EXAM CRAM

# The CCNA Cram Sheet

This Cram Sheet contains key facts about the ICND1 exam. Review this information as the last thing you do before you enter the testing center, paying special attention to those areas in which you think that you need the most review. You can transfer any of these facts from your head onto a blank sheet of paper immediately before you begin the exam.

## Networking Fundamentals

Physical components for a network include hosts, connections, switches, and routers. Physical topology describes the layout of the physical components. A logical topology communicates how the data flows through the network.

A local-area network (LAN) is a geographically close in proximity, high-speed network. A wide-area network (WAN) is a network that is using third-party services (such as an service provider) to connect devices over large geographic areas. A WAN is a collection of LANs connected over a long distance (farther than the LAN could provide).

WAN technologies include dedicated leased lines, which are a dedicated point-to-point connection that can use Point-to-Point Protocol (PPP) or High-Level Data Link Control (HDLC). Packet-switched connections share the bandwidth with other logical circuits, such as with Frame Relay.

High-speed LANs typically use Ethernet in full duplex, using switches that operate at Layer 2. Routers operate logically at Layer 3.

## Network Models

**OSI MODEL**

| Layer | Name | Protocols and Devices | PDU Name |
|---|---|---|---|
| 7 | Application | FTP, Telnet, TFTP, SMTP, SNMP, DNS, HTTP | Data |
| 6 | Presentation | ASCII, .jpg, .doc | Data |
| 5 | Session | Establishment and teardown of logical sessions | Data |
| 4 | Transport | TCP: Connection oriented, reliable<br>UDP: Connectionless, unreliable, uses upper layer protocols | Segment |
| 3 | Network | IP, routing and path determination, logical addressing<br>Routers | Packet |
| 2 | Data Link | Ethernet, Frame Relay, PPP, HDLC, MAC addresses<br>Switches | Frame |
| 1 | Physical | Bits transmitted on media<br>Hubs, repeaters | Bits |

**TCP AND UDP**

Know the following protocols and port numbers:

| TCP | | UDP | |
|---|---|---|---|
| FTP | 20, 21 | DNS | 53 |
| Telnet | 23 | DHCP | 67, 68 |
| SMTP | 25 | TFTP | 69 |
| DNS | 53 | NTP | 123 |
| HTTP | 80 | SNMP | 161 |
| POP | 110 | | |
| NNTP | 119 | | |
| HTTPS | 443 | | |

## Concepts in IP Addressing

IP is a Layer 3 media-independent connectionless protocol. Every device that is connected to the network must have a unique IP address. An IP address has two major parts: the network and the host portions.

Domain Name System (DNS) is used to map friendly names to the actual IP addresses associated with those names.

IPv4 uses a 32-bit number represented as four octets separated by periods, called dotted-decimal. IPv6 uses 128-bit numbers represented in eight groups of four hexadecimal characters each, separated by colons. Both IPv4 and IPv6 use a mask to identify how many bits going from left to right are being used to identify the network. Bits not used to identify the network are used to identify hosts on that specific network.

A default gateway is required to send a packet out of a local network.

**IPV4 ADDRESS CLASS AND RANGE**

| Class | High-Order Bits | First Octet Range |
|---|---|---|
| A | 0 | 1–126 |
| B | 10 | 128–191 |
| C | 110 | 192–223 |
| D | 1110 | 224–239 |
| E | 11110 | 240–255 |

**IPV4 ADDRESS CLASS AND DEFAULT MASKS**

| Class | Default Mask |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

**IPV4 PRIVATE IP ADDRESS RANGES**

| Class | Range |
|---|---|
| A | 10.0.0.0 to 10.255.255.255 |
| B | 172.16.0.0 to 172.31.255.255 |
| C | 192.168.0.0 to 192.168.255.255 |

Subnetting allows you to create additional subnets. Variable-length subnet masking (VLSM) allows you to use different mask lengths so as to not waste IP addresses.

To create IP subnets, you take (starting on the left) what used to be host IP bits and allocate them for subnetwork addressing. The number of bits that you allocate above and beyond the default control how many subnets you can create. The formula is two to the power of the number of bits that you take. For example, if we start with a 10.0.0.0/8 network and we use 3 additional bits to make it 10.0.0.0/11, we could create $2^3 = 8$ new subnets. Because the least significant bit of the new mask falls on the 32 value, that would be R block size for the new subnets, which would be 10.0, 10.32, 10.64, 10.96, and so on.

The number of host that can be created use the formula 2Host bits – 2. If we have a network of 10.0.0.0/28, that leaves four host bits, so we would have a possibility of 24 – 2 = 14 hosts on any network that had a /28 mask.

Subnetting is a process of moving the mask to the right.

IPv6 uses several types of addresses, including global unicast (which ranges from 2000 through 3FFF), link local unicast addresses (which begin with FE80) and multicast addresses (which begin with FF). Transition strategies include tunneling, dual stacking, and protocol translation. An anycast address is similar to unicast except that anycast packets will go to the one host that is closest as determined by the routing protocol metric. IPv6 never broadcasts; it multicasts instead.

IPv6 address compression:

Given the address 2010:0000:BBBB:000C :D000:0000:0000:0001, the following address representations are possible:

Drop leading 0s:

2010:0:BBBB:C:D000:0:0:1

Compress contiguous all-0 groups with :: once per address.

2010:0:BBBB:C:D000::1

Valid hex characters in an IPv6 address are 0–F.

IPv6 can use an EUI-64 method to create the host ID, starting with information from the MAC address being used by the interface.

The command **ipv6 unicast-routing** is off by default, and must be enabled for a router to forward the IPv6 packets of network devices.

IPv6 uses Neighbor Discovery Protocol (NDP) to determine Layer 2 addresses (replaces Address Resolution Protocol [ARP]). Autoconfiguration allows you to obtain, via plug-and-play, an IP address without using a DHCP server.

The IP stacks for IPv4 and IPv6 are completely separate from each other, as are the routing protocols for each of the stacks.

IPv6 OSPFv3 doesn't use network statements. It uses interface commands to enable each interface for OSPF. Static IPv6 routes can be created using the command **ipv6 route.**

## Working with Cisco Equipment

The console port on a router or switch can be used to initially configure the device. Ethernet ports are high-speed interfaces used to forward traffic, and can also be used to allow management traffic such as Secure Shell (SSH) over IP to the device being managed. Serial ports are slower connections (compared to Ethernet) that can be used for WAN connections.

Flash is a storage location that keeps the IOS image. NVRAM is a storage location that holds the startup configuration. RAM holds the current running configuration. The initial startup file in NVRAM is called startup config. The configuration that is running in RAM is called running config.

1. POST (power-on self-test): Device finds hardware and performs hardware-checking routines.
2. Locate IOS.
3. Load IOS.
4. Locate configuration (startup config).
5. Load configuration (running config).

The configuration register is a four-character hexadecimal value that can be changed to manipulate how the router behaves at boot. The default value is 0x2102.

The characters 0x indicate that the characters that follow are in hexadecimal. This makes it clear whether the value is "two thousand one hundred and two" or, as in this case, "two one zero two hexadecimal."

The fourth character in the configuration register is known as the boot field. Changing the value for this character will have the following effects:

- 0x2100 = Always boot to ROMmon.
- 0x2102 through 0x210F = Load the first valid IOS in flash.

The command-line interface has two primary modes: user mode and privileged mode. When in privileged mode, we can then enter configuration mode, as well as submodes, for configuration.

Context-sensitive help can be invoked by using the question mark (?).

The running configuration is stored in RAM as running config, and the startup configuration is saved in NVRAM as startup config.

Commonly used commands include **show version**, **show interface**, **show ip interface brief**, and **show running-config**.

Cisco Discovery Protocol (CDP) is a proprietary (Cisco only) data-link (Layer 2) protocol. It is enabled by default, but can be disabled globally via the **no cdp run** command. To learn remote device Layer 3 address, hardware platform, and IOS version, use **show cdp neighbor** or **show cdp entry** command.

## Securing Your Cisco Devices

You can use Telnet/SSH to remotely manage a Cisco device after it has IP addresses configured on it and interfaces enabled.

Using the command **login** on the vty lines requires the user to provide a password when connecting via Telnet. That password is configured on the vty lines.

To configure a password on all five Telnet lines, you use configuration commands similar to the following:

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

## Configuring SSH

To configure SSH on your router or switch, you need the following elements:

- A hostname
- A domain name
- An RSA key
- A username and password for local authentication

## Sample SSH Configuration

```
Switch>enable
Switch#config t
Switch(config)#hostname Branch_2960
Branch_2960(config)#ip domain-name ExamCram.net
Branch_2960(config)#crypto key generate rsa
Branch_2960(config)#username admin password ciscocisco
Branch_2960(config)#line vty 0 4
Branch_2960(config-line)#login
Branch_2960(config-line)#login local
Branch_2960(config-line)#transport input ssh
Branch_2960(config-line)#exit
```

In global configuration mode, you can use the command **ip ssh version 2**. Multiple versions of SSH are available, with Version 2 being more secure than Version 1. The command **show ip ssh** verifies that SSH is configured. The command **show ssh** shows current SSH connections to the router or switch.

You can the use of a username and password for access via Telnet or SSH by using the command **login local** on the vty line. The username required must be configured on the router as well as in global configuration mode when using **login local**.

You may use an access control list (ACL) and apply it to the vty lines to control which source addresses can connect. In addition, you can set timeouts for inactive sessions on the vty lines.

A remote AAA server may be used to control the authentication, instead of using a local username configured on the router.

Banner messages with legal warnings may also be set up on the router, via the **banner** command.

Port security is a feature used on Layer 2 switch interfaces to control the number of MAC addresses associated with that interface. When enabled, this feature allows a maximum of one MAC address to be associated with this interface. A violation of this policy results in a shutdown of the port by default. To verify port security details, use the command **show port-security**.

## Switch Operations and Configuration

The most common physical media used for Ethernet networks is twisted pair. Fiber-optic cabling allows for transmission at higher data rates over longer distances.

Ethernet physical addressing = MAC addresses. 12 hexadecimal digits.

PC to switch/hub = Straight-through cable.

Hub-hub, switch-switch, PC-PC, router-router, PC-router directly (no switch/hub): Use crossover cable.

Switches, bridges, and routers segment a network. Hubs and repeaters *extend* a network.

Switches increase the number of collision domains. Do not segment broadcast domains. Routers, Layer 3 switches, and VLANs segment broadcast domains.

A switch is a multiport bridge. Switches forward frames using hardware application-specific integrated circuits (ASIC), making them faster than bridges. Dedicated bandwidth per port.

Bridges and switches learn MACs by reading the source MAC of each frame.

Half duplex: Shared collision domain and lower throughput.

Full duplex: Point-to-point and higher throughput. Allows both ends to transmit simultaneously.

To remotely manage a switch, you need an IP address, subnet mask, and default gateway. The switch must be reachable on a port in its management VLAN.

VLANs logically divide a switch into multiple, independent networks at Layer 2.

Create separate broadcast domains in a switch, increasing the number of broadcast domains.

Span multiple switches using trunks.

Allow logical grouping of users by function.

VLAN configuration steps:

1. The VLAN must be created.
2. The desired ports must be added to the new VLAN.

Routing between VLANs requires a router or a Layer 3 switch.

Trunks carry traffic from multiple VLANs over a single connection (crossover cable). The VLAN ID is tagged using IEEE 802.1Q.

Spanning Tree Protocol (STP) provides a loop-free topology. STP does the following:

- Elects a root bridge (lowest bridge ID)
- Elects a root port for each nonroot bridge/switch (best cost, then lowest bridge ID)
- Elects a designated port for each segment
- Blocks ports (on nonroot switches) to prevent Layer 2 loops

STP cost for 100M is 19; the cost for 1G is 4.

STP port roles are as follows:

- Root port: Port forwarding toward the root bridge.
- Designated port/forwarding: Port forwarding away from the root bridge. (All ports on the root are designated.)
- Nondesignated/discarding port: Blocking/discarding frames of data.

STP types are as follows:

- 802.1D: Traditional STP
- PVST+: Cisco's enhancements to STP, allowing separate STP for each VLAN
- 802.1w: Rapid Spanning Tree, converges faster and uses features from Cisco's enhancements
- Rapid PVST+: Rapid Spanning Tree, with support for separate STP for each VLAN

The bridge ID is combination of priority, the extended system ID (VLAN number), and the base MAC address of the switch.

Priority can be changed to a lower value to cause a switch to become the root.

PortFast can reduce the time for a port to move to a forwarding state.

BPDU Guard can protect a port from seeing bridge protocol data units (BPDUs), by shutting down the port if BPDUs are seen.

EtherChannel combines multiple physical interfaces, to make them appear as a single logical interface, allowing spanning to forward across that logical interface and not waste potential bandwidth. An EtherChannel has built-in redundancy with multiple interfaces. EtherChannel can be negotiated using the Cisco proprietary Port Aggregation Protocol (PAgP) or the IEEE standard Link Aggregation Control Protocol (LACP). Static EtherChannel can also be configured manually. Cisco PAgP options are Auto and Desirable. LACPs options are Active and Passive. The following table shows the results of EtherChannel negotiations:

| Method | First Switch | Second Switch | Result |
|---|---|---|---|
| PAgP | Desirable | Desirable | Success |
| PAgP | Desirable | Auto | Success |
| PAgP | Auto | Auto | Failure |
| LACP | Active | Active | Success |
| LACP | Active | Passive | Success |
| LACP | Passive | Passive | Failure |

## Basic Routing

Routers enable communication between networks. The primary function of a router is to determine which path to use and to then forward packets.

Interior gateway protocols (IGPs) (such as Open Shortest Path First [OSPF] and Enhanced Interior Gateway Routing Protocol [EIGRP]) are routing protocols in the same domain, and exterior gateway protocols (EGPs) (such as Border Gateway Protocol [BGP]) is a routing protocol that is used between different entities/companies.

A router uses the longest match in its routing table to make a forwarding decision. If multiple routes exist for the same network, the router uses the one with the lowest administrative distance. When there are multiple routes to the same network and they have the same administrative distance, the metric or cost (lower being better) is used.

Default administrative distances for routing protocols are as follows:

| | |
|---|---|
| Connected interface | 0 |
| Static route | 1 |
| EIGRP internal | 90 |
| OSPF | 110 |
| RIP | 120 |

Routes can be learned from a router being directly connected to a network, by running a routing protocol and dynamically learning routes from another router that is running the same protocol, or by configuring a static route.

The following example shows the configuration of a static route to the network 192.168.1.0/24 using the next local hop of 10.1.1.1:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

The default route syntax, using a default next hop of 192.168.1.1, is as follows:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Link-state routing protocols send updates containing the state of their own links to all other routers on the network. Examples are OSPF and Intermediate System-to-Intermediate System (IS-IS). They calculate the paths to each destination from the topological database and place the best of them into the routing table.

Route summarization/aggregation/supernetting represents several networks/subnets as one larger network address, by shortening the subnet mask to include only the "in-common" bits from all the networks.

Summarizing is a process of moving the mask to the left. For instance, subnet 172.16.1.0/24 and 172.16.2.0/24 could both be summarized by using 172.16.0.0/22.

For OSPF, the router ID is the configured router ID. If no router ID is configured, the highest IP address on a loopback interface is used. If there are no loopback interfaces, the router ID will be the highest IP address on any other interface.

For two routers to become OSPF neighbors, they must agree on the area, the network, the authentication and the timers.

To configure OSPF, we enable a process and include a network statement as shown here:

```
Router(config)#router ospf 7

Router(config-router)#network 192.168.16.0  0.0.0.255 area 0
```

You can use the command **show ip route** to see the routing table.

Routing between VLANs can be done through an external router using the router-on-a-stick concept, or can be done internally by a multilayer switch that will do the Layer 3 routing between the subnets that are associated with each of the VLANs. When using a router to route between VLANs, using router on a stick, the switch is configured as a trunk link, and the router is configured with subinterfaces.

## Visualizing Data Flows

To communicate on an IP network, the computer needs to use an IP address. Name resolution is done through DNS. For devices to communicate on their own local network, they use ARP to discover the Layer 2 addresses of the local devices they want to communicate with. When communicating with a remote device, a local computer uses ARP to discover the Layer 2 address of its default gateway. ARP entries may be cached to avoid having to use ARP time.

Routers look at Layer 3 destination addresses, and based on their routing tables forward packets to the next logical hop in the path toward that destination.

## Access Lists

An access control list is a method to identify specific traffic. One use of an ACL is to filter traffic at an interface. ACLs are processed in a top-down fashion and may be applied to an interface inbound or outbound from the perspective of the interface it is applied to.

Implicit deny any at end: Every access list must have at least one permit; otherwise, it denies all traffic.

Standard IP access lists filter the entire IP protocol based on the source IP address/network. Standard ACL numbers range from 1 to 99. Place as close to destination as possible.

Extended IP access lists filter based on the source IP address/network, destination IP address/network, specific protocols (TCP, UDP, ICMP, and so on), and port number. Place as close to the source as possible. Extended ACL numbers range from 100 to 199 and 2000 to 2699.

One access list per direction per protocol per interface.

Wildcard mask: 0s match; 1s ignore the corresponding bit in the address.

The extended access list syntax is as follows:

```
access-list list#[permit | deny] [protocol] [source ip] [WCmask] [dest. ip][WCmask] [operator] [operand]
```

In general, place more specific statements at the top of the ACL and more general statements at the bottom. ACLs are processed from top to bottom and stop when a match occurs.

## WANs

WANs are networks that operate beyond the small geographic scope of a LAN. WANs connect two or more LANs together. WANs can use a Channel Service Unit/Data Service Unit (CSU/DSU) in combination with serial interfaces, or a CSU/DSU could be built in to an interface. Customer routers act Data Terminal Equipment (DTE), and the service provider connections to the customer are Data Circuit-Terminating Equipment (DCE), providing clocking. WAN options include digital subscriber line (DSL), cable, Ethernet, and fiber connectivity to a provider.

WAN Layer 2 protocols include PPP, HDLC, Frame Relay, DSL, PPPoE/A, Ethernet, and ATM.

WAN connection options include dedicated, circuit switched, or packet-switched.

The default encapsulation on the Cisco serial interface is Cisco's proprietary HDLC.

If you are using PPP, authentication options include Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

PPP uses Link Control Protocol (LCP) to negotiate a connection between the two ends of a PPP connection.

For CHAP authentication, the remote device must have a corresponding username entry for the local router with a matching password.

Frame Relay is a connection-oriented packet-switching service.

A permanent virtual circuit (PVC) is a point-to-point path from the service provider. Each end is identified with a local data-link connection identifier (DLCI). The local DLCI is used in mapping the remote IP address that is reachable via the local DLCI (called a Frame Relay map). Frame Relay maps may be automatically discovered or administratively configured. Local Management Interface (LMI) is a signaling standard between the local router and the service provider's Frame Relay switch. LMI can use three different standards between the router and the Frame Relay switch: Cisco, ANSI, and Q.933. Frame topologies include hub and spoke, full mesh, partial mesh, and point to point. Frame Relay subinterfaces can be used to overcome split-horizon issues. A subinterface may be point to point, with only the local router and the remote router on the WAN subnet connecting them together, or it could be configured as a multipoint, where three or more routers are connected to the same logical subnet over the Frame Relay network.

Virtual private networks (VPNs) have two major categories: site to site and remote access. They allow communications over untrusted networks (such as the Internet) and provide confidentiality through encryption, data integrity through hashing, and user verification through authentication. VPNs can be implemented using IPsec or Secure Shell (SSL). The Cisco AnyConnect VPN client supports both.

Generic routing encapsulation (GRE) is a tunneling protocol. A logical GRE tunnel could be created on top of another network (such as the Internet). The tunnel could be protected by IPsec. GRE uses protocol 47. It can be used to send traffic that would normally not be supported over the transport network. For example, IPv6 could be carried in a GRE tunnel as it is being sent over an IPv4 network.

## IP Services

IP addresses can be delivered via Dynamic Host Configuration Protocol (DHCP). DHCP can include information about the DNS server that should be used, in addition to a default gateway for the client to use.

If no DHCP server is present on a local network, a router could be configured as a DHCP relay that could forward the DHCP requests to a DHCP server.

Network Address Translation can be configured on a one-to-one mapping (NAT), or a one to many mapping (PAT, Port Address Translation).

NAT maps an IP address to a different address.

- **Static: ip nat inside source static** [*inside ip*] [*outside ip*]
- **Inside local:** A private IP address assigned to a host on the inside network
- **Inside global:** A registered Internet address that represents an inside host to an outside network
- **Outside global:** The registered address of an Internet host
- **Outside local:** The address of the Internet host as it appears on the inside network

Here is a PAT configuration example using a pool of addresses to translate to (named MyPool, starting with 24.17.5.1 and ending with 24.17.5.14):

```
access-list 1 permit 192.168.2.0 0.0.0.255

ip nat pool MyPool 24.17.5.1 24.17.5.14 netmask 255.255.255.240

ip nat inside source list 1 pool MyPool overload

interface Ethernet 0

ip nat inside

interface serial 0

ip nat outsid)
```

Network Time Protocol (NTP) provides time synchronization between network devices. NTP may be used to synchronize the time on the local router or switch with an NTP server. The commands **show ntp associations** and **show ntp status** can verify the state of the NTP.

To provide fault-tolerant default gateways, a first hop redundancy protocol (FHRP) may be used. These include the following:

- **Virtual Router Redundancy Protocol (VRRP):** Open standard
- **Hot Standby Router Protocol (HSRP):** Cisco proprietary
- **Gateway Load Balancing Protocol (GLBP):** Cisco proprietary

HSRP uses a single router to forward traffic for a single subnet, at any given time.

GLBP can load balance the traffic of a single subnet across multiple forwarders (routers) running GLBP.

Both use a virtual IP address that the clients can learn via DHCP to use a default gateway.

## Troubleshooting

Troubleshooting tools include **ping**, **telnet**, **tracert**, and **show** commands to verify the status of interface, the contents or routing tables, and the current ability to communicate with local or remote IP devices. A duplex mismatch could cause performance degradation.

One method of troubleshooting involves using the OSI model to determine at which point the network is no longer functioning.

The **show interface** command could assist us in validating Layers 1 and 2 locally. The **show CDP neighbors** command could validate Layer 2 between a local Cisco device and another directly connected Cisco device. A **ping** command could verify Layer 3 connectivity to another device. You can use a **telnet** command to verify Layer 4 and application layer connectivity.

You can use the **traceroute** command to validate the path and help to isolate a routing issue on the network.

The commands **show ip nat translations** and **show ip nat statistics** can help you determine whether NAT is working.

The command **show access-lists** shows the contents of ACLs, and **show ip interface** shows whether an ACL is applied as a filtering ACL (inbound or outbound) on an interface.

To troubleshoot or verify DHCP functions, you could use the following commands on the IOS router acting as a DHCP server: **show ip dhcp pool**, **show ip dhcp binding**, **show ip dhcp conflict**.

When troubleshooting OSPF, verify that you can reach the neighbor with a ping to verify Layers 1–3, and then use **show ip protocols** or **show ip ospf int brief** to verify that the interfaces are enabled for OSPF and **show ip ospf interface** to see the details such as timers. The command **show ip ospf neighbor** shows current OSPF neighbors.

You can verify the routing table on a router by using the **show ip route** command. For IPv6, the command is **show ipv6 route**. To verify the details of routing protocols such as OSPF and EIGRP, use **show ip protocols**.

If a client can ping based on IP address, but not based on a name, a DNS failure could be the cause. The client command of **nslookup** could be used to validate a reachable DNS server.

For troubleshooting serial interfaces, the following commands prove useful:

- **show controllers:** Validate the type of cable connected and validate that clocking is being received from the DCE
- **show interface:** Verify that interfaces are up at Layer 1 and Layer 2
- **debug ppp authentication:** See whether the PPP authentication is passing or failing
- **ping:** Validate that the other side can be reached

On Frame Relay, you can use the command **show frame-relay lmi** to verify the LMI between the router and the Frame Relay switch. The **show frame-relay map** command shows the current mappings being used by the router, and **show frame-relay pvc** shows the PVCs provided by the switch.

Commands to troubleshoot EIGRP include the following:

- **show ip eigrp neighbors**
- **show ip int brief**
- **show ip eigrp interface**
- **show ip protocols**
- **show ip route**

The commands for troubleshooting IPv6 EIGRP are similar, using the command **ipv6** in place of **ip** for many of the commands.

Commands to troubleshoot OSPF include the following:

- **show ip ospf neighbors**
- **show ip int brief**
- **show ip ospf**
- **show ip ospf interface**
- **show ip protocols**
- **show ip route**

The commands for troubleshooting IPv6 OSPFv3 are similar, using the command **ipv6** in place of **ip** for many of the commands.

You can use the **show spanning-tree** command to validate the following:

- Root bridge ID
- State of ports (root port, designated port, blocking port)
- Mode of STP being used (802.1w versus 802.1D)