Module 2

All end devices and network devices require an operating system (OS). The user can interact with the shell using a command-line interface (CLI) to use a keyboard to run CLI-based network programs, use a keyboard to enter text and text-based commands, and view output on a monitor.

As a security feature, the Cisco IOS software separates management access into the following two command modes: User EXEC Mode and Privileged EXEC Mode.

Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. Two common subconfiguration modes include: Line Configuration Mode and Interface Configuration Mode. To move in and out of global configuration mode, use the **configure terminal** privileged EXEC mode command. To return to the privileged EXEC mode, enter the **exit** global config mode command.

Each IOS command has a specific format or syntax and can only be executed in the appropriate mode. The general syntax for a command is the command followed by any appropriate keywords and arguments. The IOS has two forms of help available: context-sensitive help and command syntax check.

The first configuration command on any device should be to give it a unique device name or hostname. Network devices should always have passwords configured to limit administrative access. Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device. Configure and encrypt all passwords. Provide a method for declaring that only authorized personnel should attempt to access the device by adding a banner to the device output.

There are two system files that store the device configuration: startup-config and running-config. Running configuration files can be altered if they have not been saved. Configuration files can also be saved and archived to a text document.

IP addresses enable devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.

IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP). In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1 global configuration** command. Vlan 1 is not an actual physical interface but a virtual one.

In the same way that you use commands and utilities to verify a PC host’s network configuration, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers. The **show ip interface brief** command verifies the condition of the switch interfaces. The **ping** command can be used to test connectivity to another device on the network or a website on the internet.

## Module 3

**The Rules**

All communication methods have three elements in common: message source (sender), message destination (receiver), and channel. Sending a message is governed by rules called protocols. Protocols must include: an identified sender and receiver, common language and grammar, speed and timing of delivery, and confirmation or acknowledgment requirements. Common computer protocols include these requirements: message encoding, formatting and encapsulation, size, timing, and delivery options. Encoding is the process of converting information into another acceptable form, for transmission. Decoding reverses this process to interpret the information. Message formats depend on the type of message and the channel that is used to deliver the message. Message timing includes flow control, response timeout, and access method. Message delivery options include unicast, multicast, and broadcast.

**Protocols**

Protocols are implemented by end-devices and intermediary devices in software, hardware, or both. A message sent over a computer network typically requires the use of several protocols, each one with its own functions and format. Each network protocol has its own function, format, and rules for communications. The Ethernet family of protocols includes IP, TCP, HTTP, and many more. Protocols secure data to provide authentication, data integrity, and data encryption: SSH, SSL, and TLS. Protocols enable routers to exchange route information, compare path information, and then to select the best path to the destination network: OSPF and BGP. Protocols are used for the automatic detection of devices or services: DHCP and DNS. Computers and network devices use agreed-upon protocols that provide the following functions: addressing, reliability, flow control, sequencing, error-detection, and application interface.

**Protocol Suites**

A protocol suite is a group of inter-related protocols necessary to perform a communication function. A protocol stack shows how the individual protocols within a suite are implemented. Since the 1970s there have been several different protocol suites, some developed by a standards organization and others developed by various vendors. TCP/IP protocols are available for the application, transport, and internet layers. TCP/IP is the protocol suite used by today’s networks and internet. TCP/IP offers two important aspects to vendors and manufacturers: open standard protocol suite, and standards-based protocol suite. The TCP/IP protocol suite communication process enables such processes as a web server encapsulating and sending a web page to a client, as well as the client de-encapsulating the web page for display in a web browser.

**Standards Organizations**

Open standards encourage interoperability, competition, and innovation. Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards. Various organizations have different responsibilities for promoting and creating standards for the internet including: ISOC, IAB, IETF, and IRTF. Standards organizations that develop and support TCP/IP include: ICANN and IANA. Electronic and communications standards organizations include: IEEE, EIA, TIA, and ITU-T.

**Reference Models**

The two reference models that are used to describe network operations are OSI and TCP/IP. The OSI model has seven layers:

7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network

2 - Data Link

1 - Physical

The TCP/IP model has four layers:

4 - Application

3 - Transport

2 - Internet

1 - Network Access

**Data Encapsulation**

Segmenting messages has two primary benefits:

* By sending smaller individual pieces from source to destination, many different conversations can be interleaved on the network. This is called multiplexing.
* Segmentation can increase the efficiency of network communications. If part of the message fails to make it to the destination only the missing parts need to be retransmitted.

TCP is responsible for sequencing the individual segments. The form that a piece of data takes at any layer is called a protocol data unit (PDU). During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. When sending messages on a network, the encapsulation process works from top to bottom. This process is reversed at the receiving host and is known as de-encapsulation. De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.

**Data Access**

The network and data link layers are responsible for delivering the data from the source device to the destination device. Protocols at both layers contain a source and destination address, but their addresses have different purposes:

* **Network layer source and destination addresses** - Responsible for delivering the IP packet from the original source to the final destination, which may be on the same network or a remote network.
* **Data link layer source and destination addresses** - Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

The IP addresses indicate the original source IP address and final destination IP address. An IP address contains two parts: the network portion (IPv4) or Prefix (IPv6) and the host portion (IPv4) or Interface ID (IPv6). When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On an Ethernet network, the data link addresses are known as Ethernet Media Access Control (MAC) addresses. When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. The Ethernet frame must be sent to another device known as the router or default gateway.

## Module 4

**Purpose of the Physical Layer**

Before any network communications can occur, a physical connection to a local network must be established. A physical connection can be a wired connection using a cable or a wireless connection using radio waves. Network Interface Cards (NICs) connect a device to the network. Ethernet NICs are used for a wired connection, whereas WLAN (Wireless Local Area Network) NICs are used for wireless. The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media. This layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted onto the local media. The encoded bits that comprise a frame are received by either an end device or an intermediary device.

**Physical Layer Characteristics**

The physical layer consists of electronic circuitry, media, and connectors developed by engineers. The physical layer standards address three functional areas: physical components, encoding, and signaling. Bandwidth is the capacity at which a medium can carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Throughput is the measure of the transfer of bits across the media over a given period of time and is usually lower than bandwidth. Latency refers to the amount of time, including delays, for data to travel from one given point to another. Goodput is the measure of usable data transferred over a given period of time. The physical layer produces the representation and groupings of bits for each type of media as follows:

* **Copper cable** - The signals are patterns of electrical pulses.
* **Fiber-optic cable** - The signals are patterns of light.
* **Wireless** - The signals are patterns of microwave transmissions.

**Copper Cabling**

Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference. The timing and voltage values of the electrical pulses are also susceptible to interference from two sources: EMI and crosstalk. Three types of copper cabling are: UTP, STP, and coaxial cable (coax). UTP has an outer jacket to protect the copper wires from physical damage, twisted pairs to protect the signal from interference, and color-coded plastic insulation that electrically isolates wires from each other and identifies each pair. The STP cable uses four pairs of wires, each wrapped in a foil shield, which are then wrapped in an overall metallic braid or foil. Coaxial cable, or coax for short, gets its name from the fact that there are two conductors that share the same axis. Coax is used to attach antennas to wireless devices. Cable internet providers use coax inside their customers’ premises.

**UTP Cabling**

UTP cabling consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath. UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered other ways that they can limit the negative effect of crosstalk: cancellation and varying the number of twists per wire pair. UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE). UTP cable is usually terminated with an RJ-45 connector. The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover. Cisco has a proprietary UTP cable called a rollover that connects a workstation to a router console port.

**Fiber-Optic Cabling**

Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media. Fiber-optic cable can transmit signals with less attenuation than copper wire and is completely immune to EMI and RFI. Optical fiber is a flexible, but extremely thin, transparent strand of very pure glass, not much bigger than a human hair. Bits are encoded on the fiber as light impulses. Fiber-optic cabling is now being used in four types of industry: enterprise networks, FTTH, long-haul networks, and submarine cable networks. There are four types of fiber-optic connectors: ST, SC, LC, and duplex multimode LC. Fiber-optic patch cords include SC-SC multimode, LC-LC single-mode, ST-LC multimode, and SC-ST single-mode. In most enterprise environments, optical fiber is primarily used as backbone cabling for high-traffic point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

**Wireless Media**

Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies. Wireless does have some limitations, including: coverage area, interference, security, and the problems that occur with any shared medium. Wireless standards include the following: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16), and Zigbee (IEEE 802.15.4). Wireless LAN (WLAN) requires a wireless AP and wireless NIC adapters.

## Module 5

**Binary Number System**

Binary is a numbering system that consists of the numbers 0 and 1 called bits. In contrast, the decimal numbering system consists of 10 digits consisting of the numbers 0 – 9. Binary is important for us to understand because hosts, servers, and network devices use binary addressing, specifically, binary IPv4 addresses, to identify each other. You must know binary addressing and how to convert between binary and dotted decimal IPv4 addresses. This topic presented a few ways to convert decimal to binary and binary to decimal.

**Hexadecimal Number System**

Just as decimal is a base ten number system, hexadecimal is a base sixteen system. The base sixteen number system uses the numbers 0 to 9 and the letters A to F. The hexadecimal numbering system is used in networking to represent IPv6 addresses and Ethernet MAC addresses. IPv6 addresses are 128 bits in length and every 4 bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. To convert hexadecimal to decimal, you must first convert the hexadecimal to binary, then convert the binary to decimal. To convert decimal to hexadecimal, you must also first convert the decimal to binary.

## Module 6

**Purpose of the Data Link Layer**

The data link layer of the OSI model (Layer 2) prepares network data for the physical network. The data link layer is responsible for network interface card (NIC) to network interface card communications. Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path. The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC. The MAC sublayer provides data encapsulation through frame delimiting, addressing, and error detection. Router interfaces encapsulate the packet into the appropriate frame. A suitable media access control method is used to access each link. Engineering organizations that define open standards and protocols that apply to the network access layer include: IEEE, ITU, ISO, and ANSI.

**Topologies**

The two types of topologies used in LAN and WAN networks are physical and logical. The data link layer "sees" the logical topology of a network when controlling data access to the media. The logical topology influences the type of network framing and media access control used. Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh. Physical point-to-point topologies directly connect two end devices (nodes). Adding intermediate physical connections may not change the logical topology. In multi-access LANs, nodes are interconnected using star or extended star topologies. In this type of topology, nodes are connected to a central intermediary device. Physical LAN topologies include: star, extended star, bus, and ring. Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously. Two interconnected interfaces must use the same duplex mode or there will be a duplex mismatch creating inefficiency and latency on the link. Ethernet LANs and WLANs are examples of multi-access networks. A multi-access network is a network that can have multiple nodes accessing the network simultaneously. Some multi-access networks require rules to govern how devices share the physical media. There are two basic access control methods for shared media: contention-based access and controlled access. In contention-based multi-access networks, all nodes are operating in half-duplex. There is a process if more than one device transmits at the same time. Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.

**Data Link Frame**

The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame. The data link protocol is responsible for NIC-to-NIC communications within the same network. There are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts: header, data, and trailer. Unlike other encapsulation protocols, the data link layer appends information in the trailer. There is no one frame structure that meets the needs of all data transportation across all types of media. Depending on the environment, the amount of control information needed in the frame varies to match the access control requirements of the media and logical topology. Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection. The data link layer provides addressing used to transport a frame across shared local media. Device addresses at this layer are physical addresses. Data link layer addressing is contained within the frame header and specifies the frame destination node on the local network. The data link layer address is only used for local delivery. In a TCP/IP network, all OSI Layer 2 protocols work with IP at OSI Layer 3. However, the Layer 2 protocol used depends on the logical topology and the physical media. Each protocol performs media access control for specified Layer 2 logical topologies. The Layer 2 protocol that is used for a particular network topology is determined by the technology used to implement that topology. Data link layer protocols include: Ethernet, 802.11 Wireless, PPP, HDLC, and Frame Relay.

## Module 7

**Ethernet Frame**

Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. Ethernet uses the LLC and MAC sublayers of the data link layer to operate. Data encapsulation includes the following: Ethernet frame, Ethernet addressing, and Ethernet error detection. Ethernet LANs use switches that operate in full-duplex. The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.

**Ethernet MAC Address**

Binary number system uses the digits 0 and 1. Decimal uses 0 through 9. Hexadecimal uses 0 through 9 and the letters A through F. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model. An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes. An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor assigned value. When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

**The MAC Address Table**

A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses. The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table. As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.

**Switch Speeds and Forwarding Methods**

Switches use one of the following forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free. Two methods of memory buffering are port-based memory and shared memory. There are two types of duplex settings used for communications on an Ethernet network: full-duplex and half-duplex. Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability along with their highest common bandwidth. Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.

## Module 8

**Network Layer Characteristics**

The network layer (OSI Layer 3) provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principle network layer communication protocols. The network layer also includes the routing protocol OSPF and messaging protocols such as ICMP. Network layer protocols perform four basic operations: addressing end devices, encapsulation, routing, and de-encapsulation. IPv4 and IPv6 specify the packet structure and processing used to carry the data from one host to another host. IP encapsulates the transport layer segment by adding an IP header, which is used to deliver the packet to the destination host. The IP header is examined by Layer 3 devices (i.e., routers) as it travels across a network to its destination. The characteristics of IP are that it is connectionless, best effort, and media independent. IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. The IP protocol does not guarantee that all packets that are delivered are, in fact, received. This is the definition of the unreliable, or best effort characteristic. IP operates independently of the media that carry the data at lower layers of the protocol stack.

**IPv4 Packet**

An IPv4 packet header consists of fields containing information about the packet. These fields contain binary numbers which are examined by the Layer 3 process. The binary values of each field identify various settings of the IP packet. Significant fields in the IPv4 packet header include: version, DS, header checksum, TTL, protocol, and the source and destination IPv4 addresses.

**IPv6 Packet**

IPv6 is designed to overcome the limitations of IPv4 including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 increases the available address space, improves packet handling, and eliminates the need for NAT. The fields in the IPv6 packet header include: version, traffic class, flow label, payload length, next header, hop limit, and the source and destination IPv6 addresses.

**How a Host Routes**

A host can send a packet to itself, another local host, and a remote host. In IPv4, the source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to determine whether the destination host is on the same network. In IPv6, the local router advertises the local network address (prefix) to all devices on the network, to make this determination. The default gateway is the network device (i.e., router) that can route traffic to other networks. On a network, a default gateway is usually a router that has a local IP address in the same address range as other hosts on the local network, can accept data into the local network and forward data out of the local network, and route traffic to other networks. A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically via DHCP or it is configured manually. In IPv6, the router advertises the default gateway address, or the host can be configured manually. On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table.

**Introduction to Routing**

When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway which is usually the local router. What happens when a packet arrives on a router interface? The router examines the packet’s destination IP address and searches its routing table to determine where to forward the packet. The routing table contains a list of all known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry. The routing table of a router stores three types of route entries: directly connected networks, remote networks, and a default route. Routers learn about remote networks manually, or dynamically using a dynamic routing protocol. Static routes are route entries that are manually configured. Static routes include the remote network address and the IP address of the next hop router. OSPF and EIGRP are two dynamic routing protocols. The **show ip route** privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. At the beginning of an IPv4 routing table is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include:

**L** - Directly connected local interface IP address

**C** - Directly connected network

**S** - Static route was manually configured by an administrator

**O** - Open Shortest Path First (OSPF)

**D** - Enhanced Interior Gateway Routing Protocol (EIGRP)

## Module 9

**MAC and IP**

Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network. If the destination IP address is on the same network, the destination MAC address will be that of the destination device. When the destination IP address (IPv4 or IPv6) is on a remote network, the destination MAC address will be the address of the host default gateway (i.e., the router interface). Along each link in a path, an IP packet is encapsulated in a frame. The frame is specific to the data link technology associated that is associated with that link, such as Ethernet. If the next-hop device is the final destination, the destination MAC address will be that of the device Ethernet NIC. How are the IP addresses of the IP packets in a data flow associated with the MAC addresses on each link along the path to the destination? For IPv4 packets, this is done through a process called ARP. For IPv6 packets, the process is ICMPv6 ND.

**ARP**

Every IP device on an Ethernet network has a unique Ethernet MAC address. When a device sends an Ethernet Layer 2 frame, it contains these two addresses: destination MAC address and source MAC address. A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address. ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings. The ARP request is encapsulated in an Ethernet frame using this header information: source and destination MAC addresses and type. Only one device on the LAN will have an IPv4 address that matches the target IPv4 address in the ARP request. All other devices will not reply. The ARP reply contains the same header fields as the request. Only the device that originally sent the ARP request will receive the unicast ARP reply. After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table. When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway. This is the interface of the local router. For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. Commands may also be used to manually remove some or all of the entries in the ARP table. As a broadcast frame, an ARP request is received and processed by every device on the local network, which could cause the network to slow down. A threat actor can use ARP spoofing to perform an ARP poisoning attack.

**Neighbor Discovery**

IPv6 does not use ARP, it uses the ND protocol to resolve MAC addresses. ND provides address resolution, router discovery, and redirection services for IPv6 using ICMPv6. ICMPv6 ND uses five ICMPv6 messages to perform these services: neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect. Much like ARP for IPv4, IPv6 devices use IPv6 ND to resolve the MAC address of a device to a known IPv6 address.

## Module 10

**Configure Initial Router Settings**

The following tasks should be completed when configuring initial settings on a router.

1. Configure the device name.
2. Secure privileged EXEC mode.
3. Secure user EXEC mode.
4. Secure remote Telnet / SSH access.
5. Secure all passwords in the config file.
6. Provide legal notification.
7. Save the configuration.

**Configure Interfaces**

For routers to be reachable, the router interfaces must be configured. The Cisco ISR 4321 router is equipped with two Gigabit Ethernet interfaces: GigabitEthernet 0/0/0 (G0/0/0) and GigabitEthernet 0/0/1 (G0/0/1). The tasks to configure a router interface are very similar to a management SVI on a switch. Using the **no shutdown** command activates the interface. The interface must also be connected to another device, such as a switch or a router, for the physical layer to be active. There are several commands that can be used to verify interface configuration including the **show ip interface brief** and **show ipv6 interface brief**, the **show ip route** and **show ipv6 route**, as well as **show interfaces**, **show ip interface** and **show ipv6 interface.**

**Configure the Default Gateway**

For an end device to communicate over the network, it must be configured with the correct IP address information, including the default gateway address. The default gateway address is generally the router interface address for the router that is attached to the local network of the host. The IP address of the host device and the router interface address must be in the same network. To connect to and manage a switch over a local IP network, it must have a switch virtual interface (SVI) configured. The SVI is configured with an IPv4 address and subnet mask on the local LAN. The switch must also have a default gateway address configured to remotely manage the switch from another network. To configure an IPv4 default gateway on a switch, use the **ip default-gateway ip-address** global configuration command. Use the IPv4 address of the local router interface that is connected to the switch.

## Module 11

**IPv4 Addressing Structure**

An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion. The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network. A host requires a unique IPv4 address and a subnet mask to show the network/host portions of the address. The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, which is a “/” followed by the number of bits set to 1. Logical AND is the comparison of two bits. Only a 1 AND 1 produces a 1 and all other combination results in a 0. Any other combination results in a 0. Within each network there are network addresses, host addresses, and a broadcast address.

**IPv4 Unicast, Broadcast, and Multicast**

Unicast transmission refers to a device sending a message to one other device in one-to-one communications. A unicast packet is a packet with a destination IP address that is a unicast address which is the address of a single recipient. Broadcast transmission refers to a device sending a message to all the devices on a network in one-to-all communications. A broadcast packet has a destination IP address with all ones (1s) in the host portion, or 32 one (1) bits. Multicast transmission reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group. A multicast packet is a packet with a destination IP address that is a multicast address. IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range.

**Types of IPv4 Addresses**

Public IPv4 addresses are globally routed between ISP routers. Not all available IPv4 addresses can be used on the internet. There are blocks of addresses called private addresses that are used by most organizations to assign IPv4 addresses to internal hosts. Most internal networks use private IPv4 addresses for addressing all internal devices (intranet); however, these private addresses are not globally routable. Loopback addresses used by a host to direct traffic back to itself. Link-local addresses are more commonly known as APIPA addresses, or self-assigned addresses. In 1981, IPv4 addresses were assigned using classful addressing: A, B, or C. Public IPv4 addresses must be unique, and are globally routed over the internet. Both IPv4 and IPv6 addresses are managed by the IANA, which allocates blocks of IP addresses to the RIRs.

**Network Segmentation**

In an Ethernet LAN, devices broadcast to locate other devices using ARP. Switches propagate broadcasts out all interfaces except the interface on which it was received. Routers do not propagate broadcasts, instead each router interface connects a broadcast domain and broadcasts are only propagated within that specific domain. A large broadcast domain is a network that connects many hosts. A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network. The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets. Subnetting reduces overall network traffic and improves network performance. An administrator may subnet by location, between networks, or by device type.

**Subnet an IPv4 Network**

IPv4 subnets are created by using one or more of the host bits as network bits. This is done by extending the subnet mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits that are borrowed, the more subnets that can be defined. The more bits that are borrowed to increase the number of subnets also reduces the number of hosts per subnet. Networks are most easily subnetted at the octet boundary of /8, /16, and /24. Subnets can borrow bits from any host bit position to create other masks.

**Subnet a /16 and a /8 Prefix**

In a situation requiring a larger number of subnets, an IPv4 network is required that has more hosts bits available to borrow. To create subnets, you must borrow bits from the host portion of the IPv4 address of the existing internetwork. Starting from the left to the right with the first available host bit, borrow a single bit at a time until you reach the number of bits necessary to create the number of subnets required. When borrowing bits from a /16 address, start borrowing bits in the third octet, going from left to right. The first address is reserved for the network address and the last address is reserved for the broadcast address.

**Subnet to Meet Requirements**

A typical enterprise network contains an intranet and a DMZ. Both have subnetting requirements and challenges. The intranet uses private IPv4 addressing space. The 10.0.0.0/8 can also be subnetted using any other number of prefix lengths, such as /12, /18, /20, etc., giving the network administrator many options. Because these devices need to be publicly accessible from the internet, the devices in the DMZ require public IPv4 addresses. Organizations must maximize their own limited number of public IPv4 addresses. To reduce the number of unused host addresses per subnet, the network administrator must subnet their public address space into subnets with different subnet masks. This is known as Variable Subnet Length Masking (VLSM). Administrators must consider how many host addresses are required for each network, and how many subnets are needed.

**Variable Length Subnet Masking**

Traditional subnetting might meet an organization’s needs for its largest LAN and divide the address space into an adequate number of subnets. But it likely also results in significant waste of unused addresses. VLSM allows a network space to be divided into unequal parts. With VLSM, the subnet mask will vary depending on how many bits have been borrowed for a particular subnet (this is the “variable” part of the VLSM). VLSM is just subnetting a subnet. When using VLSM, always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied. Subnets always need to be started on an appropriate bit boundary.

**Structured Design**

A network administrator should study the network requirements to better plan how the IPv4 network subnets will be structured. This means looking at the entire network, both the intranet and the DMZ, and determining how each area will be segmented. The address plan includes determining where address conservation is needed (usually within the DMZ), and where there is more flexibility (usually within the intranet). Where address conservation is required the plan should determine how many subnets are needed and how many hosts per subnet. This is usually required for public IPv4 address space within the DMZ. This will most likely include using VLSM. The address plan includes how host addresses will be assigned, which hosts will require static IPv4 addresses, and which hosts can use DHCP for obtaining their addressing information. Within a network, there are different types of devices that require addresses: end user clients, servers and peripherals, servers that are accessible from the internet, intermediary devices, and gateways. When developing an IP addressing scheme, have a set pattern of how addresses are allocated to each type of device. This helps when adding and removing devices, filtering traffic based on IP, as well as simplifying documentation.