Fast Facts

OSI Model in Review

Table FF.1 lists the seven layers of the OSI model and significant aspects of each layer.

TABLE FF.1 The OSI Model

OSI Layer	Important Functions
Application	Provides an interface between a host's communication software and any necessary external applications. Evaluates what resources are necessary and available resources for communication between two devices. Synchronizes client/server applications. Provides error control and data integrity between applications. Provides system-independent processes to a host.
Presentation	Presents data to the application layer. Acts as a data format translator. Handles the structuring of data and negotiating data transfer syntax to Layer 7. Processes involved include data encryption, decryption, compression, and decompression.
Session	Handles dialog control among devices. Determines the beginning, middle, and end of a session or conversation that occurs between applications (intermediary).
Transport	Manages end-to-end connections and data delivery between two hosts. Segments and reassembles data. Provides transparent data transfer by hiding details of the transmission from the upper layers.
Network	Determines best path for packet delivery across the network. Determines logical addressing, which can identify the destination of a packet or datagram. Uses data packets (IP, IPX) and route update packets (RIP, EIGRP, and so on). Uses routed protocols IP, IPX, and AppleTalk DDP. Devices include routers and Layer 3 switches.
Data Link	Ensures reliable data transfer from the Network layer to the Physical layer. Oversees physical or hardware addressing. Formats packets into a frame. Provides error notification. Devices include bridges and Layer 2 switches.
Physical	Moves bits between nodes. Assists with the activation, maintenance, and deactivation of physical connectivity between devices. Devices include hubs and repeaters.

Application Protocols Supported by the Application Layer

TABLE FF.2 Application Layer Protocols

Application Protocols	Function
Telnet	A TCP/IP protocol that provides terminal emulation to a remote host by creating a virtual terminal. TeraTerm is one program that can be installed on a user computer to create Telnet sessions. This protocol requires authentication via a username and password.
Hypertext Transfer Protocol (HTTP)	Enables web browsing with the transmission of Hypertext Markup Language (HTML) documents on the Internet.
Secure Hypertext Transfer Protocol (HTTPS)	Enables secure web browsing. A secure connection is indicated when the URL begins with https:// or when a lock symbol is in the lower-right corner of the web page that is being viewed.
File Transfer Protocol (FTP)	Allows a user to transfer files. Provides access to files and directories.
Trivial File Transfer Protocol (TFTP)	A bare-bones version of FTP that does not provide access to directories. With TFTP you can simply send and receive files. Unlike FTP, TFTP is not secure and sends smaller blocks of data.
Domain Name System (DNS)	Resolves hostnames such as cisco.com into IP addresses.
Simple Mail Transfer Protocol (SMTP)	Sends email across the network.
Post Office Protocol 3 (POP3)	Receives email by accessing a network server.
Network File System (NFS)	Allows users with different operating systems (that is, NT and Unix workstations) to share files through a network. Remote files appear as though they reside on a local machine even though the local machine might be “diskless.”
Network News Transfer Protocol (NNTP)	Offers access to Usenet newsgroup postings.
Simple Network Management Protocol (SNMP)	Monitors the network and manages configurations. Collects statistics to analyze network performance and ensure network security.
Network Time Protocol (NTP)	Synchronizes clocks on the Internet to provide accurate local time on the user system.
Dynamic Host Configuration Protocol (DHCP)	Works dynamically to provide an IP address, subnet mask, domain name, and a default gateway for routers. Works with DNS and WINS (used for NetBIOS addressing).

TABLE FF.3 Control Information for Each Layer

OSI Layer	Control Information Name
Application	Data
Presentation	
Session	
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

TABLE FF.4 OSI Layers and Related TCP/IP Layers

OSI Layer	TCP/IP Layer
Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data Link Physical	Network Access

TCP uses Positive Acknowledgment and Retransmission (PAR):

1. The source device begins a timer when a segment is sent and retransmits if the timer runs out before an acknowledgment is received.
2. The source device keeps track of segments that are sent and requires an acknowledgment for each segment.
3. The destination device acknowledges when a segment is received by sending a packet to the source that iterates the next sequence number it is looking for from the source.

TABLE FF.5 The TCP Segment Header Format

Source Port	Destination Port
Sequence Number	
Acknowledgment Number	
Miscellaneous Flags	Window (Flow Control)
Checksum	Urgent
Options	

TABLE FF.6 Applications Using TCP and Related Ports

Application	Port Number(s)
FTP	20, 21
Telnet	23
SMTP	25
DNS (zone transfers)	53
HTTP	80
POP3	110
NNTP	119
HTTPS	443

TABLE FF.7 The UDP Header

Source Port	Destination Port
Length	Checksum

TABLE FF.8 Applications Using UDP and Related Ports

Application	Port Number(s)
DHCP	67, 68
DNS (name resolution)	53
TFTP	69
NTP	123
SNMP	161

Network Domains

Two domains determine data transport reliability:

- **Broadcast domain:** A group of nodes that can receive each other's broadcast messages and are segmented by routers.
- **Collision domain:** A group of nodes that share the same media and are segmented by switches. A collision occurs if two nodes attempt a simultaneous transmission. *Carrier Sense Multiple Access Collision Detection (CSMA/CD)* sends a jam signal to notify the devices that there has been a collision. The devices then halt transmission for a random backoff time.

Cabling, Lines, and Services

- **Bandwidth:** The total amount of information that can traverse a communications medium measured in millions of bits per second. Bandwidth is helpful for network performance analysis. Also, availability is increasing but limited.
- **Crosstalk:** An electrical or magnetic field that is a result of one communications signal that can affect the signal in a nearby circuit.

  Near-end Crosstalk (NEXT): Crosstalk measured at the transmitting end of a cable.

  Far-end Crosstalk (FEXT): Crosstalk measured at the far end of the cable from where the transmission was sent.

Unshielded twisted-pair (UTP) cables are vulnerable to Electromagnetic Interference (EMI) and use an RJ-45 connector. Fiber-optic cables are not susceptible to EMI.

Use a straight-through cable to connect the following devices:

- Terminated directly into a dedicated hub or switch port
- From a PC to a switch or a hub
- From a router to a switch or a hub

Use a cross-over cable to connect the following devices:

- From switch to switch
- From router to router
- From PC to PC
- From a PC to a router
- From a hub to a hub
- From a hub to a switch

Spread Spectrum Wireless LANs allow for high-speed transmissions over short distances.

Wireless Fidelity (Wi-Fi) is defined by IEEE 802.11.

TABLE FF.9 Summary of Ethernet 802.3 Characteristics

Standard	Speed	Media Type	Connector Used
10BASE-2	10Mbps	RG-58 coaxial	BNC
10BASE-5	10Mbps	RG-58 coaxial	BNC
10BASE-T	10Mbps	Category 3, 4, or 5 UTP or STP	RJ-45
10BASE-FL	10Mbps	Fiber-optic	SC or ST

TABLE FF.10 Comparison of Fast Ethernet 802.3u Characteristics

Standard	Speed	Media Type	Connector Used
100BASE-T4	100Mbps	Category 3, 4, or 5 UTP or STP	RJ-45
100BASE-TX	100Mbps	Category 5 UTP or STP	RJ-45
100BASE-FX	100Mbps	Fiber-optic	SC or ST

TABLE FF.11 Summary of Gigabit Ethernet 802.3ab Characteristics

Standard	Speed	Media Type	Connector Used
1000BASE-T or 1000BASE-TX	1000Mbps or 1Gbps	Category 5 UTP or higher	RJ-45

TABLE FF.12 Comparison of Gigabit Ethernet 802.3z Characteristics

Standard	Speed	Media Type	Connector Used
1000BASE-CX	1000Mbps or 1Gbps	Shielded copper wire	Nine-pin shielded connector
1000BASE-SX	1000Mbps or 1Gbps	MM fiber-optic	SC or ST
1000BASE-LX	1000Mbps or 1Gbps	MM or SM fiber-optic	SC or ST

MAC Addressing

A MAC address is hard-coded (burned in) on the network interface controller (NIC) of the Physical layer device attached to the network. Each MAC address must be unique and use the following format:

- Consist of 48 bits (or 6 bytes).
- Displayed by 12 hexadecimal digits (0 through 9, A through F).
- First six hexadecimal digits in the address are a vendor code or organizationally unique identifier (OUI) assigned to that NIC manufacturer.
- Last six hexadecimal digits are assigned by the NIC manufacturer and must be different from any other number assigned by that manufacturer.

Example of a MAC address: 00:00:07:A9:B2:EB

The OUI in this example is 00:00:07.

The broadcast address value is FFFF.FFFF.FFFF.

Framing and Duplex Types

802.3 frame information and parameters are as follows:

- The data-link header portion of the frame contains the Destination MAC address (6 bytes), Source MAC address (6 bytes), and Length (2 bytes).
- The Logical Link Control portion of the frame contains Destination Service Access Point (DSAP), Source Service Access Point (SSAP), and Control information. All three are 1 byte long. The Service Access Point (SAP) identifies an upper-layer protocol such as IP (06) or IPX (E0).
- The Data and cyclical redundancy check (CRC) portion of the frame is also called the data-link trailer. The Data field can be anywhere from 43 to 1497 bytes long. The frame check sequence (FCS) field is 4 bytes long. FCS or CRC provides error detection.

Bridges and switches examine the source MAC address of each inbound frame to learn MAC addresses.

Switches are multiport bridges that use ASIC hardware chips for frame forwarding. Dedicated bandwidth enables the switch port to guarantee the speed assigned to that port. For example, 100Mbps port connections get 100Mbps transmission rates.

Hubs use half-duplex technology. Switches can be set up for full duplex.

WAN Interfaces

WAN interfaces are used to provide a point of interconnection between Cisco routers and other network devices. Types of WAN interfaces include

- Basic Rate Interface (BRI)
- Synchronous Serial
- Asynchronous Serial
- High-Speed Serial Interface (HSSI)
- T1 Controller Card

BRI is an Integrated Services Digital Network (ISDN) line that consists of two 64Kbps bearer (B) channels and one 16Kbps data (D) channel.

DCE equipment might consist of a

- Modem
- Channel Service Unit/Data Service Unit (CSU/DSU)
- BRI NT-1

DTE equipment might consist of a

- Router
- PC
- Server

Memory Types

Four memory components are used by Cisco devices. Those components include ROM, flash, RAM, and NVRAM.

RAM contains the running IOS, with the exception of run from flash (RFF) routers. RAM also contains the running configuration or the active configuration that is used after a machine is booted.

IOS File Naming Conventions

Given the example filename c2600-ipbase-1.122-1.T.bin, from left to right, each portion of the filename represents the following:

- **c2600:** Hardware platform (Cisco 2600 router)
- **ipbase:** Feature set
- **1:** File format (compressed relocatable)
- **122:** IOS version number
- **l:** Maintenance release number
- **T:** Train identifier

Utilities Using ICMP

Internet Control Messaging Protocol (ICMP) is used by ping and traceroute utilities. Packet Internet Groper (ping) allows you to validate that an IP address exists and can accept requests.

- Ping is an echo and the response is an echo response.
- Routers send Destination Unreachable messages when they can't reach the destination network and they are forced to drop the packet. The router that drops the packet sends the ICMP DU message.

A traceroute traces the route or path taken from a client to a remote host. Traceroute also reports the IP addresses of the routers at each next hop on the way to the destination. This is especially useful when you suspect that a router on the route to an unreachable network is responsible for dropping the packet.

Network Security

Three classes of attack are commonly found in today's network environment:

- Access attacks
- Reconnaissance attacks
- Denial of service (DoS) attacks

Access Attacks

An access attack is just what it sounds like: an attempt to access another user account or network device through improper means. The four main types of access attacks are

- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle

Reconnaissance Attacks

The four main subcategories or methods for gathering network data for a reconnaissance attack are

- Packet sniffers
- Port scans
- Ping sweeps
- Information queries

Denial of Service (DoS) Attacks

DoS attacks are often implemented by a hacker as a means of denying a service that is normally available to a user or organization. The three main types of DoS attacks are

- Distributed DoS
- TCP SYN
- Smurf

Mitigating Network Threats

The following actions can be taken to lessen the impact of an attack on a network:

- Authentication, Authorization, and Accounting (AAA)
- Cisco access control lists (ACLs)
- Cisco IOS Secure Management features: SSH, SNMP, Syslog, and NTP
- Encryption protocols: SSH, IPsec, and SSL
- Security appliances and applications: Firewall, IPS, and IDS

IP Addressing

IPv4 addresses

- Consist of 32 bits.
- Are broken into four octets (8 bits each).

- Use dotted-decimal format; an example is 172.16.122.204.
- Minimum value (per octet) is 0, and the maximum value is 255.
- 0.0.0.0 is a network ID.
- 255.255.255.255 is a broadcast IP.

TABLE FF.13 IPv4 Address Classes

	First Octet	Second Octet	Third Octet	Fourth Octet
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

TCP/IP defines two additional address classes:

- **Class D:** Used for multicast addresses.
- **Class E:** Used for research purposes.

TABLE FF.14 Address Class Ranges

Class	First Octet Decimal Range
A	1 to 126
B	128 to 191
C	192 to 223
D	224 to 239
E	240 to 255

The 127.x.x.x address range is reserved for loopback addresses.

Default subnet masks:

- **Class A:** 255.0.0.0
- **Class B:** 255.255.0.0
- **Class C:** 255.255.255.0

Classless Addressing

Classless Interdomain Routing (CIDR) notation might also be used to identify the subnet mask. The CIDR notation for each network class can be determined by counting the 1s in binary or the number of bits that make up the network portion of the address.

The mask is written in slash notation as follows:

- **Class A:** /8
- **Class B:** /16
- **Class C:** /24

Private Ranges

IANA private address space allocations:

- **Class A:** 10.0.0.0 to 10.255.255.255
- **Class B:** 172.16.0.0 to 172.31.255.255
- **Class C:** 192.168.0.0 to 192.168.255.255

Subnetting

TABLE FF.15 Decimal to Binary Conversions

Class	First Octet Decimal Range
0	00000000
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

To calculate the hosts in a subnet, we can use the formula $2^H - 2$. The exponent H represents the number of host bits in a network.

To calculate the networks in a subnet, we can use the formula $2^N - 2$. The exponent N represents the number of subnet bits in a network.

The range of valid IP addresses in a subnet is the first IP address after the Network ID and the last IP address before the broadcast IP address.

The following represents IP subnetting:

IP address = 100.15.209.0

Subnet mask = 255.255.254.0

Network ID = 100.15.208.0

Broadcast IP = 100.15.209.255

Valid IP range = 100.15.208.1 to 100.15.209.254

IPv6

IPv6 is a workable IP version that was created in the event that the IP space from IPv4 is exhausted.

IPv6 address format summary:

- Defined by RFC 2373 and RFC 237.
- Consists of 128 bits, with a 64-bit network prefix and a 64-bit local identifier.
- Represented by 32 hexadecimal digits broken into eight smaller groups of four.
- Utilizes CIDR notation (slash notation) to discern a subnet range, so you might see the same IP address subnetted and written out as 2001:0BD2:0200:08F1:0000:0000:0000:16AB/16.

The same IPv6 IP address can be written out in all of the following ways:

2001:**0**BD2:**0**200:**0**8F1:0000:0000:0000:16AB

2001:BD2:200:8F1:0:0:0:16AB

2001:BD2:200:8F1::16AB

Types of IPv6 Addresses

- **Link-local addresses:** Addresses that have the shortest reach of the IP address types. They can only go as far as the Layer 2 domain. These addresses are autogenerated with or without the use of a DHCP server. So, when an IPv6 node goes online, this address is assigned automatically.
- **Unique/site-local addresses:** Addresses that have a broader scope than link-local addresses. They can expand to the size of an organization and are used to describe the boundary of the organizational network. These are the private addresses for IPv6.
- **Global addresses:** Addresses that have the broadest scope of all. As the name indicates, these addresses are for global use—that is, for Internet communications.
- **Multicast:** Addresses that are extremely important because of their use in group communications and broadcast messaging.

Integrating IPv4 and IPv6

There are several ways to integrate IPv4 and IPv6 addressing. You can implement dual-stack, tunneling, or translation techniques to help IPv4 and IPv6 addresses exist together on the network simultaneously.

Layer 3 Functions

Routers and Layer 3 switches perform the following functions:

- Do not forward broadcasts or multicasts by default.
- Make best path decisions.
- Filter packets with access lists.
- Remove and add Layer 2 frames.
- Use quality of service (QoS) rules for traffic types.

Routers decide which interface to forward a packet through by examining the network portion of each IP address.

IOS Terminal Access Methodologies

To gain access to an EXEC session to an IOS for configuration and administration, you can use the following methods:

- **Console:** Out-of-band CLI access via a rollover cable connected to the COM port of your terminal PC.
- **Auxiliary:** Out-of-band CLI access via rollover cable connected to external modem for remote access.
- **Telnet:** In-band CLI access to an active IP address on the device's vty lines using the Telnet protocol. Requires configuration.
- **SSH:** Secure encrypted in-band CLI access to an active IP address using the SSH protocol. Requires configuration.
- **HTTP/HTTPS:** In-band GUI access to an active IP address using the HTTP or HTTPS protocol. Requires configuration.

IOS Boot Processes

To solidify the startup process, the following is a recap of the stages of the bootup, any fallback procedures, and the memory locations involved:

1. POST located in ROM tests hardware.
2. Bootstrap located in ROM looks at boot field in configuration register to locate IOS. 0x2100 boots to ROMmon located in ROM.
3. 0x2101 to 0x210F prompt bootstrap to parse startup-config in NVRAM for any `boot system` commands. If there are any commands, do what they say.
4. If no `boot system` commands, load first file in flash. If no file in flash, TFTP boot. If no IOS file found from TFTP, go to ROMmon mode.
5. After IOS is loaded, check configuration register. If 0x2142, ignore startup-config in NVRAM. If 0x2102, load startup-config in NVRAM. If no startup-config, TFTP autoinstall. If no TFTP autoinstall configuration found, enter Setup Mode.

IOS Navigation

TABLE FF.16 IOS Navigation Modes

Mode	Prompt	Description
User EXEC	`Router>`	Basic troubleshooting and verification
Privileged EXEC	`Router#`	All available commands, including `delete`, `clear`, `erase`, `configure`, `copy`, and `reload`
Global configuration	`Router(config)#`	Configurations that apply to the entire device
Line configuration	`Router(config-line)#`	Configurations that apply to the terminal lines into a device
Interface configuration	`Router(config-if)#`	Configurations that apply to interfaces
Subinterface configuration	`Router(config-subif)#`	Configurations that apply to logical extensions of the physical interface
Router configuration	`Router(config-router)#`	Configurations that apply to routing protocols
VLAN configuration	`Switch(vlan)#`	VLAN-specific configurations in switches

Context-Sensitive Help

The question mark shows all the available commands at that particular prompt. To see all the available commands that start with a letter or letter(s), type the letter(s) immediately followed by a question mark. To see the list of commands that follows a keyword, type the keyword, a space, and a question mark. Commands can be abbreviated as long as there are enough characters to recognize what command you are entering.

Terminal Editing Keys

TABLE FF.17 Cisco IOS Terminal Editing Keystrokes

Keystroke	Function
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+B	Moves the cursor back one character.
Ctrl+F	Moves the cursor forward one character.
Esc+B	Moves the cursor back one word.
Esc+F	Moves the cursor forward one word.

Syntax Errors

- **Ambiguous command:** This error is displayed when you have not typed enough characters for the IOS to distinguish which command you want to use. In other words, several commands start with those same characters, so you must type more letters of the command for the IOS to recognize your particular command.
- **Incomplete command:** The IOS has recognized your keyword syntax with this error message; however, you need to add more keywords to tell the IOS what you want to do with this command.
- **Invalid input:** Also known as the "fat finger" error, this console error message is displayed when you mistype a command. The IOS displays a caret (^) up to the point where the IOS could understand your command.

Global Configuration Commands

TABLE FF.18 Global Configuration Commands

Command	Description
`config-register` *`register`*	Alters the configuration register.
`boot system` *`location`*	Specifies location to load IOS.
`hostname` *`hostname`*	Changes the name of the Cisco router or switch.
`banner motd` *`char banner char`*	Creates a message of the day login banner.
`ip host` *`name ipaddress`*	Configures a static mapping of a hostname to an IP address.
`ip name-server` *`ip`*	Specifies a DNS server IP address for dynamic name resolution.
`ip domain-lookup`	Enables automatic name resolution.
`ip domain-name`	Assigns a domain name to a Cisco device.

Securing the IOS

First and foremost, ensure that you physically secure access to your Cisco devices so that there are no intentional or unintentional disruptions or access to the device itself.

To secure user EXEC access to your console port:

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password password
```

To secure user EXEC access to your aux port:

```
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password password
```

To secure user EXEC access to all five Telnet lines:

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password password
```

To secure access to privileged EXEC mode:

```
Router(config)#enable secret password
Router(config)#enable password password
```

The `enable secret` global configuration command encrypts the password using a MD5 hash. If the `enable secret` and `enable password` commands are used at the same time, the `enable secret` password is used.

To encrypt the `enable password` and the line passwords, use the `service password-encryption` command.

SSH

To secure terminal access to the Cisco device, use SSH over Telnet. The steps to configure SSH are as follows:

1. Configure a hostname on the device other than the default hostname.
2. Configure a domain name for the Cisco device.
3. Generate an RSA key (recommended to be at least 1024 bits) with the `crypto key generate` command.
4. Create a username/password combination with the `username` *`username`* `password` *`password`* command.
5. (Optional) Limit the vty lines to allow SSH with only the `transport input SSH` command.

Interface Configuration Commands

TABLE FF.19 Interface Configuration Commands

Command	Description
`ip address ip` *`subnetmask`*	Assigns an IP address to an interface.
`no shutdown`	Administratively enables an interface.
`full-duplex`	Changes the duplex setting to full duplex.
`clock rate` *`speed`*	Sets the timing speed of the network on a DCE interface in bps.
`bandwidth` *`speed`*	Sets the logical bandwidth setting for routing protocols in Kbps.
`ip address dhcp`	Dynamically assigns an IP address to an interface from a DHCP server.

Switch Commands

TABLE FF.20 Switch Configuration Commands

Command	Description
`interface range` *`media range`*	Configures several interfaces with the same parameters.
`ip address` *`ipaddress`*	Assigns an IP address to a VLAN interface.
`ip default-gateway` *`ip`*	Sets the gateway of last resort for a Layer 2 switch.
`speed` *`speed`*	Changes the speed of an autosensing link in Mbps.
`duplex` *`duplex`*	Sets the duplex of a switchport.

The copy Command

The `copy` command is used to copy files from one location to another. For example, to save the current configuration, we copy the running-config in RAM to the startup-config in NVRAM using the `copy running-config startup-config` command.

The `copy` command is used to copy files between our device and a TFTP server. For instance, `copy flash tftp` backs up the IOS in flash to a TFTP server. `copy flash tftp` can be used to upgrade, downgrade, or restore an IOS back onto our device. Before copying to a TFTP server, follow these steps:

1. The TFTP server must have the TFTP service running.
2. Our device must be cabled correctly. If a switch, plug the TFTP server into the switch with a straight-through Ethernet cable. If going directly between a router and the TFTP server, use a cross-over cable.

3. You must have IP connectivity to the server.
4. There must be enough room on the TFTP server and your device's memory to store these files.

The show Command

TABLE FF.21 General show Commands

Command	Mode	Output
`show running-config`	Privileged	Current active configuration in RAM.
`show startup-config`	Privileged	Configuration stored in NVRAM that is loaded on reboot.
`show interfaces`	User and privileged	Status of the interfaces as well as physical and logical address, encapsulation, bandwidth, reliability, load, MTU, duplex, broadcasts, collisions, and frame errors.
`show ip interface brief`	User and privileged	Status of the interfaces and their logical addresses.
`show controller`	User and privileged	Microcode of the interface including DCE/DTE cable connection.
`show flash`	User and privileged	Filenames and sizes of IOS files stored in flash memory.
`show version`	User and privileged	IOS version, system uptime, amount of RAM, NVRAM, flash memory, and configuration register.

Interface Status

TABLE FF.22 Interface Status Values

Layer 1	Layer 2 (Line Protocol)	Possible Symptoms
Up	Up	None. Interface is functional.
Up	Down	Encapsulation mismatch, lack of clocking on serial interfaces.
Down	Down	Cable is disconnected or attached to a shutdown interface on the far-end device.
Administratively down	Down	Local interface was not enabled with the `no shutdown` command.

Cisco Discovery Protocol

- Proprietary Cisco Layer 2 protocol that uses multicast to gather hardware and protocol information about directly connected devices.
- Network layer protocol and media independent.
- Enabled by default on all Cisco devices, but can be disabled globally:

```
Router(config)#no cdp run
```

  or can be disabled on interface-by-interface basis:

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

- To learn the remote device's Layer 3 address and IOS version

```
Router>show cdp neighbor detail
```

  or

```
Router>show cdp entry *
```

Telnet

Telnet enables a virtual terminal connection to a remote device's IP address using the Application layer protocol called Telnet (TCP port 23 at the Transport layer).

To Telnet from IOS, enter the keyword `telnet` followed by the IP address or hostname. If you enter only an IP address or hostname in user or privileged EXEC, IOS automatically assumes that you are Telnetting. To Telnet to a Cisco device, the vty passwords must be set, or you receive the "Password required, but none set" error. To access Privileged EXEC in a Telnet session, you must have enable password set, or you receive the "% No password set" error.

- To suspend the Telnet session, press Ctrl+Shift+6, x.
- To see a list of the active sessions in the originating router, use the `show sessions` command.
- To resume a suspended session, press the Enter key from user EXEC or privileged EXEC mode, or enter `resume` followed by the session number.
- To close a Telnet session from the device you are Telnetted into, enter `exit` or `logout` from user EXEC or privileged EXEC mode.
- To close a Telnet session from the originating device, enter `disconnect` followed by the session number.
- To see log messages in your Telnet session, use the privileged EXEC mode command `terminal monitor` in the device that you are Telnetted into.

DHCP

Your Cisco device can act as a DHCP server and respond to DHCP requests on a segment. To configure the Cisco device as a DHCP server, you must first enable the interface that will receive the DHCP requests and assign an IP address to it. After the interface is enabled, you define the DHCP address pool with the `ip dhcp pool` *`poolname`* global configuration command. In `dhcp-config` mode, you can define the DHCP address scope with the `network` command followed by the IP subnet to be assigned. You can also define additional parameters such as the default gateway, DNS server, domain name, and length of the IP lease. To exclude IP addresses from being assigned (such as if you have statically assigned them to specific devices), use the `ip dhcp excluded-address` *`ip-address`* command to remove the IP(s) from the scope.

To verify the devices that have been assigned IP addresses from the DHCP address scope, use the `show dhcp bindings` command.

Switches

Switches have the following functions:

- Segment LANs into multiple collision domains.
- Learn MAC addresses by examining the source MAC address of each frame received and store them in a CAM table.
- Base their forwarding decisions based on the destination MAC address of an Ethernet frame.
- Flood broadcast, multicast, and unknown unicast frames out all ports except the one it was received.

A switch has three methods of forwarding frames:

- **Store-and-forward:** Latency varying transmission method that buffers the entire frame and calculates the CRC before forwarding the frame.
- **Cut-through:** Only looks at the destination MAC address in an Ethernet frame and forwards it.
- **Fragment-free:** Checks the first 64 bytes for frame fragments (due to collisions) before forwarding the fame.

Duplex Connections

- Half-duplex interfaces have one-way communication with suboptimal throughput because they operate in a collision domain in which CSMA/CD must be enabled. When connected to a hub, they must run half duplex.
- Full-duplex interfaces simultaneously send and receive, allowing higher throughput because CSMA/CD is disabled. Connections to other switches or devices can be full duplex.

Spanning Tree Protocol IEEE 802.1d

STP is a Layer 2 protocol that is used to prevent switching loops in networks with redundant switched paths.

TABLE FF.23 STP Port States

State	Function	Transition Time
Disabled	The interface is administratively shut down or disabled from port violation.	NA
Blocking	Does not forward any user data. All ports start out in this state. Does not send, but still can receive BPDUs to react to topology changes.	0 to 20 seconds
Listening	Begins to transition to a forwarding state by listening and sending BPDUs. No user data sent.	15 seconds
Learning	Begins to build MAC addresses learned on the interface. No user data sent.	15 seconds
Forwarding	User data forwarded.	

STP elects root bridge/switch by determining which switch has the lowest Bridge ID in the topology learned from sending and receiving BPDUs. Bridge ID is a combination of Priority and MAC address.

All nonroot switches determine root port based on the fastest (lowest cumulative cost) path back to root switch. If a tie occurs, the Bridge ID followed by port priority and port number are the tie breakers.

On each segment, the switch advertising the fastest way back to the root switch is the designated port for that segment.

If port is not a root or a designated port, it is blocking.

TABLE FF.24 Port Cost Values

Interface	Cost
10Gbps	2
1Gbps	4
100Mbps	19
10Mbps	100

STP Configuration

STP is enabled by default for all VLANs in a switch. To change the priority to a lower value for root switch elections, use one of the following commands:

```
Switch(config)#spanning-tree vlan 1 priority 4096
```

or

```
Switch(config)#spanning-tree vlan 1 root
```

STP Topology Changes and Enhancements

In the event of a topology change, formerly blocked ports might transition to a forwarding state. It might take up to 50 seconds to transition from a blocking state to a forwarding state.

An exception to these 50 seconds is if the following Cisco enhancements are in place to speed up convergence:

- **PortFast** skips the listening and learning states on end-devices such as servers, PCs, and printers. PortFast can cause switching loops if a hub or switch is connected. BPDU Guard adds protection by disabling a port if the interface receives a BPDU.
- **UplinkFast** skips the listening and learning transitions when a direct failure occurs on its root port on a switch with redundant uplinks to a distribution switch.
- **BackboneFast** speeds up convergence by skipping the max age time when switches learn of a failure indirectly.

EtherChannel

EtherChannel is a Cisco method of bundling redundant links between switches to act as a single aggregated link. This allows utilization of all the link's bandwidth, because STP treats the link as a single interface (no blocking/discarding ports). In the case of a link failure, EtherChannel automatically distributes the traffic load over the remaining links in milliseconds.

To add an interface to an EtherChannel bundle (up to eight), use the `channel-group` *`channel#`* `mode on` command in the interface configuration.

Rapid Spanning Tree Protocol

RSTP IEEE 802.1w incorporates several of Cisco's STP enhancements and ensures a safe and quick transition to a forwarding state and topology convergence by removing the overdependence on STP timers.

TABLE FF.25 RSTP Port States

State	Function	802.1d STP Equivalent
Disabled	The interface is administratively shut down or disabled from port violation.	Disabled
Discarding	Does not forward any user data. All ports start out in this state. Does not send, but still can receive BPDUs to react to topology changes.	Blocking and listening
Learning	Begins to build MAC addresses learned on the interface. No user data is sent.	Learning
Forwarding	User data is forwarded.	Forwarding

TABLE FF.26 RSTP Port Roles

State	Function	802.1d STP Equivalent
Root	The forwarding interface with the fastest (lowest cumulative path cost) to the root switch.	Root
Designated	On each segment, this forwarding interface is responsible for forwarding frames from one segment to the next.	Designated
Discarding	If the interface is not a root or designated port, it is discarding. Discarding ports are nonforwarding interfaces that do not forward traffic to avoid switching loops.	Blocking
Alternate	An interface in a discarding state that becomes the root port for a segment if the existing root port fails. Occurs when there are redundant links to the root switch in a switched network.	NA
Backup	An interface in a discarding state that becomes the designated port for a segment if the existing designated port fails. Occurs when there are redundant links to the same segment.	NA

TABLE FF.27 RSTP Link Types

State	Function
Link type point-to-point	Full-duplex links between switches
Link type shared	Half-duplex links between switches or hubs
Edge type	Connections to end devices such as PCs, printers, and servers

RSTP Convergence

Edge ports immediately transition to a forwarding state when connected to RSTP ports. For point-to-point link types, transitioning to a forwarding state involves a synchronization process:

1. After switches are connected to a point-to-point link, they exchange BPDUs.
2. If a switch determines its port will become a designated port, it sends a proposal to start forwarding to its neighbor.
3. The neighboring switch receives the proposal. If its port is a root port, it synchronizes the change by putting all nonedge ports into a discarding state and sending an agreement back to the original switch. If its port is a discarding port, it does not respond to the proposal.
4. The original switch immediately transitions to a forwarding state if it receives an agreement or eventually transitions to a forwarding state after a forward delay occurs.

RSTP uses BPDUs as keepalives to detect if a neighboring switch goes down. When the topology change is detected, RSTP immediately starts aging out the affected MAC address and tells its neighbors to do the same.

Virtual LANs (VLANs)

VLANs logically divide a switch into multiple broadcast domains at Layer 2.

Each VLAN can represent a logical grouping of users by function or department. As users in these VLANs move, we simply need to change the VLAN assigned to their switch port. VLANs also enhance security because users in one VLAN cannot communicate to users in another VLAN without the use of a Layer 3 device providing inter-VLAN routing.

VLAN Configuration

VLANs can be statically assigned to switch access ports or dynamically assigned by using a VMPS. By default, all interfaces are assigned to the management VLAN, VLAN 1.

To configure a VLAN:

1. Create the VLAN in global configuration:

```
Switch(config)#vlan 2
Switch(config-vlan)#
```

2. The VLAN must be named:

```
Switch(config-vlan)#vlan 2 name ExamPrep
```

3. The desired ports must be added to the new VLAN:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport access vlan 2
```

Voice VLANs

Voice VLANs are used to separate VoIP traffic from data on an access port for QoS, manageability, and traffic confinement.

```
Switch(config-if)#switchport voice vlan 30
```

Trunks

VLANS can span multiple switches using trunks. Trunks multiplex traffic from all VLANs over a single connection. The VLAN identifier is tagged over the trunk using one of the following tagging methods:

- **ISL:** A Cisco-proprietary trunk that encapsulates the original Ethernet frame with a 26-byte header and a 4-byte CRC.
- **IEEE 802.1q:** Standards-based VLAN tagging that inserts a 4-byte tag in the original Ethernet frame. Traffic originating from the native VLAN (VLAN 1 by default) is not tagged over the trunk. If native VLAN configuration does not match on both sides, this could cause VLAN leakage.

Trunk Configuration

```
Switch(config)#interface FastEthernet 0/24
Switch(config-if)#switchport trunk encapsulation [isl|dot1q]
Switch(config-if)#switchport mode trunk
```

Trunks can be secured by allowing only specific VLANs to traverse to switches that specifically require access to those VLANs. The command to specify the VLANs to be included in the "allowed list of VLANs" is `switchport trunk allowed vlan {add ¦ remove ¦ except} vlan_list`.

VLAN Trunking Protocol

Cisco created VTP to minimize the amount of VLAN administration in switches by enabling a VTP server to multicast VTP advertisements to other switches in the same VTP domain. Switches receiving these advertisements synchronize their VLAN database with the VLAN information advertised from the server, assuming that the revision number is higher.

TABLE FF.28 VTP Modes

Mode	Function
Server	Default VTP mode that enables you to create, modify, and delete VLANS. These VLANs are advertised to other switches and saved in the VLAN database.
Client	Cannot create, modify, or delete VLANs. Forwards advertisements received from the server, but does not save the VLAN configuration in the VLAN database.
Transparent	Creates, modifies, and deletes VLANs only on the local switch. Does not participate in VTP but forwards VTP advertisements received from servers. Also saves the VLAN configuration in the VLAN database.

VTP Configuration

Changing the VTP domain name from NULL to ExamPrep:

```
Switch(config)#vtp domain ExamPrep
```

Setting the device VLAN database password to examcram:

```
Switch(config)#vtp password examcram
```

Setting the device to VTP TRANSPARENT mode:

```
Switch(config)#vtp transparent
```

InterVLAN Routing

InterVLAN routing requires a Layer 3 device such as router or a Layer 3 switch:

- **Router-on-a-stick:** The connection between router and switch must be at least Fast Ethernet speeds and must be a trunk. The router interface consists of subinterfaces to assign an IP gateway for each VLAN. The VLAN is associated with a subinterface using the `encapsulation` command:

```
Router(config)#interface FastEthernet 0/1.2
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 2
Router(config)#interface FastEthernet 0/1.3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 3
```

- **Switched virtual interfaces:** VLAN interfaces configured in a Layer 3 switch that enables inter-VLAN routing using ASIC technology:

```
Router(config)#interface Vlan 2
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config)#interface Vlan 3
Router(config-if)#ip address 192.168.3.1 255.255.255.0
```

Port Security

Here's the configuration that limits the number of MAC addresses that can be dynamically learned on a switch port:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation {protect ¦ restrict ¦ shutdown}
```

If a violation occurs, the default response of a Catalyst switch is to shut down the port. To have the port increase a violation counter and alert an administrator using SNMP, use the `restrict` keyword. The `protect` keyword allows only traffic from the secure port and drops packets from other MAC addresses until the number of MAC addresses drops below the maximum.

To secure an interface by statically assigning the permitted MAC address(es) attached to the port, use the `switchport port-security mac-address` *`MAC_address`* command on the interface. Alternatively, you can have the switch learn these addresses up to the maximum by using sticky-learned addresses with the command `switchport port-security mac-address sticky`.

Routing Characteristics

Packets originating from a nonrouting device destined for another network are sent to their default gateway (Layer 3 device on segment). The router consults its routing table to determine if the destination network can be reached. If not, the ICMP Destination Unreachable message is sent to the source. If so, packet is forwarded out interface associated with the destination network in routing table.

Routing Sources

- **Connected interfaces:** As soon as we assign an IP address to a working (up/line protocol up) interface, the router associates the entire subnet of the interface's IP address in the routing table.
- **Static routes:** Manual entries that an administrator enters into the configuration that describe the destination network and the next hop (router along the destination path).
- **Routing protocols:** Protocols exchanged between routing devices to dynamically advertise networks.

When multiple routing sources are advertising the same IP subnet, the router uses the source with the lowest administrative distance.

TABLE FF.29 Default Administrative Distances

Routed Source	Default Distance
Connected	0
Static route	1
EIGRP (internal)	90
OSPF	110
RIPv1 and v2	120
EIGRP (external)	170

Static and Default Routes

Static routes are useful in stub networks in which we want to control the routing behavior by manually configuring destination networks into the routing table:

```
Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.2.5
```

A floating static route can be configured when redundant connections exist and you want to use the redundant link if the primary fails. This is configured by adding a higher administrative distance at the end of a static route:

```
Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.2.9 2
```

A default route is a gateway of last resort for a router when there isn't a specific match for an IP destination network in the routing table (such as packets destined for the Internet):

```
Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0
```

With routing protocols, you can specify a default network, which is a network in the routing table that routing devices consider to be the gateway of last resort. Using their routing protocols, they determine the best path to the default network:

```
Router(config)#ip default-network 192.168.1.0
```

Dynamic Routing Protocols

In complex networks with multiple pathways to destinations, dynamic routing protocols enable routers to advertise their networks to each other and dynamically react to topology changes.

Routing protocols determine the best path based on the lowest metric.

Routing Metrics

Because one of the core responsibilities of routing protocols is to build routing tables to determine optimal routing paths, we need to have some means of measuring which routes are preferred when there are multiple pathways to a destination. Routing protocols use some measure of metrics to identify which routes are optimal to reach a destination network. The lowest cumulative metric to a destination is the preferred path and the one that ultimately enters the routing table. Different routing protocols use one or several of the following metrics to calculate the best path.

TABLE FF.30 Routing Metrics

Metric	Description
Hop count	The number of routing devices that the packet must travel to reach a destination network
Bandwidth	The cumulative bandwidth of the links to the destination in kilobits per second
Delay	The length of time (measured in microseconds) a packet takes from source to destination
Reliability	The consistency of the links and paths toward the destination based on error rates of the interfaces
Load	The cumulative amount of congestion or saturation of the links toward the destination
MTU	The maximum frame size that is allowed to traverse the links to the destination
Cost	An arbitrary number typically based on the link's bandwidth

Interior and Exterior Gateway Routing Protocols

- **Interior gateway routing protocols:** IG routing protocols advertise networks and metrics within an autonomous system.
- **Exterior gateway routing protocols:** EG routing protocols advertise networks in between autonomous systems.

Classful and Classless Routing Updates

- **Classful routing:** The routing updates only contain the classful networks without any subnet mask. Summarization is automatically done when a router advertises a network out an interface that is not within the same major subnet. Classful routing protocols must have a FLSM design and do not operate correctly with discontiguous networks.
- **Classless routing:** The routing updates can contain subnetted networks because the subnet mask is advertised in the updates. Route summarization can be manually configured at any bit boundary. Classless routing protocols support VLSM designs and discontiguous networks.

Routing Protocol Classes

- **Distance vector:** The entire routing table is periodically sent to directly connected neighbors regardless of a topology change. These routing protocols manipulate the routing table updates before sending that information to their neighbors and are slow to converge when a topology change occurs.
- **Link state:** All possible link states are stored in an independent topology table in which the best routes are calculated and put into the routing table. The topology table is initially synchronized with discovered neighbors followed by frequent hello messages. These routing protocols are faster to converge than distance vector routing protocols.
- **Hybrid:** By using the best characteristics from link-state and routing protocols, these advanced routing protocols efficiently and quickly build their routing information and converge when topology changes occur.

Redistribution

Redistribution is the method of configuring routing protocols to advertise networks from other routing protocols:

- **One-way redistribution:** Networks from an edge protocol are injected into a more robust core routing protocol, but not the other way around. This method is the safest way to perform redistribution.
- **Two-way redistribution:** Networks from each routing protocol are injected into the other. This is the least preferred method because it is possible that suboptimal routing or routing loops might occur because of the network design or the difference in convergence times when a topology change occurs.

Distance Vector Routing Loop Mitigation

Distance vector routing protocols contain several measures to prevent routing loops:

- **Maximum hop counts:** To ensure that routing metrics do not increment until infinity in a routing loop, distance vector routing protocols have a maximum hop count.

TABLE FF.31 Maximum Hop Counts

Protocol	Distance Vector/Link State/Hybrid	Maximum Hop Count
RIPv1	Distance vector	15
RIPv2	Distance vector	15
EIGRP	Hybrid	224
OSPF	Link state	Infinite

- **Split horizon:** Subnets learned from neighbor routers should not be sent back out the same interface from which the original update came.
- **Route poisoning with poison reverse:** When a route to a subnet fails, the subnet is advertised with an infinite metric. Routers receiving the poisoned route override the split horizon rule and send a poison reverse back to the source.
- **Hold-down timers:** The amount of time a router ignores any information about an alternative route with a higher metric to a poisoned subnet.
- **Flash updates/triggered updates:** When a route fails, the router immediately shoots out an update as opposed to waiting for a normal update interval.

RIP and RIPv2

TABLE FF.32 RIP and RIPv2 Comparison

	RIPv1	RIPv2
Classful/classless	Classful	Both
Algorithm	Bellman-Ford	Bellman-Ford
Metric	Hops	Hops
Maximum hop count	15	15
Infinite metric	16	16
Hello/dead time	30/180	30/180
Updates	Broadcast	Multicast (224.0.0.9)
Update authentication	No	Yes
Load balancing	Equal paths	Equal Paths

RIP Configuration

The configuration for RIP is seamless as long as you remember these two simple rules:

1. Advertise only your directly connected networks.
2. Advertise only the classful network.

```
Router(config)#router rip
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
```

RIPv2 Configuration

```
Router(config)#router rip
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
Router(config-router)#version 2
Router(config-router)#no auto-summary
```

Verifying and Troubleshooting RIP

TABLE FF.33 Verifying and Troubleshooting RIP Commands

Command	Output
`show ip route`	The routing table with RIP entries represented as "R"
`show ip protocols`	RIP timers, advertised networks
`debug ip rip`	Real-time display of RIP routing updates being sent and received

Before using any `debug` commands, verify the processor utilization using the `show processes` command.

OSPF Characteristics

TABLE FF.34 OSPF Characteristics

	OSPF
Classful/classless	Classless
Algorithm	Dijkstra SPF
Metric	Cost (10^8/bandwidth bps)
Maximum hop count	None
Areas or autonomous system configuration	Areas

TABLE FF.34 *Continued*

	OSPF
Hello/dead time	10/40, 30/120
Cisco or IETF	IETF
Updates	Multicast (224.0.0.5, 224.0.0.6)
Load balancing	Equal paths
Routed protocols	IP

OSPF is a link-state routing protocol that automatically discovers its neighbors by sending hello messages to 224.0.0.5. After the neighbors are discovered, they form an adjacency by synchronizing their databases. This database lists all possible routes that the neighbor is aware of in the topology. Each subnet learned has a cost associated with it, which is calculated by taking 10^8/bandwidth. The paths with the lowest cost to a destination are put in the routing table.

TABLE FF.35 Cost Values Based on Bandwidth

Bandwidth	OSPF Cost
56Kbps	1785
64Kbps	1562
T1 (1.544 Mbps)	64
E1 (2048 Mbps)	48
Ethernet (10 Mbps)	10
Fast Ethernet (100 Mbps)	1
Gigabit Ethernet (1000 Mbps)	1

OSPF uses areas to limit the size of the topology table for devices inside that area, which allows for smaller updates and faster convergence. ABRs that sit on the border of these areas have a hierarchically function over other routers because they manually summarize networks to the rest of the OSPF autonomous system. The result of this summarization is a smaller topology and routing table because the individual subnets are not being advertised. In addition, topology changes are confined inside the area where the change occurred because other areas are not aware of the individual subnets.

Areas can be numbered from 0 to 65535. Area 0 is known as the backbone area in which all other areas must connect. An area can be configured as a stub area in which ABRs advertise default routes instead of summarized networks into an area to minimize the topology and route tables.

In broadcast and nonbroadcast multiaccess topologies, OSPF decreases the amount of update overhead by electing a DR and BDR. The DR and BDR are determined by the router that has the highest priority. In the case of a tie, the highest Router ID is a tiebreaker.

The Router ID is determined by the highest active loopback IP address that is configured when the OSPF process starts. The loopback interface is a virtual interface that does not go down unless the router is turned off. In the absence of any loopback interfaces, the highest active physical IP address is used. It is common to use a host mask (255.255.255.255) on a loopback interface.

When a topology change occurs, the update is sent to the DR and BDR to the 224.0.0.6 multicast address. The DR is responsible for sending that update to the rest of the OSPF routers by multicasting the update to 224.00.5. When a device receives an update, it immediately floods it to its neighbors before calculating the topology change.

OSPF Configuration

The first step should be to configure the loopback interface to establish the Router ID:

```
Router(config)#interface loopback 0
Router(config-if)#ip address 10.1.42.1 255.255.255.255
```

You must specify an OSPF process ID between 1 and 65535. The OSPF process ID identifies a unique instance of an OSPF process and is locally significant (does not have to match in all routers in the OSPF autonomous system):

```
Router(config)#router ospf 1
```

To associate the networks to OSPF areas, you must specify the network followed by the wildcard mask and the area:

```
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

The area can be designated as a stub area as long as there is only one pathway in and out of the area:

```
Router(config-router)#area 1 stub
```

To change the cost of a link on an interface, you must navigate to the interface and use the following command:

```
Router(config-if)#ip ospf cost 30
```

On broadcast and nonbroadcast multiaccess topologies, you should force the election by changing the default OSPF priority on the interface:

```
Router(config-if)#ip ospf priority 5
```

Verifying and Troubleshooting OSPF

TABLE FF.36 Verifying and Troubleshooting OSPF Commands

Command	Output
`show ip route`	The routing table with OSPF entries represented as "O." Routes learned from other areas also have an interarea indicator ("IA").
`show ip protocols`	OSPF process ID and advertised networks.
`show ip ospf interface`	Local router's router ID, interface topology type, link cost and priority, router ID for the DR and BDR on the segment, hello/dead intervals, and a count of how many neighbors and adjacencies.
`show ip ospf neighbor`	Neighbor table to verify neighbor IDs and if neighbor is DR or BDR.
`show ip ospf database`	OSPF subnets and advertising routers in the topology table.
`debug ip ospf events`	Real-time display of LSAs and LSUs being sent and received.

EIGRP Characteristics

TABLE FF.37 EIGRP Characteristics

	EIGRP
Classful/classless	Both
Algorithm	DUAL
Metric	32-bit composite (bandwidth plus delay)
Maximum hop count	224
Areas or autonomous system configuration	Autonomous systems
Hello/dead time	5/15, 60/180
Cisco or IETF	Cisco
Load balancing	Unequal paths
Routed protocols	IP, IPX, AppleTalk
Redistribution	Automatic with matching IGRP autonomous system number
Administrative distance	90 for internally learned networks 170 for externally learned networks
Updates	Multicast (224.0.0.10)

In the EIGRP topology table, EIGRP maintains the advertised distance and the feasible distance to every subnet. The subnet(s) with the lowest feasible distance is the route that is placed in the routing table known as the successor route. If the advertised distance of an alternative route is lower than the feasible distance of the successor route, it is a feasible successor, which

is used if the successor route fails. This is why EIGRP's DUAL algorithm makes it the fastest-converging routing protocol.

In cases in which there isn't a feasible successor, the route goes from a passive state to an active state. The state is active because the router is actively querying its neighbor for alternative paths to the destination. If a reply indicates an alternative path, that link is used.

EIGRP Configuration

Similar to IGRP, EIGRP uses the concept of autonomous system numbers in the configuration. These autonomous system numbers must match in all configured Cisco routing devices:

```
Router(config)#router eigrp 100
Router(config-router)#network 192.168.7.0
Router(config-router)#network 172.17.0.0
```

EIGRP can also load-balance over unequal paths using the `variance` command:

```
Router(config-router)#variance 10
```

Similar to RIPv2, EIGRP can be configured as classless supporting VLSM, discontiguous networks, and manual route summarization:

```
Router(config-router)#no auto-summary
```

Verifying and Troubleshooting EIGRP

TABLE FF.38 Verifying and Troubleshooting EIGRP Commands

Command	Output
`show ip route`	The routing table with OSPF entries represented as "D." External route entries learned from redistribution also have an "EX" indicator.
`show ip protocols`	EIGRP autonomous system and advertised networks.
`show ip eigrp neighbors`	Neighbor table to verify neighbors in neighbor table.
`show ip eigrp topology`	EIGRP-learned subnets and the calculated successors for each subnet based on the lowest composite metric.
`debug ip eigrp`	Real-time display of hellos and updates being sent and received.

Passive Interfaces

When interfaces are not connected to other routing devices, or you want to designate certain devices that should not receive routing updates, you can configure those interfaces as passive interfaces. When an interface is designated as a passive interface, routing updates are not sent

out that interface. However, incoming updates can still be received and processed. To configure the passive interfaces, use the `passive-interface` command in the routing process:

```
Router(config-router)#passive-interface fastethernet 0/0
```

Wireless Networking

Wireless networks have impacted our existing network environments profoundly over the last few years. Because this is the newest topic on the CCENT and CCNA exams, much of what you need to know is the foundations of wireless:

- Wireless networks exist by using FCC unmanaged/unregulated radio frequency (RF) signals. This allows corporations to implement wireless technology without FCC approval.
- The primary technologies that exist today are 802.11b, 802.11g, and 802.11a. 802.11b/g uses the 2.4GHz frequency range. 802.11a uses the 5GHz frequency range. The 2.4GHz band is much more saturated with consumer electronics (such as cordless phones and microwaves) than the 5GHz band. 802.11n is still in draft status at the time of this writing.
- Higher radio frequencies can handle more bandwidth, but they have less range than the lower radio frequencies.
- When wireless technology is implemented in a larger building, adjacent wireless access points should use different channels to avoid interfering with each other.
- The primary channels used in the U.S. for 802.11b/g are channels 1, 6, and 11. These three channels do not have any overlapping frequencies with each other.
- The Wi-Fi Alliance was an organization whose aim was to create a cross-vendor certification of wireless equipment. Purchasing equipment certified by the Wi-Fi Alliance ensures that all the wireless networking gear you use will be compatible with each other.

Wireless Security and Implementation

Because wireless networking has become so prevalent in businesses, it is imperative that every network technician know the foundations of wireless security. Table FF.39 breaks down the wireless encryption standards currently available.

TABLE FF.39 Wireless Encryption Standards

Security Standard	Encryption Strength	Key Distribution	Encryption Cipher
WEP	40-bit	Preshared keys	RC4
WEP2	104-bit	Preshared keys	RC4
WPA	128-bit	Preshared keys or 802.1x; TKIP allows dynamic key rotation	RC4
WPA2 (802.11i)	Varied strength; currently up to 256-bit	Preshared keys or 802.1x	AES

Wireless authentication adds an entirely new layer of security to your wireless network. Rather than simply requiring a preshared key (PSK) to gain access to the WLAN, users must authenticate using one of many EAP methods. Encryption keys are dynamically generated after a successful authentication.

Network authentication for LAN environments is called 802.1x (also known as EAP over LAN [EAPOL]).

When implementing wireless access points, you can choose to use a Basic Service Set (BSS), which is a single access point. Or you can choose to use an Extended Service Set (ESS), which is two or more BSSs that tie users to the same LAN. These typically have overlapping coverage areas.

The farther you move from a wireless access point, the more your speed decreases. 802.11a/b/g have the following steps:

802.11a and 802.11g:

- Step 1: 54Mbps
- Step 2: 48Mbps
- Step 3: 36Mbps
- Step 4: 24Mbps
- Step 5: 18Mbps
- Step 6: 12Mbps
- Step 7: 9Mbps
- Step 8: 6Mbps

802.11b:

- Step 1: 11Mbps
- Step 2: 5.5Mbps

- Step 3: 2Mbps
- Step 4: 1Mbps

Implementing a wireless network typically should be done in four steps:

1. Ensure hardwired operation.
2. Install the wireless access point in your tested switchport.
3. Configure a basic wireless network, and test it.
4. Add wireless security, and test it.

Cisco Access Lists

Access lists are a Cisco configuration paramount to enabling your router to do any major task. The following facts are relevant to access lists:

- A Cisco access list is nothing more than an ordered list of permit and deny statements.
- They are read by the router in a top-down format. As soon as a match condition is reached, the access list stops processing.
- If you reach the end of an access list and have not been explicitly permitted, you are implicitly denied.
- Numbered and named access lists do not allow you to reorder statements; however, named access lists allow you to delete individual access list lines.

Access lists have a number of functions on the Cisco router. The primary access lists uses are

- Packet filtering
- Quality of Service (QoS)
- Network Address Translation (NAT)
- Route filtering

There are two types of IP-based access lists:

- Standard access lists are capable of filtering traffic based only on the source IP address.
- Extended access lists are capable of filtering traffic based on protocol, source address, source port number, destination address, and destination port number.

IP Standard access lists use numbers 1 to 99, and IP Extended access lists use numbers 100 to 199.

The configuration of a standard access list uses the following syntax:

```
Router(config)#access-list <1-99> <permit/deny> <source_IP_address> <wildcard_mask>
```

The following configuration creates access list 25, which permits a single host (10.1.1.5) and the 192.168.1.0/24 subnet:

```
Router(config)#access-list 25 permit 10.1.1.5 0.0.0.0
Router(config)#access-list 25 permit 192.168.1.0 0.0.0.255
```

As a shortcut, you can use the `host` keyword instead of a wildcard mask of 0.0.0.0 and the `any` keyword instead of a wildcard mask of 255.255.255.255. The following example shows these keywords in action:

```
Router(config)#access-list 25 permit host 10.1.1.5
Router(config)#access-list 25 deny any
```

When looking to apply an access list to an interface, remember the following mantra:

One access list

- Per protocol
- Per interface
- Per direction

When trying to find what direction to apply an access list, picture yourself as a router. Hold out an arm to represent an interface. If the traffic is moving away from your body, it should be applied `out` (outbound) on the interface. If the traffic is coming into your body, it should be applied `in` (inbound) on the interface. Standard access lists are always applied closest to the destination. Extended access lists are always applied closest to the source.

The following is the generic syntax used to apply access lists to an interface:

```
Router(config-if)#ip access-group <access-list_number> <in/out>
```

The following configuration applies access list 25 in the inbound direction:

```
Router(config-if)#ip access-group 25 in
```

Access lists can also be applied to vty ports to restrict Telnet access to your router. The following configuration applies access list 25 to a router's vty ports:

```
Router(config)#line vty 0 4
Router(config-line)#access-class 25 in
```

Extended access list configuration gets slightly more complex than a standard access list. The following is the generic syntax used to create an extended access list:

```
Router(config)#access-list <100-199> <permit/deny> <protocol> <source_IP_address>
<wildcard_mask> <source_port_number> <destination_IP_address> <wildcard_mask>
<destination_port_number>
```

There are many IP-based protocols that extended access lists can permit or deny. The following is a list of the protocols you should be familiar with:

- **IP** permits or denies source/destination addresses using the entire TCP/IP protocol suite. Using this keyword permits or denies *all* access from a source to a destination.
- **TCP** permits or denies source/destination addresses using TCP-based applications. The most common applications include FTP, Telnet, SMTP, and HTTP.
- **UDP** permits or denies source/destination addresses using UDP-based applications. The most common applications include DNS and TFTP.
- **ICMP** permits or denies source/destination addresses using ICMP-based applications. The most common applications include Echo, Echo-Reply, and Unreachables.

When configuring extended access lists, you rarely, if ever, know a network device's source port number information. This number is randomly generated by the host's operating system. You should leave it blank for any CCNA-level configuration you perform.

You need to know these commonly used port numbers for the CCNA exam:

TCP Ports

- Port 21: FTP
- Port 22: SSH
- Port 23: Telnet
- Port 25: SMTP
- Port 80: HTTP
- Port 443: HTTPS

UDP Ports

- Port 53: DNS
- Port 69: TFTP

The following access list permits a single host (10.1.1.5) to access any destination using port 80 (HTTP):

```
Router(config)#access-list 150 permit tcp host 10.1.1.5 any eq 80
```

The following access list denies a network subnet (172.16.70.0/24) from accessing a single host (172.16.50.100) using port 21 (FTP):

```
Router(config)#access-list 125 deny tcp 172.16.70.0 0.0.0.255 host 172.16.50.100 eq 21
```

Often, you need to end an access list with a "permit all" statement. The following examples show how to accomplish this:

Standard access list example:

```
Router(config)#access-list 12 permit any
```

Extended access list example:

```
Router(config)#access-list 125 permit ip any any
```

Often, a router connected to the Internet denies all incoming traffic to secure the internal network. However, this prevents internal users from receiving responses to their common web browsing requests. The following extended access list entry permits any return traffic that is a response to a request originated from the internal network:

```
Router(config)#access-list 150 permit tcp any any established
```

You can verify access lists using a few `show` commands:

- `show running-config` shows the full access list configuration and the interfaces where you have applied them.
- `show ip interface` shows the inbound and outbound access lists applied to each interface.
- `show access-lists` shows all access lists created on the router and the number of times each entry has been matched.
- `show ip access-lists` shows just the IP-based access lists on the router and the number of times each entry has been matched.

Network Address Translation (NAT)

NAT is in use on virtually every Internet-connected router in the world today. This technology acts as a security boundary and Internet address sharing system. The following facts are relevant to NAT.

NAT typically operates by translating private IP addresses to public Internet addresses. The following are the private address ranges as defined by RFC 1918:

- **Class A:** 10.X.X.X
- **Class B:** 172.16.X.X to 172.31.X.X
- **Class C:** 192.168.X.X

The three primary forms of NAT are as follows:

- **Static NAT** allows you to manually map one IP address to another in a one-to-one relationship.
- **Dynamic NAT** allows you to define a pool of addresses to be translated along with a pool of addresses they will be translated to.
- **NAT Overload/PAT** allows a single Internet IP address to support many internal clients.

The standards bodies have developed many terms to describe the location of an IP address in the world of NAT:

- **Inside local addresses:** Refers to everything inside your network.
- **Inside global addresses:** The Internet valid IP address assigned to your router that is directly connected to the Internet.
- **Outside global addresses:** A standard Internet IP address accessible from any host connected to the Internet.
- **Outside local addresses:** How an Internet host is seen by the internal network as it is translated through the NAT router into your local network.

The following shows a Static NAT configuration fully translating 192.168.1.50 (on the internal network) to 5.1.1.10 (on the Internet). It then shows a single Static NAT port translation mapping 192.168.1.150 port 53 (DNS) on the internal network to 5.1.1.11 port 53 on the Internet:

```
NAT_Router(config)#interface fastethernet0
NAT_Router(config-if)#ip nat inside
NAT_Router(config)#interface serial0
NAT_Router(config-if)#ip nat outside
NAT_Router(config)#ip nat inside source static 192.168.1.50 5.1.1.10
NAT_Router(config)#ip nat inside source static udp 192.168.1.150 53 5.1.1.11 53
```

The following shows a NAT Overload/PAT configuration translating the entire internal network (192.168.1.0/24) to a single Internet address assigned to the Serial0 interface:

```
NAT_Router(config)#interface fastethernet0
NAT_Router(config-if)#ip nat inside
NAT_Router(config)#interface serial0
NAT_Router(config-if)#ip nat outside
NAT_Router(config)#access-list 50 permit 192.168.1.0 0.0.0.255
NAT_Router(config)#ip nat inside source list 50 interface serial0 overload
```

Wide-Area Networks

Wide area network (WAN) connections tie together geographically distant locations, enabling them to communicate as if directly connected. The following facts are relevant to WANs.

WAN technologies only encompass the Physical and Data Link layers of the OSI model. The three major categories of WAN technology used to connect networks today are as follows:

- **Leased lines** provide a dedicated, point-to-point link between two locations.
- **Circuit-switched networks** establish a dedicated channel (or circuit) for the duration of the transmission and then tear down the channel when the transmission is complete.
- **Packet-switched networks** enable the service provider to create a large pool of bandwidth for its clients, who establish connections through the shared bandwidth using virtual circuits.

Cisco routers connect to most WAN connections through their serial ports. The Cisco side of the connection uses either a DB-60 or Smart Serial port. The CSU/DSU that the Cisco router connects to has one of five standard connectors: V.35, X.21, EIA/TIA-232, EIA/TIA-449, or EIA/TIA-530.

At the Data Link layer, Cisco routers primarily use one of two WAN encapsulations for leased-line and circuit-switched networks:

- **Point-to-Point Protocol (PPP):** The most popular, industry-standard, feature-packed protocol for connecting routers
- **Cisco High-level Data Link Control (HDLC):** A Cisco-proprietary, low-overhead protocol that makes your WAN connections very efficient between Cisco devices

HDLC is the default encapsulation on all Cisco serial interfaces. However, PPP is used to gain more features and industry standard capabilities when connecting over the WAN. It is made up of three sublayers:

- **ISO HDLC** is responsible for enabling PPP to be supported by multiple devices.
- **Link Control Protocol (LCP)** is the feature negotiation layer that performs the following functions:

- **Authentication** requires a username and password for the connecting device.
  - **Callback** enables a dialup server (or router) running PPP to call back the person who initially dialed into the location using a predefined number.
  - **Compression** makes WAN connections more efficient by minimizing the amount of data sent.
  - **Multilink** bundles multiple WAN connections (or WAN channels in the case of ISDN) into a single, logical connection.
- **Network Control Protocol (NCP)** gives PPP the functionality to enable multiple Network layer protocols to run across a single WAN link at any given time.

When configuring PPP authentication, you can choose between two authentication protocols:

- **Password Authentication Protocol (PAP)** sends username and password once in clear-text format when authenticating.
- **Challenge Handshake Authentication Protocol (CHAP)** sends a username and hashed password when demanded by the CHAP server.

When configuring PPP compression, you can choose between three compression types:

- **Stacker:** A flat compression algorithm that is notoriously heavy on CPU resources and has less effect on the router's memory resources. Useful for WAN links with many traffic patterns.
- **Predictor:** A dictionary-based compression algorithm that is notoriously heavy on memory resources and has less effect on the router's CPU resources. Useful for WAN links with similar traffic patterns.
- **Microsoft Point-to-Point Compression (MPPC):** Used for Microsoft Windows dialup clients wanting to use compression.

To activate PPP encapsulation on an interface, use the following syntax:

```
Router(config)#interface serial 0
Router(config-if)#encapsulation ppp
```

When adding CHAP authentication to your configuration, you need to ensure that you create a user account that matches the hostname of the other side of the connection. In addition, the passwords must be the same on both sides. Here is a PPP CHAP authentication configuration between the Kirk and Spock routers:

```
Kirk(config)#username Spock password cisco
Kirk(config)#interface serial 0
Kirk(config-if)#encapsulation ppp
```

```
Kirk(config-if)#ppp authentication chap

Spock(config)#username Kirk password cisco
Spock(config)#interface serial 0
Spock(config-if)#encapsulation ppp
Spock(config-if)#ppp authentication chap
```

To enable PPP compression on an interface, you can use the following syntax:

```
Router(config-if)#compress ?
  mppc       MPPC compression type
  predictor  predictor compression type
  stac       stac compression algorithm
```

The `show interface` command is one of the most useful when verifying the PPP configuration. The connection is active when the LCP Open tag is seen, as shown here:

```
Router#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.2.2.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP, CCP, CDPCP
```

When troubleshooting PPP authentication issues, use the `debug ppp authentication` command to observe the authentication process as it occurs.

Frame Relay

Frame Relay is the only packet-switched network tested on the CCNA exam. It is one of the more popular connections in businesses today. The following facts are relevant to Frame Relay.

Frame Relay offers the high speeds demanded by the networks of today at cut-rate prices. Rather than connecting sites through individual physical interfaces, Frame Relay connects sites using virtual circuits. Virtual circuits are logical links through service provider networks that give routers the impression that they are directly linked. The more virtual circuits purchased to connect network locations, the more redundant the network connections will be; at the same time, the monthly cost will rise significantly. Because of this, there are three design strategies for provisioning virtual circuits:

- **Hub and spoke:** A centralized location (most likely, your largest, most connected office) acts as the network's "hub." All other locations are considered "spokes" and have a single virtual circuit connection back to the hub.

- **Partial mesh:** Key network sites have redundant virtual circuit connections through the Frame Relay cloud. Other noncritical sites might only have a single virtual circuit.
- **Full mesh:** Every site has a direct virtual circuit to every other site in the network.

Frame Relay also introduces another set of terminology that CCNA candidates should be familiar with:

- **Permanent Virtual Circuit (PVC):** A permanently "nailed-up" circuit through the Frame Relay service provider network.
- **Switched Virtual Circuit (SVC):** An "on-demand" connection through the Frame Relay cloud.
- **Local Management Interface (LMI):** Signaling between your router and the Frame Relay service provider.
- **Data Link Connection Identifier (DLCI):** The Data Link layer addressing used by Frame Relay to identify endpoints connected to the Frame Relay service provider.
- **Local access rate:** The maximum physical speed that a Frame Relay connection can attain.
- **Committed Information Rate (CIR):** The minimum speed the service provider commits to give you for a virtual circuit at all times.
- **Backward Explicit Congestion Notification (BECN):** A message sent by the service provider notifying a router sending at an excessive data rate to reduce its speed.
- **Forward Explicit Congestion Notification (FECN):** A message sent by the service provider notifying a receiving router to send information that can be tagged as a BECN to tell a router sending at an excessive data rate to reduce its speed.
- **Discard Eligible (DE):** Describes any traffic that you send above the CIR you have purchased.

To provide more logical configurations, Cisco routers can create multiple subinterfaces that can connect to any number of virtual circuits. Two types of subinterfaces can be created:

- **Point-to-point subinterfaces** are assigned to a single virtual circuit. Only one DLCI number assigned per point-to-point subinterface.
- **Multipoint subinterfaces** are assigned to one or more virtual circuits. Numerous DLCI numbers can be mapped under a multipoint subinterface.

Using multipoint interfaces or the physical Serial interface for multiple virtual circuits causes known problems with the distance vector routing protocol loop-prevention mechanism, split horizon.

Cisco routers initially receive a list of DLCIs they can reach from the Frame Relay service provider. There are two ways they can map the DLCI number to the remote IP address it can reach at the other end of the connection:

- **Inverse ARP** enables the router to send messages down each one of the DLCI numbers to discover the router's IP address on the remote end.
- **Static mappings** allow the Cisco administrator to manually map each DLCI number to the router's IP address on the remote end.

Understanding the states of a Frame Relay PVC can be quite useful in both the real world and the testing environment:

- **Active:** The PVC is successfully connected through between the two endpoints (routers). This is the normal state if everything is working properly.
- **Inactive:** The PVC is working properly on your end of the connection (the local side); however, the other side of the connection is either not configured or offline.
- **Deleted:** The PVC is having problems on your end (the local side) of the connection. Most likely, you are attempting to use a DLCI number that the service provider has not configured.
- **Static:** The PVC has been manually entered by you (the administrator) rather than being dynamically discovered from the service provider.

Configuring a Frame Relay interface for a single virtual circuit requires the following minimal configuration:

```
Router(config)#interface serial 0
Router(config-if)#encapsulation frame-relay
```

If you are connecting to a non-Cisco router through the Frame Relay cloud, use the command `encapsulation frame-relay ietf` to enable your interface with the industry standard Frame Relay encapsulation.

If you are using an extremely old version of the IOS (any version earlier than 11.2), the router is unable to autodetect what LMI language the service provider is using. This means that you must manually configure it using the following syntax:

```
Router(config-if)#frame-relay lmi-type ?
  cisco
  ansi
  q933a
```

The following is a sample configuration of a multipoint interface using static Frame Relay maps. In this case, 192.168.5.1 is the remote end IP address and DLCI 405 is used to get there. Likewise, 192.168.5.2 is another remote-end router that can be reached through DLCI 406:

```
Router(config)#interface serial 0/0.10 multipoint
Router(config-if)#frame map ip 192.168.5.1 405 broadcast
Router(config-if)#frame map ip 192.168.5.2 406 broadcast
```

The following is a sample configuration using the same setup as the preceding example, but using point-to-point interfaces:

```
Router(config)#interface serial 0/0.405 point-to-point
Router(config-if)#frame-relay interface-dlci 405
Router(config)#interface serial 0/0.406 point-to-point
Router(config-if)#frame-relay interface-dlci 406
```

When troubleshooting Frame Relay connections, start with the `show frame-relay lmi` command to check connectivity to the service provider. From there, use `show frame-relay pvc` to check the status of the virtual circuits.

VPN Connectivity

VPN technology allows businesses to use their existing Internet connections to connect to other offices (site-to-site VPNs) or allow telecommuting or mobile users to connect into the office network from their PCs (remote-access VPN).

VPNs provide a variety of benefits over private-line connections:

- Cost savings over private-line connections
- Remote-access connections for telecommuting or mobile users
- Scalability

At the same time, VPNs have some major drawbacks:

- Higher overhead
- Varying service levels
- Additional security considerations

VPN connections come in two major genres: site-to-site and remote-access VPNs.

Site-to-site VPNs are the direct replacement for private-line WAN connections. They allow offices to maintain permanent or semipermanent connections between each other through the Internet.

Remote-access VPNs typically are used to allow telecommuting or mobile workers to connect to the corporate network from home or hotel-like locations. These remote-access VPNs come in a couple of styles: client-based (requires the installation of a VPN client) and clientless (also known as SSL or WebVPN; users connect through a secure web page).

The key protocol that drives VPN connections is IPsec. This is actually a suite of protocols that provide standards for encryption, authentication, and data integrity.

Three primary encryption standards are used with IPsec:

- **Data Encryption Standard (DES) algorithm** was originally developed by IBM to support a 56-bit key.
- **Triple DES (3DES) algorithm** uses three different DES keys to encrypt data, thus tripling the strength of DES.
- **Advanced Encryption Standard (AES)** currently offers 128-, 192-, and 256-bit encryption.

Currently, two data-integrity standards are used with IPsec:

- **Message Digest 5 (MD5)** uses a 128-bit hashing algorithm.
- **Secure Hash Algorithm 1 (SHA**-1) uses a 160-bit hashing algorithm.