

This chapter covers the following topics that you will need to master for the CCNP Switching exam:

- **Desktop Connectivity with Ethernet**—This section covers the Ethernet, Fast Ethernet, and Gigabit Ethernet network media technologies.
- **Desktop Connectivity with Token Ring**—The Token Ring LAN media is discussed in detail, along with its use in switched networks.
- **Connecting Switches**—This section discusses the physical cabling and connectivity used with Catalyst switches, including console, Ethernet, and Token Ring interfaces.
- **Switch Management**—This section presents the basic Catalyst switch configuration and administration commands. In addition, this section also covers techniques for interswitch communication.
- **Switch Port Configuration**—This section covers the switch commands that can be used to configure a LAN port for use.

# Basic Switch and Port Configuration

---

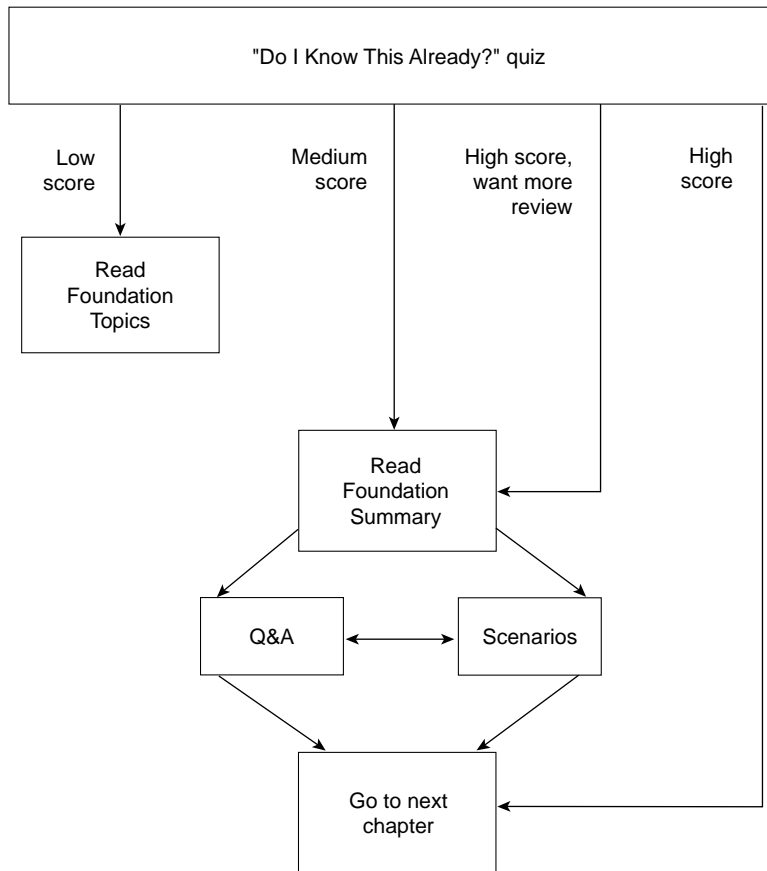
Chapter 2, “Campus Network Design Models,” dealt with the logical processes that can be used to design a campus network. Connections between switch blocks were discussed, such that traffic could be efficiently transported across the campus. Single connections, load balancing, and redundant paths were used to connect switches in modular blocks for complete connectivity. However, these paths were only functional paths—no specifics were presented about how much traffic could be handled, or what physical capabilities were supported. These topics become important when you begin to size traffic loads and actually connect Cisco switch devices.

This chapter presents the various “desktop” network technologies that can be used to establish switched connections within the campus network. As well, you will learn about switch management and the administration commands required to successfully manage switches. Finally, the chapter details the switch commands required for configuring desktop LAN ports.

## How to Best Use This Chapter

By taking the following steps, you can make better use of your study time:

- Keep your notes and the answers for all your work with this book in one place for easy reference.
- Take the “Do I Know This Already?” quiz, and write down facts and concepts, even if you never look at the information again.
- Use the diagram in Figure 3-1 to guide you to the next step.

**Figure 3-1** *How to Use This Chapter*

## “Do I Know This Already?” Quiz

The purpose of the “Do I Know This Already?” quiz is to help you decide what parts of this chapter to use. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The quiz helps you make good choices of how to spend your limited study time. The quiz is sectioned into five smaller “quizlets,” which correspond to the five major headings in the Foundation Topics section of the chapter. Although your answer may differ somewhat from the answers given, finding out if you have the basic understanding of what is presented in this chapter is more important. You will find that these questions are open-ended, rather than multiple choice as found on the exams. Thus, you can focus more on understanding the subject matter than on memorizing details.

Use the scoresheet in Table 3-1 to record your score.

**Table 3-1** *Scoresheet for Quiz and Quizlets*

Quizlet Number	Foundation Topics Sections Covering These Questions	Questions	Score
1	Desktop Connectivity with Ethernet	1–6	
2	Desktop Connectivity with Token Ring	7–8	
3	Connecting Switches	9	
4	Switch Management	10–12	
5	Switch Port Configuration	13–14	
All questions		1–14	

**1** What are the different Ethernet technologies and their associated IEEE standards?

---



---



---

**2** What benefits result with switched Ethernet over shared Ethernet?

---



---



---

**3** At what layer are traditional 10 Mbps Ethernet, Fast Ethernet, and Gigabit Ethernet different?

---



---



---

**4** Describe Cisco’s EtherChannel technology.

---



---



---

5 In a campus network, where is Fast Ethernet typically used? Where is Gigabit Ethernet typically used?

---

---

---

6 What is the maximum length of a Category 5 100BaseTX cable?

---

---

---

7 Name a type of Token Ring segmentation.

---

---

---

8 What part of a Token Ring frame specifies the exact path the frame should take to reach its destination?

---

---

---

9 What is the purpose of a Gigabit Interface Converter (GBIC)?

---

---

---

10 What must be done to a switch before Telnet access is allowed?

---

---

---

- 11 What type of user interface or command set does the Catalyst 5000 family of switches support? What type is the Catalyst 3500XL?

---

---

---

- 12 What protocol is used by a Catalyst switch to learn about neighboring routers and switches?

---

---

---

- 13 What port speeds can be assigned to a Fast Ethernet switch port?

---

---

---

- 14 What port speeds can be assigned to a Token Ring switch port?

---

---

---

The answers to the quiz are found in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Sections,” on page 477. The suggested choices for your next step are as follows:

- **7 or less overall score**—Read the entire chapter. The sections include the “Foundation Topics” and “Foundation Summary”, plus the Q&A section at the end of the chapter.
- **8–10 overall score**—Begin with the “Foundation Summary” section, and then go to the Q&A section at the end of the chapter.
- **11 or more overall score**—If you want more review on these topics, skip to the “Foundation Summary” section and then go to the Q&A section at the end of the chapter. Otherwise, move to the next chapter.

## Foundation Topics

### Desktop Connectivity with Ethernet

This section provides a review of the various “flavors” of Ethernet and their application in a campus network. Recall how the bandwidth requirements for each segment of the network are determined by the types of applications in use, the traffic flows within the network, and the size of the user community served. Ethernet scales to support increasing bandwidths, and should be chosen to match the need at each point in the campus network. As network bandwidth requirements grow, the links between access, distribution, and core layers can be scaled to match the load.

Other network media technologies available include Fiber Distribution Data Interface (FDDI), Copper Distribution Data Interface (CDDI), Token Ring, and Asynchronous Transfer Mode (ATM). Although these media are commonly used, Ethernet is emerging as the most popular choice in installed networks. Ethernet is chosen because of its low cost, availability, and scalability to higher bandwidths. Token Ring is discussed later in this chapter, while ATM is covered in Chapter 6, “Trunking with ATM LANE.”

### Ethernet

Ethernet is a LAN technology based on the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard. Ethernet offers a bandwidth of 10 Mbps between end users. In its most basic form, Ethernet is a shared media that becomes both a collision and a broadcast domain. As the number of users on the shared media increases, so does the probability that a user is trying to transmit data at any given time. Ethernet is based on the carrier sense multiple access collision detect (CSMA/CD) technology, which requires that transmitting stations back off for a random period of time when a collision occurs. The more crowded an Ethernet segment becomes, the less efficient it becomes.

Ethernet switching addresses this problem by dynamically allocating a dedicated 10 Mbps bandwidth to each of its ports. The resulting increased network performance occurs by reducing the number of users connected to an Ethernet segment.

Although the principle of switched Ethernet is to offer full dedicated bandwidth to each connected device, assuming that network performance will improve across the board when switching is introduced is a common mistake. For example, consider a workgroup of users connected by a shared media Ethernet hub. These users regularly access an enterprise server located elsewhere in the campus network. To improve performance, the decision is made to replace the hub with an Ethernet switch so that all users get dedicated 10 Mbps connections. Because the switch offers dedicated bandwidth for connections between the end user devices connected to their ports, any user-to-user traffic would probably see improved performance. However, the enterprise server is still located elsewhere in the network, and all of the switched

users must still share available bandwidth across the campus to reach it. As discussed in Chapter 2, rather than throwing raw bandwidth at a problem, a design based on careful observation of traffic patterns and flows will offer a better solution.

Because switched Ethernet can remove the possibility of collisions, stations do not have to listen to each other in order to take a turn transmitting on the wire. Instead, stations can operate in *full-duplex* mode—transmitting and receiving simultaneously. Full-duplex mode further increases network performance, with a net throughput of 10 Mbps in each direction, or 20 Mbps total on each port.

Ethernet cabling involves the use of unshielded twisted-pair (UTP) wiring (10BaseT Ethernet), usually restricted to an end-to-end distance of 100 meters (328 feet) between active devices. Keeping cable lengths as short as possible in the wiring closet will also reduce noise and crosstalk when many cables are bundled together.

In a campus network environment, Ethernet is usually used in the access layer, between end user devices and the access layer switch. Many networks still use Ethernet to connect end users to shared media hubs, which then connect to access layer switches. Ethernet is not typically used at either the distribution or core layer.

---

**NOTE**

Other cabling technologies are used in Ethernet applications (10Base2, 10Base5, 10BaseF, and so on) though they are not discussed here. For the most part, 10BaseT with UTP wiring is the most commonly used. A useful web site for further reading about Ethernet technology is Charles Spurgeon's Ethernet Web Site, at [wwwhost.ots.utexas.edu/ethernet/](http://wwwhost.ots.utexas.edu/ethernet/)

---

## Fast Ethernet

Rather than require campuses to invest in a completely new technology to gain increased bandwidth, the networking industry developed a higher-speed Ethernet based on the existing Ethernet standards. Fast Ethernet operates at 100 Mbps and is based on the IEEE 802.3u standard. The Ethernet cabling schemes, CSMA/CD operation, and all upper-layer protocol operations have been maintained with Fast Ethernet. The net result is the same data link Media Access Control (MAC) layer merged with a new physical layer.

In the campus network, Fast Ethernet can be used to link access and distribution layer switches. The larger bandwidth can support the aggregate traffic from multiple Ethernet segments in the access layer. Fast Ethernet can also be used to connect distribution layer switches to the core, with either single or multiple redundant links. It can also be used to connect faster end user workstations to the access layer switch, and to provide improved connectivity to enterprise servers. In other words, Fast Ethernet can be successfully deployed at all layers within a campus network.

Cabling for Fast Ethernet can involve either UTP or fiber. Specifications for Fast Ethernet define the media types and distances as shown in Table 3-2.



**Table 3-2** *Cabling Specifications for Fast Ethernet*

<b>Technology</b>	<b>Wiring Type</b>	<b>Pairs</b>	<b>Cable Length</b>
100BaseTX	EIA/TIA Category 5 UTP	2	100 m
100BaseT2	EIA/TIA Category 3,4,5 UTP	2	100 m
100BaseT4	EIA/TIA Category 3,4,5 UTP	4	100 m
100BaseFX	Multimode fiber (MMF) 62.5 micron core, 125 micron outer cladding (62.5/125)	1	400 m half duplex or 2000 m full duplex
	Single-mode fiber (SMF)	1	10 km

## Full-Duplex Fast Ethernet

As with traditional Ethernet, the natural progression to improve performance is to use full-duplex operation. Fast Ethernet can provide 100 Mbps in each direction on a switched connection, for 200 Mbps total throughput. This throughput is only possible when a workstation or server is directly connected to a switch port, or when two switches directly connect to each other.

The Fast Ethernet specification also offers backward compatibility to support traditional 10 Mbps Ethernet. To provide this support, two devices at each end of a network connection can automatically negotiate link capabilities so that they both can operate at a maximum common level. This negotiation involves the detection and selection of the highest physical layer technology (available bandwidth) and half-duplex or full-duplex operation. Even if one of the devices uses a fixed configuration, the other device can detect this and match the capabilities.

Autonegotiation uses the priorities shown in Table 3-3 for each mode of Ethernet to determine which technology to agree upon. If both devices can support more than one technology, then the technology with the highest priority will be used. For example, if two devices can support both 10BaseT and 100BaseTX, both devices will use the higher priority 100BaseTX mode.

**Table 3-3** *Autonegotiation Selection Priorities*

<b>Priority</b>	<b>Ethernet Mode</b>
7	100BaseT2 (full duplex)
6	100BaseT2 (half duplex)
5	100BaseTX (full duplex)
4	100BaseT4
3	100BaseTX
2	10BaseT (full duplex)
1	10BaseT

**NOTE**

To assure proper configuration at both ends of a link, Cisco recommends that the appropriate values for transmission speed and duplex mode be manually configured on switch ports.

Cisco provides one additional capability to Fast Ethernet, which allows several Fast Ethernet links to be bundled together for increased throughput. *Fast EtherChannel (FEC)* allows two to eight full-duplex Fast Ethernet links to act as a single physical link, for 400- to 1600-Mbps bandwidth. This technology is described in greater detail in Chapter 5, “Redundant Switch Links.”

For further reading about Fast Ethernet technology, refer to Cisco’s web site: [www.cisco.com/warp/public/cc/so/neso/lnso/lnmnsso/feth\\_tc.htm](http://www.cisco.com/warp/public/cc/so/neso/lnso/lnmnsso/feth_tc.htm)

---

## Gigabit Ethernet

Fast Ethernet can be scaled by an additional order of magnitude with the use of Gigabit Ethernet (which supports 1,000 Mbps or 1 Gbps) using the same IEEE 802.3 Ethernet frame format as before. This scalability allows network designers and managers to leverage existing knowledge and technologies to install, migrate, manage, and maintain Gigabit Ethernet networks.

However, the physical layer has been modified to increase data transmission speeds. Two technologies were merged together to gain the benefits of each: The IEEE 802.3 Ethernet standard and the American National Standards Institute (ANSI) X3T11 FibreChannel. IEEE 802.3 provided the foundation of frame format, CSMA/CD, full duplex, and other characteristics of Ethernet. FibreChannel provided a base of high-speed ASICs, optical components, and encoding/decoding and serialization mechanisms. The resulting protocol is termed *IEEE 802.3z Gigabit Ethernet*.

Gigabit Ethernet supports several cabling types, referred to as *1000BaseX*. Table 3-4 lists the cabling specifications for each type.

In a campus network, Gigabit Ethernet can be used in the switch block, the core block, and in the server block. In the switch block, it is used to connect access layer switches to distribution layer switches. In the core, it connects the distribution layer to the core switches, and also interconnects the core devices. For a server block, a Gigabit Ethernet switch in the server block can provide high-speed connections to individual servers.

**Table 3-4** *Gigabit Ethernet Cabling and Distance Limitations*

GE Type	Wiring Type	Pairs	Cable Length
1000BaseCX	Shielded Twisted Pair (STP)	1	25 m
1000BaseT	EIA/TIA Category 5 UTP	4	100 m
1000BaseSX	Multimode fiber (MMF) with 62.5 micron core; 850 nm laser	1	275 m
	MMF with 50 micron core; 1300 nm laser	1	550 m
1000BaseLX/LH	MMF with 62.5 micron core; 1300 nm laser	1	550 m
	Single-mode fiber (SMF) with 50 micron core; 1300 nm laser	1	550 m
	SMF with 9 micron core; 1300 nm laser	1	10 km
1000BaseZX	SMF with 9 micron core; 1550 nm laser	1	70 km
	SMF with 8 micron core; 1550 nm laser	1	100 km

Finally, Cisco has extended the concept of Fast EtherChannel to bundle several Gigabit Ethernet links to act as a single physical connection. *Gigabit EtherChannel (GEC)* allows two to eight full-duplex Gigabit Ethernet connections to be aggregated, for up to 16 Gbps throughput. Port aggregation and the EtherChannel technology are described further in Chapter 5.

---

**NOTE** The Gigabit Ethernet Alliance offers further reading about Gigabit Ethernet, and its operation, migration, and standards. Refer to the web site: [www.gigabit-ethernet.org](http://www.gigabit-ethernet.org)

---

## Desktop Connectivity with Token Ring

Token Ring is also a LAN technology that provides shared media access to many connected stations. Rather than sharing a common bus or “wire” as Ethernet does, Token Ring stations are arranged in a ring, in a daisy-chain fashion. A token is passed from station to station around the ring, giving the current token holder permission to transmit a frame onto the ring. Once the frame is sent, it is passed around the ring until it is received again by the source. The sending station is responsible for removing the frame from the ring and for introducing a new token to the next neighboring station.

Notice that only one station can transmit at a given time—the one with the token. This restriction prevents a Token Ring network from ever becoming a collision domain. Stations can expect to receive the token at regular intervals as it circulates the ring. This feature makes Token Ring deterministic and useful for delay sensitive protocols. Frames can be sent to a broadcast

MAC address, like Ethernet, causing all stations on the ring to listen. Therefore, a token ring is a broadcast domain.

A Token Ring network offers a bandwidth of 4 Mbps or 16 Mbps. At the higher rate, stations are allowed to introduce a new token as soon as they finish transmitting a frame. This *early token release* increases efficiency by letting more than one station transmit a frame during the original token's round trip. One station is elected to be the *ring monitor*, to provide recovery from runaway frames or tokens. The ring monitor will remove frames that have circled the ring once, if no other station removes them.

Traditional Token Ring networks use *multistation access units (MSAUs)* to provide connectivity between end user stations. MSAUs have several ports that a station can connect to, with either a *B connector* for Type 2 cabling or an *RJ-45 connector* for Category 5 UTP cabling. Internally, the MSAU provides station-to-station connections to form a ring segment. The *Ring-In* and *Ring-Out* connectors of a MSAU can be chained to other MSAUs to form a complete ring topology.

## Token Ring Bridging

To form larger networks, Token Rings are interconnected with bridges. Although a *transparent bridge* (or one that forwards frames based solely on MAC addresses) can be used, IBM designed and introduced Token Ring differently. *Source-route bridges* are used to forward frames between rings, based on a predetermined path. The source station includes the exact ring-and-bridge path within the frame so that specific bridges will forward the frame to the appropriate rings. Rings must be uniquely numbered and identified with the campus network, with a number between 1 and 4095. Bridges, however, do not have to be unique across the network, as long as two bridges with the same number do not connect to the same ring. Bridges are numbered 1 through 15.

The steps to determine the path a frame should take are as follows:

- Step 1** The source station first sends a test frame to see if the destination is on the local ring. If the destination responds, the source knows that it is local. If there is no response, the source station will send an *all routes explorer (ARE)* frame, which will cause all bridges to forward the frame to all rings.
- Step 2** Within the frame is a *routing information field (RIF)*. The RIF carries a record of bridges and rings traversed along the way. As the frame is forwarded, each bridge will append its bridge number and the next ring number to the RIF in the frame.
- Step 3** The destination will then reply to each ARE frame it receives, so that the source will receive a confirmation of every possible path to the destination.

For future transmissions, the source can choose the path it thinks is best (quickest response, least number of bridge hops, largest maximum transmission unit (MTU), combination of factors, and so forth). These frames will contain the exact path desired by the source station, in the form of a RIF.

In certain scenarios, hybrid bridging can be provided. Sometimes, both *source-route bridging* (SRB) and transparent bridging must occur. Here, *source-route transparent bridging* (SRT) forwards a frame according to a RIF, if present, or according to MAC address tables if it finds no RIF.

As in Ethernet switching, Token Rings can also be segmented by dividing a ring across several switch ports. While this feature increases the available bandwidth on a ring segment, it requires more in-depth forwarding decisions. Token ring switching, or more properly termed *source-route switching*, forwards frames according to a combination of MAC addresses and RIF contents.

Source-route switching differs from other forms of bridging in that it only looks at the RIF and never updates or adds to the RIF. Instead, the switch learns *route descriptors*, or the ring/bridge combinations that specify the next-hop destinations from incoming frames. The source-route switch then associates the route descriptors and MAC addresses (if needed) with outbound ports closest to the destination. When subsequent frames are received on other ports, the route descriptor is quickly indexed to lookup the outbound port.

In this fashion, source-route switching supports parallel source-route paths to destinations. The number of MAC addresses to be learned is lessened, because route descriptors point to the next-hop ports. The actual operation of source-route switching is much like virtual LANs with Ethernet. For this reason, further discussion of source-route switching is presented in Chapter 4, “VLANs and Trunking.”

Table 3-5 summarizes the attributes of each type of Token Ring connectivity and segmentation method.

**Table 3-5** *Token Ring Segmentation Methods*

<b>Method</b>	<b>Forwarding Decision</b>	<b>Frame Modification</b>	<b>Ring Numbering</b>
Transparent bridging	MAC address		N/A
Source-route bridging	RIF	RIF	Ring numbers must be unique among bridge ports.
Source-route transparent bridging	MAC address or RIF	RIF	Ring numbers must be unique among bridge ports.
Source-route switching	Route descriptor		Ring numbers can be same across switch ports (single ring can be segmented on several ports).

## Connecting Switches

Switch deployment in a network involves two steps: physical connectivity and switch configuration. This section describes the connections and cabling requirements for devices in a switch block. Cable connections must be made to the console port of a switch in order to make initial configurations. Physical connectivity between switches and end users involves cabling for the various types of LAN ports.

### Console Port Cables/Connectors

A terminal emulation program on a PC is usually required to interface with the console port on a switch. Various types of console cables and console connectors are associated with each Cisco switch family.

All Catalyst switch families use an RJ-45-to-RJ-45 *rollover cable* to make the console connection between a PC (or terminal or modem) and the console port. A rollover cable is made so that pin 1 on one RJ-45 connector goes to pin 8 on the other RJ-45 connector, pin 2 goes to pin 7, and so forth. In other words, the cable remains flat while the two RJ-45 connectors point in opposite directions.

To connect the PC end, the rollover cable plugs into an RJ-45 to DB-9 or DB-25 “Terminal” adapter (or a DB-25 “Modem” adapter for a modem connection). At the switch end, the rollover cable plugs directly into the RJ-45 jack of the console port. This situation is true for the Catalyst 1900, 2820, 2900, 3500, 2926G, 2948G, 4912G, 5000 Supervisor IIG/III/IIIG, and the 6000 switches.

On the Catalyst 4003, 5000 Supervisor I/II, and the 8500 switches, the rollover cable must connect to an RJ-45 to DB-25 “Modem” adapter. These switches have a DB-25 console port connector that is a female DCE.

Once the console port is cabled to the PC, terminal, or modem, a terminal emulation program can be started or a user connection can be made. The console ports on all switch families require an asynchronous serial connection at 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

### Ethernet Port Cables/Connectors

Catalyst switches support a variety of network connections, including all forms of Ethernet. In addition, Catalyst switches support several types of cabling, including UTP and optical fiber.

On Catalyst 1900 and 2820 series switches, the Ethernet ports are fixed-speed with 12 or 24 10BaseT and one or two 100BaseTX or 100BaseFX ports. The 10BaseT ports can be connected only to other 10BaseT-capable devices (including 10/100 autosensing devices), and the 100BaseX to other 100BaseX-capable devices. The 10BaseT and 100BaseTX ports use Category 5 UTP cabling and RJ-45 connectors.

The 100BaseFX ports use two-strand multimode fiber (MMF) with SC connectors to provide connectivity. The SC connectors on the fiber cables are square in shape. These connectors snap in and out of the switch port connector as the connector is pushed in or pulled out. One fiber strand is used as a transmit path and the other as a receive path. Therefore, the transmit fiber on one switch device should connect to the receive fiber on the other end.

The remainder of the Catalyst switch families support 10/100 autosensing (using Fast Ethernet autonegotiation) and Gigabit Ethernet. Switched 10/100 ports use RJ-45 connectors on Category 5 UTP cabling to complete the connections. These ports can be connected to other 10BaseT, 100BaseTX, or 10/100 autosensing devices. UTP cabling is arranged so that RJ-45 pins 1,2 and 3,6 form two twisted pairs. These pairs are connected straight through to the far end.

In order to connect two 10/100 switch ports back-to-back, as in an access layer to distribution layer link, a Category 5 UTP *crossover cable* must be used. In this case, RJ-45 pins 1,2 and 3,6 are still twisted pairs, but 1,2 on one end connect to 3,6 on the other end, and 3,6 on one end connect to 1,2 on the other end.

---

**NOTE**

Because UTP Ethernet connections use only pairs 1,2 and 3,6, some cable plant installers only connect these pairs and leave the remaining two pair positions empty. While this move provides Ethernet connectivity, it is not good practice for future needs. Instead, all four pairs of the RJ-45 connector should be connected end-to-end. For example, a full four-pair UTP cable plant can be used for either Ethernet or Token Ring connectivity, without rewiring. (Token Ring UTP connections use pairs 3,6 and 4,5.) Also, to be compatible with the new IEEE 802.3ab standard for Gigabit Ethernet over copper, all four pairs must be used end-to-end.

---

## Gigabit Ethernet Port Cables/Connectors

Gigabit Ethernet connections take a different approach by providing modular connectivity options. Catalyst switches with Gigabit Ethernet ports have standardized rectangular openings that accept Gigabit Interface Converters (GBICs). GBIC modules provide the media personality for the port so that various types of cables can be connected. In this way, the switch chassis is completely modular and requires no major change to accept a new media type. Instead, the appropriate GBIC module is hot-swappable and is plugged into the switch to support the new media. GBICs are available for the following Gigabit Ethernet media:

- **1000BaseSX GBIC**—short wavelength connectivity using SC fiber connectors and MMF for distances up to 550 meters (1804 feet).
- **1000BaseLX/LH GBIC**—long wavelength/long haul connectivity using SC fiber connectors and either MMF or single-mode fiber (SMF); MMF can be used for distances up to 550 meters (1804 feet) and SMF can be used for distances up to 10 km (32,810 feet).

- **1000BaseZX GBIC**—extended distance connectivity using SC fiber connectors and SMF; can be used for distances up to 70 km and even to 100 km when used with premium grade SMF.
- **GigaStack GBIC**—uses a proprietary connector with a high-data-rate copper cable with enhanced signal integrity and electromagnetic interference (EMI) performance; provides a GBIC-to-GBIC connection between stacking Catalyst switches or between any two Gigabit switch ports over a short distance.

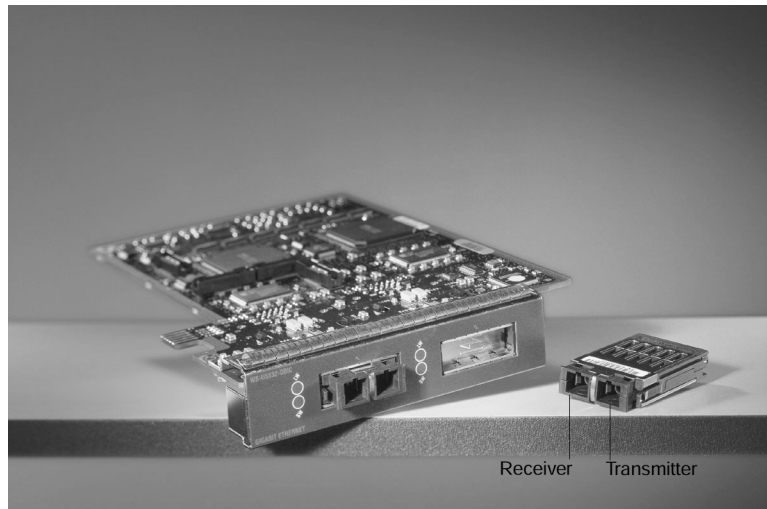
---

**CAUTION** The fiber-based GBICs always have the receive fiber on the left SC connector and the transmit fiber on the right SC connector. These GBICs could produce invisible laser radiation from the transmit SC connector. Therefore, always keep unused SC connectors covered with the rubber plugs and do not look directly into the SC connectors.

---

Figure 3-2 illustrates a fiber-based GBIC module and how one is installed in a Gigabit Ethernet switch port.

**Figure 3-2** *Gigabit Interface Converter*



## Token Ring Port Cables/Connectors

Catalyst switches support UTP Token Ring connections. These ports operate at either 4 or 16 Mbps, in several half and full-duplex modes. RJ-45 connectors on Category 5 UTP cabling use twisted pairs 3,6 and 4,5. These pairs are connected straight through to the far end.



## Switch Management

Cisco Catalyst switch devices can be configured to support many different requirements and features. When a PC is connected to the serial console port, configuration is generally done with a terminal emulator application on the PC. Further configurations can be performed through a Telnet session across the LAN or through a web-based interface. These topics will be covered in later sections.

Catalyst switches support one of two types of user interface for configuration: Cisco IOS-based commands, and **set**-based, command-line interface (CLI) commands. The IOS-based commands (found in Catalyst 1900/2820, 2900XL, and 3500XL) are similar to many IOS commands used on Cisco routers. However, the CLI commands (found in 2926G, 4000, 5000 and 6000) use **set** and **clear** commands to change configuration parameters. Both types of user interface are discussed in the sections that follow.

### Identifying the Switch

All switches come from the factory with a default configuration and a default system name or prompt. This name can be changed so that each switch in a campus network will have a unique identity. This option can be useful when you are using Telnet to move from switch to switch in a network.

### Setting the Hostname/System Name on an IOS-Based Switch

To change the host or system name on an IOS-based user interface, enter the following command in configuration mode:

```
Switch(config)# hostname hostname
```

The hostname is a string of 1 to 255 alphanumeric characters. As soon as this command is executed, the system prompt will change to reflect the new hostname.

---

**NOTE**

Configuration changes made on IOS-based switches apply only to the active *running configuration*, stored in RAM. To make the changes permanent, in effect even after a power cycle, remember to copy the switch configuration into the *startup configuration*, stored in NVRAM. You can do this by using the **copy running-config startup-config** command.

---

### Setting the Hostname/System Name on a CLI-Based Switch

To set the system name on a CLI-based user interface, the system prompt is changed with the following command:

```
Switch(enable) set system name name-string
```

As soon as this command is executed, the system name and the prompt will change to reflect the new value. This prompt is displayed at the beginning of every CLI line.

## Passwords and User Access

Normally, a network device should be configured to secure it from unauthorized access. Catalyst switches offer a simple form of security by setting passwords to restrict who can log in to the user interface. Two levels of user access are available: regular login, or *EXEC mode*, and enable login, or *privileged mode*. EXEC mode is the first level of access, which gives access to the basic user interface through any line or the console port. The privileged mode requires a second password and gives access to set or change switch operating parameters or configurations.

Cisco provides various methods for providing device security and user authentication. Many of these methods are more secure and robust than using the login passwords in Chapter 12, “Controlling Access in the Campus Environment,” describes these features in greater detail.

### Setting Login Passwords on an IOS-Based Switch

To set the login passwords on a Cisco IOS-based switch interface, enter the following commands in global configuration mode:

```
Switch(config)# enable password level 1 password
Switch(config)# enable password level 15 password
```

Here, the EXEC mode password is set with a privilege level of one (1), while the enable password is set with a privilege level of 15. The password is a string of four to eight alphanumeric characters. Passwords on these switches are not case-sensitive.

To remove a password, use the **no enable password level password** command.

### Setting Login Passwords on a CLI-Based Switch

Example 3-1 lists the commands you would enter in enable mode to set the login passwords on a Cisco switch with a CLI-based user interface.

#### Example 3-1 *Setting the Login Passwords on a Cisco Switch*

```
Switch (enable) set password
Enter old password: oldpassword
Enter new password: newpassword
Retype new password: newpassword
Password changed.
Switch (enable) set enablepass
Enter old password: oldenablepassword
Enter new password: newenablepassword
Retype new password: newenablepassword
Password changed.
Switch (enable)
```

As Example 3-1 demonstrates, “**password**” is the EXEC mode password, and the “**enablepass**” is the privileged mode password. Passwords on these switches *are* case-sensitive.

## Remote Access

By default, the switch login passwords allow user access only via the console port. In order to use Telnet to access a switch from within the campus network, to use **ping** to test the reachability of a switch, or to monitor a switch by SNMP, you must perform some configuration for remote access.

Although a switch operates at Layer 2, the switch supervisor processor must maintain an IP stack at Layer 3 for administrative purposes. An IP address and subnet mask can then be assigned to the switch so that remote communications with the switch supervisor are possible.

By default, all ports on a switch are assigned to the same virtual LAN (VLAN) or broadcast domain. The switch supervisor and its IP stack must be assigned to a VLAN before remote Telnet and **ping** sessions will be supported. VLANs are discussed further in Chapter 4.

### Enabling Remote Access on an IOS-Based Switch

On a switch with an IOS-based user interface, an IP address can be assigned to the management VLAN (default is VLAN 1) with the following commands in global configuration mode:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address ip-address netmask
Switch(config-if)# ip default-gateway ip-address
```

As demonstrated by the preceding command syntax, an IP address and subnet mask are assigned to the VLAN1 “interface,” which is really the switch supervisor’s IP stack listening on VLAN1. In order to send packets destined off the local VLAN1 subnet, a default gateway IP address is also assigned.

Again, this default gateway has nothing to do with processing packets that are passed through the switch; rather, the default gateway is only used to forward traffic between a user and the switch supervisor for management purposes.

To view the current switch IP settings, use the **show ip** command.

### Enabling Remote Access on a CLI-Based Switch

An IP address can also be configured for in-band management on a switch with a CLI-based user interface by entering the following commands in privileged mode:

```
Switch(enable) set interface sc0 ip-address netmask broadcast-address
Switch(enable) set interface sc0 vlan
Switch(enable) set ip route default gateway
```

The first command line defines the IP address and subnet mask for the switch management interface, **sc0**. The broadcast address must also be given to match the subnet and subnet mask values. In addition, the management interface is assigned to a specific VLAN with the second command line. If this command is not given, the management interface defaults to VLAN1. The third command line assigns a default gateway that will receive any packets destined off the local management interface subnet.

To view the current IP settings, use the **show interface** command.

## Communicating Between Switches

Because switch devices are usually interconnected, management is usually simplified if the switches can communicate on some level to become aware of each other. Cisco has implemented protocols on its devices so that neighboring Cisco equipment can be found. As well, some families of switch devices can be clustered and managed as a unit once they discover one another.

### Cisco Discovery Protocol

Cisco uses a proprietary protocol on both switches and routers to discover neighboring devices. The Cisco Discovery Protocol (CDP) can be enabled on interfaces to periodically advertise the existence of a device and exchange basic information with directly connected neighbors. The information exchanged in CDP messages includes the device type, links between devices, and the number of ports within each device.

By default, CDP runs on each port of a Cisco switch that is capable of using the SNAP protocol. CDP advertisements occur every 60 seconds by default. CDP communication occurs at the data link layer so that it is independent of any network layer protocol that may be running on a network segment. CDP frames are sent as multicasts, using a destination MAC address of 01:00:0c:cc:cc:cc.

Switches regard the CDP address as a special address designating a multicast frame that should not be forwarded. Instead, CDP multicast frames are redirected to the switch's management port, and are processed by the switch supervisor alone. Therefore, Cisco switches only become aware of other directly connected Cisco devices.

### Enabling CDP and Viewing CDP Information on an IOS-Based Switch

CDP is enabled by default on all switch interfaces. To enable CDP, use the following interface configuration command (use the **no** form to disable CDP):

```
Switch(config-if)# cdp enable  
Switch(config-if)# no cdp enable
```

To view information learned from CDP advertisements of neighboring Cisco devices, use one of the following commands:

```
Switch# show cdp interface [type module/port]
Switch# show cdp neighbors [type module/port] [detail]
```

The first command displays CDP information pertaining to a specific interface. If the type, module, and port information is omitted, CDP information from all interfaces is listed. The second command displays CDP information about neighboring Cisco devices. If the **detail** keyword is used, all possible CDP information about each neighbor is displayed.

### Enabling CDP and Viewing CDP Information on a CLI-Based Switch

CDP is enabled by default. To enable or disable CDP, use the following command:

```
Switch(enable) set cdp {enable | disable} module/port
```

The *module* and *port* parameters are included to enable or disable CDP on individual ports. If these values are excluded, CDP is enabled or disabled on a global basis for all ports on the switch.

To view information learned from CDP advertisements of neighboring Cisco devices, use a form of the following command:

```
Switch(enable) show cdp neighbors [module/port] [vlan | duplex | capabilities | detail]
```

Here, the module and port number can be given to view CDP information on a particular port. The **vlan** keyword displays information about the native VLAN numbers of neighboring devices. The **duplex** keyword displays the duplex type of each neighboring device. Using **capabilities** displays capability codes for the neighboring devices. The **detail** keyword displays all possible CDP information about each neighboring device, including the IP address assigned to the neighboring interface or management interface.

As demonstrated in Example 3-2, the **show cdp neighbors detail** command can be useful when you are connected to a switch and need to know more about what other switches are nearby in a network. Particularly useful are the IP address entries, allowing Telnet access to previously unknown switches.

#### Example 3-2 Displaying CDP Information for Neighboring Devices

```
Switch(enable) show cdp neighbors 4/4 detail
Port (Our Port):4/4
Device-ID:69046406
Device Addresses:
  IP Address:172.20.25.161
Holdtime:150 sec
Capabilities:TRANSPARENT_BRIDGE SWITCH
Version:
  WS-C5509 Software, Version MpsW: 5.3(0.29)BOU NmpSW: 5.3(0.29)BOU
  Copyright (c) 1995-1999 by Cisco Systems
```

**Example 3-2** *Displaying CDP Information for Neighboring Devices (Continued)*

```
Port-ID (Port on Device):4/8
Platform:WS-C6009
VTP Management Domain:unknown
Native VLAN:1
Duplex:half
Switch(enable)
```

For a quick summary of CDP status on all switch ports, use the **show cdp port** command.

## Switch Clustering and Stacking

Cisco has also implemented a proprietary method for grouping switches into a management cluster. Up to 16 switch devices can be added into a cluster, regardless of their physical location on the network. In this fashion, an entire cluster of switches can be managed through a single IP address—that of the *command switch*. Cluster management can be performed through HTML, IOS-based, and SNMP-based management interfaces on the command switch.

Cluster discovery takes place once a command switch has been assigned an IP address and configured as a command switch. CDP messages are used to discover neighboring switches that are candidates for cluster membership. Cluster discovery takes place only on switch ports that are assigned and connected to VLAN1. Only the directly connected switch devices will be discovered by the command switch. Other switches daisy-chained behind the directly connected neighbors can be manually added to the cluster.

**NOTE**

At press time, only the Catalyst 2900 and 3500 switch families (both IOS-based) are capable of cluster operations.

To configure a switch to become the command switch for a cluster, first assign an IP address for the management interface. Then, use the following command:

```
Switch(config)# cluster enable cluster-name
```

Once the command switch has been identified and configured, the cluster discovery can be viewed and managed from a web browser. Refer to the *Cluster Builder* documentation in the Catalyst 2900XL and 3500XL software documentation for further detailed information and examples. ([www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29\\_35xp/scg/kielust.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xp/scg/kielust.htm))

## Switch Port Configuration

The individual ports on a switch can be configured with various information and settings, as detailed in the following sections.

### Identifying Ports

Switch ports can have a text description added to their configuration to help identify them. This description is meant as a comment field only, as a record of port use or other unique information. The port description is shown when the switch configuration is displayed.

### Assigning a Port Description on an IOS-Based Switch

To assign a comment or description to an interface on a switch with an IOS-based user interface, enter the following command in interface configuration mode:

```
Switch(config-if)# description description-string
```

If the description string has embedded spaces between words, the entire string must be enclosed between quotation marks. To remove a description, use the **no description** interface configuration command.

### Assigning a Port Description on a CLI-Based Switch

For a switch with a CLI-based user interface, assign a port description with:

```
Switch(enable) set port name module/number description-string
```

Here, *module* is the switch module number where the port resides, and *number* is the port number on that module. The description string must be less than 21 characters, and can have embedded spaces with no special treatment. To remove a port description, use the **set port name module/number** command, followed by a carriage return (no description string).

## Port Speed

Switch ports can be assigned a specific speed through switch configuration commands. Ethernet ports can be set to speeds of *10*, *100*, and *Auto* for autonegotiate mode. Gigabit Ethernet ports are always set to a speed of *1000*. Token Ring ports can be set to speeds of *4*, *16*, and *Auto* for autosensing mode.

---

**NOTE**

If a 10/100 Fast Ethernet port is assigned a speed of **auto**, both its speed and duplex mode will be negotiated.

---

## Assigning Port Speed on an IOS-Based Switch

To specify the port speed on a particular Ethernet port, use the following interface configuration command:

```
Switch(config-if)# speed {10 | 100 | auto}
```

## Assigning Port Speed on an CLI-Based Switch

On a CLI-based switch, set the port speed with the following command:

```
Switch(enable) set port speed module/number {10 | 100 | auto}  
Switch(enable) set port speed module/number {4 | 16 | auto}
```

The first line applies to Ethernet or Fast Ethernet ports, while the second line applies to Token Ring ports.

## Ethernet Port Mode

Ethernet-based switch ports can also be assigned a specific link mode. Therefore, the port operates in half-duplex, full-duplex, or autonegotiated mode. Autonegotiation is only allowed on Fast Ethernet and Gigabit Ethernet ports. In this mode, full-duplex operation will be attempted first, and then half duplex if full duplex was not successful. The autonegotiation process repeats whenever the link status changes.

---

**NOTE**

A 10-Mbps Ethernet link defaults to half duplex, while a 100-Mbps Fast Ethernet link defaults to full duplex.

---

## Assigning the Ethernet Link Mode on an IOS-Based Switch

To set the link mode on an IOS-based switch port, enter the following command in interface configuration mode:

```
Switch(config-if)# duplex {auto | full | half}
```

If the port is not automatically enabled or activated, use the **no shutdown** interface configuration command. To view the current speed and duplex state of a port, use the **show interface** command.

## Assigning the Ethernet Link Mode on a CLI-Based Switch

To set the link mode on a CLI-based switch port, enter the following command:

```
Switch(enable) set port duplex module/number {full | half}
```



If the port is not automatically enabled or activated, use the **set port enable** command. To view the current speed and duplex status of a port, use the **show port** command.

## Token Ring Port Mode

Token Ring ports have five modes of operation:

- **Half-duplex concentrator port (hdxcpport)**—The port is connected to a single station in half-duplex mode, similar to a MAU connection.
- **Half-duplex station emulation (hdxstation)**—The port is connected to a media attachment unit (MAU) port, like a regular station.
- **Full-duplex concentrator port (fdxcport)**—The port is connected to a full-duplex station.
- **Full-duplex station emulation (fdxstation)**—The port is connected to another full-duplex Token Ring.
- **Autosensing (auto)**—The port will autosense the operating mode of the connected device or ring.

## Assigning the Token Ring Link Mode on a CLI-Based Switch

To set the Token Ring link mode on a CLI-based switch port, enter the following command:

```
Switch(enable) set tokenring portmode module/number {auto | fdxcport | hdxcpport |  
fdxstation | hdxstation}
```

## Foundation Summary

The Foundation Summary is a collection of tables and figures that provides a convenient review of many key concepts in this chapter. For those of you already comfortable with the topics in this chapter, this summary could help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final prep before the exam, the following tables and figures will hopefully be a convenient way to review the day before the exam.

**Table 3-6** *Cabling Specifications for Fast Ethernet*

Technology	Wiring Type	Pairs	Cable Length
100BaseTX	EIA/TIA Category 5 UTP	2	100 m
100BaseT2	EIA/TIA Category 3,4,5 UTP	2	100 m
100BaseT4	EIA/TIA Category 3,4,5 UTP	4	100 m
100BaseFX	Multimode fiber (MMF) 62.5 micron core, 125 micron outer cladding (62.5/125)	1	400 m half duplex or 2000 m full duplex
	Single-mode fiber (SMF)	1	10 km

**Table 3-7** *Autonegotiation Selection Priorities*

Priority	Ethernet Mode
7	100BaseT2 (full duplex)
6	100BaseT2 (half duplex)
5	100BaseTX (full duplex)
4	100BaseT4
3	100BaseTX
2	10BaseT (full duplex)
1	10BaseT

**Table 3-8** *Gigabit Ethernet Cabling and Distance Limitations*

<b>GE Type</b>	<b>Wiring Type</b>	<b>Pairs</b>	<b>Cable Length</b>
1000BaseCX	Shielded twisted-pair (STP)	1	25 m
1000BaseT	EIA/TIA Category 5 UTP	4	100 m
1000BaseSX	MMF with 62.5 micron core; 850 nm laser	1	275 m
	MMF with 50 micron core; 1300 nm laser	1	550 m
1000BaseLX/LH	MMF with 62.5 micron core; 1300 nm laser	1	550 m
	SMF with 50 micron core; 1300 nm laser	1	550 m
	SMF with 9 micron core; 1300 nm laser	1	10 km
1000BaseZX	SMF with 9 micron core; 1550 nm laser	1	70 km
	SMF with 8 micron core; 1550 nm laser	1	100 km

**Table 3-9** *Token Ring Segmentation Methods*

<b>Method</b>	<b>Forwarding Decision</b>	<b>Frame Modification</b>	<b>Ring Numbering</b>
Transparent bridging	MAC address		N/A
Source-route bridging	RIF	RIF	Ring numbers must be unique among bridge ports
Source-route transparent	MAC address or RIF	RIF	Ring numbers must be unique among bridge ports
Source-route switching	Route descriptor		Ring numbers can be same across switch ports (single ring can be segmented on several ports)

**Table 3-10** *Switch Management Configuration Commands*

<b>Task</b>	<b>IOS-Based Command</b>	<b>CLI-Based Command</b>
Identify Switch	<b>hostname</b> <i>hostname</i>	<b>set system name</b> <i>name-string</i>
Set EXEC level password	<b>enable password level 1</b> <i>password</i>	set password
Set privileged level password	<b>enable password level 15</b> <i>password</i>	set enablepass
Set IP address	<b>interface vlan 1</b> <b>ip address</b> <i>ip-address netmask</i> <b>ip default-gateway</b> <i>ip-address</i>	<b>set interface sc0</b> <i>ip-address netmask broadcast-address</i> <b>set interface sc0</b> <i>vlan</i> <b>set ip route default</b> <i>gateway</i>
CDP	<b>cdp enable</b> <b>show cdp interface</b> <i>[type module/port]</i> <b>show cdp neighbors</b> <i>[type module/port] [detail]</i>	<b>set cdp {enable   disable}</b> <i>module/port</i> <b>show cdp neighbors</b> <i>[module/port]</i> <b>[vlan   duplex   capabilities   detail]</b>
Enable cluster	<b>cluster enable</b> <i>cluster-name</i>	N/A

**Table 3-11** *Switch Port Configuration Commands*

<b>Task</b>	<b>IOS-Based Command</b>	<b>CLI-Based Command</b>
Identify port	<b>description</b> <i>description-string</i>	<b>set port name</b> <i>module/number description-string</i>
Set port speed (Ethernet)	<b>speed</b> { <b>10</b>   <b>100</b>   <b>auto</b> }	<b>set port speed</b> <i>module/number</i> { <b>10</b>   <b>100</b>   <b>auto</b> }
Set port speed (Token Ring)	N/A	<b>set port speed</b> <i>module/number</i> { <b>4</b>   <b>16</b>   <b>auto</b> }
Set port mode (Ethernet)	<b>duplex</b> { <b>auto</b>   <b>full</b>   <b>half</b> }	<b>set port duplex</b> <i>module/number</i> { <b>full</b>   <b>half</b> }
Set port mode (Token Ring)	N/A	<b>set tokenring portmode</b> <i>module/number</i> { <b>auto</b>   <b>fdxport</b>   <b>hdxport</b>   <b>fdxstation</b>   <b>hdxstation</b> }

## Q&A

The questions and scenarios in this book are more difficult than what you should experience on the actual exam. The questions do not attempt to cover more breadth or depth than the exam; however, they are designed to make sure that you know the answer. Rather than allowing you to derive the answer from clues hidden inside the question itself, the questions challenge your understanding and recall of the subject. Questions from the “Do I Know This Already?” quiz from the beginning of the chapter are repeated here to ensure that you have mastered the chapter’s topic areas. Hopefully, these questions will help limit the number of exam questions on which you narrow your choices to two options and then guess.

The answers to these questions can be found in Appendix A, on page 477.

- 1 What are the different Ethernet technologies and their associated IEEE standards?

---

---

---

- 2 What benefits result with switched Ethernet over shared Ethernet?

---

---

---

- 3 When a 10/100 Ethernet link is autonegotiating, which will be chosen if both stations can support the same capabilities—10BaseT full duplex, 100BaseTX half duplex, or 100BaseTX full duplex?

---

---

---

- 4 At what layer are traditional 10-Mbps Ethernet, Fast Ethernet, and Gigabit Ethernet different?

---

---

---

5 Describe Cisco's EtherChannel technology.

---

---

---

6 A switch port is being configured as shown below. What command is needed next to set the port to full-duplex mode?

```
Switch(config)# interface FastEthernet 0/13  
Switch(config-if)#
```

---

---

---

7 In a campus network, where is Fast Ethernet typically used? Where is Gigabit Ethernet typically used?

---

---

---

8 What is the maximum length of a Category 5 100BaseTX cable?

---

---

---

9 A CLI-based switch port has been configured for 100 Mbps full-duplex mode, but a link cannot be established. What are some commands that could be used to investigate and correct the problem?

---

---

---

10 Name a type of Token Ring segmentation.

---

---

---

- 11 What part of a Token Ring frame specifies the exact path the frame should take to reach its destination?

---

---

---

- 12 What switch command will set the enable-mode password on an IOS-based switch? A CLI-based switch?

---

---

---

- 13 What is the purpose of a GBIC?

---

---

---

- 14 What CLI-based commands will allow Telnet and **ping** access to a switch management interface at 192.168.200.10, subnet mask 255.255.255.0, on VLAN 5? Now add a command to allow access between the switch and devices located off the local VLAN 5 subnet, using a router at 192.168.200.1.

---

---

---

- 15 What must be done to a switch before Telnet access is allowed?

---

---

---

- 16 What factors determine the choice of a distribution layer switch, its access-to-distribution layer link media, and its Layer 3 processor?

---

---

---

- 17** What type of user interface or command set does the Catalyst 5000 family of switches support? What type is the Catalyst 3500XL?

---

---

---

- 18** What protocol is used by a Catalyst switch to learn about neighboring routers and switches?

---

---

---

- 19** What switch command can be used to find the IP addresses of nearby Cisco switches on a network?

---

---

---

- 20** What port speeds can be assigned to a Fast Ethernet switch port?

---

---

---

- 21** What is the purpose of switch clustering? Can clustered switches share switching loads with each other?

---

---

---

- 22** What port speeds can be assigned to a Token Ring switch port?

---

---

---