs. STPs perform a similar function in a circuit-switched network as routers do in an IP network. If Meeta wanted to call (or conference in) Nancy on her mobile phone, her SSP could query a service control point (SCP), which controls advanced features such as finding mobile subscribers' SSPs and enabling conference calls involving multiple networks.

NOTE PSTNs are being replaced with IP telephony. In the UK, for example, the service provider BT announced that it will switch off its PSTN in 2025.

DSL

Telecommunications
central office

Subscriber's home office

Voice
switch

Computer

PSTN
DSL modem
Internet
DSL
splitter

Telephone

Other

subscribers

Figure 15-2

DSL network

DSLAM

IP router

It turns out that PSTN local loops (i.e., the telephone wires that go into our homes and offices) are able to support much more bandwidth than the small amount required for voice communications. In the 1980s, telcos figured out that they could transmit digital data at frequencies above those used for voice calls without interference. This was the birth of digital subscriber line (DSL), which is a high-speed communications technology that simultaneously transmits analog voice and digital data between a home or business and the service provider’s central office.

Figure 15-2 shows a typical DSL network. In the subscriber’s home, a DSL modem creates a LAN to which computers and wireless access points can be connected. This modem, in turn, is connected to a DSL splitter if the home also has analog phone service. A bunch of DSL subscribers in the same neighborhood are then connected to a DSL access multiplexer (DSLAM) in the central office, where analog signals are sent to a voice switch (and on to the PSTN) and digital signals are routed out to the Internet.

The tricky part is that the maximum distance between the DSLAM and the DSL splitter

in the subscriber’s home cannot be greater than about 2.5 miles unless you put extenders in place to boost the signal strength.

DSL offers two broad types of services. With symmetric services, traffic flows at the same speed upstream and downstream (to and from the Internet or destination). With asymmetric services, the downstream speed is much higher than the upstream speed. The vast majority of DSL lines in use today are asymmetric, because most users usually download much more data from the Internet than they upload. The following are some of the most common types of DSL service:

- Asymmetric DSL (ADSL) These lines allocate more bandwidth for downstream data than for upstream. The technology has gone through multiple upgrades, with ADSL2+ (ITU standard G.992.5) being the latest and fastest. It has data rates of up to 24 Mbps downstream and 1.4 Mbps upstream, but can only support distances of about a mile from the central office. ADSL is generally used by residential users.
- Very high-data-rate DSL (VDSL) VDSL is basically ADSL at much higher data rates (up to 300 Mbps downstream and 100 Mbps upstream). It is capable of supporting high-bandwidth applications such as HDTV, telephone services (Voice over IP), and general Internet access over a single connection.
- G.fast Since the biggest challenge with DSL is the length of the subscriber loop, why not run fiber-optic cable from the central office to a distribution point near the home and then finish the last few hundred feet using the copper wires that are already in place? This is what G.fast (ITU standards G.9700 and G.9701) does. It can deliver data rates of up to 1 Gbps.

Dial-up Connections

Dial-up modems using PSTN were the dominant form of remote access in the early days of the Internet. Antiquated as they may seem, some organizations still have modems enabled, sometimes without the network staff being aware of them. For example, we once discovered that the facilities manager at a large school district installed a dial-up modem so he could control the HVAC systems remotely during inclement weather. Therefore, it is important to search for these systems and ensure no unauthorized modems are attached and operational.

If you find yourself using modems, some of the security measures that you should put in place for dial-up connections include

- Disable and remove nonessential modems.
- Configure the remote access server to call back the initiating phone number to ensure it is valid and authorized.
- Consolidate all modems into one location and manage them centrally, if possible.
- Whenever possible, implement use of two-factor authentication, VPNs, and NAC for remote access connections.

NOTE Despite being in wide use, DSL is an obsolescent technology. Major telecommunications companies around the world have announced plans to phase out DSL by 2025.

ISDN

ISDN Examined

ISDN breaks the telephone line into different channels and transmits data in a digital form rather than the old analog form. Three ISDN implementations are in use:

- Basic Rate Interface (BRI) ISDN This implementation operates over existing copper lines at the local loop and provides digital voice and data channels. It uses two B channels (at 64 Kbps each) to support user data or voice and one D channel (at 16 Kbps) for signaling, with a combined bandwidth of 144 Kbps. BRI ISDN is generally used for home and small office subscribers.
- Primary Rate Interface (PRI) ISDN This implementation has up to 23 B channels and 1 D channel, at 64 Kbps per channel. The total bandwidth is equivalent to a T1, which is 1.544 Mbps. This would be more suitable for an organization that requires a higher amount of bandwidth compared to BRI ISDN.
- Broadband ISDN (BISDN) This implementation can handle many different types of services simultaneously and is mainly used within telecommunications carrier backbones. When BISDN is used within a backbone, ATM is commonly employed to encapsulate data at the data link layer into cells, which travel over a SONET network.

Integrated Services Digital Network (ISDN) is another technology that leverages legacy telephone lines to enable data, voice, and signaling traffic to travel over a medium in a digital manner previously used only for analog voice transmission. ISDN uses the same wires and transmission medium used by analog dial-up technologies, but it works in a digital fashion. If a computer uses a modem to communicate with an ISP, the modem converts the data from digital to analog to be transmitted over the phone line. If that same computer was configured to use ISDN and had the necessary equipment, it would not need to convert the data from digital to analog, but would keep it in a digital form. This, of course, means the receiving end would also require the necessary equipment to receive and interpret this type of communication properly. Communicating in a purely digital form provides higher bit rates that can be sent more economically.

ISDN is a set of telecommunications services that can be used over public and private telecommunications networks. It provides a digital, point-to-point, circuit-switched medium and establishes a circuit between the two communicating devices. An ISDN connection can be used for anything a modem can be used for, but it provides more functionality and higher bandwidth. This digital service can provide bandwidth on an as-needed basis and can be used for LAN-to-LAN on-demand connectivity, instead of using an expensive dedicated link.

Analog telecommunication signals use a full channel for communication, but ISDN can break up this channel into multiple channels to move various types of data and provide full-duplex communication and a higher level of control and error handling. ISDN provides two basic services: Basic Rate Interface (BRI) and Primary Rate Interface (PRI).

BRI has two B channels that enable data to be transferred and one D channel that provides for call setup, connection management, error control, caller ID, and more. The bandwidth available with BRI is 144 Kbps, and BRI service is aimed at the small office and home office (SOHO) market. The D channel provides for a quicker call setup and process in making a connection compared to dial-up connections. An ISDN connection may require a setup connection time of only 2 to 5 seconds, whereas a modem may require a timeframe of 45 to 90 seconds. This D channel is an out-of-band communication link between the local loop equipment and the user’s system. It is considered “out-of-band” because the control data is not mixed in with the user communication data. This makes it more difficult for a would-be defrauder to send bogus instructions back to the service provider’s equipment in hopes of causing a denial of service (DoS), obtaining services not paid for, or conducting some other type of destructive behavior.

PRI has 23 B channels and one D channel, and is more commonly used in corporations. The total bandwidth is equivalent to a T1, which is 1.544 Mbps.

ISDN is not usually the primary telecommunications connection for organizations, but it can be used as a backup in case the primary connection goes down. An organization can also choose to implement dial-on-demand routing (DDR), which can work over ISDN. DDR allows an organization to send WAN data over its existing telephone lines and use the PSTN as a temporary type of WAN link. It is usually implemented by organizations that send out only a small amount of WAN traffic and is a much cheaper solution than a real WAN implementation. The connection activates when it is needed and then idles out.

NOTE ISDN has lost popularity over the years and is now a legacy technology that is seldom used. Some organizations still rely on it as a backup for communications.

Cable Modems

The cable television companies have been delivering television services to homes for years, and then they started delivering data transmission services for users who have cable modems and want to connect to the Internet at high speeds. Cable modems provide high-speed access to the Internet through existing cable coaxial and fiber lines. The cable modem provides upstream and downstream conversions.

Coaxial and fiber cables are used to deliver hundreds of television stations to users, and one or more of the channels on these lines are dedicated to carrying data. The bandwidth is shared between users in a local area; therefore, it will not always stay at a static rate. So, for example, if Mike attempts to download a program from the Internet at 5:30 ▪.▪., he most likely will have a much slower connection than if he had attempted it at 10:00 ▪.▪., because many people come home from work and hit the Internet at the same time. As more people access the Internet within his local area, Mike's Internet access performance drops.

Most cable providers comply with Data-Over-Cable Service Interface Specifications (DOCSIS), which is an international telecommunications standard that allows for the addition of high-speed data transfer to an existing cable TV (CATV) system. DOCSIS includes MAC layer security services in its Baseline Privacy Interface/Security (BPI/SEC) specifications. This protects individual user traffic by encrypting the data as it travels over the provider's infrastructure.

IP Telephony

EXAM TIP Applications that are time sensitive, such as voice and video signals, need to work over an isochronous network. An isochronous network contains the necessary protocols and devices that guarantee regular packet interarrival times.

Internet Protocol (IP) telephony is an umbrella term that describes carrying telephone traffic over IP networks. So, if we have all these high-speed digital telecommunications services and the ability to transmit Voice over IP (VoIP) networks, do we even need analog telephones anymore? The answer is a resounding no. PSTN is being replaced by data-centric, packet-oriented networks that can support voice, data, and video.

The new IP telephony networks use more efficient and secure switches, protocols, and communication links compared to PSTN but must still coexist (for now) with this older network. This means that VoIP is still going through a tricky transition stage that enables the old systems and infrastructures to communicate with the new systems until the old systems are dead and gone.

This technology gets around some of the barriers present in the PSTN today. The PSTN interface devices (telephones) have limited embedded functions and logic, and the PSTN environment as a whole is inflexible in that new services cannot be easily added. In VoIP, the interface to the network can be a computer, server, PBX, or anything else that runs a telephone application. This provides more flexibility when it comes to adding new services and provides a lot more control and intelligence to the interfacing devices. The traditional PSTN has basically dumb interfaces (telephones without much functionality), and the telecommunication infrastructure has to provide all the functionality. In VoIP, the interfaces are the “smart ones” and the network just moves data from one point to the next.

Because VoIP is a packet-oriented switching technology, the arrival times of different packets may not be regular. You may get a bunch of packets close to each other and then have random delays until the next ones arrive. This irregularity in arrival rates is referred to as jitter, which can cause loss of synchronicity in the conversation. It typically means the packets holding the other person’s voice message got queued somewhere within the network or took a different route. VoIP includes protocols to help smooth out these issues and provide a more continuous telephone call experience.

Four main components are normally used for VoIP: an IP telephony device, a callprocessing manager, a voicemail system, and a voice gateway. The IP telephony device is just a phone that has the necessary software that allows it to work as a network device. Traditional phone systems require a “smart network” and a “dumb phone.” In VoIP, the phone must be “smart” by having the necessary software to take analog signals, digitize them, break them into packets, and create the necessary headers and trailers for the packets to find their destination. The voicemail system is a storage place for messages and provides user directory lookups and call-forwarding functionality. A voice gateway carries out packet routing and provides access to legacy voice systems and backup calling processes.

When a user makes a call, his VoIP phone sends a message to the call-processing manager to indicate a call needs to be set up. When the person at the call destination takes her phone off the hook, this notifies the call-processing manager that the call has been accepted. The call-processing manager notifies both the sending and receiving phones that the channel is active, and voice data is sent back and forth over a traditional data network line.

Moving voice data through packets is more involved than moving regular data through packets. This is because voice (and video) data must be sent as a steady stream, whereas other types of traffic are more tolerant to burstiness and jitter. A delay in data transmission is not noticed as much as is a delay in voice transmission. VoIP systems have advanced features to provide voice data transmission with increased bandwidth, while reducing variability in delay, round-trip delay, and packet loss issues. These features are covered by two relevant standards: H.323 and the Session Initiation Protocol (SIP).

NOTE A media gateway is the translation unit between disparate telecommunications networks. VoIP media gateways perform the conversion between TDM voice and VoIP, for example.

VoIP vs. IP Telephony

The terms “IP telephony” and “Voice over IP” are used interchangeably, but there is a distinction:

- The term “VoIP” is widely used to refer to the actual services offered: caller ID, QoS, voicemail, and so on.
- IP telephony is an umbrella term for all real-time applications over IP, including voice over instant messaging (IM) and video conferencing.

So, “IP telephony” means that telephone and telecommunications activities are taking place over an IP network instead of the traditional PSTN. “Voice over IP” means voice data is being moved over an IP network instead of the traditional PSTN. They are basically the same thing, but VoIP focuses more on the telephone call services.

H.323

The ITU-T H.323 recommendation is a standard that deals with audio and video calls over packet-based networks. H.323 defines four types of components: terminals, gateways, multipoint control units, and gatekeepers. The terminals can be dedicated VoIP telephone sets, videoconferencing appliances, or software systems running on a traditional computer. Gateways interface between H.323 and non-H.323 networks, providing any necessary protocol translation. These gateways are needed, for instance, when using the PSTN to connect H.323 systems. Multipoint control units (MCUs) allow three or more terminals to be conferenced together and are sometimes referred to as conference call bridges. Finally, the H.323 gatekeeper is the central component of the system in that it provides call control services for all registered terminals.

Session Initiation Protocol

PART IV

An alternative standard for voice and video calls is the Session Initiation Protocol (SIP), which can be used to set up and break down the call sessions, just as SS7 does for PSTN calls. SIP is an application layer protocol that can work over TCP or UDP. It provides the foundation to allow the phone-line features that SS7 provides, such as causing a phone to ring, dialing a phone number, generating busy signals, and so on. SIP is used in applications such as video conferencing, multimedia, instant messaging, and online gaming.

SIP consists of two major components: the User Agent Client (UAC) and User Agent Server (UAS). The UAC is the application that creates the SIP requests for initiating a communication session. UACs are generally messaging tools and soft-phone applications that are used to place VoIP calls. The UAS is the SIP server, which is responsible for handling all routing and signaling involved in VoIP calls.

SIP relies on a three-way-handshake process to initiate a session. To illustrate how a SIP-based call kicks off, let’s look at an example of two people, Bill and John, trying to communicate using their VoIP phones. Bill’s system starts by sending an INVITE message to John’s system. Since Bill’s system is unaware of John’s location, the INVITE message is sent to the SIP server, which looks up John’s address in the SIP registrar server. Once the location of John’s system has been determined, the INVITE message is forwarded to his system. During this entire process, the server keeps the caller (Bill) updated by sending his system a Trying response, indicating the process is underway.

Once the INVITE message reaches John’s system, it starts ringing. While John’s system rings and waits for John to respond, it sends a Ringing response to Bill’s system, notifying Bill that the INVITE has been received and John’s system is waiting for John to accept the call. As soon as John answers the call, an OK packet is sent to Bill’s system (through the server). Bill’s system now issues an ACK packet to begin call setup. It is important to note here that SIP itself is not used to stream the conversation because it’s just a signaling protocol. The actual voice stream is carried on media protocols such as the Realtime Transport Protocol (RTP). RTP provides a standardized packet format for delivering audio and video over IP networks. Once Bill and John are done communicating, a BYE message is sent from the system terminating the call. The other system responds with an OK, acknowledging the session has ended. This handshake is illustrated in Figure 15-3.

Figure 15-3
SIP handshake

User
Agent B

User
Agent A

1. INVITE

2. Trying

3. Ringing
Ringing
User B answers
4. OK
5. ACK
6. RTP voice call
User A hangs up
7. BYE
8. OK

The SIP architecture consists of three different types of servers, which play an integral role in the entire communication process of the VoIP system:

- Proxy server Is used to relay packets within a network between the UACs