connect to
other routers within the same AS and run interior routing protocols. So, in reality, the
Internet is just a network made up of ASs and routing protocols.

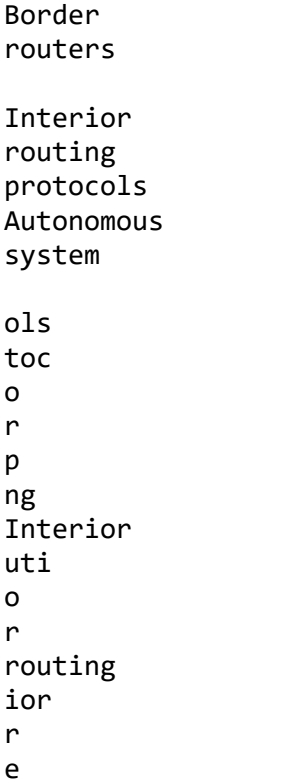


Figure 11-30 Autonomous systems

NOTE Routing protocols are used by routers to identify a path between the source and destination systems.

Dynamic vs. Static
Routing protocols can be dynamic or static. A dynamic routing protocol can discover
routes and build a routing table. Routers use these tables to make decisions on the best
route for the packets they receive. A dynamic routing protocol can change the entries
in the routing table based on changes that take place to the different routes. When a
router that is using a dynamic routing protocol finds out that a route has gone down or
is congested, it sends an update message to the other routers around it. The

other routers
use this information to update their routing table, with the goal of providing efficient
routing functionality. A static routing protocol requires the administrator to manually
configure the router’s routing table. If a link goes down or there is network congestion,
the routers cannot tune themselves to use better routes.

NOTE Route flapping refers to the constant changes in the availability of routes. Also, if a router does not receive an update that a link has gone down, the router will continue to forward packets to that route, which is referred to as a black hole.

Distance-Vector vs. Link-State

Interior Routing Protocols
Interior routing protocols (also known as Interior Gateway Protocols) route traffic within
the same AS. Just like the process for flying from one airport to another is different if you
travel domestically or internationally, routing protocols are designed differently depending on which side of the AS boundary they operate. De facto and proprietary interior
protocols are being used today. The following are just a few of them:

• Routing Information Protocol RIP is a standard that outlines how routers exchange routing table data and is considered a distance-vector protocol, which means it calculates the shortest distance between the source and destination. It is considered a legacy protocol because of its slow performance and lack of functionality. It should only be used in small networks. RIP version 1 has no authentication, and RIP version 2 sends passwords in cleartext or hashed with MD5. RIPng is the third generation of this venerable protocol. It is very similar
to version 2 but is designed for IPv6 routing.
• Open Shortest Path First OSPF uses link-state algorithms to send out routing table information. The use of these algorithms allows for smaller, more frequent routing table updates to take place. This provides a more stable network than RIP,
but requires more memory and CPU resources to support this extra processing. OSPF allows for a hierarchical routing network that has a backbone link connecting all subnets together. OSPF has replaced RIP in many networks today. Authentication can take place with cleartext passwords or hashed passwords, or

Two main types of routing protocols are used: distance-vector and link-state routing.
Distance-vector routing protocols make their routing decisions based on the distance (or
number of hops) and a vector (a direction). The protocol takes these variables

and uses
them with an algorithm to determine the best route for a packet. Link-state routing protocols build a more accurate routing table because they build a topology database of the
network. These protocols look at more variables than just the number of hops between
two destinations. They use packet size, link speed, delay, network load, and reliability as
the variables in their algorithms to determine the best routes for packets to take.
So, a distance-vector routing protocol only looks at the number of hops between two
destinations and considers each hop to be equal. A link-state routing protocol sees more
pieces to the puzzle than just the number of hops, but understands the status of each of
those hops and makes decisions based on these factors also. As you will see in the next
section, RIP is an example of a distance-vector routing protocol, and OSPF is an example
of a link-state routing protocol. OSPF is preferred and is used in large networks. RIP is
still around but should only be used in smaller networks.

you can choose to configure no authentication on the routers using this protocol.
The latest OSPF is version 3. Though it was designed to support IPv6, it also supports IPv4. Among the most important improvements is that OSPFv3 uses IPSec for authentication.
• Interior Gateway Routing Protocol IGRP is a distance-vector routing protocol that was developed by, and is proprietary to, Cisco Systems. Whereas RIP uses one criterion to find the best path between the source and destination, IGRP uses five criteria to make a “best route” decision. A network administrator can set weights on these different metrics so that the protocol works best in that
specific environment.
• Enhanced Interior Gateway Routing Protocol EIGRP is a Cisco-proprietary and advanced distance-vector routing protocol. It allows for faster router table updates than its predecessor IGRP and minimizes routing instability, which can occur after topology changes. Routers exchange messages that contain information about bandwidth, delay, load, reliability, and MTU of the path to each destination
as known by the advertising router. The latest version is 4.
• Virtual Router Redundancy Protocol VRRP is used in networks that require high availability where routers as points of failure cannot be tolerated.
It is designed to increase the availability of the default gateway by advertising
a “virtual router” as a default gateway. Two physical routers (primary and secondary) are mapped to one virtual router. If one of the physical routers fails,

the other router takes over the workload.
• Intermediate System to Intermediate System IS-IS is a link-state protocol that allows each router to independently build a database of a network's topology. Similar to the OSPF protocol, it computes the best path for traffic to travel. It is a classless and hierarchical routing protocol that is vendor neutral. Unlike other protocols (e.g., RIP and OSPF), IS-IS does not use IP addresses. Instead, it uses ISO addresses, which means that the protocol didn't have to be redesigned to support IPv6.
NOTE Although most routing protocols have authentication functionality, many routers do not have this functionality enabled.

Exterior Routing Protocols
The exterior routing protocols used by routers connecting different ASs are generically referred to as exterior gateway protocols (EGPs). The Border Gateway Protocol (BGP) enables routers on different ASs to share routing information to ensure effective and efficient routing between the different AS networks. BGP is commonly used by Internet service providers to route data from one location to the next on the Internet.
NOTE There is an exterior routing protocol called Exterior Gateway Protocol, but it has been widely replaced by BGP, and now the term "exterior gateway protocol" and the acronym EGP are used to refer generically to a type of protocol rather than to specify the outdated protocol.

BGP uses a combination of link-state and distance-vector routing algorithms. It creates a network topology by using its link-state functionality and transmits updates on a periodic basis instead of continuously, which is how distance-vector protocols work.
Network administrators can apply weights to the different variables used by link-state routing protocols when determining the best routes. These configurations are collectively called the routing policy.

Routing Protocol Attacks
Several types of attacks can take place on routers through their routing protocols. A majority of the attacks have the goal of misdirecting traffic through the use of spoofed ICMP messages. An attacker can masquerade as another router and submit routing table information to the victim router. After the victim router integrates this new information, it may be sending traffic to the wrong subnets or computers, or even to a nonexistent address (black hole). These attacks are successful mainly when routing protocol authentication is not enabled. When authentication is not required, a router can

accept routing
updates without knowing whether or not the sender is a legitimate router. An attacker
could divert a company’s traffic to reveal confidential information or to just disrupt
traffic, which would be considered a DoS attack.

Web technologies and their uses have exploded with functionality, capability, and popularity. Organizations set up internal websites for centralized business information such
as employee phone numbers, policies, events, news, and operations instructions. Many
organizations have also implemented web-based terminals that enable employees to perform their daily tasks, access centralized databases, make transactions, collaborate on
projects, access global calendars, use videoconferencing tools and whiteboard applications, and obtain often-used technical or marketing data.
Web-based clients are different from workstations that log into a network and have
their own desktop. Web-based clients limit a user’s ability to access the computer’s system
files, resources, and hard drive space; access backend systems; and perform other tasks.
The web-based client can be configured to provide a GUI with only the buttons, fields,
and pages necessary for the users to perform tasks. This gives all users a standard universal
interface with similar capabilities.
When an organization uses web-based technologies that are only available inside its
networks, it is using an intranet, a “private” network. The organization has web servers and
client machines using web browsers, and it uses the TCP/IP protocol suite. The web pages
are written in HTML or XML (eXtensible Markup Language) and are accessed via HTTP.
Using web-based technologies has many pluses. They have been around for quite some time, they are easy to implement, no major interoperability issues occur, and with
just the click of a link, a user can be taken to the location of the requested resource. Webbased technologies are not platform dependent, meaning all websites and pages may be
maintained on various platforms and different flavors of client workstations can access
them—they only need a web browser.

An extranet extends outside the bounds of the organization’s network to enable

two
or more organizations to share common information and resources. Business partners
commonly set up extranets to accommodate business-to-business communication. An extranet enables business partners to work on projects together; share marketing
information; communicate and work collaboratively on issues; post orders; and share
catalogs, pricing structures, and information on upcoming events. Trading partners
often use electronic data interchange (EDI), which provides structure and organization to
electronic documents, orders, invoices, purchase orders, and a data flow. EDI has evolved
into web-based technologies to provide easy access and easier methods of communication.
For many organizations, an extranet can create a weakness or hole in their security if
the extranet is not implemented and maintained properly. Properly configured firewalls
need to be in place to control who can use the extranet communication channels. Extranets used to be based mainly on dedicated transmission lines, which are more
difficult for attackers to infiltrate, but today many extranets are set up over the Internet,
which requires properly configured VPNs and security policies.

Metropolitan Area Networks
A metropolitan area network (MAN) is usually a backbone that connects LANs to each
other and LANs to WANs, the Internet, and telecommunications and cable networks. A
majority of today's MANs are Synchronous Optical Networks (SONETs) or FDDI rings and
Metro Ethernet provided by the telecommunications service providers. (FDDI technology was discussed earlier in the chapter.) The SONET and FDDI rings cover a large area,
and businesses can connect to the rings via T1, fractional T1, and T3 lines. Figure 11-31
illustrates two companies connected via a SONET ring and the devices usually necessary
to make this type of communication possible. This is a simplified example of a MAN. In
reality, several businesses are usually connected to one ring.
SONET is a standard for telecommunications transmissions over fiber-optic cables.
Carriers and telephone companies have deployed SONET networks for North America, and
if they follow the SONET standards properly, these various networks can intercommunicate

Business 1

Business 2

Local
loop

Local
loop
Sonet

LAN

Routers CSU/DSU

Switch

Switch

CSU/DSU Routers

LAN

Telco central office

Figure 11-31 A MAN covers a large area and enables businesses to connect to each other, to the
Internet, or to other WAN connections.

539
Nearby
city

Nearby
city

Regional
SONET ring

DSL

DSL
POP

TI
POP
TI

Long-haul
network

Local
SONET
ring

Figure 11-32 Smaller SONET rings connect to larger SONET rings to construct individual MANs.

with little difficulty. SONET is self-healing, meaning that if a break in the line occurs, it can use a backup redundant ring to ensure transmission continues. All SONET lines and rings are fully redundant. The redundant line waits in the wings in case anything happens to the primary ring.

SONET networks can transmit voice, video, and data over optical networks. Slowerspeed SONET networks often feed into larger, faster SONET networks, as shown in Figure 11-32. This enables businesses in different cities and regions to communicate.

MANs can be made up of wireless infrastructures, optical fiber, or Ethernet connections. Ethernet has evolved from just being a LAN technology to being used in MAN environments. Due to its prevalent use within organizations' networks, Ethernet is easily extended and interfaced into MAN networks. A service provider commonly uses layer 2 and 3 switches to connect optical fibers, which can be constructed in a ring, star, or partial mesh topology.

Metro Ethernet

Ethernet has been around for many years and is embedded in almost every LAN. Ethernet LANs can connect to the previously mentioned MAN technologies, or they can be extended to cover a metropolitan area, which is called Metro Ethernet.

Customer

Aggregation

Core

Aggregation

Customer

Government
GigE
10 GigE
Enterprise

Layer 2/3
switches

Content hosting

GigE
10 GigE

VCG 1
VCG 1
VCG 1

Standardsbased,
intelligent
packet-tocircuit
mapping

Layer 2/3

Standardsbased,
intelligent
packet-tocircuit
mapping

Government

Enterprise

Content hosting

Figure 11-33 MAN architecture

Ethernet on the MAN can be used as pure Ethernet or Ethernet integrated with other networking technologies, as in Multiprotocol Label Switching (MPLS). Pure Ethernet is less expensive but less reliable and scalable. MPLS-based deployments are more

expensive
but highly reliable and scalable, and are typically used by large service providers.
MAN architectures are commonly built upon three layers: access, aggregation/distribution, and core. The access layer provides services directly to the customers,
typically at data rates of 10 Gbps or less. The aggregation layer provides routing for
customer data, most of which passes on to the core layer, which operates at data rates of
100 Gbps or higher as illustrated in Figure 11-33.
Access devices exist at a customer's premises and connect the customer's equipment to
the service provider's network. The service provider's distribution network aggregates the
traffic and sends it to the provider's core network. From there, the traffic is moved to the
next aggregation network that is closest to the destination. This is similar to how smaller
highways are connected to larger interstates with on and off ramps that allow people to
quickly travel from one location to a different one.

Wide Area Networks
LAN technologies provide communication capabilities over a small geographic area,
whereas wide area network (WAN) technologies are used when communication needs to travel over a larger geographical area. LAN technologies encompass how a computer
puts its data onto a network cable, the rules and protocols of how that data is formatted
and transmitted, how errors are handled, and how the destination computer picks up
this data from the cable. When a computer on one network needs to communicate with
a network on the other side of the country or in a different country altogether, WAN
technologies kick in.
The network must have some avenue to other networks, which is most likely a router
that communicates with the organization's service provider's switches or telephone
company facilities. Just as several types of technologies lie within the LAN arena, several
technologies lie within the WAN arena. The following sections discuss the dedicated links
that oftentimes connect LANs to WANs and the various technologies used in WANs.

Dedicated Links
A dedicated link is also called a leased line or point-to-point link. It is one

single link that
is pre-established for the purposes of WAN communications between two destinations.
It is dedicated, meaning only the destination points can communicate with each other.
This link is not shared by any other entities at any time. This was the main way organizations communicated in the past, because there were not as many choices available as
there are today. Establishing a dedicated link is a good idea for two locations that will
communicate often and require fast transmission and a specific bandwidth, but it is
expensive compared to other possible technologies that enable several organizations to
share the same bandwidth and also share the cost. This does not mean that dedicated
lines are not in use; they definitely are used, but many other options are now available,
including X.25, frame relay, and ATM technologies.

T-Carriers

Channel slots
(8 bits each)

… 22 23 24 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 1 2 3 …
Previous
frame

TI frame

Next
frame

Figure 11-34 Multiplexing puts several phone calls, or data transmissions, on the same wire.

PART IV

T-carriers are dedicated lines that can carry voice and data information over trunk lines.
They were developed by AT&T and were initially implemented in the early 1960s to support pulse-code modulation (PCM) voice transmission. This was first used to digitize
the voice over a dedicated, point-to-point, high-capacity connection line. The most commonly used T-carriers are T1 lines and T3 lines. Both are digital circuits that multiplex
several individual channels into a higher-speed channel.
These lines can have multiplex functionality through time-division multiplexing (TDM). What does this multiplexing stuff really mean? It means that each channel gets
to use the path only during a specific time slot. It’s like having a time-share property

on the beach; each co-owner gets to use it, but only one can do so at a time and can only remain for a fixed number of days. Consider a T1 line, which can multiplex up to 24 channels. If a company has a PBX connected to a T1 line, which in turn connects to the telephone company switching office, 24 calls can be chopped up and placed on the T1 line and transferred to the switching office. If this company did not use a T1 line, it would need 24 individual twisted pairs of wire to handle this many calls.

As shown in Figure 11-34, data is input into these 24 channels and transmitted. Each channel gets to insert up to 8 bits into its established time slot. Twenty-four of these 8-bit time slots make up a T1 frame. That does not sound like much information, but 8,000 frames are built per second. Because this happens so quickly, the receiving end

Table 11-7
A T-Carrier
Hierarchy
Summary Chart

Carrier	# of T1s	# of Channels	Speed (Mbps)
Fractional	1/24	1	0.064
T1	1	24	1.544
T2			

4

96

6.312

T3

28

672

44.736

T4

168

4,032

274.760

does not notice a delay and does not know it is sharing its connection and bandwidth
with up to 23 other devices.
Originally, T1 and T3 lines were used by the carrier companies, but they have been
replaced mainly with optical lines. Now T1 and T3 lines feed data into these powerful
and super-fast optical lines. The T1 and T3 lines are leased to organizations and ISPs
that need high-capacity transmission capability. Sometimes, T1 channels are split up
between organizations that do not need the full bandwidth of 1.544 Mbps. These are
called fractional T lines. The different carrier lines and their corresponding characteristics
are listed in Table 11-7.
As mentioned earlier, dedicated lines have their drawbacks. They are expensive and
inflexible. If a company moves to another location, a T1 line cannot easily follow it. A
dedicated line is expensive because organizations have to pay for a dedicated connection
with a lot of bandwidth even when they do not use the bandwidth. Not many organizations
require this level of bandwidth 24 hours a day. Instead, they may have data to send out
here and there, but not continuously.
The cost of a dedicated line is determined by the distance to the destination. A T1 line
run from one building to another building 2 miles away is much cheaper than a T1 line
that covers 50 miles or a full state.

E-Carriers
E-carriers are similar to T-carrier telecommunication connections, where a single physical
wire pair can be used to carry many simultaneous voice conversations by time-division
multiplexing. Within this technology 30 channels interleave 8 bits of data in a frame.
While the T-carrier and E-carrier technologies are similar, they are not interoperable.
E-carriers are used by European countries. The E-carrier channels and associated rates
are shown in Table 11-8.
The most commonly used channels are E1 and E3 and fractional E-carrier lines.
Table 11-8
E-Carrier Characteristics

Signal	Rate
E0	64 Kbps
E1	2.048 Mbps
E2	8.448 Mbps
E3	34.368 Mbps
E4	139.264 Mbps
E5	565.148 Mbps

Table 11-9
OC Transmission Rates

Optical Carrier

Speed

OC-1

51.84 Mbps

OC-3

155.52 Mbps

OC-9

466.56 Mbps

OC-12

622.08 Mbps

OC-19

933.12 Mbps

OC-24

1.244 Gbps

OC-36

1.866 Gbps

OC-48

2.488 Gbps

OC-96

4.977 Gbps

OC-192

9.953 Gbps

OC-768

40 Gbps

OC-3072

160 Gbps

Optical Carrier

WAN Technologies

Several varieties of WAN technologies are available to organizations today. The information that an organization evaluates to decide which is the most appropriate WAN
technology for it usually includes functionality, bandwidth demands, service level agreements, required equipment, cost, and what is available from service providers. The following sections go over some of the WAN technologies available today.

CSU/DSU
A channel service unit/data service unit (CSU/DSU) is required when digital equipment
will be used to connect a LAN to a WAN. This connection can take place with T1 and
T3 lines, as shown in Figure 11-35. A CSU/DSU is necessary because the signals and
frames can vary between the LAN equipment and the WAN equipment used by service providers.

PART IV

High-speed fiber-optic connections are measured in optical carrier (OC) transmission
rates. The transmission rates are defined by rate of the bit stream of the digital signal
and are designated by an integer value of the multiple of the basic unit of rate. They are
generically referred to as OCx, where x represents a multiplier of the basic OC-1 transmission rate, which is 51.84 Mbps. The carrier levels and speeds are shown in Table 11-9.
Small and medium-sized organizations that require high-speed Internet connectivity
may use OC-3 or OC-12 connections. Service providers that require much larger amounts of bandwidth may use one or more OC-48 connections. OC-192 and greater connections are commonly used for the Internet backbone, which connects the largest
networks in the world together.

More Multiplexing
Here are some other types of multiplexing functionalities you should be aware of:
Statistical time-division multiplexing (STDM):

• Transmits several types of data simultaneously across a single transmission cable or line (such as a T1 or T3 line).
• Analyzes statistics related to the typical workload of each input device (printer, fax, computer) and determines in real time how much time each device should be allocated for data transmission.
Frequency-division multiplexing (FDM):

• An available wireless spectrum is used to move data.
• Available frequency band is divided into narrow frequency bands and used

to have multiple parallel channels for data transfer.
Amplitude
modulation
with carrier f1

Amplitude
modulation
with carrier f2

Filter

Amplitude
demodulation

Filter

Amplitude
demodulation
Frequency-division multiplexing (FDM)

Wave-division multiplexing (WDM):

- Used in fiber-optic communication.
- Multiplexes a number of optical carrier signals onto a single optical fiber.

545
Florida

Washington

Switch

Router

CSU/DSU

Switch

WAN

Router

CSU/DSU

Figure 11-35 A CSU/DSU is required for digital equipment to communicate with telecommunications lines.

Switching
Dedicated links have one single path to traverse; thus, there is no complexity when it
comes to determining how to get packets to different destinations. Only two points of

reference are needed when a packet leaves one network and heads toward the other. It gets much more complicated when thousands of networks are connected to each other, which is often when switching comes into play.

Two main types of switching can be used: circuit switching and packet switching. Circuit switching sets up a virtual connection that acts like a dedicated link between two systems. ISDN and telephone calls are examples of circuit switching, which is shown in the lower half of Figure 11-36.

When the source system makes a connection with the destination system, they set up a communication channel. If the two systems are local to each other, fewer devices need to be involved with setting up this channel. The farther the two systems are from each other, the more the devices are required to be involved with setting up the channel and connecting the two systems.

The DSU device converts digital signals from routers, switches, and multiplexers into signals that can be transmitted over the service provider's digital lines. The DSU device ensures that the voltage levels are correct and that information is not lost during the conversion. The CSU connects the network directly to the service provider's line. The CSU/DSU is not always a separate device and can be part of a networking device. The CSU/DSU provides a digital interface for data terminal equipment (DTE), such as terminals, multiplexers, or routers, and an interface to the data circuit–terminating equipment (DCE) device, such as a carrier's switch. The CSU/DSU basically works as a translator and, at times, as a line conditioner.

Figure 11-36 Circuit switching provides one road for a communication path, whereas packet switching provides many different possible roads.

Packet switching

Circuit switches

Circuit switching

An example of how a circuit-switching system works is daily telephone use. When one
person calls another, the same type of dedicated virtual communication link is set up.
Once the connection is made, the devices supporting that communication channel do
not dynamically move the call through different devices, which is what takes place in a
packet-switching environment. The channel remains configured at the original devices
until the call (connection) is done and torn down.
Packet switching, on the other hand, does not set up a dedicated virtual link, and
packets from one connection can pass through a number of different individual devices
(see the top of Figure 11-36), instead of all of them following one another through the
same devices. Some examples of packet-switching technologies are the Internet, X.25,
and frame relay. The infrastructure that supports these methods is made up of routers
and switches of different types. They provide multiple paths to the same destinations,
which offers a high degree of redundancy.
In a packet-switching network, the data is broken up into packets containing frame
check sequence (FCS) numbers. These packets go through different devices, and their
paths can be dynamically altered by a router or switch that determines a better route for
a specific packet to take. Once the packets are received at the destination computer, all
the packets are reassembled according to their FCS numbers and processed.
Because the path a packet will take in a packet-switching environment is not set in
stone, there could be variable delays when compared to a circuit-switching technology.
This is okay, because packet-switching networks usually carry data rather than voice.
Because voice connections clearly detect these types of delays, in many situations a
circuit-switching network is more appropriate for voice connections. Voice calls usually
provide a steady stream of information, whereas a data connection is “burstier” in nature.
When you talk on the phone, the conversation keeps a certain rhythm. You and your
friend do not talk extremely fast and then take a few minutes in between conversations to

stop talking and create a void with complete silence. However, this is usually how a data
connection works. A lot of data is sent from one end to the other at one time, and then
dead time occurs until it is time to send more data.

Circuit Switching vs. Packet Switching
The following points provide a concise summary of the differences between circuitand packet-switching technologies:
Circuit switching:

- Connection-oriented virtual links.
- Traffic travels in a predictable and constant manner.
- Fixed delays.
- Usually carries voice-oriented data.

Packet switching:

Frame Relay
For a long time, many organizations used dedicated links to communicate with other
organizations. Company A had a pipeline to company B that provided a certain bandwidth 24 hours a day and was not used by any other entities. This was great because
only the two companies could use the line, so a certain level of bandwidth was always
available, but it was expensive, and most organizations did not use the full bandwidth
each and every hour the link was available. Thus, organizations spent a lot of money for
a service they did not use all the time. Later, to avoid this unnecessary cost, organizations
turned to using frame relay instead of dedicated lines.
EXAM TIP Frame relay is an obsolescent technology. It is still in limited use, however, and you should be familiar with it for the CISSP exam.

Frame relay is a WAN technology that operates at the data link layer. It is a WAN
solution that uses packet-switching technology to let multiple organizations and networks
share the same WAN medium, devices, and bandwidth. Whereas direct point-to-point links have a cost based on the distance between the endpoints, the frame relay cost is
based on the amount of bandwidth used. Because several organizations and networks use
the same medium and devices (routers and switches), the cost can be greatly reduced per
organization compared to dedicated links.

- Packets can use many different dynamic paths to get to the same

destination.
• Traffic is usually bursty in nature.
• Variable delays.
• Usually carries data-oriented data.

If a company knows it will usually require a certain amount of bandwidth each day,
it can pay a certain fee to make sure this amount of bandwidth is always available to it.
If another company knows it will not have a high bandwidth requirement, it can pay a
lower fee that does not guarantee the higher bandwidth allocation. This second company
will have the higher bandwidth available to it anyway—at least until that link gets busy,
and then the bandwidth level will decrease. (Organizations that pay more to ensure that a
higher level of bandwidth will always be available pay a committed information rate, or CIR.)
Two main types of equipment are used in frame relay connections: DTE and DCE,
both of which were previously introduced in the discussion of CSU/DSU. The DTE is
usually a customer-owned device, such as a router or switch, that provides connectivity
between the organization's own network and the frame relay network. DCE is the service
provider's device, or telecommunications company's device, that does the actual data
transmission and switching in the frame relay cloud. So the DTE is an organization's
ramp onto the frame relay network, and the DCE devices actually do the work within
the frame relay cloud.
The frame relay cloud is the collection of DCE devices that provides switching and
data communications functionality. Several service providers offer this type of service, and
some providers use other providers' equipment—it can all get confusing because a packet
can take so many different routes. This collection is called a cloud to differentiate it from
other types of networks and because when a packet hits this cloud, users do not usually
know the route their frames will take. The frames will be sent either through permanent
or switched virtual circuits that are defined within the DCE or through carrier switches.
NOTE The term cloud is used in several technologies: Internet cloud, ATM cloud, frame relay cloud, cloud computing, and so on. The cloud is like a black box—we know our data goes in and we know it comes out, but we do not normally care about all the complex things that are taking place

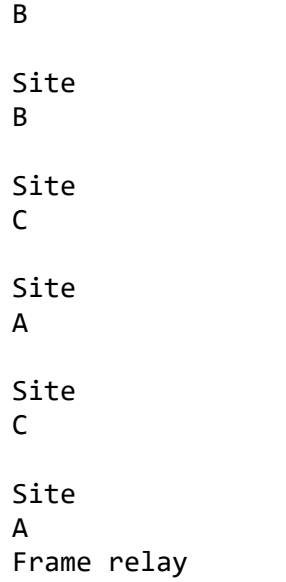
internally.

Frame relay is an any-to-any service that is shared by many users. As stated earlier, this is beneficial because the costs are much lower than those of dedicated leased lines. Because frame relay is shared, if one subscriber is not using its bandwidth, it is available for others to use. On the other hand, when traffic levels increase, the available bandwidth decreases. This is why subscribers who want to ensure a certain bandwidth is always available to them pay a higher CIR.

Figure 11-37 shows five sites being connected via dedicated lines versus five sites connected through the frame relay cloud. The first solution requires many dedicated lines that are expensive and not flexible. The second solution is cheaper and provides organizations much more flexibility.

Virtual Circuits

Frame relay (and X.25) forwards frames across virtual circuits. These circuits can be either permanent, meaning they are programmed in advance, or switched, meaning the circuit is quickly built when it is needed and torn down when it is no longer needed.



Site
E

Site
D

Private network method

Site
E

Site
D

Frame relay method
(public method)

Figure 11-37 A private network connection requires several expensive dedicated links. Frame
relay enables users to share a public network.

X.25
X.25 is an older WAN protocol that defines how devices and networks establish and
maintain connections. Like frame relay, X.25 is a switching technology that uses carrier
switches to provide connectivity for many different networks. It also provides
an any-toany connection, meaning many users use the same service simultaneously. Subscribers are
charged based on the amount of bandwidth they use, unlike dedicated links, for which
a flat fee is charged.

PART IV

The permanent virtual circuit (PVC) works like a private line for a customer with an
agreed-upon bandwidth availability. When a customer decides to pay for the CIR, a
PVC is programmed for that customer to ensure it will always receive a certain amount
of bandwidth.
Unlike PVCs, switched virtual circuits (SVCs) require steps similar to a dial-up and
connection procedure. The difference is that a permanent path is set up for PVC frames,
whereas when SVCs are used, a circuit must be built. It is similar to setting up a phone
call over the public network. During the setup procedure, the required bandwidth is
requested, the destination computer is contacted and must accept the call, a path is
determined, and forwarding information is programmed into each switch along the

SVC’s path. SVCs are used for teleconferencing, establishing temporary connections to
remote sites, data replication, and voice calls. Once the connection is no longer needed,
the circuit is torn down and the switches forget it ever existed.
Although a PVC provides a guaranteed level of bandwidth, it does not have the flexibility of an SVC. If a customer wants to use her PVC for a temporary connection,
as mentioned earlier, she must call the carrier and have it set up, which can take hours.

Data is divided into 128 bytes and encapsulated in High-level Data Link Control (HDLC) frames. The frames are then addressed and forwarded across the carrier switches.
Much of this sounds the same as frame relay—and it is—but frame relay is much more
advanced and efficient when compared to X.25, because the X.25 protocol was developed
and released in the 1970s. During this time, many of the devices connected to networks
were dumb terminals and mainframes, the networks did not have built-in functionality
and fault tolerance, and the Internet overall was not as foundationally stable and resistant
to errors as it is today. When these characteristics were not part of the Internet, X.25
was required to compensate for these deficiencies and to provide many layers of error
checking, error correcting, and fault tolerance. This made the protocol fat, which was
required back then, but today it slows down data transmission and provides a lower
performance rate than frame relay or ATM.

ATM
Asynchronous Transfer Mode (ATM) is another switching technology, but instead of being
a packet-switching method, it uses a cell-switching method. ATM is a high-speed networking technology used for LAN, MAN, WAN, and service provider connections. Like
frame relay, it is a connection-oriented switching technology, and creates and uses a fixed
channel. IP is an example of a connectionless technology. Within the TCP/IP protocol
suite, IP is connectionless and TCP is connection oriented. This means IP segments can
be quickly and easily routed and switched without each router or switch in between having to worry about whether the data actually made it to its destination—that is TCP’s
job. TCP works at the source and destination ends to ensure data was properly transmitted, and it resends data that ran into some type of problem and did not

get delivered
properly. When using ATM or frame relay, the devices in between the source and destination have to ensure that data gets to where it needs to go, unlike when a purely connectionless protocol is being used.
Since ATM is a cell-switching technology rather than a packet-switching technology,
data is segmented into fixed-size cells of 53 bytes instead of variable-size packets. This
provides for more efficient and faster use of the communication paths. ATM sets up
virtual circuits, which act like dedicated paths between the source and destination. These
virtual circuits can guarantee bandwidth and QoS. For these reasons, ATM is a good
carrier for voice and video transmission.
ATM technology is used by carriers and service providers, and is the core technology
of the Internet, but ATM technology can also be used for an organization’s private use in
backbones and connections to the service provider’s networks.
Traditionally, organizations used dedicated lines, usually T-carrier lines, to connect to
the public networks. However, organizations have also moved to implementing an ATM
switch on their network, which connects them to the carrier infrastructure. Because
the fee is based on bandwidth used instead of a continual connection, it can be much
cheaper. Some organizations have replaced their Fast Ethernet and FDDI backbones with ATM. When an organization uses ATM as a private backbone, the organization has
ATM switches that take the Ethernet frames, or whatever data link technology is being
used, and frame them into the 53-byte ATM cells.

551
Quality of Service Quality of Service (QoS) is a capability that allows a protocol
to distinguish between different classes of messages and assign priority levels. Some
applications, such as video conferencing, are time sensitive, meaning delays would cause
unacceptable performance of the application. A technology that provides QoS allows an
administrator to assign a priority level to time-sensitive traffic. The protocol then ensures
this type of traffic has a specific or minimum rate of delivery.
QoS allows a service provider to guarantee a level of service to its customers. QoS began
with ATM and then was integrated into other technologies and protocols responsible for
moving data from one place to another. Four different types of ATM QoS services

(listed
next) are available to customers. Each service maps to a specific type of data that will be
transmitted.

ATM was the first protocol to provide true QoS, but as the computing society has increased its desire to send time-sensitive data throughout many types of networks,
developers have integrated QoS into other technologies.
QoS has three basic levels:

• Best-effort service No guarantee of throughput, delay, or delivery. Traffic that has
priority classifications goes before traffic that has been assigned this classification.
Most of the traffic that travels on the Internet has this classification.
• Differentiated service Compared to best-effort service, traffic that is assigned
this classification has more bandwidth, shorter delays, and fewer dropped frames.
• Guaranteed service Ensures specific data throughput at a guaranteed speed.
Time-sensitive traffic (voice and video) is assigned this classification.
Administrators can set the classification priorities (or use a policy manager product)
for the different traffic types, which the protocols and devices then carry out.
Controlling network traffic to allow for the optimization or the guarantee of certain
performance levels is referred to as traffic shaping. Using technologies that have QoS

PART IV

• Constant bit rate (CBR) A connection-oriented channel that provides a consistent data throughput for time-sensitive applications, such as voice and video applications. Customers specify the necessary bandwidth requirement at connection setup.
• Variable bit rate (VBR) A connection-oriented channel best used for delayinsensitive applications because the data throughput flow is uneven. Customers
specify their required peak and sustained rate of data throughput.
• Unspecified bit rate (UBR) A connectionless channel that does not promise a specific data throughput rate. Customers cannot, and do not need to, control their traffic rate.
• Available bit rate (ABR) A connection-oriented channel that allows the bit rate to be adjusted. Customers are given the bandwidth that remains after a guaranteed service rate has been met.

Characteristics

Dedicated line

Dedicated, leased line that connects two locations
Expensive compared to other WAN options
Secure because only two locations are using the same medium

Frame relay

High-performance WAN protocol that uses packet-switching technology, which works over public networks
Shared media among organizations
Uses SVCs and PVCs
Fee based on bandwidth used

X.25

First packet-switching technology developed to work over public networks
Lower speed than frame relay because of its extra overhead
Uses SVCs and PVCs
Basically obsolete and replaced with other WAN protocols

ATM

High-speed bandwidth switching and multiplexing technology that has a low delay
Uses 53-byte fixed-size cells
Very fast because of the low overhead

HSSI

DTE/DCE interface to enable high-speed communication over WAN links

Table 11-10 Characteristics of WAN Technologies

capabilities allows for traffic shaping, which can improve latency and increase bandwidth
for specific traffic types, bandwidth throttling, and rate limiting.

HSSI
High-Speed Serial Interface (HSSI) is an interface used to connect multiplexers and routers to high-speed communications services such as ATM and frame relay. It supports
speeds up to 52 Mbps, as in T3 WAN connections, which are usually integrated with
router and multiplex devices to provide serial interfaces to the WAN. These interfaces
define the electrical and physical interfaces to be used by DTE/DCE devices; thus, HSSI
works at the physical layer.

WAN Technology Summary
We have covered several WAN technologies in the previous sections. Table 11-10 provides

a snapshot of the important characteristics of each.

Chapter Review
Before we can delve into communication and network security, we must first understand
how networks are put together from the ground up. In this chapter, we started with a
high-level overview of the OSI reference model because it will be the framework within
which we will build the rest of our discussion of network security. You really need to
become comfortable mapping technologies and protocols to the OSI reference model
both for the CISSP exam and for your daily work.

We next took a look at the various technologies that allow us to build networks from
the ground up. There are three types of LANs that you need to remember for the exam:
Ethernet, Token Ring, and FDDI. Recall that LANs are limited in geographical scope but
can be linked together using technologies like dedicated links, frame relay, SONET, and
ATM to form MANs and WANs. Once you extend past the local area (and oftentimes
even within it), you'll need routers to break up broadcast domains and link together the
pieces of your MAN or WAN.

Quick Review

• A protocol is a set of rules that dictates how computers communicate over networks.
• The application layer, layer 7, has services and protocols required by the user's
applications for networking functionality.
• The presentation layer, layer 6, formats data into a standardized format and deals
with the syntax of the data, not the meaning.
• The session layer, layer 5, sets up, maintains, and breaks down the dialog (session) between two applications. It controls the dialog organization and synchronization.
• The transport layer, layer 4, provides end-to-end transmissions.
• The network layer, layer 3, provides routing, addressing, and fragmentation of packets. This layer can determine alternative routes to avoid network congestion.
Routers work at the network layer, layer 3.
• The data link layer, layer 2, prepares data for the network medium by framing it.
This is where the different LAN and WAN technologies work.
• The physical layer, layer 1, provides physical connections for transmission

and
performs the electrical encoding of data. This layer transforms bits to electrical
signals.
• A network topology describes the arrangement of computers and devices.
• In a bus topology, a single cable runs the entire length of the network and nodes
attach to it through drop points.
• In a star topology, all nodes connect to a central device such as a switch using a
dedicated link.
• In a mesh topology, all nodes are connected to each other in a non-uniform
manner that provides multiple paths to most or all the nodes on the network.
• A ring topology has a series of devices connected by unidirectional transmission
links that form a closed loop and do not connect to a central system.
• Ethernet uses CSMA/CD, which means all computers compete for the shared
network cable, listen to learn when they can transmit data, and are susceptible to
data collisions.

• Token Ring, IEEE 802.5, is an older LAN implementation that uses a
tokenpassing technology.
• FDDI is a LAN and MAN technology, usually used for backbones, that uses
token-passing technology and has redundant rings in case the primary ring goes
down.
• TCP/IP is a suite of protocols that is the de facto standard for transmitting data
across the Internet. TCP is a reliable, connection-oriented protocol, while IP is
an unreliable, connectionless protocol.
• Data is encapsulated as it travels down the network stack on the source computer,
and the process is reversed on the destination computer. During encapsulation,
each layer adds its own information so the corresponding layer on the destination
computer knows how to process the data.
• Two main protocols at the transport layer are TCP and UDP.
• UDP is a connectionless protocol that does not send or receive acknowledgments
when a datagram is received. It does not ensure data arrives at its destination. It
provides “best-effort” delivery.
• TCP is a connection-oriented protocol that sends and receives acknowledgments.
It ensures data arrives at the destination.
• ARP translates the IP address into a MAC address (physical Ethernet address),
while RARP translates a MAC address into an IP address.
• ICMP works at the network layer and informs hosts, routers, and devices of
network or computer problems. It is the major component of the ping utility.
• DNS resolves hostnames into IP addresses and has distributed databases all over
the Internet to provide name resolution.

• Altering an ARP table so an IP address is mapped to a different MAC address is called ARP poisoning and can redirect traffic to an attacker's computer or an unattended system.
• 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.
• IPv4 uses 32 bits for its addresses, whereas IPv6 uses 128 bits; thus, IPv6 provides more possible addresses with which to work.
• NAT is used when organizations do not want systems to know internal hosts' addresses, and it enables organizations to use private, nonroutable IP addresses.
• Subnetting allows large IP address ranges to be divided into smaller, logical, and easier-to-maintain network segments.
• Dedicated links are usually the most expensive type of WAN connectivity method because the fee is based on the distance between the two destinations rather than on the amount of bandwidth used. T1 and T3 are examples of dedicated links.
• Frame relay and X.25 are packet-switched WAN technologies that use virtual circuits instead of dedicated ones.

• ATM transfers data in fixed cells, is a WAN technology, and transmits data at very high rates. It supports voice, data, and video applications.
• Circuit-switching technologies set up a circuit that will be used during a data transmission session. Packet-switching technologies do not set up circuits—instead, packets can travel along many different routes to arrive at the same destination.
• Three main types of multiplexing are statistical time division, frequency division, and wave division.

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 protocols is considered connection-oriented?
A. IP
C. UDP
D. TCP

2. Which of the following shows the layer sequence as layers 2, 5, 7, 4, and 3?
A. Data link, session, application, transport, and network

B. Data link, transport, application, session, and network
C. Network, session, application, network, and transport
D. Network, transport, application, session, and presentation

3. Metro Ethernet is a MAN protocol that can work in network infrastructures made up of access, aggregation, metro, and core layers. Which of the following best describes these network infrastructure layers?
A. The access layer connects the customer's equipment to a service provider's

aggregation network. Aggregation occurs on a core network. The metro layer is the metropolitan area network. The core connects different metro networks.
B. The access layer connects the customer's equipment to a service provider's core
network. Aggregation occurs on a distribution network at the core. The metro layer is the metropolitan area network.
C. The access layer connects the customer's equipment to a service provider's aggregation network. Aggregation occurs on a distribution network. The metro layer is the metropolitan area network. The core connects different access layers.
D. The access layer connects the customer's equipment to a service provider's aggregation network. Aggregation occurs on a distribution network. The metro layer is the metropolitan area network. The core connects different metro networks.

PART IV

B. ICMP

4. Systems that are built on the OSI model are considered open systems. What does
this mean?
A. They do not have authentication mechanisms configured by default.
B. They have interoperability issues.
C. They are built with internationally accepted protocols and standards so they

can easily communicate with other systems.
D. They are built with international protocols and standards so they can choose what types of systems they will communicate with.
5. Which of the following protocols work in the following layers: application, data
link, network, and transport?
A. FTP, ARP, TCP, and UDP
B. FTP, ICMP, IP, and UDP
C. TFTP, ARP, IP, and UDP
D. TFTP, RARP, IP, and ICMP
6. What takes place at the data link layer?
A. End-to-end connection
B. Dialog control
C. Framing
D. Data syntax
7. What takes place at the session layer?

A. Dialog control
B. Routing
C. Packet sequencing
D. Addressing
8. Which best describes the IP protocol?
A. A connectionless protocol that deals with dialog establishment, maintenance, and destruction
B. A connectionless protocol that deals with the addressing and routing of packets
C. A connection-oriented protocol that deals with the addressing and routing of packets
D. A connection-oriented protocol that deals with sequencing, error detection, and flow control

9. Which of the following is not one of the messages exchanged during the DHCP lease process?
i. Discover
ii. Offer
iii. Request
iv. Acknowledgment
A. All of them are exchanged
B. None of them are exchanged
C. i, ii
D. ii, iii

10. An effective method to shield networks from unauthenticated DHCP clients is through the use of _____ on network switches.
A. DHCP snooping
B. DHCP protection
C. DHCP shielding

Answers
1. D. TCP is the only connection-oriented protocol listed. A connection-oriented protocol provides reliable connectivity and data transmission, while a connectionless
protocol provides unreliable connections and does not promise or ensure data transmission.
2. A. The OSI model is made up of seven layers: application (layer 7), presentation
(layer 6), session (layer 5), transport (layer 4), network (layer 3), data link (layer 2), and physical (layer 1).
3. D. The access layer connects the customer’s equipment to a service provider’s aggregation network. Aggregation occurs on a distribution network. The metro layer is the metropolitan area network. The core connects different metro networks.
4. C. An open system is a system that has been developed based on standardized protocols and interfaces. Following these standards allows the systems to interoperate more effectively with other systems that follow the same standards.
5. C. Different protocols have different functionalities. The OSI model is an attempt to describe conceptually where these different functionalities take place

in a networking stack. The model attempts to draw boxes around reality to help people better understand the stack. Each layer has a specific functionality and has several different protocols that can live at that layer and carry out that specific functionality. These listed protocols work at these associated layers: TFTP (application), ARP (data link), IP (network), and UDP (transport).

PART IV

D. DHCP caching

6. C. The data link layer, in most cases, is the only layer that understands the environment in which the system is working, whether it be Ethernet, Token Ring, wireless, or a connection to a WAN link. This layer adds the necessary headers and trailers to the frame. Other systems on the same type of network using the same technology understand only the specific header and trailer format used in their data link technology.
7. A. The session layer is responsible for controlling how applications communicate, not how computers communicate. Not all applications use protocols that work at the session layer, so this layer is not always used in networking functions. A session layer protocol sets up the connection to the other application logically and controls the dialog going back and forth. Session layer protocols allow applications to keep track of the dialog.
8. B. The IP protocol is connectionless and works at the network layer. It adds source and destination addresses to a packet as it goes through its data encapsulation process. IP can also make routing decisions based on the destination address.
9. B. The four-step DHCP lease process is
1. DHCPDISCOVER message: This message is used to request an IP address lease from a DHCP server.
2. DHCPOFFER message: This message is a response to a DHCPDISCOVER message, and is sent by one or numerous DHCP servers.
3. DHCPREQUEST message: The client sends this message to the initial DHCP server that responded to its request.
4. DHCPACK message: This message is sent by the DHCP server to the DHCP client and is the process whereby the DHCP server assigns the IP address lease to the DHCP client.
10. A. DHCP snooping ensures that DHCP servers can assign IP addresses to only selected systems, identified by their MAC addresses. Also, advance network switches now have the capability to direct clients toward legitimate DHCP servers to get IP addresses and to restrict rogue systems from becoming DHCP servers on the network.

Wireless Networking

This chapter presents the following:

- Wireless networking
- Wireless LAN security
- Cellular networks
- Satellite communications

When wireless is perfectly applied the whole earth will be converted into a huge brain…
—Nikola Tesla

Wireless communications take place much more often than most people realize, and they involve a vast number of technologies working over a multitude of radio frequency ranges. These radio signals occupy frequency bands that may be shared with microwave, satellite, radar, and ham radio use, for example. We use these technologies for satellite communications, cellular phones, metropolitan and local area networking, and even for locking doors and controlling lights in our smart homes, as illustrated in Figure 12-1.

All these interconnected networks rely on different communications techniques, using different radio frequencies and implementing different protocols. This extremely complex ecosystem makes many of our modern conveniences possible, but also introduces significant security challenges.

In this chapter, we'll cover the fundamentals of radio communications techniques and the most important protocols you should be aware of. We then put this theoretical information into real-world contexts as we discuss the opportunities and challenges they represent. Along the way, we'll talk about security threats and how to mitigate them.

Wireless Communications Techniques

Wireless communication involves transmitting information via radio waves that move through free space. These radio signals are typically described in terms of frequency and amplitude. The frequency of a signal indicates how many radio waves travel through a fixed place each second (i.e., how close each radio wave is to the one before it). Frequency is measured in hertz (Hz) and dictates the amount of data that can be carried and how far. The higher the frequency, the more data the signal can carry, but the shorter its range.

Figure 12-1
Various wireless
networks

Satellite network

Wireless wide area
networks
4G/LTE
Wireless metropolitan
area networks

WiMAX
Wi-Fi AP

Wireless local area
networks

Wireless personal area
networks

ZigBee
Bluetooth

The amplitude of a radio signal indicates its power, which in turn dictates how far it can go. Amplitude usually is measured in watts or milliwatts (one-thousandth of a watt), but you may also see it expressed in decibels per milliwatt (dBm or dBmW), which is a measure of comparison to one milliwatt. For example, a wireless access point may allow you to configure the transmit power in increments from 0 dBm (1 mW) up to 23 dBm (200 mW).

In a wired network, each computer and device has its own cable connecting it to the network in some fashion. In wireless technologies, each device must instead share the allotted radio frequency spectrum with all other wireless devices that need to communicate. This spectrum of frequencies is finite in nature, which means it cannot grow if more and more devices need to use it. The same thing happens with Ethernet—all the computers on a segment share the same medium, and only one computer can send data at any given time. Otherwise, a collision can take place. Wired networks using Ethernet employ the CSMA technology (described in Chapter 11). Wireless LAN (WLAN) technology is actually very similar to Ethernet, but it uses CSMA/CA (collision avoidance). The wireless device sends out a broadcast indicating it is going to transmit data. This is received by other devices on the shared medium, which causes them to hold

off on transmitting information. It is all about trying to eliminate or reduce collisions.
A number of techniques have been developed to allow wireless devices to access and
share this limited amount of medium for communication purposes. The goal of each of
these wireless technologies is to split the available frequency into usable portions, since it
is a limited resource, and to allow the devices to share those portions efficiently. The most

popular approach is called spread spectrum, though orthogonal frequency division multiplexing (OFDM) is widely used also. Because spread-spectrum technology is so prevalent,
we'll get into it in a fair amount of detail in the next section.

Spread Spectrum

Frequency Hopping Spread Spectrum
Frequency hopping spread spectrum (FHSS) takes the total amount of spectrum and splits
it into smaller subchannels. The sender and receiver work at one of these subchannels for
a specific amount of time and then move to another subchannel. The sender puts the first
piece of data on one frequency, the second on a different frequency, and so on. The FHSS
algorithm determines the individual frequencies that will be used and in what order, and
this is referred to as the sender and receiver's hop sequence.

Radio frequencies cover a wide range, or spectrum, of frequencies. Some parts of this
spectrum are allocated by national governments or international agreements for specific
purposes. A radio frequency band is a subset of the radio spectrum designated for a specific use. For example, the range of radio frequencies between 1.8 and 29.7 megahertz
(MHz) is almost universally considered the amateur radio band. A well-known frequency
band is frequently labeled using just a single frequency, such as when we refer to the
2.4-GHz band used in many Wi-Fi systems. This band actually corresponds to the range
of frequencies between 2.4 and 2.5 GHz. The challenge is how to dynamically allocate
individual frequencies to specific sets of transmitters and receivers without them stepping
all over each other. This is where spread-spectrum techniques come in handy.

Spread spectrum means that something is distributing individual signals across the allocated frequencies in some fashion. So, when a spread-spectrum technique is used, the sender spreads its data across the frequencies over which it has permission to communicate. This allows for more effective use of the available spectrum, because the sending system can use more than one frequency at a time.

Think of spread spectrum in terms of investments. In conventional radio transmissions, all the data is transmitted on a specific frequency (as in amplitude modulated [AM] radio systems) or on a narrow band of frequencies (as in frequency modulated [FM] radio). This is like investing only in one stock; it is simple and efficient, but may not be ideal in risky environments. The alternative is to diversify your portfolio, which is normally done by investing a bit of your money in each of many stocks across a wide set of industries. This is more complex and inefficient, but can save your bottom line when the stock in one of your selected companies takes a nose-dive. This example is akin to direct sequence spread spectrum (DSSS), which we discuss in an upcoming section.

There is in theory another way to minimize your exposure to volatile markets. Suppose the cost of buying and selling was negligible. You could then invest all your money in a single stock, but only for a brief period of time, sell it as soon as you turn a profit, and then reinvest all your proceeds in another stock. By jumping around the market, your exposure to the problems of any one company are minimized. This approach would be comparable to frequency hopping spread spectrum (FHSS), discussed next. The point is that spread-spectrum communications are used primarily to reduce the effects of adverse conditions such as crowded radio bands, interference, and eavesdropping.

Interference is a large issue in wireless transmissions because it can corrupt signals as they travel. Interference can be caused by other devices working in the same frequency space. The devices' signals step on each other's toes and distort the data being sent. The FHSS approach to this is to hop between different frequencies so that if another device is operating at the same frequency, it will not be drastically affected.

Consider another analogy: Suppose George and Marge work in the same room. They could get into each other's way and affect each other's work. But if they periodically change rooms, the probability of them interfering with each other is reduced.

A hopping approach also makes it much more difficult for eavesdroppers to listen in on and reconstruct the data being transmitted when used in technologies other than WLAN. FHSS has been used extensively in military wireless communications devices because the only way the enemy could intercept and capture the transmission is by knowing the hopping sequence. The receiver has to know the sequence to be able to obtain the data. But in today's WLAN devices, the hopping sequence is known and does not provide any security.

So how does this FHSS stuff work? The sender and receiver hop from one frequency to another based on a predefined hop sequence. Several pairs of senders and receivers can move their data over the same set of frequencies because they are all using different hop sequences. Let's say you and Marge share a hop sequence of 1, 5, 3, 2, 4, and Nicole and Ed have a sequence of 4, 2, 5, 1, 3. Marge sends her first message on frequency 1, and Nicole sends her first message on frequency 4 at the same time. Marge's next piece of data is sent on frequency 5, the next on 3, and so on until each reaches its destination, which is your wireless device. So your device listens on frequency 1 for a half-second, and then listens on frequency 5, and so on, until it receives all of the pieces of data that are on the line on those frequencies at that time. Ed's device is listening to the same frequencies but at different times and in a different order, so his device never receives Marge's message because it is out of sync with his predefined sequence. Without knowing the right code, Ed treats Marge's messages as background noise and does not process them.

Direct Sequence Spread Spectrum

Direct sequence spread spectrum (DSSS) takes a different approach by applying sub-bits to a message. The sub-bits are used by the sending system to generate a different format of the data before the data is transmitted. The receiving end uses these sub-bits to reassemble the signal into the original data format. The sub-bits are called chips, and the sequence of how the sub-bits are applied is referred to as the chipping code. When the sender's data is combined with the chip, the signal appears as random noise to anyone who does not know the chipping sequence. This is why the sequence is

sometimes called a pseudo-noise sequence. Once the sender combines the data with the chipping sequence, the new form of the information is modulated with a radio carrier signal, and it is shifted to the necessary frequency and transmitted. What the heck does that mean? When using wireless transmissions, the data is actually moving over radio signals that work in specific frequencies. Any data to be moved in this fashion must have a carrier signal, and this carrier signal works in its own specific range, which is a frequency.
So you can think of it this way: once the data is combined with the chipping code, it is put into a car (carrier signal), and the car travels down its specific road (frequency) to get to its destination.

Spread Spectrum Types
This technology transmits data by "spreading" it over a broad range of frequencies:

- FHSS moves data by changing frequencies.
- DSSS takes a different approach by applying sub-bits to a message and uses all of the available frequencies at the same time.

FHSS vs. DSSS
FHSS uses only a portion of the total spectrum available at any one time, while the DSSS technology uses all of the available spectrum continuously. DSSS spreads the signals over a wider frequency band, whereas FHSS uses a narrowband carrier that changes frequently across a wide band.
Since DSSS sends data across all frequencies at once, it has higher data rates than FHSS. The first wireless WAN standard, 802.11, used FHSS, but as data requirements increased, DSSS was implemented. By using FHSS, the 802.11 standard can provide a data throughput of only 1 to 2 Mbps. By using DSSS instead, 802.11b provides a data throughput of up to 11 Mbps.

Orthogonal Frequency Division Multiplexing
Besides spread-spectrum techniques, another common approach to trying to move even more data over wireless frequency signals is called orthogonal frequency division multiplexing (OFDM). OFDM is a digital multicarrier modulation scheme that compacts multiple modulated carriers tightly together, reducing the required spectrum. The modulated

signals are orthogonal (perpendicular) and do not interfere with each other. OFDM uses a composite of narrow channel bands to enhance its performance in high-frequency bands. OFDM is officially a multiplexing technology and not a spread-spectrum technology, but is used in a similar manner.

A large number of closely spaced orthogonal subcarrier signals are used, and the data is divided into several parallel data streams or channels, one for each subcarrier. Channel equalization is simplified because OFDM uses many slowly modulated narrowband signals rather than one rapidly modulated wideband signal.

PART IV

The receiver basically reverses the process, first by demodulating the data from the carrier signal (removing it from the car). The receiver must know the correct chipping sequence to change the received data into its original format. This means the sender and receiver must be properly synchronized.

The sub-bits provide error-recovery instructions, just as parity does in RAID technologies. If a signal is corrupted using FHSS, it must be re-sent; but by using DSSS, even if the message is somewhat distorted, the signal can still be regenerated because it can be rebuilt from the chipping code bits. The use of this code allows for prevention of interference, allows for tracking of multiple transmissions, and provides a level of error correction.

OFDM is used for several wideband digital communication types such as digital television, audio broadcasting, DSL broadband Internet access, wireless networks, and 4G/5G mobile communications.

Wireless Networking Fundamentals

The techniques we've covered so far deal with how we create radio links between devices, but how do we build on those links to create networks? Fundamentally, there are three topologies used to build wireless networks: star, mesh, and point to point. The star topology is by far the most prevalent because it is used in both WLANs and cellular networks, both of which have endpoints connecting to a specialized network device that handles layer 2 forwarding and, in some cases, layer 3 routing. The mesh topology is common for low-power devices in close proximity to each other, such as those used in smart

homes, as
well as in devices that span a large area, such as environmental sensors in wildlife refuges.
Finally, point-to-point wireless topologies are common when connecting buildings as
part of a metropolitan area network (MAN).
Before we get into the myriad of wireless protocols that enable the various types of
wireless networks, let’s take a closer look at what makes a typical WLAN work.

WLAN Components
A WLAN uses a transceiver, called an access point (AP), also known as a wireless access
point (WAP), which connects to an Ethernet cable that is the link wireless devices use
to access resources on the wired network, as shown in Figure 12-2. When the AP is connected to the LAN Ethernet by a wired cable, it is the component that connects the wired

Figure 12-2
Access points
allow wireless
devices to
participate in
wired LANs.

Station
Access point

and the wireless worlds. The APs are in fixed locations throughout a network and work
as communication beacons. Let’s say a wireless user has a device with a wireless network
interface card (NIC), which modulates the user’s data onto radio frequency signals that
are accepted and processed by the AP. The signals transmitted from the AP are received by
the wireless NIC and converted into a digital format, which the device can understand.
When APs are used to connect wireless and wired networks, this is referred to as an
infrastructure WLAN, which is used to extend an existing wired network. When there is
just one AP and it is not connected to a wired network, it is considered to be in standalone mode and just acts as a wireless hub. An ad hoc WLAN has no APs; the wireless
devices communicate with each other through their wireless NICs instead of going through
a centralized device.
EXAM TIP
WLANs.

Ad hoc WLANs are inherently less secure than infrastructure

NOTE When wireless devices work in infrastructure mode, the AP and wireless clients form a group referred to as a Basic Service Set (BSS). This group is assigned a name, which is the SSID value.

When WLAN technologies first came out, authentication was simple and largely ineffective against many attackers. As wireless communication increased in use and many deficiencies were identified in these networks, a steady stream of improved approaches were developed and standardized. These covered both performance and security issues.

WLAN Standards
Standards are developed so that many different vendors can create various products that will work together seamlessly. Standards are usually developed on a consensus basis among the different vendors in a specific industry. The IEEE develops standards for a wide range of technologies—wireless being one of them.
The first WLAN standard, 802.11, was developed in 1997 and provided a 1- to 2-Mbps transfer rate. It worked in the 2.4-GHz frequency band, which is one of the free industrial, scientific, and medical (ISM) bands established by the International

PART IV

For a wireless device and AP to communicate, they must be configured to communicate over the same channel. A channel is a certain frequency within a given frequency band.
The AP is configured to transmit over a specific channel, and the wireless device “tunes” itself to be able to communicate over this same frequency.
Any hosts that wish to participate within a particular WLAN must be configured with the proper Service Set ID (SSID). Various hosts can be segmented into different WLANs by using different SSIDs. The reasons to segment a WLAN into portions are the same reasons wired systems are segmented on a network: the users require access to different resources, have different business functions, or have different levels of trust.

Table 12-1
Generational
Wi-Fi

Technology Supported	Wi-Fi Generation
802.11b	Wi-Fi 1
802.11a	Wi-Fi 2
802.11g	Wi-Fi 3
802.11n	Wi-Fi 4
802.11ac	Wi-Fi 5
802.11ax	Wi-Fi 6

Telecommunication Union (ITU). This means that organizations and users in most countries do not need a license to use this range. The 802.11 standard outlines how wireless clients and APs communicate; lays out the specifications of their interfaces; dictates how signal transmission should take place; and describes how authentication, association, and security should be implemented.

Now just because life is unfair, a long list of standards actually fall under the 802.11 main standard. You have probably seen the alphabet soup of 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (and a bunch of others). While the original 802.11 standard created the world of WLANs, the unrelenting pace of progress required changes and improvements over time. To try and make sense of things, the Wi-Fi Alliance created a scheme for numbering the generations of 802.11 protocols in 2018. This was done to help consumers differentiate products based on the most advanced 802.11-based technology supported by a given device. Table 12-1 lists the six generations of Wi-Fi, which we describe in the following sections.

NOTE Wi-Fi generations 1–3 are not formally defined by the Wi-Fi Alliance but

are commonly understood to map to the technologies shown in Table 12-1.

802.11b
This standard was the first extension to the 802.11 WLAN standard. (Although 802.11a
was conceived and approved first, it was not released first because of the technical complexity involved with this proposal.) 802.11b provides a transfer rate of up to 11 Mbps
and works in the 2.4-GHz frequency range. It uses DSSS and is backward-compatible
with 802.11 implementations.

802.11a
This standard uses a different method of modulating data onto the necessary radio carrier signals. Whereas 802.11b uses DSSS, 802.11a uses OFDM and works in the 5-GHz
frequency band. Because of these differences, 802.11a is not backward-compatible with
802.11b or 802.11. Several vendors have developed products that can work with both
802.11a and 802.11b implementations; the devices must be properly configured or be
able to sense the technology already being used and configure themselves appropriately.

As previously discussed, OFDM is a modulation scheme that splits a signal over several
narrowband channels. The channels are then modulated and sent over specific frequencies.
Because the data is divided across these different channels, any interference from the
environment will degrade only a small portion of the signal. This allows for greater
throughput. Like FHSS and DSSS, OFDM is a physical layer specification. It can be used
to transmit high-definition digital audio and video broadcasting as well as WLAN traffic.
This technology offers advantages in two areas: speed and frequency. 802.11a provides
up to 54 Mbps, and it does not work in the already very crowded 2.4-GHz spectrum.
The 2.4-GHz frequency band is referred to as a “dirty” frequency because several devices
already work there—microwaves, cordless phones, baby monitors, and so on. In many
situations, this means that contention for access and use of this frequency can cause loss
of data or inadequate service. But because 802.11a works at a higher frequency, it does
not provide the same range as the 802.11b and 802.11g standards. The maximum speed

for 802.11a is attained at short distances from the AP, up to 25 feet.

802.11g

802.11n (Wi-Fi 4)
This standard is designed to be much faster than 802.11g, with throughput at 100 Mbps,
and it works at the same frequency range as 802.11a (5 GHz). The intent is to maintain
some backward-compatibility with current Wi-Fi standards, while combining a mix of
the current technologies. This standard uses a concept called multiple input, multiple
output (MIMO) to increase the throughput. This requires the use of two receive and two
transmit antennas to broadcast in parallel using a 20-MHz channel.

802.11ac (Wi-Fi 5)
The IEEE 802.11ac WLAN standard is an extension of 802.11n. It also operates on the
5-GHz band, but increases throughput to 1.3 Gbps. 802.11ac is backward compatible
with 802.11a, 802.11b, 802.11g, and 802.11n, but if in compatibility mode it slows
down to the speed of the slower standard. A major improvement is the use of multiuser
MIMO (MU-MIMO) technology, which supports up to four data streams, allowing that
many endpoints to simultaneously use a channel. Another benefit of this newer standard
is its support for beamforming, which is the shaping of radio signals to improve
their performance in specific directions. In simple terms, this means that 802.11ac is better able
to maintain high data rates at longer ranges than its predecessors.

802.11ax (Wi-Fi 6)
Higher data rates are not always the best way to solve problems, and in the race for faster
standards, we took a bunch of shortcuts that made them inefficient. The 802.11ax
standard aims to address efficiency rather than faster speeds. A significant improvement it has

PART IV

The 802.11g standard provides for higher data transfer rates—up to 54 Mbps. This is
basically a speed extension for 802.11b products. If a product meets the specifications of
802.11b, its data transfer rates are up to 11 Mbps, and if a product is based on 802.11g,
that new product can be backward-compatible with older equipment but work at a much
higher transfer rate.

is a new multiuser OFDM technology that replaces the single-user focused technology used in the 802.11a/g/n/ac standards. This means that multiple stations get to use available channels much more efficiently. In addition, the new standard doubles the number of streams supported by MU-MIMO, which means more stations can use it at the same time. These and many other improvements make 802.11ax much faster and better able to handle very crowded environments.

Other Wireless Network Standards

So far, we've focused pretty heavily on radio-based WLANs. There are other wireless network standards that you should know, at least at a superficial level. These include light-based WLANs and radio-based MANs and PANs. We describe the most important of these standards in the following sections.

Li-Fi

Li-Fi is a wireless networking technology that uses light rather than radio waves to transmit and receive data. It is essentially Wi-Fi using lights instead of radios. You can also think of it as fiber-optic communications without the fiber (i.e., over free space). It turns out that light, like radio, is an electromagnetic wave. The difference is that light is on a much higher frequency range and, thus, can carry significantly more information, at least in theory. Imagine if every light fixture in your home or workplace was able to modulate data onto the light it generates, while your computing device (laptop, smartphone, or whatever) could sense it and use its own light source (maybe the flash on your smartphone) to send data back to the light bulb. Because of the frequencies involved, our eyes are not able to perceive the tiny fluctuations in frequency. Besides, Li-Fi can work over infrared light too, which we can't see anyway.

One of the key benefits of Li-Fi (besides speed and ubiquity) is that it is very constrained to a particular space. Each light bulb has a cone of illumination within which it communicates with specific devices. You don't have to worry about an attacker with a sophisticated antenna picking up your signals a mile away. You can also be pretty confident of who you are communicating with because they have to be right there under the light source. These relatively small areas of service (by a given light source) are called attocells. The prefix atto- means quintillionth (which is a pretty small number), but,

importantly, it’s the next prefix down after femto-, as in femtocells, which are tiny cells
used in some cellular networks.
At the time of this writing, Li-Fi technology is in its infancy but holds great promise.
There are still many challenges to overcome, including co-channel interference (where multiple light sources overlap each other), roaming (seamlessly transferring a
communications channel to an adjacent attocell or to an RF-based system if the user
wanders out of the supported area), and endpoint interface devices (the sensors and light
sources that would have to be built into each laptop, smartphone, etc.). Still, the benefits
are many. Apart from the ones mentioned in the previous paragraph, Li-Fi promises to
support much higher densities of endpoints, with much lower latencies, and in places
where RF can be problematic (e.g., healthcare facilities, aircraft cabins, and power plants).

569
802.16
IEEE standard 802.16 is a MAN wireless standard that allows for wireless traffic to cover
a much wider geographical area, where stations can be as far as 70 km apart. It uses some
of the same bands as WLAN standards, specifically 2.4 GHz and 5 GHz, but uses up to 256 subcarriers with variable data rates to efficiently handle lots of traffic across large
distances. This technology is also referred to as broadband wireless access.
A commercial technology that is based on 802.16 is WiMAX, which was widely touted as a replacement for second-generation (2G) digital cellular networks, particularly
in rural areas. While this did not happen across the board (it largely lost out to Long
Term Evolution or LTE), 802.16, and WiMAX in particular, remains in widespread use,
especially outside the United States. A common implementation of 802.16 technology
is shown in Figure 12-3.
NOTE IEEE 802.16 is a standard for vendors to follow to allow for interoperable broadband wireless connections. IEEE does not test for compliance to this standard. The WiMAX Forum runs a certification program that is intended to guarantee compliance with the standard and interoperability with equipment between vendors.
PART IV

1 A subscriber sends
wireless traffic at speeds
ranging from 2 Mbps to 155 Mbps
from a fixed antennna on a building.

2 The base station recevies transmissions from multiple sites and sends traffic over wireless or wired links to a switching center using 802.16 protocol.

Switching center
Wireless or wired link using 802.16 protocol
Residential subscriber

3

Base station

Office building subscribers

Figure 12-3

Broadband wireless in MAN

The switching center sends traffic to an ISP or the public-switched telephone network.

ISP

802.15.4

The IEEE 802.15.4 standard deals with a much smaller geographical network, which is referred to as a wireless personal area network (WPAN). This technology allows for connectivity to take place among “disadvantaged” devices, which are the ubiquitous low-cost, low-data-rate, low-power, extended-life ones such as the embedded devices introduced in Chapter 7. For example, if you are using active radio frequency identification (RFID) or Industrial Internet of Things (IIoT) devices, odds are that you are using 802.15.4. This standard is optimized for situations in which machines communicate directly with other machines over relatively short distances (typically no more than 100 meters). For this reason, this standard is a key enabler of the Internet of Things (IoT), in which everything from your thermostat to your door lock is (relatively) smart and connected.

The 802.15.4 standard defines the physical (PHY) layer and Media Access Control

(MAC) sublayer of the data link layer in the OSI model. At the physical layer, it uses DSSS. For MAC, it uses CSMA-CA. In terms of topology, this standard supports star, tree, and mesh networks. The catch is that, regardless of the topology, 802.15.4 requires a full-function device (FFD) that acts as a central node for the network (even if it is not logically or physically placed at its center). This central device is called the coordinator for one or more connected reduced-function devices (RFDs). This makes a lot of sense in a star or tree topology, where you have a regular computer as the hub or root node. It might be a bit less intuitive when you think of mesh networks such as you would find in a smart home network, but we'll get into that when we discuss ZigBee in the next section.

There are multiple extensions to the base 802.15.4 standard that optimize it for specific geographic regions or applications. You may come across the following:

802.15.4c

For use in China

802.15.4d

For use in Japan

802.15.4e

For industrial applications

802.15.4f

For active (i.e., battery powered) radio frequency identification (RFID)

802.15.4g

For smart utility networks (SUNs)

Because this standard was intended to support embedded devices in close proximity to each other, the typical range is only about 10 meters (though it could reach 1 km in optimal conditions) and the data rates are quite low. While nodes frequently communicate at the maximum rate of 250 Kbps, there are also lower rates of 100, 20, and even 10 Kbps for smaller devices that have to last a long time on small batteries. Despite the low data rates, devices that implement this standard are able to support real-time applications (i.e., those that require extremely low latencies) through the use of Guaranteed Time Slot (GTS) reservations. Note that when a GTS is used, the channel access technique used has to be time division multiple access (TDMA) instead of the

more typical
CSMA/CA. TDMA is a technique that divides each communications channel into multiple time slots to increase the data rates by taking advantage of the fact that not every
station will be transmitting all the time.

Security-wise, 802.15.4 implements access control lists (ACLs) by default, so nodes
can decide whether to communicate with other nodes based on their claimed physical
address. Keep in mind, however, that spoofing a physical address is trivial. The standard
also offers (but does not require) two other security mechanisms that you should know.
The first is support for symmetric key encryption using the Advanced Encryption Standard (AES) with 128-bit keys, used to protect message confidentiality and integrity. The
second is a frame counter feature that protects against replay attacks by tracking the last
message received from another node and ensuring a new message is more recent than it.

ZigBee
ZigBee is one of the most popular standards based on IEEE 802.15.4. It sits right on
top of the layer 1 and layer 2 services provided by 802.15.4 and adds networking and
application layer support.
Layer 7–Application
ZigBee
Layer 3–Network

Layer 2–Data link
802.15.4
Layer 1–Physical

ZigBee is intended to be simpler and cheaper than most WPAN protocols and is very
popular in the embedded device market. You can find ZigBee in a variety of home automation, industrial control, medical, and sensor network applications. Figure 12-4

Figure 12-4
ZigBee in a
smart home

Smart
light bulb