Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**9**

**Wide Area Networking**

* [Module Introduction](javascript://)
* **9-1**[WAN Essentials](javascript://)
  + **9-1a**[Entry Point Equipment](javascript://)
* **9-2**[Routing Protocols](javascript://)
  + **9-2a**[Routing Tables](javascript://)
  + **9-2b**[Routing Path Types](javascript://)
  + **9-2c**[Route](javascript://)
  + **9-2d**[Routing Metrics](javascript://)
  + **9-2e**[Routing Protocols to Determine Best Paths](javascript://)
  + **9-2f**[Interior and Exterior Gateway Protocols](javascript://)
  + **9-2g**[Routing Redundancy](javascript://)
* **9-3**[WAN Connectivity](javascript://)
  + **9-3a**[DSL (Digital Subscriber Line)](javascript://)
  + **9-3b**[Cable Broadband](javascript://)
  + **9-3c**[Fiber](javascript://)
  + **9-3d**[Leased Lines](javascript://)
  + **9-3e**[MPLS (Multiprotocol Label Switching)](javascript://)
  + **9-3f**[Cloud Connectivity Options](javascript://)
  + **9-3g**[Software-defined WAN (SD-WAN)](javascript://)
* **9-4**[Wireless WANs](javascript://)
  + **9-4a**[Cellular](javascript://)
  + **9-4b**[Satellite](javascript://)
* **9-5**[Troubleshooting Connections](javascript://)
  + **9-5a**[Internet Connectivity Issues](javascript://)
  + **9-5b**[Interface Problems](javascript://)
  + **9-5c**[Routing Issues](javascript://)
* **9-6**[Module Review](javascript://)
  + **9-6a**[Module Summary](javascript://)
  + **9-6b**[Key Terms](javascript://)
  + **9-6c**[Review Questions](javascript://)
  + **9-6d**[Hands-On Projects](javascript://)
  + **9-6e**[Capstone Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Introduction

### Objectives

After reading this module and completing the exercises, you should be able to:

* **1**Identify the fundamental elements of WAN service options
* **2**Explain how routers manage internetwork communications
* **3**Compare and contrast WAN connectivity technologies
* **4**Explain the most common wireless WAN technologies
* **5**Troubleshoot common connection problems

**On the Job**

The European “cooperative” public Internet Exchange model has come to the United States in the last few years, changing WAN internetworking considerations related to cloud service access. These days, WAN networking is as much about connecting to cloud services as to far-away offices. A public IX (Internet Exchange) is a less-expensive, cooperative way to directly or near-directly peer with other companies’ networks, rather than paying an ISP for expensive Internet bandwidth. In this model, for small fees associated with running the cooperative network at a few data centers in a metropolitan area, we can peer directly with content partners’ networks. This requires no ISP in the middle and makes it possible to route directly to our peers.

Last year, one of our SaaS security software delivery teams advocated for hosting their application at data centers directly connected to a public IX in the United States rather than at our traditional data centers. The SaaS application is very sensitive to Internet latency, and more than 50 percent of its traffic is exchanged with just a few content providers, including Microsoft, Amazon hosting services, and Google.

At first, I couldn’t understand the rationale for adding more data center locations when we already had quite a few. Then the SaaS security team showed me traffic tests. I also ran my own. I learned that the other traffic providers were a hop or two closer when tested from the IX location. More importantly, when connected to the IX network’s peering, we saw much faster effective transport speeds with all of our big content partners. Because a peering network allows less expensive Internet transit, some companies might prefer IX routes to routes over the Internet, resulting in better results than the hops saved would suggest.

In a couple of locations, we looked at extending an IX network to our nearby facilities via WAN circuits. But when we compared the cost of the extension to just renting data center space at the IX, it made more sense to host at the location where the IX was already connected, even after buying more network gear.

Public “cooperative” IX examples include the following:

* AMS-IX (Bay Area Internet Exchange)
* SFMIX (San Francisco Metro Internet Exchange)
* FL-IX (Florida Internet Exchange)
* NYIIX (New York International Internet Exchange)

The United States also has some older Internet Exchange providers, but usually their hosting fees are higher, making total cost potentially much higher than in this newer model.

**Brooke Noelke**

**Cloud Service Architect**

**McAfee**

In previous modules, you have learned about basic transmission media, network models, and networking hardware associated with LANs. This module focuses on WANs (wide area networks), which, as you know, are networks that connect two or more geographically distinct LANs. WANs are of significant concern for organizations attempting to meet the needs of telecommuting workers, global business partners, and Internet-based commerce.

The distance requirements of WANs affect their entire infrastructure, and, as a result, WANs differ from LANs in many respects. To understand the fundamental difference between a LAN and a WAN, think of the hallways and stairs of your house or school as LAN pathways. These interior passages allow you to go from room to room. To reach destinations outside the building, however, you need to use sidewalks and streets. These public thoroughfares are analogous to WAN pathways—except that WAN pathways are not necessarily public.

This module discusses WAN topologies and various technologies used by WANs. It also notes some potential pitfalls in establishing and maintaining WAN connections.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-1WAN Essentials

### Certification

* 1.2

Explain the characteristics of network topologies and network types.

Average reading time: 11 minutes

A WAN traverses a significant distance and usually supports very high data throughput. Each of the following scenarios demonstrates a need for a WAN:

* A bank with offices around the state needs to connect those offices with each other to gather transaction and account information into a central database. Furthermore, it needs to connect with global financial clearinghouses to, for example, conduct transactions with other institutions.
* Regional sales representatives for a national pharmaceutical company need to submit their sales figures to a file server at the company’s headquarters and receive email from the company’s mail server.
* An automobile manufacturer in Detroit contracts its plastic parts manufacturing to a Delaware-based company. Through WAN links, the auto manufacturer can video conference with the plastics manufacturer, exchange specification data, and even examine the parts for quality from a remote location.
* A clothing manufacturer sells its products over the Internet to customers worldwide.

Although all these businesses need WANs, they might not need the same kinds of WANs. Depending on the traffic load, budget, geographical breadth, and commercially available technology, each might implement a different transmission method. For every business need, a few WAN connection types might be capable of meeting that need. At the same time, many WAN technologies can coexist on the same network to meet different needs.

The following list summarizes the major characteristics of WANs and explains how a WAN differs from a LAN:

* LANs connect nodes, such as workstations, servers, printers, and other devices, in a small geographical area on a single organization’s network, whereas WANs use networking devices, such as routers and modems, to connect networks spread over a wide geographical area.
* LANs and WANs may differ at layers 1 and 2 of the OSI model in access methods, topologies, and, sometimes, transmission media. For example, the way DSL transmits bits over a WAN differs from the way Ethernet transmits bits over a LAN.
* Both LANs and WANs use the same protocols from OSI layers 3 and above. Recall that layer 3 protocols are responsible for directing data between LANs.
* LANs are mostly owned and operated by the companies that use them. On the other hand, WANs are usually owned and operated by telcos (telecommunications carriers), also known as NSPs (network service providers), such as AT&T, Verizon, Spectrum, and Comcast. Corporations lease WAN connections from these carriers, often with payments based on the amount of bandwidth used or reserved. Alternatively, as you read about in the [On the Job](javascript://) story at the beginning of this module, corporations might connect directly to an IX (Internet Exchange), sometimes called an IXP (Internet Exchange point). This is similar to the difference between buying merchandise at retail prices versus buying products wholesale through a purchasing cooperative. IXs are where the networks of ISPs and other telecommunications providers intersect. By connecting directly into an IX, companies are able to cut out some of the “middleman” expense of WAN connections.

As you can see, WANs are used to connect LANs. Recall that CANs (campus area networks) and MANs (metropolitan area networks) also connect LANs. Typically, a CAN is a collection of LANs within a single property or nearby properties, such as buildings belonging to a school where all the buildings and most or all the network media spanning those connections are confined within land owned by the school. With a CAN, it’s likely that a single organization (or group of organizations) owns all the connected LANs and most or all the networking media connecting those LANs.

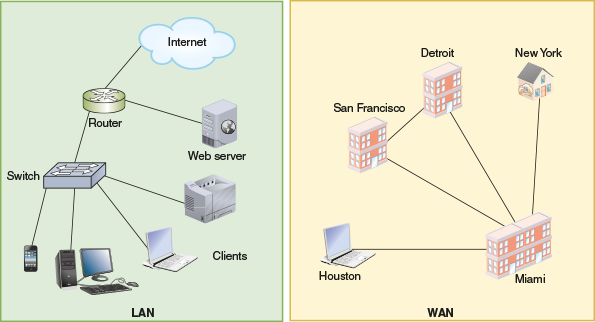
Similarly, a MAN is a collection of LANs within a limited geographical area, such as a downtown area or even a city, county, or province. With MANs, many customers might own one or more of the connected LANs, and a single, third-party provider leases use of the networking media connecting these LANs. These connections often must be made across property not owned by either the MAN provider or the MAN customers. MAN connections might be made available to the general public (such as when a city makes high-speed Internet access available to all downtown area residents), or it might be restricted to a single customer (such as when a hospital is connected to its satellite medical offices). The following list gives examples where MANs can be useful:

* Connecting a city’s police stations
* Connecting a hospital with its regional medical centers
* Connecting a home office with its branch offices and a warehouse location

The reason to make these distinctions between WANs, MANs, CANs, and LANs is because different technologies and protocols have been developed to best serve each of these markets. Networking technology that works well for a [**long-haul connection**](javascript://) across hundreds of miles to support the Internet backbone isn’t well suited for network connections between two buildings situated next door to each other, even though both these networks might connect multiple LANs. Throughout this module, you’ll learn more about the nuances of when to use various technologies, depending on distances, networking media, and types of communications needed on the network. [Figure 9-1](javascript://) illustrates this fundamental difference between WAN and LAN connectivity.

**Figure 9-1**

Differences in scale between LAN and WAN



Enlarge Image

The individual geographic locations or endpoints connected by a WAN are known as WAN sites. A WAN link is a connection between one WAN site (or endpoint) and another site (or endpoint). WAN links can be point-to-point (connects one site to only one other site) or multipoint (connects one site to two or more other sites).

Go to pg.

[**help**](javascript://)

Application Opened

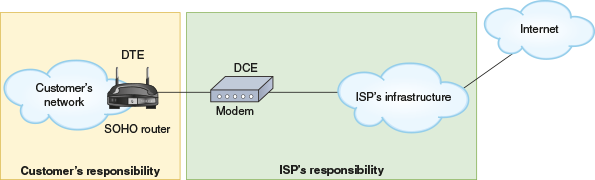
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-1aEntry Point Equipment

If you have DSL or cable Internet service, you connect your home router to a modem. A [**modem**](javascript://) is a modulation/demodulation device that converts between digital and analog signals. The customer’s endpoint device on a WAN is called the DTE (data terminal equipment), and the carrier’s endpoint device for the WAN is called the DCE (data circuit-terminating equipment). In this case, the router is the DTE, usually owned by the customer, and the modem is the DCE, usually owned by the ISP. [Figure 9-2](javascript://) shows this setup, with a router and modem at the customer’s site defining the dividing line between each network.

**Figure 9-2**

A router and a modem define the endpoints where a LAN connects to a WAN



Enlarge Image

Generally, the DTE is the responsibility of the customer and the DCE is the responsibility of the ISP. The DTE communicates on the LAN, and the DCE communicates on the WAN. Sometimes the DTE and DCE are combined in the same device. For example, a router might have one WAN network adapter, or WIC (WAN interface connector), that connects to a fiber-optic WAN and one LAN network adapter that connects to an Ethernet, twisted-pair LAN.

When working with your network’s connection to your ISP at the service-related entry point, you need to know the difference between equipment that belongs to the ISP and equipment that belongs to the subscriber. Equipment located on the customer’s premises, regardless of who owns it and who is responsible for it, is called CPE (customer premises equipment). Equipment belonging to the ISP, despite its location on the customer’s premises, should only be serviced by the ISP’s technicians even if it is located on the customer’s side of the demarc (demarcation point). Equipment owned by the customer is the responsibility of the customer and will not be serviced by the ISP. The following list describes devices commonly found at or near the demarc:

* **NIU (network interface unit)**—The NIU, also called NID (network interface device), at the demarc connects the ISP’s local loop to the customer’s network. A more intelligent version of an NIU is a **[smartjack](javascript://)**, or INID (Intelligent NID), which can provide diagnostic information about the interface. For example, a smartjack might include loopback capabilities. Just like the loopback adapter you use to test a port or cable on your computer, the smartjack can loop the ISP’s signal back to the CO (central office) for testing. The ISP is responsible for all wiring leading up to the NIU and for the NIU itself. The customer is responsible for everything past the NIU unless the equipment is owned by the ISP, such as with a line driver, CSU/DSU, or set-top box.
* **Line driver**—Essentially a repeater, a line driver can be installed either on copper lines (in which case, it is called a copper line driver) or fiber lines (in which case, it is called a fiber line driver) to boost the signal across greater distances. The device might be placed on either side of the demarc and, if located on the customer’s side, might be owned by either party.
* **CSU/DSU (channel service unit/data service unit)**—This device serves as the endpoint for a dedicated connection between an ISP and a customer. Like line drivers, these devices can be owned by either party, depending upon who is responsible for providing this device according to the terms of service. However, the CSU/DSU is typically placed on the customer’s side of the demarc between the demarc and the first router.

Now that you understand the basic components that differentiate WANs from LANs, you’re ready to learn about specific technologies and types.

### Exam Tip

The CompTIA Network+ exam expects you to know about a variety of ISP connection types and to be able to identify the networking environments best suited to each. For wired WANs and related technologies, you need to know about leased lines, DSL, cable broadband, metro-optical networks, MPLS, SD-WAN, and cloud connectivity options. Wireless WANs covered later in this module include satellite and cellular technologies.

**Remember This…**

* Compare LANs, CANs, MANs, and WANs.
* Explain the purpose of a smartjack.

**Self-Check**

1. Which network type supports long-haul connections between ISPs?

Answer

* 1. WAN
  2. CAN
  3. MAN
  4. LAN

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-2Routing Protocols

### Certification

* 1.1

Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

* 2.2

Compare and contrast routing technologies and bandwidth management concepts.

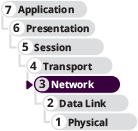
* 3.3

Explain high availability and disaster recovery concepts and summarize which is the best solution.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

Average reading time: 33 minutes



You’ve spent a lot of time over the past few modules learning how switches work, both at layer 2 and layer 3, within a corporate network. As you know, routers serve as gateways to connect networks. To study WAN technologies, you must learn more about how routers work. A router joins two or more networks and passes packets from one network to another. Routers are responsible for determining the next network to which a packet should be forwarded on its way to its destination. A typical router consists of an internal processor, an operating system, memory, input and output jacks for different types of network connectors (depending on the network type), and, usually, a management console interface. Three examples of routers are shown in [Figure 9-3](javascript://), with the most complex on the left and the simplest on the right. High-powered, multiprotocol routers may have several slot bays to accommodate multiple network interfaces. At the other end of the scale are simple, inexpensive routers often used in small offices and homes, and they require little configuration.

**Figure 9-3**

ISP, business, and consumer routers



Enlarge Image

Courtesy of Juniper Networks, Inc Courtesy of NETGEAR

A router’s strength lies in its intelligence—that is, its ability to interact with transmissions and make decisions. Although any one router can be specialized for a variety of tasks, all routers can do the following:

* Connect dissimilar networks, such as a LAN and a WAN, which use different types of protocols.
* Interpret layer 3 and often layer 4 addressing and other information contained in these headers.
* Determine the best path for data to travel from point A to point B. The [**best path**](javascript://) is the most efficient route to the message’s destination calculated by the router, based upon the information the router has available to it.
* Reroute traffic if the path of first choice is down but another path is available.

In addition to performing these basic functions, routers may perform any of the following optional functions:

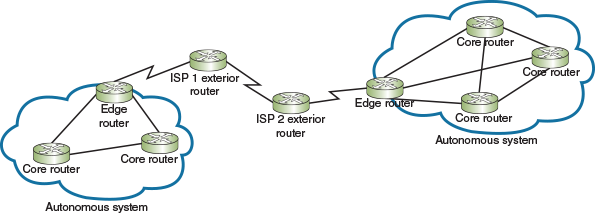
* Filter broadcast transmissions to alleviate network congestion.
* Acting as a simple firewall, prevent certain types of traffic from getting to a network, enabling customized segregation and security.
* Support simultaneous local and remote connectivity.
* Provide high network fault tolerance through redundant components such as power supplies or network interfaces.
* Monitor network traffic and report statistics.
* Diagnose internal or other connectivity problems and trigger alarms.

Routers are often categorized according to their location on a network or the Internet and the routing protocols they use. The various categories are described in the following list and diagrammed in [Figure 9-4](javascript://):

* [**Core routers**](javascript://), also called [**interior routers**](javascript://), are located inside networks within the same autonomous system. An [**AS (autonomous system)**](javascript://) is a group of networks, often on the same domain, that are operated by the same organization. For example, Cengage might have several LANs that all fall under its domain with each LAN connected to the others by core routers. An AS is sometimes referred to as a trusted network because the entire domain is under the organization’s control. Core routers communicate only with routers within the same AS.
* [**Edge routers**](javascript://), or [**border routers**](javascript://), connect an autonomous system with an outside network, also called an untrusted network. For example, the router that connects a business with its ISP is an edge router.
* [**Exterior router**](javascript://) refers to any router outside the organization’s AS, such as a router on the Internet backbone. Sometimes a technician might refer to their own edge router as an exterior router because it communicates with routers outside the AS. But keep in mind that every router communicating over the Internet is a trusted edge router for some organization’s AS, even if that organization is a large telecommunications company managing a portion of the Internet backbone.

**Figure 9-4**

Core, edge, and exterior routers



Enlarge Image

On small office or home office LANs, routers are simple to install: Plug in the network cable from the cable modem connected to your ISP on one port and connect your computer(s) to your LAN through another port or by a wireless connection. Turn on the router and computer and use a web-based utility program on the router to set it up.

However, high-powered, multiprotocol routers can be a challenge to install on sizable networks. Typically, an engineer must be very familiar with routing technology to figure out how to place and configure a router to the best advantage. If you plan to specialize in network design, engineering, or management, you should research router types and their capabilities further. As you learn more about how routers work, keep in mind that layer 3 and layer 4 switches can perform the same functions.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2aRouting Tables

A [**routing table**](javascript://) is a database that holds information about where hosts are located and the most efficient way to reach them. As you know, a router has two or more network ports, or interfaces, and each port connects to a different network. Each network connection is assigned an interface ID, and logically, the router belongs to every network it connects to. A router relies on its routing table to identify which network a host belongs to and which of the router’s interfaces points toward the best next hop to reach that network.

For example, in [Figure 9-5](javascript://), suppose a workstation in LAN A wants to print to the network printer in LAN D. The following steps describe how routing tables would be used in this transmission:

1. Step 1

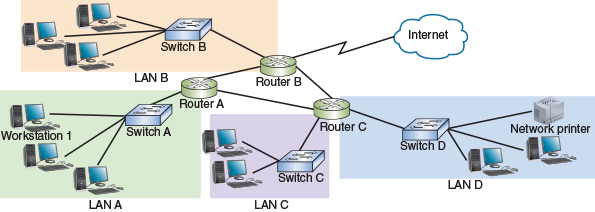
Workstation 1 issues a print command to a network printer. IP on the workstation recognizes that the IP address of the printer is on a different LAN than the workstation and forwards the transmission through switch A to its default gateway, router A.

1. Step 2

Router A examines the destination IP address in the packet’s header and searches its routing table to determine which of its interfaces the message should go to. [Table 9-1](javascript://) shows how a routing table is designed, with each entry explained in plain English instead of using IP addresses and other data. Each row in the routing table describes one route, including a destination network and how to get there. The first two columns provide information used to match messages to a route. The next two columns provide forwarding information for the route. Routing metrics are route ratings used as tie breakers when needed.

**Figure 9-5**

Routers rely on routing tables to locate destination hosts



Enlarge Image

**Table 9-1**

### Portions of Router A’s Routing Table in Plain English

| **Destination network ID** | **Netmask** | **Gateway** | **Interface** | **Routing metrics (tie breaker)** |
| --- | --- | --- | --- | --- |
| LAN A’s IP address | LAN A’s netmask | None (This is router A’s own LAN.) | Port that points toward switch A | 1 |
| LAN B’s IP address | LAN B’s netmask | Router B’s IP address | Port that points toward router B | 4 |
| LAN C’s IP address | LAN C’s netmask | Router C’s IP address | Port that points toward router C | 5 |
| LAN D’s IP address | LAN D’s netmask | Router B’s IP address | Port that points toward router B | 10 |
| LAN D’s IP address | LAN D’s netmask | Router C’s IP address | Port that points toward router C | 5 |
| IP address on the Internet | That host’s netmask | Router B’s IP address | Port that points toward router B | 23 |
| 0.0.0.0 (wildcard entry for any network) | 0 (wildcard entry for any netmask) | Router B’s IP address | Port that points toward router B | 3 |

Here’s a breakdown of how the route-search process uses information in [Table 9-1](javascript://):

* + Router A examines all rows in its routing table. In each row, it uses information in the first two columns—the destination network’s IP address and netmask—to calculate the range of IP addresses included in that network.
  + If the message’s destination IP address fits in the calculated range for a route, the router then reads the IP address of the gateway in the third column. This gateway is the next hop router. It also reads in the fourth column the interface it will use to send the message out.
  + If it finds more than one possible route, the router uses [**routing metrics**](javascript://) (information about each route) in the last column to determine which route is most efficient. The smaller the metrics number, the better the route. Notice in [Figure 9-5](javascript://) and in [Table 9-1](javascript://) that two routes can reach the network printer on LAN D. Of these two routes, the router would select the one with the lower metrics value. You’ll learn more about routing metrics later in this module.
  + If it doesn’t find a matching entry, the router looks for 0.0.0.0 in the first column. This route is the [**default route**](javascript://)—the route to use if no other route is a match. In most cases, the routing table must contain a default route so it can handle traffic with no predefined route, such as DNS messages. The gateway in the third column of this route is called the [**gateway of last resort**](javascript://), which is the router that accepts unrouteable messages from other routers.
  + If no default route is defined, the router will drop the message.

In this scenario, router A finds two matches with LAN D’s network information and chooses the best of these two options based on their respective routing metrics. Router A then determines that it should send the message out the port that faces router C.

1. Step 3

Before it forwards the message, router A decreases the number of hops tallied in the TTL (time to live) field of the packet header. It then sends the message to router C.

1. Step 4

Router C decreases the packet’s hop count by 1, reads the packet’s destination IP address, searches its routing table for matching network information, and determines the message is destined for its own LAN D. It sends the message to switch D on LAN D.

1. Step 5

Using its ARP table, switch D matches the destination IP address with the printer’s MAC address. If switch D didn’t have a matching entry in its ARP table for the network printer’s IP address, it would use an ARP broadcast to request the printer’s MAC address. Switch D then delivers the transmission to the printer, which picks up the message and begins printing.

**Note 9-1**

What’s the difference between a default gateway, a default route, and a gateway of last resort?

* Most hosts have a default gateway—a router or layer 3 switch—where they send all routable messages. Hosts can’t communicate with other networks without a default gateway.
* Most routers have a default route as a backup route when no other route can be determined.
* The default route points to a gateway of last resort. A router’s gateway of last resort is where it sends messages addressed to networks the router can’t find in its routing table.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2bRouting Path Types

Routing paths are determined in one of two ways as described next:

* [**Static routes**](javascript://)—A network administrator configures a routing table to direct messages along specific paths between networks. For example, it’s not uncommon to see a static route between a small business and its ISP. However, static routes can’t adapt to network congestion, failed connections, or device relocations, and they require human intervention to configure or adjust.
* [**Dynamic routes**](javascript://)—A router automatically calculates the best path between two networks and accumulates this information in its routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute messages through a different path. When a router is added to a network, dynamic routing ensures that the new router’s routing tables are updated.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2cRoute

The **route** utility allows you to view a host’s routing table. The route command can also be used to add or delete static routes, which you’ll practice doing in a project at the end of this module. Here are some variations of the route command for different operating systems:

* **Linux or UNIX**—Enter route at a shell prompt.
* **Windows**—Enter route print in a CLI.
* **Cisco’s IOS**—Enter show ip route at the CLI using privileged EXEC mode.

Routing tables on workstations typically contain no more than a few, unique entries, including the default gateway and loopback address. However, routing tables on Internet backbone routers, such as those operated by ISPs, maintain hundreds of thousands of entries.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2dRouting Metrics

Finding the best route or best path for messages to take across networks is one of the most valued and sophisticated functions performed by a router. Some examples of routing metrics used to determine the best path include the following:

* Hop count, which is the number of network segments crossed
* Theoretical bandwidth and actual throughput on a potential path
* Delay, or latency, on a potential path, which decreases performance
* Load, which is the traffic or processing burden sustained by a router in the path
* MTU (maximum transmission unit), which is the largest IP packet size in bytes allowed by routers in the path without fragmentation (excludes the frame used by the local network)
* [**Routing cost**](javascript://), which is a value assigned to a particular route as judged by the network administrator; the more desirable the path, the lower its cost
* Reliability of a potential path, based on historical performance
* A network’s topology

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2eRouting Protocols to Determine Best Paths

To determine the best path, routers communicate with each other through [**routing protocols**](javascript://). Routing protocol messages, similar to scouting parties exploring unknown terrain, go forth to collect data about current network status and contribute to the selection of best paths. Routers use this data to create their routing tables. Keep in mind that routing protocols are not the same as routable protocols such as IP (which can be routed across networks). However, routing protocols might piggyback on IP to reach their destinations. Also, the various routing protocols operate at different layers of the OSI model—usually layer 3, layer 4, or layer 7. However, this discussion is primarily concerned with the effects that routing protocols have on layer 3 routing activities.

Routers rate the reliability and priority of a routing protocol’s data based on these criteria:

* [**AD (administrative distance)**](javascript://)—Each routing protocol is assigned a default AD, which is a number indicating the protocol’s reliability, with lower values being given higher priority. This assignment can be changed by a network administrator when one protocol should take precedence over a previously higher-rated protocol on that network.
* [**Convergence time**](javascript://)—Routing protocols are also rated on the time it takes to recognize a best path in the event of a change or network outage. Some routing protocols are more efficient than others at communicating topology changes across the network.
* [**Overhead**](javascript://)—A routing protocol is rated on its overhead, or the burden placed on the underlying network to support the protocol. The difference here is related to how much processing power each routing protocol requires of routers and how much information must be transferred between routers and how often.

The most common routing protocols are summarized in [Table 9-2](javascript://) and are described in more detail in the following sections. Other routing protocols exist, but their descriptions exceed the scope of this course.

**Table 9-2**

### Summary of Common Routing Protocols

| **Routing protocol** | **Type** | **Algorithm used** |
| --- | --- | --- |
| RIP (Routing Information Protocol) | IGP | Distance-vector |
| RIPv2 (Routing Information Protocol, version 2) | IGP | Distance-vector |
| OSPF (Open Shortest Path First) | IGP | Link-state |
| IS-IS (Intermediate System to Intermediate System) | IGP | Link-state |
| EIGRP (Enhanced Interior Gateway Routing Protocol) | IGP | Advanced distance-vector |
| BGP (Border Gateway Protocol) | EGP | Advanced distance-vector or path vector |

### Exam Tip

[Table 9-2](javascript://) provides an overview of the routing protocols covered in this module. For the CompTIA Network+ exam, it’s important to know which routing protocols function within an autonomous system and which of these protocols communicate between these systems. You’ll also want to know the classification of protocols, especially distance-vector versus link-state.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

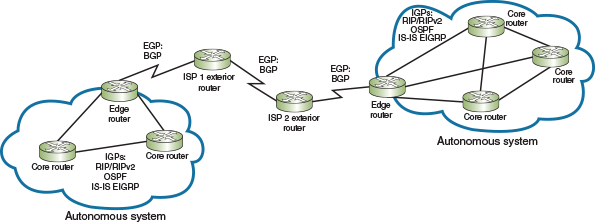
## 9-2fInterior and Exterior Gateway Protocols

As you examine [Table 9-2](javascript://), you can see that a routing protocol is classified as either an IGP or an EGP. Here’s an explanation of the two types, which are diagrammed in [Figure 9-6](javascript://):

* [**IGPs (interior gateway protocols)**](javascript://) are routing protocols used by core routers and edge routers within autonomous systems. IGPs are often grouped according to the algorithms they use to calculate best paths, as follows:
  + [**Distance-vector routing protocols**](javascript://) calculate the best path to a destination based on the distance to that destination. Some distance-vector routing protocols factor only the number of hops to the destination, whereas others consider route latency and other network traffic characteristics. Distance-vector routing protocols periodically exchange their entire routing tables with neighboring routers even if there’s not been a change to a route, which requires the transfer of large amounts of data simply to keep routing tables updated. Also, routers relying on this type of routing protocol must accept the data they receive from their neighbors and cannot independently assess network conditions two or more hops away. This limitation is sometimes called “routing by rumor,” and it results in slow convergence and higher likelihood of persistent errors when network conditions change. RIP and RIPv2 are distance-vector routing protocols.
  + [**Link-state routing protocols**](javascript://) focus less on the number of hops between routers and more on the state of a connection. These protocols collect information about all their connected links and send that information to other routers on the network. Other routers, then, can use this information about links throughout the network to build their own routing tables, independently mapping the network and determining the best path between itself and a message’s destination node. These protocols tend to adapt more quickly to changes in the network, but they can also be more complex to configure and troubleshoot. They also require more processing power to incorporate information from throughout the network to build each device’s routing table. Part of this resource demand is offset by the fact link-state routing protocols only send information when something changes. OSPF and IS-IS are link-state routing protocols, and they’re highly scalable for very large networks.
  + [**Hybrid routing protocols**](javascript://) exhibit characteristics of both distance-vector and link-state routing protocols. For example, Cisco’s EIGRP functions primarily as a distance-vector routing protocol but incorporates elements of link-state routing, for example, by syncing link information across the network only when something changes.
* [**EGPs (exterior gateway protocols)**](javascript://) are routing protocols used by edge routers and exterior routers to distribute data outside of autonomous systems. The one EGP protocol you need to know for the Network+ exam is the only EGP currently in use, BGP.

**Figure 9-6**

BGP is the only routing protocol that communicates across the Internet



Enlarge Image

**Note 9-2**

An older routing protocol named Exterior Gateway Protocol is obsolete. However, the generic term exterior gateway protocol now refers to any routing protocol that routes information between autonomous systems.

Let’s look at the details of these routing protocols, beginning with RIP and RIPv2, which are both outdated but still in use on many networks because of their simplicity and compatibility with older routers.

### Legacy Networking: RIP (Routing Information Protocol)

[**RIP (Routing Information Protocol)**](javascript://), a distance-vector routing protocol, is the oldest routing protocol. Here are some notable considerations when using RIP on a network.

Advantages:

* **Simplicity**—Quick and easy configuration.
* **Stability**—Prevents routing loops from continuing indefinitely by limiting the number of hops a message can take between its source and its destination to 15. If the number of hops in a path exceeds 15, the network destination is considered unreachable.

Disadvantages:

* **Limited metrics**—Only considers the number of hops between nodes when determining the best path rather than other, more complex factors.
* **Excessive overhead**—Broadcasts routing tables every 30 seconds to other routers, regardless of whether the tables have changed.
* **Poor convergence time**—Might take several minutes for new information to propagate to the far reaches of the network.
* **Limited network size**—Does not work well in very large network environments where data might have to travel through more than 15 routers to reach its destination (for example, on a metro network).
* **Slower and less secure**—Outdated by newer routing protocols.

Developers have improved RIP since its release in 1988 and informally renamed the original RIP as RIPv1 (Routing Information Protocol, version 1). The next version of RIP was published in 1994 and standardized by the IETF in 1998. [**RIPv2 (Routing Information Protocol, version 2)**](javascript://) generates less broadcast traffic and functions more securely than RIPv1. An extension to RIPv2 that was first proposed in 1997 is RIPng (RIP next generation), which extends RIP support to IPv6. Still, RIPv2 and RIPng cannot exceed 15 hops, and they are also considered outdated routing protocols.

**Note 9-3**

When discussing limitations of routing protocols, the 15-hop limit is specific to RIP and its later versions. This is an identifying factor you can use to distinguish RIP from other routing protocols.

### OSPF (Open Shortest Path First)

[**OSPF (Open Shortest Path First)**](javascript://) is an IGP and a link-state routing protocol used on core or edge routers. It was introduced as an improvement to RIP and can coexist with RIP or RIPv2 on a network. Characteristics include the following:

* **Supports large networks**—Imposes no hop limits on a transmission path.
* **Complex algorithms**—Calculates more efficient best paths than RIP. Under optimal network conditions, the best path is the most direct path between two points. If excessive traffic levels or an outage prevent data from following the most direct path, a router might determine that the most efficient path actually goes through additional routers.
* **Shared data**—Maintains a database of the other routers’ links. If OSPF learns of the failure of a given link, the router can rapidly compute an alternate path.
* **Low overhead, fast convergence**—Demands more memory and CPU power for calculations, but keeps network bandwidth to a minimum with a very fast convergence time, often invisible to users.
* **Stability**—Uses algorithms that prevent routing loops.
* **Multi-vendor routers**—Supported by all modern routers. It is commonly used on autonomous systems that rely on a mix of routers from different manufacturers.

### IS-IS (Intermediate System to Intermediate System)

Another IGP, which is also a link-state routing protocol, is [**IS-IS (Intermediate System to Intermediate System)**](javascript://). IS-IS uses a best-path algorithm similar to OSPF’s. It was originally codified by ISO, which referred to routers as “intermediate systems,” thus the protocol’s name. Unlike OSPF, however, IS-IS is designed for use on core routers only. Also, IS-IS is not handcuffed to IPv4 like OSPF is, so it’s easy to adapt to IPv6. Service providers generally prefer to use IS-IS in their own networks because it’s more scalable than OSPF, but OSPF is still more common.

### EIGRP (Enhanced Interior Gateway Routing Protocol)

[**EIGRP (Enhanced Interior Gateway Routing Protocol)**](javascript://), an IGP, was developed in the mid-1980s by Cisco Systems. It is an advanced distance-vector protocol that combines some of the features of a link-state protocol and so is sometimes referred to as a hybrid protocol. With a fast convergence time and low network overhead, it’s easier to configure and less CPU-intensive than OSPF. EIGRP also offers the benefits of supporting multiple protocols and limiting unnecessary network traffic between routers.

Originally, EIGRP was proprietary to Cisco routers. In 2013, parts of the EIGRP standard were released to the public so that networks running routers from other vendors can now use EIGRP. It accommodates very large and heterogeneous networks, but it is still optimized for Cisco routers and not many manufacturers have made the transition. On LANs that use Cisco routers exclusively, EIGRP is generally preferred over OSPF.

### BGP (Border Gateway Protocol)

The only current EGP is [**BGP (Border Gateway Protocol)**](javascript://), which has been dubbed the “protocol of the Internet.” Whereas OSPF and IS-IS scouting parties only scout out their home territory, a BGP scouting party can go cross-country. BGP spans multiple autonomous systems and is used by edge and exterior routers on the Internet. Here are some special characteristics of BGP:

* **Path-vector routing protocol**—Communicates via BGP-specific messages that travel between routers over TCP sessions.
* **Efficient**—Determines best paths based on many factors.
* **Customizable**—Can be configured to follow policies that might, for example, avoid a certain router, or instruct a group of routers to prefer one route over other available routes.

BGP is the most complex of the routing protocols mentioned in this module. If you maintain networks for an ISP or large telecommunications company, you will need to understand BGP in depth.

Go to pg.

[**help**](javascript://)

Application Opened

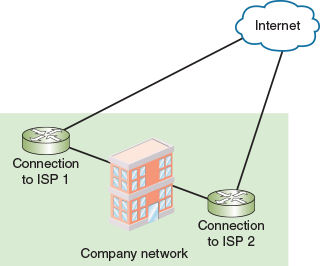
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2gRouting Redundancy

Recall that fault tolerance on a network is accomplished through using redundant hardware, connections, services, and copies of data. For example, if one router fails, another router can take over. You might even have a cluster of routers so your network could tolerate the failure of multiple devices without losing service. On a small network, having two or three ISP connections with one or two routers for each might provide sufficient redundancy. Larger networks should also have multiple ISP connections with each using geographically separate hardware and network media. For example, you might want one ISP connection to enter your property from one direction and another ISP connection to enter from the other side of your building or campus (see [Figure 9-7](javascript://)). These diverse paths increase your network’s fault tolerance should the proverbial backhoe damage underground lines from one ISP, or in case of flooding, fire, power outage, or other damage that is restricted to a relatively small area.

**Figure 9-7**

Redundant ISP connections to the Internet



If you’re paying for two or more ISP connections, should you use both of them all the time, or should one be kept only as a backup when the first one fails? This question highlights the key difference between two contrasting redundancy techniques, as described next:

* [**Active-active redundancy**](javascript://)—All redundant resources are active at all times, and work is distributed among them. For example, you might load balance your Internet traffic between two ISP connections, but either ISP service could take over if the other one fails. This arrangement can provide increased performance during normal operation, as all your available resources are actively working. You might have the load distributed evenly among all resources, or you might have one or more redundant resources running a reduced load.
* [**Active-passive redundancy**](javascript://)—Only one or a few redundant resources are active at any time with the backup devices on standby ready to fill in if they’re needed. For example, you might run all your Internet traffic over a single ISP service, but you have a second one on standby in case it’s needed.

So how do you make this happen when you’re running two routers in a network? For example, you know you can only configure one default gateway on your computer. Do you configure half your network hosts to use one default gateway and half to use the other? Is there a way to make them automatically failover if one gateway fails?

Instead of managing redundancy manually, you can configure an [**FHRP (First Hop Redundancy Protocol)**](javascript://) on a router or layer 3 switch to provide a single VIP (Virtual IP) address as the default gateway that, in turn, potentially points to multiple routers. Two popular FHRPs you learned about in an earlier module and a third FHRP that is gaining in popularity are described next:

* **VRRP (Virtual Router Redundancy Protocol)—**Industry standard across vendors. The VIP points to the primary, active router, and all other routers stand by as potential backups. Configurations are made using the vrrp command.
* **HSRP (Hot Standby Routing Protocol)**—Proprietary to Cisco. The VIP points to the active router, a standby router is configured for auto failover, and other routers listen for indications the active and standby routers have both failed. Configurations are made using the standby command.
* **GLBP (Gateway Load Balancing Protocol)**—Also proprietary to Cisco devices. GLBP gateways are weighted according to priority, and traffic is load balanced among all gateways. Configurations are made using the glbp command.

**Remember This…**

* Identify the primary differences between the routing protocols RIP, RIPv2, OSPF, EIGRP, and BGP.
* Compare link-state, distance-vector, and hybrid routing protocol characteristics.
* Explain how to configure router redundancy using common FHRPs.
* Use the route command to view routing tables in various OSs.

**Self-Check**

1. Which routing protocol runs between your network’s edge router and your ISP’s edge router?

Answer

* 1. EIGRP
  2. RIPv2
  3. OSPF
  4. BGP

1. Which command will output your Windows computer’s routing table?

Answer

* 1. show ip route
  2. route print
  3. route

1. Which routing protocol is limited to 15 hops?

Answer

* 1. EIGRP
  2. OSPF
  3. BGP
  4. RIPv2

**You’re Ready**

You’re now ready to complete [Project 9-1: Create a Routing Table Entry in Windows](javascript://), or you can wait until you’ve finished reading this module.

**You’re Ready**

You’re now ready to complete [Project 9-2: Create a Path MTU Black Hole](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-3WAN Connectivity

### Certification

* 1.2

Explain the characteristics of network topologies and network types.

* 1.8

Summarize cloud concepts and connectivity options.

* 2.1

Compare and contrast various devices, their features, and their appropriate placement on the network.

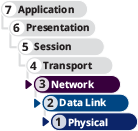
* 2.2

Compare and contrast routing technologies and bandwidth management concepts.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

Average reading time: 42 minutes



Connecting your network to other networks plays an integral role in building and managing a network. However, the tools you’ll use to connect networks vary greatly according to the size of your network, your network’s bandwidth needs, and the relative locations of your network’s segments. Imagine you’re starting a new company. Initially, you’re working from home and the only employee is you. Your WAN requirements consist entirely of connecting your home network to the Internet. However, as your company grows, you’ll need other kinds of WAN connections. Throughout this section, you’ll read about WAN connectivity options that will serve your company as it expands from your basement into a global entity. Notice the ways your WAN needs shift over time and what technologies are available to meet those needs.

Some of these service options are called by common names that you might recognize if you’ve ever shopped around for home or business Internet service or if you’ve noticed commercials or billboards advertising Internet subscription options. Many of these connections use existing telephone lines, the existing cable TV infrastructure, or specialized copper or fiber cables. Later in this module, you’ll also learn about WAN services provided wirelessly, including cellular and satellite connections.

As you compare options for WAN services, keep in mind a significant difference between technologies—whether the connection is shared among many customers or dedicated to one customer. The following list explains these two options:

* [**Broadband**](javascript://)—Especially well-suited for residential customers, the cables (whether telephone, coaxial, or fiber) and available bandwidth are shared between multiple customers. The ISP makes a “best effort” attempt to provide up to the advertised bandwidth, and actual performance varies considerably during busy usage. Bandwidth is also [**asymmetrical**](javascript://), or asynchronous, meaning download speeds (data traveling from the carrier’s switching facility to the customer) are faster than upload speeds (data traveling from the customer to the carrier’s switching facility). For a higher premium, businesses can get faster broadband speeds and possibly one or more static IP addresses included in the package. However, uptime, service, and bandwidth are still not guaranteed.
* [**DIA (dedicated Internet access)**](javascript://)—The cable itself or a portion of its available bandwidth is dedicated to a single customer; this is more common for business customers and comes with an SLA-defined (service-level agreement) guarantee of minimum uptime percentages and maximum recovery times if the service goes down. Bandwidth is [**symmetrical**](javascript://), or synchronous, meaning download and upload speeds are about the same. This is especially important for businesses that back up large amounts of data online. The subscription will also often include a certain number of static IP addresses.

**Applying Concepts 9-1**

### Test Your Internet Connection’s Speed

You can test your own Internet connection to see what the current upload and download speeds are using a [**bandwidth speed tester**](javascript://), or a speed test website. During the test, data will be sent to your computer and then requested from your computer to measure download and upload speeds, respectively. Complete the following steps:

1. 1

In your browser, go to [speedtest.net](http://speedtest.net/" \t "_blank). At the time of this writing, you start the test by clicking **GO**. The test begins, as shown in [Figure 9-8](javascript://).

1. 2

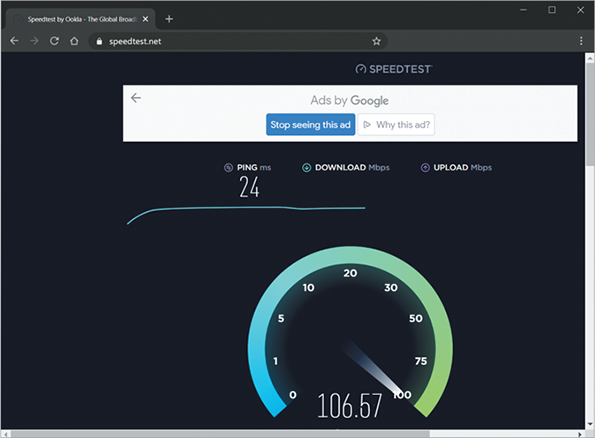
Wait for the test to complete and then write down your speed test results. What are your current download and upload speeds?

1. 3

Try a different site and compare results. Go to [verizon.com/speedtest](http://verizon.com/speedtest" \t "_blank), click **Get started** and wait for the test to complete (see [Figure 9-9](javascript://)). What are the results this time? How do they compare to your first results? Why do you think this is?

**Figure 9-8**

Speed test in progress

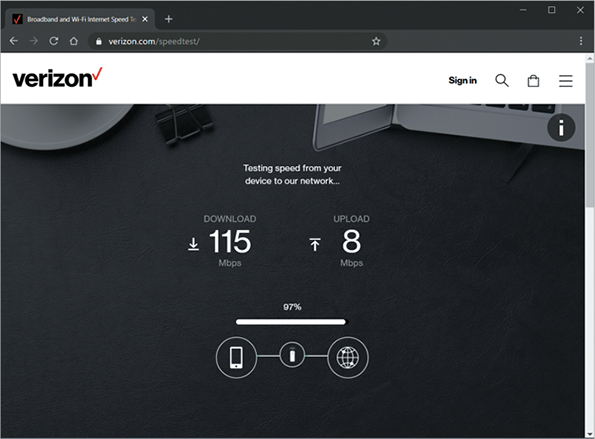


Enlarge Image

Source: Ookla, LLC

**Figure 9-9**

Another speed test for comparison



Enlarge Image

Source: Verizon

While these websites are designed to test throughput between your network and a host on the Internet, you can also use throughput testing software, such as Lakehorn’s Network Speed Tester, to check the performance of your local network. Recall from [Hands-On Project 5-4](javascript://) that you also used the TotuSoft LAN Speed Test application and the TamoSoft Throughput Test application.

These first three WAN connectivity options cover broadband ISP services you might use for your home office: DSL, cable, and fiber Internet. Then you’ll learn about high-speed WAN service options more commonly used by businesses.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

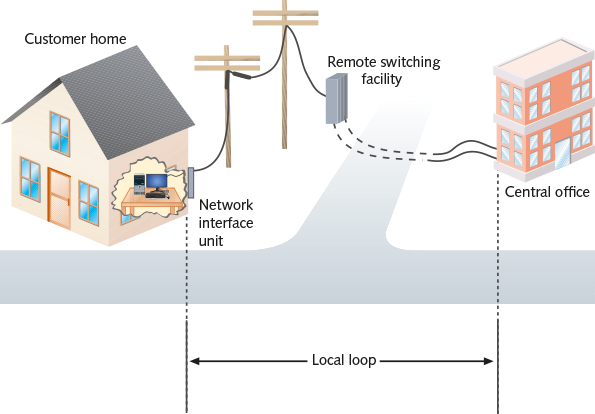
## 9-3aDSL (Digital Subscriber Line)

[**DSL (digital subscriber line)**](javascript://) is a WAN connection method introduced by researchers at Bell Laboratories in the mid-1990s. It operates over the [**PSTN (public switched telephone network)**](javascript://), also called POTS (plain old telephone service), which is a network of lines and carrier equipment that provide landline telephone service to homes and businesses. Originally, the PSTN carried only analog traffic. All its lines were copper wires, and switching was handled by operators who manually connected calls upon request. Today, switching is computer controlled, and nearly all the PSTN uses digital transmission and fiber for backbone connections. Signals may deliver voice, video, or data traffic and travel over fiber-optic or twisted-pair copper cable connections.

The telephone company terminates lines and switches calls between different locations at the CO (central office). The portion of the PSTN that connects any residence or business to the nearest CO is known as the [**local loop**](javascript://), or the “last mile” (though it is not necessarily a mile long), as illustrated in [Figure 9-10](javascript://). It’s the part of the PSTN most likely to still use copper wire and carry analog signals. That’s because extending fiber-optic cable to every residence and business is costly. However, fully digital connections are increasingly common, especially for businesses that rely heavily on WAN connections. No matter what kind of media is used, the end of the local loop—and the end of the carrier’s responsibility for the network—is the customer’s demarcation point where wires terminate at the NIU.

**Figure 9-10**

Local loop portion of the PSTN



Enlarge Image

DSL can support multiple data and voice channels over a single line, but it can span only limited distances without the help of repeaters. Also, the distance between the customer and the central office affects the actual throughput a customer experiences. Close to the central office, DSL achieves its highest maximum throughput. The farther away the customer’s premises, the lower the throughput.

To understand how DSL and voice signals can share the same line, it’s helpful to note that telephone lines carry voice signals over a very small range of frequencies between 300 and 3300 Hz. This leaves higher, inaudible frequencies unused and available for carrying data. DSL uses data modulation techniques at the physical layer of the OSI model to achieve extraordinary data throughput over regular telephone lines. Recall that modulation techniques can allow a single channel to carry more data per cycle of a signal. Depending on its version, a DSL connection might use a modulation technique based on amplitude or phase modulation to alter the waves at higher frequencies to carry data. The types of modulation used by different DSL versions affect their throughput and the distance their signals can travel before requiring a repeater. Modulation is performed by a DSL modem. A [**DSL modem**](javascript://), such as the one shown in [Figure 9-11](javascript://), contains ports to connect both to your incoming telephone line and to your computer or network connectivity device.

**Figure 9-11**

A DSL modem



Source: Zoom Telephonics, Inc.

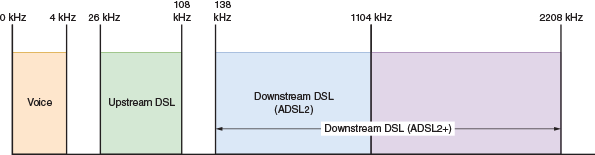
### Types of DSL

The types of DSL vary according to their throughput rates, data modulation techniques, capacity, and distance limitations, as well as how they use the PSTN. The term xDSL (extended DSL) refers to all DSL varieties. In each case, the x in xDSL is replaced by the variety’s name (there’s that algebra again). The better-known DSL varieties include the following:

* **ADSL (asymmetric DSL)**—Faster download speeds than upload speeds and is the most common form of DSL. Asymmetrical communication is well suited to users who receive more information from the network than they send to it—for example, people watching movies online or people surfing the web. ADSL and VDSL (discussed next) create multiple narrow channels in the higher frequency range to carry more data. For these versions, a splitter must be installed at the carrier and at the customer’s premises to separate the data signal from the voice signal before it reaches the terminal equipment (for example, the phone or the computer). The latest version of ADSL is ADSL2+, which extends the reach of DSL to within two kilometers of the provider’s location. It also provides a maximum theoretical throughput of 24 Mbps downstream and a maximum of 3.3 Mbps upstream (depending on how close it is to its source). The reason upstream and downstream bandwidth are different on a DSL line is because of the way the bandwidth is broken up for different purposes. [Figure 9-12](javascript://) shows the distribution of bandwidth for voice, upstream, and downstream communications.
* **VDSL (very high bit rate DSL or variable DSL)**—Faster than ADSL and is also asymmetric, with faster download speeds than upload speeds. A VDSL line that carries up to 52 Mbps in one direction and up to 16 Mbps in the opposite direction can extend only a maximum of 1.6 km before dropping to speeds similar to ADSL2+. VDSL2 offers throughput speeds nearing 100 Mbps in both directions but drops off quickly at even shorter distances. These limitations might suit businesses located close to a telephone company’s CO (for example, in the middle of a metropolitan area), but it won’t work for most individuals.
* **SDSL (symmetric DSL)**—Equal download and upload speeds maxing out around 2 Mbps. Symmetrical transmission is suited to users who both upload and download significant amounts of data—for example, a bank’s branch office that sends large volumes of account information to the central server at the bank’s headquarters and, in turn, receives large amounts of account information from the central server at the bank’s headquarters. SDSL cannot use the same wire pair that is used for voice signals. Instead, this type of DSL uses the extra pair of wires contained in a telephone cable (which are otherwise typically unused).

**Figure 9-12**

More bandwidth allocated for downstream than upstream



Enlarge Image

**Note 9-4**

Published distance limitations and throughput can vary from one service provider to another, depending on how far the provider is willing to guarantee a particular level of service. In addition, service providers may limit each user’s maximum throughput based on terms of the service agreement. For example, in 2011, AT&T capped the total amount of data transfer allowed for each of its DSL subscribers to 150 GB per month. The company instituted the new policy in response to a dramatic spike in downstream bandwidth usage due to Netflix streaming. In fact, in 2010, Netflix accounted for nearly 30 percent of all downstream Internet traffic requested by fixed users in the United States. Today, many providers cap a subscriber’s high-speed data usage, although typically the caps are higher now than the one in this example.

Telecommunications carriers and related vendors have positioned DSL as a competitor for cable broadband and leased line services. The installation, hardware, and monthly access costs for DSL are significantly less than the cost for other options, but the cost in comparison with cable broadband varies widely by location. At the time of this writing, DSL home Internet service costs approximately $35 per month in the United States, though prices vary by speed and location. Generally speaking, DSL throughput rates, especially upstream, are lower than cable broadband, which is its main competition among residential customers.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

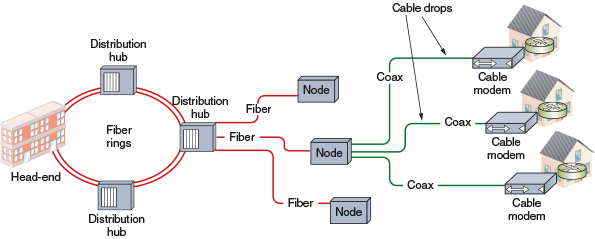
## 9-3bCable Broadband

While local and long-distance phone companies strive to make DSL the preferred method of Internet access for consumers, cable companies are pushing their own connectivity option. [**Cable broadband**](javascript://) (also called cable Internet or cable modem access) is based on the coaxial cable wiring used for TV signals, although in reality, much of the coaxial infrastructure has been replaced with fiber. Cable broadband was standardized by an international, cooperative effort orchestrated by CableLabs that yielded a suite of specifications called [**DOCSIS (Data Over Cable Service Interface Specifications)**](javascript://). Cable broadband service is typically offered at asymmetric speeds, such as up to 70 Mbps download and 7 Mbps upload. The newest DOCSIS standard, 4.0, theoretically allows for symmetric multi-gigabit speeds up to 10 Gbps downstream and 6 Gbps upstream, thus rivaling some fiber-optic Internet service options once experienced speeds start to approach the standard’s defined maximums.

In fact, many cable companies employ fiber cabling for a significant portion of their physical infrastructure. As illustrated in [Figure 9-13](javascript://), [**HFC (hybrid fiber coaxial)**](javascript://) networks use fiber-optic cabling to connect the cable company’s distribution center, or headend, to distribution hubs and then to optical nodes near customers. Either fiber-optic or coaxial cable then connects a node to each customer’s business or residence via a connection known as a cable drop.

**Figure 9-13**

HFC infrastructure



Enlarge Image

Cable broadband connections require that the customer use a special [**cable modem**](javascript://), a device that modulates and demodulates signals for transmission and reception via cable wiring (see [Figure 9-14](javascript://)). The cable modem must conform to the correct version of DOCSIS supported by the ISP. Most newer cable modems use DOCSIS 3.1 with 4.0 becoming available, but ISPs might charge extra when later modem models are used. [Table 9-3](javascript://) presents the versions of DOCSIS along with their specifications.

**Figure 9-14**

A cable modem



Source: Zoom Telephonics, Inc.

**Table 9-3**

### DOCSIS Versions and Specifications

| **Version** | **Maximum upstream throughput** | **Maximum downstream throughput** | **Description** |
| --- | --- | --- | --- |
| DOCSIS 1.x (1.0 and 1.1) | 10 Mbps | 40 Mbps | Outdated; single channel; throughput was shared among customers |
| DOCSIS 2.x (2.0 and 2.0 + IPv6) | 30 Mbps | 40 Mbps | Outdated; single channel; reduces disparity between upstream and downstream throughputs |
| DOCSIS 3.0 | 100 Mbps | 1000 Mbps | Multiple channels: minimum of 4, no maximum |
| DOCSIS 3.1 | 1–2 Gbps | 10 Gbps | In 2017, CableLabs published Full Duplex DOCSIS 3.1, which offers symmetrical Gigabit upload and download speeds. |
| DOCSIS 4.0 | 6 Gbps | 10 Gbps | Expanding upon DOCSIS 3.1 standards, CableLabs added RF bandwidth options for upstream speeds to support full-duplex, multigigabit throughput. |

Like DSL modems, cable modems operate at the physical and data link layers of the OSI model, and, therefore, do not manipulate higher-layer protocols like IP. The cable modem connects to a customer’s PC via the NIC’s RJ-45, USB, or wireless interface. Alternatively, the cable modem could connect to a networking device, such as a switch or router, thereby supplying bandwidth to a LAN rather than to just one computer. It’s also possible to use a device that combines cable modem functionality with a SOHO router to share available bandwidth on an entire network.

**Applying Concepts 9-2**

### Determine a Cable Modem’s DOCSIS Version

You can determine the DOCSIS version of a cable modem on a SOHO network with a little detective work. This activity requires a SOHO network serviced by cable broadband and a computer (Windows, Linux, or Mac) connected to the network. Alternatively, you can find a cable modem for sale online and use the posted information and photos for parts of this activity. Complete the following steps to identify the DOCSIS version of a cable modem:

1. 1

Examine the labels on the cable modem to determine the device’s manufacturer and model number. In some cases, the DOCSIS version might be printed on one of these labels. If you’re looking at a cable modem online, examine the posted specifications for this information. If the DOCSIS version isn’t labeled or posted, continue with the following steps.

1. 2

Research the manufacturer and model number information online. You might find the DOCSIS information while conducting your research. If not, the minimum information you need is the cable modem’s default internal IP address (such as 192.168.0.1 or 192.168.100.1) and admin username and password (if there is one).

1. 3

Choose one of the following options:

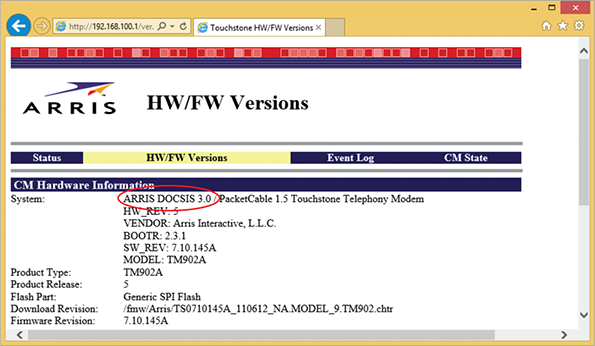
* 1. If you’re researching a cable modem listed online, check the manufacturer’s website for an emulator to interact with the cable modem’s user interface. Alternatively, you can choose a TP-Link cable modem emulator at [tp-link.com/us/support/emulator](http://tp-link.com/us/support/emulator" \t "_blank)**/**.
  2. If you’re working with a cable modem on your own network, enter the default internal IP address in a web browser and log on if necessary.

1. 4

Explore the user interface to locate the cable modem’s hardware information. [Figure 9-15](javascript://) shows the hardware information for a cable modem made by ARRIS. What is the DOCSIS version of your cable modem?

**Figure 9-15**

This cable modem’s DOCSIS version is 3.0



Enlarge Image

Source: ARRIS

Like DSL, cable broadband provides a dedicated and always-up, or continuous, connection that does not require dialing up a service provider to create the connection. Unlike DSL, cable broadband requires many subscribers to share the same local line, thus raising concerns about security and actual (versus theoretical) throughput. For example, if your cable company supplied you and five of your neighbors with cable broadband services, one of your neighbors could, with some technical prowess, capture the data that you transmit to the Internet. (Modern cable networks provide encryption for data traveling to and from customer premises; however, these encryption schemes can be thwarted.)

Moreover, the throughput of a cable line is fixed. As with any fixed resource, the more one person uses, the less that is left for others. In other words, the greater the number of users sharing a single line, the less throughput available to each individual user. Cable companies counter this perceived disadvantage by rightly claiming that at some point (for example, at a remote switching facility), a telephone company’s DSL bandwidth is also fixed and shared among a group of customers.

In the United States, cable broadband access costs approximately $30–$60 per month when bundled with cable TV and/or digital voice services. Cable broadband is less often used in businesses than DSL, primarily because most office buildings do not contain an existing coaxial cable infrastructure.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3cFiber

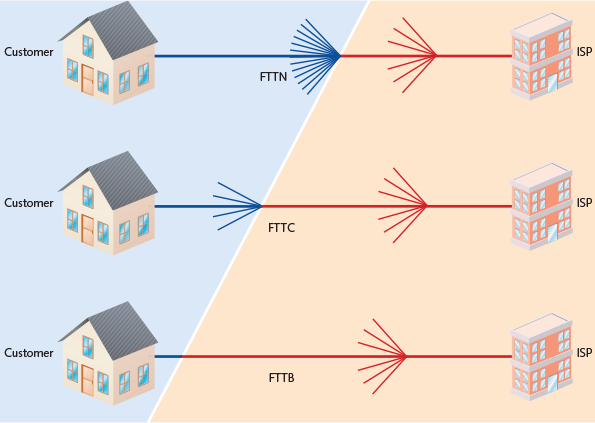
The fact is, most of the Internet backbone already runs on fiber. Even if you connect your new home office to the Internet via an old-school dial-up connection, most of the distance your data travels on the Internet will run over fiber cables. It’s that last mile to your location that really slows your data down. While DSL and cable broadband offer significantly faster speeds than dial-up, they’re still very slow by modern standards.

A growing trend in ISP offerings for WAN connection services is to offer FTTN (fiber-to-the-node), FTTH (fiber-to-the-home), or similar arrangements. In these scenarios, the ISP runs a fiber connection to one of a few nearby locations, as illustrated in [Figure 9-16](javascript://) and described next:

* **FTTN (fiber-to-the-node** or **fiber-to-the-neighborhood)**—A nearby service junction that serves a few hundred customers
* **FTTC (fiber-to-the-curb)**—A nearby pole or equipment cabinet that serves a few customers
* **FTTB (fiber-to-the-building)** or **FTTH (fiber-to-the-home)**—The junction box at the demarc to your building

**Figure 9-16**

Getting fiber closer to your own network increases your Internet speeds



Enlarge Image

As you can see, each progressive scenario brings the fiber closer to your own network. The closest options cost more but also reduce the distance over which your data must traverse copper cabling.

While this option has limited availability in many market areas, those who can choose fiber often do. Fiber’s higher speeds, with symmetric speeds often reaching as high as 1–2 Gbps for home or small business fiber services, offset the increased cost of up to $100 monthly. Additionally, so long as the ISP can provide you with a fiber connection, your distance from their offices won’t negatively affect your experienced speeds.

Fiber technology and availability to business customers—and even to residential customers—continues to improve. Rising market demand for last-mile fiber service is causing increased investments by ISPs into their access-level fiber infrastructure. Traditionally, fiber investment focused on long-haul connections across hundreds and thousands of miles. In contrast, [**MONs (metropolitan optical networks)**](javascript://) bring fiber to the customer. This dense, localized grid of junctions and fiber cables attempts to make direct fiber connections available to as many customers as possible while balancing the significant expense of replacing existing telephone and coaxial cable infrastructure with fiber equipment and fiber-optimized technologies.

You’ve already learned about some of the technologies that handle multiple signals on each fiber connection, such as DWDM (dense wavelength division multiplexing). However, DWDM does not easily lend itself to handling the high numbers of communications channels and the wide variety of network protocols needed within a metro network environment. This mismatch between what pre-existing fiber technology was designed to do and what is needed in the metro market is sometimes referred to as the “metro gap.” In response to these emerging needs, newer technology has been developed or adapted to support MONs and the expectations of customers in these markets. With 100 Gbps speeds already available on long-haul connections, the industry is now aiming for similar speeds for MONs on the ISP’s end of broadband fiber connections.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3dLeased Lines

When you first established your imaginary company at the beginning of this section, broadband access to the Internet from your basement office was sufficient. Perhaps you began with cable or DSL and then, as you started to earn profits, you moved to a fiber connection. Excitingly, your business continued to grow. Within a few months, your basement was no longer large enough to hold all your inventory. Initially, you rented storage space in a small warehouse while you continued to work from home. But soon you realized you were spending several hours a week at the storage unit and out of touch with your customers and small group of employees. You moved into a larger warehouse rental that included office space, and you decided to open two storefronts, one in your hometown and another in a neighboring city.

At this point, you realize your broadband Internet connection can no longer provide the support your business needs. Instead of basic Internet access, you need to connect your three locations with higher and more reliable throughput speeds to support the following activities:

* VoIP calls with customers and vendors
* E-commerce traffic to your website
* Sales activity from physical storefronts
* Upload and download traffic to exchange large graphic files with customers

You call your local ISP asking how to get dedicated WAN connections. The ISP suggests that you consider [**leased lines**](javascript://) for each location, which would provide dedicated bandwidth on fiber optic connections. What are the advantages and disadvantages of this option for your business?

Where fiber broadband offers the benefits of fiber optic technology, leased fiber takes all that speed boost and pools the bandwidth for a single customer. While a leased line’s dedicated bandwidth might be listed at a lower speed than the maximum theoretical speeds advertised for fiber broadband services, a dedicated line offers the following advantages:

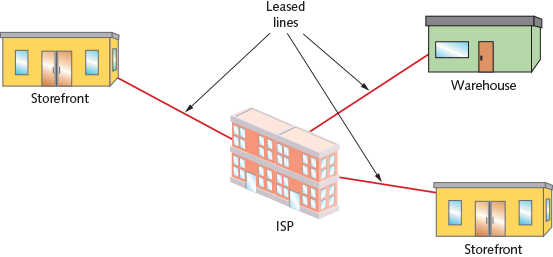
* **Dedicated bandwidth**—The customer pays for a specific bandwidth (such as 2 Gbps) and reserves that bandwidth for their sole use without having to share it with other customers. Throughput won’t fluctuate in response to traffic demands from other customers.
* **Symmetrical bandwidth**—Leased line speeds are typically symmetrical, meaning upload and download speeds will be the same.
* **SLA-backed guarantee**—Performance is backed by SLA-enforced uptime, repair time, and possibly backup options (such as having a broadband connection available during an outage). If bandwidth falls below a defined threshold, the customer has options for recourse to protect their business activities during the outage.

When subscribing to a leased line, existing fiber optic cabling can be configured for the leased line, or a dedicated fiber optic cable must be installed to connect the customer to the nearest ISP exchange, or PoP (Point of Presence). Some of this installation cost is covered by the ISP, but certain expenses might be charged back to the customer. Alternatively, new cables can be installed to directly connect a business’s own locations. For example, each branch office might have a direct line to the company’s own headquarters.

Ongoing monthly costs of a leased line vary greatly depending on many factors, including required bandwidth and the distance to the ISP’s exchange or between the company’s own locations. Typical costs will range between $300 and $1000 monthly. This can get especially expensive for multiple leased lines, as shown in [Figure 9-17](javascript://). However, this particular arrangement gives each location allotted bandwidth directly to the ISP and on to the Internet. From the ISP’s central office, communications between your locations (such as between the warehouse and a storefront) traverse the ISP’s high-speed backbone network to connect the two leased lines. Further, more locations can easily be added to the company’s leased line network by subscribing to a new leased line for each new location. Alternatively, sometimes what’s needed is a point-to-point leased line between two customer locations. In this case, the ISP cannot provide supportive services, such as monitoring uptime or optimizing VoIP traffic.

**Figure 9-17**

Each location needs its own leased line



Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

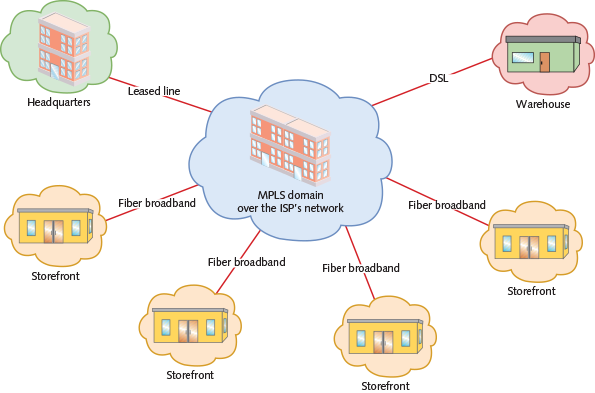
## 9-3eMPLS (Multiprotocol Label Switching)

Your leased lines serve the company well for nearly two years. Both storefronts quickly gain a loyal customer following, and you’re able to optimize your logistics at the warehouse to efficiently service both storefronts and all website customers. As the word spreads and business continues to boom, you decide over the next year to open three more storefronts throughout your region. You also recognize your warehouse space is no longer sufficient, and your employees are tightly cramped in the existing office space. These growing pains lead to the decision to move to a standalone warehouse space and to open a headquarters office in a separate location. With all these new locations to network, managing so many leased lines is becoming unfeasible. Further, you’re told by your IT staff that leased lines don’t offer the level of nuanced control they need for handling the different types of applications on your network. Their suggested solution: MPLS.

[**MPLS (multiprotocol label switching)**](javascript://) was introduced by the IETF (Internet Engineering Task Force) in 1999. As its name implies, MPLS enables multiple types of layer 3 protocols to travel over any one of several connection-oriented layer 2 protocols. Essentially, MPLS allows you to use any connectivity option for each site that makes sense while centrally managing bandwidth between each site. For example, in [Figure 9-18](javascript://), you might have your warehouse connected to the ISP using DSL while your storefronts use fiber broadband and your central office has a leased line.

**Figure 9-18**

MPLS provides cohesive WAN management for multiple connection types



Enlarge Image

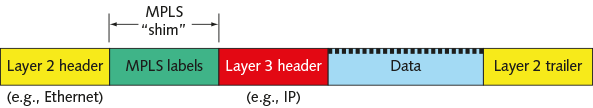
Despite the various service levels of each location’s connection to the ISP, you can manage segmentation and QoS for different types of traffic across your entire network, even if your locations are spread hundreds or thousands of miles apart. These advantages are explained next:

* [**QoS (quality of service)**](javascript://) refers to a group of techniques for adjusting the priority assigned to various types of traffic. For example, you might want to prioritize VoIP traffic over email traffic. One of the characteristics that sets MPLS apart from other WAN technologies is its ability to support QoS traffic shaping across WAN connections.
* Additionally, you can set routes for traffic between sites so the ISP’s routers don’t have to stop and think with each packet where that packet should go next. Essentially, MPLS lets routers function more like switches, working with information in layer 2 headers instead of having to dig to layer 3 and process routing information. This saves time and reduces latency.

With MPLS, the first ISP router (the provider’s edge router, also called the MPLS ingress router) receives a message in a data stream and adds one or more labels to the layer 3 packet. These MPLS labels together are sometimes called a shim because of their placement between layer 3 and layer 2 information. For this reason, MPLS is sometimes said to belong to “layer 2.5.” Next, the network’s layer 2 protocol header is added, as shown in [Figure 9-19](javascript://).

**Figure 9-19**

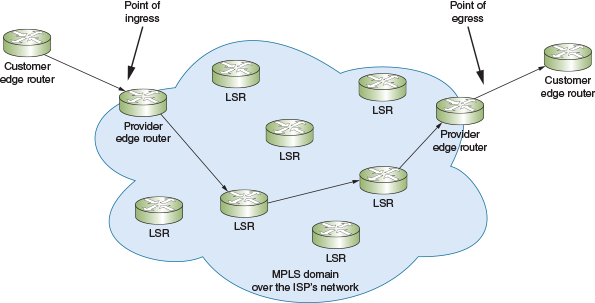
MPLS shim within a frame



These MPLS labels include information about where the router should forward the message next and, sometimes, prioritization information. Each router in the data stream’s path (see [Figure 9-20](javascript://)) revises the label to indicate the packet’s next hop. In this manner, routers on a network can take into consideration network congestion, QoS indicators assigned to the messages, plus other criteria; however, these transit routers, called LSRs (label switching routers), don’t have to take time to map a path for the messages. Network engineers maintain significant control in setting these paths. Consequently, MPLS offers potentially faster transmission than traditionally routed networks.

**Figure 9-20**

Label switching routers simply forward the message without calculating routes



Enlarge Image

While MPLS does offer decreased latency, this benefit is not quite as noticeable today as it was when MPLS first became available. The primary benefits of MPLS today include the following:

* MPLS connections are highly scalable for businesses, which means a business can add more and longer connections for less cost than similarly scaled leased lines.
* Customers can prioritize their own traffic across the WAN according to QoS attributes, such as giving VoIP traffic higher priority over email traffic.
* The ability to label traffic offers more reliability, predictability, and security (when properly implemented) than when using cheaper connections over the open Internet.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3fCloud Connectivity Options

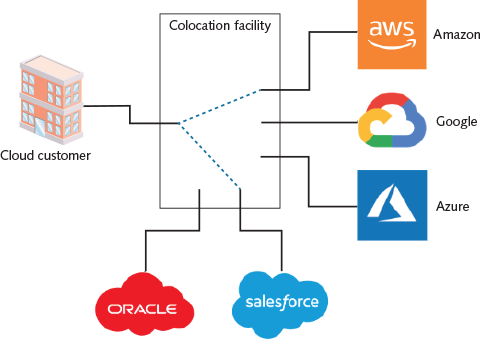
Over the next few months, as you’re working through the growing pains of adding new storefronts and moving offices, your IT team suggests some additional improvements to your network configurations that will better serve your company into the next phase. Primarily, they suggest that you migrate many of your network resources to the cloud. For example, you don’t need to host your own email servers, and running your website from the cloud will allow that resource to scale as needed without having to purchase new hardware in the future. You give your team the green light to begin the migration of a few servers with the intent of a larger scale migration when the transition to your new offices is scheduled to be completed.

During the initial migration, your team sets up a group of VPN (virtual private network) connections to your cloud resources from each of your company locations. This process requires the installation of a VPN device at each location. The VPNs travel over each location’s Internet connection, giving employees direct and secure access to your first few cloud resources like email and, eventually, to a lot more resources like the customer database and HR tools.

At first, the VPNs work well enough. Later in the year, as the cloud migration nears completion, it becomes obvious that a VPN will not be sufficient for the home office. Instead, your cloud provider recommends a [**private-direct connection**](javascript://), or [**interconnection**](javascript://), to their cloud infrastructure. In this scenario, you lease a dedicated line from your ISP to one of your cloud provider’s PoPs, or colocation facilities (see [Figure 9-21](javascript://)). From there, you pay for the connection to the cloud provider’s physical infrastructure and, usually, some kind of data transfer fees (such as $.02 per GB transferred out of the cloud provider’s network).

**Figure 9-21**

A colocation facility offers connections to multiple cloud platforms



As you research your cloud provider’s available PoP locations, you realize the colocation you’ve chosen also offers private-direct connections with another cloud provider your team has been considering for a multicloud deployment. The cost efficiency of leasing a single direct line to this colocation will more than pay for itself over time now that you can use the same physical line for multiple purposes. This benefit also opens additional opportunities to host more resources in your hybrid cloud, including virtual desktops for your home office.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3gSoftware-defined WAN (SD-WAN)

Over the next couple of years, you settle into your new offices. All your stores and your website continue to thrive. Customers are happy, and so are your employees. Suddenly, a random social media video featuring some of your products goes viral on the Internet, and you start getting a rapid increase in website traffic. Interestingly, much of that traffic originates from three Asian countries. Order volumes to these countries spike. You’re sure it won’t last long, but six months later, these sales numbers have only increased. As you further investigate your popularity explosion in these countries, you make some connections with new business associates in those areas. Casual chit-chat turns into some serious discussion about expanding your company into India and Thailand. You’re committed to hiring locals to provide everything from order management and HR to customer support. At the same time, this expansion will require a significant investment in new overseas locations for storefronts, offices, and a warehouse, which also means needing new WAN connections.

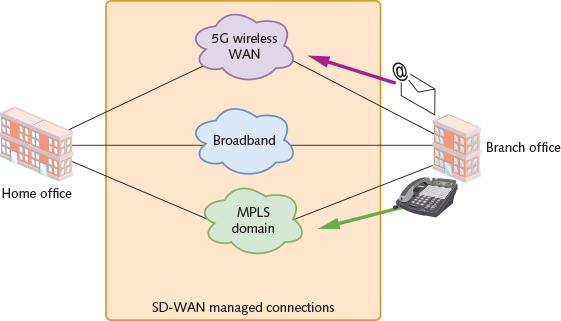
As you discuss the pending expenditure in these other countries with your IT team, you realize the need for centralized management of company network resources. MPLS connections all the way to Asia won’t suffice to meet your company’s needs over the coming years. Instead, your team suggests a newer solution called SD-WAN.

Similar to its SDN cousin, [**SD-WAN (software-defined wide area network)**](javascript://) relies on abstracted, centralized control of networking devices to manage network functions across a diverse infrastructure. SD-WAN offers the following benefits:

* **Transport agnostic**—As shown in [Figure 9-22](javascript://), an SD-WAN controller can manage network configurations at multiple locations throughout the world, regardless of the type of connection each segment uses to reach the SD-WAN (such as broadband, leased line, MPLS, cellular, and others).
* **Active-active load balancing and automatic failover**—An SD-WAN managed network offers active-active load balancing where it can choose the best physical WAN connection for different types of traffic according to traffic prioritization and current network conditions. For example, suppose a branch office has three Internet connections as shown in [Figure 9-23](javascript://): an MPLS connection, a broadband connection, and a 5G wireless connection. SD-WAN can route traffic over each of these connections according to each data stream’s configured priority. If one WAN connection goes down, the SD-WAN controller can switch traffic to another WAN connection.
* **Intent-based management**—A network admin can indicate in the controller’s GUI their intent for traffic, such as limiting bandwidth for a specific application, and the SD-WAN controller institutes all configuration changes needed on all affected network devices.
* **Zero-touch provisioning**—An SD-WAN edge device can be shipped to a branch location where a non-technical person can plug in the device without any configuration needed on-site. The device then finds and checks in with the remote SD-WAN controller for further instructions. Trained technicians at the home office can remotely finish deploying the SD-WAN configurations at the branch office without any additional assistance from on-site personnel.
* **Reduced cost**—Because SD-WAN solutions can be deployed over any kind of underlying WAN connection (such as cable, DSL, fiber broadband, or 5G), expensive leased lines and MPLS connections can be abandoned in favor of SD-WAN management for many of a company’s connections. While the company might not replace all their MPLS or leased line connections, SD-WAN can be used to optimally manage all available WAN connections and minimize the need for more expensive WAN services.

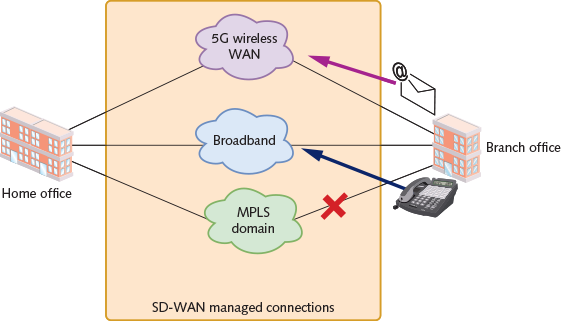
**Figure 9-22**

SD-WAN supports many underlying WAN connectivity technologies



**Figure 9-23**

The SD-WAN controller can direct traffic through the optimal path for that traffic at a given time



Improvements to SD-WAN technologies are still needed surrounding security when traffic traverses the Internet, costs for underlying WAN connections (such as MPLS), and flexibility for cloud and mobile users. Still, the advantages offered by SD-WAN are causing an industry shift away from older, more traditional WAN connectivity options.

Your fictional company has used a wide variety of wired WAN technologies through its journey from your basement to its global presence. Similar to LANs, WANs utilize multiple wireless technologies as well. You’ll read about two of the most common of these in the next section.

**Applying Concepts 9-3**

### Explore Internet Connection Options in Your Area

Selecting a particular WAN solution because its theoretical maximum speed is faster than another solution’s theoretical maximum speed won’t help much if your local carrier doesn’t actually offer service at that speed. Selecting a WAN solution for a corporation requires familiarity with the options available in your area and their actual performance levels relative to each other. Complete the following steps to evaluate the ISP options available to a business in your area:

1. 1

Compile a list of ISPs in your town or city. If you live in a rural area with few options, select a nearby city with more options so that you’ll be able to include some of the private WAN technologies in addition to residential WAN offerings.

1. 2

Check the website for each ISP to determine what broadband and dedicated services they offer in your area, both for residential customers and corporate customers. Include both wired and wireless options. Answer the following questions:

* 1. What are their advertised speeds?
  2. How much does each solution cost on a monthly basis?
  3. What installation fees are there, if any?
  4. How far away are you located from their CO? (If you’re researching another city besides your own, use a fictional location in that same city.)
  5. What effect will this distance likely have on the actual speeds of each service option?

1. 3

Search online for consumer reviews of each ISP in your list. What kinds of ratings does each ISP receive online?

**Remember This…**

* Explain various WAN services, including DSL, cable, MONs, leased lines, MPLS, cloud connectivity options, and SD-WAN.
* Use a bandwidth speed tester to check a WAN connection’s speed.

**Self-Check**

1. You just moved into a rural office space that has telephone service but no cable. Which WAN service could you use without needing to install new wiring to your location?

Answer

* 1. Fiber broadband
  2. DSL
  3. Leased fiber
  4. Cable broadband

1. Which of these WAN services is backed by an SLA?

Answer

* 1. DSL
  2. Leased line
  3. Fiber broadband
  4. Cable broadband

1. Which WAN service offers active-active load balancing?

Answer

* 1. Cable broadband
  2. DSL
  3. SD-WAN
  4. Fiber broadband

**You’re Ready**

You’re now ready to complete [Project 9-3: Create WAN Links in Packet Tracer](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-4Wireless WANs

### Certification

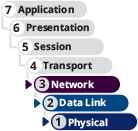
* 1.2

Explain the characteristics of network topologies and network types.

* 2.4

Given a scenario, install and configure the appropriate wireless standards and technologies.

Average reading time: 16 minutes



The best 802.11ac signal can travel approximately a quarter of a mile. But other types of wireless networks can connect stations over much longer distances. For example, in large cities, dozens of surveillance cameras trained on municipal buildings and parks beam video images to central public safety headquarters. Meanwhile, in developing countries, wireless signals deliver lectures and training videos to students in remote, mountainous regions. In rural areas of the United States, elderly patients at home wear medical monitoring devices, such as blood pressure sensors and blood glucose meters, which use wireless networks to convey information to their doctors hundreds of miles away. Such networks can even alert paramedics in case of an emergency. All of these are examples of wireless WANs. Unlike wireless LANs, wireless WANs are designed for high-throughput, long-distance digital data exchange. The following sections describe a variety of ways wireless clients can communicate across a city or state.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

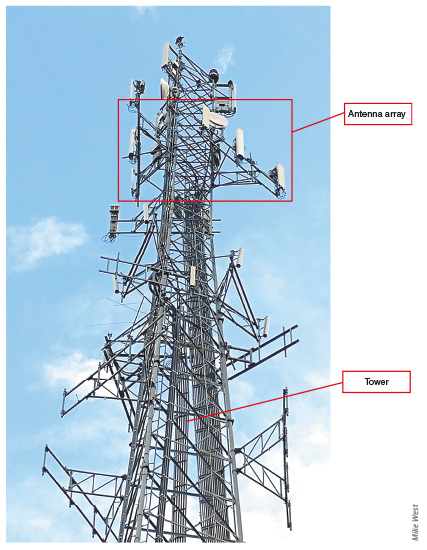
## 9-4aCellular

Cellular networks were initially designed to provide analog phone service. However, since the first mobile phones became available to consumers in the 1970s, cellular services have changed dramatically. In addition to voice signals, cellular networks now deliver text messages, web pages, music, and videos to smartphones and other handheld devices. Cellular networking is a complex topic, with rapidly evolving encoding and access methods, changing standards, and innovative vendors vying to dominate the market. This module does not detail the various encoding and access methods used on cellular networks. To prepare you for the CompTIA Network+ exam, this section describes current cellular data technology and explains the role it plays in wide area networking.

Although their access methods and features might differ, all cellular networks share a similar infrastructure in which coverage areas are divided into cells. Each cell is served by an antenna array and its base station, together called a [**cell site**](javascript://). The tower—the tall part you can easily see from a distance—is often owned by a third-party entity similar to how owners of office buildings or malls lease out portions of their property to other businesses. Cellular providers lease space on the towers for their antenna arrays, as shown in [Figure 9-24](javascript://), and space on the ground for base station equipment.

**Figure 9-24**

This tower offers space for several antenna arrays



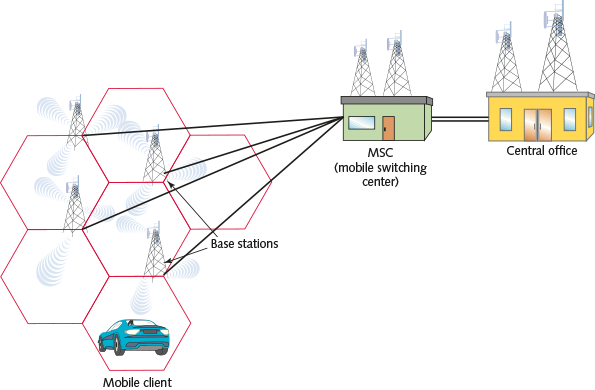
Enlarge Image

Mike West

At the base station, a controller assigns frequencies to mobile clients and manages communication with them. In network diagrams, cells are depicted as hexagons. Multiple cells share borders to form a network in a honeycomb pattern, as shown in [Figure 9-25](javascript://). Antennas are positioned at three corners of each cell, radiating their signals and providing coverage over three equidistant lobes. When a client passes from one coverage area to another, the mobile device begins communicating with a different antenna. Its communication might change frequencies or even carriers between cells. The transition, which normally happens without the user’s awareness, is known as a handoff.

**Figure 9-25**

Cellular network



Enlarge Image

Cell sizes vary from roughly 1000 feet to 12 miles in diameter. The size of a cell depends on the network’s access method and the region’s topology, population, and amount of cellular traffic. An urban area with dense population and high volume of data and voice traffic might use cells with a diameter of only 2000 feet, their antennas mounted on tall buildings (see [Figure 9-26a](javascript://)) or disguised to look like landscaping (see [Figure 9-26b](javascript://)). In sparsely populated rural areas, with antennas mounted on isolated hilltop towers, cells might span more than 10 miles. In theory, the division of a network into cells provides thorough coverage over any given area. In reality, cells are misshapen due to terrain, EMI, and antenna radiation patterns. Some edges overlap and others don’t meet up, leaving gaps in coverage.

**Figure 9-26**

a) Cellular antennas on a tall building; b) A concealed tower



Enlarge Image

Chichimaru/ [Shutterstock.com](http://shutterstock.com/" \t "_blank); Cary Kalscheuer/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

As shown earlier in [Figure 9-25](javascript://), each base station is connected to an MSC (mobile switching center), also called an MTSO (mobile telecommunications switching office), by a wireless link or fiber-optic cabling. The MSC might be located inside a telephone company’s central office or it might stand alone and connect to the central office via another fiber-optic cable or a microwave link. At the MSC, the mobile network intersects with the wider wired network. Equipment at an MSC manages mobile clients, monitoring their location and usage patterns, and switches cellular calls. It also assigns each mobile client an IP address. From the switching center, packets sent from cellular networks are routed to wired data networks through backbones using WAN technologies you learned about earlier in this module.

To put today’s services in context, it’s useful to understand that each leap in cellular technology has been described as a new generation. Each successive generation has brought a greater range of services, better quality, and higher throughputs, as described in the following list:

* 1G (first generation) services from the 1970s and 1980s were analog.
* 2G (second generation) services in the 1990s used digital transmission and paved the way for texting and media downloads on mobile devices. Data transmission on 2G systems didn’t exceed 240 Kbps.
* [**3G (third generation)**](javascript://) services were released in the early 2000s. Data rates rose to 384 Kbps. To switch to fully digital transmissions, two competing 2G technologies emerged as market leaders for 3G, as follows:
  + [**GSM (Global System for Mobile Communications)**](javascript://) is an open standard that is accepted and used worldwide. Digital communication of data is separated by timeslots on a channel using [**TDMA (time division multiple access)**](javascript://), which is similar to TDM (time division multiplexing). The primary difference is that multiplexed TDM signals all come from the same source (such as a router), while multiplexed TDMA signals come from several sources (such as several smartphones in the same vicinity). First introduced with the release of 2G devices, GSM initially only provided voice communications but added data services with the evolution of GPRS (General Packet Radio Services) and EGPRS (Enhanced GPRS), also called EDGE (Enhanced Data rates for GSM Evolution). GSM networks require that a cellular device have a [**SIM (Subscriber Identity Module) card**](javascript://) containing a microchip to hold data about the subscription a user has with the cellular carrier.
  + [**CDMA (Code Division Multiple Access)**](javascript://) differs from GSM in that it spreads a signal over a wider bandwidth so multiple users occupy the same channel, a technology called spread-spectrum. Codes on the packets keep the various calls separated. CDMA networks do not require a SIM card in a cellular device because devices are compared against a whitelist, which is a database of subscribers that contains information on their subscriptions with the provider. However, CDMA networks (such as Verizon’s) still require SIM cards to use their LTE (Long Term Evolution) features. While CDMA and GSM co-exist in the United States, globally GSM is by far the more popular technology.
* [**4G (fourth generation)**](javascript://) services are characterized by an all-IP network for both data and voice transmission. 4G standards, released in 2008, specify minimum throughputs of 100 Mbps with the goal of supporting 1 Gbps speeds. Variations of 4G include the following:
  + [**LTE (Long-Term Evolution)**](javascript://) is essentially the result of a marketing debacle. 4G standards were released ahead of their time, that is, before available hardware was capable of providing the required speeds to qualify as 4G. However, the new 4G protocols and techniques that did work supported better speeds than 3G, and cellular providers had already begun marketing new 4G networks and devices. So LTE became an ambiguous marketing term that meant “faster than 3G but not really 4G.” As hardware has improved, so have LTE speeds. Typical speeds now for LTE connections might reach 100 Mbps download and up to 75 Mbps upload.
  + [**LTE-A (LTE-Advanced)**](javascript://) can more realistically approach 4G standards. Sometimes misleadingly called 5G E (5G Evolution), LTE-A is basically true 4G as defined back in 2008 but only recently emerging in real-world networks.
* [**5G (fifth generation)**](javascript://) services require minimum speeds of 1 Gbps and max out at 20 Gbps download and 10 Gbps upload; however, actual speeds vary greatly. The 5G standards were initially released in 2016; cellular companies began deploying 5G infrastructure and devices in 2019. Note that the term 5G is completely unrelated to the 5-GHz band used by Wi-Fi. The following technologies contribute to 5G improvements:
  + **Bands**—One factor in experienced speeds is the band used. Some 5G providers (such as T-Mobile) have focused on building out widely available 5G infrastructure using the same lower bands that 4G uses, resulting in only moderately improved speeds. Other 5G providers (such as Verizon) are focusing instead on higher-density but less widely available infrastructure that uses new and smaller millimeter-wave frequencies in a newly available higher band. These dense but weaker frequencies provide high speeds for short distances while offering much lower resilience across long distances or when crossing obstacles such as walls and landscaping. When you are standing near a cell site, you could experience a strong 5G signal (with speeds easily exceeding 1 Gbps). But that speed could plummet to closer to 4G speeds at 200–300 Mbps if you walk around the corner of a nearby building or stand behind a tree.
  + **Cell density**—To reach a reasonable level of availability and effectiveness, many small 5G antennas must be installed in close proximity to each other so 5G clients can receive a close and strong signal throughout the coverage area.
  + **Channels**—5G works to increase speeds by using wider channels, similar to how Wi-Fi’s 5-GHz band can be bonded into larger channels. Where 4G uses up to seven 20-MHz channels, 5G can use up to eight 100-MHz channels in the high band, which ranges from 20 to 100 GHz. Low band 5G (narrow but long-reaching frequencies) uses the same channels as 4G under 2 GHz. Mid band 5G (in the range of 2–10 GHz) offers two 100-MHz channels with the ability to stack low-band 20-MHz channels.
  + **Client volume**—While 5G cells must be placed closer together so millimeter-wave frequencies can reach clients, each cell site can support more clients. This will work well for sensor networks and IoT devices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4bSatellite

In 1945, Arthur C. Clarke (the author of 2001: A Space Odyssey) wrote an article in which he described the possibility of communication between manned space stations that continually orbited the Earth. Other scientists recognized the value of using satellites to convey signals from one location on Earth to another. By the 1960s, the United States was using satellites to transmit telephone and television signals across the Atlantic Ocean. Since then, the proliferation of this technology and reductions in its cost have made satellite transmission appropriate and available for transmitting consumer voice, video, music, and data.

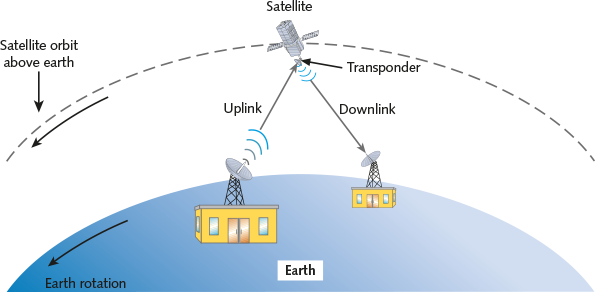
### Satellite Orbits

Most satellites circle the Earth 22,300 miles above the equator in a geosynchronous orbit. GEO (geosynchronous earth orbit) satellites orbit the Earth at the same rate as the Earth turns. A special case of geosynchronous orbit, called geostationary orbit (because it appears stationary from Earth), stays directly above the equator. This is especially common with communications satellites. Consequently, at every point in their orbit, the satellites maintain a constant distance from a specific point on the Earth’s equator.

Satellites are generally used to relay information from one point on Earth to another. Information must first be transmitted to the satellite from Earth in an uplink from an Earth-based transmitter. Often, the uplink signal information is scrambled (in other words, its signal is encoded) before transmission to prevent unauthorized interception. At the satellite, a transponder receives the uplink signal, then transmits it to an Earth-based receiver in a downlink. Each satellite uses unique frequencies for its downlink. These frequencies, as well as the satellite’s orbit location, are assigned and regulated by the FCC. Back on Earth, the downlink is picked up by a dish-shaped antenna. The dish shape concentrates the signal so that it can be interpreted by a receiver. [Figure 9-27](javascript://) provides a simplified view of satellite communication.

**Figure 9-27**

Satellite communication



Enlarge Image

Geosynchronous earth orbiting satellites are the type used by the most popular satellite data service providers. This technology is well established, and it’s the least expensive of all satellite technology. Also, because many of these satellites remain in a fixed position relative to the Earth’s surface, stationary receiving dishes on Earth can be counted on to receive satellite signals reliably, weather permitting.

### Satellite Internet Services

A handful of companies offer high-bandwidth Internet access via GEO satellite links. Each subscriber uses a small satellite antenna and receiver, or satellite modem, to exchange signals with the service provider’s satellite network. Clients may be fixed, such as rural residents who are too remote for DSL, or mobile subscribers, such as travelers on ocean-going yachts.

Clients can exchange signals with satellites as long as they have a line-of-sight path from an unobstructed view of the sky. To establish a satellite Internet connection, each subscriber must have a fixed dish antenna, which is approximately 2 feet high by 3 feet wide (see [Figure 9-28](javascript://)). In North America, these dish antennas are pointed toward the Southern Hemisphere (because many geosynchronous satellites travel over the equator). The dish antenna’s receiver is connected via cable to a modem. This modem typically uses an Ethernet interface to connect with the subscriber’s router or computer.

**Figure 9-28**

A small satellite dish provides Internet connection



Andrey\_Popov/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

As with several other wireless WAN technologies, satellite services are typically asymmetrical, and bandwidth is shared among many subscribers. Throughputs vary and are controlled by the service provider. Downlink speeds might reach 100 Mbps, while uplink rates are much slower. Compared with other wireless WAN options, satellite services are slower and suffer more latency. In addition, the inconsistent latency causes jitter problems, degrading signal quality. Given these drawbacks, satellite data service is preferred only in circumstances that allow few alternatives or in cases where satellite receiving equipment is already installed.

**Remember This…**

* Explain cellular and satellite Internet options.
* Compare cellular technologies, including 3G, 4G, 5G, LTE, CDMA, and GSM.

**Self-Check**

1. Which cellular generation was the first to offer speeds up to 1 Gbps?

Answer

* 1. 2G
  2. 3G
  3. 4G-LTE
  4. 4G

1. Which wired WAN service offers speeds most comparable to the highest satellite Internet speeds in a similar price range?

Answer

* 1. DSL
  2. Cable broadband
  3. Fiber broadband
  4. Leased fiber

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-5Troubleshooting Connections

### Certification

* 3.1

Given a scenario, use the appropriate statistics and sensors to ensure network availability.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

* 5.5

Given a scenario, troubleshoot general networking issues.

Average reading time: 21 minutes

As a network administrator, one of your primary responsibilities is to keep connections within and between networks working well. With this in mind, there are steps you can take to troubleshoot a problem with a WAN connection before contacting your ISP, and there are preventive measures you can perform to avoid having the problem in the first place.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5aInternet Connectivity Issues

When you lose Internet connectivity, a little troubleshooting can help determine the location of the problem and the party responsible for repairing the connection. The following list presents some common issues to look for on your own equipment:

* **Interference**—Obviously, interference can cause problems with a wireless connection, and you have already learned that interference can wreak havoc with wired connections as well. Intermittent problems or problems that affect unrelated portions of a network are common indicators of interference issues.
* **DNS issues**—Correct DNS server information and a functioning DNS server are critical requirements for enabling Internet access. Computers can be programmed to use DNS servers on a corporate network or the ISP’s DNS servers, or alternatively, they can be pointed to public DNS servers such as those run by Google or Cloudflare.
* **Router misconfiguration**—Routing tables with incorrect routes can result in dropped messages with no error feedback. Other router configuration issues to consider when Internet connectivity fails might include blocked ports that should be open, speed or duplex mismatches, incorrect IP address range or subnet mask, or an incorrect default gateway. Similarly, attackers can take advantage of some types of router misconfigurations that result in network failure due to an attack. You’ll learn more about router security later in this course.
* **Interface error**—Misconfigured interfaces, such as an incorrect default gateway or missing DNS server addresses, can result in interface errors. One possible evaluation technique for bypassing an interface error, which will help confirm that the interface misconfiguration is the issue, is to switch to a different interface on the same device. For example, if your computer’s wired connection is having problems, try connecting to the network using the computer’s wireless interface.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5bInterface Problems

Interface problems can be challenging to track down. Several commands provide insights into device and interface performance, vulnerabilities, and misconfigurations that might be causing problems. A thorough device configuration review can often locate problems that don’t necessarily generate symptoms pointing directly to their cause. On routers and switches, this requires checking overall device configuration as well as individual interface configurations. The following discussion focuses on Cisco devices so you can practice using these commands in Packet Tracer. However, most other networking brands, such as Juniper and Huawei, use similar commands and modes to accomplish similar tasks.

With Cisco devices, recall that different commands are available depending on the mode you’re in. For example, when you first start working with a router, you begin in the user EXEC mode. To step up to the privileged EXEC mode, you enter enable, which can also be abbreviated as simply en. [Table 9-4](javascript://) explains the most used modes on Cisco routers and switches.

**Table 9-4**

### Cisco CLI Modes

| **Mode** | **Default prompt on a router** | **Command to enter mode** | **Description** |
| --- | --- | --- | --- |
| User EXEC | Router> | Login to device | Offers limited commands to evaluate current configurations without making changes to the configuration. |
| Privileged EXEC | Router# | enable or en | Typically requires a password and offers access to all EXEC commands, which provide tools for testing and helpful information about the current configurations. You can also run EXEC commands from other modes by prefacing the EXEC command with the do command. |
| Global configuration | Router(config)# | configure terminal or conf t | Allows device configuration changes and gives access to more specific configuration modes. |
| Interface configuration | Router(config-if)# | interface or int | Allows configuration changes to an interface. Specific configuration modes for features or protocols allow changes to configurations such as interfaces, DHCP, and routing. Configuration submodes and subsubmodes dig deeper into configuration options. |

Enlarge Table

To take one step down from a higher mode into a lower mode, enter the exit command. From any higher mode, enter the end command or press Ctrl+Z to return to privileged EXEC mode.

### Show Config

As you’ve seen in the Capstone Projects, when making a configuration change to a Cisco device, those changes are held in the running configuration file. You can see the device’s running-config file with the command show running-config (or sh run). The output is likely several pages long. Use the following keys to navigate the output:

* Press Enter to move down one line at a time.
* Press the spacebar to move down one page at a time.
* Press Tab or the down arrow to exit the output.

The temporary running-config file is held in the device’s RAM and is, therefore, reset when the device is restarted. To make your changes persist beyond a device’s power cycle, you must copy the running-config file to the startup-config file with the command copy running-config startup-config (or copy run start).

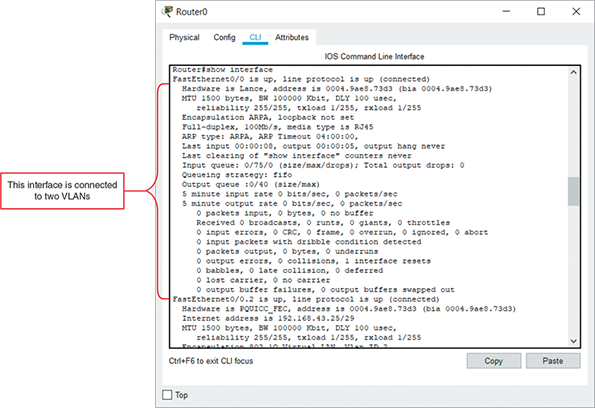
The startup-config file is not stored in RAM but instead is stored in NVRAM, which persists through a power cycle. To see the device’s stored startup-config file, enter the command show startup-config (or sh start).

### Show Interface

Interface configuration, status, and statistics can all provide helpful information in troubleshooting a network connection problem. To get an overview of all the device’s interfaces, enter the command show interface (or sh int). [Figure 9-29](javascript://) shows output for a Cisco router’s interface that is connected to two VLANs on a switch.

**Figure 9-29**

A router’s interface information



Enlarge Image

Source: Cisco Systems, Inc.

Notice the following information in this output:

* **Link state**—Indicates whether the interface is up or down. The first portion, FastEthernet0/0, refers to the physical layer: Is a physical cable connected to the interface? The second portion, line protocol, refers to the data link layer: Are basic protocols functioning properly across the link, such as clocking and framing? If the interface is “administratively down,” it has been shut down using the shutdown command or has encountered a configured limitation, such as a security breach. Bring it back up using the no shutdown (or no shut) command.
* **MTU**—Indicates the maximum network-layer packet size the interface can support. The Ethernet standard MTU is 1500 bytes.
* **BW (bandwidth)**—Indicates the link’s supported bandwidth, which is used by routing protocols to calculate best paths. The rest of the information on this line is also used for routing metrics, including delay, reliability, and load.
* **Encapsulation**—For Ethernet networks, the encapsulation value is always set to ARPA. The statement “loopback not set” does not refer to the loopback interface but to the interface’s current mode. Loopback mode is sometimes used for testing.
* **Duplex and speed**—Indicates if the link is operating in full-duplex mode, the link’s bandwidth (such as 100 Mbps), and the physical connection type (such as RJ-45).
* **Send and receive traffic statistics**—Interface statistics are tracked over time and can be cleared. Information here will indicate when the statistics were most recently reset. The next several lines indicate statistics that have been gathered since the most recent reset and include number of packets dropped due to queue overflow, average input and output rates, total number of packets and bytes received or sent by the system, and number of broadcast frames, runts, and giants received. [**Runts**](javascript://) are messages that are too small and were dropped—on Ethernet networks, this minimum size is 64 bytes. Excessive collisions on a network can result in high numbers of runts being reported. [**Giants**](javascript://) are frames that are too large, and these are also dropped. On Ethernet networks, this maximum frame size is usually 1518 bytes, although jumbo frames over this size might be supported. Excessive giants being reported is usually a result of misconfigurations. Additional statistics indicate the number of CRC errors. CRC (Cyclic Redundancy Checksum) confirms the data in a message has not been corrupted. A [**CRC error**](javascript://) indicates messages are being damaged in transit, such as when there’s a cable problem or a damaged NIC.

While the show interface command displays OSI layer 1 and 2 information, the show ip interface (or sh ip int) command focuses on detailed layer 3 information, such as IP addressing, helper address, accounting, compression, NAT, and many other settings. For a more concise list of interfaces, IP addresses, and interface status, enter the command show ip interface brief (or sh ip int br).

Go to pg.

[**help**](javascript://)

Application Opened

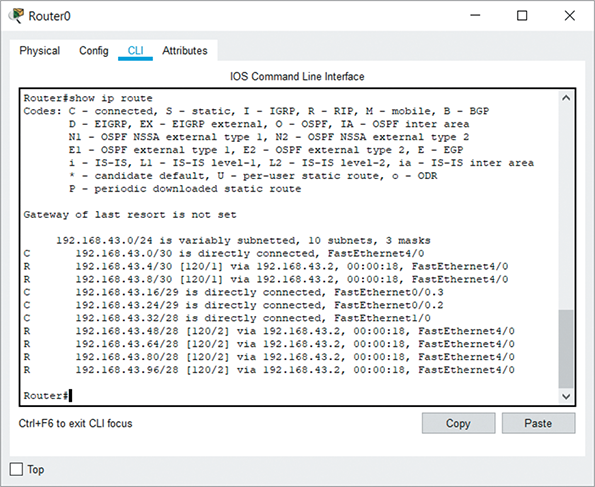
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5cRouting Issues

Just as interfaces must be properly configured for network connections to work as expected, misconfigured routing tables also can cause problems for network connections. On a Cisco router, the show ip route command lists the router’s routing table information, as shown in [Figure 9-30](javascript://).

**Figure 9-30**

A router’s routing table



Enlarge Image

Source: Cisco Systems, Inc.

The routing table lists several types of routes and other information about the routes. Some of the most used route types and information are described next:

* **C (connected)**—Networks directly connected to the router’s own interfaces are classified as C (connected).
* **S (static)**—Static routes are manually configured by a network admin.
* **Protocol**—Codes identify the routing protocol used to configure the route, such as R (RIP), B (BGP), D (EIGRP), and O (OSPF).
* **Gateway of last resort**—This route identifies the path for messages when another route doesn’t apply.

Common routing issues include the following:

* **Missing route**—If no matching route exists for a message, the message will be dropped. For this reason, a gateway of last resort should be configured to handle messages with no matching route. You can add a gateway of last resort using one of the following commands: ip default-gateway (used when no routing is configured on the router), ip default-network (requires that routing is configured on the router and chooses a classful default route from existing routes), or ip route 0.0.0.0 0.0.0.0 (sets a default route for messages with no matching route in the routing table and requires that routing is configured on the router). A similar problem is caused when existing routes are not being advertised through routing protocols. As you’ll see in a project at the end of this module, you need to identify which of its connected routes you want each router to advertise.
* [**Routing loop**](javascript://)—Routing protocols can sometimes route messages continuously through the same paths without the message ever reaching its destination, which can negatively impact network performance. Making too many topology changes too quickly can cause this problem, as routers need time to adjust to each change. Distance-vector routing protocols reach convergence more slowly than other types of routing protocols. A conservative TTL (time-to-live) can ensure these stray packets are dropped after so many hops. Limitations can also be placed on the routers’ ability to share their routing tables with neighbors so this sharing moves outward from each router without old information looping back on itself—this is called a split horizon. Similarly, a routing timer ensures that all the routers in the system share their routing tables at the same time. This way, there’s no question as to which routing table entry is the most recent when something has changed on the network.
* [**Asymmetrical routing**](javascript://)—This is caused when messages going in one direction in a conversation (such as from a web server to a client) travel a different path than messages going in the other direction (such as from client to web server). While this is typically unavoidable (especially when using BGP on the Internet) and is not a problem, it can cause issues for NAT and for firewalls that need to see traffic in both directions of a conversation to properly apply filtering rules. Firewalls often rely on TCP sessions to approve outgoing traffic in response to approved incoming traffic. If some incoming traffic hits a different firewall than the one a server is configured to use for its outgoing messages, the firewall might incorrectly reject outgoing traffic that should have been approved. For organizations using multiple firewalls, thoughtful configuration of traffic flow and internal routing can be used to avoid problems with asymmetrical routing.

[Table 9-5](javascript://) summarizes commonly used Cisco commands for routers and switches, many of which you’ve used in the Packet Tracer projects in this course.

**Table 9-5**

### Common Cisco Commands

| **Command** | **Mode** | **Purpose** |
| --- | --- | --- |
| ? | Any | When entered alone, outputs a list of available commands in the current mode. When entered after portions of a command, outputs a list of available parameters for that command. When entered after one or a few letters, outputs a list of commands beginning with those letters. |
| show running-config  or sh run | Privileged EXEC | Displays the running-config file. |
| copy running-config startup-config  or copy run start | Privileged EXEC | Copies the running configuration to the startup-config file. |
| show mac address-table | Privileged EXEC | Displays MAC address table on a switch. |
| show vlan brief  or sh vlan br | Privileged EXEC | Displays a concise list of VLAN assignment information on a switch. |
| show ip route  or sh ip ro | EXEC | Displays a router’s routing table. Add parameters to specify types of routes, such as show ip route rip. Delete a route from the routing table with the command clear ip route x.x.x.x (where the last part lists the IP address of the target network you want to clear from the routing table). |
| show ip protocol database | Any | Displays a routing protocol’s routing database on a router, such as show ip rip database. |
| ip route destinationaddress subnetmask nexthopaddress | Global configuration | Sets a static route on a router. |
| show interface  or sh int | EXEC | Displays physical and data link layer information about a device’s interfaces. |
| show ip interface brief  or sh ip int br | EXEC | Displays concise network layer information about a device’s interfaces. |
| show interface trunk or sh int tr | EXEC | Displays trunks configured on a switch. |
| show interface switchport or sh int sw | EXEC | Displays detailed VLAN configurations for each of a switch’s interfaces. |
| interface fastethernet0/0  or int fa0/0 | Global configuration | Enters interface configuration mode for specified interface. |
| ip address address subnet  or ip addr address subnet | Interface configuration | Sets IP information for an interface. |
| no shutdown  or no shut | Interface configuration | Enables an interface. Similarly, shutdown will disable an interface. |
| ip name-server dns1address  dns2address | Global configuration | Sets DNS server addresses. |
| hostname | Global configuration | Changes the device’s name. |

Enlarge Table

**Applying Concepts 9-4**

### Internet Down

One evening, you’re up late working to meet a fast-approaching deadline when suddenly your Internet connection fails. Much of your work requires Internet access for research, but you belay the panic for a few moments to evaluate the situation:

* You try a couple different websites in your browser, then open a different browser application and try a couple websites again. None of the sites will load.
* You check all the cable connections between your computer and your network’s demarc. Everything looks normal.
* You power cycle the modem and router by unplugging both devices from the electrical outlet, waiting a few minutes, plugging in the modem, waiting for it to establish a connection with the ISP, and then plugging in the router.
* You check the Network Connections status on your computer and confirm that you have a functioning connection with your network.
* You try again to navigate to a website in your browser, but the page still won’t load.
* You open a PowerShell window and ping one of Google’s servers at 8.8.8.8. The ping works.
* You ping Google’s website at [google.com](http://google.com/" \t "_blank), but this time it doesn’t work.
* You pull up an outage reporting website for your ISP on your smartphone and find that a few hundred other people have reported an outage in your area.

With a quick adjustment, you get your Internet service functioning again and continue with your work. Which of the following did you do and why?

1. You switched out the Ethernet cable connecting your modem to your router because the cable was damaged.
2. You used ipconfig to release the IP address on your computer and get a new one from your network’s DHCP service because your computer had a duplicate IP address.
3. You changed the DNS settings on your router to point to Google’s DNS servers instead of the DNS servers of your ISP because the ISP’s DNS servers are down.
4. You switched to a different ISP because the former ISP’s service was unreliable.
5. You replaced the router with a new router you had ready to go, knowing that the old router had already exceeded its life expectancy and had finally ceased to function.
6. You created an ad hoc network with another computer on your network and used that computer’s access to the Internet to continue your research because the Wi-Fi radio on your computer had died and will need to be replaced.
7. You performed a factory reset on your modem so it would reinitiate a connection with the ISP.
8. You updated the default gateway on your computer because it was unable to communicate with the router.
9. You restarted your computer because Windows had updates that needed to be installed.

**Remember This…**

* Use basic network platform commands, including show interface, show config, and show route.
* Analyze connection problems using interface information, including link state, speed/duplex, and traffic statistics.
* Troubleshoot common routing issues, including missing route, routing loop, and asymmetrical routing.

**Self-Check**

1. Where is a router’s hostname stored when you first change the name?

Answer

* 1. Routing table
  2. Startup-config file
  3. Whitelist
  4. Running-config file

1. Which problem is most likely caused by a damaged cable?

Answer

* 1. Routing loop
  2. CRC error
  3. Asymmetrical route
  4. Excessive giants

**You’re Ready**

You’re now ready to complete [Project 9-4: Explore IOS Command Modes in Packet Tracer](javascript://), or you can wait until you’ve finished the Review Questions for this module.

**You’re Ready**

After you finish the Hands-On Projects, you’re ready to complete the [Module 9 Capstone Projects](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 9-6a**Module Summary**

### WAN Essentials

* A WAN traverses a significant distance and usually supports very high data throughput. Although many types of businesses need WANs, they might not need the same kinds of WANs.
* Typically, a CAN is a collection of LANs within a single property or nearby properties, such as buildings belonging to a school where all the buildings and most or all the network media spanning those connections are confined within land owned by the school. With a CAN, it’s likely that a single organization (or group of organizations) owns all the connected LANs and most or all the networking media connecting those LANs.
* A MAN is a collection of LANs within a limited geographical area, such as a downtown area or even a city, county, or province. With MANs, many customers might own one or more of the connected LANs, and a single, third-party provider leases use of the networking media connecting these LANs. These connections often must be made across property not owned by either the MAN provider or the MAN customers. MAN connections might be made available to the general public, or it might be restricted to a single customer.
* A modem is a modulation/demodulation device that converts between digital and analog signals. The customer’s endpoint device on a WAN is called the DTE (data terminal equipment), and the carrier’s endpoint device for the WAN is called the DCE (data circuit-terminating equipment). The NIU, also called NID (network interface device), at the demarc connects the ISP’s local loop to the customer’s network. A more intelligent version of an NIU is a smartjack, or INID (Intelligent NID), which can provide diagnostic information about the interface.

### Routing Protocols

* A router joins two or more networks and passes packets from one network to another. Routers are responsible for determining the next network to which a packet should be forwarded on its way to its destination. Routers are often categorized according to their location on a network or the Internet and the routing protocols they use. The various categories include core routers, edge routers, and exterior routers.
* A routing table is a database that holds information about where hosts are located and the most efficient way to reach them. A router relies on its routing table to identify which network a host belongs to and which of the router’s interfaces points toward the best next hop to reach that network. Routing paths are determined by static routes or dynamic routes, which are listed in the routing table. The route utility allows you to view a host’s routing table.
* To determine the best path, routers communicate with each other through routing protocols. Routers rate the reliability and priority of a routing protocol’s data based on AD (administrative distance), convergence time, and overhead.
* IGPs (interior gateway protocols) are routing protocols used by core routers and edge routers within autonomous systems. IGPs are often grouped according to the algorithms they use to calculate best paths, including distance-vector routing protocols, link-state routing protocols, and hybrid routing protocols. EGPs (exterior gateway protocols) are routing protocols used by edge routers and exterior routers to distribute data outside of autonomous systems. The only EGP protocol currently in use is BGP.
* The most popular routing protocols in use today include RIP (Routing Information Protocol) and RIPv2 (Routing Information Protocol, version 2), which are legacy protocols, and the link-state routing protocol OSPF (Open Shortest Path First), the similar IS-IS (Intermediate System to Intermediate System), Cisco’s hybrid protocol EIGRP (Enhanced Interior Gateway Routing Protocol), and the Internet protocol BGP (Border Gateway Protocol).
* Three popular FHRPs (First Hop Redundancy Protocol) used by routers and layer 3 switches to provide a single VIP (Virtual IP) address as the default gateway to a network are VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Routing Protocol), and GLBP (Gateway Load Balancing Protocol).

### WAN Connectivity

* Two categories of WAN connectivity services are broadband, where the cables (whether telephone, coaxial, or fiber) and available bandwidth are shared between multiple customers, and DIA (dedicated Internet access), where the cable or a portion of its available bandwidth is dedicated to a single customer.
* DSL (digital subscriber line) is a WAN connection method that operates over the PSTN (public switched telephone network), which is a network of lines and carrier equipment that provide landline telephone service to homes and businesses.
* Cable broadband (also called cable Internet or cable modem access) is based on the coaxial cable wiring used for TV signals, although in reality, much of the coaxial infrastructure has been replaced with fiber.
* To reduce the distance signals must travel over copper cables to reach customers, many ISPs use MONs (metropolitan optical networks) to offer FTTN (fiber-to-the-node), FTTH (fiber-to-the-home), or similar arrangements. A MON is a dense, localized grid of junctions and fiber cables that attempts to make direct fiber connections available to as many customers as possible while balancing the significant expense of replacing existing telephone and coaxial cable infrastructure with fiber equipment and fiber-optimized technologies.
* Leased lines provide dedicated bandwidth on fiber optic connections. The customer pays for a specific bandwidth (such as 2 Gbps) and reserves that bandwidth for their sole use without having to share it with other customers. Throughput won’t fluctuate in response to traffic demands from other customers.
* MPLS (multiprotocol label switching) enables multiple types of layer 3 protocols to travel over any one of several connection-oriented layer 2 protocols. One of the characteristics that sets MPLS apart from other WAN technologies is its ability to support QoS traffic shaping across WAN connections.
* With a private-direct connection, or interconnection, to the cloud, you lease a dedicated line from your ISP to one of your cloud provider’s PoPs, or colocation facilities. From there, you pay for the connection to the cloud provider’s physical infrastructure and, usually, some kind of data transfer fees.
* SD-WAN (software-defined wide area network) relies on abstracted, centralized control of networking devices to manage network functions across a diverse infrastructure. SD-WAN offers the following benefits: transport agnostic, active-active load balancing, automatic failover, intent-based management, zero-touch provisioning, and reduced cost compared to services such as leased lines and MPLS.

### Wireless WANs

* With 3G (third generation) cellular services, data rates rose to 384 Kbps. To switch to fully digital transmissions, two competing 2G technologies emerged as market leaders for 3G: GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access).
* 4G (fourth generation) services are characterized by an all-IP network for both data and voice transmission. 4G standards, released in 2008, specify minimum throughputs of 100 Mbps with the goal of supporting 1 Gbps speeds. LTE (Long-Term Evolution) became an ambiguous marketing term that meant “faster than 3G but not really 4G.” As hardware has improved, so have LTE speeds. Typical speeds now for LTE connections might reach 100 Mbps download and up to 75 Mbps upload. LTE-A (LTE-Advanced) can more realistically approach 4G standards. Sometimes misleadingly called 5G E (5G Evolution), LTE-A is basically true 4G as defined back in 2008 but only recently emerging in real-world networks.
* 5G (fifth generation) services require minimum speeds of 1 Gbps and max out at 20 Gbps download and 10 Gbps upload, however, actual speeds vary greatly. 5G relies on three frequency bands called low band, mid-band, and high band.
* Satellite Internet clients can exchange signals with satellites as long as they have a line-of-sight path from an unobstructed view of the sky. To establish a satellite Internet connection, each subscriber must have a fixed dish antenna pointed toward the sky over the equator. The dish antenna’s receiver is connected via cable to a modem. As with several other wireless WAN technologies, satellite services are typically asymmetrical, and bandwidth is shared among many subscribers. Throughputs vary and are controlled by the service provider. Downlink speeds might reach 100 Mbps, while uplink rates are much slower.

### Troubleshooting Connections

* When making a configuration change to a Cisco device, those changes are held in the running configuration file. You can see the device’s running-config file with the command show running-config (or sh run).
* Interface configuration, status, and statistics can all provide helpful information in troubleshooting a network connection problem. To get an overview of all the device’s interfaces, enter the command show interface (or sh int).
* Just as interfaces must be properly configured for network connections to work as expected, misconfigured routing tables also can cause problems for network connections. On a Cisco router, the show ip route command lists the router’s routing table information.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 9-6a**Module Summary**

### WAN Essentials

* A WAN traverses a significant distance and usually supports very high data throughput. Although many types of businesses need WANs, they might not need the same kinds of WANs.
* Typically, a CAN is a collection of LANs within a single property or nearby properties, such as buildings belonging to a school where all the buildings and most or all the network media spanning those connections are confined within land owned by the school. With a CAN, it’s likely that a single organization (or group of organizations) owns all the connected LANs and most or all the networking media connecting those LANs.
* A MAN is a collection of LANs within a limited geographical area, such as a downtown area or even a city, county, or province. With MANs, many customers might own one or more of the connected LANs, and a single, third-party provider leases use of the networking media connecting these LANs. These connections often must be made across property not owned by either the MAN provider or the MAN customers. MAN connections might be made available to the general public, or it might be restricted to a single customer.
* A modem is a modulation/demodulation device that converts between digital and analog signals. The customer’s endpoint device on a WAN is called the DTE (data terminal equipment), and the carrier’s endpoint device for the WAN is called the DCE (data circuit-terminating equipment). The NIU, also called NID (network interface device), at the demarc connects the ISP’s local loop to the customer’s network. A more intelligent version of an NIU is a smartjack, or INID (Intelligent NID), which can provide diagnostic information about the interface.

### Routing Protocols

* A router joins two or more networks and passes packets from one network to another. Routers are responsible for determining the next network to which a packet should be forwarded on its way to its destination. Routers are often categorized according to their location on a network or the Internet and the routing protocols they use. The various categories include core routers, edge routers, and exterior routers.
* A routing table is a database that holds information about where hosts are located and the most efficient way to reach them. A router relies on its routing table to identify which network a host belongs to and which of the router’s interfaces points toward the best next hop to reach that network. Routing paths are determined by static routes or dynamic routes, which are listed in the routing table. The route utility allows you to view a host’s routing table.
* To determine the best path, routers communicate with each other through routing protocols. Routers rate the reliability and priority of a routing protocol’s data based on AD (administrative distance), convergence time, and overhead.
* IGPs (interior gateway protocols) are routing protocols used by core routers and edge routers within autonomous systems. IGPs are often grouped according to the algorithms they use to calculate best paths, including distance-vector routing protocols, link-state routing protocols, and hybrid routing protocols. EGPs (exterior gateway protocols) are routing protocols used by edge routers and exterior routers to distribute data outside of autonomous systems. The only EGP protocol currently in use is BGP.
* The most popular routing protocols in use today include RIP (Routing Information Protocol) and RIPv2 (Routing Information Protocol, version 2), which are legacy protocols, and the link-state routing protocol OSPF (Open Shortest Path First), the similar IS-IS (Intermediate System to Intermediate System), Cisco’s hybrid protocol EIGRP (Enhanced Interior Gateway Routing Protocol), and the Internet protocol BGP (Border Gateway Protocol).
* Three popular FHRPs (First Hop Redundancy Protocol) used by routers and layer 3 switches to provide a single VIP (Virtual IP) address as the default gateway to a network are VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Routing Protocol), and GLBP (Gateway Load Balancing Protocol).

### WAN Connectivity

* Two categories of WAN connectivity services are broadband, where the cables (whether telephone, coaxial, or fiber) and available bandwidth are shared between multiple customers, and DIA (dedicated Internet access), where the cable or a portion of its available bandwidth is dedicated to a single customer.
* DSL (digital subscriber line) is a WAN connection method that operates over the PSTN (public switched telephone network), which is a network of lines and carrier equipment that provide landline telephone service to homes and businesses.
* Cable broadband (also called cable Internet or cable modem access) is based on the coaxial cable wiring used for TV signals, although in reality, much of the coaxial infrastructure has been replaced with fiber.
* To reduce the distance signals must travel over copper cables to reach customers, many ISPs use MONs (metropolitan optical networks) to offer FTTN (fiber-to-the-node), FTTH (fiber-to-the-home), or similar arrangements. A MON is a dense, localized grid of junctions and fiber cables that attempts to make direct fiber connections available to as many customers as possible while balancing the significant expense of replacing existing telephone and coaxial cable infrastructure with fiber equipment and fiber-optimized technologies.
* Leased lines provide dedicated bandwidth on fiber optic connections. The customer pays for a specific bandwidth (such as 2 Gbps) and reserves that bandwidth for their sole use without having to share it with other customers. Throughput won’t fluctuate in response to traffic demands from other customers.
* MPLS (multiprotocol label switching) enables multiple types of layer 3 protocols to travel over any one of several connection-oriented layer 2 protocols. One of the characteristics that sets MPLS apart from other WAN technologies is its ability to support QoS traffic shaping across WAN connections.
* With a private-direct connection, or interconnection, to the cloud, you lease a dedicated line from your ISP to one of your cloud provider’s PoPs, or colocation facilities. From there, you pay for the connection to the cloud provider’s physical infrastructure and, usually, some kind of data transfer fees.
* SD-WAN (software-defined wide area network) relies on abstracted, centralized control of networking devices to manage network functions across a diverse infrastructure. SD-WAN offers the following benefits: transport agnostic, active-active load balancing, automatic failover, intent-based management, zero-touch provisioning, and reduced cost compared to services such as leased lines and MPLS.

### Wireless WANs

* With 3G (third generation) cellular services, data rates rose to 384 Kbps. To switch to fully digital transmissions, two competing 2G technologies emerged as market leaders for 3G: GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access).
* 4G (fourth generation) services are characterized by an all-IP network for both data and voice transmission. 4G standards, released in 2008, specify minimum throughputs of 100 Mbps with the goal of supporting 1 Gbps speeds. LTE (Long-Term Evolution) became an ambiguous marketing term that meant “faster than 3G but not really 4G.” As hardware has improved, so have LTE speeds. Typical speeds now for LTE connections might reach 100 Mbps download and up to 75 Mbps upload. LTE-A (LTE-Advanced) can more realistically approach 4G standards. Sometimes misleadingly called 5G E (5G Evolution), LTE-A is basically true 4G as defined back in 2008 but only recently emerging in real-world networks.
* 5G (fifth generation) services require minimum speeds of 1 Gbps and max out at 20 Gbps download and 10 Gbps upload, however, actual speeds vary greatly. 5G relies on three frequency bands called low band, mid-band, and high band.
* Satellite Internet clients can exchange signals with satellites as long as they have a line-of-sight path from an unobstructed view of the sky. To establish a satellite Internet connection, each subscriber must have a fixed dish antenna pointed toward the sky over the equator. The dish antenna’s receiver is connected via cable to a modem. As with several other wireless WAN technologies, satellite services are typically asymmetrical, and bandwidth is shared among many subscribers. Throughputs vary and are controlled by the service provider. Downlink speeds might reach 100 Mbps, while uplink rates are much slower.

### Troubleshooting Connections

* When making a configuration change to a Cisco device, those changes are held in the running configuration file. You can see the device’s running-config file with the command show running-config (or sh run).
* Interface configuration, status, and statistics can all provide helpful information in troubleshooting a network connection problem. To get an overview of all the device’s interfaces, enter the command show interface (or sh int).
* Just as interfaces must be properly configured for network connections to work as expected, misconfigured routing tables also can cause problems for network connections. On a Cisco router, the show ip route command lists the router’s routing table information.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**9**

**Wide Area Networking**

* [Module Introduction](javascript://)
* **9-1**[WAN Essentials](javascript://)
  + **9-1a**[Entry Point Equipment](javascript://)
* **9-2**[Routing Protocols](javascript://)
  + **9-2a**[Routing Tables](javascript://)
  + **9-2b**[Routing Path Types](javascript://)
  + **9-2c**[Route](javascript://)
  + **9-2d**[Routing Metrics](javascript://)
  + **9-2e**[Routing Protocols to Determine Best Paths](javascript://)
  + **9-2f**[Interior and Exterior Gateway Protocols](javascript://)
  + **9-2g**[Routing Redundancy](javascript://)
* **9-3**[WAN Connectivity](javascript://)
  + **9-3a**[DSL (Digital Subscriber Line)](javascript://)
  + **9-3b**[Cable Broadband](javascript://)
  + **9-3c**[Fiber](javascript://)
  + **9-3d**[Leased Lines](javascript://)
  + **9-3e**[MPLS (Multiprotocol Label Switching)](javascript://)
  + **9-3f**[Cloud Connectivity Options](javascript://)
  + **9-3g**[Software-defined WAN (SD-WAN)](javascript://)
* **9-4**[Wireless WANs](javascript://)
  + **9-4a**[Cellular](javascript://)
  + **9-4b**[Satellite](javascript://)
* **9-5**[Troubleshooting Connections](javascript://)
  + **9-5a**[Internet Connectivity Issues](javascript://)
  + **9-5b**[Interface Problems](javascript://)
  + **9-5c**[Routing Issues](javascript://)
* **9-6**[Module Review](javascript://)
  + **9-6a**[Module Summary](javascript://)
  + **9-6b**[Key Terms](javascript://)
  + **9-6c**[Review Questions](javascript://)
  + **9-6d**[Hands-On Projects](javascript://)
  + **9-6e**[Capstone Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Introduction

### Objectives

After reading this module and completing the exercises, you should be able to:

* **1**Identify the fundamental elements of WAN service options
* **2**Explain how routers manage internetwork communications
* **3**Compare and contrast WAN connectivity technologies
* **4**Explain the most common wireless WAN technologies
* **5**Troubleshoot common connection problems

**On the Job**

The European “cooperative” public Internet Exchange model has come to the United States in the last few years, changing WAN internetworking considerations related to cloud service access. These days, WAN networking is as much about connecting to cloud services as to far-away offices. A public IX (Internet Exchange) is a less-expensive, cooperative way to directly or near-directly peer with other companies’ networks, rather than paying an ISP for expensive Internet bandwidth. In this model, for small fees associated with running the cooperative network at a few data centers in a metropolitan area, we can peer directly with content partners’ networks. This requires no ISP in the middle and makes it possible to route directly to our peers.

Last year, one of our SaaS security software delivery teams advocated for hosting their application at data centers directly connected to a public IX in the United States rather than at our traditional data centers. The SaaS application is very sensitive to Internet latency, and more than 50 percent of its traffic is exchanged with just a few content providers, including Microsoft, Amazon hosting services, and Google.

At first, I couldn’t understand the rationale for adding more data center locations when we already had quite a few. Then the SaaS security team showed me traffic tests. I also ran my own. I learned that the other traffic providers were a hop or two closer when tested from the IX location. More importantly, when connected to the IX network’s peering, we saw much faster effective transport speeds with all of our big content partners. Because a peering network allows less expensive Internet transit, some companies might prefer IX routes to routes over the Internet, resulting in better results than the hops saved would suggest.

In a couple of locations, we looked at extending an IX network to our nearby facilities via WAN circuits. But when we compared the cost of the extension to just renting data center space at the IX, it made more sense to host at the location where the IX was already connected, even after buying more network gear.

Public “cooperative” IX examples include the following:

* AMS-IX (Bay Area Internet Exchange)
* SFMIX (San Francisco Metro Internet Exchange)
* FL-IX (Florida Internet Exchange)
* NYIIX (New York International Internet Exchange)

The United States also has some older Internet Exchange providers, but usually their hosting fees are higher, making total cost potentially much higher than in this newer model.

**Brooke Noelke**

**Cloud Service Architect**

**McAfee**

In previous modules, you have learned about basic transmission media, network models, and networking hardware associated with LANs. This module focuses on WANs (wide area networks), which, as you know, are networks that connect two or more geographically distinct LANs. WANs are of significant concern for organizations attempting to meet the needs of telecommuting workers, global business partners, and Internet-based commerce.

The distance requirements of WANs affect their entire infrastructure, and, as a result, WANs differ from LANs in many respects. To understand the fundamental difference between a LAN and a WAN, think of the hallways and stairs of your house or school as LAN pathways. These interior passages allow you to go from room to room. To reach destinations outside the building, however, you need to use sidewalks and streets. These public thoroughfares are analogous to WAN pathways—except that WAN pathways are not necessarily public.

This module discusses WAN topologies and various technologies used by WANs. It also notes some potential pitfalls in establishing and maintaining WAN connections.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-1WAN Essentials

### Certification

* 1.2

Explain the characteristics of network topologies and network types.

Average reading time: 11 minutes

A WAN traverses a significant distance and usually supports very high data throughput. Each of the following scenarios demonstrates a need for a WAN:

* A bank with offices around the state needs to connect those offices with each other to gather transaction and account information into a central database. Furthermore, it needs to connect with global financial clearinghouses to, for example, conduct transactions with other institutions.
* Regional sales representatives for a national pharmaceutical company need to submit their sales figures to a file server at the company’s headquarters and receive email from the company’s mail server.
* An automobile manufacturer in Detroit contracts its plastic parts manufacturing to a Delaware-based company. Through WAN links, the auto manufacturer can video conference with the plastics manufacturer, exchange specification data, and even examine the parts for quality from a remote location.
* A clothing manufacturer sells its products over the Internet to customers worldwide.

Although all these businesses need WANs, they might not need the same kinds of WANs. Depending on the traffic load, budget, geographical breadth, and commercially available technology, each might implement a different transmission method. For every business need, a few WAN connection types might be capable of meeting that need. At the same time, many WAN technologies can coexist on the same network to meet different needs.

The following list summarizes the major characteristics of WANs and explains how a WAN differs from a LAN:

* LANs connect nodes, such as workstations, servers, printers, and other devices, in a small geographical area on a single organization’s network, whereas WANs use networking devices, such as routers and modems, to connect networks spread over a wide geographical area.
* LANs and WANs may differ at layers 1 and 2 of the OSI model in access methods, topologies, and, sometimes, transmission media. For example, the way DSL transmits bits over a WAN differs from the way Ethernet transmits bits over a LAN.
* Both LANs and WANs use the same protocols from OSI layers 3 and above. Recall that layer 3 protocols are responsible for directing data between LANs.
* LANs are mostly owned and operated by the companies that use them. On the other hand, WANs are usually owned and operated by telcos (telecommunications carriers), also known as NSPs (network service providers), such as AT&T, Verizon, Spectrum, and Comcast. Corporations lease WAN connections from these carriers, often with payments based on the amount of bandwidth used or reserved. Alternatively, as you read about in the [On the Job](javascript://) story at the beginning of this module, corporations might connect directly to an IX (Internet Exchange), sometimes called an IXP (Internet Exchange point). This is similar to the difference between buying merchandise at retail prices versus buying products wholesale through a purchasing cooperative. IXs are where the networks of ISPs and other telecommunications providers intersect. By connecting directly into an IX, companies are able to cut out some of the “middleman” expense of WAN connections.

As you can see, WANs are used to connect LANs. Recall that CANs (campus area networks) and MANs (metropolitan area networks) also connect LANs. Typically, a CAN is a collection of LANs within a single property or nearby properties, such as buildings belonging to a school where all the buildings and most or all the network media spanning those connections are confined within land owned by the school. With a CAN, it’s likely that a single organization (or group of organizations) owns all the connected LANs and most or all the networking media connecting those LANs.

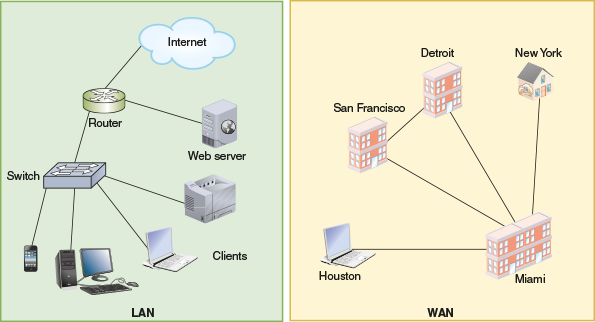
Similarly, a MAN is a collection of LANs within a limited geographical area, such as a downtown area or even a city, county, or province. With MANs, many customers might own one or more of the connected LANs, and a single, third-party provider leases use of the networking media connecting these LANs. These connections often must be made across property not owned by either the MAN provider or the MAN customers. MAN connections might be made available to the general public (such as when a city makes high-speed Internet access available to all downtown area residents), or it might be restricted to a single customer (such as when a hospital is connected to its satellite medical offices). The following list gives examples where MANs can be useful:

* Connecting a city’s police stations
* Connecting a hospital with its regional medical centers
* Connecting a home office with its branch offices and a warehouse location

The reason to make these distinctions between WANs, MANs, CANs, and LANs is because different technologies and protocols have been developed to best serve each of these markets. Networking technology that works well for a [**long-haul connection**](javascript://) across hundreds of miles to support the Internet backbone isn’t well suited for network connections between two buildings situated next door to each other, even though both these networks might connect multiple LANs. Throughout this module, you’ll learn more about the nuances of when to use various technologies, depending on distances, networking media, and types of communications needed on the network. [Figure 9-1](javascript://) illustrates this fundamental difference between WAN and LAN connectivity.

**Figure 9-1**

Differences in scale between LAN and WAN



Enlarge Image

The individual geographic locations or endpoints connected by a WAN are known as WAN sites. A WAN link is a connection between one WAN site (or endpoint) and another site (or endpoint). WAN links can be point-to-point (connects one site to only one other site) or multipoint (connects one site to two or more other sites).

Go to pg.

[**help**](javascript://)

Application Opened

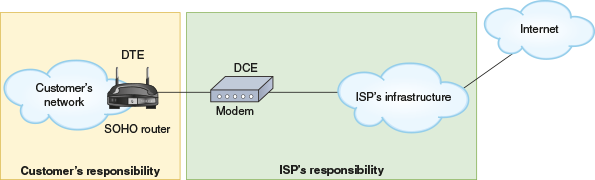
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-1aEntry Point Equipment

If you have DSL or cable Internet service, you connect your home router to a modem. A [**modem**](javascript://) is a modulation/demodulation device that converts between digital and analog signals. The customer’s endpoint device on a WAN is called the DTE (data terminal equipment), and the carrier’s endpoint device for the WAN is called the DCE (data circuit-terminating equipment). In this case, the router is the DTE, usually owned by the customer, and the modem is the DCE, usually owned by the ISP. [Figure 9-2](javascript://) shows this setup, with a router and modem at the customer’s site defining the dividing line between each network.

**Figure 9-2**

A router and a modem define the endpoints where a LAN connects to a WAN



Enlarge Image

Generally, the DTE is the responsibility of the customer and the DCE is the responsibility of the ISP. The DTE communicates on the LAN, and the DCE communicates on the WAN. Sometimes the DTE and DCE are combined in the same device. For example, a router might have one WAN network adapter, or WIC (WAN interface connector), that connects to a fiber-optic WAN and one LAN network adapter that connects to an Ethernet, twisted-pair LAN.

When working with your network’s connection to your ISP at the service-related entry point, you need to know the difference between equipment that belongs to the ISP and equipment that belongs to the subscriber. Equipment located on the customer’s premises, regardless of who owns it and who is responsible for it, is called CPE (customer premises equipment). Equipment belonging to the ISP, despite its location on the customer’s premises, should only be serviced by the ISP’s technicians even if it is located on the customer’s side of the demarc (demarcation point). Equipment owned by the customer is the responsibility of the customer and will not be serviced by the ISP. The following list describes devices commonly found at or near the demarc:

* **NIU (network interface unit)**—The NIU, also called NID (network interface device), at the demarc connects the ISP’s local loop to the customer’s network. A more intelligent version of an NIU is a **[smartjack](javascript://)**, or INID (Intelligent NID), which can provide diagnostic information about the interface. For example, a smartjack might include loopback capabilities. Just like the loopback adapter you use to test a port or cable on your computer, the smartjack can loop the ISP’s signal back to the CO (central office) for testing. The ISP is responsible for all wiring leading up to the NIU and for the NIU itself. The customer is responsible for everything past the NIU unless the equipment is owned by the ISP, such as with a line driver, CSU/DSU, or set-top box.
* **Line driver**—Essentially a repeater, a line driver can be installed either on copper lines (in which case, it is called a copper line driver) or fiber lines (in which case, it is called a fiber line driver) to boost the signal across greater distances. The device might be placed on either side of the demarc and, if located on the customer’s side, might be owned by either party.
* **CSU/DSU (channel service unit/data service unit)**—This device serves as the endpoint for a dedicated connection between an ISP and a customer. Like line drivers, these devices can be owned by either party, depending upon who is responsible for providing this device according to the terms of service. However, the CSU/DSU is typically placed on the customer’s side of the demarc between the demarc and the first router.

Now that you understand the basic components that differentiate WANs from LANs, you’re ready to learn about specific technologies and types.

### Exam Tip

The CompTIA Network+ exam expects you to know about a variety of ISP connection types and to be able to identify the networking environments best suited to each. For wired WANs and related technologies, you need to know about leased lines, DSL, cable broadband, metro-optical networks, MPLS, SD-WAN, and cloud connectivity options. Wireless WANs covered later in this module include satellite and cellular technologies.

**Remember This…**

* Compare LANs, CANs, MANs, and WANs.
* Explain the purpose of a smartjack.

**Self-Check**

1. Which network type supports long-haul connections between ISPs?

Answer

* 1. WAN
  2. CAN
  3. MAN
  4. LAN

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-2Routing Protocols

### Certification

* 1.1

Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

* 2.2

Compare and contrast routing technologies and bandwidth management concepts.

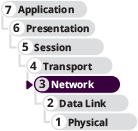
* 3.3

Explain high availability and disaster recovery concepts and summarize which is the best solution.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

Average reading time: 33 minutes



You’ve spent a lot of time over the past few modules learning how switches work, both at layer 2 and layer 3, within a corporate network. As you know, routers serve as gateways to connect networks. To study WAN technologies, you must learn more about how routers work. A router joins two or more networks and passes packets from one network to another. Routers are responsible for determining the next network to which a packet should be forwarded on its way to its destination. A typical router consists of an internal processor, an operating system, memory, input and output jacks for different types of network connectors (depending on the network type), and, usually, a management console interface. Three examples of routers are shown in [Figure 9-3](javascript://), with the most complex on the left and the simplest on the right. High-powered, multiprotocol routers may have several slot bays to accommodate multiple network interfaces. At the other end of the scale are simple, inexpensive routers often used in small offices and homes, and they require little configuration.

**Figure 9-3**

ISP, business, and consumer routers



Enlarge Image

Courtesy of Juniper Networks, Inc Courtesy of NETGEAR

A router’s strength lies in its intelligence—that is, its ability to interact with transmissions and make decisions. Although any one router can be specialized for a variety of tasks, all routers can do the following:

* Connect dissimilar networks, such as a LAN and a WAN, which use different types of protocols.
* Interpret layer 3 and often layer 4 addressing and other information contained in these headers.
* Determine the best path for data to travel from point A to point B. The [**best path**](javascript://) is the most efficient route to the message’s destination calculated by the router, based upon the information the router has available to it.
* Reroute traffic if the path of first choice is down but another path is available.

In addition to performing these basic functions, routers may perform any of the following optional functions:

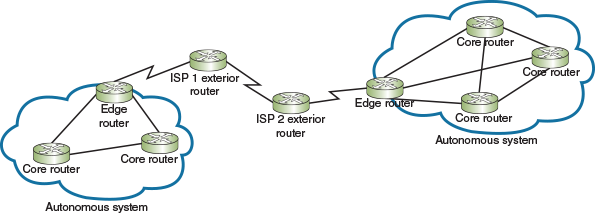
* Filter broadcast transmissions to alleviate network congestion.
* Acting as a simple firewall, prevent certain types of traffic from getting to a network, enabling customized segregation and security.
* Support simultaneous local and remote connectivity.
* Provide high network fault tolerance through redundant components such as power supplies or network interfaces.
* Monitor network traffic and report statistics.
* Diagnose internal or other connectivity problems and trigger alarms.

Routers are often categorized according to their location on a network or the Internet and the routing protocols they use. The various categories are described in the following list and diagrammed in [Figure 9-4](javascript://):

* [**Core routers**](javascript://), also called [**interior routers**](javascript://), are located inside networks within the same autonomous system. An [**AS (autonomous system)**](javascript://) is a group of networks, often on the same domain, that are operated by the same organization. For example, Cengage might have several LANs that all fall under its domain with each LAN connected to the others by core routers. An AS is sometimes referred to as a trusted network because the entire domain is under the organization’s control. Core routers communicate only with routers within the same AS.
* [**Edge routers**](javascript://), or [**border routers**](javascript://), connect an autonomous system with an outside network, also called an untrusted network. For example, the router that connects a business with its ISP is an edge router.
* [**Exterior router**](javascript://) refers to any router outside the organization’s AS, such as a router on the Internet backbone. Sometimes a technician might refer to their own edge router as an exterior router because it communicates with routers outside the AS. But keep in mind that every router communicating over the Internet is a trusted edge router for some organization’s AS, even if that organization is a large telecommunications company managing a portion of the Internet backbone.

**Figure 9-4**

Core, edge, and exterior routers



Enlarge Image

On small office or home office LANs, routers are simple to install: Plug in the network cable from the cable modem connected to your ISP on one port and connect your computer(s) to your LAN through another port or by a wireless connection. Turn on the router and computer and use a web-based utility program on the router to set it up.

However, high-powered, multiprotocol routers can be a challenge to install on sizable networks. Typically, an engineer must be very familiar with routing technology to figure out how to place and configure a router to the best advantage. If you plan to specialize in network design, engineering, or management, you should research router types and their capabilities further. As you learn more about how routers work, keep in mind that layer 3 and layer 4 switches can perform the same functions.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2aRouting Tables

A [**routing table**](javascript://) is a database that holds information about where hosts are located and the most efficient way to reach them. As you know, a router has two or more network ports, or interfaces, and each port connects to a different network. Each network connection is assigned an interface ID, and logically, the router belongs to every network it connects to. A router relies on its routing table to identify which network a host belongs to and which of the router’s interfaces points toward the best next hop to reach that network.

For example, in [Figure 9-5](javascript://), suppose a workstation in LAN A wants to print to the network printer in LAN D. The following steps describe how routing tables would be used in this transmission:

1. Step 1

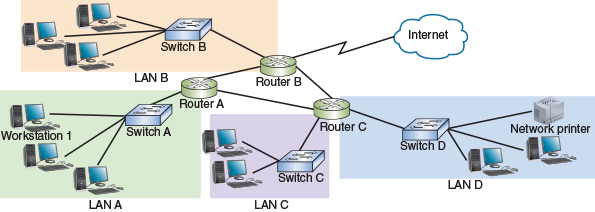
Workstation 1 issues a print command to a network printer. IP on the workstation recognizes that the IP address of the printer is on a different LAN than the workstation and forwards the transmission through switch A to its default gateway, router A.

1. Step 2

Router A examines the destination IP address in the packet’s header and searches its routing table to determine which of its interfaces the message should go to. [Table 9-1](javascript://) shows how a routing table is designed, with each entry explained in plain English instead of using IP addresses and other data. Each row in the routing table describes one route, including a destination network and how to get there. The first two columns provide information used to match messages to a route. The next two columns provide forwarding information for the route. Routing metrics are route ratings used as tie breakers when needed.

**Figure 9-5**

Routers rely on routing tables to locate destination hosts



Enlarge Image

**Table 9-1**

### Portions of Router A’s Routing Table in Plain English

| **Destination network ID** | **Netmask** | **Gateway** | **Interface** | **Routing metrics (tie breaker)** |
| --- | --- | --- | --- | --- |
| LAN A’s IP address | LAN A’s netmask | None (This is router A’s own LAN.) | Port that points toward switch A | 1 |
| LAN B’s IP address | LAN B’s netmask | Router B’s IP address | Port that points toward router B | 4 |
| LAN C’s IP address | LAN C’s netmask | Router C’s IP address | Port that points toward router C | 5 |
| LAN D’s IP address | LAN D’s netmask | Router B’s IP address | Port that points toward router B | 10 |
| LAN D’s IP address | LAN D’s netmask | Router C’s IP address | Port that points toward router C | 5 |
| IP address on the Internet | That host’s netmask | Router B’s IP address | Port that points toward router B | 23 |
| 0.0.0.0 (wildcard entry for any network) | 0 (wildcard entry for any netmask) | Router B’s IP address | Port that points toward router B | 3 |

Here’s a breakdown of how the route-search process uses information in [Table 9-1](javascript://):

* + Router A examines all rows in its routing table. In each row, it uses information in the first two columns—the destination network’s IP address and netmask—to calculate the range of IP addresses included in that network.
  + If the message’s destination IP address fits in the calculated range for a route, the router then reads the IP address of the gateway in the third column. This gateway is the next hop router. It also reads in the fourth column the interface it will use to send the message out.
  + If it finds more than one possible route, the router uses [**routing metrics**](javascript://) (information about each route) in the last column to determine which route is most efficient. The smaller the metrics number, the better the route. Notice in [Figure 9-5](javascript://) and in [Table 9-1](javascript://) that two routes can reach the network printer on LAN D. Of these two routes, the router would select the one with the lower metrics value. You’ll learn more about routing metrics later in this module.
  + If it doesn’t find a matching entry, the router looks for 0.0.0.0 in the first column. This route is the [**default route**](javascript://)—the route to use if no other route is a match. In most cases, the routing table must contain a default route so it can handle traffic with no predefined route, such as DNS messages. The gateway in the third column of this route is called the [**gateway of last resort**](javascript://), which is the router that accepts unrouteable messages from other routers.
  + If no default route is defined, the router will drop the message.

In this scenario, router A finds two matches with LAN D’s network information and chooses the best of these two options based on their respective routing metrics. Router A then determines that it should send the message out the port that faces router C.

1. Step 3

Before it forwards the message, router A decreases the number of hops tallied in the TTL (time to live) field of the packet header. It then sends the message to router C.

1. Step 4

Router C decreases the packet’s hop count by 1, reads the packet’s destination IP address, searches its routing table for matching network information, and determines the message is destined for its own LAN D. It sends the message to switch D on LAN D.

1. Step 5

Using its ARP table, switch D matches the destination IP address with the printer’s MAC address. If switch D didn’t have a matching entry in its ARP table for the network printer’s IP address, it would use an ARP broadcast to request the printer’s MAC address. Switch D then delivers the transmission to the printer, which picks up the message and begins printing.

**Note 9-1**

What’s the difference between a default gateway, a default route, and a gateway of last resort?

* Most hosts have a default gateway—a router or layer 3 switch—where they send all routable messages. Hosts can’t communicate with other networks without a default gateway.
* Most routers have a default route as a backup route when no other route can be determined.
* The default route points to a gateway of last resort. A router’s gateway of last resort is where it sends messages addressed to networks the router can’t find in its routing table.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2bRouting Path Types

Routing paths are determined in one of two ways as described next:

* [**Static routes**](javascript://)—A network administrator configures a routing table to direct messages along specific paths between networks. For example, it’s not uncommon to see a static route between a small business and its ISP. However, static routes can’t adapt to network congestion, failed connections, or device relocations, and they require human intervention to configure or adjust.
* [**Dynamic routes**](javascript://)—A router automatically calculates the best path between two networks and accumulates this information in its routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute messages through a different path. When a router is added to a network, dynamic routing ensures that the new router’s routing tables are updated.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2cRoute

The **route** utility allows you to view a host’s routing table. The route command can also be used to add or delete static routes, which you’ll practice doing in a project at the end of this module. Here are some variations of the route command for different operating systems:

* **Linux or UNIX**—Enter route at a shell prompt.
* **Windows**—Enter route print in a CLI.
* **Cisco’s IOS**—Enter show ip route at the CLI using privileged EXEC mode.

Routing tables on workstations typically contain no more than a few, unique entries, including the default gateway and loopback address. However, routing tables on Internet backbone routers, such as those operated by ISPs, maintain hundreds of thousands of entries.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2dRouting Metrics

Finding the best route or best path for messages to take across networks is one of the most valued and sophisticated functions performed by a router. Some examples of routing metrics used to determine the best path include the following:

* Hop count, which is the number of network segments crossed
* Theoretical bandwidth and actual throughput on a potential path
* Delay, or latency, on a potential path, which decreases performance
* Load, which is the traffic or processing burden sustained by a router in the path
* MTU (maximum transmission unit), which is the largest IP packet size in bytes allowed by routers in the path without fragmentation (excludes the frame used by the local network)
* [**Routing cost**](javascript://), which is a value assigned to a particular route as judged by the network administrator; the more desirable the path, the lower its cost
* Reliability of a potential path, based on historical performance
* A network’s topology

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2eRouting Protocols to Determine Best Paths

To determine the best path, routers communicate with each other through [**routing protocols**](javascript://). Routing protocol messages, similar to scouting parties exploring unknown terrain, go forth to collect data about current network status and contribute to the selection of best paths. Routers use this data to create their routing tables. Keep in mind that routing protocols are not the same as routable protocols such as IP (which can be routed across networks). However, routing protocols might piggyback on IP to reach their destinations. Also, the various routing protocols operate at different layers of the OSI model—usually layer 3, layer 4, or layer 7. However, this discussion is primarily concerned with the effects that routing protocols have on layer 3 routing activities.

Routers rate the reliability and priority of a routing protocol’s data based on these criteria:

* [**AD (administrative distance)**](javascript://)—Each routing protocol is assigned a default AD, which is a number indicating the protocol’s reliability, with lower values being given higher priority. This assignment can be changed by a network administrator when one protocol should take precedence over a previously higher-rated protocol on that network.
* [**Convergence time**](javascript://)—Routing protocols are also rated on the time it takes to recognize a best path in the event of a change or network outage. Some routing protocols are more efficient than others at communicating topology changes across the network.
* [**Overhead**](javascript://)—A routing protocol is rated on its overhead, or the burden placed on the underlying network to support the protocol. The difference here is related to how much processing power each routing protocol requires of routers and how much information must be transferred between routers and how often.

The most common routing protocols are summarized in [Table 9-2](javascript://) and are described in more detail in the following sections. Other routing protocols exist, but their descriptions exceed the scope of this course.

**Table 9-2**

### Summary of Common Routing Protocols

| **Routing protocol** | **Type** | **Algorithm used** |
| --- | --- | --- |
| RIP (Routing Information Protocol) | IGP | Distance-vector |
| RIPv2 (Routing Information Protocol, version 2) | IGP | Distance-vector |
| OSPF (Open Shortest Path First) | IGP | Link-state |
| IS-IS (Intermediate System to Intermediate System) | IGP | Link-state |
| EIGRP (Enhanced Interior Gateway Routing Protocol) | IGP | Advanced distance-vector |
| BGP (Border Gateway Protocol) | EGP | Advanced distance-vector or path vector |

### Exam Tip

[Table 9-2](javascript://) provides an overview of the routing protocols covered in this module. For the CompTIA Network+ exam, it’s important to know which routing protocols function within an autonomous system and which of these protocols communicate between these systems. You’ll also want to know the classification of protocols, especially distance-vector versus link-state.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

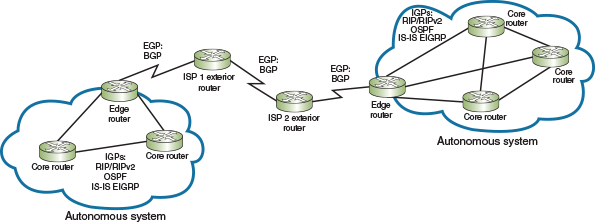
## 9-2fInterior and Exterior Gateway Protocols

As you examine [Table 9-2](javascript://), you can see that a routing protocol is classified as either an IGP or an EGP. Here’s an explanation of the two types, which are diagrammed in [Figure 9-6](javascript://):

* [**IGPs (interior gateway protocols)**](javascript://) are routing protocols used by core routers and edge routers within autonomous systems. IGPs are often grouped according to the algorithms they use to calculate best paths, as follows:
  + [**Distance-vector routing protocols**](javascript://) calculate the best path to a destination based on the distance to that destination. Some distance-vector routing protocols factor only the number of hops to the destination, whereas others consider route latency and other network traffic characteristics. Distance-vector routing protocols periodically exchange their entire routing tables with neighboring routers even if there’s not been a change to a route, which requires the transfer of large amounts of data simply to keep routing tables updated. Also, routers relying on this type of routing protocol must accept the data they receive from their neighbors and cannot independently assess network conditions two or more hops away. This limitation is sometimes called “routing by rumor,” and it results in slow convergence and higher likelihood of persistent errors when network conditions change. RIP and RIPv2 are distance-vector routing protocols.
  + [**Link-state routing protocols**](javascript://) focus less on the number of hops between routers and more on the state of a connection. These protocols collect information about all their connected links and send that information to other routers on the network. Other routers, then, can use this information about links throughout the network to build their own routing tables, independently mapping the network and determining the best path between itself and a message’s destination node. These protocols tend to adapt more quickly to changes in the network, but they can also be more complex to configure and troubleshoot. They also require more processing power to incorporate information from throughout the network to build each device’s routing table. Part of this resource demand is offset by the fact link-state routing protocols only send information when something changes. OSPF and IS-IS are link-state routing protocols, and they’re highly scalable for very large networks.
  + [**Hybrid routing protocols**](javascript://) exhibit characteristics of both distance-vector and link-state routing protocols. For example, Cisco’s EIGRP functions primarily as a distance-vector routing protocol but incorporates elements of link-state routing, for example, by syncing link information across the network only when something changes.
* [**EGPs (exterior gateway protocols)**](javascript://) are routing protocols used by edge routers and exterior routers to distribute data outside of autonomous systems. The one EGP protocol you need to know for the Network+ exam is the only EGP currently in use, BGP.

**Figure 9-6**

BGP is the only routing protocol that communicates across the Internet



Enlarge Image

**Note 9-2**

An older routing protocol named Exterior Gateway Protocol is obsolete. However, the generic term exterior gateway protocol now refers to any routing protocol that routes information between autonomous systems.

Let’s look at the details of these routing protocols, beginning with RIP and RIPv2, which are both outdated but still in use on many networks because of their simplicity and compatibility with older routers.

### Legacy Networking: RIP (Routing Information Protocol)

[**RIP (Routing Information Protocol)**](javascript://), a distance-vector routing protocol, is the oldest routing protocol. Here are some notable considerations when using RIP on a network.

Advantages:

* **Simplicity**—Quick and easy configuration.
* **Stability**—Prevents routing loops from continuing indefinitely by limiting the number of hops a message can take between its source and its destination to 15. If the number of hops in a path exceeds 15, the network destination is considered unreachable.

Disadvantages:

* **Limited metrics**—Only considers the number of hops between nodes when determining the best path rather than other, more complex factors.
* **Excessive overhead**—Broadcasts routing tables every 30 seconds to other routers, regardless of whether the tables have changed.
* **Poor convergence time**—Might take several minutes for new information to propagate to the far reaches of the network.
* **Limited network size**—Does not work well in very large network environments where data might have to travel through more than 15 routers to reach its destination (for example, on a metro network).
* **Slower and less secure**—Outdated by newer routing protocols.

Developers have improved RIP since its release in 1988 and informally renamed the original RIP as RIPv1 (Routing Information Protocol, version 1). The next version of RIP was published in 1994 and standardized by the IETF in 1998. [**RIPv2 (Routing Information Protocol, version 2)**](javascript://) generates less broadcast traffic and functions more securely than RIPv1. An extension to RIPv2 that was first proposed in 1997 is RIPng (RIP next generation), which extends RIP support to IPv6. Still, RIPv2 and RIPng cannot exceed 15 hops, and they are also considered outdated routing protocols.

**Note 9-3**

When discussing limitations of routing protocols, the 15-hop limit is specific to RIP and its later versions. This is an identifying factor you can use to distinguish RIP from other routing protocols.

### OSPF (Open Shortest Path First)

[**OSPF (Open Shortest Path First)**](javascript://) is an IGP and a link-state routing protocol used on core or edge routers. It was introduced as an improvement to RIP and can coexist with RIP or RIPv2 on a network. Characteristics include the following:

* **Supports large networks**—Imposes no hop limits on a transmission path.
* **Complex algorithms**—Calculates more efficient best paths than RIP. Under optimal network conditions, the best path is the most direct path between two points. If excessive traffic levels or an outage prevent data from following the most direct path, a router might determine that the most efficient path actually goes through additional routers.
* **Shared data**—Maintains a database of the other routers’ links. If OSPF learns of the failure of a given link, the router can rapidly compute an alternate path.
* **Low overhead, fast convergence**—Demands more memory and CPU power for calculations, but keeps network bandwidth to a minimum with a very fast convergence time, often invisible to users.
* **Stability**—Uses algorithms that prevent routing loops.
* **Multi-vendor routers**—Supported by all modern routers. It is commonly used on autonomous systems that rely on a mix of routers from different manufacturers.

### IS-IS (Intermediate System to Intermediate System)

Another IGP, which is also a link-state routing protocol, is [**IS-IS (Intermediate System to Intermediate System)**](javascript://). IS-IS uses a best-path algorithm similar to OSPF’s. It was originally codified by ISO, which referred to routers as “intermediate systems,” thus the protocol’s name. Unlike OSPF, however, IS-IS is designed for use on core routers only. Also, IS-IS is not handcuffed to IPv4 like OSPF is, so it’s easy to adapt to IPv6. Service providers generally prefer to use IS-IS in their own networks because it’s more scalable than OSPF, but OSPF is still more common.

### EIGRP (Enhanced Interior Gateway Routing Protocol)

[**EIGRP (Enhanced Interior Gateway Routing Protocol)**](javascript://), an IGP, was developed in the mid-1980s by Cisco Systems. It is an advanced distance-vector protocol that combines some of the features of a link-state protocol and so is sometimes referred to as a hybrid protocol. With a fast convergence time and low network overhead, it’s easier to configure and less CPU-intensive than OSPF. EIGRP also offers the benefits of supporting multiple protocols and limiting unnecessary network traffic between routers.

Originally, EIGRP was proprietary to Cisco routers. In 2013, parts of the EIGRP standard were released to the public so that networks running routers from other vendors can now use EIGRP. It accommodates very large and heterogeneous networks, but it is still optimized for Cisco routers and not many manufacturers have made the transition. On LANs that use Cisco routers exclusively, EIGRP is generally preferred over OSPF.

### BGP (Border Gateway Protocol)

The only current EGP is [**BGP (Border Gateway Protocol)**](javascript://), which has been dubbed the “protocol of the Internet.” Whereas OSPF and IS-IS scouting parties only scout out their home territory, a BGP scouting party can go cross-country. BGP spans multiple autonomous systems and is used by edge and exterior routers on the Internet. Here are some special characteristics of BGP:

* **Path-vector routing protocol**—Communicates via BGP-specific messages that travel between routers over TCP sessions.
* **Efficient**—Determines best paths based on many factors.
* **Customizable**—Can be configured to follow policies that might, for example, avoid a certain router, or instruct a group of routers to prefer one route over other available routes.

BGP is the most complex of the routing protocols mentioned in this module. If you maintain networks for an ISP or large telecommunications company, you will need to understand BGP in depth.

Go to pg.

[**help**](javascript://)

Application Opened

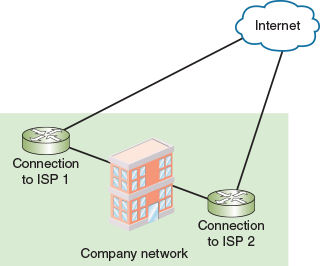
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2gRouting Redundancy

Recall that fault tolerance on a network is accomplished through using redundant hardware, connections, services, and copies of data. For example, if one router fails, another router can take over. You might even have a cluster of routers so your network could tolerate the failure of multiple devices without losing service. On a small network, having two or three ISP connections with one or two routers for each might provide sufficient redundancy. Larger networks should also have multiple ISP connections with each using geographically separate hardware and network media. For example, you might want one ISP connection to enter your property from one direction and another ISP connection to enter from the other side of your building or campus (see [Figure 9-7](javascript://)). These diverse paths increase your network’s fault tolerance should the proverbial backhoe damage underground lines from one ISP, or in case of flooding, fire, power outage, or other damage that is restricted to a relatively small area.

**Figure 9-7**

Redundant ISP connections to the Internet



If you’re paying for two or more ISP connections, should you use both of them all the time, or should one be kept only as a backup when the first one fails? This question highlights the key difference between two contrasting redundancy techniques, as described next:

* [**Active-active redundancy**](javascript://)—All redundant resources are active at all times, and work is distributed among them. For example, you might load balance your Internet traffic between two ISP connections, but either ISP service could take over if the other one fails. This arrangement can provide increased performance during normal operation, as all your available resources are actively working. You might have the load distributed evenly among all resources, or you might have one or more redundant resources running a reduced load.
* [**Active-passive redundancy**](javascript://)—Only one or a few redundant resources are active at any time with the backup devices on standby ready to fill in if they’re needed. For example, you might run all your Internet traffic over a single ISP service, but you have a second one on standby in case it’s needed.

So how do you make this happen when you’re running two routers in a network? For example, you know you can only configure one default gateway on your computer. Do you configure half your network hosts to use one default gateway and half to use the other? Is there a way to make them automatically failover if one gateway fails?

Instead of managing redundancy manually, you can configure an [**FHRP (First Hop Redundancy Protocol)**](javascript://) on a router or layer 3 switch to provide a single VIP (Virtual IP) address as the default gateway that, in turn, potentially points to multiple routers. Two popular FHRPs you learned about in an earlier module and a third FHRP that is gaining in popularity are described next:

* **VRRP (Virtual Router Redundancy Protocol)—**Industry standard across vendors. The VIP points to the primary, active router, and all other routers stand by as potential backups. Configurations are made using the vrrp command.
* **HSRP (Hot Standby Routing Protocol)**—Proprietary to Cisco. The VIP points to the active router, a standby router is configured for auto failover, and other routers listen for indications the active and standby routers have both failed. Configurations are made using the standby command.
* **GLBP (Gateway Load Balancing Protocol)**—Also proprietary to Cisco devices. GLBP gateways are weighted according to priority, and traffic is load balanced among all gateways. Configurations are made using the glbp command.

**Remember This…**

* Identify the primary differences between the routing protocols RIP, RIPv2, OSPF, EIGRP, and BGP.
* Compare link-state, distance-vector, and hybrid routing protocol characteristics.
* Explain how to configure router redundancy using common FHRPs.
* Use the route command to view routing tables in various OSs.

**Self-Check**

1. Which routing protocol runs between your network’s edge router and your ISP’s edge router?

Answer

* 1. EIGRP
  2. RIPv2
  3. OSPF
  4. BGP

1. Which command will output your Windows computer’s routing table?

Answer

* 1. show ip route
  2. route print
  3. route

1. Which routing protocol is limited to 15 hops?

Answer

* 1. EIGRP
  2. OSPF
  3. BGP
  4. RIPv2

**You’re Ready**

You’re now ready to complete [Project 9-1: Create a Routing Table Entry in Windows](javascript://), or you can wait until you’ve finished reading this module.

**You’re Ready**

You’re now ready to complete [Project 9-2: Create a Path MTU Black Hole](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-3WAN Connectivity

### Certification

* 1.2

Explain the characteristics of network topologies and network types.

* 1.8

Summarize cloud concepts and connectivity options.

* 2.1

Compare and contrast various devices, their features, and their appropriate placement on the network.

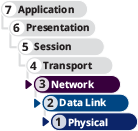
* 2.2

Compare and contrast routing technologies and bandwidth management concepts.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

Average reading time: 42 minutes



Connecting your network to other networks plays an integral role in building and managing a network. However, the tools you’ll use to connect networks vary greatly according to the size of your network, your network’s bandwidth needs, and the relative locations of your network’s segments. Imagine you’re starting a new company. Initially, you’re working from home and the only employee is you. Your WAN requirements consist entirely of connecting your home network to the Internet. However, as your company grows, you’ll need other kinds of WAN connections. Throughout this section, you’ll read about WAN connectivity options that will serve your company as it expands from your basement into a global entity. Notice the ways your WAN needs shift over time and what technologies are available to meet those needs.

Some of these service options are called by common names that you might recognize if you’ve ever shopped around for home or business Internet service or if you’ve noticed commercials or billboards advertising Internet subscription options. Many of these connections use existing telephone lines, the existing cable TV infrastructure, or specialized copper or fiber cables. Later in this module, you’ll also learn about WAN services provided wirelessly, including cellular and satellite connections.

As you compare options for WAN services, keep in mind a significant difference between technologies—whether the connection is shared among many customers or dedicated to one customer. The following list explains these two options:

* [**Broadband**](javascript://)—Especially well-suited for residential customers, the cables (whether telephone, coaxial, or fiber) and available bandwidth are shared between multiple customers. The ISP makes a “best effort” attempt to provide up to the advertised bandwidth, and actual performance varies considerably during busy usage. Bandwidth is also [**asymmetrical**](javascript://), or asynchronous, meaning download speeds (data traveling from the carrier’s switching facility to the customer) are faster than upload speeds (data traveling from the customer to the carrier’s switching facility). For a higher premium, businesses can get faster broadband speeds and possibly one or more static IP addresses included in the package. However, uptime, service, and bandwidth are still not guaranteed.
* [**DIA (dedicated Internet access)**](javascript://)—The cable itself or a portion of its available bandwidth is dedicated to a single customer; this is more common for business customers and comes with an SLA-defined (service-level agreement) guarantee of minimum uptime percentages and maximum recovery times if the service goes down. Bandwidth is [**symmetrical**](javascript://), or synchronous, meaning download and upload speeds are about the same. This is especially important for businesses that back up large amounts of data online. The subscription will also often include a certain number of static IP addresses.

**Applying Concepts 9-1**

### Test Your Internet Connection’s Speed

You can test your own Internet connection to see what the current upload and download speeds are using a [**bandwidth speed tester**](javascript://), or a speed test website. During the test, data will be sent to your computer and then requested from your computer to measure download and upload speeds, respectively. Complete the following steps:

1. 1

In your browser, go to [speedtest.net](http://speedtest.net/). At the time of this writing, you start the test by clicking **GO**. The test begins, as shown in [Figure 9-8](javascript://).

1. 2

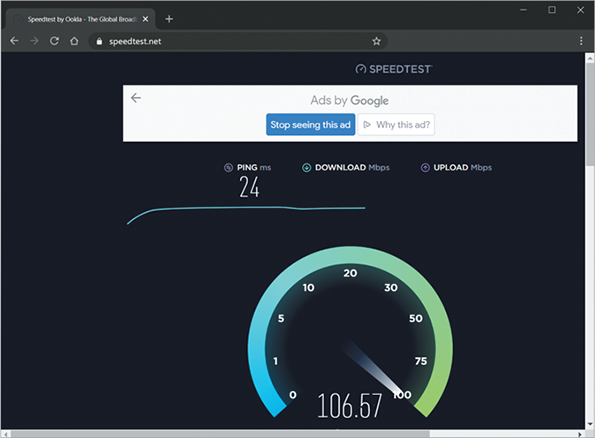
Wait for the test to complete and then write down your speed test results. What are your current download and upload speeds?

1. 3

Try a different site and compare results. Go to [verizon.com/speedtest](http://verizon.com/speedtest), click **Get started** and wait for the test to complete (see [Figure 9-9](javascript://)). What are the results this time? How do they compare to your first results? Why do you think this is?

**Figure 9-8**

Speed test in progress

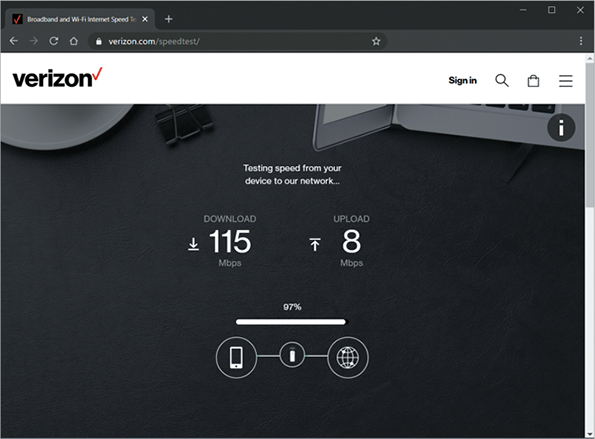


Enlarge Image

Source: Ookla, LLC

**Figure 9-9**

Another speed test for comparison



Enlarge Image

Source: Verizon

While these websites are designed to test throughput between your network and a host on the Internet, you can also use throughput testing software, such as Lakehorn’s Network Speed Tester, to check the performance of your local network. Recall from [Hands-On Project 5-4](javascript://) that you also used the TotuSoft LAN Speed Test application and the TamoSoft Throughput Test application.

These first three WAN connectivity options cover broadband ISP services you might use for your home office: DSL, cable, and fiber Internet. Then you’ll learn about high-speed WAN service options more commonly used by businesses.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

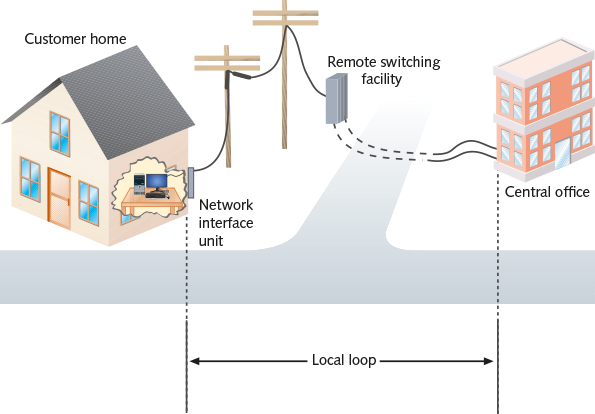
## 9-3aDSL (Digital Subscriber Line)

[**DSL (digital subscriber line)**](javascript://) is a WAN connection method introduced by researchers at Bell Laboratories in the mid-1990s. It operates over the [**PSTN (public switched telephone network)**](javascript://), also called POTS (plain old telephone service), which is a network of lines and carrier equipment that provide landline telephone service to homes and businesses. Originally, the PSTN carried only analog traffic. All its lines were copper wires, and switching was handled by operators who manually connected calls upon request. Today, switching is computer controlled, and nearly all the PSTN uses digital transmission and fiber for backbone connections. Signals may deliver voice, video, or data traffic and travel over fiber-optic or twisted-pair copper cable connections.

The telephone company terminates lines and switches calls between different locations at the CO (central office). The portion of the PSTN that connects any residence or business to the nearest CO is known as the [**local loop**](javascript://), or the “last mile” (though it is not necessarily a mile long), as illustrated in [Figure 9-10](javascript://). It’s the part of the PSTN most likely to still use copper wire and carry analog signals. That’s because extending fiber-optic cable to every residence and business is costly. However, fully digital connections are increasingly common, especially for businesses that rely heavily on WAN connections. No matter what kind of media is used, the end of the local loop—and the end of the carrier’s responsibility for the network—is the customer’s demarcation point where wires terminate at the NIU.

**Figure 9-10**

Local loop portion of the PSTN



Enlarge Image

DSL can support multiple data and voice channels over a single line, but it can span only limited distances without the help of repeaters. Also, the distance between the customer and the central office affects the actual throughput a customer experiences. Close to the central office, DSL achieves its highest maximum throughput. The farther away the customer’s premises, the lower the throughput.

To understand how DSL and voice signals can share the same line, it’s helpful to note that telephone lines carry voice signals over a very small range of frequencies between 300 and 3300 Hz. This leaves higher, inaudible frequencies unused and available for carrying data. DSL uses data modulation techniques at the physical layer of the OSI model to achieve extraordinary data throughput over regular telephone lines. Recall that modulation techniques can allow a single channel to carry more data per cycle of a signal. Depending on its version, a DSL connection might use a modulation technique based on amplitude or phase modulation to alter the waves at higher frequencies to carry data. The types of modulation used by different DSL versions affect their throughput and the distance their signals can travel before requiring a repeater. Modulation is performed by a DSL modem. A [**DSL modem**](javascript://), such as the one shown in [Figure 9-11](javascript://), contains ports to connect both to your incoming telephone line and to your computer or network connectivity device.

**Figure 9-11**

A DSL modem



Source: Zoom Telephonics, Inc.

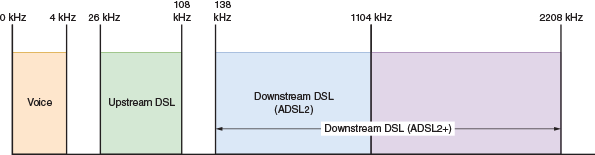
### Types of DSL

The types of DSL vary according to their throughput rates, data modulation techniques, capacity, and distance limitations, as well as how they use the PSTN. The term xDSL (extended DSL) refers to all DSL varieties. In each case, the x in xDSL is replaced by the variety’s name (there’s that algebra again). The better-known DSL varieties include the following:

* **ADSL (asymmetric DSL)**—Faster download speeds than upload speeds and is the most common form of DSL. Asymmetrical communication is well suited to users who receive more information from the network than they send to it—for example, people watching movies online or people surfing the web. ADSL and VDSL (discussed next) create multiple narrow channels in the higher frequency range to carry more data. For these versions, a splitter must be installed at the carrier and at the customer’s premises to separate the data signal from the voice signal before it reaches the terminal equipment (for example, the phone or the computer). The latest version of ADSL is ADSL2+, which extends the reach of DSL to within two kilometers of the provider’s location. It also provides a maximum theoretical throughput of 24 Mbps downstream and a maximum of 3.3 Mbps upstream (depending on how close it is to its source). The reason upstream and downstream bandwidth are different on a DSL line is because of the way the bandwidth is broken up for different purposes. [Figure 9-12](javascript://) shows the distribution of bandwidth for voice, upstream, and downstream communications.
* **VDSL (very high bit rate DSL or variable DSL)**—Faster than ADSL and is also asymmetric, with faster download speeds than upload speeds. A VDSL line that carries up to 52 Mbps in one direction and up to 16 Mbps in the opposite direction can extend only a maximum of 1.6 km before dropping to speeds similar to ADSL2+. VDSL2 offers throughput speeds nearing 100 Mbps in both directions but drops off quickly at even shorter distances. These limitations might suit businesses located close to a telephone company’s CO (for example, in the middle of a metropolitan area), but it won’t work for most individuals.
* **SDSL (symmetric DSL)**—Equal download and upload speeds maxing out around 2 Mbps. Symmetrical transmission is suited to users who both upload and download significant amounts of data—for example, a bank’s branch office that sends large volumes of account information to the central server at the bank’s headquarters and, in turn, receives large amounts of account information from the central server at the bank’s headquarters. SDSL cannot use the same wire pair that is used for voice signals. Instead, this type of DSL uses the extra pair of wires contained in a telephone cable (which are otherwise typically unused).

**Figure 9-12**

More bandwidth allocated for downstream than upstream



Enlarge Image

**Note 9-4**

Published distance limitations and throughput can vary from one service provider to another, depending on how far the provider is willing to guarantee a particular level of service. In addition, service providers may limit each user’s maximum throughput based on terms of the service agreement. For example, in 2011, AT&T capped the total amount of data transfer allowed for each of its DSL subscribers to 150 GB per month. The company instituted the new policy in response to a dramatic spike in downstream bandwidth usage due to Netflix streaming. In fact, in 2010, Netflix accounted for nearly 30 percent of all downstream Internet traffic requested by fixed users in the United States. Today, many providers cap a subscriber’s high-speed data usage, although typically the caps are higher now than the one in this example.

Telecommunications carriers and related vendors have positioned DSL as a competitor for cable broadband and leased line services. The installation, hardware, and monthly access costs for DSL are significantly less than the cost for other options, but the cost in comparison with cable broadband varies widely by location. At the time of this writing, DSL home Internet service costs approximately $35 per month in the United States, though prices vary by speed and location. Generally speaking, DSL throughput rates, especially upstream, are lower than cable broadband, which is its main competition among residential customers.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

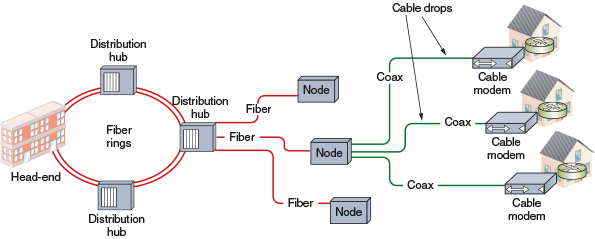
## 9-3bCable Broadband

While local and long-distance phone companies strive to make DSL the preferred method of Internet access for consumers, cable companies are pushing their own connectivity option. [**Cable broadband**](javascript://) (also called cable Internet or cable modem access) is based on the coaxial cable wiring used for TV signals, although in reality, much of the coaxial infrastructure has been replaced with fiber. Cable broadband was standardized by an international, cooperative effort orchestrated by CableLabs that yielded a suite of specifications called [**DOCSIS (Data Over Cable Service Interface Specifications)**](javascript://). Cable broadband service is typically offered at asymmetric speeds, such as up to 70 Mbps download and 7 Mbps upload. The newest DOCSIS standard, 4.0, theoretically allows for symmetric multi-gigabit speeds up to 10 Gbps downstream and 6 Gbps upstream, thus rivaling some fiber-optic Internet service options once experienced speeds start to approach the standard’s defined maximums.

In fact, many cable companies employ fiber cabling for a significant portion of their physical infrastructure. As illustrated in [Figure 9-13](javascript://), [**HFC (hybrid fiber coaxial)**](javascript://) networks use fiber-optic cabling to connect the cable company’s distribution center, or headend, to distribution hubs and then to optical nodes near customers. Either fiber-optic or coaxial cable then connects a node to each customer’s business or residence via a connection known as a cable drop.

**Figure 9-13**

HFC infrastructure



Enlarge Image

Cable broadband connections require that the customer use a special [**cable modem**](javascript://), a device that modulates and demodulates signals for transmission and reception via cable wiring (see [Figure 9-14](javascript://)). The cable modem must conform to the correct version of DOCSIS supported by the ISP. Most newer cable modems use DOCSIS 3.1 with 4.0 becoming available, but ISPs might charge extra when later modem models are used. [Table 9-3](javascript://) presents the versions of DOCSIS along with their specifications.

**Figure 9-14**

A cable modem



Source: Zoom Telephonics, Inc.

**Table 9-3**

### DOCSIS Versions and Specifications

| **Version** | **Maximum upstream throughput** | **Maximum downstream throughput** | **Description** |
| --- | --- | --- | --- |
| DOCSIS 1.x (1.0 and 1.1) | 10 Mbps | 40 Mbps | Outdated; single channel; throughput was shared among customers |
| DOCSIS 2.x (2.0 and 2.0 + IPv6) | 30 Mbps | 40 Mbps | Outdated; single channel; reduces disparity between upstream and downstream throughputs |
| DOCSIS 3.0 | 100 Mbps | 1000 Mbps | Multiple channels: minimum of 4, no maximum |
| DOCSIS 3.1 | 1–2 Gbps | 10 Gbps | In 2017, CableLabs published Full Duplex DOCSIS 3.1, which offers symmetrical Gigabit upload and download speeds. |
| DOCSIS 4.0 | 6 Gbps | 10 Gbps | Expanding upon DOCSIS 3.1 standards, CableLabs added RF bandwidth options for upstream speeds to support full-duplex, multigigabit throughput. |

Like DSL modems, cable modems operate at the physical and data link layers of the OSI model, and, therefore, do not manipulate higher-layer protocols like IP. The cable modem connects to a customer’s PC via the NIC’s RJ-45, USB, or wireless interface. Alternatively, the cable modem could connect to a networking device, such as a switch or router, thereby supplying bandwidth to a LAN rather than to just one computer. It’s also possible to use a device that combines cable modem functionality with a SOHO router to share available bandwidth on an entire network.

**Applying Concepts 9-2**

### Determine a Cable Modem’s DOCSIS Version

You can determine the DOCSIS version of a cable modem on a SOHO network with a little detective work. This activity requires a SOHO network serviced by cable broadband and a computer (Windows, Linux, or Mac) connected to the network. Alternatively, you can find a cable modem for sale online and use the posted information and photos for parts of this activity. Complete the following steps to identify the DOCSIS version of a cable modem:

1. 1

Examine the labels on the cable modem to determine the device’s manufacturer and model number. In some cases, the DOCSIS version might be printed on one of these labels. If you’re looking at a cable modem online, examine the posted specifications for this information. If the DOCSIS version isn’t labeled or posted, continue with the following steps.

1. 2

Research the manufacturer and model number information online. You might find the DOCSIS information while conducting your research. If not, the minimum information you need is the cable modem’s default internal IP address (such as 192.168.0.1 or 192.168.100.1) and admin username and password (if there is one).

1. 3

Choose one of the following options:

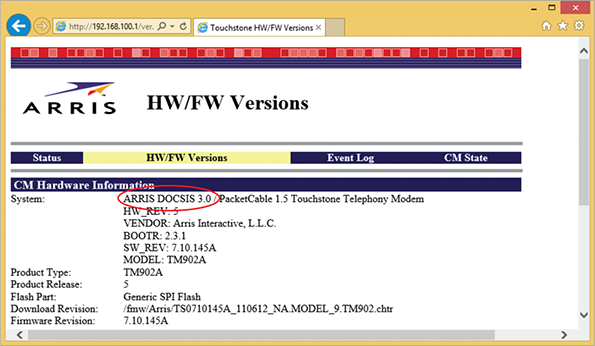
* 1. If you’re researching a cable modem listed online, check the manufacturer’s website for an emulator to interact with the cable modem’s user interface. Alternatively, you can choose a TP-Link cable modem emulator at [tp-link.com/us/support/emulator](http://tp-link.com/us/support/emulator)**/**.
  2. If you’re working with a cable modem on your own network, enter the default internal IP address in a web browser and log on if necessary.

1. 4

Explore the user interface to locate the cable modem’s hardware information. [Figure 9-15](javascript://) shows the hardware information for a cable modem made by ARRIS. What is the DOCSIS version of your cable modem?

**Figure 9-15**

This cable modem’s DOCSIS version is 3.0



Enlarge Image

Source: ARRIS

Like DSL, cable broadband provides a dedicated and always-up, or continuous, connection that does not require dialing up a service provider to create the connection. Unlike DSL, cable broadband requires many subscribers to share the same local line, thus raising concerns about security and actual (versus theoretical) throughput. For example, if your cable company supplied you and five of your neighbors with cable broadband services, one of your neighbors could, with some technical prowess, capture the data that you transmit to the Internet. (Modern cable networks provide encryption for data traveling to and from customer premises; however, these encryption schemes can be thwarted.)

Moreover, the throughput of a cable line is fixed. As with any fixed resource, the more one person uses, the less that is left for others. In other words, the greater the number of users sharing a single line, the less throughput available to each individual user. Cable companies counter this perceived disadvantage by rightly claiming that at some point (for example, at a remote switching facility), a telephone company’s DSL bandwidth is also fixed and shared among a group of customers.

In the United States, cable broadband access costs approximately $30–$60 per month when bundled with cable TV and/or digital voice services. Cable broadband is less often used in businesses than DSL, primarily because most office buildings do not contain an existing coaxial cable infrastructure.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3cFiber

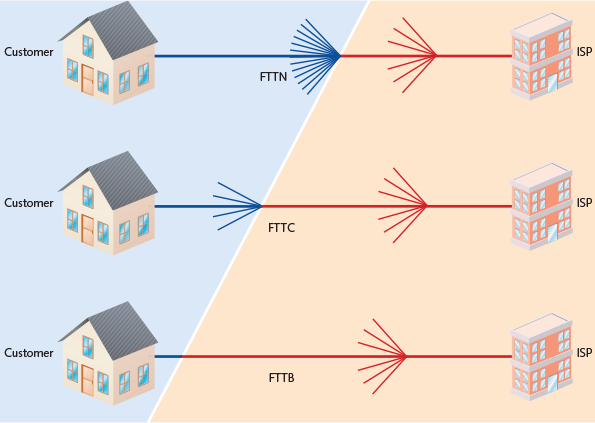
The fact is, most of the Internet backbone already runs on fiber. Even if you connect your new home office to the Internet via an old-school dial-up connection, most of the distance your data travels on the Internet will run over fiber cables. It’s that last mile to your location that really slows your data down. While DSL and cable broadband offer significantly faster speeds than dial-up, they’re still very slow by modern standards.

A growing trend in ISP offerings for WAN connection services is to offer FTTN (fiber-to-the-node), FTTH (fiber-to-the-home), or similar arrangements. In these scenarios, the ISP runs a fiber connection to one of a few nearby locations, as illustrated in [Figure 9-16](javascript://) and described next:

* **FTTN (fiber-to-the-node** or **fiber-to-the-neighborhood)**—A nearby service junction that serves a few hundred customers
* **FTTC (fiber-to-the-curb)**—A nearby pole or equipment cabinet that serves a few customers
* **FTTB (fiber-to-the-building)** or **FTTH (fiber-to-the-home)**—The junction box at the demarc to your building

**Figure 9-16**

Getting fiber closer to your own network increases your Internet speeds



Enlarge Image

As you can see, each progressive scenario brings the fiber closer to your own network. The closest options cost more but also reduce the distance over which your data must traverse copper cabling.

While this option has limited availability in many market areas, those who can choose fiber often do. Fiber’s higher speeds, with symmetric speeds often reaching as high as 1–2 Gbps for home or small business fiber services, offset the increased cost of up to $100 monthly. Additionally, so long as the ISP can provide you with a fiber connection, your distance from their offices won’t negatively affect your experienced speeds.

Fiber technology and availability to business customers—and even to residential customers—continues to improve. Rising market demand for last-mile fiber service is causing increased investments by ISPs into their access-level fiber infrastructure. Traditionally, fiber investment focused on long-haul connections across hundreds and thousands of miles. In contrast, [**MONs (metropolitan optical networks)**](javascript://) bring fiber to the customer. This dense, localized grid of junctions and fiber cables attempts to make direct fiber connections available to as many customers as possible while balancing the significant expense of replacing existing telephone and coaxial cable infrastructure with fiber equipment and fiber-optimized technologies.

You’ve already learned about some of the technologies that handle multiple signals on each fiber connection, such as DWDM (dense wavelength division multiplexing). However, DWDM does not easily lend itself to handling the high numbers of communications channels and the wide variety of network protocols needed within a metro network environment. This mismatch between what pre-existing fiber technology was designed to do and what is needed in the metro market is sometimes referred to as the “metro gap.” In response to these emerging needs, newer technology has been developed or adapted to support MONs and the expectations of customers in these markets. With 100 Gbps speeds already available on long-haul connections, the industry is now aiming for similar speeds for MONs on the ISP’s end of broadband fiber connections.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3dLeased Lines

When you first established your imaginary company at the beginning of this section, broadband access to the Internet from your basement office was sufficient. Perhaps you began with cable or DSL and then, as you started to earn profits, you moved to a fiber connection. Excitingly, your business continued to grow. Within a few months, your basement was no longer large enough to hold all your inventory. Initially, you rented storage space in a small warehouse while you continued to work from home. But soon you realized you were spending several hours a week at the storage unit and out of touch with your customers and small group of employees. You moved into a larger warehouse rental that included office space, and you decided to open two storefronts, one in your hometown and another in a neighboring city.

At this point, you realize your broadband Internet connection can no longer provide the support your business needs. Instead of basic Internet access, you need to connect your three locations with higher and more reliable throughput speeds to support the following activities:

* VoIP calls with customers and vendors
* E-commerce traffic to your website
* Sales activity from physical storefronts
* Upload and download traffic to exchange large graphic files with customers

You call your local ISP asking how to get dedicated WAN connections. The ISP suggests that you consider [**leased lines**](javascript://) for each location, which would provide dedicated bandwidth on fiber optic connections. What are the advantages and disadvantages of this option for your business?

Where fiber broadband offers the benefits of fiber optic technology, leased fiber takes all that speed boost and pools the bandwidth for a single customer. While a leased line’s dedicated bandwidth might be listed at a lower speed than the maximum theoretical speeds advertised for fiber broadband services, a dedicated line offers the following advantages:

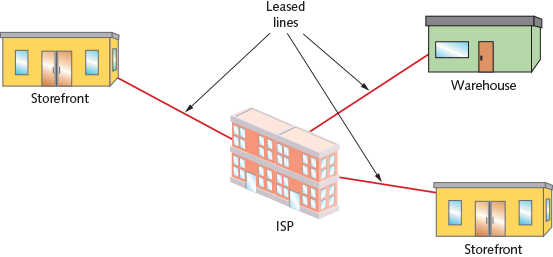
* **Dedicated bandwidth**—The customer pays for a specific bandwidth (such as 2 Gbps) and reserves that bandwidth for their sole use without having to share it with other customers. Throughput won’t fluctuate in response to traffic demands from other customers.
* **Symmetrical bandwidth**—Leased line speeds are typically symmetrical, meaning upload and download speeds will be the same.
* **SLA-backed guarantee**—Performance is backed by SLA-enforced uptime, repair time, and possibly backup options (such as having a broadband connection available during an outage). If bandwidth falls below a defined threshold, the customer has options for recourse to protect their business activities during the outage.

When subscribing to a leased line, existing fiber optic cabling can be configured for the leased line, or a dedicated fiber optic cable must be installed to connect the customer to the nearest ISP exchange, or PoP (Point of Presence). Some of this installation cost is covered by the ISP, but certain expenses might be charged back to the customer. Alternatively, new cables can be installed to directly connect a business’s own locations. For example, each branch office might have a direct line to the company’s own headquarters.

Ongoing monthly costs of a leased line vary greatly depending on many factors, including required bandwidth and the distance to the ISP’s exchange or between the company’s own locations. Typical costs will range between $300 and $1000 monthly. This can get especially expensive for multiple leased lines, as shown in [Figure 9-17](javascript://). However, this particular arrangement gives each location allotted bandwidth directly to the ISP and on to the Internet. From the ISP’s central office, communications between your locations (such as between the warehouse and a storefront) traverse the ISP’s high-speed backbone network to connect the two leased lines. Further, more locations can easily be added to the company’s leased line network by subscribing to a new leased line for each new location. Alternatively, sometimes what’s needed is a point-to-point leased line between two customer locations. In this case, the ISP cannot provide supportive services, such as monitoring uptime or optimizing VoIP traffic.

**Figure 9-17**

Each location needs its own leased line



Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

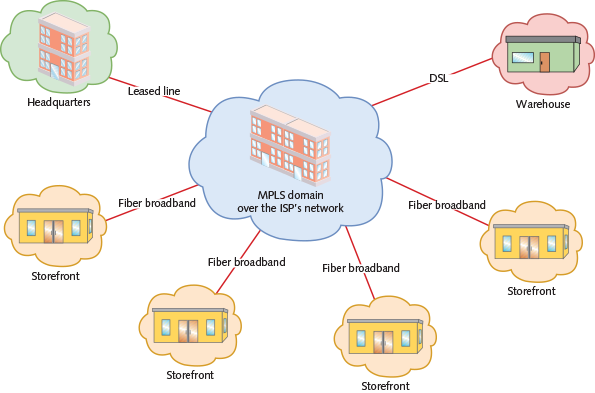
## 9-3eMPLS (Multiprotocol Label Switching)

Your leased lines serve the company well for nearly two years. Both storefronts quickly gain a loyal customer following, and you’re able to optimize your logistics at the warehouse to efficiently service both storefronts and all website customers. As the word spreads and business continues to boom, you decide over the next year to open three more storefronts throughout your region. You also recognize your warehouse space is no longer sufficient, and your employees are tightly cramped in the existing office space. These growing pains lead to the decision to move to a standalone warehouse space and to open a headquarters office in a separate location. With all these new locations to network, managing so many leased lines is becoming unfeasible. Further, you’re told by your IT staff that leased lines don’t offer the level of nuanced control they need for handling the different types of applications on your network. Their suggested solution: MPLS.

[**MPLS (multiprotocol label switching)**](javascript://) was introduced by the IETF (Internet Engineering Task Force) in 1999. As its name implies, MPLS enables multiple types of layer 3 protocols to travel over any one of several connection-oriented layer 2 protocols. Essentially, MPLS allows you to use any connectivity option for each site that makes sense while centrally managing bandwidth between each site. For example, in [Figure 9-18](javascript://), you might have your warehouse connected to the ISP using DSL while your storefronts use fiber broadband and your central office has a leased line.

**Figure 9-18**

MPLS provides cohesive WAN management for multiple connection types



Enlarge Image

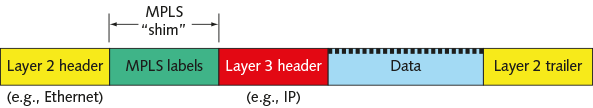
Despite the various service levels of each location’s connection to the ISP, you can manage segmentation and QoS for different types of traffic across your entire network, even if your locations are spread hundreds or thousands of miles apart. These advantages are explained next:

* [**QoS (quality of service)**](javascript://) refers to a group of techniques for adjusting the priority assigned to various types of traffic. For example, you might want to prioritize VoIP traffic over email traffic. One of the characteristics that sets MPLS apart from other WAN technologies is its ability to support QoS traffic shaping across WAN connections.
* Additionally, you can set routes for traffic between sites so the ISP’s routers don’t have to stop and think with each packet where that packet should go next. Essentially, MPLS lets routers function more like switches, working with information in layer 2 headers instead of having to dig to layer 3 and process routing information. This saves time and reduces latency.

With MPLS, the first ISP router (the provider’s edge router, also called the MPLS ingress router) receives a message in a data stream and adds one or more labels to the layer 3 packet. These MPLS labels together are sometimes called a shim because of their placement between layer 3 and layer 2 information. For this reason, MPLS is sometimes said to belong to “layer 2.5.” Next, the network’s layer 2 protocol header is added, as shown in [Figure 9-19](javascript://).

**Figure 9-19**

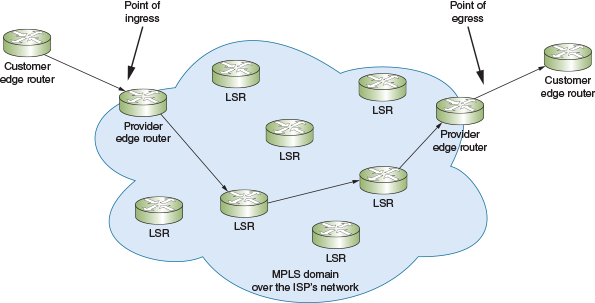
MPLS shim within a frame



These MPLS labels include information about where the router should forward the message next and, sometimes, prioritization information. Each router in the data stream’s path (see [Figure 9-20](javascript://)) revises the label to indicate the packet’s next hop. In this manner, routers on a network can take into consideration network congestion, QoS indicators assigned to the messages, plus other criteria; however, these transit routers, called LSRs (label switching routers), don’t have to take time to map a path for the messages. Network engineers maintain significant control in setting these paths. Consequently, MPLS offers potentially faster transmission than traditionally routed networks.

**Figure 9-20**

Label switching routers simply forward the message without calculating routes



Enlarge Image

While MPLS does offer decreased latency, this benefit is not quite as noticeable today as it was when MPLS first became available. The primary benefits of MPLS today include the following:

* MPLS connections are highly scalable for businesses, which means a business can add more and longer connections for less cost than similarly scaled leased lines.
* Customers can prioritize their own traffic across the WAN according to QoS attributes, such as giving VoIP traffic higher priority over email traffic.
* The ability to label traffic offers more reliability, predictability, and security (when properly implemented) than when using cheaper connections over the open Internet.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3fCloud Connectivity Options

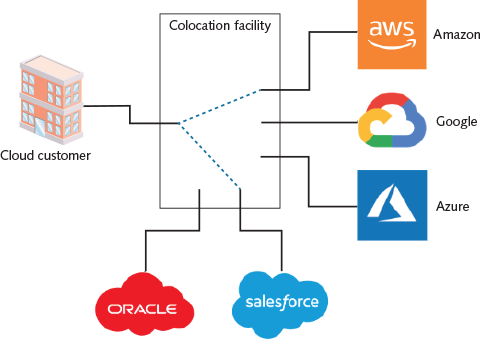
Over the next few months, as you’re working through the growing pains of adding new storefronts and moving offices, your IT team suggests some additional improvements to your network configurations that will better serve your company into the next phase. Primarily, they suggest that you migrate many of your network resources to the cloud. For example, you don’t need to host your own email servers, and running your website from the cloud will allow that resource to scale as needed without having to purchase new hardware in the future. You give your team the green light to begin the migration of a few servers with the intent of a larger scale migration when the transition to your new offices is scheduled to be completed.

During the initial migration, your team sets up a group of VPN (virtual private network) connections to your cloud resources from each of your company locations. This process requires the installation of a VPN device at each location. The VPNs travel over each location’s Internet connection, giving employees direct and secure access to your first few cloud resources like email and, eventually, to a lot more resources like the customer database and HR tools.

At first, the VPNs work well enough. Later in the year, as the cloud migration nears completion, it becomes obvious that a VPN will not be sufficient for the home office. Instead, your cloud provider recommends a [**private-direct connection**](javascript://), or [**interconnection**](javascript://), to their cloud infrastructure. In this scenario, you lease a dedicated line from your ISP to one of your cloud provider’s PoPs, or colocation facilities (see [Figure 9-21](javascript://)). From there, you pay for the connection to the cloud provider’s physical infrastructure and, usually, some kind of data transfer fees (such as $.02 per GB transferred out of the cloud provider’s network).

**Figure 9-21**

A colocation facility offers connections to multiple cloud platforms



As you research your cloud provider’s available PoP locations, you realize the colocation you’ve chosen also offers private-direct connections with another cloud provider your team has been considering for a multicloud deployment. The cost efficiency of leasing a single direct line to this colocation will more than pay for itself over time now that you can use the same physical line for multiple purposes. This benefit also opens additional opportunities to host more resources in your hybrid cloud, including virtual desktops for your home office.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-3gSoftware-defined WAN (SD-WAN)

Over the next couple of years, you settle into your new offices. All your stores and your website continue to thrive. Customers are happy, and so are your employees. Suddenly, a random social media video featuring some of your products goes viral on the Internet, and you start getting a rapid increase in website traffic. Interestingly, much of that traffic originates from three Asian countries. Order volumes to these countries spike. You’re sure it won’t last long, but six months later, these sales numbers have only increased. As you further investigate your popularity explosion in these countries, you make some connections with new business associates in those areas. Casual chit-chat turns into some serious discussion about expanding your company into India and Thailand. You’re committed to hiring locals to provide everything from order management and HR to customer support. At the same time, this expansion will require a significant investment in new overseas locations for storefronts, offices, and a warehouse, which also means needing new WAN connections.

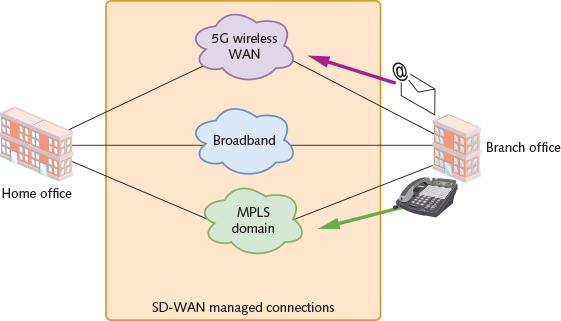
As you discuss the pending expenditure in these other countries with your IT team, you realize the need for centralized management of company network resources. MPLS connections all the way to Asia won’t suffice to meet your company’s needs over the coming years. Instead, your team suggests a newer solution called SD-WAN.

Similar to its SDN cousin, [**SD-WAN (software-defined wide area network)**](javascript://) relies on abstracted, centralized control of networking devices to manage network functions across a diverse infrastructure. SD-WAN offers the following benefits:

* **Transport agnostic**—As shown in [Figure 9-22](javascript://), an SD-WAN controller can manage network configurations at multiple locations throughout the world, regardless of the type of connection each segment uses to reach the SD-WAN (such as broadband, leased line, MPLS, cellular, and others).
* **Active-active load balancing and automatic failover**—An SD-WAN managed network offers active-active load balancing where it can choose the best physical WAN connection for different types of traffic according to traffic prioritization and current network conditions. For example, suppose a branch office has three Internet connections as shown in [Figure 9-23](javascript://): an MPLS connection, a broadband connection, and a 5G wireless connection. SD-WAN can route traffic over each of these connections according to each data stream’s configured priority. If one WAN connection goes down, the SD-WAN controller can switch traffic to another WAN connection.
* **Intent-based management**—A network admin can indicate in the controller’s GUI their intent for traffic, such as limiting bandwidth for a specific application, and the SD-WAN controller institutes all configuration changes needed on all affected network devices.
* **Zero-touch provisioning**—An SD-WAN edge device can be shipped to a branch location where a non-technical person can plug in the device without any configuration needed on-site. The device then finds and checks in with the remote SD-WAN controller for further instructions. Trained technicians at the home office can remotely finish deploying the SD-WAN configurations at the branch office without any additional assistance from on-site personnel.
* **Reduced cost**—Because SD-WAN solutions can be deployed over any kind of underlying WAN connection (such as cable, DSL, fiber broadband, or 5G), expensive leased lines and MPLS connections can be abandoned in favor of SD-WAN management for many of a company’s connections. While the company might not replace all their MPLS or leased line connections, SD-WAN can be used to optimally manage all available WAN connections and minimize the need for more expensive WAN services.

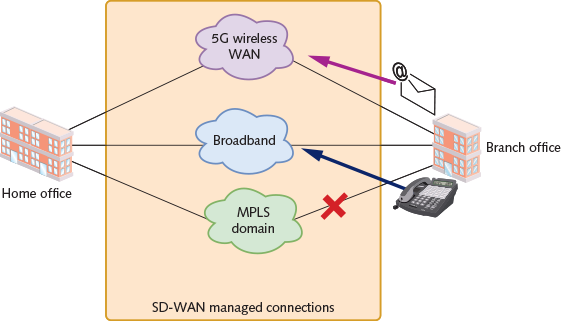
**Figure 9-22**

SD-WAN supports many underlying WAN connectivity technologies



**Figure 9-23**

The SD-WAN controller can direct traffic through the optimal path for that traffic at a given time



Improvements to SD-WAN technologies are still needed surrounding security when traffic traverses the Internet, costs for underlying WAN connections (such as MPLS), and flexibility for cloud and mobile users. Still, the advantages offered by SD-WAN are causing an industry shift away from older, more traditional WAN connectivity options.

Your fictional company has used a wide variety of wired WAN technologies through its journey from your basement to its global presence. Similar to LANs, WANs utilize multiple wireless technologies as well. You’ll read about two of the most common of these in the next section.

**Applying Concepts 9-3**

### Explore Internet Connection Options in Your Area

Selecting a particular WAN solution because its theoretical maximum speed is faster than another solution’s theoretical maximum speed won’t help much if your local carrier doesn’t actually offer service at that speed. Selecting a WAN solution for a corporation requires familiarity with the options available in your area and their actual performance levels relative to each other. Complete the following steps to evaluate the ISP options available to a business in your area:

1. 1

Compile a list of ISPs in your town or city. If you live in a rural area with few options, select a nearby city with more options so that you’ll be able to include some of the private WAN technologies in addition to residential WAN offerings.

1. 2

Check the website for each ISP to determine what broadband and dedicated services they offer in your area, both for residential customers and corporate customers. Include both wired and wireless options. Answer the following questions:

* 1. What are their advertised speeds?
  2. How much does each solution cost on a monthly basis?
  3. What installation fees are there, if any?
  4. How far away are you located from their CO? (If you’re researching another city besides your own, use a fictional location in that same city.)
  5. What effect will this distance likely have on the actual speeds of each service option?

1. 3

Search online for consumer reviews of each ISP in your list. What kinds of ratings does each ISP receive online?

**Remember This…**

* Explain various WAN services, including DSL, cable, MONs, leased lines, MPLS, cloud connectivity options, and SD-WAN.
* Use a bandwidth speed tester to check a WAN connection’s speed.

**Self-Check**

1. You just moved into a rural office space that has telephone service but no cable. Which WAN service could you use without needing to install new wiring to your location?

Answer

* 1. Fiber broadband
  2. DSL
  3. Leased fiber
  4. Cable broadband

1. Which of these WAN services is backed by an SLA?

Answer

* 1. DSL
  2. Leased line
  3. Fiber broadband
  4. Cable broadband

1. Which WAN service offers active-active load balancing?

Answer

* 1. Cable broadband
  2. DSL
  3. SD-WAN
  4. Fiber broadband

**You’re Ready**

You’re now ready to complete [Project 9-3: Create WAN Links in Packet Tracer](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-4Wireless WANs

### Certification

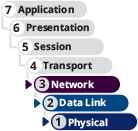
* 1.2

Explain the characteristics of network topologies and network types.

* 2.4

Given a scenario, install and configure the appropriate wireless standards and technologies.

Average reading time: 16 minutes



The best 802.11ac signal can travel approximately a quarter of a mile. But other types of wireless networks can connect stations over much longer distances. For example, in large cities, dozens of surveillance cameras trained on municipal buildings and parks beam video images to central public safety headquarters. Meanwhile, in developing countries, wireless signals deliver lectures and training videos to students in remote, mountainous regions. In rural areas of the United States, elderly patients at home wear medical monitoring devices, such as blood pressure sensors and blood glucose meters, which use wireless networks to convey information to their doctors hundreds of miles away. Such networks can even alert paramedics in case of an emergency. All of these are examples of wireless WANs. Unlike wireless LANs, wireless WANs are designed for high-throughput, long-distance digital data exchange. The following sections describe a variety of ways wireless clients can communicate across a city or state.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

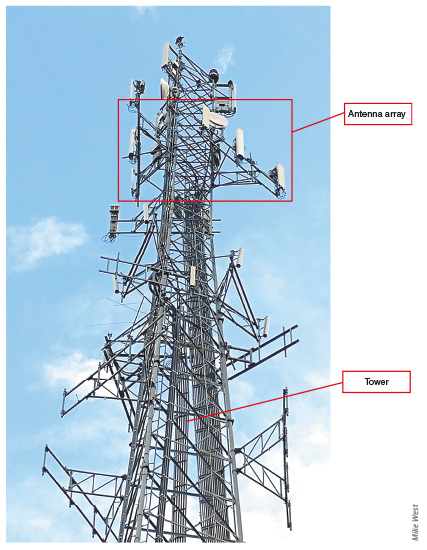
## 9-4aCellular

Cellular networks were initially designed to provide analog phone service. However, since the first mobile phones became available to consumers in the 1970s, cellular services have changed dramatically. In addition to voice signals, cellular networks now deliver text messages, web pages, music, and videos to smartphones and other handheld devices. Cellular networking is a complex topic, with rapidly evolving encoding and access methods, changing standards, and innovative vendors vying to dominate the market. This module does not detail the various encoding and access methods used on cellular networks. To prepare you for the CompTIA Network+ exam, this section describes current cellular data technology and explains the role it plays in wide area networking.

Although their access methods and features might differ, all cellular networks share a similar infrastructure in which coverage areas are divided into cells. Each cell is served by an antenna array and its base station, together called a [**cell site**](javascript://). The tower—the tall part you can easily see from a distance—is often owned by a third-party entity similar to how owners of office buildings or malls lease out portions of their property to other businesses. Cellular providers lease space on the towers for their antenna arrays, as shown in [Figure 9-24](javascript://), and space on the ground for base station equipment.

**Figure 9-24**

This tower offers space for several antenna arrays



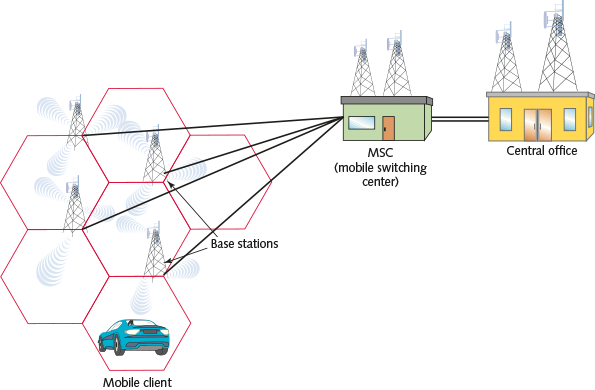
Enlarge Image

Mike West

At the base station, a controller assigns frequencies to mobile clients and manages communication with them. In network diagrams, cells are depicted as hexagons. Multiple cells share borders to form a network in a honeycomb pattern, as shown in [Figure 9-25](javascript://). Antennas are positioned at three corners of each cell, radiating their signals and providing coverage over three equidistant lobes. When a client passes from one coverage area to another, the mobile device begins communicating with a different antenna. Its communication might change frequencies or even carriers between cells. The transition, which normally happens without the user’s awareness, is known as a handoff.

**Figure 9-25**

Cellular network



Enlarge Image

Cell sizes vary from roughly 1000 feet to 12 miles in diameter. The size of a cell depends on the network’s access method and the region’s topology, population, and amount of cellular traffic. An urban area with dense population and high volume of data and voice traffic might use cells with a diameter of only 2000 feet, their antennas mounted on tall buildings (see [Figure 9-26a](javascript://)) or disguised to look like landscaping (see [Figure 9-26b](javascript://)). In sparsely populated rural areas, with antennas mounted on isolated hilltop towers, cells might span more than 10 miles. In theory, the division of a network into cells provides thorough coverage over any given area. In reality, cells are misshapen due to terrain, EMI, and antenna radiation patterns. Some edges overlap and others don’t meet up, leaving gaps in coverage.

**Figure 9-26**

a) Cellular antennas on a tall building; b) A concealed tower



Enlarge Image

Chichimaru/ [Shutterstock.com](http://shutterstock.com/); Cary Kalscheuer/ [Shutterstock.com](http://shutterstock.com/)

As shown earlier in [Figure 9-25](javascript://), each base station is connected to an MSC (mobile switching center), also called an MTSO (mobile telecommunications switching office), by a wireless link or fiber-optic cabling. The MSC might be located inside a telephone company’s central office or it might stand alone and connect to the central office via another fiber-optic cable or a microwave link. At the MSC, the mobile network intersects with the wider wired network. Equipment at an MSC manages mobile clients, monitoring their location and usage patterns, and switches cellular calls. It also assigns each mobile client an IP address. From the switching center, packets sent from cellular networks are routed to wired data networks through backbones using WAN technologies you learned about earlier in this module.

To put today’s services in context, it’s useful to understand that each leap in cellular technology has been described as a new generation. Each successive generation has brought a greater range of services, better quality, and higher throughputs, as described in the following list:

* 1G (first generation) services from the 1970s and 1980s were analog.
* 2G (second generation) services in the 1990s used digital transmission and paved the way for texting and media downloads on mobile devices. Data transmission on 2G systems didn’t exceed 240 Kbps.
* [**3G (third generation)**](javascript://) services were released in the early 2000s. Data rates rose to 384 Kbps. To switch to fully digital transmissions, two competing 2G technologies emerged as market leaders for 3G, as follows:
  + [**GSM (Global System for Mobile Communications)**](javascript://) is an open standard that is accepted and used worldwide. Digital communication of data is separated by timeslots on a channel using [**TDMA (time division multiple access)**](javascript://), which is similar to TDM (time division multiplexing). The primary difference is that multiplexed TDM signals all come from the same source (such as a router), while multiplexed TDMA signals come from several sources (such as several smartphones in the same vicinity). First introduced with the release of 2G devices, GSM initially only provided voice communications but added data services with the evolution of GPRS (General Packet Radio Services) and EGPRS (Enhanced GPRS), also called EDGE (Enhanced Data rates for GSM Evolution). GSM networks require that a cellular device have a [**SIM (Subscriber Identity Module) card**](javascript://) containing a microchip to hold data about the subscription a user has with the cellular carrier.
  + [**CDMA (Code Division Multiple Access)**](javascript://) differs from GSM in that it spreads a signal over a wider bandwidth so multiple users occupy the same channel, a technology called spread-spectrum. Codes on the packets keep the various calls separated. CDMA networks do not require a SIM card in a cellular device because devices are compared against a whitelist, which is a database of subscribers that contains information on their subscriptions with the provider. However, CDMA networks (such as Verizon’s) still require SIM cards to use their LTE (Long Term Evolution) features. While CDMA and GSM co-exist in the United States, globally GSM is by far the more popular technology.
* [**4G (fourth generation)**](javascript://) services are characterized by an all-IP network for both data and voice transmission. 4G standards, released in 2008, specify minimum throughputs of 100 Mbps with the goal of supporting 1 Gbps speeds. Variations of 4G include the following:
  + [**LTE (Long-Term Evolution)**](javascript://) is essentially the result of a marketing debacle. 4G standards were released ahead of their time, that is, before available hardware was capable of providing the required speeds to qualify as 4G. However, the new 4G protocols and techniques that did work supported better speeds than 3G, and cellular providers had already begun marketing new 4G networks and devices. So LTE became an ambiguous marketing term that meant “faster than 3G but not really 4G.” As hardware has improved, so have LTE speeds. Typical speeds now for LTE connections might reach 100 Mbps download and up to 75 Mbps upload.
  + [**LTE-A (LTE-Advanced)**](javascript://) can more realistically approach 4G standards. Sometimes misleadingly called 5G E (5G Evolution), LTE-A is basically true 4G as defined back in 2008 but only recently emerging in real-world networks.
* [**5G (fifth generation)**](javascript://) services require minimum speeds of 1 Gbps and max out at 20 Gbps download and 10 Gbps upload; however, actual speeds vary greatly. The 5G standards were initially released in 2016; cellular companies began deploying 5G infrastructure and devices in 2019. Note that the term 5G is completely unrelated to the 5-GHz band used by Wi-Fi. The following technologies contribute to 5G improvements:
  + **Bands**—One factor in experienced speeds is the band used. Some 5G providers (such as T-Mobile) have focused on building out widely available 5G infrastructure using the same lower bands that 4G uses, resulting in only moderately improved speeds. Other 5G providers (such as Verizon) are focusing instead on higher-density but less widely available infrastructure that uses new and smaller millimeter-wave frequencies in a newly available higher band. These dense but weaker frequencies provide high speeds for short distances while offering much lower resilience across long distances or when crossing obstacles such as walls and landscaping. When you are standing near a cell site, you could experience a strong 5G signal (with speeds easily exceeding 1 Gbps). But that speed could plummet to closer to 4G speeds at 200–300 Mbps if you walk around the corner of a nearby building or stand behind a tree.
  + **Cell density**—To reach a reasonable level of availability and effectiveness, many small 5G antennas must be installed in close proximity to each other so 5G clients can receive a close and strong signal throughout the coverage area.
  + **Channels**—5G works to increase speeds by using wider channels, similar to how Wi-Fi’s 5-GHz band can be bonded into larger channels. Where 4G uses up to seven 20-MHz channels, 5G can use up to eight 100-MHz channels in the high band, which ranges from 20 to 100 GHz. Low band 5G (narrow but long-reaching frequencies) uses the same channels as 4G under 2 GHz. Mid band 5G (in the range of 2–10 GHz) offers two 100-MHz channels with the ability to stack low-band 20-MHz channels.
  + **Client volume**—While 5G cells must be placed closer together so millimeter-wave frequencies can reach clients, each cell site can support more clients. This will work well for sensor networks and IoT devices.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4bSatellite

In 1945, Arthur C. Clarke (the author of 2001: A Space Odyssey) wrote an article in which he described the possibility of communication between manned space stations that continually orbited the Earth. Other scientists recognized the value of using satellites to convey signals from one location on Earth to another. By the 1960s, the United States was using satellites to transmit telephone and television signals across the Atlantic Ocean. Since then, the proliferation of this technology and reductions in its cost have made satellite transmission appropriate and available for transmitting consumer voice, video, music, and data.

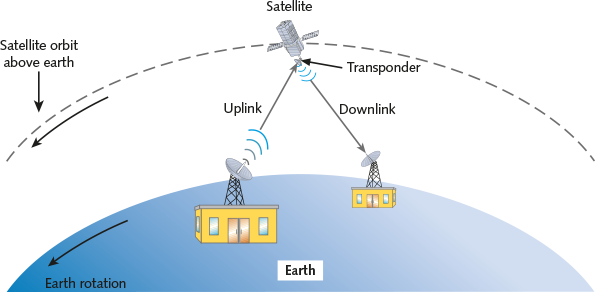
### Satellite Orbits

Most satellites circle the Earth 22,300 miles above the equator in a geosynchronous orbit. GEO (geosynchronous earth orbit) satellites orbit the Earth at the same rate as the Earth turns. A special case of geosynchronous orbit, called geostationary orbit (because it appears stationary from Earth), stays directly above the equator. This is especially common with communications satellites. Consequently, at every point in their orbit, the satellites maintain a constant distance from a specific point on the Earth’s equator.

Satellites are generally used to relay information from one point on Earth to another. Information must first be transmitted to the satellite from Earth in an uplink from an Earth-based transmitter. Often, the uplink signal information is scrambled (in other words, its signal is encoded) before transmission to prevent unauthorized interception. At the satellite, a transponder receives the uplink signal, then transmits it to an Earth-based receiver in a downlink. Each satellite uses unique frequencies for its downlink. These frequencies, as well as the satellite’s orbit location, are assigned and regulated by the FCC. Back on Earth, the downlink is picked up by a dish-shaped antenna. The dish shape concentrates the signal so that it can be interpreted by a receiver. [Figure 9-27](javascript://) provides a simplified view of satellite communication.

**Figure 9-27**

Satellite communication



Enlarge Image

Geosynchronous earth orbiting satellites are the type used by the most popular satellite data service providers. This technology is well established, and it’s the least expensive of all satellite technology. Also, because many of these satellites remain in a fixed position relative to the Earth’s surface, stationary receiving dishes on Earth can be counted on to receive satellite signals reliably, weather permitting.

### Satellite Internet Services

A handful of companies offer high-bandwidth Internet access via GEO satellite links. Each subscriber uses a small satellite antenna and receiver, or satellite modem, to exchange signals with the service provider’s satellite network. Clients may be fixed, such as rural residents who are too remote for DSL, or mobile subscribers, such as travelers on ocean-going yachts.

Clients can exchange signals with satellites as long as they have a line-of-sight path from an unobstructed view of the sky. To establish a satellite Internet connection, each subscriber must have a fixed dish antenna, which is approximately 2 feet high by 3 feet wide (see [Figure 9-28](javascript://)). In North America, these dish antennas are pointed toward the Southern Hemisphere (because many geosynchronous satellites travel over the equator). The dish antenna’s receiver is connected via cable to a modem. This modem typically uses an Ethernet interface to connect with the subscriber’s router or computer.

**Figure 9-28**

A small satellite dish provides Internet connection



Andrey\_Popov/ [Shutterstock.com](http://shutterstock.com/)

As with several other wireless WAN technologies, satellite services are typically asymmetrical, and bandwidth is shared among many subscribers. Throughputs vary and are controlled by the service provider. Downlink speeds might reach 100 Mbps, while uplink rates are much slower. Compared with other wireless WAN options, satellite services are slower and suffer more latency. In addition, the inconsistent latency causes jitter problems, degrading signal quality. Given these drawbacks, satellite data service is preferred only in circumstances that allow few alternatives or in cases where satellite receiving equipment is already installed.

**Remember This…**

* Explain cellular and satellite Internet options.
* Compare cellular technologies, including 3G, 4G, 5G, LTE, CDMA, and GSM.

**Self-Check**

1. Which cellular generation was the first to offer speeds up to 1 Gbps?

Answer

* 1. 2G
  2. 3G
  3. 4G-LTE
  4. 4G

1. Which wired WAN service offers speeds most comparable to the highest satellite Internet speeds in a similar price range?

Answer

* 1. DSL
  2. Cable broadband
  3. Fiber broadband
  4. Leased fiber

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 9-5Troubleshooting Connections

### Certification

* 3.1

Given a scenario, use the appropriate statistics and sensors to ensure network availability.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

* 5.5

Given a scenario, troubleshoot general networking issues.

Average reading time: 21 minutes

As a network administrator, one of your primary responsibilities is to keep connections within and between networks working well. With this in mind, there are steps you can take to troubleshoot a problem with a WAN connection before contacting your ISP, and there are preventive measures you can perform to avoid having the problem in the first place.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5aInternet Connectivity Issues

When you lose Internet connectivity, a little troubleshooting can help determine the location of the problem and the party responsible for repairing the connection. The following list presents some common issues to look for on your own equipment:

* **Interference**—Obviously, interference can cause problems with a wireless connection, and you have already learned that interference can wreak havoc with wired connections as well. Intermittent problems or problems that affect unrelated portions of a network are common indicators of interference issues.
* **DNS issues**—Correct DNS server information and a functioning DNS server are critical requirements for enabling Internet access. Computers can be programmed to use DNS servers on a corporate network or the ISP’s DNS servers, or alternatively, they can be pointed to public DNS servers such as those run by Google or Cloudflare.
* **Router misconfiguration**—Routing tables with incorrect routes can result in dropped messages with no error feedback. Other router configuration issues to consider when Internet connectivity fails might include blocked ports that should be open, speed or duplex mismatches, incorrect IP address range or subnet mask, or an incorrect default gateway. Similarly, attackers can take advantage of some types of router misconfigurations that result in network failure due to an attack. You’ll learn more about router security later in this course.
* **Interface error**—Misconfigured interfaces, such as an incorrect default gateway or missing DNS server addresses, can result in interface errors. One possible evaluation technique for bypassing an interface error, which will help confirm that the interface misconfiguration is the issue, is to switch to a different interface on the same device. For example, if your computer’s wired connection is having problems, try connecting to the network using the computer’s wireless interface.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5bInterface Problems

Interface problems can be challenging to track down. Several commands provide insights into device and interface performance, vulnerabilities, and misconfigurations that might be causing problems. A thorough device configuration review can often locate problems that don’t necessarily generate symptoms pointing directly to their cause. On routers and switches, this requires checking overall device configuration as well as individual interface configurations. The following discussion focuses on Cisco devices so you can practice using these commands in Packet Tracer. However, most other networking brands, such as Juniper and Huawei, use similar commands and modes to accomplish similar tasks.

With Cisco devices, recall that different commands are available depending on the mode you’re in. For example, when you first start working with a router, you begin in the user EXEC mode. To step up to the privileged EXEC mode, you enter enable, which can also be abbreviated as simply en. [Table 9-4](javascript://) explains the most used modes on Cisco routers and switches.

**Table 9-4**

### Cisco CLI Modes

| **Mode** | **Default prompt on a router** | **Command to enter mode** | **Description** |
| --- | --- | --- | --- |
| User EXEC | Router> | Login to device | Offers limited commands to evaluate current configurations without making changes to the configuration. |
| Privileged EXEC | Router# | enable or en | Typically requires a password and offers access to all EXEC commands, which provide tools for testing and helpful information about the current configurations. You can also run EXEC commands from other modes by prefacing the EXEC command with the do command. |
| Global configuration | Router(config)# | configure terminal or conf t | Allows device configuration changes and gives access to more specific configuration modes. |
| Interface configuration | Router(config-if)# | interface or int | Allows configuration changes to an interface. Specific configuration modes for features or protocols allow changes to configurations such as interfaces, DHCP, and routing. Configuration submodes and subsubmodes dig deeper into configuration options. |

Enlarge Table

To take one step down from a higher mode into a lower mode, enter the exit command. From any higher mode, enter the end command or press Ctrl+Z to return to privileged EXEC mode.

### Show Config

As you’ve seen in the Capstone Projects, when making a configuration change to a Cisco device, those changes are held in the running configuration file. You can see the device’s running-config file with the command show running-config (or sh run). The output is likely several pages long. Use the following keys to navigate the output:

* Press Enter to move down one line at a time.
* Press the spacebar to move down one page at a time.
* Press Tab or the down arrow to exit the output.

The temporary running-config file is held in the device’s RAM and is, therefore, reset when the device is restarted. To make your changes persist beyond a device’s power cycle, you must copy the running-config file to the startup-config file with the command copy running-config startup-config (or copy run start).

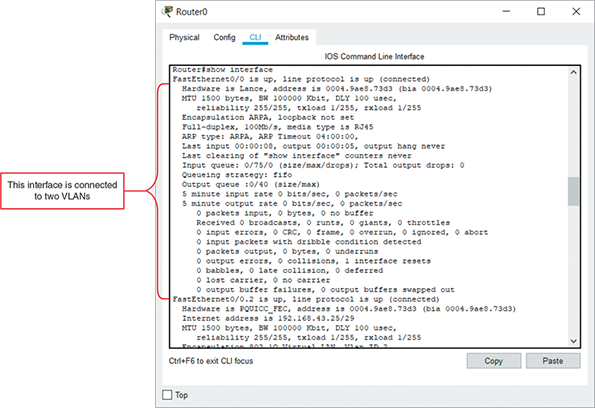
The startup-config file is not stored in RAM but instead is stored in NVRAM, which persists through a power cycle. To see the device’s stored startup-config file, enter the command show startup-config (or sh start).

### Show Interface

Interface configuration, status, and statistics can all provide helpful information in troubleshooting a network connection problem. To get an overview of all the device’s interfaces, enter the command show interface (or sh int). [Figure 9-29](javascript://) shows output for a Cisco router’s interface that is connected to two VLANs on a switch.

**Figure 9-29**

A router’s interface information



Enlarge Image

Source: Cisco Systems, Inc.

Notice the following information in this output:

* **Link state**—Indicates whether the interface is up or down. The first portion, FastEthernet0/0, refers to the physical layer: Is a physical cable connected to the interface? The second portion, line protocol, refers to the data link layer: Are basic protocols functioning properly across the link, such as clocking and framing? If the interface is “administratively down,” it has been shut down using the shutdown command or has encountered a configured limitation, such as a security breach. Bring it back up using the no shutdown (or no shut) command.
* **MTU**—Indicates the maximum network-layer packet size the interface can support. The Ethernet standard MTU is 1500 bytes.
* **BW (bandwidth)**—Indicates the link’s supported bandwidth, which is used by routing protocols to calculate best paths. The rest of the information on this line is also used for routing metrics, including delay, reliability, and load.
* **Encapsulation**—For Ethernet networks, the encapsulation value is always set to ARPA. The statement “loopback not set” does not refer to the loopback interface but to the interface’s current mode. Loopback mode is sometimes used for testing.
* **Duplex and speed**—Indicates if the link is operating in full-duplex mode, the link’s bandwidth (such as 100 Mbps), and the physical connection type (such as RJ-45).
* **Send and receive traffic statistics**—Interface statistics are tracked over time and can be cleared. Information here will indicate when the statistics were most recently reset. The next several lines indicate statistics that have been gathered since the most recent reset and include number of packets dropped due to queue overflow, average input and output rates, total number of packets and bytes received or sent by the system, and number of broadcast frames, runts, and giants received. [**Runts**](javascript://) are messages that are too small and were dropped—on Ethernet networks, this minimum size is 64 bytes. Excessive collisions on a network can result in high numbers of runts being reported. [**Giants**](javascript://) are frames that are too large, and these are also dropped. On Ethernet networks, this maximum frame size is usually 1518 bytes, although jumbo frames over this size might be supported. Excessive giants being reported is usually a result of misconfigurations. Additional statistics indicate the number of CRC errors. CRC (Cyclic Redundancy Checksum) confirms the data in a message has not been corrupted. A [**CRC error**](javascript://) indicates messages are being damaged in transit, such as when there’s a cable problem or a damaged NIC.

While the show interface command displays OSI layer 1 and 2 information, the show ip interface (or sh ip int) command focuses on detailed layer 3 information, such as IP addressing, helper address, accounting, compression, NAT, and many other settings. For a more concise list of interfaces, IP addresses, and interface status, enter the command show ip interface brief (or sh ip int br).

Go to pg.

[**help**](javascript://)

Application Opened

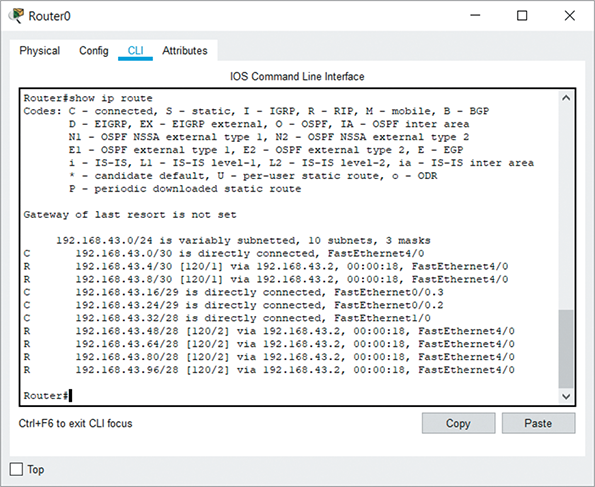
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5cRouting Issues

Just as interfaces must be properly configured for network connections to work as expected, misconfigured routing tables also can cause problems for network connections. On a Cisco router, the show ip route command lists the router’s routing table information, as shown in [Figure 9-30](javascript://).

**Figure 9-30**

A router’s routing table



Enlarge Image

Source: Cisco Systems, Inc.

The routing table lists several types of routes and other information about the routes. Some of the most used route types and information are described next:

* **C (connected)**—Networks directly connected to the router’s own interfaces are classified as C (connected).
* **S (static)**—Static routes are manually configured by a network admin.
* **Protocol**—Codes identify the routing protocol used to configure the route, such as R (RIP), B (BGP), D (EIGRP), and O (OSPF).
* **Gateway of last resort**—This route identifies the path for messages when another route doesn’t apply.

Common routing issues include the following:

* **Missing route**—If no matching route exists for a message, the message will be dropped. For this reason, a gateway of last resort should be configured to handle messages with no matching route. You can add a gateway of last resort using one of the following commands: ip default-gateway (used when no routing is configured on the router), ip default-network (requires that routing is configured on the router and chooses a classful default route from existing routes), or ip route 0.0.0.0 0.0.0.0 (sets a default route for messages with no matching route in the routing table and requires that routing is configured on the router). A similar problem is caused when existing routes are not being advertised through routing protocols. As you’ll see in a project at the end of this module, you need to identify which of its connected routes you want each router to advertise.
* [**Routing loop**](javascript://)—Routing protocols can sometimes route messages continuously through the same paths without the message ever reaching its destination, which can negatively impact network performance. Making too many topology changes too quickly can cause this problem, as routers need time to adjust to each change. Distance-vector routing protocols reach convergence more slowly than other types of routing protocols. A conservative TTL (time-to-live) can ensure these stray packets are dropped after so many hops. Limitations can also be placed on the routers’ ability to share their routing tables with neighbors so this sharing moves outward from each router without old information looping back on itself—this is called a split horizon. Similarly, a routing timer ensures that all the routers in the system share their routing tables at the same time. This way, there’s no question as to which routing table entry is the most recent when something has changed on the network.
* [**Asymmetrical routing**](javascript://)—This is caused when messages going in one direction in a conversation (such as from a web server to a client) travel a different path than messages going in the other direction (such as from client to web server). While this is typically unavoidable (especially when using BGP on the Internet) and is not a problem, it can cause issues for NAT and for firewalls that need to see traffic in both directions of a conversation to properly apply filtering rules. Firewalls often rely on TCP sessions to approve outgoing traffic in response to approved incoming traffic. If some incoming traffic hits a different firewall than the one a server is configured to use for its outgoing messages, the firewall might incorrectly reject outgoing traffic that should have been approved. For organizations using multiple firewalls, thoughtful configuration of traffic flow and internal routing can be used to avoid problems with asymmetrical routing.

[Table 9-5](javascript://) summarizes commonly used Cisco commands for routers and switches, many of which you’ve used in the Packet Tracer projects in this course.

**Table 9-5**

### Common Cisco Commands

| **Command** | **Mode** | **Purpose** |
| --- | --- | --- |
| ? | Any | When entered alone, outputs a list of available commands in the current mode. When entered after portions of a command, outputs a list of available parameters for that command. When entered after one or a few letters, outputs a list of commands beginning with those letters. |
| show running-config  or sh run | Privileged EXEC | Displays the running-config file. |
| copy running-config startup-config  or copy run start | Privileged EXEC | Copies the running configuration to the startup-config file. |
| show mac address-table | Privileged EXEC | Displays MAC address table on a switch. |
| show vlan brief  or sh vlan br | Privileged EXEC | Displays a concise list of VLAN assignment information on a switch. |
| show ip route  or sh ip ro | EXEC | Displays a router’s routing table. Add parameters to specify types of routes, such as show ip route rip. Delete a route from the routing table with the command clear ip route x.x.x.x (where the last part lists the IP address of the target network you want to clear from the routing table). |
| show ip protocol database | Any | Displays a routing protocol’s routing database on a router, such as show ip rip database. |
| ip route destinationaddress subnetmask nexthopaddress | Global configuration | Sets a static route on a router. |
| show interface  or sh int | EXEC | Displays physical and data link layer information about a device’s interfaces. |
| show ip interface brief  or sh ip int br | EXEC | Displays concise network layer information about a device’s interfaces. |
| show interface trunk or sh int tr | EXEC | Displays trunks configured on a switch. |
| show interface switchport or sh int sw | EXEC | Displays detailed VLAN configurations for each of a switch’s interfaces. |
| interface fastethernet0/0  or int fa0/0 | Global configuration | Enters interface configuration mode for specified interface. |
| ip address address subnet  or ip addr address subnet | Interface configuration | Sets IP information for an interface. |
| no shutdown  or no shut | Interface configuration | Enables an interface. Similarly, shutdown will disable an interface. |
| ip name-server dns1address  dns2address | Global configuration | Sets DNS server addresses. |
| hostname | Global configuration | Changes the device’s name. |

Enlarge Table

**Applying Concepts 9-4**

### Internet Down

One evening, you’re up late working to meet a fast-approaching deadline when suddenly your Internet connection fails. Much of your work requires Internet access for research, but you belay the panic for a few moments to evaluate the situation:

* You try a couple different websites in your browser, then open a different browser application and try a couple websites again. None of the sites will load.
* You check all the cable connections between your computer and your network’s demarc. Everything looks normal.
* You power cycle the modem and router by unplugging both devices from the electrical outlet, waiting a few minutes, plugging in the modem, waiting for it to establish a connection with the ISP, and then plugging in the router.
* You check the Network Connections status on your computer and confirm that you have a functioning connection with your network.
* You try again to navigate to a website in your browser, but the page still won’t load.
* You open a PowerShell window and ping one of Google’s servers at 8.8.8.8. The ping works.
* You ping Google’s website at [google.com](http://google.com/), but this time it doesn’t work.
* You pull up an outage reporting website for your ISP on your smartphone and find that a few hundred other people have reported an outage in your area.

With a quick adjustment, you get your Internet service functioning again and continue with your work. Which of the following did you do and why?

1. You switched out the Ethernet cable connecting your modem to your router because the cable was damaged.
2. You used ipconfig to release the IP address on your computer and get a new one from your network’s DHCP service because your computer had a duplicate IP address.
3. You changed the DNS settings on your router to point to Google’s DNS servers instead of the DNS servers of your ISP because the ISP’s DNS servers are down.
4. You switched to a different ISP because the former ISP’s service was unreliable.
5. You replaced the router with a new router you had ready to go, knowing that the old router had already exceeded its life expectancy and had finally ceased to function.
6. You created an ad hoc network with another computer on your network and used that computer’s access to the Internet to continue your research because the Wi-Fi radio on your computer had died and will need to be replaced.
7. You performed a factory reset on your modem so it would reinitiate a connection with the ISP.
8. You updated the default gateway on your computer because it was unable to communicate with the router.
9. You restarted your computer because Windows had updates that needed to be installed.

**Remember This…**

* Use basic network platform commands, including show interface, show config, and show route.
* Analyze connection problems using interface information, including link state, speed/duplex, and traffic statistics.
* Troubleshoot common routing issues, including missing route, routing loop, and asymmetrical routing.

**Self-Check**

1. Where is a router’s hostname stored when you first change the name?

Answer

* 1. Routing table
  2. Startup-config file
  3. Whitelist
  4. Running-config file

1. Which problem is most likely caused by a damaged cable?

Answer

* 1. Routing loop
  2. CRC error
  3. Asymmetrical route
  4. Excessive giants

**You’re Ready**

You’re now ready to complete [Project 9-4: Explore IOS Command Modes in Packet Tracer](javascript://), or you can wait until you’ve finished the Review Questions for this module.

**You’re Ready**

After you finish the Hands-On Projects, you’re ready to complete the [Module 9 Capstone Projects](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 9-6a**Module Summary**

### WAN Essentials

* A WAN traverses a significant distance and usually supports very high data throughput. Although many types of businesses need WANs, they might not need the same kinds of WANs.
* Typically, a CAN is a collection of LANs within a single property or nearby properties, such as buildings belonging to a school where all the buildings and most or all the network media spanning those connections are confined within land owned by the school. With a CAN, it’s likely that a single organization (or group of organizations) owns all the connected LANs and most or all the networking media connecting those LANs.
* A MAN is a collection of LANs within a limited geographical area, such as a downtown area or even a city, county, or province. With MANs, many customers might own one or more of the connected LANs, and a single, third-party provider leases use of the networking media connecting these LANs. These connections often must be made across property not owned by either the MAN provider or the MAN customers. MAN connections might be made available to the general public, or it might be restricted to a single customer.
* A modem is a modulation/demodulation device that converts between digital and analog signals. The customer’s endpoint device on a WAN is called the DTE (data terminal equipment), and the carrier’s endpoint device for the WAN is called the DCE (data circuit-terminating equipment). The NIU, also called NID (network interface device), at the demarc connects the ISP’s local loop to the customer’s network. A more intelligent version of an NIU is a smartjack, or INID (Intelligent NID), which can provide diagnostic information about the interface.

### Routing Protocols

* A router joins two or more networks and passes packets from one network to another. Routers are responsible for determining the next network to which a packet should be forwarded on its way to its destination. Routers are often categorized according to their location on a network or the Internet and the routing protocols they use. The various categories include core routers, edge routers, and exterior routers.
* A routing table is a database that holds information about where hosts are located and the most efficient way to reach them. A router relies on its routing table to identify which network a host belongs to and which of the router’s interfaces points toward the best next hop to reach that network. Routing paths are determined by static routes or dynamic routes, which are listed in the routing table. The route utility allows you to view a host’s routing table.
* To determine the best path, routers communicate with each other through routing protocols. Routers rate the reliability and priority of a routing protocol’s data based on AD (administrative distance), convergence time, and overhead.
* IGPs (interior gateway protocols) are routing protocols used by core routers and edge routers within autonomous systems. IGPs are often grouped according to the algorithms they use to calculate best paths, including distance-vector routing protocols, link-state routing protocols, and hybrid routing protocols. EGPs (exterior gateway protocols) are routing protocols used by edge routers and exterior routers to distribute data outside of autonomous systems. The only EGP protocol currently in use is BGP.
* The most popular routing protocols in use today include RIP (Routing Information Protocol) and RIPv2 (Routing Information Protocol, version 2), which are legacy protocols, and the link-state routing protocol OSPF (Open Shortest Path First), the similar IS-IS (Intermediate System to Intermediate System), Cisco’s hybrid protocol EIGRP (Enhanced Interior Gateway Routing Protocol), and the Internet protocol BGP (Border Gateway Protocol).
* Three popular FHRPs (First Hop Redundancy Protocol) used by routers and layer 3 switches to provide a single VIP (Virtual IP) address as the default gateway to a network are VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Routing Protocol), and GLBP (Gateway Load Balancing Protocol).

### WAN Connectivity

* Two categories of WAN connectivity services are broadband, where the cables (whether telephone, coaxial, or fiber) and available bandwidth are shared between multiple customers, and DIA (dedicated Internet access), where the cable or a portion of its available bandwidth is dedicated to a single customer.
* DSL (digital subscriber line) is a WAN connection method that operates over the PSTN (public switched telephone network), which is a network of lines and carrier equipment that provide landline telephone service to homes and businesses.
* Cable broadband (also called cable Internet or cable modem access) is based on the coaxial cable wiring used for TV signals, although in reality, much of the coaxial infrastructure has been replaced with fiber.
* To reduce the distance signals must travel over copper cables to reach customers, many ISPs use MONs (metropolitan optical networks) to offer FTTN (fiber-to-the-node), FTTH (fiber-to-the-home), or similar arrangements. A MON is a dense, localized grid of junctions and fiber cables that attempts to make direct fiber connections available to as many customers as possible while balancing the significant expense of replacing existing telephone and coaxial cable infrastructure with fiber equipment and fiber-optimized technologies.
* Leased lines provide dedicated bandwidth on fiber optic connections. The customer pays for a specific bandwidth (such as 2 Gbps) and reserves that bandwidth for their sole use without having to share it with other customers. Throughput won’t fluctuate in response to traffic demands from other customers.
* MPLS (multiprotocol label switching) enables multiple types of layer 3 protocols to travel over any one of several connection-oriented layer 2 protocols. One of the characteristics that sets MPLS apart from other WAN technologies is its ability to support QoS traffic shaping across WAN connections.
* With a private-direct connection, or interconnection, to the cloud, you lease a dedicated line from your ISP to one of your cloud provider’s PoPs, or colocation facilities. From there, you pay for the connection to the cloud provider’s physical infrastructure and, usually, some kind of data transfer fees.
* SD-WAN (software-defined wide area network) relies on abstracted, centralized control of networking devices to manage network functions across a diverse infrastructure. SD-WAN offers the following benefits: transport agnostic, active-active load balancing, automatic failover, intent-based management, zero-touch provisioning, and reduced cost compared to services such as leased lines and MPLS.

### Wireless WANs

* With 3G (third generation) cellular services, data rates rose to 384 Kbps. To switch to fully digital transmissions, two competing 2G technologies emerged as market leaders for 3G: GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access).
* 4G (fourth generation) services are characterized by an all-IP network for both data and voice transmission. 4G standards, released in 2008, specify minimum throughputs of 100 Mbps with the goal of supporting 1 Gbps speeds. LTE (Long-Term Evolution) became an ambiguous marketing term that meant “faster than 3G but not really 4G.” As hardware has improved, so have LTE speeds. Typical speeds now for LTE connections might reach 100 Mbps download and up to 75 Mbps upload. LTE-A (LTE-Advanced) can more realistically approach 4G standards. Sometimes misleadingly called 5G E (5G Evolution), LTE-A is basically true 4G as defined back in 2008 but only recently emerging in real-world networks.
* 5G (fifth generation) services require minimum speeds of 1 Gbps and max out at 20 Gbps download and 10 Gbps upload, however, actual speeds vary greatly. 5G relies on three frequency bands called low band, mid-band, and high band.
* Satellite Internet clients can exchange signals with satellites as long as they have a line-of-sight path from an unobstructed view of the sky. To establish a satellite Internet connection, each subscriber must have a fixed dish antenna pointed toward the sky over the equator. The dish antenna’s receiver is connected via cable to a modem. As with several other wireless WAN technologies, satellite services are typically asymmetrical, and bandwidth is shared among many subscribers. Throughputs vary and are controlled by the service provider. Downlink speeds might reach 100 Mbps, while uplink rates are much slower.

### Troubleshooting Connections

* When making a configuration change to a Cisco device, those changes are held in the running configuration file. You can see the device’s running-config file with the command show running-config (or sh run).
* Interface configuration, status, and statistics can all provide helpful information in troubleshooting a network connection problem. To get an overview of all the device’s interfaces, enter the command show interface (or sh int).
* Just as interfaces must be properly configured for network connections to work as expected, misconfigured routing tables also can cause problems for network connections. On a Cisco router, the show ip route command lists the router’s routing table information.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 9-6a**Module Summary**

### WAN Essentials

* A WAN traverses a significant distance and usually supports very high data throughput. Although many types of businesses need WANs, they might not need the same kinds of WANs.
* Typically, a CAN is a collection of LANs within a single property or nearby properties, such as buildings belonging to a school where all the buildings and most or all the network media spanning those connections are confined within land owned by the school. With a CAN, it’s likely that a single organization (or group of organizations) owns all the connected LANs and most or all the networking media connecting those LANs.
* A MAN is a collection of LANs within a limited geographical area, such as a downtown area or even a city, county, or province. With MANs, many customers might own one or more of the connected LANs, and a single, third-party provider leases use of the networking media connecting these LANs. These connections often must be made across property not owned by either the MAN provider or the MAN customers. MAN connections might be made available to the general public, or it might be restricted to a single customer.
* A modem is a modulation/demodulation device that converts between digital and analog signals. The customer’s endpoint device on a WAN is called the DTE (data terminal equipment), and the carrier’s endpoint device for the WAN is called the DCE (data circuit-terminating equipment). The NIU, also called NID (network interface device), at the demarc connects the ISP’s local loop to the customer’s network. A more intelligent version of an NIU is a smartjack, or INID (Intelligent NID), which can provide diagnostic information about the interface.

### Routing Protocols

* A router joins two or more networks and passes packets from one network to another. Routers are responsible for determining the next network to which a packet should be forwarded on its way to its destination. Routers are often categorized according to their location on a network or the Internet and the routing protocols they use. The various categories include core routers, edge routers, and exterior routers.
* A routing table is a database that holds information about where hosts are located and the most efficient way to reach them. A router relies on its routing table to identify which network a host belongs to and which of the router’s interfaces points toward the best next hop to reach that network. Routing paths are determined by static routes or dynamic routes, which are listed in the routing table. The route utility allows you to view a host’s routing table.
* To determine the best path, routers communicate with each other through routing protocols. Routers rate the reliability and priority of a routing protocol’s data based on AD (administrative distance), convergence time, and overhead.
* IGPs (interior gateway protocols) are routing protocols used by core routers and edge routers within autonomous systems. IGPs are often grouped according to the algorithms they use to calculate best paths, including distance-vector routing protocols, link-state routing protocols, and hybrid routing protocols. EGPs (exterior gateway protocols) are routing protocols used by edge routers and exterior routers to distribute data outside of autonomous systems. The only EGP protocol currently in use is BGP.
* The most popular routing protocols in use today include RIP (Routing Information Protocol) and RIPv2 (Routing Information Protocol, version 2), which are legacy protocols, and the link-state routing protocol OSPF (Open Shortest Path First), the similar IS-IS (Intermediate System to Intermediate System), Cisco’s hybrid protocol EIGRP (Enhanced Interior Gateway Routing Protocol), and the Internet protocol BGP (Border Gateway Protocol).
* Three popular FHRPs (First Hop Redundancy Protocol) used by routers and layer 3 switches to provide a single VIP (Virtual IP) address as the default gateway to a network are VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Routing Protocol), and GLBP (Gateway Load Balancing Protocol).

### WAN Connectivity

* Two categories of WAN connectivity services are broadband, where the cables (whether telephone, coaxial, or fiber) and available bandwidth are shared between multiple customers, and DIA (dedicated Internet access), where the cable or a portion of its available bandwidth is dedicated to a single customer.
* DSL (digital subscriber line) is a WAN connection method that operates over the PSTN (public switched telephone network), which is a network of lines and carrier equipment that provide landline telephone service to homes and businesses.
* Cable broadband (also called cable Internet or cable modem access) is based on the coaxial cable wiring used for TV signals, although in reality, much of the coaxial infrastructure has been replaced with fiber.
* To reduce the distance signals must travel over copper cables to reach customers, many ISPs use MONs (metropolitan optical networks) to offer FTTN (fiber-to-the-node), FTTH (fiber-to-the-home), or similar arrangements. A MON is a dense, localized grid of junctions and fiber cables that attempts to make direct fiber connections available to as many customers as possible while balancing the significant expense of replacing existing telephone and coaxial cable infrastructure with fiber equipment and fiber-optimized technologies.
* Leased lines provide dedicated bandwidth on fiber optic connections. The customer pays for a specific bandwidth (such as 2 Gbps) and reserves that bandwidth for their sole use without having to share it with other customers. Throughput won’t fluctuate in response to traffic demands from other customers.
* MPLS (multiprotocol label switching) enables multiple types of layer 3 protocols to travel over any one of several connection-oriented layer 2 protocols. One of the characteristics that sets MPLS apart from other WAN technologies is its ability to support QoS traffic shaping across WAN connections.
* With a private-direct connection, or interconnection, to the cloud, you lease a dedicated line from your ISP to one of your cloud provider’s PoPs, or colocation facilities. From there, you pay for the connection to the cloud provider’s physical infrastructure and, usually, some kind of data transfer fees.
* SD-WAN (software-defined wide area network) relies on abstracted, centralized control of networking devices to manage network functions across a diverse infrastructure. SD-WAN offers the following benefits: transport agnostic, active-active load balancing, automatic failover, intent-based management, zero-touch provisioning, and reduced cost compared to services such as leased lines and MPLS.

### Wireless WANs

* With 3G (third generation) cellular services, data rates rose to 384 Kbps. To switch to fully digital transmissions, two competing 2G technologies emerged as market leaders for 3G: GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access).
* 4G (fourth generation) services are characterized by an all-IP network for both data and voice transmission. 4G standards, released in 2008, specify minimum throughputs of 100 Mbps with the goal of supporting 1 Gbps speeds. LTE (Long-Term Evolution) became an ambiguous marketing term that meant “faster than 3G but not really 4G.” As hardware has improved, so have LTE speeds. Typical speeds now for LTE connections might reach 100 Mbps download and up to 75 Mbps upload. LTE-A (LTE-Advanced) can more realistically approach 4G standards. Sometimes misleadingly called 5G E (5G Evolution), LTE-A is basically true 4G as defined back in 2008 but only recently emerging in real-world networks.
* 5G (fifth generation) services require minimum speeds of 1 Gbps and max out at 20 Gbps download and 10 Gbps upload, however, actual speeds vary greatly. 5G relies on three frequency bands called low band, mid-band, and high band.
* Satellite Internet clients can exchange signals with satellites as long as they have a line-of-sight path from an unobstructed view of the sky. To establish a satellite Internet connection, each subscriber must have a fixed dish antenna pointed toward the sky over the equator. The dish antenna’s receiver is connected via cable to a modem. As with several other wireless WAN technologies, satellite services are typically asymmetrical, and bandwidth is shared among many subscribers. Throughputs vary and are controlled by the service provider. Downlink speeds might reach 100 Mbps, while uplink rates are much slower.

### Troubleshooting Connections

* When making a configuration change to a Cisco device, those changes are held in the running configuration file. You can see the device’s running-config file with the command show running-config (or sh run).
* Interface configuration, status, and statistics can all provide helpful information in troubleshooting a network connection problem. To get an overview of all the device’s interfaces, enter the command show interface (or sh int).
* Just as interfaces must be properly configured for network connections to work as expected, misconfigured routing tables also can cause problems for network connections. On a Cisco router, the show ip route command lists the router’s routing table information.

Go to pg.

[**help**](javascript://)