### **Enterprise Networking, Security, and Automation**

**Module 1**

**OSPF Features and Characteristics**

Open Shortest Path First (OSPF) is a link-state routing protocol that was developed as an alternative for the distance vector Routing Information Protocol (RIP). OSPF has significant advantages over RIP in that it offers faster convergence and scales to much larger network implementations. OSPF is a link-state routing protocol that uses the concept of areas for scalability. A link is an interface on a router. A link is also a network segment that connects two routers, or a stub network such as an Ethernet LAN that is connected to a single router. All link-state information includes the network prefix, prefix length, and cost. All routing protocols use routing protocol messages to exchange route information. The messages help build data structures, which are then processed using a routing algorithm. Routers running OSPF exchange messages to convey routing information using five types of packets: the Hello packet, the database description packet, the link-state request packet, the link-state update packet, and the link-state acknowledgment packet. OSPF messages are used to create and maintain three OSPF databases: the adjacency database creates the neighbor table, the link-state database (LSDB) creates the topology table, and the forwarding database creates the routing table. The router builds the topology table using results of calculations based on the Dijkstra SPF (shortest-path first) algorithm. The SPF algorithm is based on the cumulative cost to reach a destination. In OSPF, cost is used to determine the best path to the destination. To maintain routing information, OSPF routers complete a generic link-state routing process to reach a state of convergence:

1. Establish Neighbor Adjacencies
2. Exchange Link-State Advertisements
3. Build the Link State Database
4. Execute the SPF Algorithm
5. Choose the Best Route

With single-area OSPF any number can be used for the area, best practice is to use area 0. Single-area OSPF is useful in smaller networks with few routers. With multiarea OSPF, one large routing domain can be divided into smaller areas, to support hierarchical routing. Routing still occurs between the areas (interarea routing), while many of the processor intensive routing operations, such as recalculating the database, are kept within an area. OSPFv3 is the OSPFv2 equivalent for exchanging IPv6 prefixes. Recall that in IPv6, the network address is referred to as the prefix and the subnet mask is called the prefix-length.

**OSPF Packets**

OSPF uses the following link-state packets (LSPs) to establish and maintain neighbor adjacencies and exchange routing updates: 1 Hello, 2 DBD, 3 LSR, 4 LSU, and 5 LSAck. LSUs are also used to forward OSPF routing updates, such as link changes. Hello packets are used to:

* Discover OSPF neighbors and establish neighbor adjacencies.
* Advertise parameters on which two routers must agree to become neighbors.
* Elect the Designated Router (DR) and Backup Designated Router (BDR) on multiaccess networks like Ethernet. Point-to-point links do not require DR or BDR.

Some important fields in the Hello packet are type, router ID, area ID, network mask, hello interval, router priority, dead interval, DR, BDR and list of neighbors.

**OSPF Operation**

When an OSPF router is initially connected to a network, it attempts to:

* Create adjacencies with neighbors
* Exchange routing information
* Calculate the best routes
* Reach convergence

The states that OSPF progresses through to do this are down state, init state, two-way state, ExStart state, Exchange state, loading state, and full state. When OSPF is enabled on an interface, the router must determine if there is another OSPF neighbor on the link by sending a Hello packet that contains its router ID out all OSPF-enabled interfaces. The Hello packet is sent to the reserved All OSPF Routers IPv4 multicast address 224.0.0.5. Only OSPFv2 routers will process these packets. When a neighboring OSPF-enabled router receives a Hello packet with a router ID that is not within its neighbor list, the receiving router attempts to establish an adjacency with the initiating router. After the Two-Way state, routers transition to database synchronization states, which is a three step process:

1. Decide First Router
2. Exchange DBDs
3. Send an LSR

Multiaccess networks can create two challenges for OSPF regarding the flooding of LSAs: the creation of multiple adjacencies and extensive flooding of LSAs. A dramatic increase in the number of routers also dramatically increases the number of LSAs exchanged between the routers. This flooding of LSAs significantly impact the operation of OSPF. If every router in a multiaccess network had to flood and acknowledge all received LSAs to all other routers on that same multiaccess network, the network traffic would become quite chaotic. This is why DR and BDR election is necessary. On multiaccess networks, OSPF elects a DR to be the collection and distribution point for LSAs sent and received. A BDR is also elected in case the DR fails.

**Module 2**

**OSPF Router ID**

OSPFv2 is enabled using the **router ospf** process-id global configuration mode command. The process-id value represents a number between 1 and 65,535 and is selected by the network administrator. An OSPF router ID is a 32-bit value, represented as an IPv4 address. The router ID is used by an OSPF-enabled router to synchronize OSPF databases and participate in the election of the DR and BDR. Cisco routers derive the router ID based on one of three criteria, in the following preferential order:

1. The router ID is explicitly configured using the OSPF **router-id** rid router configuration mode command. The rid value is any 32-bit value expressed as an IPv4 address.
2. If the router ID is not explicitly configured, the router chooses the highest IPv4 address of any of configured loopback interfaces.
3. If no loopback interfaces are configured, then the router chooses the highest active IPv4 address of any of its physical interfaces.

The router ID can be assigned to a loopback interface. The IPv4 address for this type of loopback interface should be configured using a 32-bit subnet mask (255.255.255.255), creating a host route. A 32-bit host route would not get advertised as a route to other OSPF routers. After a router selects a router ID, an active OSPF router does not allow the router ID to be changed until the router is reloaded or the OSPF process is reset. Use the **clear ip ospf process** command to reset the adjacencies. You can then verify that R1 is using the new router ID command with the **show ip protocols** command piped to display only the router ID section.

**Point-to-Point OSPF Networks**

The network command is used to determine which interfaces participate in the routing process for an OSPFv2 area. The basic syntax for the **network** command is **network** network-address wildcard-mask **area** area-id. Any interfaces on a router that match the network address in the **network** command can send and receive OSPF packets. When configuring single-area OSPFv2, the **network** command must be configured with the same area-id value on all routers. The wildcard mask is typically the inverse of the subnet mask configured on that interface. In a wildcard mask:

* **Wildcard mask bit 0** - Matches the corresponding bit value in the address
* **Wildcard mask bit 1** - Ignores the corresponding bit value in the address

Within routing configuration mode, there are two ways to identify the interfaces that will participate in the OSPFv2 routing process. One way is when the wildcard mask identifies the interface based on the network addresses. Any active interface that is configured with an IPv4 address belonging to that network will participate in the OSPFv2 routing process. The other way is OSPFv2 can be enabled by specifying the exact interface IPv4 address using a quad zero wildcard mask. To configure OSPF directly on the interface, use the **ip ospf** interface configuration mode command. The syntax is **ip ospf** process-id **area** area-id. Sending out unneeded messages on a LAN affects the network through inefficient use of bandwidth and resources, and creates an increased security risk. Use the **passive-interface** router configuration mode command to stop transmitting routing messages through a router interface, but still allow that network to be advertised to other routers. The **show ip protocols** command is then used to verify that the Loopback 0 interface is listed as passive. The DR/ BDR election process is unnecessary as there can only be two routers on the point-to-point network between R1 and R2. Use the interface configuration command **ip ospf network point-to-point** on all interfaces where you want to disable the DR/BDR election process. Use loopbacks to simulate more networks than the equipment can support. By default, loopback interfaces are advertised as /32 host routes. To simulate a real LAN, the Loopback 0 interface is configured as a point-to-point network.

**OSPF Network Types**

Routers can be connected to the same switch to form a multiaccess network. Ethernet LANs are the most common example of broadcast multiaccess networks. In broadcast networks, all devices on the network see all broadcast and multicast frames. The DR is responsible for collecting and distributing LSAs . The DR uses the multicast IPv4 address 224.0.0.5 which is meant for all OSPF routers. If the DR stops producing Hello packets, the BDR promotes itself and assumes the role of DR. All other routers become a DROTHER. DROTHERs use the multiaccess address 224.0.0.6 (all designated routers) to send OSPF packets to the DR and BDR. Only the DR and BDR listen for 224.0.0.6. To verify the roles of the OSPFv2 router, use the **show ip ospf interface** command. To verify the OSPFv2 adjacencies, use the **show ip ospf neighbor** command. The state of neighbors in multiaccess networks can be:

* **FULL/DROTHER** - This is a DR or BDR router that is fully adjacent with a non-DR or BDR router.
* **FULL/DR** - The router is fully adjacent with the indicated DR neighbor.
* **FULL/BDR** - The router is fully adjacent with the indicated BDR neighbor.
* **2-WAY/DROTHER** - The non-DR or BDR router has a neighbor relationship with another non-DR or BDR router.

The OSPF DR and BDR election decision is based on the following criteria, in sequential order:

1. The routers in the network elect the router with the highest interface priority as the DR. The router with the second highest interface priority is elected as the BDR. The priority can be configured to be any number between 0 – 255. If the interface priority value is set to 0, that interface cannot be elected as DR nor BDR. The default priority of multiaccess broadcast interfaces is 1. Therefore, unless otherwise configured, all routers have an equal priority value and must rely on another tie breaking method during the DR/BDR election.
2. If the interface priorities are equal, then the router with the highest router ID is elected the DR. The router with the second highest router ID is the BDR.

OSPF DR and BDR elections are not pre-emptive. If the DR fails, the BDR is automatically promoted to DR. This is the case even if another DROTHER with a higher priority or router ID is added to the network after the initial DR/BDR election. However, after a BDR is promoted to DR, a new BDR election occurs and the DROTHER with the highest priority or router ID is elected as the new BDR. To set the priority of an interface, use the command **ip ospf priority** value, where value is 0 to 255. If the value is 0, the router will not become a DR or BDR. If the value is 1 to 255, then the router with the higher priority value will more likely become the DR or BDR on the interface.

**Modify Single-Area OSPFv2**

OSPF uses cost as a metric. A lower cost indicates a better path than a higher cost. The Cisco cost of an interface is inversely proportional to the bandwidth of the interface. Therefore, a higher bandwidth indicates a lower cost. The formula used to calculate the OSPF cost is: Cost = reference bandwidth / interface bandwidth. Because the OSPF cost value must be an integer, FastEthernet, Gigabit Ethernet, and 10 GigE interfaces share the same cost. To correct this situation, you can adjust the reference bandwidth with the **auto-cost reference-bandwidth** command on each OSPF router, or manually set the OSPF cost value with the **ip ospf cost** command. To adjust the reference bandwidth, use the **auto-cost reference-bandwidth** Mbps router configuration command. The cost of an OSPF route is the accumulated value from one router to the destination network. OSPF cost values can be manipulated to influence the route chosen by OSPF. To change the cost value report by the local OSPF router to other OSPF routers, use the interface configuration command **ip ospf cost** value. If the Dead interval expires before the routers receive a Hello packet, OSPF removes that neighbor from its link-state database (LSDB). The router floods the LSDB with information about the down neighbor out all OSPF-enabled interfaces. Cisco uses a default of 4 times the Hello interval or 40 seconds on multiaccess and point-to-point networks. To verify the OSPFv2 interface intervals, use the **show ip ospf interface** command. OSPFv2 Hello and Dead intervals can be modified manually using the following interface configuration mode commands: **ip ospf hello-interval** seconds and **ip ospf dead-interval** seconds.

**Default Route Propagation**

In OSPF terminology, the router located between an OSPF routing domain and a non-OSPF network is called the ASBR. To propagate a default route, the ASBR must be configured with a default static route using the **ip route 0.0.0.0 0.0.0.0** [next-hop-address | exit-intf] command, and the **default-information originate** router configuration command. This instructs the ASBR to be the source of the default route information and propagate the default static route in OSPF updates. Verify the default route settings on the ASBR using the **show ip route** command.

**Verify Single-Area OSPFv2**

The following two commands are used to verify routing:

* **show ip interface brief** – Used to verify that the desired interfaces are active with correct IP addressing.
* **show ip route**- Used to verify that the routing table contains all the expected routes.

Additional commands for determining that OSPF is operating as expected include: **show ip ospf neighbor**, **show ip protocols**, **show ip ospf**, and **show ip ospf interface**.

Use the **show ip ospf neighbor** command to verify that the router has formed an adjacency with its neighboring routers. For each neighbor, this command displays:

* **Neighbor ID** - The router ID of the neighboring router.
* **Pri** - The OSPFv2 priority of the interface. This value is used in the DR and BDR election.
* **State** - The OSPFv2 state of the interface. FULL state means that the router and its neighbor have identical OSPFv2 LSDBs. On multiaccess networks, such as Ethernet, two routers that are adjacent may have their states displayed as 2WAY. The dash indicates that no DR or BDR is required because of the network type.
* **Dead Time** - The amount of time remaining that the router waits to receive an OSPFv2 Hello packet from the neighbor before declaring the neighbor down. This value is reset when the interface receives a Hello packet.
* **Address** - The IPv4 address of the neighbor’s interface to which this router is directly connected.
* **Interface** - The interface on which this router has formed adjacency with the neighbor.

The **show ip protocols** command is a quick way to verify vital OSPF configuration information such as the OSPFv2 process ID, the router ID, interfaces explicitly configured to advertise OSPF routes, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for OSPF. Use the **show ip ospf** command to examine the OSPFv2 process ID and router ID. This command displays the OSPFv2 area information and the last time the SPF algorithm was executed. The **show ip ospf interface** command provides a detailed list for every OSPFv2-enabled interface. Specify an interface for just one interface to display the process ID, the local router ID, the type of network, OSPF cost, DR and BDR information on multiaccess links, and adjacent neighbors.

**Module 3**

Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people’s privacy, and compromise the integrity of information. Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack. An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network.

The term ‘threat actor’ includes hackers and any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack. There are “White Hat”, “Gray Hat”, and “Black Hat” hackers. Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and more. Hacktivists tend to rely on fairly basic, freely available tools. State-sponsored hackers create advanced, customized attack code, often using previously undiscovered software vulnerabilities called zero-day vulnerabilities.

Attack tools have become more sophisticated and highly automated. These new tools require less technical knowledge to implement. Ethical hacking involves many different types of tools used to test the network and keep its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. Common types of attacks are: eavesdropping, data modification, IP address spoofing, password-based, denial-of-service, man-in-the-middle, compromised-key, and sniffer.

The three most common types of malware are worms, viruses, and Trojan horses. A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. A virus executes a specific unwanted, and often harmful, function on a computer. A Trojan horse is non-self-replicating. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within. Other types of malware are: adware, ransomware, rootkit, and spyware.

Networks are susceptible to the following types of attacks: reconnaissance, access, and DoS. Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. Types of access attacks are: password, spoofing, trust exploitations, port redirections, man-in-the-middle, and buffer overflow. Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. DoS and DDoS are attacks that create some sort of interruption of network services to users, devices, or applications.

Threat actors can send packets using a spoofed source IP address. Threat actors can also tamper with the other fields in the IP header to carry out their attacks. IP attack techniques include: ICMP, amplification and reflection, address spoofing, MITM, and session hijacking. Threat actors use ICMP for reconnaissance and scanning attacks. They launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors often use amplification and reflection techniques to create DoS attacks.

TCP segment information appears immediately after the IP header. TCP provides reliable delivery, flow control, and stateful communication. TCP attacks include: TCPSYN Flood attack, TCP reset attack, and TCP Session hijacking. UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is not protected by encryption. UDP Flood attacks send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The result is very similar to a DoS attack.

Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” This mean that any host can claim to be the owner of any IP or MAC. A threat actor can poison the ARP cache of devices on the local network, creating an MITM attack to redirect traffic. ARP cache poisoning can be used to launch various man-in-the-middle attacks. DNS attacks include: open resolver attacks, stealth attacks, domain shadowing attacks, and tunneling attacks. To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic. A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

Most organizations follow the CIA information security triad: confidentiality, integrity, and availability. To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. This is known as defense-in-depth. A firewall is a system, or group of systems, that enforces an access control policy between networks. To defend against fast-moving and evolving attacks, you may need an intrusion detection systems (IDS), or the more scalable intrusion prevention systems (IPS).

The four elements of secure communications are data integrity, origin authentication, data confidentiality, and data non-repudiation. Hash functions guarantee that message data has not changed accidentally or intentionally. Three well-known hash functions are MD5 with 128-bit digest, SHA hashing algorithm, and SHA-2. To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC). HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key. Symmetric encryption algorithms using DES, 3DES, AES, SEAL, and RC are based on the premise that each communicating party knows the pre-shared key. Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI). Diffie-Hellman (DH) is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before.

**Module 4**

**Purpose of ACLs**

Several tasks performed by routers require the use of ACLs to identify traffic. An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. A router does not have any ACLs configured by default. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if the packet can be forwarded. An ACL uses a sequential list of permit or deny statements, known as ACEs. Cisco routers support two types of ACLs: standard ACLs and extended ACLs. An inbound ACL filters packets before they are routed to the outbound interface. If the packet is permitted by the ACL, it is then processed for routing. An outbound ACL filters packets after being routed, regardless of the inbound interface. When an ACL is applied to an interface, it follows a specific operating procedure:

1. The router extracts the source IPv4 address from the packet header.
2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE in a sequential order.
3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

**Wildcard Masks**

An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol. A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, they differ in the way they match binary 1s and 0s. **Wildcard mask bit 0** matches the corresponding bit value in the address. **Wildcard mask bit 1** ignores the corresponding bit value in the address. A wildcard mask is used to filter traffic for one host, one subnet, and a range IPv4 addresses. A shortcut to calculating a wildcard mask is to subtract the subnet mask from 255.255.255.255. Working with decimal representations of binary wildcard mask bits can be simplified by using the Cisco IOS keywords **host** and **any** to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read the ACE.

**Guidelines for ACL creation**

There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (i.e, IPv4 and IPv6) router interface can have up to four ACLs applied. Specifically, a router interface can have one outbound IPv4 ACL, one inbound IPv4 ACL, one inbound IPv6 ACL , and one outbound IPv6 ACL. ACLs do not have to be configured in both directions. The number of ACLs and their direction applied to the interface will depend on the security policy of the organization. Basic planning is required before configuring an ACL and includes the following best practices:

* Base ACLs on the organizational security policies.
* Write out what you want the ACL to do.
* Use a text editor to create, edit, and save all of your ACLs.
* Document the ACLs using the **remark** command.
* Test the ACLs on a development network before implementing them on a production network.

**Types of IPv4 ACLs**

There are two types of IPv4 ACLs: standard ACLs and Extended ACLs. Standard ACLs permit or deny packets based only on the source IPv4 address. Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. ACLs number 1 -to 99, or 1300 to 1999, are standard ACLs. ACLs number 100-199, or 2000 to 2699, are extended ACLs. Named ACLs is the preferred method to use when configuring ACLs. Specifically, standard and extended ACLs can be named to provide information about the purpose of the ACL.

The following summarizes the rules to follow for named ACLs:

* Assign a name to identify the purpose of the ACL.
* Names can contain alphanumeric characters.
* Names cannot contain spaces or punctuation.
* It is suggested that the name be written in CAPITAL LETTERS.
* Entries can be added or deleted within the ACL.

Every ACL should be placed where it has the greatest impact on efficiency. Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure. Standard ACLs should be located as close to the destination as possible. If a standard ACL was placed at the source of the traffic, the "permit" or "deny" will occur based on the given source address no matter where the traffic is destined. Placement of the ACL may depend on the extent of organizational control, bandwidth of the networks, and ease of configuration.

**Module 5**

**Configure Standard IPv4 ACLs**

All access control lists (ACLs) must be planned, especially for ACLs requiring multiple access control entries (ACEs). When configuring a complex ACL, it is suggested that you use a text editor and write out the specifics of the policy to be implemented, add the IOS configuration commands to accomplish those tasks, include remarks to document the ACL, copy and paste the commands on a lab device, and always thoroughly test an ACL to ensure that it correctly applies the desired policy. To create a numbered standard ACL, use the **ip access-list** *access-list-number* global configuration command. Use the **no access-list** *access-list-number* global configuration command to remove a numbered standard ACL. Use the **show ip interface** command to verify if an interface has an ACL applied to it. In addition to standard numbered ACLs, there are named standard ACLs. ACL names are alphanumeric, case sensitive, and must be unique. Capitalizing ACL names is not required but makes them stand out when viewing the running-config output. To create a named standard ACL, use the **ip access-list standard** *access-list-name* global configuration command. Use the **no ip access-list** **standard** *access-list-name* global configuration command to remove a named standard IPv4 ACL. After a standard IPv4 ACL is configured, it must be linked to an interface or feature. To bind a numbered or named standard IPv4 ACL to an interface, use the **ip access-group** {*access-list-number* | *access-list-name*} { **in** | **out** } global configuration command. To remove an ACL from an interface, first enter the **no ip access-group** interface configuration command. To remove the ACL from the router, use the **no access-list** global configuration command.

**Modify IPv4 ACLs**

To modify an ACL, use a text editor or use sequence numbers. ACLs with multiple ACEs should be created in a text editor. This allows you to plan the required ACEs, create the ACL, and then paste it into the router interface. An ACL ACE can also be deleted or added using the ACL sequence numbers. Sequence numbers are automatically assigned when an ACE is entered. These numbers are listed in the **show access-lists** command. The **show running-config** command does not display sequence numbers. Named ACLs can also use sequence numbers to delete and add ACEs. The **show access-lists** command shows statistics for each statement that has been matched. The **clear access-list counters** command to clear the ACL statistics.

**Secure VTY Ports with a Standard IPv4 ACL**

ACLs typically filter incoming or outgoing traffic on an interface. However, a standard ACL can also be used to secure remote administrative access to a device using the vty lines. The two steps to secure remote administrative access to the vty lines are to create an ACL to identify which administrative hosts should be allowed remote access and to apply the ACL to incoming traffic on the vty lines. The **in** keyword is the most commonly used option to filter incoming vty traffic. The **out** parameter filters outgoing vty traffic and is rarely applied. Both named and numbered access lists can be applied to vty lines. Identical restrictions should be set on all the vty lines, because a user can attempt to connect to any of them. After the ACL to restrict access to the vty lines is configured, it is important to verify that it is working as expected. Use the **show ip interface** command to verify if an interface has an ACL applied to it. To verify the ACL statistics, issue the **show access-lists** command.

**Configure Extended IPv4 ACLs**

Extended ACLs are used more often than standard ACLs because they provide a greater degree of control. They can filter on source address, destination address, protocol (i.e., IP, TCP, UDP, ICMP), and port number. This provides a greater range of criteria on which to base the ACL. Like standard ACLs, extended ACLs can be created as numbered extended ACL and named extended ACL. Numbered Extended ACLs are created using the same global configuration commands that are used for standard ACLs. The procedural steps for configuring extended ACLs are the same as for standard ACLs. However, the command syntax and parameters are more complex to support the additional features provided by extended ACLs. To create a numbered extended ACL, use the Router(config)# **access-list** *access-list-number* {**deny** | **permit** | **remark** *text*} *protocol* *source source-wildcard* [*operator* [*port*]] *destination* *destination-wildcard* [*operator* [*port*]] [**established**] [**log**] global configuration command. Extended ACLs can filter on many different types of internet protocols and ports. Selecting a *protocol* influences *port* options. For instance, selecting the **tcp** protocol would provide TCP related ports options. Configuring the port number is required when there is not a specific protocol name listed such as SSH (port number 22) or HTTPS (port number 443). TCP can also perform basic stateful firewall services using the TCP **established** keyword. The keyword enables inside traffic to exit the inside private network and permits the returning reply traffic to enter the inside private network. After an ACL has been configured and applied to an interface, use Cisco IOS **show** commands to verify the configuration. The **show ip interface** command is used to verify the ACL on the interface and the direction in which it was applied.

**Module 6**

**NAT Characteristics**

There are not enough public IPv4 addresses to assign a unique address to each device connected to the internet. Private IPv4 addresses cannot be routed over the internet. To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must first be translated to a public address. NAT provides the translation of private addresses to public addresses. The primary use of NAT is to conserve public IPv4 addresses. It allows networks to use private IPv4 addresses internally and provides translation to a public address only when needed. When an internal device sends traffic out of the network, the NAT-enabled router translates the internal IPv4 address of the device to a public address from the NAT pool. In NAT terminology, the inside network is the set of networks that is subject to translation. The outside network refers to all other networks. When determining which type of address is used, it is important to remember that NAT terminology is always applied from the perspective of the device with the translated address:

* **Inside address** - The address of the device which is being translated by NAT.
* **Outside address** - The address of the destination device.

NAT also uses the concept of local or global with respect to addresses:

* **Local address** - A local address is any address that appears on the inside portion of the network.
* **Global address** - A global address is any address that appears on the outside portion of the network.

**Types of NAT**

Static NAT uses a one-to-one mapping of local and global addresses. These mappings are configured by the network administrator and remain constant. Static NAT is particularly useful for web servers or devices that must have a consistent address that is accessible from the internet, such as a company web server. Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions. Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Similar to static NAT, dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions. Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses. This is the most common form of NAT for both the home and the enterprise. PAT ensures that devices use a different TCP port number for each session with a server on the internet. PAT attempts to preserve the original source port. However, if the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group. PAT translates most common protocols carried by IPv4 that do not use TCP or UDP as a transport layer protocol. The most common of these is ICMPv4.

| Table caption | |
| --- | --- |
| **NAT** | **PAT** |
| One-to-one mapping between Inside Local and Inside Global addresses. | One Inside Global address can be mapped to many Inside Local address. |
| Uses only IPv4 addresses in translation process. | Uses IPv4 addresses and TCP or UDP source port numbers in translation process. |
| A unique Inside Global address is required for each inside host accessing the outside network. | A single unique Inside Global address can be shared by many inside hosts accessing the outside network. |

**NAT Advantages and Disadvantages**

Advantages: NAT conserves the legally registered addressing scheme by allowing the privatization of intranets. NAT increases the flexibility of connections to the public network. NAT provides consistency for internal network addressing schemes. NAT hides user IPv4 addresses.

Disadvantages: NAT increases forwarding delays because the translation of each IPv4 address within the packet headers takes time. The process of two layers of NAT translation is known as Carrier Grade NAT (CGN). End-to-end addressing is lost. Many internet protocols and applications depend on end-to-end addressing from the source to the destination. End-to-end IPv4 traceability is also lost. Using NAT also complicates the use of tunneling protocols, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

**Static NAT**

Static NAT is a one-to-one mapping between an inside address and an outside address. Static NAT allows external devices to initiate connections to internal devices using the statically assigned public address. The first task is to create a mapping between the inside local address and the inside global addresses using the **ip nat inside source static** command. After the mapping is configured, the interfaces participating in the translation are configured as inside or outside relative to NAT using the **ip nat inside** and **ip nat outside** commands. To verify NAT operation use the **show ip nat translations** command. To verify that the NAT translation is working, it is best to clear statistics from any past translations using the **clear ip nat statistics** command before testing.

**Dynamic NAT**

Dynamic NAT automatically maps the inside local addresses to inside global addresses. Dynamic NAT, like static NAT, requires the configuration of the inside and outside interfaces participating in NAT. Dynamic NAT uses a pool of addresses translating a single inside address to a single outside address. The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come first-served basis. With this type of translation there must be enough addresses in the pool to accommodate all the inside devices needing concurrent access to the outside network. If all addresses in the pool are in use, a device must wait for an available address before it can access the outside network.

To configure dynamic NAT, first define the pool of addresses that will be used for translation using the **ip nat pool** command. The addresses are defined by indicating the starting IPv4 address and the ending IPv4 address of the pool. The **netmask** or **prefix-length** keyword indicates which address bits belong to the network and which bits belong to the host for the range of addresses. Configure a standard ACL to identify (permit) only those addresses that are to be translated. Bind the ACL to the pool, using the following command syntax: Router(config)# **ip nat inside source list** {*access-list-number* | *access-list-name*} **pool** *pool-name*. Identify which interfaces are inside, in relation to NAT. Identify which interfaces are outside, in relation to NAT.

To verify dynamic NAT configurations, The output of the **show ip nat translations** command shown displays all static translations that have been configured and any dynamic translations that have been created by traffic. Adding the **verbose** keyword displays additional information about each translation, including how long ago the entry was created and used. By default, translation entries time out after 24 hours, unless the timers have been reconfigured with the **ip nat translation timeout** *timeout-seconds* command in global configuration mode. To clear dynamic entries before the timeout has expired, use the **clear ip nat translation** privileged EXEC mode command.

**PAT**

There are two ways to configure PAT, depending on how the ISP allocates public IPv4 addresses. In the first instance, the ISP allocates a single public IPv4 address that is required for the organization to connect to the ISP and in the other, it allocates more than one public IPv4 address to the organization. To configure PAT to use a single IPv4 address, simply add the keyword **overload** to the **ip nat inside source** command. The rest of the configuration is the similar to static and dynamic NAT configuration except that with PAT, multiple hosts can use the same public IPv4 address to access the internet. To configure PAT for a dynamic NAT address pool, simply add the keyword **overload** to the **ip nat inside source** command. Multiple hosts can share an IPv4 address from the pool because PAT is enabled with the keyword **overload**.

To verify PAT configurations us the **show ip nat translations** command. The source port numbers in the NAT table differentiate the transactions. The **show ip nat statistics** command verifies that the NAT-POOL has allocated a single address for multiple translations. Included in the output is information about the number and type of active translations, NAT configuration parameters, the number of addresses in the pool, and how many have been allocated.

**NAT64**

IPv6 was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary. However, IPv6 does include its own IPv6 private address space, unique local addresses (ULAs). IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4 but have a different purpose. ULA addresses are meant for only local communications within a site. ULA addresses are not meant to provide additional IPv6 address space, nor to provide a level of security; however, IPv6 does provide for protocol translation between IPv4 and IPv6 known as NAT64. NAT for IPv6 is used in a much different context than NAT for IPv4. The varieties of NAT for IPv6 are used to transparently provide access between IPv6-only and IPv4-only networks. To aid in the move from IPv4 to IPv6, the IETF has developed several transition techniques to accommodate a variety of IPv4-to-IPv6 scenarios, including dual-stack, tunneling, and translation. Dual-stack is when the devices are running protocols associated with both the IPv4 and IPv6. Tunneling for IPV6 is the process of encapsulating an IPv6 packet inside an IPv4 packet. This allows the IPv6 packet to be transmitted over an IPv4-only network. NAT for IPv6 should not be used as a long-term strategy, but as a temporary mechanism to assist in the migration from IPv4 to IPv6.

**Module 7**

**Purpose of WANs**

A Wide Area Network (WAN) is required to connect beyond the boundary of the LAN. A WAN is a telecommunications network that spans over a relatively large geographical area. A WAN operates beyond the geographic scope of a LAN. A private WAN is a connection that is dedicated to a single customer. A public WAN connection is typically provided by an ISP or telecommunications service provider using the internet. WAN topologies are described using a logical topology. WANs are implemented using the following logical topologies: Point-to-Point, Hub-and-Spoke, Dual-homed, Fully Meshed, and Partially Meshed. A single-carrier connection is when an organization connects to only one service provider. A dual-carrier connection provides redundancy and increases network availability. The organization negotiates separate SLAs with two different service providers. Network requirements of a company can change dramatically as the company grows over time. Distributing employees saves costs in many ways, but it puts increased demands on the network. Small companies may use a single LAN connected to a wireless router to share data and peripherals. Connection to the internet is through a broadband service provider. A slightly larger company may use a Campus Area Network (CAN). A CAN interconnects several LANs within a limited geographical area. An even larger company may require a metropolitan area network (MAN) to interconnect sites within the city. A MAN is larger than a LAN but smaller than a WAN. A global company may require teleworking and virtual teams using web-based applications, including web-conferencing, e-learning, and online collaboration tools. Site-to-site and remote access Virtual Private Networks (VPNs) enable the company to use the internet to securely connect with employees and facilities around the world.

**WAN Operations**

Modern WAN standards are defined and managed by a number of recognized authorities: TIA/EIA, ISO, and IEEE. Most WAN standards focus on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). Layer 1 protocols describe the electrical, mechanical, and operational components needed to transmit bits over a WAN. Layer 1 optical fiber protocol standards include SDH, SONET, and DWDM. Layer 2 protocols define how data will be encapsulated into a frame. Layer 2 protocols include broadband, wireless, Ethernet WAN, MPLS, PPP, HDLC. The WAN physical layer describes the physical connections between the company network and the service provider network. There are specific terms used to describe WAN connections between the subscriber (i.e., the company / client) and the WAN service provider: DTE, DCE, CPE, POP, Demarcation Point, Local Loop, CO, Toll network, Backhaul network, and Backbone network. The end-to-end data path over a WAN is usually from source DTE to the DCE, then to the WAN cloud, then to the DCE to and finally to the destination DTE. Devices used in this path include voiceband modem, DSL and Cable modems, CSU/DSU, Optical converter, wireless router or access point, and other WAN core devices. Serial communication transmits bits sequentially over a single channel. In contrast, parallel communications simultaneously transmit several bits using multiple wires. A circuit-switched network establishes a dedicated circuit (or channel) between endpoints before the users can communicate. During transmission over a circuit-switched network, all communication uses the same path. The two most common types of circuit-switched WAN technologies are PSTN and ISDN. Packet-switching segments traffic data into packets that are routed over a shared network. Common types of packet-switched WAN technologies are Ethernet WAN and MPLS. There are two optical fiber OSI layer 1 standards. SDH/SONET define how to transfer multiple data, voice, and video communications over optical fiber using lasers or LEDs over great distances. Both standards are used on the ring network topology that contains redundant fiber paths allowing traffic to flow in both directions. DWDM is a newer technology that increases the data-carrying capacity SDH and SONET by simultaneously sending multiple streams of data (multiplexing) using different wavelengths of light.

**Traditional WAN Connectivity**

In the 1980s, organizations started to see the need to interconnect their LANs with other locations. They needed their networks to connect to the local loop of a service provider by using dedicated lines or by using switched services from a service provider. When permanent dedicated connections were required, a point-to-point link using copper media was used to provide a pre-established WAN communications path from the customer premises to the provider network. Dedicated leased lines were T1/E1 or T3/E3 lines. Circuit-switched connections were provided by PSTN carriers. The local loop connecting the CPE to the CO was copper media. ISDN is a circuit-switching technology that enables the PSTN local loop to carry digital signals. This provided higher capacity switched connections than dialup access. Packet switching segments data into packets that are routed over a shared network. Packet-switching networks allow many pairs of nodes to communicate over the same channel. Frame Relay is a simple Layer 2 NBMA WAN technology used to interconnect enterprise LANs. ATM technology is capable of transferring voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture.

**Modern WAN Connectivity**

Modern WAN connectivity options include dedicated broadband, Ethernet WAN and MPLS (packet-switched), along with various wired and wireless version of internet-based broadband. Service providers now offer Ethernet WAN service using fiber-optic cabling. Ethernet WAN reduces expenses and administration, is easily integrated with existing networks, and enhances business productivity. MPLS is a high-performance service provider WAN routing technology to interconnect clients. MPLS supports a variety of client access methods (e.g., Ethernet, DSL, Cable, Frame Relay). MPLS can encapsulate all types of protocols including IPv4 or IPv6 traffic.

**Internet-Based Connectivity**

Internet-based broadband connectivity is an alternative to using dedicated WAN options. There are wired and wireless versions of broadband VPN. Wired options use permanent cabling e.g., copper or fiber) to provide consistent bandwidth, and reduce error rates and latency. Examples of wired broadband connectivity are Digital Subscriber Line (DSL), cable connections, and optical fiber networks. Examples of wireless broadband include cellular 3G/4G/5G or satellite internet services. DSL is a high-speed, always-on, connection technology that uses existing twisted-pair telephone lines to provide IP services to users. All forms of DSL are categorized as either ADSL or SDSL. The DSL modem converts the Ethernet signals from the teleworker device to a DSL signal, which is transmitted to a DSLAM at the provider location. The advantage that DSL has over cable technology is that DSL is not a shared medium. ISPs still use PPP as the Layer 2 protocol for broadband DSL connections. A DSL modem has a DSL interface to connect to the DSL network and an Ethernet interface to connect to the client device. Ethernet links do not natively support PPP. Cable technology is a high-speed always-on connection technology that uses a cable company coaxial cable to provide IP services to users. Cable operators deploy hybrid fiber-coaxial (HFC) networks to enable high-speed transmission of data to cable modems. The cable system uses a coaxial cable to carry radio frequency (RF) signals to the end user. Many municipalities, cities, and providers install fiber optic cable to the user location. This is commonly referred to as Fiber to the x (FTTx) and versions are FTTH, FTTB, and FTTN.

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device they are using. Until recently, one limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or a wireless modem that has a wired connection to the internet. Newer developments in wireless technology include Municipal Wi-Fi, Cellular, Satellite internet, and WiMAX. To address security concerns, broadband services provide capabilities for using Virtual Private Networks (VPN) connections to a network device that accepts VPN connections, which is typically located at the corporate site. A VPN is an encrypted connection between private networks over a public network, such as the internet. Instead of using a dedicated Layer 2 connection, such as a leased line, a VPN uses virtual connections called VPN tunnels. VPN tunnels are routed through the internet from the private network of the company to the remote site or employee host. Common VPN implementations include site-to-site and remote access. ISP connectivity options include single-homed, dual-homed, multihomed, and dual-multihomed. Cable, DSL, fiber-to-the-home, cellular/mobile, municipal Wi-Fi, and satellite internet all have advantages and disadvantages. Perform a cost-versus-benefit analysis before choosing an internet-based connectivity solution.

Module 8

A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network. A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network. Benefits of VPNs are cost savings, security, scalability, and compatibility. VPNs are commonly deployed in one of the following configurations: site-to-site or remote-access. VPNs can be managed and deployed as enterprise VPNs and service provider VPNs.

Remote-access VPNs let remote and mobile users securely connect to the enterprise by creating an encrypted tunnel. Remote access VPNs can be created using either IPsec or SSL. When a client negotiates an SSL VPN connection with the VPN gateway, it actually connects using TLS. SSL uses the public key infrastructure and digital certificates to authenticate peers. Site-to-site VPNs are used to connect networks across an untrusted network such as the internet. In a site-to-site VPN, end hosts send and receive normal unencrypted TCP/IP traffic through a VPN terminating device. The VPN terminating device is typically called a VPN gateway. A VPN gateway could be a router or a firewall. GRE is a non-secure site-to-site VPN tunneling protocol. DMVPN is a Cisco software solution for easily building multiple, dynamic, scalable VPNs. Like DMVPNs, IPsec VTI simplifies the configuration process required to support multiple sites and remote access. IPsec VTI configurations are applied to a virtual interface instead of static mapping the IPsec sessions to a physical interface. IPsec VTI can send and receive both IP unicast and multicast encrypted traffic. MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider. There are two types of MPLS VPN solutions supported by service providers, Layer 3 MPLS VPN and Layer 2 MPLS VPN.

IPsec protects and authenticates IP packets between source and destination. IPsec can protect traffic from Layer 4 through Layer 7. Using the IPsec framework, IPsec provides confidentiality, integrity, origin authentication, and Diffie-Hellman. Choosing the IPsec protocol encapsulation is the first building block of the framework. IPsec encapsulates packets using AH or ESP. The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm. The HMAC is an algorithm that guarantees the integrity of the message using a hash value. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. A PSK value is entered into each peer manually. The PSK is combined with other information to form the authentication key. RSA authentication uses digital certificates to authenticate the peers. The local device derives a hash and encrypts it with its private key. The encrypted hash is attached to the message and is forwarded to the remote end and acts like a signature. DH provides a way for two peers to establish a shared secret key that only they know, even though they are communicating over an insecure channel.

**Module 9**

**Network Transmission Quality**

Voice and live video transmissions create higher expectations for quality delivery among users, and create a need for Quality of Service (QoS). Congestion occurs when multiple communication lines aggregate onto a single device such as a router, and then much of that data is placed on just a few outbound interfaces, or onto a slower interface. Congestion can also occur when large data packets prevent smaller packets from being transmitted in a timely manner. Without any QoS mechanisms in place, packets are processed in the order in which they are received. When congestion occurs, network devices such as routers and switches can drop packets. This means that time-sensitive packets, such as real-time video and voice, will be dropped with the same frequency as data that is not time-sensitive, such as email and web browsing. When the volume of traffic is greater than what can be transported across the network, devices queue (hold) the packets in memory until resources become available to transmit them. Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed. One QoS technique that can help with this problem is to classify data into multiple queues. Network congestion points are ideal candidates for QoS mechanisms to mitigate delay and latency. Two types of delays are fixed and variable. Sources of delay are code delay, packetization delay, queuing delay, serialization delay, propagation delay, and de-jitter delay. Jitter is the variation in the delay of received packets. Due to network congestion, improper queuing, or configuration errors, the delay between each packet can vary instead of remaining constant. Both delay and jitter need to be controlled and minimized to support real-time and interactive traffic.

**Traffic Characteristics**

Voice and video traffic are two of the main reasons for QoS. Voice traffic is smooth and benign, but it is sensitive to drops and delays. Voice can tolerate a certain amount of latency, jitter, and loss without any noticeable effects. Latency should be no more than 150 milliseconds (ms). Jitter should be no more than 30 ms, and voice packet loss should be no more than 1%. Voice traffic requires at least 30 Kbps of bandwidth. Video traffic is more demanding than voice traffic because of the size of the packets it sends across the network. Video traffic is bursty, greedy, drop sensitive, and delay sensitive. Without QoS and a significant amount of extra bandwidth, video quality typically degrades. UDP ports such as 554, are used for the Real-Time Streaming Protocol (RSTP) and should be given priority over other, less delay-sensitive, network traffic. Similar to voice, video can tolerate a certain amount of latency, jitter, and loss without any noticeable effects. Latency should be no more than 400 milliseconds (ms). Jitter should be no more than 50 ms, and video packet loss should be no more than 1%. Video traffic requires at least 384 Kbps of bandwidth. Data traffic is not as demanding as voice and video traffic. Data packets often use TCP applications which can retransmit data and, therefore, are not sensitive to drops and delays. Although data traffic is relatively insensitive to drops and delays compared to voice and video, a network administrator still needs to consider the quality of the user experience, sometimes referred to as Quality of Experience (QoE). The two main factors that a network administrator needs to ask about the flow of data traffic are if the data comes from an interactive application and if the data is mission critical.

**Queuing Algorithms**

The QoS policy implemented by the network administrator becomes active when congestion occurs on the link. Queuing is a congestion management tool that can buffer, prioritize, and, if required, reorder packets before being transmitted to the destination. This course focuses on the following queuing algorithms: First-In, First-Out (FIFO), Weighted Fair Queuing (WFQ), Class-Based Weighted Fair Queuing (CBWFQ), and Low Latency Queuing (LLQ). FIFO queuing buffers and forwards packets in the order of their arrival. FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority. When FIFO is used, important or time-sensitive traffic can be dropped when there is congestion on the router or switch interface. WFQ is an automated scheduling method that provides fair bandwidth allocation to all network traffic. WFQ applies priority, or weights, to identified traffic and classifies it into conversations or flows. WFQ classifies traffic into different flows based on packet header addressing, including such characteristics as source and destination IP addresses, MAC addresses, port numbers, protocol, and Type of Service (ToS) value. The ToS value in the IP header can be used to classify traffic. CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. With CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. LLQ feature brings strict priority queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive packets, such as voice, to be sent before packets in other queues, reducing jitter in voice conversations.

**QoS Models**

There are three models for implementing QoS: Best-effort model, Integrated services (IntServ), and Differentiated services (DiffServ). The Best-effort model is the most scalable but does not guarantee delivery and does not give any packet preferential treatment. The IntServ architecture model was developed to meet the needs of real-time applications, such as remote video, multimedia conferencing, data visualization applications, and virtual reality. IntServ is a multiple-service model that can accommodate many QoS requirements. IntServ explicitly manages network resources to provide QoS to individual flows or streams, sometimes called microflows. It uses resource reservation and admission-control mechanisms as building blocks to establish and maintain QoS. The DiffServ QoS model specifies a simple and scalable mechanism for classifying and managing network traffic. The DiffServ design overcomes the limitations of both the best-effort and IntServ models. The DiffServ model can provide an “almost guaranteed” QoS, while still being cost-effective and scalable. DiffServ divides network traffic into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. It is possible to choose many levels of service with DiffServ.

**QoS Implementation Techniques**

There are three categories of QoS tools: classification and marking tools, congestion avoidance tools, and congestion management tools. Before a packet can have a QoS policy applied to it, the packet has to be classified. Classification and marking allows us to identify or “mark” types of packets. Classification determines the class of traffic to which packets or frames belong. Methods of classifying traffic flows at Layer 2 and 3 include using interfaces, ACLs, and class maps. Traffic can also be classified at Layers 4 to 7 using Network Based Application Recognition (NBAR). The Type of Service (IPv4) and Traffic Class (IPv6) carry the packet marking as assigned by the QoS classification tools. The field is then referred to by receiving devices which forward the packets based on the appropriate assigned QoS policy. These fields have 6-bits allocated for QoS. Called the Differentiated Services Code Point (DSCP) field, these six bits offer a maximum of 64 possible classes of service. The field is then referred to by receiving devices which forward the packets based on the appropriate assigned QoS policy. The 64 DSCP values are organized into three categories: Best-Effort (BE), Expedited Forwarding (EF), Assured Forwarding (AF). Because the first 3 most significant bits of the DSCP field indicate the class, these bits are also called the Class Selector (CS) bits. Traffic should be classified and marked as close to its source as technically and administratively feasible. This defines the trust boundary. Congestion management includes queuing and scheduling methods where excess traffic is buffered or queued (and sometimes dropped) while it waits to be sent out an egress interface. Congestion avoidance tools help to monitor network traffic loads in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks before congestion becomes a problem. Cisco IOS QoS includes weighted random early detection (WRED) as a possible congestion avoidance solution. The WRED algorithm allows for congestion avoidance on network interfaces by providing buffer management and allowing TCP traffic to decrease, or throttle back, before buffers are exhausted. Traffic shaping and traffic policing are two mechanisms provided by Cisco IOS QoS software to prevent congestion.

**Module 10**

**Device Discovery with CDP**

Cisco Discovery Protocol (CDP) is a Cisco proprietary Layer 2 protocol that is used to gather information about Cisco devices which share the same data link. The device sends periodic CDP advertisements to connected devices. CDP can be used as a network discovery tool to determine the information about the neighboring devices. This information gathered from CDP can help build a logical topology of a network when documentation is missing or lacking in detail. CDP can assist in network design decisions, troubleshooting, and making changes to equipment. On Cisco devices, CDP is enabled by default. To verify the status of CDP and display information about CDP, enter the **show cdp** command. To enable CDP globally for all the supported interfaces on the device, enter **cdp run** in the global configuration mode. To enable CDP on the specific interface, enter the **cdp enable** command. To verify the status of CDP and display a list of neighbors, use the **show cdp neighbors** command in the privileged EXEC mode. The **show cdp neighbors** command provides helpful information about each CDP neighbor device, including device identifiers, port identifier, capabilities list, and platform. Use the **show cdp interface** command to display the interfaces that are CDP enabled on a device.

**Device Discovery with LLDP**

Cisco devices also support Link Layer Discovery Protocol (LLDP), which is a vendor-neutral neighbor discovery protocol similar to CDP. This protocol advertises its identity and capabilities to other devices and receives the information from a physically connected Layer 2 device. To enable LLDP globally on a Cisco network device, enter the **lldp run** command in the global configuration mode. To verify LLDP has been enabled on the device, enter the **show lldp** command in privileged EXEC mode. With LLDP enabled, device neighbors can be discovered by using the **show lldp neighbors** command. When more details about the neighbors are needed, the **show lldp neighbors detail** command can provide information, such as the neighbor IOS version, IP address, and device capability.

**NTP**

The software clock on a router or switch starts when the system boots and is the primary source of time for the system. When the time is not synchronized between devices, it will be impossible to determine the order of the events and the cause of an event. You can manually configure the date and time, or you can configure the NTP. This protocol allows routers on the network to synchronize their time settings with an NTP server. When NTP is implemented in the network, it can be set up to synchronize to a private master clock or it can synchronize to a publicly available NTP server on the Internet. NTP networks use a hierarchical system of time sources and each level in this system is called a stratum. The synchronized time is distributed across the network by using NTP. Authoritative time sources, also referred to as stratum 0 devices, are high-precision timekeeping devices. Stratum 1 devices are directly connected to the authoritative time sources. Stratum 2 devices, such as NTP clients, synchronize their time by using the NTP packets from stratum 1 servers. The **ntp server** ip-address command is issued in global configuration mode to configure a device as the NTP server. To verify the time source is set to NTP, use the **show clock detail** command. The **show ntp associations** and **show ntp status** commands are used to verify that a device is synchronized with the NTP server.

**SNMP**

SNMP allows administrators to manage servers, workstations, routers, switches, and security appliances, on an IP network. SNMP is an application layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements: SNMP manager, SNMP agents, and the MIB. To configure SNMP on a networking device, you must define the relationship between the manager and the agent. The SNMP manager is part of an NMS. The SNMP manager can collect information from an SNMP agent by using the “get” action and can change configurations on an agent by using the “set” action. SNMP agents can forward information directly to a network manager by using “traps”. The SNMP agent responds to SNMP manager GetRequest-PDUs (to get an MIB variable) and SetRequest-PDUs (to set an MIB variable). An NMS periodically uses the get request to poll the SNMP agents by querying the device for data. A network management application can collect information to monitor traffic loads and to verify device configurations of managed devices.

SNMPv1, SNMPv2c, and SNMPv3 are all versions of SNMP. SNMPv1 is a legacy solution. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers that is able to access the agent's MIB is defined by a community string. SNMPv2c includes a bulk retrieval mechanism and more detailed error message reporting. SNMPv3 provides for both security models and security levels. SNMP community strings are read-only (ro) and read-write (rw). They are used to authenticate access to MIB objects. The MIB organizes variables hierarchically. MIB variables enable the management software to monitor and control the network device. OIDs uniquely identify managed objects in the MIB hierarchy. The snmpget utility gives some insight into the basic mechanics of how SNMP works. The Cisco SNMP Navigator on the [http://www.cisco.com](http://www.cisco.com/) website allows a network administrator to research details about a particular OID.

**Syslog**

The most common method of accessing system messages is to use a protocol called syslog. The syslog protocol uses UDP port 514 to allow networking devices to send their system messages across the network to syslog servers. The syslog logging service provides three primary functions: gather logging information for monitoring and troubleshooting, select the type of logging information that is captured, and specify the destinations of captured syslog messages. Destinations for syslog messages include the logging buffer (RAM inside a router or switch), console line, terminal line, and syslog server. This table shows syslog levels:

| Severity NameSeverity LevelExplanationEmergencyLevel 0System UnusableAlertLevel 1Immediate Action NeededCriticalLevel 2Critical ConditionErrorLevel 3Error ConditionWarningLevel 4Warning ConditionNotificationLevel 5Normal, but Significant ConditionInformationalLevel 6Informational MessageDebuggingLevel 7Debugging Message | | |
| --- | --- | --- |
| **Severity Name** | **Severity Level** | **Explanation** |
| Emergency | Level 0 | System Unusable |
| Alert | Level 1 | Immediate Action Needed |
| Critical | Level 2 | Critical Condition |
| Error | Level 3 | Error Condition |
| Warning | Level 4 | Warning Condition |
| Notification | Level 5 | Normal, but Significant Condition |
| Informational | Level 6 | Informational Message |
| Debugging | Level 7 | Debugging Message |

Syslog facilities identify and categorize system state data for error and event message reporting. Common syslog message facilities reported on Cisco IOS routers include: IP, OSPF protocol, SYS operating system, IPsec, and IF. The default format of syslog messages on Cisco IOS software is: %facility-severity-MNEMONIC: description. Use the command **service timestamps log datetime** to force logged events to display the date and time.

**Router and Switch File Maintenance**

The Cisco IFS lets the administrator navigate to different directories and list the files in a directory, and to create subdirectories in flash memory or on a disk. Use the **show file systems command** to display lists all of the available file systems on a Cisco router. Use the directory command **dir** to display the directory of bootflash. Use the change directory command **cd** to view the contents of NVRAM. Use the present working directory command **pwd** to that you are viewing the current directory. Use the **show file systems** command to view the file systems on a Catalyst switch or a Cisco router. Configuration files can be saved to a text file by using Tera Term. A configuration can be copied from a file and then directly pasted to a device. Configuration files can be stored on a TFTP server, or a USB drive. To save the running configuration or the startup configuration to a TFTP server, use either the **copy running-config tftp** or **copy startup-config tftp** command. Use the **dir** command to view the contents of the USB flash drive. Use the **copy run usbflash0:/** command to copy the configuration file to the USB flash drive. Use the **dir** command to see the file on the USB drive. Use the **more** command to see the contents of the drive. For encrypted passwords, such as the enable secret passwords, the passwords must be replaced after recovery.

**IOS Image Management**

Cisco IOS Software images and configuration files can be stored on a central TFTP server to control the number of IOS images and the revisions to those IOS images, as well as the configuration files that must be maintained. Select a Cisco IOS image file that meets the requirements in terms of platform, features, and software. Download the file from cisco.com and transfer it to the TFTP server. Ping the TFTP server. Verify the amount of free flash. The amount of free flash can be verified by using the **show flash:** command. If there is enough free flash to hold the new IOS image, copy the new IOS image to flash. To upgrade to the copied IOS image after that image is saved on the router's flash memory, configure the router to load the new image during bootup by using the **boot system** command. Save the configuration. Reload the router to boot the router with new image. After the router has booted, to verify the new image has loaded, use the **show version** command.

**Module 11**

**Hierarchical Networks**

All enterprise networks must: support critical applications, support converged network traffic, support diverse business needs, and provide centralized administrative control. The Cisco Borderless Network provides the framework to unify wired and wireless access, including policy, access control, and performance management across many different device types. The borderless network is built on a hierarchical infrastructure of hardware that is scalable and resilient. Two proven hierarchical design frameworks for campus networks are the three-tier layer and the two-tier layer models. The three critical layers within these tiered designs are the access, distribution, and core layers. The access layer represents the network edge, where traffic enters or exits the campus network. Access layer switches connect to distribution layer switches, which implement network foundation technologies such as routing, quality of service, and security. The distribution layer interfaces between the access layer and the core layer. The primary purpose of the core layer is to provide fault isolation and high-speed backbone connectivity. Networks have fundamentally changed to switched LANs in a hierarchical network, providing QoS, security, support for wireless connectivity and IP telephony and mobility services.

**Scalable Networks**

A basic network design strategy includes the following recommendations: use expandable, modular equipment, or clustered devices; design a hierarchical network to include modules that can be added, upgraded, and modified; create a hierarchical IPv4 and IPv6 address strategy; and choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network. Implement redundant links in the network between critical devices and between access layer and core layer devices. Implement multiple links between equipment, with either link aggregation (EtherChannel) or equal cost load balancing, to increase bandwidth. Use a scalable routing protocol and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table. Implement wireless connectivity to allow for mobility and expansion. One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices. Another method of implementing redundancy is to create redundant paths. A well-designed network not only controls traffic, but also limits the size of failure domains. Switch blocks act independently of the others, so the failure of a single device does not cause the network to go down. Link aggregation, such as EtherChannel, allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links. Wireless connectivity expands the access layer. When implementing a wireless network, you must consider the types of wireless devices to use, wireless coverage requirements, interference considerations, and security. Link-state routing protocols such as OSPF, work well for larger hierarchical networks where fast convergence is important. OSPF routers establish and maintain neighbor adjacencies with other connected OSPF routers, they synchronize their link-state database. When a network change occurs, link state updates are sent, informing other OSPF routers of the change and establishing a new best path.

**Switch Hardware**

There are several categories of switches for enterprise networks including campus LAN, cloud-managed, data center, service provider, and virtual networking. Form factors for switches include fixed configuration, modular configuration, and stackable configuration. The thickness of a switch is expressed in number of rack units. The port density of a switch refers to the number of ports available on a single switch. Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling. Multilayer switches are typically deployed in the core and distribution layers of an organization's switched network. Multilayer switches are characterized by their ability to build a routing table, support a few routing protocols, and forward IP packets at a rate close to that of Layer 2 forwarding. Business considerations for switch selection include cost, port density, power, reliability, port speed, frame buffers, and scalability.

**Router Hardware**

Routers use the network portion (prefix) of the destination IP address to route packets to the proper destination. They select an alternate path if a link or path goes down. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway. Routers also serve other beneficial functions:

* They provide broadcast containment by limiting broadcasts to the local network.
* They interconnect geographically separated locations.
* They group users logically by application or department within a company, who have command needs or require access to the same resources.
* They provide enhanced security by filtering unwanted traffic through access control lists.

Cisco has several categories of routers including branch, network edge, service provider and industrial. Branch routers optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures. Network edge routers deliver high-performance, highly secure, and reliable services that unite campus, data center, and branch networks. Service provider routers differentiate the service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services. Industrial routers are designed to provide enterprise-class features in rugged and harsh environments. Cisco router form factors include the Cisco 900 Series, the ASR 9000 and 1000 Series, the 5500 Series, and the Cisco 800. Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built-in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. Routers come with a variety of different interfaces, such as Fast Ethernet, Gigabit Ethernet, Serial, and Fiber-Optic.

**Module 12**

**Network Documentation**

Common network documentation includes: physical and logical network topologies, network device documentation recording all pertinent device information, and network performance baseline documentation. Information found on a physical topology typically includes the device name, device location (address, room number, rack location, etc.), interface and ports used, and cable type. Network device documentation for a router may include the interface, IPv4 address, IPv6 address, MAC address and routing protocol. Network device documentation for a switch may include the port, access, VLAN, trunk, EtherChannel, native, and enabled. Network device documentation for end-systems may include device name, OS, services, MAC address, IPv4 and IPv6 addresses, default gateway, and DNS. A network baseline should answer the following questions:

* How does the network perform during a normal or average day?
* Where are the most errors occurring?
* What part of the network is most heavily used?
* What part of the network is least used?
* Which devices should be monitored and what alert thresholds should be set?
* Can the network meet the identified policies?

When conducting the initial baseline, start by selecting a few variables that represent the defined policies, such as interface utilization and CPU utilization. A logical network topology diagram can be useful in identifying key devices and ports to monitor. The length of time and the baseline information being gathered must be long enough to determine a “normal” picture of the network. When documenting the network, gather information directly from routers and switches using the **show**, **ping**, **traceroute**, and **telnet** commands.

**Troubleshooting Process**

The troubleshooting process should be guided by structured methods. One method is the seven-step troubleshooting process: 1. Define the problem, 2. Gather information, 3. Analyze information, 4. Eliminate possible causes, 5. Propose hypothesis, 6. Test hypothesis, and 7. Solve the problem. When talking to end users about their network problems, ask both open and closed-ended questions. Use the **show**, **ping**, **traceroute**, and **telnet** commands to gather information from devices. Use the layered models to perform bottom-up, top-down, or divide-and-conquer troubleshooting. Other models include follow-the-path, substitution, comparison, and educated guess. Software problems are often solved using a top-down approach while hardware-based problems are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide-and-conquer method.

**Troubleshooting Tools**

Common software troubleshooting tools include NMS tools, knowledge bases, and baselining tools. A protocol analyzer, such as Wireshark, decodes the various protocol layers in a recorded frame and presents this information in an easy to use format. Hardware troubleshooting tools include digital multimeters, cable testers, cable analyzers, portable network analyzers, and Cisco Prime NAM. Syslog server can also be used as a troubleshooting tool. Implementing a logging facility for network troubleshooting. Cisco devices can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Event messages can be sent to one or more of the following: console, terminal lines, buffered logging, SNMP traps, and syslog. The lower the level number, the higher the severity level. The **logging trap** *level* command limits messages logged to the syslog server based on severity. The level is the name or number of the severity level. Only messages equal to or numerically lower than the specified level are logged.

**Symptoms and Causes of Network Problems**

Failures and suboptimal conditions at the physical layer usually cause networks to shut down. Network administrators must have the ability to effectively isolate and correct problems at this layer. Symptoms include performance lower than baseline, loss of connectivity, congestion, high CPU utilization, and console error messages. The causes are usually power-related, hardware faults, cabling faults, attenuation, noise, interface configuration errors, exceeding component design limits, and CPU overload.

Data link layer problems cause specific symptoms that, when recognized, will help identify the problem quickly. Symptoms include no functionality/connectivity at Layer 2 or above, network operating below baseline levels, excessive broadcasts, and console messages. The causes are usually encapsulation errors, address mapping errors, framing errors, and STP failures or loops.

Network layer problems include any problem that involves a Layer 3 protocol, both routed protocols (such as IPv4 or IPv6) and routing protocols (such as EIGRP, OSPF, etc.). Symptoms include network failure and suboptimal performance. The causes are usually general network issues, connectivity issues, routing table problems, neighbor issues, and the topology database.

Transport layer problems can arise from transport layer problems on the router, particularly at the edge of the network where traffic is examined and modified. Symptoms include connectivity and access issues. Causes are likely to be misconfigured NAT or ACLs. ACL misconfigurations commonly occur at the selection of traffic flow, order of access control entries, implicit deny any, addresses and IPv4 wildcard masks, selection of transport layer protocol, source and destination ports, use of the established keyword, and uncommon protocols. There are several problems with NAT including misconfigured NAT inside, NAT outside, or ACL. Common interoperability areas with NAT include BOOTP and DHCP, DNS, SNMP, and tunneling and encryption protocols.

Application layer problems can result in unreachable or unusable resources when the physical, data link, network, and transport layers are functional. It is possible to have full network connectivity, but the application simply cannot provide data. Another type of problem at the application layer occurs when the physical, data link, network, and transport layers are functional, but the data transfer and requests for network services from a single network service or application do not meet the normal expectations of a user.

**Troubleshooting IP Connectivity**

Diagnosing and solving problems is an essential skill for network administrators. There is no single recipe for troubleshooting, and a problem can be diagnosed in many ways. However, by employing a structured approach to the troubleshooting process, an administrator can reduce the time it takes to diagnose and solve a problem.

End-to-end connectivity problems are usually what initiates a troubleshooting effort. Two of the most common utilities used to verify a problem with end-to-end connectivity are **ping** and **traceroute.** The **ping** command uses a Layer 3 protocol that is a part of the TCP/IP suite called ICMP. The **traceroute** command is commonly performed when the **ping** command fails.

**Step 1**. Verify the physical layer. The most commonly used Cisco IOS commands for this purpose are **show processes cpu**, **show memory**, and **show interfaces**.

**Step 2**. Check for duplex mismatches. Another common cause for interface errors is a mismatched duplex mode between two ends of an Ethernet link. In many Ethernet-based networks, point-to-point connections are now the norm, and the use of hubs and the associated half-duplex operation is becoming less common. Use the **show interfaces** *interface* command to diagnose this problem.

**Step 3**. Verify addressing on the local network. When troubleshooting end-to-end connectivity, it is useful to verify mappings between destination IP addresses and Layer 2 Ethernet addresses on individual segments. The **arp** Windows command displays and modifies entries in the ARP cache that are used to store IPv4 addresses and their resolved Ethernet physical (MAC) addresses. The **netsh interface ipv6 show neighbor** Windows command output lists all devices that are currently in the neighbor table. The **show ipv6 neighbors** command output displays an example of the neighbor table on the Cisco IOS router. Use the **show mac address-table** command to display the MAC address table on the switch.

VLAN assignment is another issue to consider when troubleshooting end-to-end connectivity. Use the **arp** Windows command to see the entry for a default gateway. Use the **show mac address-table** command to check the switch MAC table. This may show that not a VLAN assignments are correct.

**Step 4**. Verify the default gateway. The command output of the **show ip route** Cisco IOS command is used to verify the default gateway of a router. On a Windows host, the **route print** Windows command is used to verify the presence of the IPv4 default gateway.

In IPv6, the default gateway can be configured manually, using stateless autoconfiguration (SLAAC), or by using DHCPv6. The **show ipv6 route** Cisco IOS command is used to check for the IPv6 default route on a router. The **ipconfig** Windows command is used to verify if a PC1 has an IPv6 default gateway. The command output of the **show ipv6 interface** *interface* will tell you if a router is or is not enabled as an IPv6 router. Enable a router as an IPv6 router using the **ipv6 unicast-routing** command. To verify that a host has the default gateway set, use the **ipconfig** command on the Microsoft Windows PC or the **ifconfig** command on Linux and Mac OS X.

**Step 5**. Verify correct path. The routers in the path make the routing decision based on information in the routing tables. Use the **show ip route** | **begin Gateway** command for an IPv4 routing table. Use the **show ipv6 route** command for an IPv6 routing table.

**Step 6**. Verify the transport layer. Two of the most common issues that affect transport layer connectivity include ACL configurations and NAT configurations. A common tool for testing transport layer functionality is the Telnet utility.

**Step 7**. Verify ACLs. Use the **show ip access-lists** command to display the contents of all IPv4 ACLs and the **show ipv6 access-list** command to show the contents of all IPv6 ACLs configured on a router. Verify which interface has the ACL applied using the **show ip interfaces** command.

**Step 8**. Verify DNS. To display the DNS configuration information on the switch or router, use the **show running-config** command. Use the **ip host** command to enter name to IPv4 mapping to the switch or router as shown in the command output.

**Module 13**

**Cloud Computing**

Cloud computing involves large numbers of computers connected through a network that can be physically located anywhere. Cloud computing can reduce operational costs by using resources more efficiently. Cloud computing addresses a variety of data management issues:

* It enables access to organizational data anywhere and at any time.
* It streamlines the organization’s IT operations by subscribing only to needed services.
* It eliminates or reduces the need for onsite IT equipment, maintenance, and management.
* It reduces cost for equipment, energy, physical plant requirements, personnel training needs.
* It enables rapid responses to increasing data volume requirements.

The three main cloud computing services defined by the National Institute of Standards and Technology (NIST) are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With SaaS, the cloud provider is responsible for access to applications and services, such as email, communication, and Office 365 that are delivered over the internet. With PaaS, the cloud provider is responsible for providing users access to the development tools and services used to deliver the applications. With IaaS, the cloud provider is responsible for giving IT managers access to the network equipment, virtualized network services, and supporting network infrastructure. The four types of clouds are public, private, hybrid, and community. Cloud-based applications and services offered in a public cloud are made available to the general population. Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government. A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a separate object, but both are connected using a single architecture. A community cloud is created for exclusive use by a specific community.

**Virtualization**

The terms “cloud computing” and “virtualization” are often used interchangeably; however, they mean different things. Virtualization is the foundation of cloud computing. Virtualization separates the operating system (OS) from the hardware. Historically, enterprise servers consisted of a server OS, such as Windows Server or Linux Server, installed on specific hardware. All of a server’s RAM, processing power, and hard drive space were dedicated to the service. When a component fails, the service that is provided by this server becomes unavailable. This is known as a single point of failure. Another problem with dedicated servers is that they often sat idle for long periods of time, waiting until there was a need to deliver the specific service they provide. This wastes energy and resources (server sprawl). Virtualization reduces costs because less equipment is required, less energy is consumed, and less space is required. It provides for easier prototyping, faster server provisioning, increased server uptime, improved disaster recovery, and legacy support. A computer system consists of the following abstraction layers: services, OS, firmware, and hardware. With Type 1 hypervisors, the hypervisor is installed directly on the server or networking hardware. A Type 2 hypervisor is software that creates and runs VM instances. It can be installed on top of the OS or can be installed between the firmware and the OS. A Type 2 hypervisor is software that creates and runs VM instances.

**Virtual Network Infrastructure**

Type 1 hypervisors are also called the “bare metal” approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors have direct access to the hardware resources and are more efficient than hosted architectures. They improve scalability, performance, and robustness. Type 1 hypervisors require a “management console” to manage the hypervisor. Management software is used to manage multiple servers using the same hypervisor. The management console can automatically consolidate servers and power on or off servers as required. The management console provides recovery from hardware failure. Some management consoles also allow server over allocation. Server virtualization hides server resources, such as the number and identity of physical servers, processors, and OSs from server users. This practice can create problems if the data center is using traditional network architectures. Another problem is that traffic flows differ substantially from the traditional client-server model. Typically, a data center has a considerable amount of traffic being exchanged between virtual servers. These flows are called East-West traffic and can change in location and intensity over time. North-South traffic occurs between the distribution and core layers and is typically traffic destined for offsite locations such as another data center, other cloud providers, or the internet.

**Software-Defined Networking**

Two major network architectures have been developed to support network virtualization: Software-Defined Networking (SDN) and Cisco Application Centric Infrastructure (ACI). SDN is an approach to networking where the network is software programmable remotely. Components of SDN may include OpenFlow, OpenStack, and other components. The SDN controller is a logical entity that enables network administrators to manage and dictate how the data plane of switches and routers should handle network traffic. A network device contains a control plane and a data plane. The control plane is regarded as the brains of a device. It is used to make forwarding decisions. The control plane contains Layer 2 and Layer 3 route forwarding mechanisms, such as routing protocol neighbor tables and topology tables, IPv4 and IPv6 routing tables, STP, and the ARP table. Information sent to the control plane, is processed by the CPU. The data plane, also called the forwarding plane, is typically the switch fabric connecting the various network ports on a device. The data plane of each device is used to forward traffic flows. Routers and switches use information from the control plane to forward incoming traffic out the appropriate egress interface. Information in the data plane is typically processed by a special data plane processor without the CPU getting involved. Cisco Express Forwarding (CEF) uses the control plane and data plane to process packets. CEF is an advanced, Layer 3 IP switching technology that enables forwarding of packets to occur at the data plane without consulting the control plane. SDN is basically the separation of the control plane and data plane. The control plane function is removed from each device and is performed by a centralized controller. The centralized controller communicates control plane functions to each device. The management plane is responsible for managing a device through its connection to the network. Network administrators use applications such as Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), Secure FTP, and Secure Hypertext Transfer Protocol (HTTPS) to access the management plane and configure a device. Protocols like Simple Network Management Protocol (SNMP) use the management plane.

**Controllers**

The SDN controller is a logical entity that enables network administrators to manage and dictate how the data plane of switches and routers should handle network traffic. The SDN controller defines the data flows between the centralized control plane and the data planes on individual routers and switches. Each flow traveling through the network must first get permission from the SDN controller, which verifies that the communication is permissible according to the network policy. If the controller allows a flow, it computes a route for the flow to take and adds an entry for that flow in each of the switches along the path. The controller populates flow tables. Switches manage the flow tables. A flow table matches incoming packets to a particular flow and specifies the functions that are to be performed on the packets. There may be multiple flow tables that operate in a pipeline fashion. A flow table may direct a flow to a group table, which may trigger a variety of actions that affect one or more flows. A meter table triggers a variety of performance-related actions on a flow including the ability to rate-limit the traffic. Cisco developed the Application Centric Infrastructure (ACI) which is a more advanced and innovative way than earlier SDN approaches. Cisco ACI is a hardware solution for integrating cloud computing and data center management. At a high level, the policy element of the network is removed from the data plane. This simplifies the way data center networks are created. The three core components of the ACI architecture are Application Network Profile (ANP), Application Policy Infrastructure Controller (APIC), and Cisco Nexus 9000 Series switches. The Cisco ACI fabric is composed of the APIC and the Cisco Nexus 9000 series switches using two-tier spine-leaf topology. When compared to SDN, the APIC controller does not manipulate the data path directly. Instead, the APIC centralizes the policy definition and programs the leaf switches to forward traffic based on the defined policies. There are three types of SDN. Device-based SDN is when the devices are programmable by applications running on the device itself or on a server in the network. Controller-based SDN uses a centralized controller that has knowledge of all devices in the network. Policy based SDN is similar to controller-based SDN where a centralized controller has a view of all devices in the network. Policy-based SDN includes an additional Policy layer that operates at a higher level of abstraction. Policy-based SDN is the most robust, providing for a simple mechanism to control and manage policies across the entire network. Cisco APIC-EM is an example of policy-based SDN. Cisco APIC-EM provides a single interface for network management including discovering and accessing device and host inventories, viewing the topology, tracing a path between end points, and setting policies. The APIC-EM Path Trace tool allows the administrator to easily visualize traffic flows and discover any conflicting, duplicate, or shadowed ACL entries. This tool examines specific ACLs on the path between two end nodes, displaying any potential issues.

**Module 14**

Automation is any process that is self-driven, reducing and potentially eliminating, the need for human intervention. Whenever a course of action is taken by a device based on an outside piece of information, then that device is a smart device. For smart devices to “think”, they need to be programmed using network automation tools.

Data formats are simply a way to store and interchange data in a structured format. One such format is called Hypertext Markup Language (HTML). Common data formats that are used in many applications including network automation and programmability are JavaScript Object Notation (JSON), eXtensible Markup Language (XML), and YAML Ain’t Markup Language (YAML). Data formats have rules and structure similar to what we have with programming and written languages.

An API is a set of rules describing how one application can interact with another, and the instructions to allow the interaction to occur. Open/Public APIs are, as the name suggests, publicly available. Internal/Private APIs are used only within an organization. Partner APIs are used between a company and its business partners. There are four types of web service APIs: Simple Object Access Protocol (SOAP), Representational State Transfer (REST), eXtensible Markup Language-Remote Procedure Call (XML-RPC), and JavaScript Object Notation-Remote Procedure Call (JSON-RPC).

A REST API defines a set of functions developers can use to perform requests and receive responses via HTTP protocol such as GET and POST. Conforming to the constraints of the REST architecture is generally referred to as being “RESTful”. RESTful APIs use common HTTP methods including POST, GET, PUT, PATCH and DELETE. These methods correspond to RESTful operations: Create, Read, Update, and Delete (or CRUD). Web resources and web services such as RESTful APIs are identified using a URI. A URI has two specializations, Uniform Resource Name (URN) and Uniform Resource Locator (URL). In a RESTful Web service, a request made to a resource's URI will elicit a response. The response will be a payload typically formatted in JSON. The different parts of the API request are API server, Resources, and Query. Queries can include format, key, and parameters.

There are now new and different methods for network operators to automatically monitor, manage, and configure the network. These include protocols and technologies such as REST, Ansible, Puppet, Chef, Python, JSON, XML, and more. Configuration management tools use RESTful API requests to automate tasks and scale across thousands of devices. Characteristics of the network that benefit from automation include software and version control, device attributes such as names, addressing, and security, protocol configurations, and ACL configurations. Configuration management tools typically include automation and orchestration. Orchestration is the arranging of the automated tasks that results in a coordinate process or workflow. Ansible, Chef, Puppet, and SaltStack all come with API documentation for configuring RESTful API requests.

IBN builds on SDN, taking a software-centric, fully automated approach to designing and operating networks. Cisco views IBN as having three essential functions: translation, activation, and assurance. The physical and virtual network infrastructure is a fabric. The term fabric describes an overlay that represents the logical topology used to virtually connect to devices. The underlay network is the physical topology that includes all hardware required to meet business objectives. Cisco implements the IBN fabric using Cisco DNA. The business intent is securely deployed into the network infrastructure (the fabric). Cisco DNA then continuously gathers data from a multitude of sources (devices and applications) to provide a rich context of information. Cisco DNA Center is the foundational controller and analytics platform at the heart of Cisco DNA. Cisco DNA Center is a network management and command center for provisioning and configuring network devices. It is a single interface hardware and software platform that focuses on assurance, analytics, and automation.