



CCNA Routing and Switching: Introduction to Networks 5.1 Appendices

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA Routing and Switching: Introduction to Networks course as part of an official Cisco Networking Academy Program.

Chapter 1 Appendix

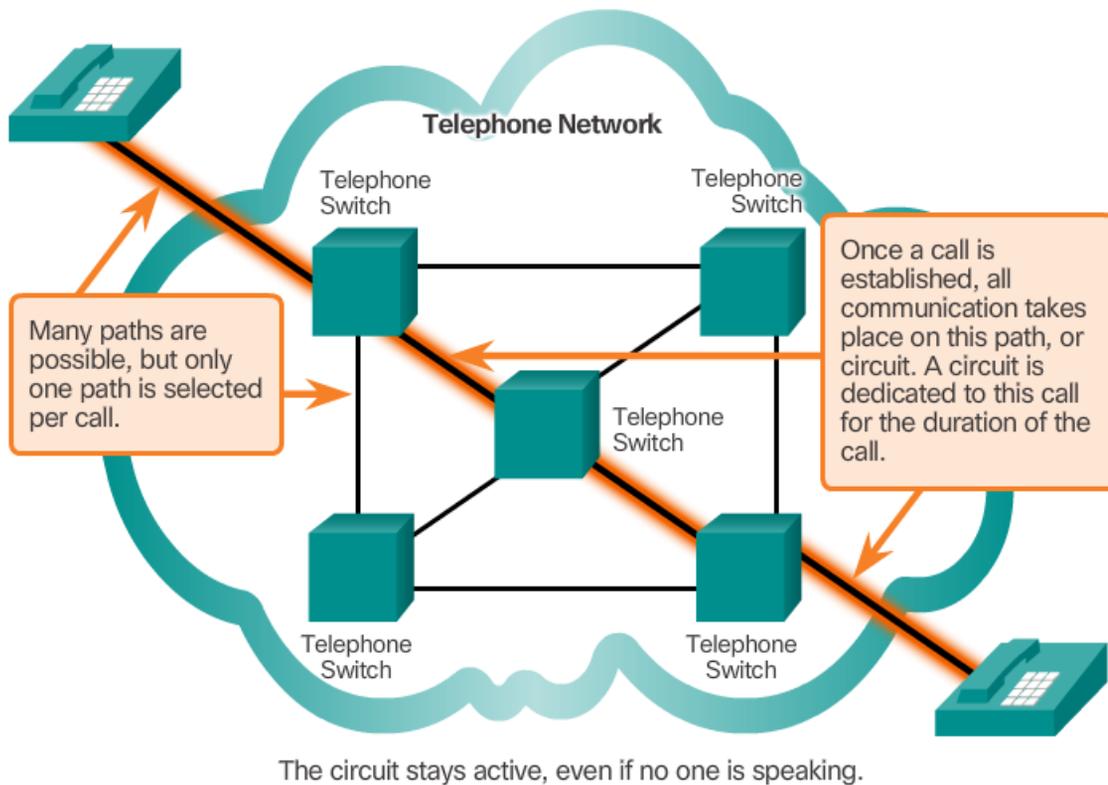
Fault Tolerance

The expectation is that the Internet is always available to the millions of users who rely on it. This requires a network architecture that is built to be fault tolerant. A fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected by it. It is also built in a way that allows quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages can be instantly sent over a different link. Having multiple paths to a destination is known as redundancy.

Circuit-Switched Connection-Oriented Networks

To understand the need for redundancy, we can look at how early telephone systems worked. When a person made a call using a traditional telephone set, the call first went through a setup process. This process identified the telephone switching locations between the person making the call (the source) and the phone set receiving the call (the destination). A temporary path, or circuit, was created for the duration of the telephone call. If any link or device in the circuit failed, the call was dropped. To reconnect, a new call had to be made, with a new circuit. This connection process is referred to as a circuit-switched process and is illustrated Figure A1-1.

Figure A1-1: Circuit Switching in a Telephone Network



There are many, many circuits, but a finite number. During peak periods, some calls may be denied.

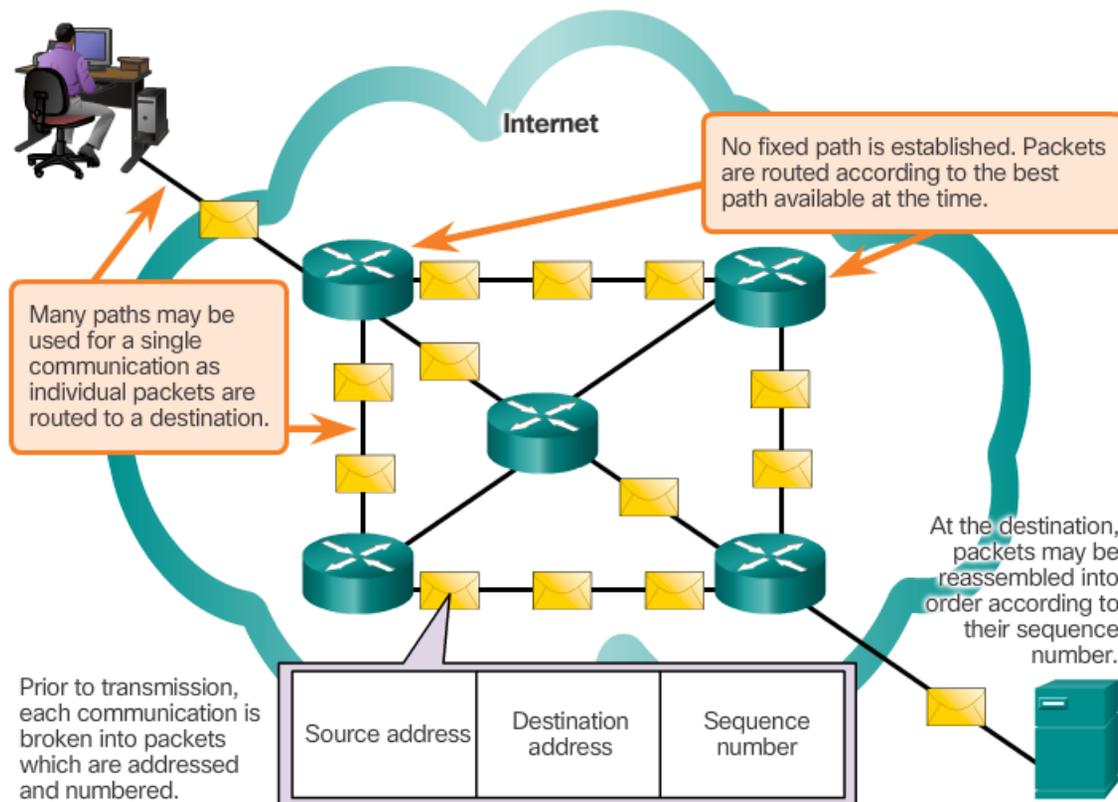
Many circuit-switched networks give priority to existing circuit connections at the expense of new circuit requests. After a circuit is established, even if no communication is occurring between the persons on either end of the call, the circuit remains connected and resources used until one of the parties disconnects the call. Because there are only so many circuits that can be created, it is possible to get a message that all circuits are busy and a call cannot be placed. The cost to create many alternate paths with enough capacity to support a large number of simultaneous circuits, and the technologies necessary to dynamically recreate dropped circuits in the event of a failure, is why circuit switched technology was not optimal for the Internet.

Packet-Switched Networks

In the search for a network that was more fault tolerant, the early Internet designers researched packet switched networks. The premise for this type of network is that a single message can be broken into multiple message blocks, with each message block containing addressing information to

indicate the origination point and final destination. Using this embedded information, these message blocks, called packets, can be sent through the network along various paths, and can be reassembled into the original message when reaching their destination, as illustrated in Figure A1-2.

Figure A1-2: Packet Switching in a Data Network



During peak periods, communication may be delayed, but not denied.

The devices within the network itself are typically unaware of the content of the individual packets. Only visible are the addresses of both the source and the final destination. These addresses are often referred to as IP addresses, represented in a dotted decimal format such as 10.10.10.10. Each packet is sent independently from one location to another. At each location, a routing decision is made as to which path to use to forward the packet towards its final destination. This would be like writing a long message to a friend using ten postcards. Each postcard has the destination address of the recipient. As the postcards are forwarded through the postal system, the destination address is used to determine the next path that postcard should take. Eventually, they will be delivered to the address on the postcards.

If a previously used path is no longer available, the routing function can dynamically choose the next best available path. Because the messages are sent in pieces, rather than as a single complete message, the few packets that may be lost can be retransmitted to the destination along a different path. In many cases, the destination device is unaware that any failure or rerouting occurred. Using our postcard analogy, if one of the postcards is lost along the way, only that postcard needs to be mailed again.

The need for a single, reserved circuit from end-to-end does not exist in a packet switched network. Any piece of a message can be sent through the network using any available path. Additionally, packets containing pieces of messages from different sources can travel the network at the same time. By providing a method to dynamically use redundant paths, without intervention by the user, the Internet has become a fault tolerant method of communication. In our mail analogy, as our postcard travels through the postal system they will share transportation with other postcards, letters and packages. For example, one of the postcards may be placed on an airplane, along with lots of other packages and letters that are being transported toward their final destination.

Although packet-switched connectionless networks are the primary infrastructure for today's Internet, there are some benefits to a connection-oriented system like the circuit-switched telephone system. Because resources at the various switching locations are dedicated to providing a finite number of circuits, the quality and consistency of messages transmitted across a connection-oriented network can be guaranteed. Another benefit is that the provider of the service can charge the users of the network for the period of time that the connection is active. The ability to charge users for active connections through the network is a fundamental premise of the telecommunication service industry.

Scalability

Thousands of new users and service providers connect to the Internet each week. In order for the Internet to support this rapid amount of growth, it must be scalable. A scalable network can expand quickly to support new users and applications without impacting the performance of the service

being delivered to existing users. The Figures A1-3, A1-4, and A1-5 show the tier structure of the Internet.

Figure A1-3: Tier 1

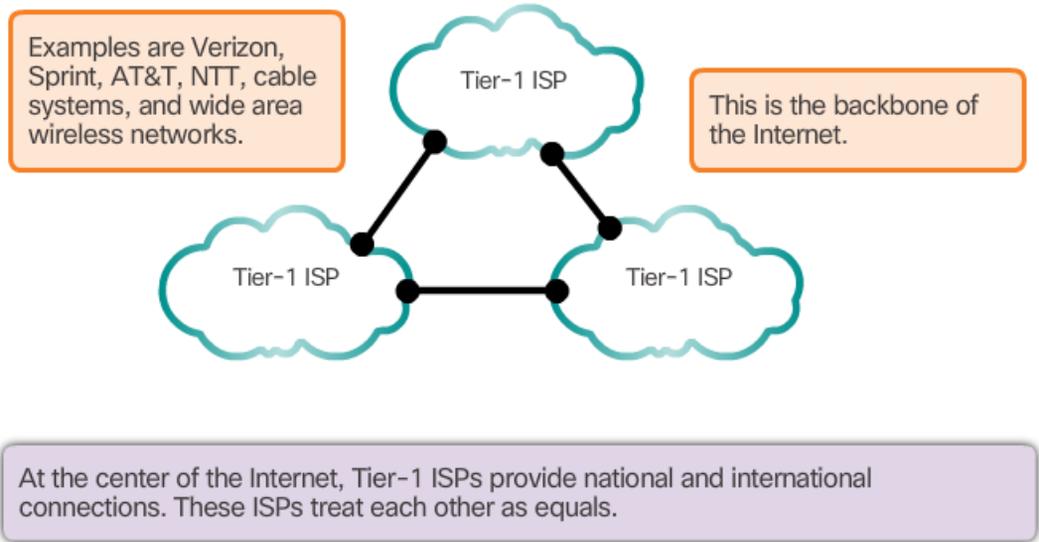


Figure A1-4: Tier 2

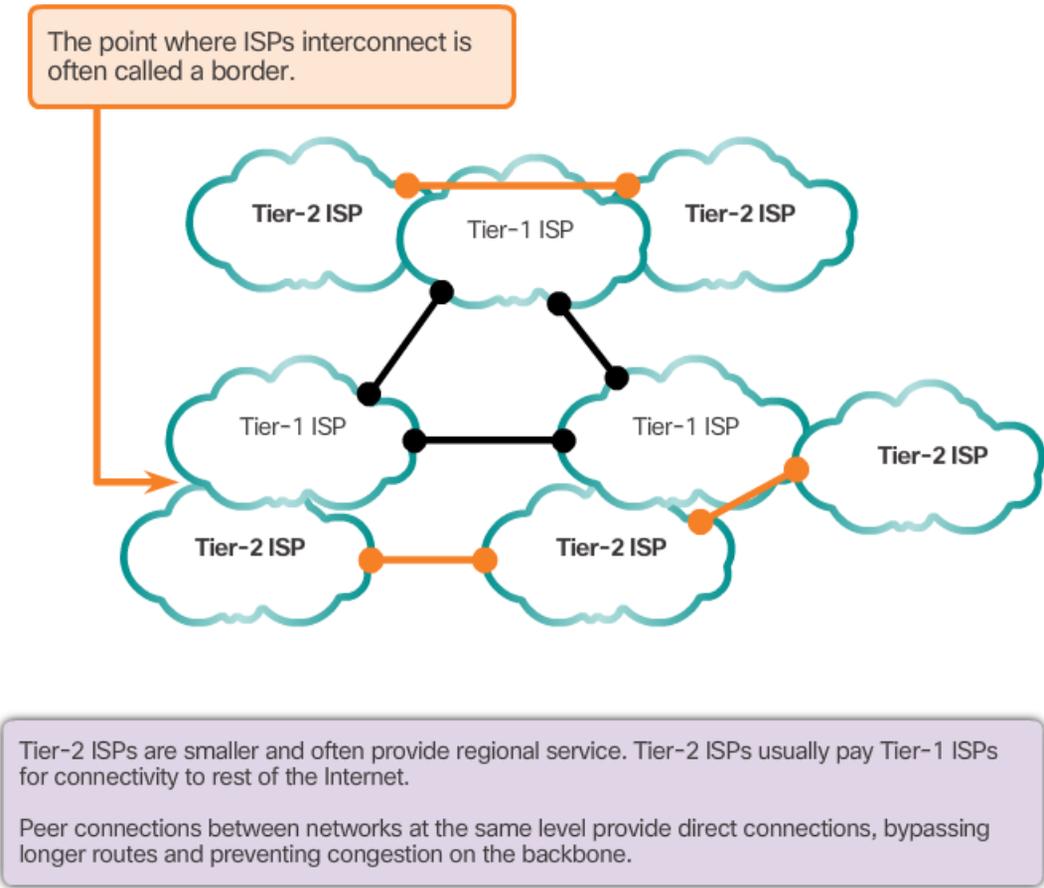
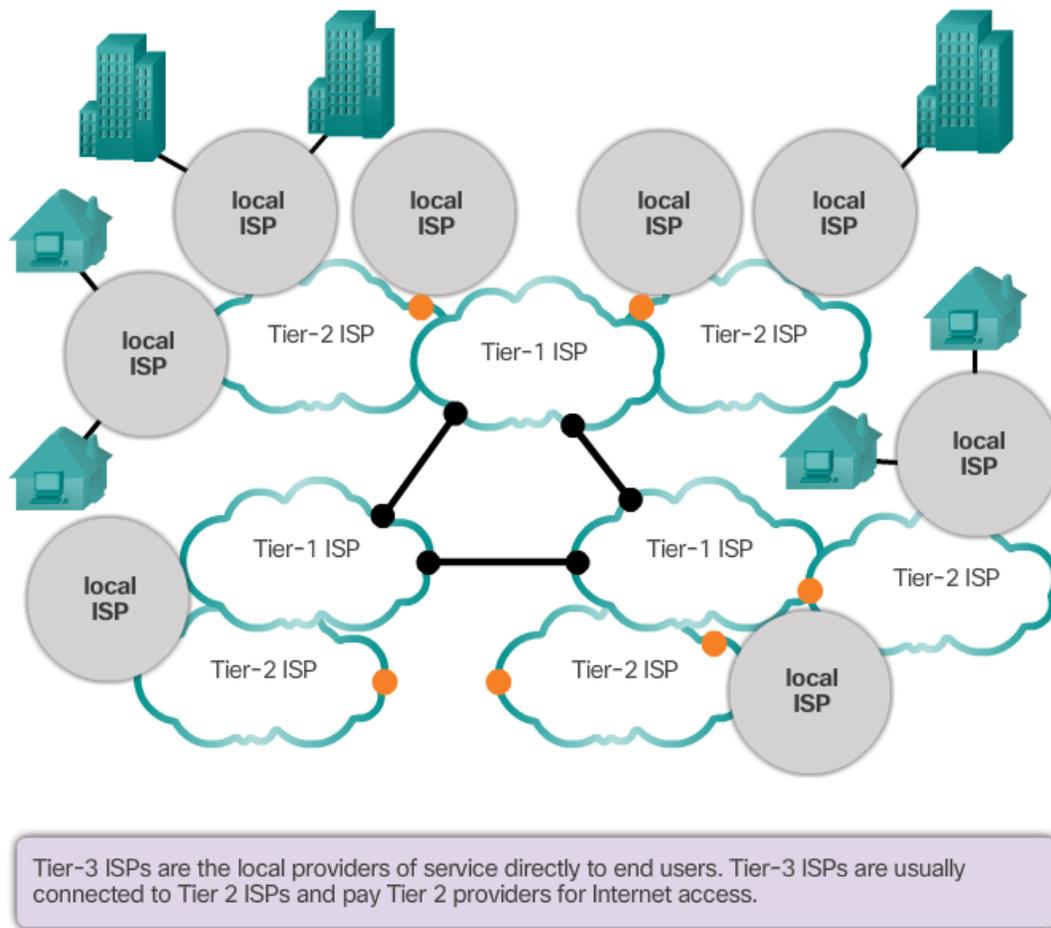


Figure A1-5: Tier 3



The fact that the Internet is able to expand at the rate that it is, without seriously impacting the performance experienced by individual users, is a function of the design of the protocols and underlying technologies on which it is built. The Internet has a hierarchical layered structure for addressing, for naming, and for connectivity services. As a result, network traffic that is destined for local or regional services does not need to traverse to a central point for distribution. Common services can be duplicated in different regions, thereby keeping traffic off the higher level backbone networks.

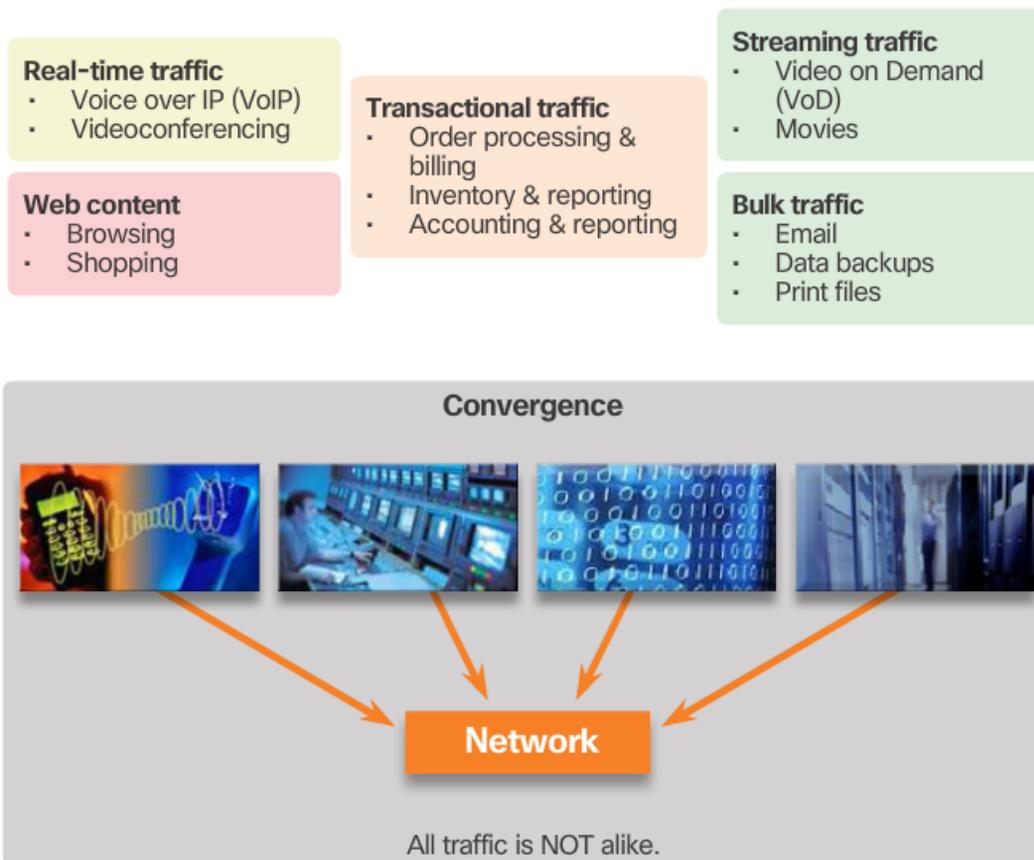
Scalability also refers to the ability to accept new products and applications. Although there is no single organization that regulates the Internet, the many individual networks that provide Internet connectivity cooperate to follow accepted standards and protocols. The adherence to standards enables the manufacturers of hardware and software to concentrate on product development and improvements in the areas of performance and capacity, knowing that the new products can integrate with and enhance the existing infrastructure.

The current Internet architecture, while highly scalable, may not always be able to keep up with the pace of user demand. New protocols and addressing structures are under development to meet the increasing rate at which Internet applications and services are being added.

Quality of Service

Quality of Service (QoS) is also an ever increasing requirement of networks today. New applications available to users over internetworks, such as voice and live video transmissions, as shown in Figure A1-6, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses?

Figure A1-6: Converged Networks

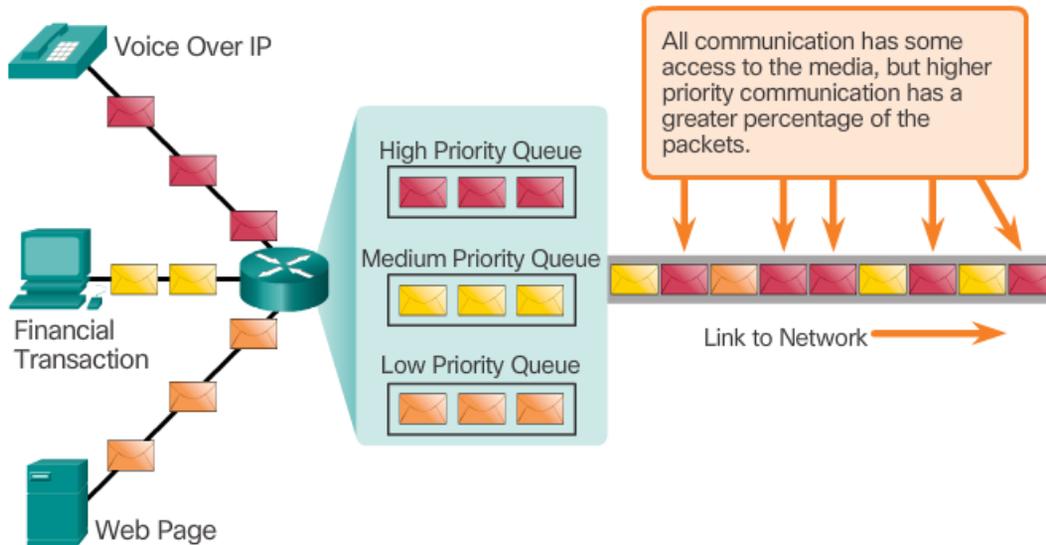


Networks must provide predictable, measurable, and at times, guaranteed services. The packet-switched network architecture does not guarantee that all packets that comprise a particular message will arrive on time, in their correct order, or even that they will arrive at all.

Networks also need mechanisms to manage congested network traffic. Network bandwidth is the measure of the data carrying capacity of the network. In other words, how much information can be transmitted within a specific amount of time? Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion. The network simply has more bits to transmit than what the bandwidth of the communication channel can deliver.

In most cases, when the volume of packets is greater than what can be transported across the network, devices queue, or hold, the packets in memory until resources become available to transmit them, as shown in Figure A1-7. Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed. If the number of packets to be queued continues to increase, the memory queues fill up and packets are dropped.

Figure A1-7: Using Queues to Prioritize Communication



Queuing according to data type enables voice data to have priority over transaction data, which has priority over web data.

Achieving the required QoS by managing the delay and packet loss parameters on a network becomes the secret to a successful end-to-end application quality solution. One way this can be accomplished is through classification. To create QoS classifications of data, we use a combination of communication characteristics and the relative importance assigned to the application, as shown in Figure A1-8. We then treat all data within the same classification according to the same rules. For example, communication that is time-sensitive, such as voice transmissions, would be classified differently from communication that can tolerate delay, such as file transfers.

Figure A1-8: Quality of Service Matters

Communication Type	Without QoS	With QoS
Streaming video or audio	 <p>Choppy picture starts and stops.</p>	 <p>Clear, continuous service.</p>
Vital Transactions	<p>Time : Price</p> <p>02:14:05 : \$1.54</p> <p>Just one second earlier...</p>	<p>Time : Price</p> <p>02:14:04 : \$1.52</p> <p>The price may be better.</p>
Downloading web pages (often lower priority)	 <p>Web pages arrive a bit later...</p>	 <p>But the end result is identical.</p>

Examples of priority decisions for an organization might include:

- **Time-sensitive communication** - increase priority for services like telephony or video distribution
- **Non time-sensitive communication** - decrease priority for web page retrieval or email
- **High importance to organization** - increase priority for production control or business transaction data
- **Undesirable communication** - decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment

Security

The Internet has evolved from a tightly controlled internetwork of educational and government organizations to a widely accessible means for transmission of business and personal communications. As a result, the security requirements of the network have changed. The network infrastructure, services, and the data contained on network attached devices are crucial personal and business assets. Compromising the integrity of these assets could have serious consequences, such as:

- Network outages that prevent communications and transactions from occurring, with consequent loss of business
- Intellectual property (research ideas, patents, or designs) that is stolen and used by a competitor
- Personal or private information that is compromised or made public without the users consent
- Misdirection and loss of personal or business funds
- Loss of important data that takes a significant labor to replace, or is irreplaceable

There are two types of network security concerns that must be addressed: network infrastructure security and information security.

Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them.

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices. Security measures taken in a network should:

- Prevent unauthorized disclosure
- Prevent theft of information (Figure A1-9)
- Prevent unauthorized modification of information
- Prevent Denial of Service (DoS)

Figure A1-9: Security is Important for How We Use a Network

Unauthorized Transactions

Your First Bank

SEND PAYMENT TO
Box 1234
Anytown, USA

CREDIT CARD STATEMENT

ACCOUNT NUMBER 4125-235-412	NAME John Doe	STATEMENT DATE 2/13/01	PAYMENT DUE DATE 3/09/01
CREDIT LINE \$1200.00	CREDIT AVAILABLE \$1074.76	NEW BALANCE \$125.24	MINIMUM PAYMENT DUE \$20.00

REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT	AMOUNT
48387382		3/25	PAYMENT THANK YOU	-168.80
32F14883	1/12	1/15	RECORD RECYCLER ANYTOWN USA	14.83
89102082	1/13	1/15	REEFORAMA REST ANYTOWN USA	39.55
8K34FD32	1/18	1/18	GREAT INSPECTORATIONS BIG CITY USA	27.50
84KT3293A	1/20	1/21	DINO-GRS PETROLSUM ANYTOWN USA	17.26
873DAS321	2/09	2/09	SHIRTS 'N SUCH TOWNVILLEUSA	40.10

Previous Balance	(*)	168.80	Current Amount Due	125.24
Purchases	(*)	125.24	Amount Past Due	
Cash Advances	(*)		Amount Over Credit Line	
Payments	(-)	168.80	Minimum Payment Due	20.00
Credits	(-)			
FINANCE CHARGES	(*)			
Late Charges	(*)			
NEW BALANCE	(*)	125.24		

FINANCE CHARGE SUMMARY	PURCHASES	ADVANCES	For Customer Service Call: 1-800-XXX-XXXX
Periodic Rate	1.65%	0.054%	For Lost or Stolen Card, Call: 1-800-XXX-XXXX
Annual Percentage Rate	19.80%	19.80%	24-Hour Telephone Numbers

Please make check or money order payable to Your First Bank. Include account number on front.



Unauthorized use of our communications data can have severe consequences.

In order to achieve the goals of network security, there are three primary requirements:

- **Ensuring confidentiality** - Data confidentiality means that only the intended and authorized recipients - individuals, processes, or devices – can access and read data. This is accomplished by having a strong system for user authentication, enforcing passwords that are difficult to guess, and requiring users to change them frequently. Encrypting data, so that only the intended recipient can read it, is also part of confidentiality.
- **Maintaining communication integrity** - Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination. Data integrity can be compromised when information has been corrupted - willfully or accidentally. Data integrity is made possible by requiring validation of the sender as well as using mechanisms to validate that the packet has not changed during transmission.
- **Ensuring availability** - Availability means having the assurance of timely and reliable access to data services for authorized users. Network firewall devices, along with desktop and server antivirus software can ensure system reliability and the robustness to detect, repel, and cope with such attacks. Building fully redundant network infrastructures, with few single points of failure, can reduce the impact of these threats.

Chapter 2 Appendix

Cisco IOS Command Reference

The Cisco IOS Command Reference is a collection of online documentation which describes in detail the IOS commands used on Cisco devices. The Command Reference is the ultimate source of information for a particular IOS command, similar to how a dictionary is the ultimate source for information about a particular word.

The Command Reference is a fundamental resource that network engineers use to check various characteristics of a given IOS command. Some of the more common characteristics are:

- **Syntax** - the most detailed version of the syntax for a command that can be found
- **Default** - the manner in which the command is implemented on a device with a default configuration
- **Mode** - the configuration mode on the device where the command is entered
- **History** - descriptions of how the command is implemented relative to the IOS version
- **Usage Guidelines** - guidelines describing specifically how to implement the command
- **Examples** - useful examples that illustrate common scenarios that use the command

To navigate to the Command Reference and find a particular command follow the steps below:

Step 1. Go to www.cisco.com (<http://www.cisco.com/>).

Step 2. Click **Support**.

Step 3. Click **Networking Software** (IOS & NX-OS).

Step 4. Click **15.2M&T** (for example).

Step 5. Click **Reference Guides**.

Step 6. Click **CommandReferences**.

Step 7. Click the particular technology that encompasses the command you are referencing.

Step 8. Click the link on the left that alphabetically matches the command you are referencing.

Step 9. Click the link for the command.

For example, the **description** command is found under the *Cisco IOS Interface and Hardware Component Command Reference*, under the link for the alphabetic range *D through E*.

Note: Complete PDF versions of the command references for a particular technology can be downloaded from links on the page that you reach after completing Step 7 above.

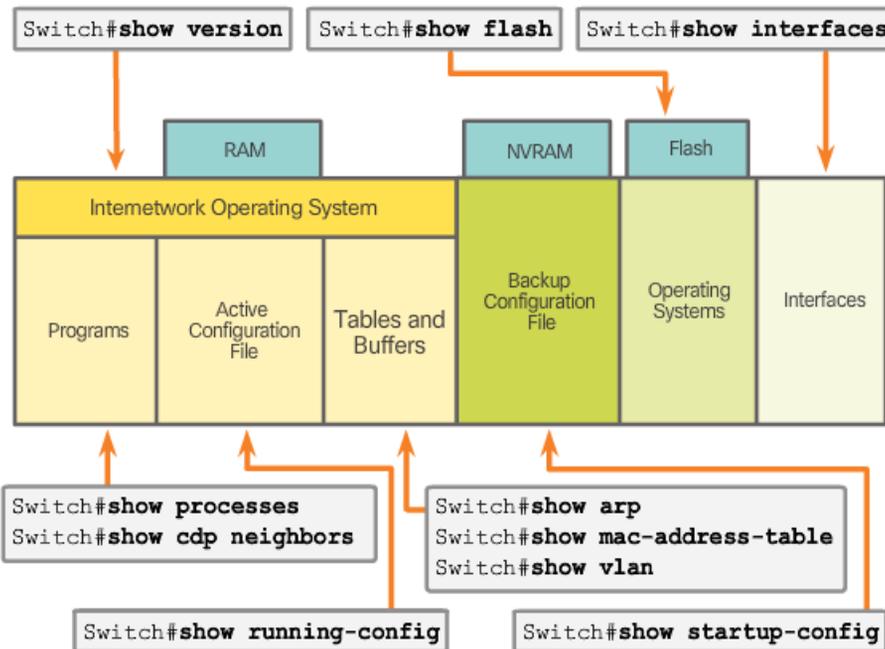
IOS Examination Commands

In order to verify and troubleshoot network operation, we must examine the operation of the devices. The basic examination command is the **show** command.

There are many different variations of this command. As you develop more skill with the IOS, you will learn to use and interpret the output of the **show** commands. Use the **show ?** command to get a list of available commands in a given context, or mode.

A typical **show** command can provide information about the configuration, operation, and status of parts of a Cisco switch or router. Figure A2-1 highlights some of the common IOS commands.

Figure A2-1: Common IOS Show Commands



IOS **show** commands can provide information about the configuration, operation, and status of parts of a Cisco switch or router.

In this course, we focus on mostly basic **show** commands.

A very commonly used **show** command is **show interfaces**. This command displays statistics for all interfaces on the device. To view the statistics for a specific interface, enter the **show interfaces** command followed by the specific interface type and slot/port number. For example:

```
Switch# show interfaces fastethernet 0/1
```

Some other **show** commands frequently used by network technicians include:

show startup-config - Displays the saved configuration located in NVRAM.

show running-config - Displays the contents of the currently running configuration file.

The More Prompt

When a command returns more output than can be displayed on a single screen, the **--More--** prompt appears at the bottom of the screen. When a **-More-** prompt appears, press the **Space bar** to view the next portion of output. To display only the next line, press the **Enter** key. If any other key is pressed, the output is cancelled and you are returned to the prompt.

Chapter 4 Appendix

Physical Layer Encoding and Signaling

Encoding

Common network encoding methods include:

- **Manchester encoding:** A 0 is represented by a high to low voltage transition and a 1 is represented as a low to high voltage transition. This type of encoding is used in older versions of Ethernet, RFID and Near Field Communication.
- **Non-Return to Zero (NRZ):** This is a common means of encoding data that has two states termed “zero” and “one” and no neutral or rest position. A 0 may be represented by one voltage level on the media and a 1 might be represented by a different voltage on the media.

Note: Faster data rates require more complex encoding, such as 4B/5B, however, explanation of these methods is beyond the scope of this course.

Signaling

The physical layer must generate the electrical, optical, or wireless signals that represent the “1” and “0” on the media. The method of representing the bits is called the signaling method. The physical layer standards must define what type of signal represents a “1” and what type of signal represents a “0”. This can be as simple as a change in the level of an electrical signal or optical pulse. For example, a long pulse might represent a 1, whereas a short pulse represents a 0.

This is similar to how Morse code is used for communication. Morse code is another signaling method that uses a series of on-off tones, lights, or clicks to send text over telephone wires or between ships at sea.

Signals can be transmitted in one of two ways:

- **Asynchronous:** Data signals are transmitted without an associated clock signal. The time spacing between data characters or blocks may be of arbitrary duration, meaning the spacing is not standardized. Therefore, frames require start and stop indicator flags.
- **Synchronous:** Data signals are sent along with a clock signal which occurs at evenly spaced time durations referred to as the bit time.

Figure A4-1: Signaling Methods

Media	Physical Components	Frame Encoding Technique	Signalling Method
Copper cable	<ul style="list-style-type: none">• UTP• Coaxial• Connectors• NICs• Ports• Interfaces	<ul style="list-style-type: none">• Manchester Encoding• Non-Return to Zero (NRZ) techniques• 4B/5B codes are used with Multi-Level Transition Level 3 (MLT-3) signaling• 8B/10B• PAM5	<ul style="list-style-type: none">• Changes in the electromagnetic field• Intensity of the electromagnetic field• Phase of the electromagnetic wave

There are many ways to transmit signals. A common method to send data is using modulation techniques. Modulation is the process by which the characteristic of one wave (the signal) modifies another wave (the carrier). The following modulation techniques have been widely used in transmitting data on a medium:

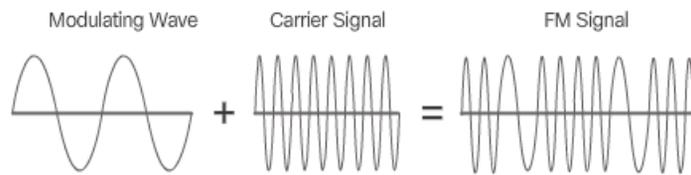
- **Frequency modulation (FM):** A method of transmission in which the carrier frequency varies in accordance with the signal.
- **Amplitude modulation (AM):** A transmission technique in which the amplitude of the carrier varies in accordance with the signal.
- **Pulse-coded modulation (PCM):** A technique in which an analog signal, such as a voice, is converted into a digital signal by sampling the signal’s amplitude and expressing the different amplitudes as a binary number. The sampling rate must be at least twice the highest frequency in the signal.

The nature of the actual signals representing the bits on the media will depend on the signaling method in use. Some methods may use one attribute of signal to represent a single 0 and use another attribute of signal to represent a single 1.

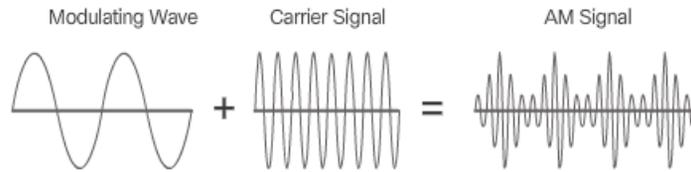
Figure 2 illustrates the how AM and FM techniques are used to send a signal.

Figure A4-2: AM and FM Techniques

Frequency Modulation (FM)



Amplitude Modulation (AM)



802.11 Wi-Fi Standards

Various 802.11 standards have evolved over the years and are highlighted in Figure A4-3. Standards include:

Figure A4-3: 802.11 Standards

Standard	Maximum Speed	Frequency	Backward Compatible
802.11a	54 Mb/s	5 GHz	No
802.11b	11 Mb/s	2.4 GHz	No
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

- **IEEE 802.11a:** Operates in the 5 GHz frequency band and offers speeds of up to 54 Mb/s. Because this standard operates at higher frequencies, it has a smaller coverage area and is less effective at penetrating building structures. Devices operating under this standard are not interoperable with the 802.11b and 802.11g standards described below.
- **IEEE 802.11b:** Operates in the 2.4 GHz frequency band and offers speeds of up to 11 Mb/s. Devices implementing this standard have a longer range and are better able to penetrate building structures than devices based on 802.11a.
- **IEEE 802.11g:** Operates in the 2.4 GHz frequency band and offers speeds of up to 54 Mbps. Devices implementing this standard therefore operate at the same radio frequency and range as 802.11b but with the bandwidth of 802.11a.
- **IEEE 802.11n:** Operates in the 2.4 GHz and 5 GHz frequency bands. The typical expected data rates range from 150 Mb/s to 600 Mb/s with a distance range of up to 70 meters. It is backward compatible with 802.11a/b/g devices.
- **IEEE 802.11ac:** Operates in the 5 GHz frequency band providing data rates ranging from 450 Mb/s to 1.3 Gb/s (1300 Mb/s.) It is backward compatible with 802.11a/n devices.
- **IEEE 802.11ad:** Also known as "WiGig". It uses a tri-band Wi-Fi solution using 2.4 GHz, 5 GHz, and 60 GHz and offers theoretical speeds of up to 7 Gb/s.

Controlled Access

When using the controlled access method, network devices take turns, in sequence, to access the medium. If an end device does not need to access the medium, then the opportunity passes to the next end device. This process is facilitated by use of a token. An end device acquires the token and places a frame on the media, no other device can do so until the frame has arrived and been processed at the destination, releasing the token.

Note: This method is also known as scheduled access or deterministic.

Although controlled access is well-ordered and provides predictable throughput, deterministic methods can be inefficient because a device has to wait for its turn before it can use the medium.

Controlled access examples include:

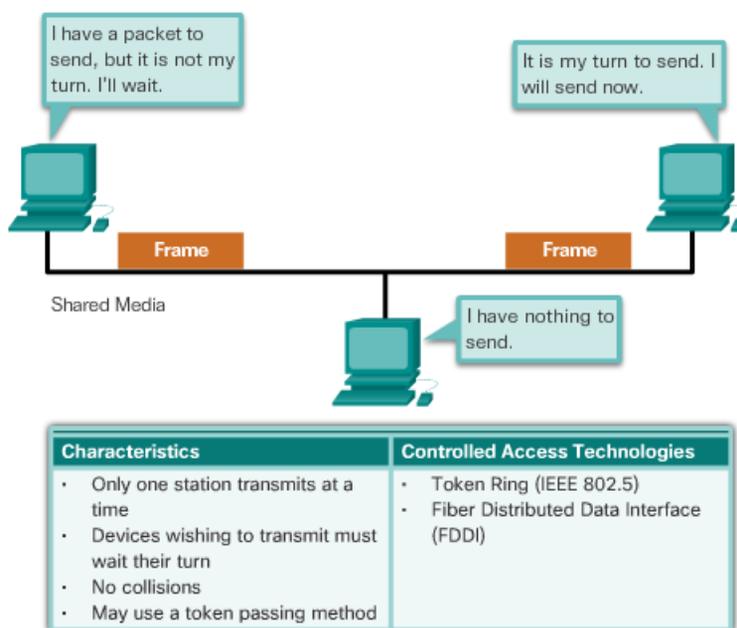
- Token Ring (IEEE 802.5)
- Fiber Distributed Data Interface (FDDI) which is based on the IEEE 802.4 token bus protocol.

Note: Both of these media access control methods are considered obsolete.

Figure A4-4 illustrates the following:

- How controlled access methods operate
- Characteristics of controlled access methods
- Examples of controlled access methods

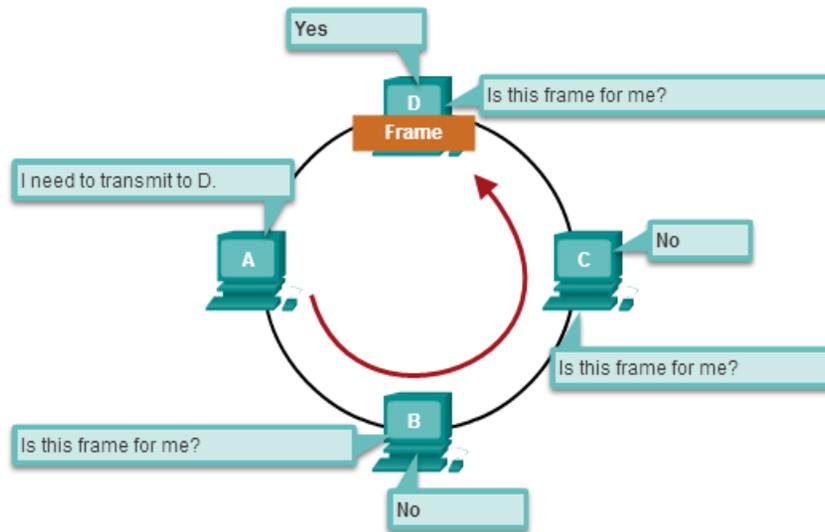
Figure A4-4: Controlled Access



Ring Topology

In a logical ring topology shown in Figure A4-5, each node in turn receives a frame. If the frame is not addressed to the node, the node passes the frame to the next node. This allows a ring to use a controlled media access control technique called token passing.

Figure A4-5: Logical Ring Topology



Nodes in a logical ring topology remove the frame from the ring, examine the address, and send it on if it is not addressed for that node. In a ring, all nodes around the ring (between the source and destination node) examine the frame.

There are multiple media access control techniques that could be used with a logical ring, depending on the level of control required. For example, only one frame at a time is usually carried by the media. If there is no data being transmitted, a signal (known as a token) may be placed on the media and a node can only place a data frame on the media when it has the token.

Remember that the data link layer "sees" a logical ring topology. The actual physical cabling topology could be another topology.

The Frame Trailer

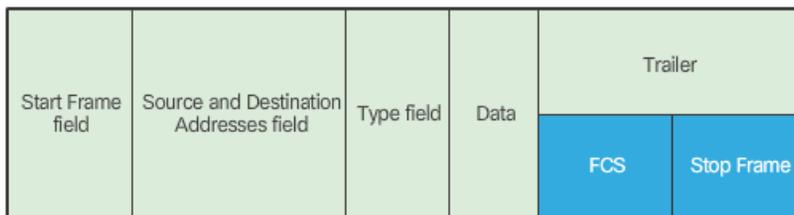
Data link layer protocols add a trailer to the end of each frame. The trailer is used to determine if the frame arrived without error. This process is called error detection and is accomplished by placing a logical or mathematical summary of the bits that comprise the frame in the trailer. Error detection is added at the data link layer because the signals on the media could be subject to interference, distortion, or loss that would substantially change the bit values that those signals represent.

A transmitting node creates a logical summary of the contents of the frame. This is known as the cyclic redundancy check (CRC) value. This value is placed in the Frame Check Sequence (FCS) field of the frame to represent the contents of the frame.

The FCS and Stop Frame portions of the trailer in Figure A4-6 are described as follows:

- **FCS** - This field is used for error checking. The source calculates a number based on the frame's data and places that number in the FCS field. The destination then recalculates the data to see if the FCS matches. If they don't match, the destination deletes the frame.
- **Stop Frame** - This field, also called the Frame Trailer, is an optional field that is used when the length of the frame is not specified in the Type/Length field. It indicates the end of the frame when transmitted.

Figure A4-6: Contents of the Frame Trailer



When the frame arrives at the destination node, the receiving node calculates its own logical summary, or CRC, of the frame. The receiving node compares the two CRC values. If the two values are the same, the frame is considered to have arrived as transmitted. If the CRC value in the FCS differs from the CRC calculated at the receiving node, the frame is discarded.

Therefore, the FCS field is used to determine if errors occurred in the transmission and reception of the frame. The error detection mechanism provided by the use of the FCS field discovers most errors caused on the media.

There is always the small possibility that a frame with a good CRC result is actually corrupt. Errors in bits may cancel each other out when the CRC is calculated. Upper layer protocols would then be required to detect and correct this data loss.

Ethernet Frame

Ethernet is the dominant LAN technology. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.

Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. Ethernet is the most widely used LAN technology and supports data bandwidths of 10 Mbps, 100 Mbps, 1 Gbps (1,000 Mbps), or 10 Gbps (10,000 Mbps).

The basic frame format and the IEEE sublayers of OSI Layers 1 and 2 remain consistent across all forms of Ethernet. However, the methods for detecting and placing data on the media vary with different implementations.

Ethernet provides unacknowledged connectionless service over a shared media using CSMA/CD as the media access methods. Shared media requires that the Ethernet frame header use a data link layer address to identify the source and destination nodes. As with most LAN protocols, this address is referred to as the MAC address of the node. An Ethernet MAC address is 48 bits and is generally represented in hexadecimal format.

Figure A4-7 shows the many fields of the Ethernet frame. At the data link layer, the frame structure is nearly identical for all speeds of Ethernet. However, at the physical layer, different versions of Ethernet place the bits onto the media differently. Ethernet is discussed in more detail in the next chapter.

Figure A4-7: Fields of the Ethernet Frame

Frame						
Field name	Preamble	Destination	Source	Type	Data	Frame Check Sequence
Size	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

Preamble - Used for synchronization; also contains a delimiter to mark the end of the timing information

Destination Address - 48-bit MAC address for the destination node

Source Address - 48-bit MAC address for the source node

Type - Value to indicate which upper layer protocol will receive the data after the Ethernet process is complete

Data or payload - This is the PDU, typically an IPv4 packet, that is to be transported over the media.

Frame Check Sequence (FCS) - A value used to check for damaged frames

PPP Frame

Another data link layer protocol is the Point-to-Point Protocol (PPP). PPP is a protocol used to deliver frames between two nodes. Unlike many data link layer protocols that are defined by electrical engineering organizations, the PPP standard is defined by RFCs. PPP was developed as a WAN protocol and remains the protocol of choice to implement many serial WANs. PPP can be used on various physical media, including twisted pair, fiber-optic lines, and satellite transmission, as well as for virtual connections.

PPP uses a layered architecture. To accommodate the different types of media, PPP establishes logical connections, called sessions, between two nodes. The PPP session hides the underlying physical media from the upper PPP protocol. These sessions also provide PPP with a method for encapsulating multiple protocols over a point-to-point link. Each protocol encapsulated over the link establishes its own PPP session.

PPP also allows the two nodes to negotiate options within the PPP session. This includes authentication, compression, and multilink (the use of multiple physical connections). Figure A4-8 shows the basic fields in a PPP frame.

Figure A4-8: Fields of the PPP Frame

Frame						
Field name	Flag	Address	Control	Protocol	Data	FCS
Size	1 byte	1 byte	1 byte	2 bytes	variable	2 or 4 bytes

Flag - A single byte that indicates the beginning or end of a frame. The flag field consists of the binary sequence 01111110.

Address - A single byte that contains the standard PPP broadcast address. PPP does not assign individual station addresses.

Control - A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.

Protocol - Two bytes that identify the protocol encapsulated in the data field of the frame. The most up-to-date values of the protocol field are specified in the most recent Assigned Numbers Request For Comments (RFC).

Data - Zero or more bytes that contain the datagram for the protocol specified in the protocol field.

Frame Check Sequence (FCS) - Normally 16 bits (2 bytes). By prior agreement, consenting PPP implementations can use a 32-bit (4-byte) FCS for improved error detection.

802.11 Wireless Frame

The IEEE 802.11 standard uses the same 802.2 LLC and 48-bit addressing scheme as other 802 LANs. However, there are many differences at the MAC sublayer and physical layer. In a wireless environment, the environment requires special considerations. There is no definable physical connectivity; therefore, external factors may interfere with data transfer and it is difficult to control access. To meet these challenges, wireless standards have additional controls.

The IEEE 802.11 standard is commonly referred to as Wi-Fi. It is a contention-based system using a CSMA/CA media access process. CSMA/CA specifies a random backoff procedure for all nodes that are waiting to transmit. The most likely opportunity for medium contention is just after the medium becomes available. Making the nodes back off for a random period greatly reduces the likelihood of a collision.

802.11 networks also use data link acknowledgements to confirm that a frame is received successfully. If the sending station does not detect the acknowledgement frame, either because the original data frame or the acknowledgment was not received intact, the frame is retransmitted. This explicit acknowledgement overcomes interference and other radio-related problems.

Other services supported by 802.11 are authentication, association (connectivity to a wireless device), and privacy (encryption).

As shown in Figure A4-9, an 802.11 frame contains these fields:

- **Protocol Version field:** Version of 802.11 frame in use
- **Type and Subtype fields:** Identifies one of three functions and sub functions of the frame: control, data, and management
- **To DS field:** Set to 1 in data frames destined for the distribution system (devices in the wireless structure)
- **From DS field:** Set to 1 in data frames exiting the distribution system
- **More Fragments field:** Set to 1 for frames that have another fragment
- **Retry field:** Set to 1 if the frame is a retransmission of an earlier frame
- **Power Management field:** Set to 1 to indicate that a node will be in power-save mode
- **More Data field:** Set to 1 to indicate to a node in power-save mode that more frames are buffered for that node
- **Wired Equivalent Privacy (WEP) field:** Set to 1 if the frame contains WEP encrypted information for security
- **Order field:** Set to 1 in a data type frame that uses Strictly Ordered service class (does not need reordering)
- **Duration/ID field:** Depending on the type of frame, represents either the time, in microseconds, required to transmit the frame or an association identity (AID) for the station that transmitted the frame
- **Destination Address (DA) field:** MAC address of the final destination node in the network
- **Source Address (SA) field:** MAC address of the node that initiated the frame
- **Receiver Address (RA) field:** MAC address that identifies the wireless device that is the immediate recipient of the frame
- **Fragment Number field:** Indicates the number for each fragment of a frame

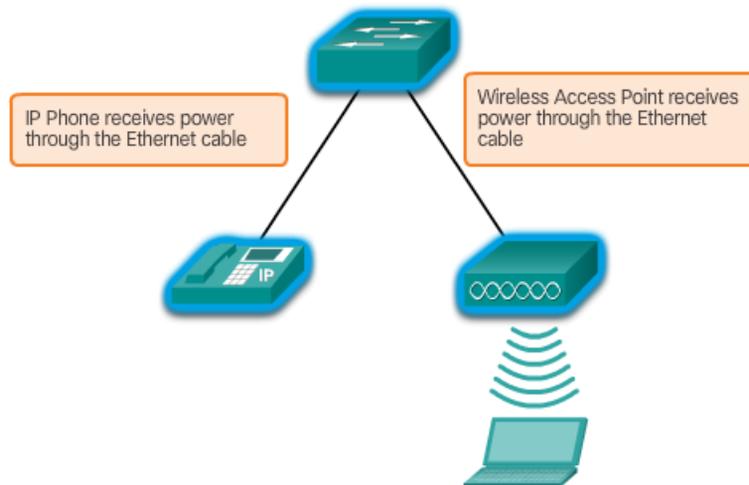
Chapter 5 Appendix

Fixed versus Modular Switches

When selecting a switch, it is important to understand the key features of the switch options available. This means that it is necessary to decide on features such as whether Power over Ethernet (PoE) is necessary, and the preferred "forwarding rate".

As shown in Figure A5-1, PoE allows a switch to deliver power to a device, such as IP phones and some wireless access points, over the existing Ethernet cabling. This allows more flexibility for installation.

Figure A5-1: Power over Ethernet (PoE)



The forwarding rate defines the processing capabilities of a switch by rating how much data the switch can process per second. Switch product lines are classified by forwarding rates. Entry-layer switches have lower forwarding rates than enterprise-layer switches. Other considerations include whether the device is stackable or non-stackable as well as the thickness of the switch (expressed in number of rack units), and port density, or the number of ports available on a single switch. The port density of a device can vary depending on whether the device is a fixed configuration device or a modular device.

These options are sometimes referred to as switch form factors. Figure A5-2 displays examples of fixed configuration, modular, and stackable configuration switches.

Figure A5-2: Switch Form Factors



Fixed Configuration Switches

Features and options are limited to those that originally come with the switch.



Modular Configuration Switches

The chassis accepts line cards that contain the ports.



Stackable Configuration Switches

Stackable switches, connected by a special cable, effectively operate as one large switch.

Fixed Configuration Switches

Fixed configuration switches are just as you might expect, fixed in their configuration. What that means is that you cannot add features or options to the switch beyond those that originally came with the switch. The particular model you purchase determines the features and options available. For example, if you purchase a 24-port gigabit fixed switch, you cannot add additional ports when you need them. There are typically different configuration choices that vary in how many and what types of ports are included.

Modular Switches

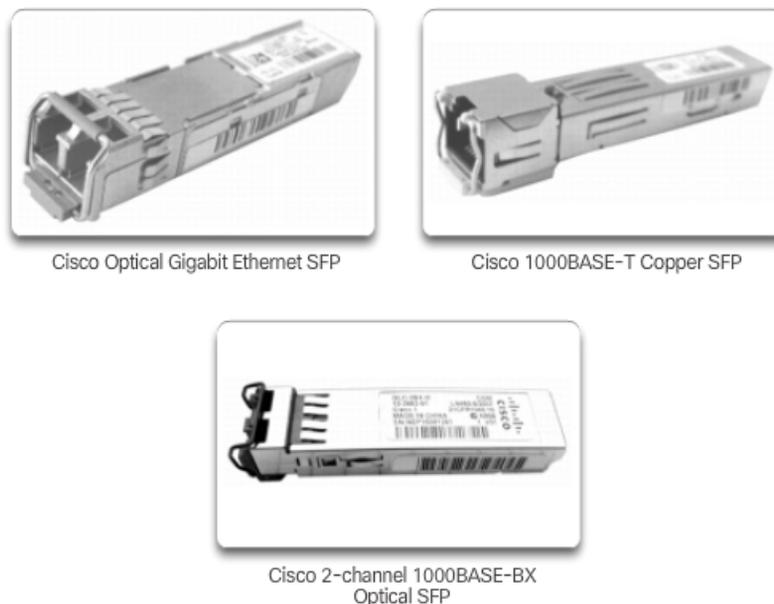
Modular switches offer more flexibility in their configuration. Modular switches typically come with different sized chassis that allow for the installation of different numbers of modular line cards. The line cards actually contain the ports. The line card fits into the switch chassis like expansion cards fit into a PC. The larger the chassis, the more modules it can support. As you can see in the figure, there can be many different chassis sizes to choose from. If you bought a modular switch with a 24-port line card, you could easily add an additional 24 port line card, to bring the total number of ports up to 48.

Module Options for Cisco Switch Slots

The Cisco switch product lines are widely deployed globally, in large part due to the flexibility they provide for add-on options. Not only does the Cisco IOS have the richest set of features available relative to any other network operating system, but the IOS is tailor fit to each Cisco networking device, switches in particular.

To illustrate the options available, which are literally too voluminous to list here, we focus on the Catalyst 3560 switches. The Catalyst 3560 switches have Small Form-Factor Pluggable (SFP) ports that support a number of SFP transceiver modules. Some example SFP modules are shown in Figure A5-3.

Figure A5-3: SFP Modules



Here is a list of the SFP modules supported on one or more types of 3560 switches:

Fast Ethernet SFP Modules –

- 100BASE-FX (multimode fiber-optic (MMF)) for 2 kilometers (km)
- 100BASE-LX10 (single-mode fiber-optic (SMF)) for 2km
- 100BASE-BX10 (SMF) for 10 km
- 100BASE-EX (SMF) for 40 km
- 100BASE-ZX (SMF) for 80 km

Gigabit Ethernet SFP Modules –

- 1000BASE-SX 50/62.5 μ m (MMF) up to 550/220 m
- 1000BASE-LX/LH (SMF/MMF) up to 10/0.550 k
- 1000BASE-ZX (SMF) up to 70 km
- 1000BASE-BX10-D&1000BASE-BX10-U (SMF) up to 10 km

- 1000BASE-T (copper wire transceiver)

10 Gigabit Ethernet SFP Modules –

- 10G-SR (MMF) up to 400 m
- 10G-SR-X (MMF) up to 400 m (supporting extended temperature range)
- 10G-LRM (MMF) up to 220 m
- FET-10G (MMF) up to 100 m (for Nexus fabric uplinks)
- 10G-LR (SMF) up to 10 km
- 10G-LR-X (SMF) up to 10 km (supporting extended temperature range)
- 10G-ER (SMF) up to 40 km
- 10G-ZR (SMF) up to 80 km
- Twinax (copper wire transceiver) up to 10 m
- Active Optical up to 10 m (for intra/inter-rack connections)

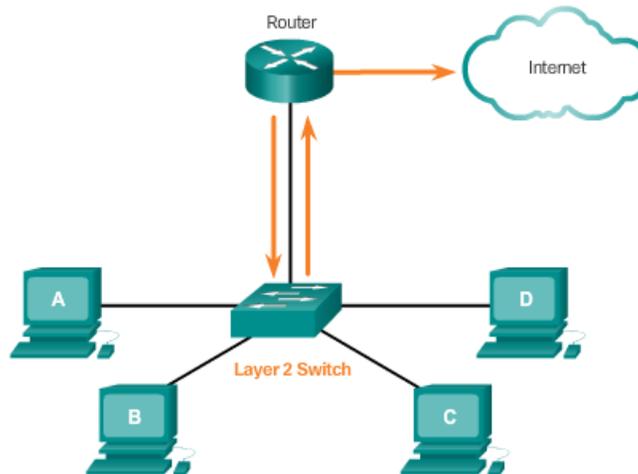
40 Gigabit Ethernet and 100 Gigabit Ethernet modules are supported on high-end Cisco devices, such as the Catalyst 6500, the CRS router, the ASR 9000 series router, and the Nexus 7000 series switch.

Layer 2 versus Layer 3 Switching

In addition to determining the various switch form factors, it may also be necessary to choose between a Layer 2 LAN switch and a Layer 3 switch.

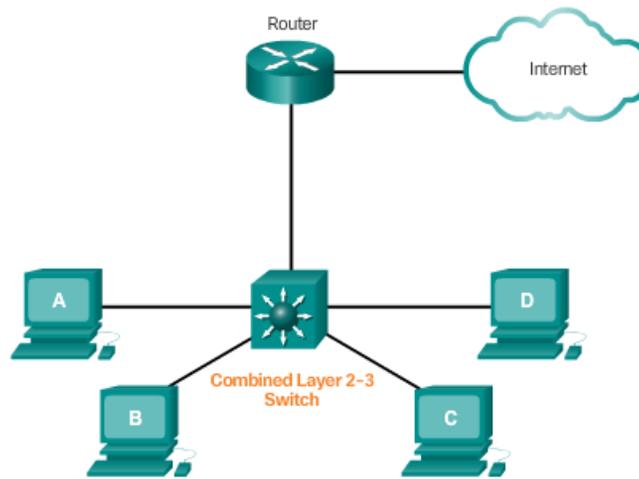
Recall that a Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address and depends upon routers to pass data between independent IP subnetworks (see Figure A5-4).

A5-4: Layer 2 Switching



As shown in Figure A5-6, a Layer 3 switch, such as the Catalyst 3560, functions similarly to a Layer 2 switch, such as the Catalyst 2960, but instead of using only the Layer 2 MAC address information for forwarding decisions, a Layer 3 switch can also use IP address information.

A5-6: Layer 3 Switching



Instead of only learning which MAC addresses are associated with each of its ports, a Layer 3 switch can also learn which IP addresses are associated with its interfaces. This allows the Layer 3 switch to direct traffic throughout the network based on IP address information as well.

Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN. Because Layer 3 switches have specialized switching hardware, they can typically route data as quickly as they can switch.

Cisco Express Forwarding

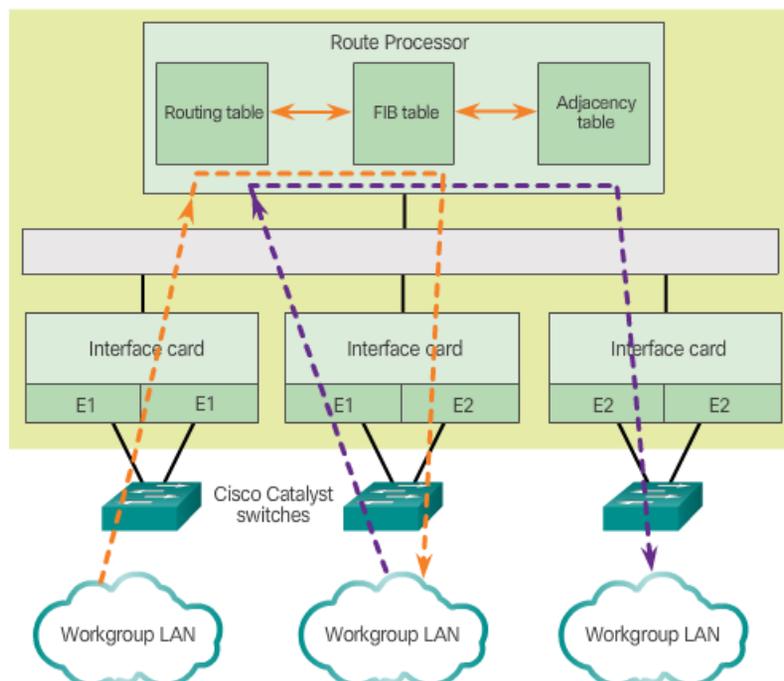
Cisco devices which support Layer 3 switching utilize Cisco Express Forwarding (CEF). This forwarding method is quite complex, but fortunately, like any good technology, is carried out in large part "behind the scenes". Normally very little CEF configuration is required on a Cisco device.

Basically, CEF decouples the usual strict interdependence between Layer 2 and Layer 3 decision making. What makes forwarding IP packets slow is the constant referencing back-and-forth between Layer 2 and Layer 3 constructs within a networking device. So, to the extent that Layer 2 and Layer 3 data structures can be decoupled, forwarding is accelerated.

The two main components of CEF operation, as shown in Figure A5-6, are the:

- Forwarding Information Base (FIB)
- Adjacency tables

Figure A5-6: Cisco Express Forwarding



The FIB is conceptually similar to a routing table. A router uses the routing table to determine best path to a destination network based on the network portion of the destination IP address. With CEF, information previously stored in the route cache is, instead, stored in several data

structures for CEF switching. The data structures provide optimized lookup for efficient packet forwarding. A networking device uses the FIB lookup table to make destination-based switching decisions without having to access the route cache.

The FIB is updated when changes occur in the network and contains all routes known at the time.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries.

The separation of the reachability information (in the FIB table) and the forwarding information (in the adjacency table), provides a number of benefits:

- The adjacency table can be built separately from the FIB table, allowing both to be built without any packets being process switched.
- The MAC header rewrite used to forward a packet is not stored in cache entries, so changes in a MAC header rewrite string do not require invalidation of cache entries.

CEF is enabled by default on most Cisco devices that perform Layer 3 switching.

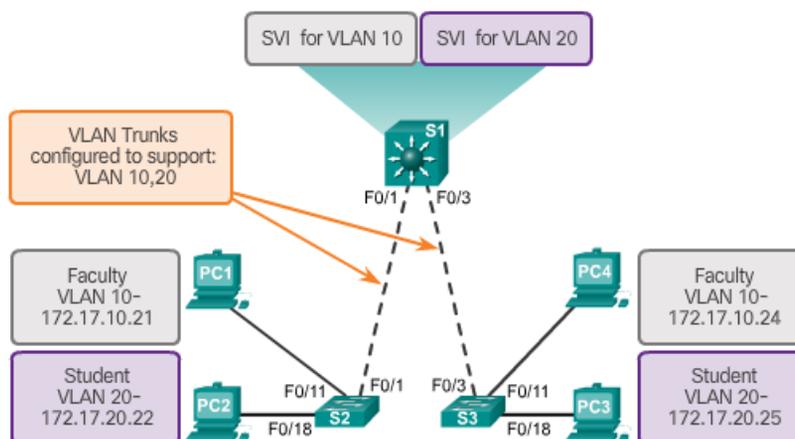
Types of Layer 3 Interfaces

Cisco networking devices support a number of distinct types of Layer 3 interfaces. A Layer 3 interface is one that supports forwarding IP packets toward a final destination based on the IP address.

The major types of Layer 3 interfaces are:

- **Switch Virtual Interface (SVI)** - Logical interface on a switch associated with a virtual local area network (VLAN) (Figure A5-7).
- **Routed Port** - Physical port on a Layer 3 switch configured to act as a router port.
- **Layer 3 EtherChannel** - Logical interface on a Cisco device associated with a bundle of routed ports.

Figure A5-7: Switch Virtual Interfaces



An SVI for the default VLAN (VLAN1) must be enabled to provide IP host connectivity to the switch and permit remote switch administration. SVIs must also be configured to allow routing between VLANs. SVIs are logical interfaces configured for specific VLANs; to route between two or more VLANs, each VLAN must have a separate SVI enabled.

Routed ports enable (Layer 3) Cisco switches to effectively serve as routers. Each port on such a switch can be configured as a port on an independent IP network.

Layer 3 EtherChannels are used to bundle Layer 3 Ethernet links between Cisco devices in order to aggregate bandwidth, typically on uplinks.

Note: In addition to SVIs and L3 EtherChannels, other logical interfaces on Cisco devices include loopback interfaces and tunnel interfaces.

Configuring a Routed Port on a Layer 3 Switch

A switch port can be configured to be a Layer 3 routed port and behave like a regular router interface. Specifically, a routed port:

- Is not associated with a particular VLAN.
- Can be configured with a Layer 3 routing protocol.
- Is a Layer 3 interface only and does not support Layer 2 protocol.

The configuration steps are shown in Figure A5-8.

Figure A5-8: Routed Port Configuration

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar 1 00:15:40.115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
Vlan1          unassigned      YES unset  administratively down  down
FastEthernet0/1 unassigned      YES unset  down                down
FastEthernet0/2 unassigned      YES unset  down                down
FastEthernet0/3 unassigned      YES unset  down                down
FastEthernet0/4 unassigned      YES unset  down                down
FastEthernet0/5 unassigned      YES unset  down                down
FastEthernet0/6 192.168.200.1  YES manual  up                up
FastEthernet0/7 unassigned      YES unset  up                  up
FastEthernet0/8 unassigned      YES unset  up                  up
<output omitted>
```

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration

Chapter 6 Appendix

Host Routing Tables

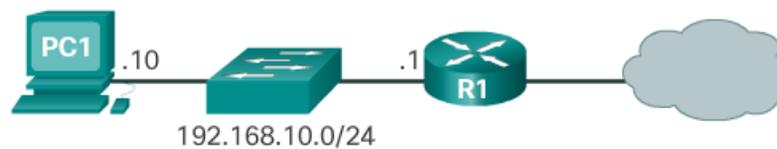
To access a resource on a network, your host will determine the route to the destination host using its routing table. The host routing table is similar to that of a router, but is specific to the local host and much less complex.

IPv4 Host Routing Table

On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table. Both commands generate the same output. The output may seem overwhelming at first, but is fairly simple to understand.

Figure A6-1 displays the IPv4 Route Table section of the output.

Figure A6-1: IPv4 Host Routing Table



```
C:\Users\PC1>netstat -r

<Output omitted>

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.10.1    192.168.10.10    25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
192.168.10.0               255.255.255.0    On-link         192.168.10.10    281
192.168.10.10              255.255.255.255 On-link         192.168.10.10    281
192.168.10.255            255.255.255.255 On-link         192.168.10.10    281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         192.168.10.10    281
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         192.168.10.10    281
=====

<Output omitted>
```

Notice the output is divided into five columns which identify:

- **Network Destination** - Lists the reachable networks.
- **Netmask** - Lists a subnet mask that informs the host how to determine the network and the host portions of the IP address.
- **Gateway** - Lists the address used by the local computer to get to a remote network destination. If a destination is directly reachable, it will show as "on-link" in this column.
- **Interface** - Lists the address of the physical interface used to send the packet to the gateway that is used to reach the network destination.
- **Metric** - Lists the cost of each route and is used to determine the best route to a destination.

IPv4 Host Routing Entries

To help simplify the output, the destination networks can be grouped into five sections as identified by the highlighted areas in Figure A6-2:

Figure A6-2: IPv4 Host Entries



```
C:\Users\PC1> netstat -r

<Output omitted>

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.10.1    192.168.10.10    25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
192.168.10.0               255.255.255.0    On-link         192.168.10.10    281
192.168.10.10              255.255.255.255 On-link         192.168.10.10    281
192.168.10.255             255.255.255.255 On-link         192.168.10.10    281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         192.168.10.10    281
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         192.168.10.10    281
=====

<Output omitted>
```

0.0.0.0

The local default route; that is, all packets with destinations that do not match other specified addresses in the routing table are forwarded to the gateway. Therefore, all non-matching destination routes are sent to the gateway with IP address 192.168.10.1 (R1) exiting from the interface with IP address 192.168.10.10. Note that the final destination address specified in the packet does not change; rather, the host simply knows to forward the packet to the gateway for further processing.

127.0.0.0 – 127.255.255.255

These loopback addresses all relate to the direct connection and provide services to the local host.

192.168.10.0 - 192.168.10.255

These addresses all relate to the host and local network. All packets with destination addresses that fall into this category will exit out of the 192.168.10.10 interface.

- **192.168.10.0** - The local network route address; represents all computers on the 192.168.10.x network.
- **192.168.10.10** - The address of the local host.
- **192.168.10.255** - The network broadcast address; sends messages to all hosts on the local network route.

224.0.0.0

These are special multicast class D addresses reserved for use through either the loopback interface (127.0.0.1) or the host IP address (192.168.10.10).

255.255.255.255

The last two addresses represent the limited broadcast IP address values for use through either the loopback interface (127.0.0.1) or the host IP address (192.168.10.10). These addresses can be used to find a DHCP server before the local IP is determined.

Sample IPv4 Host Routing Table

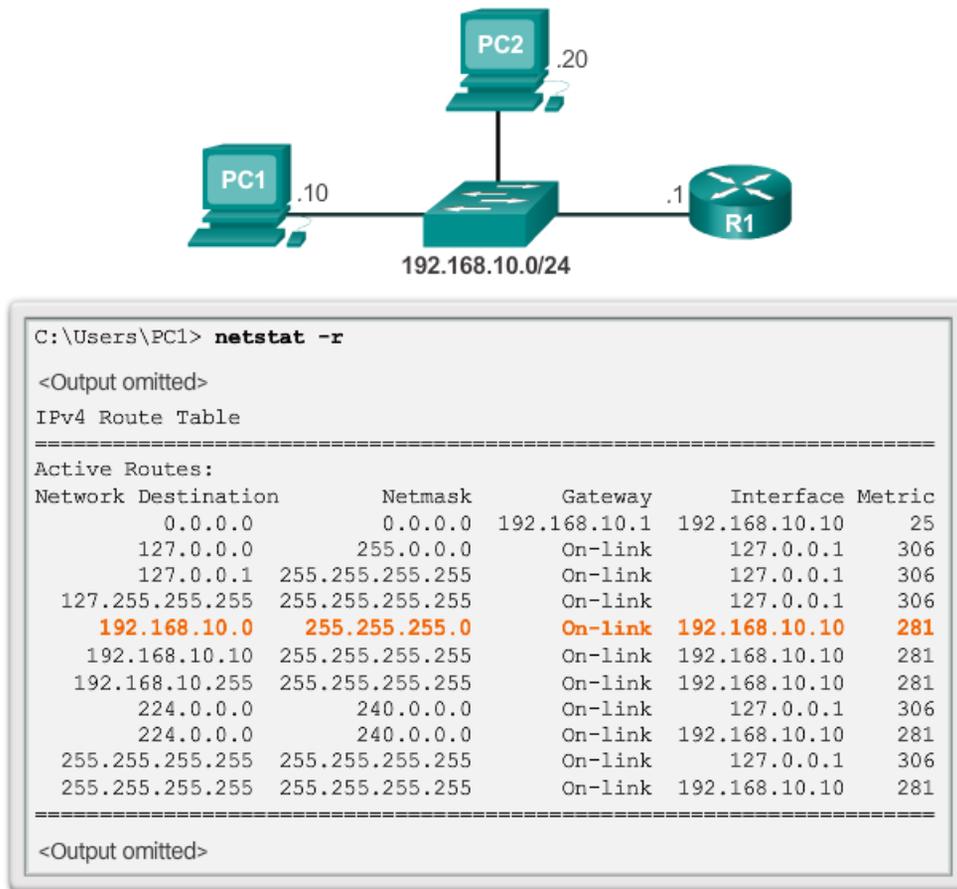
If PC1 wanted to send a packet to 192.168.10.20, it would:

1. Consult the IPv4 Route Table.

- Match the destination IP address with the 192.168.10.0 Network Destination entry to reveal that the host is on the same network (On-link).
- PC1 would then send the packet toward the final destination using its local interface (192.168.10.10).

Figure A6-3 highlights the matched route.

Figure A6-3: Routing to a Local Destination



If PC1 wanted to send a packet to a remote host located at 10.10.10.10, it would:

- Consult the IPv4 Route Table.
- Find that there is no exact match for the destination IP address.
- Choose the local default route (0.0.0.0) to reveal that it should forward the packet to the 192.168.10.1 gateway address.
- PC1 then forwards the packet to the gateway for using its local interface (192.168.10.10). The gateway device then determines the next path for the packet to reach the final destination address of 10.10.10.10.

Figure A6-4 highlights the matched route.

Figure A6-4: Routing to a Remote Destination



```

C:\Users\PC1> netstat -r

<Output omitted>
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.10.1    192.168.10.10    25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
192.168.10.0               255.255.255.0   On-link         192.168.10.10    281
192.168.10.10              255.255.255.255 On-link         192.168.10.10    281
192.168.10.255            255.255.255.255 On-link         192.168.10.10    281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         192.168.10.10    281
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         192.168.10.10    281
=====
<Output omitted>

```

Sample IPv6 Host Routing Table

The output of the IPv6 Route Table differs in column headings and format due to the longer IPv6 addresses.

The IPv6 Route Table section displays four columns which identify:

- **If** - Lists the interface numbers from the Interface List section of the **netstat -r** command. The interface numbers correspond to the network capable interface on the host, including Ethernet, Wi-Fi, and Bluetooth adapters.
- **Metric** - Lists the cost of each route to a destination. Lower numbers indicate preferred routes.
- **Network Destination** - Lists the reachable networks.
- **Gateway** - Lists the address used by the local host to forward packets to a remote network destination. On-link indicates that the host is currently connected to it.

For example, the Figure A6-5 displays the IPv6 Route section generated by the **netstat -r** command.

Figure A6-5: IPv6 Host Routing Table

fe80::2c30:3071:e718:a926/128
2001:db8:9d38:953c:2c30:3071:e718:a926/128



```
C:\Users\PC1> netstat -r
<Output omitted>
IPv6 Route Table
=====
Active Routes:
  If Metric Network Destination      Gateway
  16     58  ::/0                                On-link
  1     306  ::1/128                              On-link
  16     58  2001::/32                             On-link
  16    306  2001:0:9d38:953c:2c30:3071:e718:a926/128
                                           On-link
  15   281  fe80::/64                             On-link
  16   306  fe80::/64                             On-link
  16   306  fe80::2c30:3071:e718:a926/128
                                           On-link
  15   281  fe80::b1ee:c4ae:a117:271f/128
                                           On-link
  1     306  ff00::/8                               On-link
  16   306  ff00::/8                               On-link
  15   281  ff00::/8                               On-link
=====
<Output omitted>
```

The figure reveals the following network destinations:

- **::/0** - This is the IPv6 equivalent of the local default route.
- **::1/128** - This is equivalent to the IPv4 loopback address and provides services to the local host.
- **2001::/32** - This is the global unicast network prefix.
- **2001:0:9d38:953c:2c30:3071:e718:a926/128** - This is the global unicast IPv6 address of the local computer.
- **fe80::/64** - This is the local link network route address and represents all computers on the local link IPv6 network.
- **fe80::2c30:3071:e718:a926/128** - This is the link local IPv6 address of the local computer.
- **ff00::/8** - These are special reserved multicast class D addresses equivalent to the IPv4 224.x.x.x addresses.

Note: Interfaces in IPv6 commonly have two IPv6 addresses: a link local address and a global unicast address. Also, notice that there are no broadcast addresses in IPv6. IPv6 addresses will be discussed further in the next chapter.

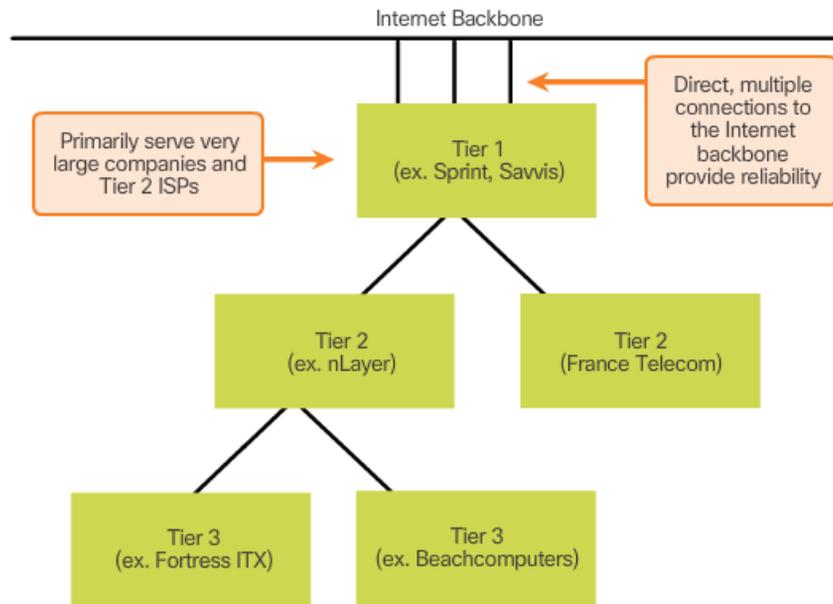
Chapter 7 Appendix

To get access to the services of the Internet, we have to connect our data network to the Internet using an Internet Service Provider (ISP).

ISPs have their own set of internal data networks to manage Internet connectivity and to provide related services. Among the other services that an ISP generally provides to its customers are DNS services, email services, and a website. Depending on the level of service required and available, customers use different tiers of an ISP.

ISPs are designated by a hierarchy based on their level of connectivity to the Internet backbone. Each lower tier obtains connectivity to the backbone via a connection to a higher tier ISP. As shown in Figure A7-1, at the top of the ISP hierarchy are Tier 1 ISPs.

Figure A7-1: Tier 1 ISPs

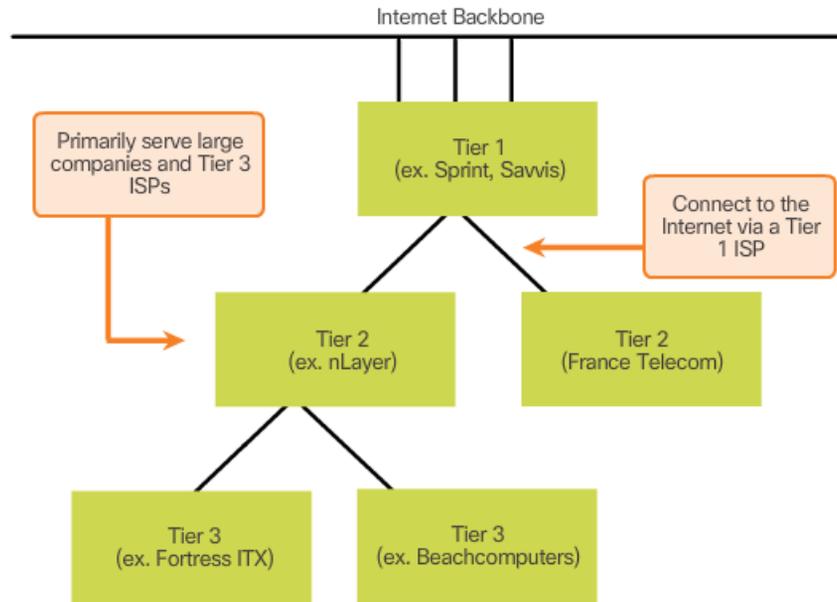


These ISPs are large national or international ISPs that are directly connected to the Internet backbone. The customers of Tier 1 ISPs are either lower-tiered ISPs or large companies and organizations. Because they are at the top of Internet connectivity, they engineer highly reliable connections and services. Among the technologies used to support this reliability are multiple connections to the Internet backbone.

The primary advantages for customers of Tier 1 ISPs are reliability and speed. Because these customers are only one connection away from the Internet, there are fewer opportunities for failures or traffic bottlenecks. The drawback for Tier 1 ISP customers is its high cost.

As shown in Figure A7-2, Tier 2 ISPs acquire their Internet service from Tier 1 ISPs.

Figure A7-2: Tier 2 ISPs

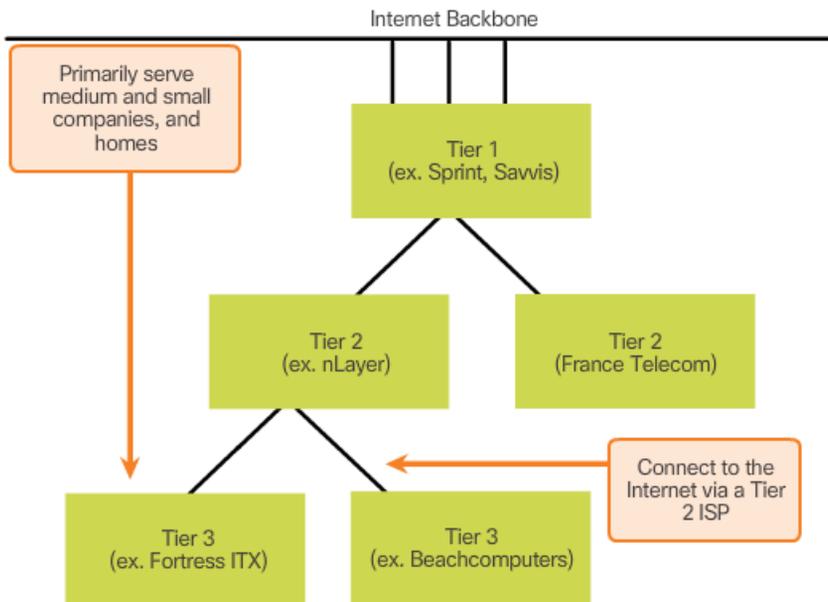


Tier 2 ISPs generally focus on business customers. Tier 2 ISPs usually offer more services than the other two tiers of ISPs. These Tier 2 ISPs tend to have the IT resources to operate their own services such as DNS, email servers, and web servers. Other services that Tier 2 ISPs may offer include website development and maintenance, e-commerce/e-business, and VoIP.

The primary disadvantage of Tier 2 ISPs, as compared to Tier 1 ISPs, is slower Internet access. Because Tier 2 ISPs are at least one more connection away from the Internet backbone, they also tend to have lower reliability than Tier 1 ISPs.

As shown in Figure A7-3, Tier 3 ISPs purchase their Internet service from Tier 2 ISPs.

Figure A7-3: Tier 3 ISPs



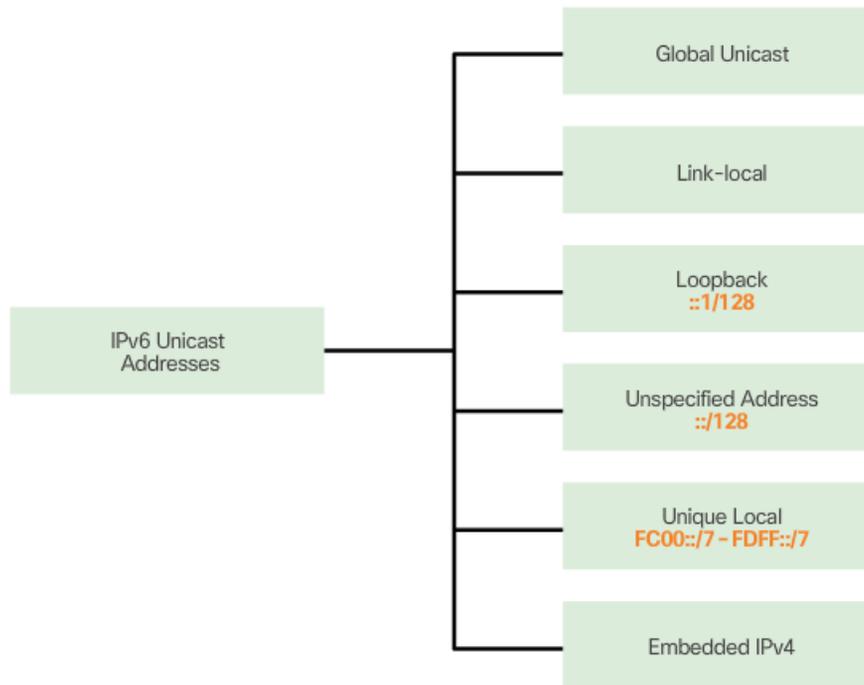
The focus of these ISPs is the retail and home markets in a specific locale. Tier 3 customers typically do not need many of the services required by Tier 2 customers. Their primary need is connectivity and support.

These customers often have little or no computer or network expertise. Tier 3 ISPs often bundle Internet connectivity as a part of network and computer service contracts for their customers. While they may have reduced bandwidth and less reliability than Tier 1 and Tier 2 providers, they are often good choices for small to medium size companies.

Other Types of IPv6 Unicast Addresses

All IPv6 unicast address types are shown in Figure A7-4. Global unicast addresses (GUA), link-local unicast, and unique local unicast address are discussed in the chapter content. Additional types of IPv6 unicast addresses include loopback, unspecified and embedded IPv4.

A7-4: IPv6 Unicast Address Types



Loopback

The loopback address is used by a host to send a packet to itself and cannot be assigned to a physical interface. Similar to an IPv4 loopback address, you can ping an IPv6 loopback address to test the configuration of TCP/IP on the local host. The IPv6 loopback address is all-0s except for the last bit, represented as `::1/128` or just `::1` in the compressed format.

Unspecified address

An unspecified address is an all-0s address represented in the compressed format as `::/128` or just `::` in the compressed format. It cannot be assigned to an interface and is only used as a source address in an IPv6 packet. An unspecified address is used as a source address when the device does not yet have a permanent IPv6 address or when the source of the packet is irrelevant to the destination.

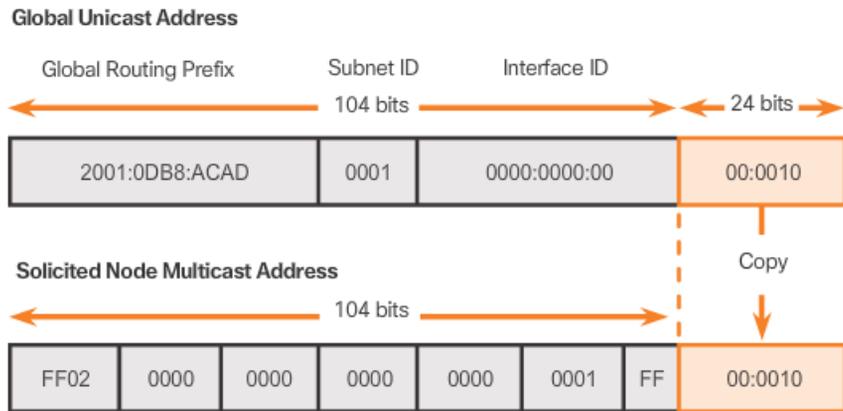
IPv4 embedded

The last type of unicast address type is the IPv4 embedded address. These addresses are used to help transition from IPv4 to IPv6. IPv4 embedded addresses are beyond the scope of this course.

IPv6 Solicited Node Multicast

A solicited-node multicast address is an address that matches only the last 24 bits of the IPv6 global unicast address of a device, as shown in Figure A7-5. The only devices that need to process these packets are those devices that have these same 24 bits in the least significant, far right portion of their Interface ID.

Figure A7-5: IPv6 Solicited Node Multicast Address Structure



IPv6 Global Unicast Address: 2001:0DB8:ACAD:0001:0000:0000:0000:0010

IPv6 Solicited Node Multicast Address: FF02:0:0:0:0:0:0:1:FF00:0010

An IPv6 solicited-node multicast address is automatically created when the global unicast or link-local unicast addresses are assigned. The IPv6 solicited-node multicast address is created by combining a special FF02:0:0:0:0:0:1:FF00::/104 prefix with the far right 24 bits of its unicast address.

The solicited-node multicast address consists of two parts:

- **FF02:0:0:0:0:0:1:FF00::/104 multicast prefix** – This is the first 104 bits of the all solicited-node multicast address.
- **Least significant 24-bits** – These are the last or far right 24 bits of the solicited-node multicast address. These bits are copied from the far right 24 bits of the global unicast or link-local unicast address of the device.

Note: Only 104 bits are taken from the special solicited node prefix. The last byte (00) is not used when creating the solicited node address. It is necessary to include the 00 when referring to the solicited node prefix because the compressed address of ff02:0:0:0:0:0:1:ff/104 is expanded to ff02:0000:0000:0000:0000:0001:00ff/104, which is not the correct prefix.

It is possible that multiple devices will have the same solicited-node multicast address. Although rare, this can occur when devices have the same far right 24 bits in their Interface IDs. This does not create any problems because the device will still process the encapsulated message, which will include the complete IPv6 address of the device in question.

Chapter 8 Appendix

Note: Chapter 8 of the *Introduction to Networks Course Booklet* references additional IPv4 subnetting labs and a Packet Tracer activity that can be found in the appendix. Labs and Packet Tracer activities are not available for the Course Booklet. They are supplemental, not necessary to complete the requirements of the course, and are no longer part of the latest version of the online curriculum.

Subnetting IPv6 into the Interface ID

Similar to borrowing bits from the host portion of an IPv4 address, with IPv6 bits can be borrowed from the interface ID to create additional IPv6 subnets. This is typically done for security reasons to create fewer hosts per subnet and not necessarily to create additional subnets.

When extending the subnet ID by borrowing bits from the interface ID, the best practice is to subnet on a nibble boundary. A nibble is 4 bits or one hexadecimal digit. As shown in the figure, the /64 subnet prefix is extended 4 bits or 1 nibble to /68. Doing this reduces the size of the interface ID by 4 bits, from 64 to 60 bits.

Subnetting on nibble boundaries means only using nibble aligned subnet masks. Starting at /64, the nibble aligned subnet masks are /68, /72, /76, /80, etc.

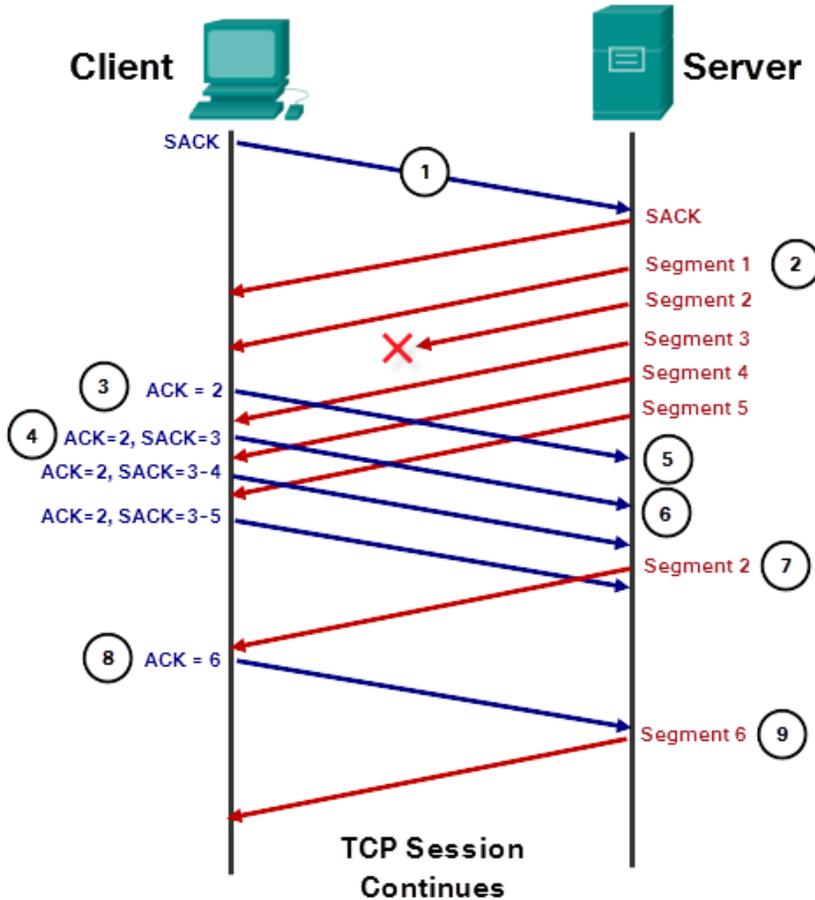
Subnetting on a nibble boundary creates subnets by using the additional hexadecimal value. In the example, the new subnet ID consists of the 5 hexadecimal values, ranging from 00000 through FFFFF.

It is possible to subnet within a nibble boundary, within a hexadecimal digit, but it is not recommended or even necessary. Subnetting within a nibble takes away the advantage easily determining the prefix from the interface ID. For example, if a /66 prefix length is used, the first two bits would be part of the subnet ID and the second two bits would be part of the interface ID.

Chapter 9 Appendix

TCP Selective Acknowledgment

Selective acknowledgment (SACK) is a strategy that corrects the inefficiency of TCP acknowledgments when there are one or more lost segments. SACK is an optional implementation of TCP introduced with [RFC 2018 \(https://tools.ietf.org/html/rfc2018\)](https://tools.ietf.org/html/rfc2018). Support of SACK is negotiated during the establishment of the TCP connection. If both hosts support SACK, then it will be used during the connection. The figure illustrates the use of TCP SACK.



Step 1. Both Client and Server indicate the support of SACK during the establishment of the TCP connection. This occurs as part of the normal three-way handshake process.

Step 2. As part of a larger data stream, the Server sends the first 5 TCP segments to the Client. Segment 2 is lost and never arrives at the Client.

Step 3. The Client receives Segment 1 but has not yet received Segment 2. The Client sends Acknowledgement 2 to the Server indicating that it has received Segment 1 and is still expecting Segment 2.

Step 4. The next segments received by the Client are Segment 3, Segment 4 and Segment 5. This is where SACK comes into effect. The Client sends duplicate acknowledgements for the first segment but this time includes the SACK option to show which segments it has received. The client sends three duplicate acknowledgments, one for each successive segment received, but also letting the Server know it is still expecting Segment 2. Each duplicate acknowledgment includes the SACK option indicating the range of segments the Client has received.

Step 5. The Server receives the acknowledgement that the client has received the Segment 1 and is awaiting Segment 2.

Step 6. The Server receives a duplicate acknowledgment of segment 1, which includes the first acknowledgment with the SACK option. This acknowledgment with the SACK option indicates that the Client has received Segment 3 (SACK=3) but still hasn't received Segment 2 (ACK=2).

Step 7. The server resends Segment 2. The Client receives the other duplicate acknowledgements of Segment 1 with SACK options indicating that the Client has also received Segment 4 and Segment 5. Notice that the Server does not need to resend Segments 3 through 5.

Step 8. The Client receives Segment 2 and now has Segment 1 through Segment 5. The Client sends Acknowledgment 6 to inform the Server that this is the next segment it is expecting.

Step 9. The Server sends Segment 6 and any other segments in the transmission queue. Depending on the window size of the Client, the Server could have sent Segment 6 and additional segments prior to receiving the acknowledgement.

Chapter 11 Appendix

More on AAA

Authentication

Users and administrators must prove that they are who they say they are. Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods. For example: "I am user 'student'. I know the password to prove that I am user 'student'."

In a small network, local authentication is often used. With local authentication, each device maintains its own database of username/password combinations. However, when there are more than a few user accounts in a local device database, managing those user accounts becomes complex. Additionally, as the network grows and more devices are added to the network, local authentication becomes difficult to maintain and does not scale. For example, if there are 100 network devices, all user accounts must be added to all 100 devices.

For larger networks, a more scalable solution is external authentication. External authentication allows all users to be authenticated through an external network server. The two most popular options for external authentication of users are RADIUS and TACACS+:

- RADIUS is an open standard with low use of CPU resources and memory. It is used by a range of network devices, such as switches, routers, and wireless devices.
- TACACS+ is a security mechanism that enables modular authentication, authorization, and accounting services. It uses a TACACS+ daemon running on a security server.

Authorization

After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. An example is, "User 'student' can access host serverXYZ using Telnet only."

Accounting

Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made. Accounting keeps track of how network resources are used. An example is, "User 'student' accessed host serverXYZ using Telnet for 15 minutes."

Home and Small Office Routers

Although the skills required to implement Wireless LANs (WLANs) are not currently part of the CCNA Routing and Switching exams, the following content is provided as a resource for students who wish to explore this topic.

Multi-Function Device

The use of networking is not limited to small businesses and large organizations. Another environment that is increasingly taking advantage of networking technology is the home. Home networks are being used to provide connectivity and Internet sharing among multiple personal computers systems and laptops throughout the house. They also allow individuals to take advantage of various services such as print sharing to a network printer, centralized storage of photos, music, and movies on a network attached storage (NAS) appliance; as well as allowing other end user devices, such as tablet computers, cell phones, and even home appliances, such as a television, to have access to Internet services.

A home network is very similar to a small-business network. However, most home networks, and many small business networks, do not require high-volume devices, such as dedicated routers and switches. Smaller scale devices, as long as they provide the same functionality of routing and switching, are all that are required. For this reason, many home and small business networks utilize the service of a multi-function device.

For the purpose of this course, multi-function devices will be referred to as integrated routers.

An integrated router is like having several different devices connected together. For example, the connection between the switch and the router still occurs, but it occurs internally. When a packet is forwarded from one device to another on the same local network, the integrated switch will automatically forward the packet to the destination device. If a packet is forwarded to a device on a remote network, however, the integrated switch will then forward the packet to the internal router connection. The internal router will then determine the best path and forward the packet out accordingly.

Most integrated routers offer both wired switching capabilities and wireless connectivity, and serve as the access point (AP) in the wireless network, as shown in Figure 1. Wireless connectivity is a popular, flexible, and cost-effective way for homes, and businesses alike, to provide network services to end devices.

Figure 1: Multi-Function Device

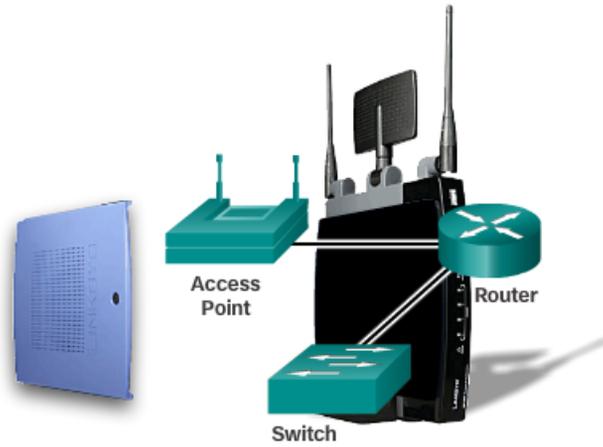


Table 1 lists some common advantages and limitations for using wireless.

Table 1: Wireless Advantages and Limitations

Advantages	Limitations
Mobility - allows for easy connection of both stationary and mobile clients	Interference - Wireless technology is susceptible to interference from other devices that produce electromagnetic energies. This includes: cordless phones, microwaves, televisions, and other wireless LAN implementations.
Scalability - can be easily expanded to allow more users to connect and to increase the coverage area	Network and Data security - Wireless LAN technology is designed to provide access to the data being transmitted, not security of the data. Additionally, it can provide an unprotected entrance into the wired network.
Flexibility - provides anytime, anywhere connectivity	Technology - Wireless LAN technology continues to evolve. Wireless LAN technology does not currently provide the speed or reliability of wired LANs.
Cost Savings - equipment costs continue to fall as the technology matures	Reliability in harsh environments - easy to install in emergency and hostile environments
Reduced installation time - installation of a single piece of equipment can provide connectivity for a large number of people	

In addition to supporting routing, switching and wireless connectivity, many additional features may be available on an integrated router, including: DHCP service, a firewall, and even network attached storage services.

Types of Integrated Routers

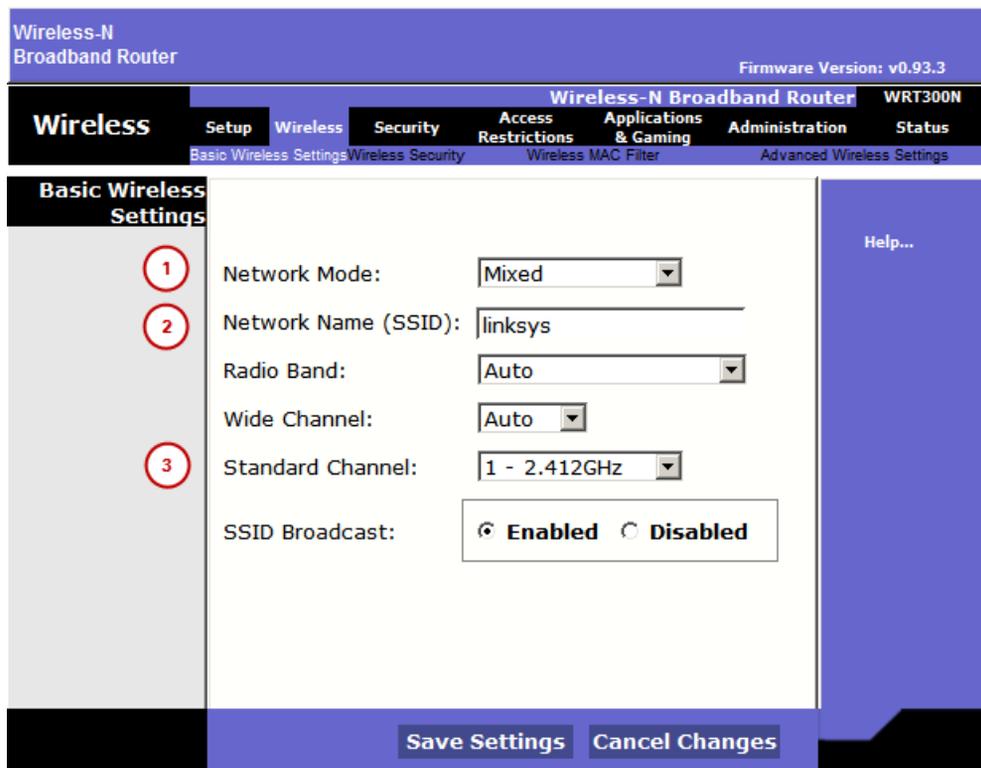
Integrated routers can range from small devices designed for home office and small business applications to more powerful devices that can support enterprise branch offices.

All integrated routers allow for basic configuration settings such as passwords, IP addresses, and DHCP settings, which are the same whether the device is being used to connect wired or wireless hosts. However, if using the wireless functionality, additional configuration parameters are required, such as setting the wireless mode, SSID, and the wireless channel.

Wireless Capability

Figure 2 shows the basic wireless setting interface for the wireless router in Packet Tracer. The numbered settings in the figure are discussed below.

Figure 2: Basic Wireless Settings Interface



Wireless Mode

The wireless mode refers to setting the IEEE 802.11 wireless standard that the network will use. There are four amendments to the IEEE 802.11 standard that describe different characteristics for wireless communications; they are 802.11a, 802.11b, 802.11g, and 802.11n. In Figure 2, the

Most integrated wireless routers support 802.11b, 802.11g, and 802.11n. The three technologies are compatible, but all devices on the network must operate at the same standard common to all devices. For example, at number 1 in Figure 2 the wireless mode (or network mode) is set to "Mixed". If an 802.11n router is connected to a laptop with 802.11n, the network would function as an 802.11n standard. However, add an 802.11b wireless printer to the network. Both the router and the laptop will revert to using the slower 802.11b standard for all communications. Therefore, keeping older wireless devices on the network will make the entire network slow down. It is important to keep that in mind when deciding whether or not to keep older wireless devices.

Service Set Identifier (SSID)

There may be many other wireless networks in your area. It is important that the wireless devices connect to the correct WLAN. This is done using a Service Set Identifier (SSID). At number 2 in Figure 2, the SSID is currently set to "linksys". This should be changed to an appropriate name for the WLAN.

The SSID is a case-sensitive, alpha-numeric name for your home wireless network. The name can be up to 32-characters in length. The SSID is used to tell wireless devices which WLAN they belong to and with which other devices they can communicate. Regardless of the type of WLAN installation, all wireless devices in a WLAN must be configured with the same SSID in order to communicate. If SSID broadcast is disabled, then devices must be manually configured with the SSID.

Wireless Channel

Channels are created by dividing up the available radio frequency spectrum. Each channel is capable of carrying a different conversation. This is similar to the way that multiple television channels are transmitted across a single medium. Multiple APs can function in close proximity to one another as long as they use different channels for communication. The channel at number 3 in Figure 2 is currently set to channel 1 of the 2.4GHz frequency.

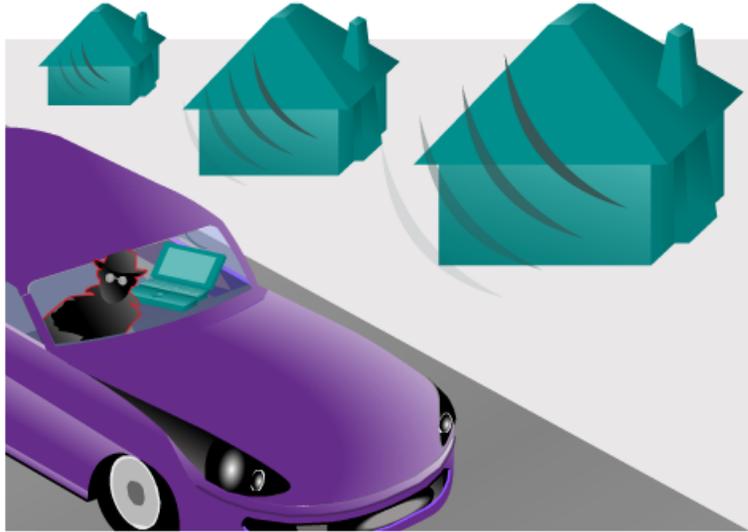
Basic Security of Wireless

Security measures should also be planned and configured before connecting the AP to the network or ISP. Basic security measures include:

- Change default values for the SSID, usernames, and passwords
- Disable broadcast SSID
- Configure encryption using WEP or WPA

Encryption is the process of transforming data so that even if it is intercepted it is unusable. These basic measures help prevent others from connecting to the WLAN, as shown in Figure 3.

Figure 3: Wardriving Attacker



Wardriving is the process of driving around an area searching for wireless LANs. Once discovered, the location of the WLAN is logged and shared. The goal of wardriving is to bring attention to the fact that most wireless networks are insecure and also to show the widespread acceptance and use of wireless LAN technology.

A similar process to wardriving is known as warwalking where the person walks around an area to discover wireless access. Once access is discovered a chalk mark is placed in front of the location to indicate the status of the wireless connection.

Wired Equivalency Protocol (WEP)

WEP is an advanced security feature that encrypts network traffic as it travels through the air. WEP uses pre-configured keys to encrypt and decrypt data.

A WEP key is entered as a string of numbers and letters and is generally 64 bits or 128 bits long. In some cases, WEP supports 256 bit keys as well. To simplify creating and entering these keys, many devices include a Passphrase option. The passphrase is an easy way to remember the word or phrase used to automatically generate a key.

In order for WEP to function, the AP, as well as every wireless device allowed to access the network must have the same WEP key entered. Without this key, devices will not be able to understand the wireless transmissions.

There are weaknesses within WEP, including the use of a static key on all WEP enabled devices. There are applications available to attackers that can be used to discover the WEP key. These applications are readily available on the Internet. Once the attacker has extracted the key, they have complete access to all transmitted information.

One way to overcome this vulnerability is to change the key frequently. Another way is to use a more advanced and secure form of encryption known as Wi-Fi Protected Access (WPA).

Wi-Fi Protected Access (WPA)

WPA also uses encryption keys from 64 bits up to 256 bits. However, WPA, unlike WEP, generates new, dynamic keys each time a client establishes a connection with the AP. For this reason, WPA is considered more secure than WEP because it is significantly more difficult to crack.

There are several other security implementations that can be configured on a wireless AP, including MAC address filtering, authentication, and traffic filtering. You can investigate these settings on the wireless router in Packet Tracer.