##################
31 Before CCNA
##################

#################
OSI
#################

7 Refers to interfaces betweeen networks and application software also includes authentication service

6 Defines the organization and format of data includes encryption

5 Entablish end to end bidirectional flows beteween end points includes managing transaction flows

4 Provides a vriety of services between 2 computers including connection stablishment and termination ,
flow control error recovery segmentation of large data block into smaller

3 refers to logical addressing path and path determination

2 formats data into frame appropiate for transmission onto some phisical medium Defines rules for when the medium can be used. Defines the means by which to recognize transmission errors.

1 Defines the electrical, optical, cabling, connectors, and procedural details required for transmitting bits, represented as some form of energy passing over a physical medium.

TCP/IP Layers and Protocols
The TCP/IP model defines four categories of functions that must occur for communications to succeed. Most protocol models describe vendor-specific protocol stacks. However, because the TCP/IP model is an open standard, one company does not control the definition of the model.

TCP/IP

Application Represents data to the user and controls dialogue examples DNS,Telnet, SMTP, POP3, IMAP, DHCP,HTTP,FTP,SNMP

Transport Supports communication between diverse devices across diverse networks Examples TCP, UDP

Internet Determines the best path through the network Examples IP, ARP, ICMP

Network access Controls the hardware devices and media that make up the network Exanple Ethernet,Wireless

Error Recovery

TCP provides error recovery, also known as reliability, during data transfer sessions between two end devices that have established a connection. The Sequence and Acknowledgment fields in the TCP header track every byte of data transfer and ensure that missing bytes are retransmitted.

TCP Header

TCP provides error recovery, but to do so, it consumes more bandwidth and uses more processing cycles than UDP.TCP and UDP rely on IP for end-to-end delivery.TCP is concerned with provid- ing services to the applications of the sending and receiving computers.To provide all these services, TCP uses a variety of fields in its header

Flow control

TCP handles flow control through a process called windowing.The two end devices negotiate the window size when initially establishing the connection; then they dynamically renegotiate window size during the life of the connection, increasing its size until it reaches the maximum window size of 65,535 bytes or until errors occur.Window size is specified in the Window field of the TCP header. After sending the amount of data specified in the window size, the source must receive an acknowledgment before sending the next window size of data.

Connection Stablishment and termination

Connection establishment is the process of initializing Sequence and Acknowledgment fields and agreeing on port numbers and window size.The three-way connection establishment phase

When data transfer is complete, a four-way termination sequence occurs.This sequence uses an additional flag, called the FIN bit

UDP

TCP establishes and terminates connections between endpoints, whereas UDP does not.Therefore, UDP is called a connectionless protocol. It provides no reliability, no windowing, and no reordering of the data. However, UDP does provide data transfer and multiplexing using port numbers, and it does so with fewer bytes of overhead and less processing than TCP. Applications that use UDP, such as VoIP, trade the possibility of some data loss for less delay.

############################
Cabling and connection
############################

Use straight-through cables for the following connections:
■ Switch to router Ethernet port
■ Computer to switch
■ Computer to hub

Use crossover cables for the following connections:
■ Switch to switch
■ Switch to hub
■ Hub to hub
■ Router to router (Ethernet ports)
■ Computer to computer
■ Computer to router Ethernet port

The two ways to configure Cisco devices are as follows:
■ Console terminal: Use an RJ-45–to–RJ-45 rollover cable and a computer with the terminal communications software (such as HyperTerminal or Tera Term) to establish a direct connection. Optionally, you can connect a mini-USB cable to the mini-USB console port, if available.
■ Remote terminal: Use an external modem connected to the auxiliary port (routers only) to remotely configure the device.

After a device is configured, you can access it using three additional methods:
■ Establish a terminal (vty) session using Telnet.
■ Configure the device through the current connection (console or auxiliary) or download a previously written startup config file from a Trivial File Transfer Protocol (TFTP) server on the network.
■ Download a configuration file using a network management software application.

CLI EXEC Sessions
Cisco IOS separates the EXEC session into two basic access levels:
■ User EXEC mode: Access to only a limited number of basic monitoring and troubleshooting
commands, such as show and ping
■ Privileged EXEC mode: Full access to all device commands, including configuration and
management

Half Duplex, Full Duplex, and Port Speed

Half-duplex communication is unidirectional data flow in which a device can either send or receive on an Ethernet LAN—but not both at the same time.Today’s LAN networking devices and end device network interface cards (NICs) operate at full duplex as long as the device is connected to another device capable of full-duplex communication. Full-duplex communication increases the effective bandwidth by allowing both ends of

a connection to transmit and receive data simultane- ously; this is known as bidirectional.This microsegmented LAN is collision free. Gigabit Ethernet
and 10-Gbps NICs require full-duplex connections to operate. Port speed is simply the bandwidth rating of the port.The most common speeds today are 100 Mbps, 1 Gbps, and 10 Gbps.
Although the default duplex and speed setting for Cisco Catalyst 2960 and 3560 switches is auto, you can manually configure speed with the speed and duplex commands.

Automatic Medium-Dependent Interface Crossover (auto-MDIX)

In the past, switch-to-switch or switch-to-router connections required using different Ethernet cables (crossover or straight-through). Using the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface eliminates this problem.When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.
The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches.The Gigabit Ethernet standard requires auto-MDIX, so any 1000-Mbps port has this capability.When using auto-MDIX on an interface, the interface speed and duplex must be set to auto so that the feature operates correctly.

################################
Hierarchical campus design
################################

Hierarchical Campus Designs
Hierarchical campus design involves dividing the network into discrete layers. Each layer provides specific functions that define its role within the overall network. By separating the various functions that exist on a network, the network design becomes modular, which facilitates scalability and performance.The hierarchical design model is divided into three layers:
■ Access layer: Provides local and remote user access
■ Distribution layer: Controls the flow of data between the access and core layers
■ Core layer: Acts as the high-speed redundant backbone

For smaller networks, the core is often collapsed into the distribution layer for a two-tier design

##############
Routing
##############

Packet Forwarding

Packet forwarding by routers is accomplished through path determination and switching functions. The path determination function is the process the router use to determine which path to use when forwarding a packet.To determine the best path, the router searches its routing table for a network address that matches the packet’s destination IP address.

This search results in one of three path determinations:

■ Directly connected network: If the destination IP address of the packet belongs to a device on a network that is directly connected to one of the router’s interfaces, that packet is forward- ed directly to that device.This means the destination IP address of the packet is a host address on the same network as this router’s interface.

■ Remote network: If the destination IP address of the packet belongs to a remote network, the packet is forwarded to another router. Remote networks can be reached only by forwarding packets to another router.

■ No route determined: If the destination IP address of the packet does not belong to a con- nected or remote network and the router does not have a default route, the packet is discarded. The router sends an Internet Control Message Protocol (ICMP) Unreachable message to the source IP address of the packet.

In the first two results, the router completes the process by switching the packet out the correct interface. It does this by reencapsulating the IP packet into the appropriate Layer 2 data-link frame format for the exit interface.The type of interface determines the type of Layer 2 encapsulation. For example, if the exit interface is Fast Ethernet, the packet is encapsulated in an Ethernet frame. If the exit interface is a serial interface configured for PPP, the IP packet is encapsulated in a PPP frame.

Routing Methods

A router can learn routes from three basic sources:

■ Directly connected routes: Automatically entered in the routing table when an interface is activated with an IP address
■ Static routes: Manually configured by the network administrator and entered in the routing table if the exit interface for the static route is active
■ Dynamic routes: Learned by the routers through sharing routes with other routers that use the same routing protocol

In many cases, the complexity of the network topology, the number of networks, and the need for the network to automatically adjust to changes require the use of a dynamic routing protocol. Dynamic routing certainly has several advantages over static routing; however, networks still use static routing

Routing protocols are classified into different groups according to their characteristics:
■ IGP or EGP
■ Distance vector or link state
■ Classful or classless

IGP and EGP

An autonomous system (AS) is a collection of routers under a common administration that presents a common, clearly defined routing policy to the Internet.Typical examples are a large company's internal network and an ISP's network. Most company networks are not autonomous systems; in most cases, a company network is a network within its ISP's autonomous system. Because the Internet is based on the autonomous system concept, two types of routing protocols are required:

■ Interior gateway protocols (IGP): Used for intra-AS routing—that is, routing inside an AS

■ Exterior gateway protocols (EGP): Used for inter-AS routing—that is, routing between
autonomous systems

Distance Vector Routing Protocols

Distance vector means that routes are advertised as vectors of distance and direction. Distance is defined in terms of a metric such as hop count, and direction is the next-hop router or exit inter- face. Distance vector protocols typically use the Bellman-Ford algorithm for the best-path route determination.

Some distance vector protocols periodically send complete routing tables to all connected neigh- bors. In large networks, these routing updates can become enormous, causing significant traffic on the links.

Although the Bellman-Ford algorithm eventually accumulates enough knowledge to maintain a database of reachable networks, the algorithm does not allow a router to know the exact topology of an internetwork.The router knows only the routing information received from its neighbors. Distance vector protocols use routers as signposts along the path to the final destination.The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there.A distance vector routing protocol does not have a map of the network topology.

Distance vector protocols work best in these situations:
■ When the network is simple and flat and does not require a hierarchical design
■ When the administrators do not have enough knowledge to configure and troubleshoot link-state protocols
■ When specific types of networks, such as hub-and-spoke networks, are being implemented
■ When worst-case convergence times in a network are not a concern

Link-State Routing Protocols

In contrast to distance vector routing protocol operation, a router configured with a link-state rout- ing protocol can create a complete view, or topology, of the network by gathering information from all the other routers.Think of a link-state routing protocol as having a complete map of the network topology.The signposts along the way from source to destination are not necessary because all link-state routers are using an identical map of the network.A link-state router uses the link-state information to create a topology map and to select the best path to each destination network in the topology.
With some distance vector routing protocols, routers periodically send updates of their routing information to their neighbors. Link-state routing protocols do not use periodic updates. After the network has converged, a link-state update is sent only when the topology changes.
Link-state protocols work best in these situations:
■ When the network design is hierarchical, which is typically the case in large networks
■ When the administrators have good knowledge of the implemented link-state routing protocol
■ When fast convergence of the network is crucial

Classful Routing Protocols

Classful routing protocols do not send subnet mask information in routing updates.The first routing protocols, such as Routing Information Protocol (RIP), were classful.When those protocols were created, network addresses were allocated based on class: Class A, B, or C. A routing protocol did not need to include the subnet mask in the routing update because the network mask could be determined based on the first octet of the network address.
Classful routing protocols can still be used in some of today's networks, but because they do not include the subnet mask, they cannot be used in all situations. Classful routing protocols cannot be used when a network is subnetted using more than one subnet mask. In other words, classful routing protocols do not support variable-length subnet masking (VLSM). Other limitations come into play with classful routing protocols, including their inability to sup- port discontiguous networks and supernets. Classful routing protocols include Routing Information Protocol version 1 (RIPv1) and Interior Gateway Routing Protocol (IGRP).

Classless Routing Protocols

Classless routing protocols include the subnet mask with the network address in routing updates. Today's networks are no longer allocated based on class, and the subnet mask cannot be determined by the value of the first octet. Classless routing protocols are required in most networks today because of their support for VLSM and discontiguous networks and supernets. Classless routing protocols include Routing Information Protocol version 2 (RIPv2), Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP).

Dynamic Routing Metrics

In some cases, a routing protocol learns of more than one route to the same destination from the same routing source.To select the best path, the routing protocol must be capable of evaluating and differentiating among the available paths.A metric is used for this purpose.Two different routing protocols might choose different paths to the same destination because they use different metrics. Metrics used in IP routing protocols include the following:

■ RIP—Hop count: The best path is chosen by the route with the lowest hop count.
■ IGRP and EIGRP—Bandwidth, delay, reliability, and load: The best path is chosen by the route with the smallest composite metric value calculated from these multiple parameters. By default, only bandwidth and delay are used.
■ IS-IS and OSPF—Cost: The best path is chosen by the route with the lowest cost. The Cisco implementation of OSPF uses bandwidth to determine the cost.

routing protocols are capable of automatically load balancing traffic for up to four equal-cost routes, by default. EIGRP is also capable of load balancing across unequal-cost paths.

Administrative Distance

Sometimes a router learns a route to a remote network from more than one routing source. For example, a static route might have been configured for the same network/subnet mask that was learned dynamically by a dynamic routing protocol, such as RIP.The router must choose which route to install.
Although it is less common, more than one dynamic routing protocol can be deployed in the same network. In some situations, it might be necessary to route the same network address using multiple routing protocols, such as RIP and OSPF. Because different routing protocols use different metrics—for example, RIP uses hop count and OSPF uses bandwidth—it is not possible to compare metrics to determine the best path.
Administrative distance (AD) defines the preference of a routing source. Each routing source— including specific routing protocols, static routes, and even directly connected networks—is priori- tized in order of most preferable to least preferable, using an AD value. Cisco routers use the AD feature to select the best path when they learn about the same destination network from two or more different routing sources.

The AD value is an integer value from 0 to 255.The lower the value, the more preferred the route source. An administrative distance of 0 is the most preferred. Only a directly connected network has an AD of 0, which cannot be changed. An AD of 255 means the router will not believe the source of that route, and it will not be installed in the routing table

Routing Loop Prevention

Without preventive measures, distance vector routing protocols can cause severe routing loops in a network.A routing loop is a condition in which a packet is continuously transmitted within a series of routers without ever reaching its intended destination network.A routing loop can occur when two or more routers have inaccurate routing information to a destination network.

Several mechanisms are available to eliminate routing loops, primarily with distance vector routing protocols.These mechanisms include the following:
■ A maximum metric to prevent count to infinity: To eventually stop the incrementing of a metric during a routing loop, infinity is defined by setting a maximum metric value. For example, RIP defines infinity as 16 hops, an unreachable metric.When the routers “count to infinity,” they mark the route as unreachable.

■ Hold-down timers: Routers are instructed to hold any changes that might affect routes for a specified period of time. If a route is identified as down or possibly down, any other informa- tion for that route containing the same status, or worse, is ignored for a predetermined amount of time (the hold-down period) so that the network has time to converge.

■ Hold-down timers: Routers are instructed to hold any changes that might affect routes for a specified period of time. If a route is identified as down or possibly down, any other informa- tion for that route containing the same status, or worse, is ignored for a predetermined amount of time (the hold-down period) so that the network has time to converge.

■ Route poisoning or poison reverse: The route is marked as unreachable in a routing update that is sent to other routers. Unreachable is interpreted as a metric that is set to the maximum.

■ Triggered updates: A routing table update is sent immediately in response to a routing change.Triggered updates do not wait for update timers to expire.The detecting router immediately sends an update message to adjacent routers.

■ TTL field in the IP header: The Time To Live (TTL) field avoids a situation in which an undeliverable packet circulates endlessly on the network. With TTL, the source device of the packet sets the 8-bit field with a value.This TTL value is decreased by 1 by every router in the path until the packet reaches its destination. If the TTL value reaches 0 before the packet arrives at its destination, the packet is discarded, and the router sends an ICMP error message back to the source of the IP packet.

Link-State Routing Protocol Features

Just as distance vector protocols send routing updates to their neighbors, link-state protocols send link-state updates to neighboring routers, which then forward that information to their neighbors, and so on. Also as with distance vector protocols, at the end of the process, routers that use link-state protocols add the best routes to their routing tables, based on metrics. However, beyond this level of explanation, these two types of routing protocol algorithms have little in common.

Link-state routers flood detailed information about the internetwork to all the other routers so that every router has the same information about the internetwork. Routers use this link-state database (LSDB) to calculate the current best routes to each subnet.

OSPF, the most popular link-state IP routing protocol, advertises information in routing update messages of various types.The updates contain information called link-state advertisements (LSA).
After the LSA has been flooded, even if the LSAs do not change, link-state protocols require periodic reflooding of the LSAs by default every 30 minutes. However, if an LSA changes, the router immediately floods the changed LSA.

Calculating the Dijkstra Algorithm

The flooding process alone does not cause a router to learn what routes to add to the IP
routing table. Link-state protocols must then find and add routes to the IP routing table by using the Dijkstra shortest path first (SPF) algorithm.
The SPF algorithm is run on the LSDB to create the SPF tree.The LSDB holds all the information about all the possible routers and links. Each router must view itself as the starting point and each subnet as the destination, and it must use the SPF algorithm to build its own SPF tree to pick the best route to each subnet.

To pick the best route, a router's SPF algorithm adds the cost associated with each link between itself and the destination subnet over each possible route.

Two Router Functions

When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination.The primary functions of a router are to
■ Determine the best path for forwarding packets, based on the information in its routing table
■ Forward packets toward their destinations

Longest Match Determines Best Path

The best path in the routing table is also known as the longest match.The router uses the longest match process to find a match between the destination IP address of the packet and a routing entry in the routing table.The prefix length of the route in the routing table is used to determine the minimum number of far-left bits that must match.The longest match is the route in the routing table that has the greatest number of far-left bits matching the destination IP address of the packet.The route with the greatest number of equivalent far-left bits, or the longest match, is always the preferred route.

Three Packet Forwarding Decisions

After a router has determined the best path based on the longest match in the routing table, it can do one of three things:
■ Forward the packet to a device on a directly connected network
■ Forward the packet to a next-hop router
■ Drop the packet because there is no match in the routing table
The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. For example, the data link frame format for a serial link could be Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) protocol, or some other Layer 2 protocol.

Components of the RoutingTable

A router examines the destination IP address of a packet 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 forwards a packet using the best (longest) matching route entry.

Recall that a routing table stores three types of routing entries:

■ Directly connected networks: These network route entries are active router interfaces.

■ Remote networks: These network route entries are connected to other routers. Routers learn about remote networks either by being explicitly configured by an administrator or by exchanging route information using a dynamic routing protocol

■ Default route: The default route is used when there is no better (longer) match in the IP routing table.

At the beginning of each routing table entry is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include these:
■ L: Directly connected local interface IP address
■ C: Directly connected network
■ S: Static route manually configured by an administrator
■ O: OSPF
■ D: EIGRP

Static and Default Routing Overview

When a router configured with a dynamic routing protocol can learn routes from other routers without additional input from the network administrator, why would you use static routing? Situations vary, and other reasons might be unique to a particular implementation, but, in general, you use static routing in these cases:

■ In a small network that requires only simple routing
■ In a hub-and-spoke network topology
■ When you want to create a quick ad hoc route
■ As a backup when the primary route fails
In general, you do not use static routes in these cases:
■ In a large network
■ When the network is expected to scale

Static routes are commonly used when you are routing from a larger network to a stub network (a network that is accessed by a single link). Static routes can also be useful for specifying a default route or gateway of last resort

IPv4 Static Routes Using the Exit Interface Parameter

To avoid a recursive lookup and have a router immediately send packets to the exit interface, con- figure the static route using the exit-interface parameter instead of the ip-address next-hop parameter.

Default Route

A default route is a route that matches all packets. Commonly called a quad-zero route, a default route uses 0.0.0.0 (thus the term quad-zero) for both the network-address and the subnet-mask param- eters, as in this syntax

#########
OSPF
#########

OSPF Message Format

The data portion of an OSPF message is encapsulated in a packet.This data field can include one of five OSPF packet type

The OSPF packet header is included with every OSPF packet, regardless of its type.The OSPF packet header and packet type–specific data are then encapsulated in an IP packet. In the IP packet header, the protocol field is set to 89 to indicate OSPF, and the destination address is typically set to one of two multicast addresses: 224.0.0.5 or 224.0.0.6. If the OSPF packet is encapsulated in
an Ethernet frame, the destination MAC address is also a multicast address: 01-00-5E-00-00-05 or 01-00-5E-00-00-06.

Each of the five OSPF packet types serves a specific purpose in the routing process:
■ Hello: Hello packets establish and maintain adjacency with other OSPF routers.

■ DBD: The database description (DBD) packet contains an abbreviated list of the sending router's link-state database. Receiving routers use it to check against the local link-state database.
■ LSR: Receiving routers can request more information about any entry in the DBD by sending a link-state request (LSR).
■ LSU: Link-state update (LSU) packets reply to LSRs and announce new information. LSUs contain 11 types of link-state advertisements (LSAs).
■ LSAck: When an LSU is received, the router sends a link-state acknowledgment (LSAck) to confirm receipt of the LSU.

Neighbor Establishment

OSPF neighbors exchange hello packets to establish adjacency

OSPF information

■ Type: OSPF packet type: Hello (Type 1), DBD (Type 2), LS Request (Type 3), LS Update (Type 4), LS ACK (Type 5)
■ Router ID: ID of the originating router
■ Area ID: Area from which the packet originated
■ Network Mask: Subnet mask associated with the sending interface
■ Hello Interval: Number of seconds between the sending router's hellos
■ Router Priority: Used in DR/BDR election
■ Designated Router (DR): Router ID of the DR, if any
■ Backup Designated Router (BDR): Router ID of the BDR, if any
■ List of Neighbors: The OSPF router ID of the neighboring router(s)

Hello packets are used to do the following:

■ Discover OSPF neighbors and establish neighbor adjacencies
■ Advertise parameters on which two routers must agree to become neighbors
■ Elect the DR and BDR on multiaccess networks such as Ethernet and Frame Relay

Receiving an OSPF hello packet on an interface confirms for a router that another OSPF router exists on this link. OSPF then establishes adjacency with the neighbor.To establish adjacency, two OSPF routers must have the following matching interface values:
■ Hello Interval
■ Dead Interval
■ Network Type
■ Area ID

Before the two routers can establish adjacency, both interfaces must be part of the same network, including the same subnet mask. Full adjacency happens after the two routers have exchanged any necessary LSUs and have identical link-state databases. By default, OSPF hello packets are sent to the multicast address 224.0.0.5 (ALLSPFRouters) every 10 seconds on multiaccess and point-to- point segments and every 30 seconds on nonbroadcast multiaccess (NBMA) segments (Frame Relay, X.25,ATM).The default dead interval is four times the hello interval.

OSPF DR and BDR

Multiaccess networks create two challenges for OSPF regarding the flooding of LSAs:

- Creation of multiple adjacencies, with one adjacency for every pair of routers
- Extensive flooding of LSAs

The solution to managing the number of adjacencies and the flooding of LSAs on a multiaccess network is the designated router (DR).To reduce the amount of OSPF traffic on multiaccess networks, OSPF elects a DR and a backup DR (BDR).The DR is responsible for updating all other OSPF routers when a change occurs in the multiaccess network.The BDR monitors the DR and takes over as DR if the current DR fails.All other routers become DROTHERs. A DROTHER is a router that is neither the DR nor the BDR.

OSPF Algorithm

Each OSPF router maintains a link-state database containing the LSAs received from all other routers.When a router has received all the LSAs and built its local link-state database, OSPF uses Dijkstra's shortest path first (SPF) algorithm to create an SPF tree.This algorithm accumulates costs along each path, from source to destination.The SPF tree is then used to populate the IP routing table with the best paths to each network

Each router determines its own cost to each destination in the topology. In other words, each router uses the SPF algorithm to calculate the cost of each path to a network and determines the best path to that network from its own perspective.

Link-State Routing Process

The following list summarizes the link-state routing process OSPF uses.All OSPF routers complete the following generic link-state routing process to reach a state of convergence:

Step 1 Each router learns about its own links and its own directly connected networks.This is done by detecting that an interface has a Layer 3 address configured and is in the up state.

Step 2 Each router is responsible for establishing adjacency with its neighbors on directly connected networks by exchanging hello packets.

Step 3. Each router builds a link-state packet (LSP) containing the state of each directly connected link.This is done by recording all the pertinent information about each neighbor, including neighbor ID, link type, and bandwidth.

Step 4. Each router floods the LSP to all neighbors, which then store all LSPs received in a database. Neighbors then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local database.

Step 5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network.The SPF algorithm is used to construct the map of the topology and determine the best path to each network.All routers have a common map or tree of the topology, but each router independently determines the best path to each network within that topology.

OSPFv2 Versus OSPFv3

OSPFv3 has the same functionality as OSPFv2 but uses IPv6 as the network layer transport, communicating with OSPFv3 peers and advertising IPv6 routes. OSPFv3 also uses the SPF algorithm as the computation engine to determine the best paths throughout the routing domain.
As with all other IPv6 routing protocols, OSPFv3 has separate processes from its IPv4 counterpart. OSPFv2 and OSPFv3 each have separate adjacency tables, OSPF topology tables, and IP routing tables.

Multiarea OSPF Operation

Single-area OSPF works fine in smaller networks in which the number of links is manageable. However, consider an OSPF single-area network with 900 routers and several thousand subnets. In this situation, the single-area design causes the following problems:
■ Large routing tables: By default, OSPF does not summarize routing updates.
■ Large link-state database (LSDB): In a single area, each router must maintain a database of all active links in the routing domain, regardless of whether that router is currently using a particular link.
■ Frequent SPF calculations: In a large network, changes to the LSDB can cause routers to spend many CPU cycles recalculating the SPF algorithm and updating the routing table.
To address these issues, OSPF supports hierarchical design through the uses of multiple OSPF areas. Multiarea OSPF is useful in larger network deployments to reduce processing and memory overhead.This involves breaking the one large LSDB into several smaller LSDBs by using multiple OSPF areas.

Multiarea OSPF Design

Multiarea OSPF design follows a couple basic rules:
■ Put all interfaces connected to the same subnet inside the same area.
■ An area should be contiguous.
■ Some routers might be internal to an area, with all interfaces assigned to that single area.
■ Some routers might be area border routers (ABRs) because some interfaces connect to the
backbone area and some connect to nonbackbone areas.

■ All nonbackbone areas must connect to the backbone area (Area 0) by having at least one ABR connected to both the backbone area and the nonbackbone area.

Multiarea OSPF Improves Performance

In multiarea OSPF, all areas must connect to the backbone area. Routing still occurs between the areas. ABRs send interarea routes between areas. However, the CPU intensive routing operation of recalculating the SPF algorithm is done only for routes within an area.A change in one area does not cause an SPF algorithm recalculation in other areas.

The following list summarizes how multiarea OSPF improves OSPF performance:
■ The smaller per-area LSDB requires less memory.
■ Routers require fewer CPU cycles to process the smaller per-area LSDB with the SPF algorithm, reducing CPU overhead and improving convergence time.
■ Changes in the network (for example, links failing and recovering) require SPF calculations only on routers connected to the area where the link changed state, reducing the number of routers that must rerun SPF.
■ Less information must be advertised between areas, reducing the bandwidth required to send LSAs.

Process ID

process-id is a number between 1 and 65535 and is chosen by the network administrator.The process ID is locally significant. It does not have to match other OSPF routers to establish adjacencies with those neighbors.This differs from Enhanced Interior Gateway Routing Protocol (EIGRP).The EIGRP process ID and autonomous system number must match before two EIGRP neighbors can become adjacent.

Router ID

The router ID plays an important role in OSPF, uniquely identifying each router in the OSPF routing domain. Cisco routers derive the router ID as follows:

Step 1. The router uses the IP address configured with the OSPF router-id command.

Step 2. If the router ID is not configured, the router chooses the highest IP address of any of its
loopback interfaces.

Step 3. If no loopback interfaces are configured, the router chooses the highest active IP address of any of its physical interfaces.

Because the network administrator can control the OSPF router-id command and because loop- back interfaces clutter the routing table, it is a best practice to configure the router-id command. The router-id command accepts an IPv4 address as its only argument.

The OSPF network command uses a combination of network-address and wildcard-mask.The network address, along with the wildcard mask, specifies the interface or range of interfaces that will be enabled for OSPF using this network command.

The wildcard mask is customarily configured as the inverse of a subnet mask

area area-id refers to the OSPF area.An OSPF area is a group of routers that share link-state infor- mation.All OSPF routers in the same area must have the same link-state information in their link- state databases.Therefore, all the routers within the same OSPF area must be configured with the same area ID on all routers. By convention, the area ID is 0.

Passive Interfaces

By default, OSPF messages are forwarded out all OSPF-enabled interfaces. However, these messages really need to be sent out only interfaces that connect to other OSPF-enabled routers. Sending out unneeded messages on a LAN affects the network in three ways:
■ Inefficient use of bandwidth: Available bandwidth is consumed by transporting unnecessary messages.
■ Inefficient use of resources: All devices on the LAN must process the message.
■ Increased security risk: OSPF messages can be intercepted, and routing updates can be
modified, corrupting the routing table.
Use the passive-interface command to prevent OSPF updates from being sent out unnecessary interfaces

As an alternative, you can make all interfaces passive by using the passive-interface default command.Then you can reenable interfaces that should not be passive by using the no passive- interface interface command.

Cisco IOS Software uses the cumulative bandwidths of the outgoing interfaces from the router to the destination network as the cost value. At each router, the cost for an interface is calculated using the following formula:
Cisco IOS Cost for OSPF = 108/bandwidth in bps

In this calculation, the value 108 is known as the reference bandwidth

An advantage of configuring a cost over setting the interface bandwidth is that the router does not have to calculate the metric when the cost is manually configured. Also, the ip ospf cost command is useful in multivendor environments, where non-Cisco routers can use a metric other than bandwidth to calculate the OSPF costs.

point-to-point links do not elect a DR or BDR.

Hello and Dead Intervals

The default hello interval on multiaccess and point-to-point networks is 10 seconds. Nonbroadcast multiaccess (NBMA) networks default to a 30-second hello interval.The default dead interval is four times the hello interval.

OSPF Network Types

OSPF defines five network types:

■ Point-to-point: Two routers interconnected over a common link. No other routers are on the link. This is often the configuration in WAN links.
■ Broadcast multiaccess: Multiple routers interconnected over an Ethernet network.
■ NBMA: Multiple routers interconnected in a network that does not allow broadcasts, such as
Frame Relay.
■ Point-to-multipoint: Multiple routers interconnected in a hub-and-spoke topology over an NBMA network. Often used to connect branch sites (spokes) to a central site (hub).
■ Virtual links: Special OSPF network used to interconnect distant OSPF areas to the backbone area.
Multiaccess networks create two challenges for OSPF regarding the flooding of LSAs:
■ Creation of multiple adjacencies: Ethernet networks can potentially interconnect many OSPF routers over a common link. Using the formula n(n – 1) / 2, where n equals the number of routers, 5 routers would require 10 separate neighbor adjacencies; 10 routers would require 45

■ Extensive flooding of LSAs: Link-state routers flood their link-state packets when OSPF is initialized or when the topology changes.This flooding can become excessive without a mechanism to reduce the number of adjacencies.

DR/BDR Election

The solution to managing the number of adjacencies and the flooding of LSAs on a multiaccess network is the designated router (DR).To reduce the amount of OSPF traffic on multiaccess networks, OSPF elects a DR and backup DR (BDR).The DR is responsible for updating all other OSPF routers when a change occurs in the multiaccess network.The BDR monitors the DR and takes over as DR if the current DR fails.
The following criteria are used to elect the DR and BDR:
■ The DR is the router with the highest OSPF interface priority.
■ The BDR is the router with the second-highest OSPF interface priority.
■ If OSPF interface priorities are equal, the highest router ID breaks the tie.
When the DR is elected, it remains the DR until one of the following conditions occurs:
■ The DR fails.
■ The OSPF process on the DR fails.
■ The multiaccess interface on the DR fails.
If the DR fails, the BDR assumes the role of DR, and an election is held to choose a new BDR. If a new router enters the network after the DR and BDR have been elected, it will not become the DR or the BDR even if it has a higher OSPF interface priority or router ID than the current DR or BDR.The new router can be elected the BDR if the current DR or BDR fails. If the current DR fails, the BDR becomes the DR, and the new router can be elected the new BDR.
Without additional configuration, you can control the routers that win the DR and BDR elections by doing either of the following:
■ Boot the DR first, followed by the BDR, and then boot all other routers.
■ Shut down the interface on all routers and then issue no shutdown on the DR, then the
BDR, and then all other routers.
The recommended way to control DR/BDR elections, however, is to change the interface priority.

Controlling the DR/BDR Election

Because the DR becomes the focal point for the collection and distribution of LSAs in a multiaccess network, this router must have sufficient CPU and memory capacity to handle the responsibility. Instead of relying on the router ID to decide which routers are elected the DR and BDR, it is better to control the election of these routers with the ip ospf priority interface command:

The priority value defaults to 1 for all router interfaces, which means the router ID determines the DR and BDR. If you change the default value from 1 to a higher value, however, the router with the highest priority becomes the DR, and the router with the next highest priority becomes the BDR.A value of 0 makes the router ineligible to become a DR or BDR.

Troubleshooting OSPF

OSPF States When troubleshooting OSPF neighbors, be aware that the FULL and TWO-WAY states are normal. All other states are transitory.

OSPF Adjacency

Lack of adjacency is a common issue in OSPF troubleshooting because the two OSPF neighbors must agree on several settings. OSPF adjacencies do not form for several reasons:

- The interfaces are not on the same network.
- OSPF network types do not match.
- OSPF hello or dead timers do not match.
- The interface to the neighbor is incorrectly configured as passive.
- An OSPF network command is missing or incorrect.
- Authentication is misconfigured.

#############
ACL
#############

ACL Operation

A router’s default operation is to forward all packets, as long as a route exists for the packet and the link is up. ACLs can help implement a basic level of security. However, they are not the only security solution a large organization should implement. In fact, ACLs increase the latency of routers. If an organization is very large, with routers managing the traffic of hundreds or thousands of users, the administrator more than likely will use a combination of other security implementations

Defining an ACL

An ACL is a router configuration script (that is, a list of statements) that controls whether a router permits or denies packets to pass, based on criteria in the packet header.To determine whether a packet is permitted or denied, it is tested against the ACL statements in sequential order.When a statement matches, no more statements are evaluated; the packet is either permitted or denied.There is an implicit deny any statement at the end of an ACL. If a packet does not match any of the statements in the ACL, it is dropped.

Processing Interface ACLs

ACLs can be applied to an interface for inbound and outbound traffic. However, you need a separate ACL for each direction
For inbound traffic, the router checks for an inbound ACL applied to the interface before doing a route table lookup.Then, for outbound traffic, the router makes sure that a route to the destination exists before checking for ACLs. Finally, if an ACL statement results in a dropped packet, the router sends an ICMP destination unreachable message.

List Logic with IP ACLs

An ACL is a list of commands that are processed in order, from the first statement in the list to the last statement. Each command has different matching logic that the router must apply to each packet when filtering is enabled. ACLs use first-match logic. If a packet matches one line in the ACL, the router takes the action listed in that line of the ACL and ignores the rest of the ACL statements.

Types of ACL

■ Standard IPv4 ACLs: Filter traffic based on source address only

■ Extended IPv4 and IPv6 ACLs: Can filter traffic based on source and destination address,
specific protocols, and source and destination TCP and UDP ports

You can use two methods to identify both standard and extended ACLs:

■ Numbered IPv4 ACLs: Use a number for identification

■ Named IPv4 and IPv6 ACLs: Use a descriptive name or number for identification

Named ACLs must be used with some types of Cisco IOS configurations, including IPv6 ACLs.
However, they provide two basic benefits for standard and extended IPv4 ACLs:

■ By using a descriptive name (such as BLOCK-HTTP), a network administrator can more quickly determine the purpose of an ACL.This is particularly helpful in larger networks, where a router can have many ACLs with hundreds of statements.

Named IP ACLs give you more flexibility in working with the ACL entries. In addition to using more memorable names, using named ACLs instead of numbered ACLs enables you to delete individual statements in a named IP access list.

ACL Design Guidelines

Well-designed and -implemented ACLs add an important security component to your network. Follow these general principles to ensure that the ACLs you create have the intended results:
■ Based on the test conditions, choose a standard or extended, numbered, or named ACL.
■ Only one ACL is allowed per protocol, per direction, and per interface.
■ Organize the ACL to enable processing from the top down. Organize your ACL so that more specific references to a network, subnet, or host appear

before more general ones. Place conditions that occur more frequently before conditions that occur less frequently.
■ All ACLs contain an implicit deny any statement at the end.
■ Create the ACL before applying it to an interface.
■ Depending on how you apply the ACL, the ACL filters traffic either going through the router or going to and from the router, such as traffic to or from the vty lines.
■ You typically should place extended ACLs as close as possible to the source of the traffic that you want to deny. Because standard ACLs do not specify destination addresses, you must put the standard ACL as close as possible to the destination of the traffic you want to deny so that the source can reach intermediary networks.

Adding Comments to Named or Numbered IPv4 ACLs

You can add comments to ACLs by using the remark argument in place of permit or deny. Remarks are descriptive statements that you can use to better understand and troubleshoot either named or numbered ACLs.

A standard IPv6 ACL includes both source and destination address information, but it does not include TCP, UDP, or ICMPv6 information.

###############
NAT
###############

NAT translates nonroutable, private, internal addresses into routable public addresses. NAT also has the benefit of hiding internal IPv4 addresses from outside networks.

A NAT-enabled device typically operates at the border of a stub network.

■ Inside local address: Most likely a private address.

■ Inside global address: A valid public address that the inside host is given when it exits
the NAT router.

■ Outside global address: A reachable IPv4 address assigned to a host on the Internet.

■ Outside local address: The local IPv4 address assigned to a host on the outside network. In most situations, this address is identical to the outside global address of that outside device.

Dynamic and Static NAT

The two types of NAT translation are as follows:

■ Dynamic NAT: Uses a pool of public addresses and assigns them on a first-come, first-served basis or reuses an existing public address

configured on an interface.When a host with a private IPv4 address requests access to the Internet, dynamic NAT chooses an IPv4 address from the pool that another host is not already using. Instead of using a pool, dynamic NAT can be configured to overload an existing public address configured on an interface.

■ Static NAT: Uses a one-to-one mapping of local and global addresses.These mappings remain constant. Static NAT is particularly useful for web servers or hosts that must have a consistent address that is accessible from the Internet.

#NAT Overload

NAT overloading (also called Port Address Translation [PAT]) maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.To do this, a port number also tracks each private address.When a response comes back from the outside, source port numbers determine the correct client for the NAT router to translate the packets.

NAT Benefits
Using NAT offers the following benefits:
■ NAT conserves registered IPv4 address space because, with NAT overload, internal hosts can share a single public IPv4 address for all external communications.
■ NAT increases the flexibility of connections to the public network. Multiple pools, backup pools, and load-balancing pools can be implemented to ensure reliable public network connections.
■ NAT allows the existing scheme to remain while supporting a new public addressing scheme. This means that an organization can change ISPs without needing to change any of its inside clients.
■ NAT provides a layer of network security because private networks do not advertise their inside local addresses outside the organization. However, the phrase NAT firewall is misleading; NAT does not replace firewalls

NAT Limitations
The limitations of using NAT include the following:
■ Performance is degraded: NAT increases switching delays because translating each IPv4 address within the packet headers takes time.
■ End-to-end functionality is degraded: Many Internet protocols and applications depend on end-to-end functionality, with unmodified packets forwarded from the source to the destination.
■ End-to-end IP traceability is lost: Tracing packets that undergo numerous packet address changes over multiple NAT hops becomes much more difficult, making troubleshooting challenging.
■ Tunneling is more complicated: Using NAT also complicates tunneling protocols, such as IPsec, because NAT modifies values in the headers that interfere with the integrity checks that IPsec and other tunneling protocols do.

■ Services can be disrupted: Services that require the initiation of TCP connections from the outside network, or stateless protocols such as those using UDP, can be disrupted.

#########
QOS
#########

QoS
Normal default operation for switches and routers is to process frames and packets in the order in which they are received.This first-in, first-out (FIFO) queueing mechanism does not discriminate between traffic types.
QoS tools are used to classify traffic types based on the following four characteristics:
■ Latency (delay): Latency, or delay, is the amount of time it takes for data to be sent to the receiver. QoS tools can reduce the delay for time-sensitive packets, such as voice and video.
■ Jitter: Jitter is the variance in the delay of packets. QoS tools can even out the delay of packets to improve end-user experience.
■ Loss: Loss refers to the number of lost messages, usually as a percentage of the packets sent. QoS tools reduce packet loss, especially for time-sensitive traffic.
■ Bandwidth: Bandwidth is a measure of the amount of data an interface can send every second. QoS tools can manage which traffic type gets to use the bandwidth next and how much of the bandwidth each type of traffic gets over time.

■ Classification and marking: QoS tools monitor traffic flows and classify packets based on the header contents. Messages are then marked by changing bits in the header.
■ Congestion avoidance: When traffic exceeds available network resources, some traffic might be selectively dropped, delayed, or re-marked to avoid congestion.
■ Congestion management: QoS tools manage the scheduling and shaping of traffic while packets wait their turn in a queue to exit the interface.

Classification and Marking

Classification refers to the process of matching fields in the headers to take some type of QoS action on the packet.These fields can include all the normal fields filtered by ACLs, as well as the Type of Service (ToS) field in an IPv4 packet or Traffic Class field in an IPv6 packet.Marking refers to the process of changing bit values in the ToS or Traffic Class field.The contents of these two fields are identical

DSCP and IPP

DSCP bits provide 64 different classifications that QoS can use.This is a vast improvement over the eight classifications allotted for the 3 bits in the previous IP Precedence (IPP) field For backward compatibility, the

DSCP bits include the Class Selector (CS) values that are designated to match the IPP bits

For Layer 2 trunk links, the third byte of the 4-byte 802.1Q header is reserved for Class of Service (CoS), and QoS tools can use it to mark frames. However, this field exists only as long as the frame is traversing trunk links To continue the same level of service as traffic is routed on Layer 3, the ToS field must be marked.

EF and AF
Expedited Forwarding (EF) is a single DSCP decimal value of 46 that is suggested for use with packets that require low latency, low jitter, and low loss. QoS implementations typically use EF to mark voice packets

Congestion Management

Congestion management refers to the QoS tools used to manage queues as packets wait to exit an interface. Most networking devices can have a queuing system that can classify packets into multiple queues.A scheduler then decides which message to take next when the interface becomes available.
A popular tool is Class-Based Weighted Fair Queueing (CBWFQ), which assigns classes of traffic to queues and guarantees a minimum bandwidth for a queue.The scheduler then uses a round-robin algorithm to cycle through the queues in order,

However, CBWFQ alone does not satisfy the needs of the most time-sensitive traffic type during periods of heavy bandwidth congestion. Each voice call needs between 30 and 320 kbps, maximum delay of 150 ms, maximum jitter of 30 ms, and less than 1% packet loss.The solution is to add Low Latency Queueing (LLQ) to CBWFQ.The scheduler always takes the next voice packet from the LLQ

Policing, Shaping, andTCP Discards

Two tools that can help manage and avoid congestion on heavily utilized links are policing
and shaping. Although these tools are not commonly used throughout the enterprise, they are particularly helpful at the WAN edge. Both tools attempt to keep the bit rate at or below a specified speed. Policers drop packets, and shapers delay packets by placing them in a queue.

Policing makes sense at the WAN edge. For example, consider a Metro Ethernet WAN link that is contracted to allow no more than 200 Mbps

The service provider (SP) uses policing to match the Committed Information Rate (CIR). If the customer exceeds the 200-Mbps CIR, the SP can drop the excess packets or remark the excess packets but still allow them through. Later, the excess packets can be discarded if the SP's network experiences congestion. Policing features include the following:
■ Measure traffic over time and compare to a configured policing rate
■ Allow for bursting traffic during slow times

■ Discard excess messages or remark for discard later if congestion occurs downstream

On the customer side of the link he network administrator can use a shaper to slow traffic to match the 200-Mbps CIR.The shaper slows traffic by queuing packets and then scheduling packets based on the shaping rate

Shaping cannot slow the physical speed of an interface. Instead, it sends and waits.

This send-wait tactic can adversely impact time-sensitive voice and video traffic.Therefore, it is recommended that you set the time interval to 10 ms.Then the shaper will send 1000 Mbps for 2 ms and wait for 8 ms.This ensures that a voice packet will not have to wait more than 10 ms before being sent, which is well below the 150 ms maximum delay requirement.

The key features of shapers follow:
■ Measure traffic over time and compare it to a configured shaping rate
■ Allow for bursting traffic during slow times
■ Slow packets by queuing them and, over time, releasing them from the queue at the shaping rate

QoS and TCP

Without congestion-avoidance tools, tail drop can occur

As the lower queues fill up, the packets received last are dropped. TCP's connection-oriented services help QoS tools minimize tail drop. Recall that TCP uses a windowing process between sender and receiver to dynamically change the amount of data that is sent before an acknowledgment must be received. QoS tools can exploit this windowing feature by discarding some TCP segments before the queues fill.This forces the TCP connections to slow, reduces congestion, and avoids tail drop.

QoS tools monitor the depth of the queues over time. Configured thresholds specify what percentage of TCP packets should be dropped as the queue fills

###############
Switching
###############

Switches replaced hubs as local-area network (LAN) intermediary devices because a switch can segment collision domains and provide enhanced security.

When choosing a switch, these are the main factors to consider:

■ Cost: The cost is determined by the number and type of ports, network management capabilities, embedded security technologies, and optional advanced switching technologies.
■ Interface characteristics: The number of ports must be sufficient both for now and for future expansion. Other characteristics include uplink speeds, a mixture of UTP and fiber, and modularity.
■ Hierarchical network layer: Switches at the access layer have different requirements than switches at the distribution or core layers.

Access Layer Switches
Access layer switches facilitate the connection of end devices to the network. Features of access layer switches include the following:
■ Port security
■ VLANs
■ Fast Ethernet/Gigabit Ethernet
■ Power over Ethernet (PoE)
■ Link aggregation
■ Quality of service (QoS)

Distribution Layer Switches
Distribution layer switches receive the data from the access layer switches and forward it to the core layer switches. Features of distribution layer switches include the following:
■ Layer 3 support
■ High forwarding rate
■ Gigabit Ethernet/10 Gigabit Ethernet
■ Redundant components
■ Security policies/access control lists
■ Link aggregation
■ QoS

Core Layer Switches
Core layer switches make up the backbone and are responsible for handling the majority of data on a switched LAN. Features of core layer switches include the following:
■ Layer 3 support
■ Very high forwarding rate
■ Gigabit Ethernet/10 Gigabit Ethernet
■ Redundant components
■ Link aggregation
■ QoS

Switch Logic

#Ethernet switches selectively forward individual frames from a receiving port to the port where the destination node is connected. During this instant, the switch creates a full-bandwidth, logical, point-to-point connection between the two nodes.
Switches create this logical connection based on the source and destination Media Access Control (MAC) addresses in the Ethernet header.

Specifically, the primary job of a LAN switch is to receive Ethernet frames and then make a decision to either forward the frame or ignore the frame.To accomplish this, the switch performs three actions:

Decides when to forward a frame or when to filter (not forward) a frame, based on the destination MAC address

Learns MAC addresses by examining the source MAC address of each frame the switch receives

Creates a (Layer 2) loop-free environment with other switches by using Spanning Tree Protocol (STP)

To make stored in switch decides how to forward and/or filter the frame.

In addition to forwarding and filtering frames, the switch refreshes the timestamp for the source MAC address of the frame

Entries that are not refreshed eventually are removed (after the default 300 seconds in Cisco IOS).

forwards the frame out all active ports (in a process known as flooding) except for the port on which the frame was received

Collision and broadcast Domain

A collision domain is the set of LAN interfaces whose frames could collide with each other.All shared media environments, such as those created by using hubs, are collision domains.When one host is attached to a switch port, the switch creates a dedicated connection, thereby eliminating the potential for a collision. Switches reduce collisions and improve bandwidth use on network segments because they provide full-duplex, dedicated bandwidth to each network segment.
OuLt of the box, however, a switch cannot provide relief from broadcast traffic. A collection of con- nected switches forms one large broadcast domain. If a frame with the destination address FFFF. FFFF.FFFF crosses a switch port, that switch must flood the frame out all other active ports. Each attached device must then process the broadcast frame at least up to the network layer. Routers andVLANs are used to segment broadcast domains

Switch FOrwarding method

Switches use one of the following forwarding methods to switch data between network ports:
■ Store-and-forward switching: The switch stores received frames in its buffers, analyzes each frame for information about the destination, and evaluates the data integrity using the cyclic redundancy check (CRC) in the frame trailer.The entire frame is stored, and the CRC is calculated before any of the frame is forwarded. If the CRC passes, the frame is forwarded to the destination.

■ Cut-through switching: The switch buffers just enough of the frame to read the destination MAC address so that it can determine which port to forward the data to.When the switch determines a match between the destination MAC address and an entry in the MAC address table, the frame is forwarded out the appropriate port(s).This happens as the rest of the initial frame is still being received.The switch does not perform any error checking on the frame.

■ Fragment-free mode: The switch waits for the collision window (64 bytes) to pass before forwarding the frame.This means that each frame is checked into the data field to make sure that no fragmentation has occurred. Fragment-free mode provides better error checking than cut-through, with practically no increase in latency.

Symetric and Asymetric

Symmetric switching provides switched connections between ports with the same bandwidth,
such as all 100-Mbps ports or all 1000-Mbps ports.An asymmetric LAN switch provides switched connections between ports of unlike bandwidth, such as a combination of 10-Mbps, 100-Mbps, and 1000-Mbps ports.

Memory Bufering

Switches store frames for a brief time in a memory buffer.Two methods of memory buffering exist:
■ Port-based memory: Frames are stored in queues that are linked to specific incoming ports.
■ Shared memory: Frames are deposited into a common memory buffer that all ports on the switch share.

Layer 2 Layer 3 switch

A Layer 2 LAN switch performs switching and filtering based only on MAC addresses.A Layer 2 switch is completely transparent to network protocols and user applications.A Layer 3 switch func- tions similarly to a Layer 2 switch. But instead of using only the Layer 2 MAC address information for forwarding decisions, a Layer 3 switch can also use IP address information. Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN. Because Layer 3 switches have specialized switching hardware, they can typically route data as quickly as they can switch data.

Ethernet Overview

802.3 is the IEEE standard for Ethernet, and the two terms are commonly used interchangeably. The terms Ethernet and 802.3 both refer to a family of standards that together define the physical and data link layers of the definitive LAN technology

Ethernet separates the functions of the data link layer into two distinct sublayers:
■ Logical Link Control (LLC) sublayer: Defined in the 802.2 standard
■ Media Access Control (MAC) sublayer: Defined in the 802.3 standard

The LLC sublayer handles communication between the network layer and the MAC sublayer. In general, LLC provides a way to identify the protocol that is passed from the data link layer to the network layer. In this way, the fields of the MAC sublayer are not populated with protocol type information, as was the case in earlier Ethernet implementations.

The MAC sublayer has two primary responsibilities:
■ Data encapsulation: Included here is frame assembly before transmission, frame parsing upon reception of a frame, data link layer MAC addressing, and error detection.
■ Media Access Control: Because Ethernet is a shared medium and all devices can transmit at any time, media access is controlled by a method called Carrier Sense Multiple Access/Collision Detect (CSMA/CD) when operating in half-duplex mode.

At the physical layer, Ethernet specifies and implements encoding and decoding schemes that enable frame bits to be carried as signals across both unshielded twisted pair (UTP) copper cables and optical fiber cables. In early implementations, Ethernet used coaxial cabling.

Legacy Ethernet Technologies

Ethernet is best understood by first considering the two early Ethernet specifications, 10BASE-5 and 10BASE-2.With these two specifications, the network engineer installs a series of coaxial cables connecting each device on the Ethernet network
The series of cables creates an electrical circuit, called a bus, that is shared among all devices on the Ethernet.When a computer wants to send some bits to another computer on the bus, it sends an electrical signal, and the electricity propagates to all devices on the Ethernet.

#CSMA/CD

Because Ethernet is a shared medium in which every device has the right to send at any time, it also defines a specification to ensure that only one device sends traffic at a time.The CSMA/CD algorithm defines how the Ethernet logical bus is accessed.

CSMA/CD logic helps prevent collisions and also defines how to act when a collision does occur. The CSMA/CD algorithm works like this:

A device with a frame to send listens until the Ethernet is not busy. When the Ethernet is not busy, the sender(s) begin(s) sending the frame. The sender(s) listen(s) to make sure that no collision occurs.

If a collision occurs, the devices that were sending a frame each send a jamming signal to ensure that all stations recognize the collision.

When the jamming is complete, each sender randomizes a timer and waits until the timer expires before trying to resend the collided frame.

When each random timer expires, the process starts again from the beginning.

When CSMA/CD is in effect, a device’s network interface card (NIC) operates in half-duplex mode, either sending or receiving frames. CSMA/CD is disabled when a NIC autodetects that it can operate in—or is manually configured to operate in—full-duplex mode. In full-duplex mode, a NIC can send and receive simultaneously.

UDP cabling

The three most common Ethernet standards used today—10BASE-T (Ethernet), 100BASE-TX (Fast Ethernet, or FE), and 1000BASE-T (Gigabit Ethernet, or GE)—use UTP cabling. Some key differences exist, particularly with the number of wire pairs needed in each case and the type (category) of cabling.
The UTP cabling in popular Ethernet standards includes either two or four pairs of wires.The cable ends typically use an RJ-45 connector.The RJ-45 connector has eight specific physical locations into which the eight wires in the cable can be inserted; these are called pin positions or, simply, pins.
The Telecommunications Industry Association (TIA) and the Electronics Industry Alliance (EIA) define standards for UTP cabling, with color coding for wires and standard pinouts on the cables.

For the exam, you should be well prepared to choose which type of cable (straight-through or crossover) is needed in each part of the network. In short, devices on opposite ends of a cable that use the same pair of pins to transmit need a crossover cable. Devices that use an opposite pair of pins to transmit need a straight-through cable

Pins trasnmision

1000BASE-T requires four wire pairs because Gigabit Ethernet transmits and receives on each of the four wire pairs simultaneously.

However, Gigabit Ethernet does have a concept of straight-through and crossover cables, with a minor difference in the crossover cables.The pinouts for a straight-through cable are the same—pin 1 to pin 1,pin 2 to pin 2,and so on.
A crossover cable has the 568A standard on one end and the 568B standard on the other end.This crosses the pairs at pins 1,2 and 3,6

Benefits of using switches

A collision domain is a set of devices whose frames may collide.All devices on a 10BASE-2, 10BASE-5, or other network using a hub risk

collisions between the frames that they send.Thus, devices on one of these types of Ethernet networks are in the same collision domain and use CSMA/CD to detect and resolve collisions.
LAN switches significantly reduce, or even eliminate, the number of collisions on a LAN. Unlike a hub, a switch does not create a single shared bus. Instead, a switch does the following:
■ It interprets the bits in the received frame so that it can typically send the frame out the one required port instead of out all other ports.
■ If a switch needs to forward multiple frames out the same port, the switch buffers the frames in memory, sending one at a time and thereby avoiding collisions.
In addition, switches with only one device cabled to each port of the switch allow the use of full-duplex operation. Full-duplex operation means that the NIC can send and receive concurrently, effectively doubling the bandwidth of a 100-Mbps link to 200 Mbps—100 Mbps for sending and 100 Mbps for receiving.
These seemingly simple switch features provide significant performance improvements compared with using hubs. In particular, consider these points:
■ If only one device is cabled to each port of a switch, no collisions can occur.
■ Devices connected to one switch port do not share their bandwidth with devices connected to another switch port. Each has its own separate bandwidth, meaning that a switch with 100-Mbps ports has 100 Mbps of bandwidth per port.

Ethernet adressing
The IEEE defines the format and assignment of LAN addresses.To ensure a unique MAC address, the first half of the address identifies the manufacturer of the card.This code is called the organiza- tionally unique identifier (OUI). Each manufacturer assigns a MAC address with its own OUI as the first half of the address.The second half of the address is assigned by the manufacturer and is never used on another card or network interface with the same OU

Ethernet also has group addresses, which identify more than one NIC or network interface.The IEEE defines two general categories of group addresses for Ethernet:
■ Broadcast addresses: A broadcast address implies that all devices on the LAN should process the frame and has the value FFFF.FFFF.FFFF.
■ Multicast addresses: A multicast address allows a subset of devices on a LAN to communi- cate.When IP multicasts over an Ethernet network, the multicast MAC addresses that IP uses follow this format: 0100.5exx.xxxx.The xx.xxxx portion is divided between IPv4 multicast (00:0000–7F.FFFF) and MPLS multicast (80:0000–8F:FFFF). Multiprotocol Label Switching (MPLS) is a CCNP topic

Ethernet Framing

The physical layer helps you get a string of bits from one device to another.The framing of the
bits allows the receiving device to interpret the bits.The term framing refers to the definition of the fields assumed to be in the data that is

received. Framing defines the meaning of the bits transmitted and received over a network.

The role of Phisical Layer

We have already discussed the most popular cabling used in LANs: UTP.To fully understand the operation of the network, you should know some additional basic concepts of the physical layer.
The OSI physical 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 delivery of frames across the local media requires the following physical layer elements:
■ The physical media and associated connectors
■ A representation of bits on the media
■ Encoding of data and control information
■ Transmitter and receiver circuitry on the network devices Data is represented on three basic forms of network media:
■ Copper cable
■ Fiber
■ Wireless (IEEE 802.11)

Bits are represented on the medium by changing one or more of the following characteristics of a signal:
■ Amplitude
■ Frequency
■ Phase
The nature of the actual signals representing the bits on the media depends on the signaling method in use. Some methods use one attribute of a signal to represent a single 0 and use another attribute of a signal to represent a single 1

DTP Dynamic Trunking Protocol

Dynamic Trunking Protocol (DTP) is a Cisco-proprietary protocol that negotiates both the status
of trunk ports and the trunk encapsulation of trunk ports. DTP manages trunk negotiation only if the port on the other switch is configured in a trunk mode that supports DTP.A switch port on a Cisco Catalyst switch supports a number of trunking modes.The trunking mode defines how the port negotiates using DTP to set up a trunk link with its peer port.The following is a brief descrip- tion of each trunking mode:
■ If the switch is configured with the switchport mode trunk command, the switch port periodically sends DTP messages to the remote port, advertising that it is in an unconditional trunking state.
■ If the switch is configured with the switchport mode trunk dynamic auto command,
the local switch port advertises to the remote switch port that it is able to trunk but does not request to go to the trunking state. After a DTP negotiation, the local port ends up in the trunking state only if the remote port trunk mode has been configured so that the status is on or desirable. If both ports on the switches are set to auto, they do not

negotiate to be in a trunking state.They negotiate to be in the access mode state.

■ If the switch is configured with the switchport mode dynamic desirable command, the local switch port advertises to the remote switch port that it is able to trunk and asks the remote switch port to go to the trunking state. If the local port detects that the remote port has been configured as on, desirable, or auto mode, the local port ends up in the trunking state. If the remote switch port is in the nonegotiate mode, the local switch port remains as a nontrunking port.

■ If the switch is configured with the switchport nonegotiate command, the local port is con- sidered to be in an unconditional trunking state. Use this feature when you need to configure a trunk with a switch from another switch vendor.

STP Algorithm

STP is an IEEE Committee standard defined as 802.1D. STP places certain ports in the blocking state so that they do not listen to, forward, or flood data frames. STP creates a tree that ensures that only one path exists for each network segment at any one time. If any segment experiences a disruption in connectivity, STP rebuilds a new tree by activating the previously inactive but redundant path.

The algorithm STP uses chooses the interfaces that should be placed into a forwarding state. For any interfaces not chosen to be in a forwarding state, STP places the interfaces in blocking state.

Switches exchange STP configuration messages every 2 seconds, by default, using a multicast
frame called the bridge protocol data unit (BPDU). Blocked ports listen for these BPDUs to detect whether the other side of the link is down, thus requiring an STP recalculation. One piece of information included in the BPDU is the bridge ID (BID)

STP Convergence

STP convergence is the process by which switches collectively realize that something has changed
in the LAN topology.The switches determine whether they need to change which ports block and which ports forward.The following steps summarize the STP algorithm used to achieve convergence:

Root Bridge and Root Port Election

Elect a root bridge (that is, the switch with the lowest BID). Only one root bridge can exist per network.All ports on the root bridge are forwarding ports.

Elect a root port for each nonroot switch, based on the lowest root path cost. Each nonroot switch has one root port.The root port is the port through which the nonroot bridge has its best path to the root bridge.

Elect a designated port for each segment, based on the lowest root path cost. Each link has one designated port.

The root ports and designated ports transition to the forwarding state, and the other ports stay in the blocking state.

STP Varieties

Several varieties of STP emerged after the original IEEE 802.1D:
■ STP: The original specification of STP, defined in 802.1D, provides a loop-free topology in a network with redundant links. STP is sometimes referred to as Common Spanning Tree (CST) because it assumes one spanning tree instance for the entire bridged network, regardless of the number ofVLANs.
■ PVST+: Per-VLAN Spanning Tree Plus (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning tree instance for each VLAN configured in the network.
■ RSTP: Rapid STP (RSTP), or IEEE 802.1w, is an evolution of STP that provides faster convergence than STP. However, RSTP still provides for only a single instance of STP.
■ Rapid PVST+: Rapid PVST+ is a Cisco enhancement of RSTP that uses PVST+. Rapid PVST+ provides a separate instance of 802.1w per VLAN.
■ MSTP and MST: Multiple Spanning Tree Protocol (MSTP) is an IEEE standard inspired by the earlier Cisco-proprietary Multiple Instance STP (MISTP) implementation. MSTP maps multipleVLANs into the same spanning tree instance.The Cisco implementation of MSTP
is Multiple Spanning Tree (MST), which provides up to 16 instances of RSTP and combines manyVLANs with the same physical and logical topology into a common RSTP instance.

PVST Operation

PVST Plus (PVST+) is the default setting on all Cisco Catalyst switches. In a PVST+ environment, you can tune the spanning-tree parameters so that half the VLANs forward on
each uplink trunk.You do this by configuring one switch to be elected the root bridge for half
of theVLANs in the network and a second switch to be elected the root bridge for the other half of the VLANs.

Port State

The spanning tree is determined immediately after a switch is finished booting. If a switch port transitions directly from the blocking state to the forwarding state without information about the full topology during the transition, the port can temporarily create a data loop. For this reason, STP introduces the five port states

Extended System ID

PVST+ requires a separate instance of spanning tree for eachVLAN.The BID field in the BPDU must carry VLAN ID (VID) information

BID includes

■ Bridge Priority: A 4-bit field is still used to carry bridge priority. However, the priority is conveyed in discrete values in increments of

4096 instead of discrete values in increments of 1 because only the first 4 most-significant bits are available from the 16-bit field.
■ Extended System ID: A 12-bit field carrying the VID for PVST+.
■ MAC Address: A 6-byte field with the MAC address of a single switch.

Rapid PVST+ Operation

In Rapid PVST+, a single instance of RSTP runs for eachVLAN.This is why Rapid PVST+ has a very high demand for switch resources (CPU cycles and RAM).

With RSTP, the IEEE improved the convergence performance of STP from 50 seconds to less
than 10 seconds with its definition of Rapid STP (RSTP) in the standard 802.1w. RSTP is identical to STP in the following ways:
■ It elects the root switch by using the same parameters and tiebreakers.
■ It elects the root port on nonroot switches by using the same rules.
■ It elects designated ports on each LAN segment by using the same rules.
■ It places each port in either forwarding or discarding state, although RSTP calls the blocking state the discarding state.

RSTP Interface Behavior

The main changes with RSTP can be seen when changes occur in the network. RSTP acts differently on some interfaces based on what is connected to the interface:
■ Edge-type behavior and PortFast: RSTP improves convergence for edge-type connections by immediately placing the port in forwarding state when the link is physically active.
■ Link-type shared: RSTP does not do anything differently from STP on link-type shared links. However, because most links between switches today are full duplex, point-to-point, and not shared, this does not matter.
■ Link-type point-to-point: RSTP improves convergence over full-duplex links between switches. RSTP recognizes the loss of the path to the root bridge through the root port in 6 seconds (based on three times the hello timer value of 2 seconds). RSTP thus recognizes a lost path to the root much more quickly.

Edge Port

In addition to the port roles just described, RSTP uses an edge port concept that corresponds to the PVST+ PortFast feature. An edge port connects directly to an end device. Therefore, the switch assumes that no other switch is connected to it. RSTP edge ports should immediately transition to the forwarding state, thereby skipping the time-consuming original 802.1D listening and learning port states.The only caveat is that the port must be a point-to-point link. If it is a shared link, the port is not an edge port, and PortFast should not be configured.Why? Another switch could be added to a shared link—on purpose or inadvertently

Configuring PortFast and BPDU Guard

To speed convergence for access ports when they become active, you can use Cisco's proprietary PortFast technology. After PortFast is configured and a port is activated, the port immediately transitions from the blocking state to the forwarding state.
In a valid PortFast configuration, BPDUs should never be received because receipt of a BPDU indicates that another bridge or switch is connected to the port, potentially causing a spanning tree loop.When it is enabled, BPDU Guard puts the port in an errdisabled (error-disabled) state upon receipt of a BPDU.This effectively shuts down the port.The BPDU Guard feature provides a secure response to invalid configurations because you must manually put the interface back into service.

CDP and LLDP

Cisco Discovery Protocol (CDP) is a Cisco-proprietary Layer 2 protocol used to gather information about Cisco devices on the same data link. Cisco devices also support Link Layer Discovery Protocol (LLDP), which is a standards-based neighbor discovery protocol similar to CDP.

CDP runs on all Cisco-manufactured equipment. It gathers the protocol addresses of neighboring devices and discovers the platforms of those devices. CDP runs over the data link layer only.
This means that two systems that support different Layer 3 protocols can learn about each other.

CDP can assist in network discovery and troubleshooting. CDP advertises the following helpful information:
■ Device ID: The hostname of the neighboring device
■ Addresses: The IPv4 and IPv6 addresses used by the device

■ Port ID: The name of the local port or the remote port
■ Capabilities: Whether the device is a router or a switch or has other capabilities
■ Version: The version of CDP running on the device
■ Platform: The hardware platform of the device, such as a Cisco 1941 router or 2960 switch

You can also disable CDP on a per-interface basis.This configuration option is a security best prac- tice for interfaces that are connected to untrusted networks.To disable CDP on an interface, use the no cdp enable command

To adjust the time for CDP advertisements, use the cdp timer global configuration command:

The range is 5 to 254 seconds, and the default is 60 seconds. If you modify the CDP timer, you should also modify the holdtime with the cdp holdtime global configuration command:

The show cdp neighbors detail command lists all the information CDP gathers about directly connected neighbors.

LLDP Overview

In addition to supporting CDP, Cisco devices also support LLDP, which is a vendor-neutral open standard (IEEE 802.1AB). LLDP works with routers, switches, and wireless LAN access points. As with CDP, LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. Also as with CDP, LLDP enables two systems running different network layer protocols to learn about each other.

LLDP Configuration
To enable LLDP globally, enter the lldp run command

When enabled globally, LLDP is enabled on all interfaces.To disable LLDP on an interface, use the no lldp transmit and no lldp receive commands

To adjust the time for LLDP advertisements, use the lldp timer global configuration command

The range is 5 to 65534 seconds, and the default is 30 seconds. If you modify the CDP timer, you should also modify the holdtime with the cdp holdtime global configuration command:

The range is from 0 to 65535, and the default is 120 seconds.You can also modify the delay time for LLDP to initialize on any interface with the lldp reinit global configuration command

###########
Routers
###########

Routers
Routers are the primary devices used to interconnect networks—LANs,WANs, and WLANs.When choosing a router, the main factors to consider are as follows:
■ Expandability: Provides flexibility to add new modules as needs change.
■ Media: Determines the type of interfaces the router needs to support for the various network
connections.
■ Operating system features: Determines the version of IOS loaded on the router. Different IOS versions support different feature sets. Features to consider include security, QoS,VoIP, and routing complexity, among others.

■ Console ports: Two console ports for the initial configuration, using a regular RJ-45 port and a USB Type-B (mini-B USB) connector.
■ AUX port: An RJ-45 port for remote management access.
■ LAN interfaces: Two Gigabit Ethernet interfaces for LAN access (G0/0/0 and G0/0/1). If the RJ-45 G0/0/0 port is used, then the small form-factor pluggable (SFP) port cannot be used.WAN services would then be provided through an expansion card in the network interface module (NIM) slots.
■ Ethernet WAN: The other G0/0/0 physical port, an SFP port that would support various Ethernet WAN connections, typically fiber. If it is used, the Gi0/0 RJ-45 port is disabled.
■ NIM slots: Two slots that support different types of interface modules, including serial (shown in Figure 31-10), digital subscriber line (DSL), switch port, and wireless.

##################
FHRP
##################

A redundancy protocol provides the mechanism for determining which router should take the active role in forwarding traffic. It also determines when a standby router must take over the forwarding role.The transition from one forwarding rout- er to another is transparent to the end devices.This capability of a network to dynamically recover from the failure of a device acting as a default gateway is known as first-hop redundancy.

The following list defines the three options available for FHRPs:
■ Hot Standby Router Protocol (HSRP): A Cisco-proprietary FHRP designed to allow for transparent failover of a first-hop IPv4 device.The function of the HSRP standby router is to monitor the operational status of the HSRP group and to quickly assume packet-forwarding responsibility if the active router fails. HSRP for IPv6 provides support for IPv6 networks.
■ Virtual Router Redundancy Protocol (VRRP): An IETF standard that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on an IPv4 LAN. Its operation is similar to that of HSRP. VRRPv3 supports IPv4 and IPv6.
■ Gateway Load Balancing Protocol (GLBP): A Cisco-proprietary FHRP that protects data traffic from a failed router or circuit, as in HSRP and VRRP, while also allowing load balanc- ing (also called load sharing) between a group of redundant routers. GLBP for IPv6 provides support for IPv6 networks.

HSRP Operation

HSRP uses an active/standby model in which one router actively assumes the role of default gate- way for devices on the subnet. One or more routers on the same subnet are then in standby mode. The HSRP active router implements a virtual IP address and matching virtual MAC address.This virtual IP address is part of the HSRP configuration and

belongs to the same subnet as the physical interface IP address, but it is a different IP address.The router then automatically creates the virtual MAC address. All the cooperating HSRP routers know these virtual addresses, but only the HSRP active router uses these addresses at any one point in time.

HSRP Priority and Preemption

By default, the router with the numerically highest IPv4 address is elected as the active HSRP router.To configure a router to be the active router, regardless of IPv4 addressing, use the standby priority interface configuration command.The default priority is 100.The router with the highest priority will be the active HSRP router, assuming that no election has already occurred.
To force a new HSRP election, preemption must be enabled with the standby preempt interface configuration command.

DHCP Options

A Cisco router can be configured to handle DHCP requests in two ways: as a DHCP server or as
a DHCP relay agent. A Cisco router can also be configured as a DHCP client, requesting an IPv4 address from a DHCP server for one or more of its interfaces.All these options can be configured at the same time on the same device.

Verifying DHCP Operation

show ip dhcp binding

Configuring a router To relay DHCP

In a complex network, the DHCPv4 servers are usually contained in a server farm.Therefore, clients typically are not on the same subnet as the DHCPv4 server, as in the previous example. To ensure that broadcasted DHCPDISCOVER messages are sent to the remote DHCPv4 server, use the ip helper-address command.

##################
Firewalls
#################

Firewalls
A firewall is a networking device, either hardware or software based, that controls access to the organization’s network.This controlled access is designed to protect data and resources from outside threats.

A stateful firewall allows traffic to originate from an inside, trusted network and go out to an untrusted network, such as the Internet.The firewall allows return traffic that comes back from the untrusted network to the trusted network. However, the firewall blocks traffic that originates from an untrusted network.

############
IDS IPS
############

IDS and IPS
Both intrusion detection systems (IDS) and intrusion prevention systems (IPS) can recognize network attacks; they differ primarily in their network placement. An IDS device receives a copy of traffic to be analyzed. An IPS device is placed inline with the traffic

An IDS is a passive detection system. It can detect the presence of an attack, log the information, and send an alert.
An IPS has the same functionality as an IDS, but in addition, an IPS is an active device that continually scans the network, looking for inappropriate activity. It can shut down any potential threats.The IPS looks for any known signatures of common attacks and automatically tries to prevent those attacks.

############
NGFW
############

Although the term next-generation in relation to firewalls has been around at least since the earlier 2010s, it can be misleading. Next-generation firewalls (NGFWs) or next-generation IPSs (NGIPSs) are actually what Cisco currently sells as its Cisco Adaptative Security Appliance (ASA) and Firepower product lines

An NGFW typically has the following features:
■ Traditional firewall: An NGFW performs traditional firewall functions, such as stateful firewall filtering, NAT/PAT, and VPN termination.
■ Application Visibility and Control (AVC): AVC makes it possible to look deeply into the application layer data to identify the application to defend against attacks that use random port numbers.
■ Advanced Malware Protection (AMP): AMP can block file transfers that would install malware and save copies of files for later analysis.
■ Uniform resource locator (URL) filtering: URL filtering examines the URLs in each web request, categorizes the URLs, and either filters or rate limits the traffic based on rules. The Cisco Talos security group monitors and creates reputation scores for each domain known in the Internet, and URL filtering can use those scores in its decisions to categorize, filter, or rate limit.
■ NGIPS: Cisco’s NGFW products can also run their NGIPS feature along with the firewall

##############
SNMP
##############

SNMP Operation
SNMP is an application layer protocol that provides a message format for communication between managers and agents.

SNMP Components
The SNMP system consists of three elements:
■ SNMP manager
■ SNMP agents (managed node)
■ Management Information Base (MIB)

SNMP Messages
The SNMP manager is part of a network management system (NMS) and runs SNMP management software. SNMP agents are managed devices.The MIB stores SNMP variables.
SNMP uses three basic messages between SNMP managers and agents: get, set, and trap messages. The SNMP manager uses get messages to poll a device for information and set messages to change a device parameter.An SNMP agent can use SNMP traps to independently notify the NMS when a problem occurs.

For example, SNMP can monitor the CPU utilization on a Cisco router.The NMS can sample this value periodically and warn the network administrator when the value deviates from the baseline. An SNMP agent can also be configured to send a trap message when CPU utilization is driving away from normal values for the network

SNMP Versions
Several versions of SNMP exist:
■ SNMPv1: The original SNMP, defined in RFC 1157.
■ SNMPv2c: Defined in RFCs 1901 to 1908. Utilizes a community string-based administrative framework.
■ SNMPv3: Interoperable standards-based protocol originally defined in RFCs 2273 to 2275. Provides secure access to devices by authenticating and encrypting packets over the network.
SNMPv1 and SNMPv2c use community strings that control access to the MIB. Community strings are plaintext passwords.Two types of community strings exist:
■ Read-only (ro): Provides access to the MIB variables but does not allow these variables to be changed (only read)
■ Read-write (rw): Provides read and write access to all objects in the MIB

The Management Information Base

The Management Information Base

The MIB organizes variables hierarchically. MIB variables enable the management software to monitor and control the network device. Formally, the MIB defines each variable as an object ID (OID). OIDs uniquely identify managed objects in the MIB hierarchy.The MIB organizes the OIDs based on RFC standards into a hierarchy of OIDs, usually shown as a tree.

Syslog

It is a popular protocol that many networking devices use, including routers, switches, application servers, firewalls, and other network appliances.These devices can send their messages across the network to be stored on syslog servers for later access by network administrators.

Syslog Operation
Syslog uses UDP port 514 to send event notification messages across IP networks to event message collectors,

The syslog logging service provides three primary capabilities:
■ Gathering logging information for monitoring and troubleshooting
■ Selecting the type of logging information that is captured
■ Specifying the destinations of captured syslog messages
On Cisco network devices, the syslog protocol starts by sending system messages and debug output to a local logging process internal to the device. It is possible to remotely monitor system messages by viewing the logs on a syslog server or by accessing the device through Telnet, Secure Shell (SSH), or the console port.
Cisco devices produce syslog messages as a result of network events. Every syslog message contains a severity level and a facility.

In addition to specifying the severity, syslog messages contain information on the facility. Syslog facilities are service identifiers that identify and categorize system state data for error and event message reporting.The logging facility options that are available are specific to the networking device. Common syslog message facilities reported on Cisco IOS routers include the following:
■ IP
■ OSPF protocol
■ SYS operating system
■ IP Security (IPsec)
■ Interface IP (IF)

Configuring and Verifying Syslog
By default, Cisco routers and switches send log messages for all severity levels to the console. On some Cisco IOS versions, the device also buffers log messages by default.To enable these two settings, use the logging console and logging buffered global configuration commands, respectively.

NTP

As you know, routers and switches issue log messages in response to different events. For example, when an interface fails, the device creates log messages.With default settings, Cisco IOS sends these messages to the console port. But Cisco IOS can be configured also to send messages to a syslog server, where they can be stored for administration review and troubleshooting

A log message typically lists the date and time as part of the message so that a network engineer who looks back at the message knows exactly when that message occurred.
Network Time Protocol (NTP) provides a way to synchronize the time-of-day clock so that timestamps are consistent across devices, making troubleshooting easier.
To configure a router or switch to synchronize its time with an existing NTP server, use the ntp server command

ntp associations command lists a single line of output for every other NTP device with which the router has associated.
A router or a switch can actually be the NTP server with just one command (ntp master) as well. In addition, NTP can use authentication so that a router or switch does not get fooled into changing its timestamp.

Commands for Managing Configuration Files

The Cisco IOS Software copy command enables you to move configuration files from one component or device to another, such as RAM, NVRAM, or a TFTP server.

Managing Cisco IOS Images

As a network grows, storing Cisco IOS Software images and configuration files on the central TFTP server gives you control over the number and revision level of Cisco IOS images and configuration files that must be maintained. Use the show version command to verify the Cisco IOS image currently running on the device

################
IPV6
################

Overview and Benefits of IPv6

Scaling networks today requires a limitless supply of IP addresses and improved mobility that private addressing and NAT alone cannot meet. IPv6 satisfies the increasingly complex requirements of hierarchical

addressing that IPv4 does not provide.The main benefits and features of IPv6 include the following:

■ Extended address space: A 128-bit address space represents about 340 trillion trillion trillion addresses.

■ Stateless address autoconfiguration: IPv6 provides host devices with a method for generat- ing their own routable IPv6 addresses. IPv6 also supports stateful configuration using DHCPv6.

■ Eliminates the need for NAT/PAT: NAT/PAT was conceived as part of the solution to IPv4 address depletion.With IPv6, address depletion is no longer an issue. NAT64, however, does play an important role in providing backward compatibility with IPv4.

■ Simpler header: A simpler header offers several advantages over IPv4:

■ Better routing efficiency for performance and forwarding-rate scalability

■ No broadcasts and, thus, no potential threat of broadcast storms

■ No requirement for processing checksums

■ Simpler and more efficient extension header mechanisms

Mobility and security: Mobility and security help ensure compliance with mobile IP and IPsec standards:

■ IPv4 does not automatically enable mobile devices to move without breaks in established network connections.

■ In IPv6, mobility is built in, which means that any IPv6 node can use mobility when necessary.

■ IPsec is enabled on every IPv6 node and is available for use, making the IPv6 Internet more secure.

Transition strategies:You can incorporate existing IPv4 capabilities with the added features of IPv6 in several ways:

■ You can implement a dual-stack method, with both IPv4 and IPv6 configured on the interface of a network device.

■ You can use tunneling, which will become more prominent as the adoption of IPv6 grows.

IPv6 Address Types

IPv4 has three address types: unicast, multicast, and broadcast. IPv6 does not use broadcast addresses. Instead, IPv6 uses unicast, multicast, and anycast addresses

Unicast

A unicast address uniquely identifies an interface on an IPv6 device.A packet sent to a unicast address is received by the interface that is assigned to that address. Much as with IPv4, source IPv6 addresses must be unicast addresses.

Global Unicast Address

IPv6 has an address format that enables aggregation upward, eventually to the ISP. An IPv6 global unicast address is globally unique. Like a public IPv4 address, it can be routed in the Internet without modification. An IPv6 global unicast address consists of a 48-bit global routing prefix, a 16-bit subnet ID, and a 64-bit interface ID.

In IPv6, an interface can be configured with multiple global unicast addresses, which can be on the same or different subnets. In addition, an interface does not have to be configured with a global unicast address, but it must at least have a link-local address.

Link local Address

Link-local addresses are confined to a single link.They need to be unique only to that link because packets with a link-local source or destination address are not routable off the link.

Loopback Address

The loopback address for IPv6 is an all-0s address except for the last bit, which is set to 1. As in IPv4, an end device uses the IPv6 loopback address to send an IPv6 packet to itself to test the TCP/IP stack.The loopback address cannot be assigned to an interface and is not routable outside the device.

Unspecified Address

The unspecified unicast address is the all-0s address, represented as ::. It cannot be assigned to an interface but is reserved for communications when the sending device does not have a valid IPv6 address yet.

For example, a device uses :: as the source address when using the duplicate address detection (DAD) process.The DAD process ensures a unique link-local address. Before a device can begin using its newly created link-local address, it sends out an all-nodes multicast to all devices on the link, with its new address as the destination. If the device receives a response, it knows that link- local address is in use and, therefore, needs to create another link-local address.

Unique Local Address

These are private addresses. However, unlike in IPv4, IPv6 ULAs are globally unique.This is possible because of the relatively large amount of address space in the Global ID portion

Unique local addresses have the following characteristics:

■ Possess a globally unique prefix or at least have a very high probability of being unique
■ Allow sites to be combined or privately interconnected without address conflicts or addressing renumbering
■ Remain independent of any Internet service provider and can be used within a site without having Internet connectivity
■ If accidentally leaked outside a site by either routing or the Domain Name System (DNS), don't cause a conflict with any other addresses
■ Can be used just like a global unicast address

Multicast

Multicast is a technique by which a device sends a single packet to multiple destinations simultaneously.An IPv6 multicast address defines a group of devices known as a multicast group and is equivalent to IPv4 224.0.0.0/4. IPv6 multicast addresses have the prefix FF00::/8.

Two types of IPv6 multicast addresses are used:
■ Assigned multicast
■ Solicited-node multicast

Assigned Multicast

Assigned multicast addresses are used in context with specific protocols. Two common IPv6 assigned multicast groups include the following:
■ FF02::1 All-nodes multicast group: This is a multicast group that all IPv6-enabled devices join. As with a broadcast in IPv4, all IPv6 interfaces on the link process packets sent to this address. For example, a router sending an ICMPv6 Router Advertisement (RA) uses the all- nodes FF02::1 address. IPv6-enabled devices can then use the RA information to learn the link's address information, such as prefix, prefix length, and default gateway.

■ FF02::2 All-routers multicast group: This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the ipv6 unicast-routing global configuration command.A packet sent to this group is received and processed by all IPv6 routers on the link or network. For example, IPv6-enabled devices send ICMPv6 Router Solicitation (RS) messages to the all-routers multicast address requesting an RA message.

Solicited-Node Multicast

In addition to every unicast address assigned to an interface, a device has a special multicast address known as a solicited-node multicast address These multicast addresses are automatically created using a special mapping of the device's unicast address with the solicited-node multicast prefix FF02:0:0:0:0:1:FF00::/104.

■ Address resolution: In this mechanism, which is equivalent to ARP in IPv4, an IPv6 device sends an NS message to a solicited-node multicast address to learn the link layer address of a device on the same link.The device recognizes the IPv6 address of the destination on that link but needs to know its data link address.

■ Duplicate address detection (DAD): As mentioned earlier, DAD allows a device to verify that its unicast address is unique on the link.An NS message is sent to the device's own solicited-node multicast address to determine whether anyone else has this same address.

■ FF02:0:0:0:0:FF00::/104 multicast prefix: This is the first 104 bits of the all solicited-node multicast address.

■ Least significant 24 bits: These bits are copied from the far-right 24 bits of the global unicast or link-local unicast address of the device.

Anycast

The last major classification of IPv6 address types is the anycast address.An anycast address can be assigned to more than one device or interface.A packet sent to an anycast address is routed to the "nearest" device that is configured with the anycast address

Conventions for Writing IPv6 Addresses

IPv6 conventions use 32 hexadecimal numbers, organized into eight hextets of four hex digits separated by colons, to represent a 128-bit IPv6 address. For example:
2340:1111:AAAA:0001:1234:5678:9ABC
To make things a little easier, two rules allow you to shorten what must be configured for an IPv6 address:
■ Rule 1: Omit the leading 0s in any given hextet.
■ Rule 2: Omit the all-0s hextets. Represent one or more consecutive hextets of all hex 0s with
a double colon (::), but only for one such occurrence in a given address.

Conventions for Writing IPv6 Prefixes

An IPv6 prefix represents a range or block of consecutive IPv6 addresses.The number that represents the range of addresses, called a prefix, is usually seen in IP routing tables, just as you see IP subnet numbers in IPv4 routing tables.
As with IPv4, when writing or typing a prefix in IPv6, the bits past the end of the prefix length are all binary 0s.The following IPv6 address is an example of an address assigned to a host:

2000:1234:5678:9ABC:1234:5678:9ABC:1111/64 The prefix in which this address resides is as follows: 2000:1234:5678:9ABC:0000:0000:0000:0000/64 When abbreviated, this is: 2000:1234:5678:9ABC::/64

The following list summarizes some key points about how to write IPv6 prefixes:

■ The prefix has the same value as the IP addresses in the group for the first number of bits, as defined by the prefix length.
■ Any bits after the prefix length number of bits are binary 0s.
■ The prefix can be abbreviated with the same rules as for IPv6 addresses.
■ If the prefix length is not on a hextet boundary, write down the value for the entire hextet.

IPv6 Subnetting

In many ways, subnetting IPv6 addresses is much simpler than subnetting IPv4 addresses. A typical site is assigned an IPv6 address space with a /48 prefix length. Because the least significant bits are used for the interface ID, that leaves 16 bits for the subnet ID and a /64 subnet prefix length

EUI-64 Concept

(EUI stands for Extended Unique Identifier)

the second half of the IPv6 address is called the interface ID.The value of the interface ID portion of a global unicast address can be set to any value, as long as no other host in the same subnet attempts to use the same value. However, the size of the interface ID was chosen to allow easy autoconfiguration of IP addresses by plugging the MAC address of a network card into the interface ID field in an IPv6 address.

MAC addresses are 6 bytes (48 bits) in length.To complete the 64-bit interface ID, IPv6 fills in 2 more bytes by separating the MAC address into two 3-byte halves. It then inserts hex FFFE between the halves and sets the seventh bit in the first byte to binary 1 to form the interface ID

Stateless Address Autoconfiguration

IPv6 supports two methods of dynamic configuration of IPv6 addresses:
■ Stateless address autoconfiguration (SLAAC): A host dynamically learns the /64
prefix through the IPv6 Neighbor Discovery Protocol (NDP) and then calculates the rest of its address by using the EUI-64 method.
■ DHCPv6: This works the same conceptually as DHCP in IPv4.

By using the EUI-64 process and Neighbor Discovery Protocol (NDP), SLAAC allows a device

to determine its entire global unicast address without any manual configuration and without a DHCPv6 server.

Migration to IPv6

Two major transition strategies are currently used to migrate to IPv6:
NDP Router Solicitation
“Need information from the router”
■ Dual-stacking: In this integration method, a node has implementation and connectivity to both an IPv4 network and an IPv6 network.This is the recommended option and involves running IPv4 and IPv6 at the same time.
■ Tunneling: Tunneling is a method for transporting IPv6 packets over IPv4-only networks by encapsulating the IPv6 packet inside IPv4. Several tunneling techniques are available.

Because of the simplicity of running dual-stacking, it will most likely be the preferred strategy as IPv4-only networks begin to disappear. But it will probably still be decades before we see enterprise networks running exclusively IPv6

################
Wireless
################

WLCs can use the older Lightweight Access Point Protocol (LWAPP) or the more current Control and Provisioning of Wireless Access Points (CAPWAP).With a WLC,VLAN pooling can be used to assign IP addresses to wireless clients from a pool of IP subnets and their associated VLANs.

Wireless Standards

The IEEE 802.11 WLAN standards define how radio frequencies (RFs) are used for wireless links. To avoid interference, different channels within an RF can be used.

The RF spectrum includes all types of radio communications, including the 2.4-GHz and 5-GHz frequencies used by wireless devices.

Channels

A frequency range is typically called a band of frequencies For example, a wireless LAN device with a 2.4-GHz antenna can actually use any frequency from 2.4000 to 2.4835 GHz.The 5-GHz band lies between 5.150 and 5.825 GHz.

The bands are further subdivided into frequency channels. Channels become particularly important when the wireless devices in a specific area become saturated. Each channel is known by a chan- nel number and is assigned to a specific frequency.As long as the channels are defined by a national or international standards body, they can be used consistently in all locations

The only way to avoid any overlap between adjacent channels is to configure access points (APs) to use only channels 1, 6, and 11.

802.11 Standards

Most of the standards specify that a wireless device must have one antenna to transmit and receive wireless signals on the specified radio frequency (2.4 GHz or 5 GHz). Some of the newer standards that transmit and receive at higher speeds require APs and wireless clients to have multiple antennas using the multiple input, multiple output (MIMO) technology. MIMO uses multiple antennas as both the transmitter and receiver to improve communication performance. Up to four antennas can be supported.

Wireless Topologies

The 802.11 standard identifies two main wireless topology modes: infrastructure mode and Independent Basic Service Set (IBSS). IBSS is also knows as ad hoc mode.With the ubiquity of wireless networks, mesh topologies are now common.

With infrastructure mode, wireless clients interconnect via an AP configuration of the APs to share the same SSID allows wireless clients to roam between BSAs.

Infrastructure mode terminology includes the following:

■ Basic service set (BSS): This consists of a single AP interconnecting all associated wireless clients.

■ Basic service area (BSA): This is the area that is bound by the reach of the AP’s signal.The BSA is also called a cell

■ Basic service set identifier (BSSID): This is the unique, machine-readable identifier for the AP that is in the format of a MAC address and is usually derived from the AP’s wireless MAC address.

■ Service set identifier (SSID): This is a human-readable, non-unique identifier used by the AP to advertise its wireless service.

■ Distribution system (DS): APs connect to the network infrastructure using the wired DS, such as Ethernet. An AP with a wired connection to the DS is responsible for translating frames between 802.3 Ethernet and 802.11 wireless protocols.

■ Extended service set (ESS): When a single BSS provides insufficient coverage, two or more BSSs can be joined through a common DS into an ESS.An ESS is the union of two or more BSSs interconnected by a wired DS. Each ESS is identified by its SSID, and each BSS is identified by its BSSID.

IBSS, or Ad Hoc Mode

In the 802.11 standard, Independent Basic Service Set (IBSS) is defined as two devices connected wirelessly in a peer-to-peer (P2P) manner without the use of an AP. One device takes the role of advertising the wireless network to clients.The IBSS allows two devices to communicate directly without the need for any other wireless devices IBSSs do not scale well beyond 8 to 10 devices.

Mesh

Having a wired DS connecting all APs is not always practical or necessary. Instead, APs can be configured to connect in mesh mode. In this mode, APs bridge client traffic between each other

Each AP in the mesh maintains a BSS on one channel used by wireless clients.Then the APs bridge between each other using other channels.The mesh network runs its own dynamic routing protocol to determine the best path to the wired network.

AP Architectures

APs can be networked together in a variety of architectures.The size and scalability of the network determine which architecture is most suited for a given implementation.

An autonomous AP is a self-contained device with both wired and wireless hardware so that it can bridge to the wired VLAN infrastructure wireless clients that belong to SSIDs, Each autonomous AP must be configured with a management IP address so that it can be remotely accessed using Telnet, SSH, or a web interface. Each AP must be individually managed and maintained unless you use a management platform such as Cisco DNA Center.

Cloud-Based AP Architecture

Cloud-based AP management is an alternative to purchasing a management platform.The AP management function is pushed into the Internet cloud. For example, Cisco Meraki is a cloud-based AP management service that allows you to automatically deploy Cisco Meraki APs.These APs can then be managed from the Meraki cloud web interface (dashboard)

there are two distinct paths for data traffic and for management traffic, corresponding to the following two functions:
■ A control plane: Traffic used to control, configure, manage, and monitor the AP itself
■ A data plane: End-user traffic passing through the AP

Lightweight AP Architectures

Wireless LAN controllers (WLCs) use Lightweight Access Point Protocol (LWAPP) to communicate with lightweight APs (LAPs)
LAPs are useful in situations where many APs are required in the network.They are “lightweight” because they only perform the 802.11 wireless operation for wireless clients. Each LAP is automatically configured and managed by the WLC.

link aggregation group (LAG) so they can be bundled together. Much like EtherChannel, LAG provides redundancy and load balancing.

CAPWAP Operation

The division of labor between the WLC and LAPs is known as split-MAC architecture.The LAP must interact with wireless clients on some low level, known as the Media Access Control (MAC) layer. These functions must stay with the LAP hardware, closest to the clients.The management functions are not integral to handling frames but are things that should be centrally administered.Therefore, those functions can be moved to a centrally located platform away from the AP

LWAPP has been replaced with the Control and Provisioning of Wireless Access Points (CAPWAP) tunneling protocol to implement these split-MAC functions. CAPWAP uses two tunnels—one for control and one for data

■ CAPWAP control message tunnel: Carries exchanges that are used to configure the LAP and manage its operation.The control messages are authenticated and encrypted, so the LAP is securely controlled by only the appropriate WLC and then transported over the control tunnel using UDP port 5246.

■ CAPWAP data tunnel: Used for packets traveling to and from wireless clients that are associ- ated with the AP. Data packets are transported over the data tunnel using UDP port 5247 but are not encrypted by default.When data encryption is enabled for a LAP, packets are protected with Datagram Transport Layer Security (DTLS).

Wireless Security Protocols

Wireless traffic is inherently different from traffic traveling over a wired infrastructure.Any wireless device operating in the same frequency can hear the frames and potentially read them. Therefore,WLANs need to be secured to allow only authorized users and devices and to prevent eavesdropping and tampering of wireless traffic.

Wireless Authentication Methods

For wireless devices to communicate over a network, they must first associate with the AP. An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it. During this process, transmitted frames can reach any device within range. If the wireless connection is not secured, then others can read the traffic

The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:
■ Open system authentication: Should only be used in situations where security is of no concern.The wireless client is responsible for

providing security such as by using a virtual private network (VPN) to connect securely.
■ Shared key authentication: Provides mechanisms shown in Table 22-3 to authenticate and encrypt data between a wireless client and an AP. However, the password must be pre-shared between the parties to allow connection.

WPA and WPA2

Home routers typically have two choices for authentication:WPA and WPA2.WPA2 is the stronger of the two.WPA2 authentication methods included the following:
■ Personal: Intended for home or small office networks, users authenticate using a pre-shared key (PSK).Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
■ Enterprise: Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security.The device must be authenticated by the RADIUS server, and then users must authenticate using the 802.1X standard, which uses Extensible Authentication Protocol (EAP) for authentication.

802.1X/EAP

With open and WEP authentication, wireless clients are authenticated locally at the AP without further intervention.The scenario changes with 802.1X:The client uses open authentication to associate with the AP, and then the client authentication process occurs at a dedicated authentication server.

■ Supplicant: The client device that is requesting access.
■ Authenticator: The network device that provides access to the network. In Figure 22-11, the
AP forwards the supplicant’s message to the WLC.
■ Authentication server (AS): The device that permits or denies network access based on a user database and policies (usually a RADIUS server).

WPA3

WPA3 includes four features:

■ WPA3-Personal: In WPA2-Personal, threat actors can listen in on the “handshake” between a wireless client and the AP and use brute-force attacks to try to guess the PSK. WPA3-Personal thwarts such attacks by using Simultaneous Authentication of Equals (SAE), a feature specified in the IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.

■ WPA3-Enterprise: WPA3-Enterprise still uses 802.1X/EAP authentication. However,
it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards.WPA3-

Enterprise adheres to the Commercial National Security Algorithm (CNSA) suite, which is commonly used in high-security Wi-Fi networks.

■ Open networks: Open networks in WPA2 send user traffic in unauthenticated plaintext. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.

■ IoT onboarding: Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices that were not previously configured,WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration and need any easy way to get connected to the wireless network. Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hard-coded public key.The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code.The network administrator can scan the QR code and quickly onboard the device.Although DPP is not strictly part of theWPA3 standard, it will replace WPS over time.

Wireless Encryption Methods

Encryption is used to protect data. An intruder may be able to captured encrypted data, but he or she would not be able to decipher it in any reasonable amount of time.The following encryption protocols are used with wireless authentication:
■ Temporal Key Integrity Protocol (TKIP): TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment and addresses the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP but encrypts the Layer 2 payload using TKIP and carries out a message integrity check (MIC) in the encrypted packet to ensure that the message has not been altered.
■ Advanced Encryption Standard (AES): AES is the encryption method used by WPA2. It is the preferred method because it is a very strong method of encryption. It uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), which allows destination hosts to recognize if the encrypted and nonencrypted bits have been altered.
■ The Galois/Counter Mode Protocol (GCMP): This is a robust authenticated encryption suite that is more secure and more efficient than CCMP. GCMP is used in WPA3.

##################
Security
##################

Endpoint Security

Endpoints are hosts including laptops, desktops, servers, and IP phones. In addition, a network that has a bring your own device (BYOD) policy

includes employee-owned devices. Endpoints are par- ticularly susceptible to malware-related attacks that originate through email or web browsing. If an endpoint is infiltrated, it can become a point from which a threat actor can gain access to critical system devices, such as servers and sensitive information.
Endpoints are best protected by host-based Cisco Advanced Malware Protection (AMP) software. AMP products include endpoint solutions such as Cisco AMP for Endpoints. In addition, content security appliances provide fine-grained control over email and web browsing for an organization's users.
Cisco has two content security appliance products:
■ Cisco Email Security Appliance (ESA)
■ Cisco Web Security Appliance (WSA)

Cisco ESA

Cisco ESA is special device designed to monitor email's primary protocol, Simple Mail Transfer Protocol (SMTP). Cisco ESA can do the following:
■ Block known threats
■ Remediate against stealth malware that evades initial detection
■ Discard emails with bad links

■ Block access to newly infected sites
■ Encrypt content in outgoing email to prevent data loss

Cisco WSA

Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting. Cisco WSA provides complete control over how users access the Internet. Certain features and applications, such as chat, messaging, video, and audio can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization's requirements. WSA can perform blacklisting of URLs, URL filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

Access Control

Many types of authentication can be performed on networking devices to control access, and each method offers varying levels of security.

Local Authentication

The simplest method of remote access authentication is to configure a login and password combination on console, vty lines, and aux ports

This method, however, provides no accountability,and the password is sent in plaintext.Anyone with the password can gain entry to the device.

Instead of using a shared password with no usernames, you can use the username username secret password command to configure local username/password pairs. Require a username/password

pair with the login local line configuration command. Use the no password line configuration command to remove any configured passwords

SSH Configuration

Secure Shell (SSH) is considered a security best practice because Telnet (port 23) uses insecure plaintext transmission of both the login and the data across the connection. SSH (port 22) is a more secure form of remote access:

■ It requires a username and a password, both of which are encrypted during transmissions.
■ The username and password can be authenticated using the local database method.
■ It provides more accountability because the username is recorded when a user logs in.

Switch Port Hardening

default configuration exposes switches to some security threats.The following are security best practices for unused interfaces:

■ Administratively disable the interface by using the shutdown interface subcommand.
■ PreventVLAN trunking by making the port a nontrunking interface using the switchport
mode access interface subcommand.
■ Assign the port to an unusedVLAN by using the switchport access vlan number interface
subcommand.
■ Set the native VLAN to not be VLAN 1 but to instead be an unused VLAN, using the
switchport trunk native vlan vlan-id interface subcommand.

Even when you shut down unused ports on the switches, if a device is connected to one of those ports and the interface is enabled, trunking can occur. In addition, all ports are in VLAN 1 by default. A good practice is to put all unused ports in a black hole VLAN.

AAA

Configuring usernames and passwords on all your network devices is not very scalable.A better option is to use an external server to centralize and secure all username/password pairs.To address this issue, Cisco devices support the authentication, authorization, and accounting (AAA) framework to help secure device access.
Cisco devices support two AAA authentication protocols:
■ Terminal Access Controller Access Control System Plus (TACACS+, pronounced as “tack-axe plus”)
■ Remote Authentication Dial-In User Service (RADIUS)

The choice of TACACS+ or RADIUS depends on the needs of the organization. For example, a large ISP might select RADIUS because it supports the

detailed accounting required for billing users.An organization with various user groups might selectTACACS+ because it requires authorization policies to be applied on a per-user or per-group basis.

Both TACACS+ and RADIUS use a client/server model, where an authenticating device is the client talking to an AAA server

802.1X

IEEE 802.1X is a standard port-based access control and authentication protocol. It is ideal for restricting unauthorized access through publicly available LAN devices, such as switches and wireless access points.

802.1X defines three roles for devices in the network

■ Client (supplicant): This is usually the 802.1X-enabled port on the device that requests access to LAN and switch services and responds to requests from the switch. In Figure 20-4, the device is a PC running 802.1X-compliant client software.
■ Switch (authenticator): The switch controls physical access to the network, based on the authentication status of the client.The switch acts as a proxy between the client and the authentication server. It requests identifying information from the client, verifies that informa- tion with the authentication server, and relays a response to the client.
■ Authentication server: The authentication server performs the actual authentication of the client.The authentication server validates the identity of the client and notifies the switch about whether the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. RADIUS is the only supported authentication server.

The 802.1X process is summarized as follows:

■ The RADIUS authentication server is configured with usernames and passwords.
■ Each LAN switch is enabled as an 802.1X authenticators, is configured with the IP address of
the authentication server, and has 802.1X enabled on all required ports.

■ Users that connect devices to 802.1X-enabled ports must know the username/password before they can access the network.

#Port Security

If you know which devices should be cabled and connected to particular interfaces on a switch, you can use port security to restrict that interface so that only the expected devices can use it.This reduces exposure to some types of attacks in which the attacker connects a laptop to the wall socket or uses the cable attached to another end device to gain access to the network.

Port Security Configuration

Port security configuration involves several steps. Basically, you need to make the port an access port, which means the port is not doing anyVLAN trunking.You then need to enable port security and configure the Media Access Control (MAC) addresses of the devices allowed to use that port.The following list outlines the steps in port security configuration, including the configuration commands used:

1-Configure the interface for static access mode by using the switchport mode access interface subcommand.
2-Enable port security by using the switchport port-security interface subcommand.
3-(Optional) Override the maximum number of allowed MAC addresses associated with the interface (1) by using the switchport port-security maximum number interface subcommand.
4-(Optional) Override the default action when there is a security violation (shutdown) by using the switchport port-security violation {protect | restrict | shutdown} interface subcommand.
5-(Optional) Predefine any allowed source MAC address(es) for this interface by using the switchport port-security mac-address mac-address command. Use the command multiple times to define more than one MAC address.
6-(Optional) Instead of taking step 5, configure the interface to dynamically learn and configure the MAC addresses of currently connected hosts by configuring the switchport port-security mac-address sticky interface subcommand.

When an unauthorized device attempts to send frames to the switch interface, the switch can issue informational messages, discard frames from that device, or even discard frames from all devices
by effectively shutting down the interface. Exactly which action the switch port takes depends on the option you configure in the switchport port-security violation command actions that the switch will take based on whether you configure the option protect, restrict, or shutdown (default).

To verify port security configuration, use the more general show port-security command or the more specific show port-security interface type number command

Port Security Aging

Port security aging can be used to set the aging time for static and dynamic secure addresses on a port.Two types of aging are supported per port:
■ Absolute: The secure addresses on the port are deleted after the specified aging time.
■ Inactivity: The secure addresses on the port are deleted only if they are inactive for the
specified aging time.
Use the switchport port-security aging command to enable or disable static aging for the secure port or to set the aging time or type

Port Restoration After a Violation

When port security is activated on an interface, the default action when a violation occurs is to shut down the port.A security violation can occur in one of two ways:
■ The maximum number of secure MAC addresses has been added to the address table for that interface, and a station whose MAC address is not in the address table attempts to access the interface.
■ An address learned or configured on one secure interface is seen on another secure interface in the sameVLAN.
When a violation occurs, a syslog message is sent to the console, stating that the interface is now in the err-disable state.The console messages include the port number and the MAC address that caused the violation

You can use the show interface type number status or show port-security interface type number command to verify the current state of the port.To restore the port, you must first manually shut down the interface and then reactivate it

LAN Threat Mitigation

This section reviews LAN threats and mitigation techniques for VLAN attacks, DHCP attacks, and ARP attacks.

Native and Management VLAN Modification

The IEEE 802.1Q specification defines a native VLAN to maintain backward compatibility with untagged traffic that is common in legacy LAN scenarios.A nativeVLAN serves as a common identifier on opposite ends of a trunk link.VLAN 1 is the nativeVLAN by default.

A management VLAN is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the managementVLAN by default.The managementVLAN is assigned an IP address and subnet mask, allowing the switch to be managed through HTTP,Telnet, SSH, or SNMP.
It is a best practice to configure the nativeVLAN as an unusedVLAN distinct fromVLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain. Likewise, the management VLAN should be configured as something other thanVLAN 1.The management and nativeVLANs can be config- ured as the same VLAN

VLAN Attacks

VLAN attacks can be launched in one of three ways:
■ Spoofing Dynamic Trunking Protocol (DTP) messages: Spoofing DTP messages from the attacking host can cause the switch to enter trunking mode. From here, the attacker can send traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.
■ Introducing a rogue switch and enabling trunking: After doing this, an attacker can access all the VLANs on the victim switch from the rogue switch.
■ Mounting a double-tagging (or double-encapsulated) attack: This type of VLAN hop- ping attack takes advantage of the way hardware on most switches operates.A threat actor in specific situations could embed a hidden 802.1Q tag inside the frame that already has an 802.1Q tag.This

tag allows the frame to go to aVLAN that the original 802.1Q tag did not specify.

VLAN Attack Mitigation

Use the following steps to mitigate VLAN hopping attacks:

1-Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.

2-Disable unused ports and put them in an unusedVLAN.

3-Manually enable the trunk link on a trunking port by using the switchport mode
trunk command.

4-Disable DTP (auto trunking) negotiations on trunking ports by using the switchport
nonegotiate command.

5-Set the nativeVLAN to aVLAN other thanVLAN 1 by using the switchport trunk native vlan vlan_number command.

DHCP Attacks

Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

DHCP Starvation Attacks

The goal of a DHCP starvation attack is to create a denial-of-service condition for connecting clients. DHCP starvation attacks require an attack tool such as Gobbler. Gobbler looks at the entire scope of leasable IP addresses and tries to lease them all. Specifically, it creates DHCP discovery messages with bogus MAC addresses.

DHCP Spoofing Attacks

A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. For example, in Figure 20-6, R1 is configured to relay DHCP requests to the DHCP server attached to R2.

DHCP Snooping

To protect against DHCP attacks, DHCP snooping uses the concept of trusted and untrusted ports.

Some critical features of a DHCP snooping configuration include the following:

■ Trusted ports: Trusted ports allow all incoming DHCP messages.
■ Untrusted ports, server messages: Untrusted ports discard all incoming messages that are considered server messages.

■ Untrusted ports, client messages: Untrusted ports apply more complex logic for messages considered client messages.They check whether each incoming DHCP message conflicts with existing DHCP binding table information; if so, they discard the DHCP message. If the message has no conflicts, the switch allows the message through, which typically results in the addition of new DHCP binding table entries.
■ Rate limiting: This feature optionally limits the number of received DHCP messages per second per port.

Use the following steps to enable DHCP snooping:

1-Enable DHCP snooping by using the ip dhcp snooping global configuration command.

2- On trusted ports, use the ip dhcp snooping trust interface configuration command.

3- Limit the number of DHCP discovery messages that can be received per second on untrusted ports by using the ip dhcp snooping limit rate number interface configuration command.This helps mitigate DHCP starvation attacks.

4- Enable DHCP snooping by VLAN or by a range of VLANs by using the ip dhcp snooping vlan global configuration command.

ARP Attacks

On Ethernet LANs, hosts are allowed to send an unsolicited Address Resolution Protocol (ARP) reply called a gratuitous ARP message.These ARP messages cause all other hosts on the LAN to store the MAC address and IP address in their ARP caches.The problem is that an attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch would update its MAC table accordingly.Therefore, any host can claim to be the owner of any IP and MAC address combination.

Dynamic ARP Inspection

To prevent ARP spoofing and then ARP poisoning, a switch must ensure that only valid ARP requests and replies are relayed. Dynamic ARP inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by doing the following:
■ Not relaying invalid or gratuitous ARP replies out to other ports in the same VLAN
■ Intercepting all ARP requests and replies on untrusted ports
■ Verifying each intercepted packet for a valid IP-to-MAC binding
■ Dropping and logging ARP replies coming from invalid source to prevent ARP poisoning
■ Error disabling the interface if the configured DAI number of ARP packets is exceeded
To mitigate the chances of ARP spoofing and ARP poisoning, follow these DAI implementation guidelines:
■ Enable DHCP snooping globally.

■ Enable DHCP snooping on selectedVLANs.

■ Enable DAI on selectedVLANs.
■ Configure trusted interfaces for DHCP snooping and ARP inspection.

DAI can also be configured to check for both destination or source MAC and IP addresses with the ip arp inspection validate command. Only one command can be configured. Entering multiple ip arp inspection validate commands overwrites the previous command.To include more
than one validation method, enter them on the same command line,

Attack Vectors and Data Exfiltration

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate outside or inside a network. For example, threat actors may target a network through the Internet to disrupt network operations and create a denial of service (DoS) attack.An internal user, such as an employee, might accidentally or intentionally disrupt the network or steal confidential data. Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices.
Employees may also have knowledge of the corporate network, its resources, and its confidential data. Data loss or data exfiltration occurs when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. Network security professionals must protect the organization’s data. Various data loss prevention (DLP) controls must be implemented, combining strategic, operational, and tactical measures

Types of Malware

Malware, which is short for malicious software, is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks.Viruses, worms, and Trojan horses are types of malware:

■ A worm executes arbitrary code and installs copies of itself in the memory of the infected computer.The main purpose of a worm is to automatically replicate itself and spread across the network from system to system.

■ A virus is malicious software that executes a specific, unwanted, often harmful function on a computer.

■ A Trojan horse is a non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file.When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within.

Network Attacks

Network attacks include reconnaissance attacks, access attacks, DoS attacks, social engineering attacks, and attacks to exploit the vulnerabilities of the TCP/IP protocol suite.

Reconnaissance Attacks

Reconnaissance is information gathering.Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access attacks or DoS attacks

Access Attacks

The purpose of access attacks is to gain entry to web accounts, confidential databases, and other sensitive information.Threat actors use access attacks on network devices and computers to retrieve data, gain access, or escalate access privileges to administrator status \

Social Engineering Attacks

In social engineering attacks, threat actors attempt to manipulate individuals into performing actions or divulging confidential information.

DoS and DDoS Attacks

A DoS attack creates some sort of interruption of network services to users, devices, or applications. DoS attacks are created in two ways:
■ Overwhelming quantity of traffic: The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle.This causes transmission and response times to slow down. It can also crash a device or service.
■ Maliciously formatted packets: The threat actor sends a maliciously formatted packet to a host or an application, and the receiver is unable to handle it.This causes the receiving device to run very slowly or crash.

DoS attacks are relatively simple to conduct, even by an unskilled threat actor. A DDoS attack is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor may build a network of infected hosts, known as zombies. A network of zombies is called a botnet.The threat actor can then use a command-and-control (CnC) program to instruct the botnet of zombies to carry out a DDoS attack.

IP Attacks

IP does not validate whether the source IP address contained in a packet actually came from that source. For this reason, 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. Security analysts must understand the different fields in both the IPv4 and IPv6 headers.

Transport Layer Attacks

Threat actors conduct port scans of target devices to discover which services are available.A threat actor can exploit TCP and UDP in the following ways:

■ TCP SYN flood attack: This type of attack exploits the TCP three-way handshake. The threat actor continually sends TCP SYN session request packets with a randomly spoofed source IP address to a target. The target device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet.The responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections, and TCP services are denied to legitimate users.

■ TCP reset attack: A threat actor could use a TCP reset attack to send a spoofed packet containing a TCP RST to one or both endpoints.This creates a DoS condition for the connection.

■ TCP session hijacking: A threat actor takes over an already-authenticated host as it communicates with the target.The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not receive, data from the target device.

■ UDP flood attack: The threat actor uses a tool to send a flood of UDP packets, often from a spoofed host, to a server on the subnet.The program sweeps through all the known ports, trying to find closed ports.This causes the server to reply with an ICMP port unreachable message. Because there are many closed ports on the server, there is a lot of traffic on the segment, which uses up most of the bandwidth.The result is very similar to the result of a DoS attack.

##############
WAN
##############

WAN Topologies

■ Point-to-point: Typically uses a dedicated leased-line connection, such as T1/E1.

■ Hub-and-spoke: Offers a single-homed, point-to-multipoint topology in which a single interface on the hub router can be shared with multiple spoke routers through the use of virtual interfaces.

■ Full mesh: Gives each router a connection to every other router. Requires a large number of virtual interfaces.

■ Dual-homed: Provides redundancy for a single-homed hub-and-spoke topology by providing a second hub to connect to spoke routers.

A business can choose to implement a variety of these topologies. For example, an enterprise
might choose to implement a full mesh topology between its regional headquarters. It might use
a hub-and-spoke topology between regional headquarters and branch offices. If two of the branch offices communicate frequently, the network administrators might contract for a point-to-point link to reduce the traffic load on the hub routers. Using dual-homed connections to the Internet ensures that customers, partners, and teleworkers can always access the enterprise's resources.

Dedicated Connection Options

Also called leased lines, dedicated connections are pre-established point-to-point WAN connections from the customer premises through the provider network to a remote destination

Leased lines are usually more expensive than switched services because of the dedicated, always-on cost of providing WAN service to the customer.The dedicated capacity removes latency and jitter and provides a layer of security because only the customer's traffic is allowed

Circuit-Switched Connection Options

The two main types of circuit-switched connections are analog dialup and ISDN. Both technologies have limited implementation bases in today's networks. However, they are both still used in remote rural areas and other areas of the globe where more recent technologies are not yet available.
Analog dialup uses modems at very low-speed connections that might be adequate for the exchange of sales figures, prices, routine reports, and email, or as an emergency backup link.
ISDN turns the local loop into a TDM digital connection, which enables it to carry digital signals that result in higher-capacity switched connections than are available with analog modems.Two types of ISDN interfaces exist:
■ Basic Rate Interface (BRI): Provides two 64-kbps B-channels for voice or data transfer and a 16-kbps D-channel for control signaling.
■ Primary Rate Interface (PRI): Provides 23 B-channels with 64 kbps and 1 D-channel with 64 kbps in North America, for a total bit rate of up to 1.544 Mbps. Europe uses 30 B-channels and 1 D-channel, for a total bit rate of up to 2.048 Mbps.

Packet-Switched Connection Options

The most common packet-switching technologies used in today's enterprise WANs include Metro Ethernet and MPLS. Legacy technologies include X.25 and ATM.

Metro Ethernet
Metro Ethernet (MetroE) uses IP-aware Ethernet switches in the service provider's network cloud to offer enterprises converged voice, data, and video services at Ethernet speeds. Consider some benefits of Metro Ethernet:
■ Reduced expenses and administration: Enables businesses to inexpensively connect numerous sites in a metropolitan area to each other and to the Internet without the need for expensive conversions to ATM or Frame Relay
■ Easy integration with existing networks: Connects easily to existing Ethernet LANs
■ Enhanced business productivity: Enables businesses to take advantage of productivity- enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications,VoIP, and streaming and broadcast video

MPLS
Multiprotocol Label Switching (MPLS) has the following characteristics:
■ Multiprotocol: MPLS can carry any payload, including IPv4, IPv6, Ethernet, ATM, DSL, and Frame Relay traffic.
■ Labels: MPLS uses labels inside the service provider's network to identify paths between distant routers instead of between endpoints.
■ Switching: MPLS actually routes IPv4 and IPv6 packets, but everything else is switched.

Internet Connection Options

Broadband connection options typically are used to connect telecommuting employees to
a corporate site over the Internet.These options include Digital Subscriber Line (DSL), cable, and wireless.

DSL
DSL technology, is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data and provides IP services to subscribers.

Current DSL technologies use sophisticated coding and modulation techniques to achieve data rates of up to 8.192 Mbps. A variety of DSL types, standards, and emerging technologies exist. DSL is
a popular choice for enterprise IT departments to support home workers.

Cable Modem
A cable modem provides an always-on connection and simple installation a subscriber connects a computer or LAN router to the cable modem, which

translates the digital signals into the broadband frequencies used for transmitting on a cable television network.

Wireless
In the past, the main limitation of wireless access was the need to be within range of a wireless router or a wireless modem with a wired connection to the Internet; however, the following wireless technologies enable users to connect to the Internet from almost any location:
■ Municipal Wi-Fi: Many cities have begun setting up municipal wireless networks. Some of these networks provide high-speed Internet access for free or for substantially less than the price of other broadband services.
■ WiMAX: Worldwide Interoperability for Microwave Access (WiMAX) is an IEEE 802.16 technology that is just beginning to come into use. It provides high-speed broadband service with wireless access and provides broad coverage similar to a cell phone network instead of through small Wi-Fi hotspots.
■ Satellite Internet: This technology is typically used in rural areas where cable and DSL are unavailable.
■ Cellular service: Cellular service is an option for connecting users and remote locations where no other WAN access technology is available. Common cellular access methods include 3G/4G (third generation and fourth generation) and Long-Term Evolution (LTE) cellular access.

VPN Technology

A virtual private network (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, which are routed through the Internet from the company's private network to the remote site or employee host.

VPN Benefits
Benefits ofVPN include the following:
■ Cost savings: Eliminates the need for expensive dedicated WAN links and modem banks
■ Security: Uses advanced encryption and authentication protocols that protect data from unauthorized access
■ Scalability: Can add large amounts of capacity without adding significant infrastructure
■ Compatibility with broadband technology: Supported by broadband service providers, so mobile workers and telecommuters can take advantage of their home high-speed Internet service to access their corporate networks

Types of VPN Access

■ Site-to-site VPNs: Site-to-site VPNs connect entire networks to each other. For example,
a site-to-siteVPN can connect a branch office network to a company headquarters network,Each site is equipped with a VPN gateway, such as a router, firewall,VPN concentrator, or security appliance. In the figure,

a remote branch office uses a site-to-site VPN to connect with the corporate head office.

■ Remote-access VPNs: Remote-access VPNs enable individual hosts, such as telecommuters, mobile users, and extranet consumers, to access a company network securely over the Internet,
Each host typically has client software for a client-based VPN connection or uses a web browser for clientlessVPN connection.Web-based clientlessVPNs are also typically called clientless Secure Sockets Layer (SSL) connections. However, the VPN is actually established using Transport Layer Security (TLS).TLS is the newer version of SSL and is sometimes expressed as SSL/TLS.

■ Generic Routing Encapsulation (GRE): A standard IPsec VPN (non-GRE) can only create secure tunnels for unicast traffic. GRE is a nonsecure site-to-site VPN tunneling protocol that can support multicast and broadcast traffic needed for network layer protocols. However, GRE does not by default support encryption; therefore, it does not provide a secure VPN tunnel.To solve this problem, you can encapsulate routing protocol traffic by using a GRE packet and then encapsulate the GRE packet into an IPsec packet to forward it securely to the destinationVPN gateway.The terms used to describe the encapsulation of GRE over IPsec tunnel are passenger protocol for the routing protocol, carrier protocol for GRE, and transport protocol for IPsec

■ Dynamic Multipoint VPN (DMVPN): DMVPN is a Cisco-proprietary solution for building many VPNs in an easy, dynamic, and scalable manner. DMVPN allows a network administrator to dynamically form hub-to-spoke tunnels and spoke-to-spoke tunnels

DMVPN simplifies the VPN tunnel configuration and provides a flexible option for connecting a central site with branch sites. It uses a hub-and-spoke configuration to establish a full mesh topology. Spoke sites establish secure VPN tunnels with the hub site. Each site is configured using Multipoint Generic Routing Encapsulation (mGRE).The mGRE tunnel interface allows a single GRE interface to dynamically support multiple IPsec tunnels.

DMVPN uses the following technologies:
■ Next Hop Resolution Protocol (NHRP): Maps public IP addresses for all tunnel spokes
■ IPsec encryption: Provides the security to transport private information over public networks
■ mGRE: Allows a single interface to support multiple IPsec tunnels
■ IPsec Virtual Tunnel Interface (VTI): Like DMVPN,VTI simplifies the configuration process required to support multiple sites and remote access. IPsec VTI is capable of sending and receiving both IP unicast and multicast encrypted traffic.Therefore, routing protocols are automatically supported without the need to configure GRE tunnels.
■ Service provider MPLS VPNs: MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider. Two types of MPLSVPN solutions are supported by service providers:

■ Layer 3 MPLS VPN: The service provider participates in customer routing, redistributing the routes through the MPLS network to the customer's remote locations.
■ Layer 2 MPLS VPN: The service provider is not involved in the customer routing. Instead, the provider deploys Virtual Private LAN Service (VPLS) to emulate an Ethernet multiaccess LAN segment over the MPLS network. No routing is involved. The customer's routers effectively belong to the same multiaccess network.

VPN Components

■ An existing enterprise network with servers and workstations
■ A connection to the Internet
■ VPN gateways, such as routers, firewalls,VPN concentrators, and Adaptive Security Appliances (ASAs), that act as endpoints to establish, manage, and control VPN connections
■ Appropriate software to create and manageVPN tunnels

Establishing Secure VPN Connections

VPNs secure data by encapsulating and encrypting it.With regard toVPNs, encapsulation and encryption are defined as follows:
■ Encapsulation is also called tunneling because encapsulation transmits data transparently from source network to destination network through a shared network infrastructure.
■ Encryption codes data into a different format by using a secret key, which is then used on the other side of the connection for decryption.

VPN Tunneling

Tunneling uses three classes of protocols:
■ Carrier protocol: The protocol over which information travels, such as Frame Relay, PPP, or MPLS
■ Encapsulating protocol: The protocol that is wrapped around the original data, such as GRE, IPsec, L2F, PPTP, or L2TP
■ Passenger protocol: The protocol over which the original data was carried, such as IPX, AppleTalk, IPv4, or IPv6

VPN Encryption Algorithms

Packet from the VPN
Packet in Transmission Through the Internet
Internet

The degree of security provided by any encryption algorithm depends on the key's length. Some of the most common encryption algorithms and the lengths of the keys they use are as follows:
■ Data Encryption Standard (DES) algorithm: Uses a 56-bit key and ensures high-performance encryption. DES is a symmetric key cryptosystem.
■ Triple DES (3DES) algorithm: A newer variant of DES that encrypts with one key, decrypts with a different key, and then encrypts a final time with another key.
■ Advanced Encryption Standard (AES): Provides stronger security than DES and is computationally more efficient than 3DES. AES offers three key lengths: 128-, 192-, and 256-bit keys.
■ Rivest, Shamir, and Adleman (RSA): An asymmetric key cryptosystem.The keys use a bit length of 512, 768, 1024, or larger.

With symmetric encryption, the encryption key and decryption key are the same.With asymmetric encryption, they are different.

Hashes

VPNs use a keyed hashed message authentication code (HMAC) data-integrity algorithm to guarantee a message's integrity and authenticity without any additional mechanisms.

The cryptographic strength of the HMAC depends on the cryptographic strength of the underlying hash function, the key's size and quality, and the size of the hash output length, in bits.There are two common HMAC algorithms:

■ Message Digest 5 (MD5): Uses a 128-bit shared secret key

■ Secure Hash Algorithm 1 (SHA-1): Uses a 160-bit secret key

VPN Authentication

The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure.The two peer authentication methods are as follows:

■ Pre-Shared Key (PSK): A secret key is shared between the two parties using a secure channel before it needs to be used.

■ RSA signature: This method uses the exchange of digital certificates to authenticate the peers.

IPsec Security Protocols

Both IPsec and SSLVPN technologies offer access to virtually any network application or resource. However, when security is an issue, IPsec is the superior choice

IPsec spells out the messaging necessary to secureVPN communications but relies on existing algorithms.The two main IPsec framework protocols are as follows:

■ Authentication Header (AH): Used when confidentiality is not required or permitted.AH provides data authentication and integrity for IP packets passed between two systems. It veri- fies the originators of any messages and that any message passed has not been modified during transit. AH does not provide data confidentiality (encryption) of packets. Used alone, the AH protocol provides weak protection. Consequently, it is used with the ESP protocol to provide data encryption and tamper-aware security features.

■ Encapsulating Security Payload (ESP): Provides confidentiality and authentication by encrypting the IP packet. Although both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.

IPsec relies on existing algorithms to implement encryption, authentication, and key exchange.

IPsec provides the framework, and the administrator chooses the algorithms used to implement the security services within that framework

Cloud services

Cloud providers can offer a variety of services to meet the needs of customers, including these:

■ Software as a Service (SaaS): The cloud provider is responsible for access to services that are delivered over the Internet, such as email, communication, and Office 365. Users only need to provide their data.

■ Platform as a Service (PaaS): The cloud provider is responsible for access to the development tools and services used to deliver the applications. Customers can customize the virtualized hardware.

■ Infrastructure as a Service (IaaS): The cloud provider is responsible for access to the network equipment, virtualized network services, and network infrastructure support.

■ Public clouds: Cloud-based applications and services offered in a public cloud are made available to the general population.The public cloud uses the Internet to provide services.

■ Private clouds: Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity,such as the government.A private cloud uses the organization’s private network

■ Hybrid clouds: A hybrid cloud is made up of two or more clouds (for example, part private and part public). Each part remains a distinct object, but the two parts are connected using a single architecture.

■ Community clouds: A community cloud is created for exclusive use by a specific community.The differences between public clouds and community clouds are the functional needs that have been customized for the community.

##################################
Automation and Programbility
##################################

Software-Defined Networking

Network programmability refers to the trend toward software-defined networking (SDN).At its core, SDN decouples the data, control, and management planes from the physical device, virtualizes them, and defines the networking functions in software.This creates an architecture that can be more efficiently and effectively managed through programmatic control.

Data, Control, and Management Planes

A traditional networking device contains two planes.The data plane is responsible for forwarding data as quickly as possible. To do so, it relies on tables built by the control plane. Actions taken by the data plane include the following:

- Layer 2 and Layer 3 de-encapsulation/encapsulation
- Addition or removal of an 802.1Q trunking header
- MAC address table lookups
- IP routing table lookups
- Data encryption and addition of a new IP header (as inVPNs)
- Change to the source or destination IP address (with NAT)
- Message discard due to a filter (such as an ACL or port security)

The control plane does all the calculations for populating tables used by the data plane and manages control messages between other networking devices. Figure 3-6 provides an example of OSPF operating on the control plane while the data plane is responsible for forwarding packets using the best route.

The following are the most common control plane protocols:

- Routing protocols (OSPF, EIGRP, RIP, BGP)
- IPv4 ARP
- IPv6 NDP
- Switch MAC learning
- STP

The management plane is responsible for all functions that are not directly related to controlling the data plane. Management protocols

Controllers

Traditionally, the control plane has been part of the device OS and has been distributed across every device.That means every device must spend some resources calculating and maintaining Layer 2 and Layer 3 data structures (ARP tables, routing tables, and so on).When viewed as a whole, the network’s control plane is distributed across all the networking devices.

In SDN, the functions of the control plane can be completely removed from the physical networking devices and placed in a centralized application called a controller.This frees up the devices to focus on data plane tasks.

The controller sits at the top of a network topology diagram, and the connections to the networking devices are called the southbound interface (SBI)

A northbound interface (NBI) also exists between the SDN controller and the applications that are installed on the controller.These applications are what enable network programmability.

SDN Examples: Open SDN and OpenFlow

The Open Networking Foundation (ONF) model of SDN uses an SBI called OpenFlow. OpenFlow is a protocol used between the controller and the networking devices to manage traffic flows. ONF's controller, OpenDaylight, is the result of a collaborative effort among many vendors, including Cisco.

In addition to OpenFlow, the controller has SBIs for other activities, such as configuring network devices (NetConf), managing routing (BGP-LS and PCEP), and switching traffic between VMs (OVSDB).
NBIs typically include Java APIs for applications and the RESTful API. REST (Representational State Transfer) uses HTTP messages to transfer data to other applications that are not running on the controller.
The definition and operation of these SBI and NBI protocols is beyond the scope of the exam. Just know that the ONF is continuously researching better protocols for implementation in the OpenDaylight project.
The Cisco commercial version of the OpenDaylight controller is the Cisco Open SDN Controller (OSC). OSC is available in a limited number of Cisco routers and switches.

SDN Examples: The Cisco Application Centric Infrastructure

The Cisco in-house SDN solution for data centers is Application Centric Infrastructure (ACI). ACI uses the concept of endpoint groups and policies.An endpoint group is a collection of similarVMs, such as a set of virtual switches for one of the data center's tenants. Policies define which endpoint groups can communicate with whom.
The Cisco Application Policy Infrastructure Controller (APIC) uses the endpoint topology and policies to direct the network regarding what needs to be in the forwarding tables and how to easily react to VM changes. ACI uses a partially centralized control plane, RESTful and native APIs, and OpFlex as an SBI

OpFlex is the Cisco solution for SBI communication with networking devices.Whereas OpenFlow centralizes the network control by pushing commands directly from the SDN controller, OpFlex uses policies to push command implementation down to a distributed network of controllers.

SDN Examples: Spine and Leaf

Cisco ACI uses a spine and leaf design.The physical network has a number of spine switches and
a number of leaf switches, as shown in Figure 3-11.The figure shows the links between switches, which can be single links or multiple parallel links. Spine and leaf switches are connected using the following design guidelines:

- Each leaf switch must connect to every spine switch.
- Each spine switch must connect to every leaf switch.
- Leaf switches cannot connect to each other.
- Spine switches cannot connect to each other.
- Endpoints connect only to the leaf switches.

SDN Examples: The Cisco APIC Enterprise Module

(APIC-EM)
APIC-EM is the Cisco SDN offering for enterprises.The APIC-EM solution uses a controller to manage existing network devices but also attempts to support new generations of Cisco enterprise routers and switches by using SBIs that are familiar to network administrators, such as remote access to the CLI (Telnet and SSH) and SNMP support.
Cisco also supplies a variety of applications that reside on the controller—some that use information gathered by the controller and some that control the operation of the network devices.A RESTful northbound API makes it easy to collect information about the entire network.
To support the existing enterprise infrastructure of switches and routers, the control and data planes remain unchanged.

SDA Architecture
SDA uses a controller and application programming interfaces (APIs) to communicate via southbound interfaces (SBIs) with the network infrastructure
Cisco DNA Center is an example of a controller. SBIs include Telnet/SSH, SNMP, NETCONF, and RESTCONF.

Fabric
The network infrastructure, called the fabric, is divided into two parts:
■ Underlay: This is most closely associated with the physical network. The underlay reveals additional devices and specifies how these devices are connected. Endpoints access the network through the Layer 2 devices.The underlay control plane is responsible for simple forwarding tasks.
■ Overlay: This is where tunneling protocols like Virtual Extensible LAN (VXLAN) are implemented to transport Layer 3 protocols such as IP Security (IPsec) and Control and Provisioning of Wireless Access Points (CAPWAP).The overlay is where policies are specified. The overlay is not concerned with how the devices are physically or logically connected. Its job is to abstract these inherent complexities and limitations.

Underlay
The underlay includes the switches, routers, cables, and wireless links used to create the physical network. It also includes the configuration and operation of the underlay to support the work of the overlay network.

The SDA underlay configuration includes different SDA the roles filled by each device.These roles include
■ Fabric edge node: A switch that connects to endpoint devices
■ Fabric border node: A switch that connects to devices outside SDA’s control, such as
switches that connect to the WAN routers
■ Fabric control node: A switch that performs special control plane functions for the underlay, requiring more CPU and memory

Overlay
Cisco chose theVXLAN protocol to create the tunnels used by SDA.When an SDA endpoint (for example, an end-user computer) sends a data link frame

to an SDA edge node, the ingress edge node encapsulates the frame and sends it across a VXLAN tunnel to the egress edge node

#Cisco DNA Center
Cisco DNA Center has two roles:
■ A controller in a network that uses Cisco SDA
■ A network management platform for traditional (non-SDA) network devices

Cisco DNA Center supports several southbound APIs so that the controller can communicate with the devices it manages:
■ Telnet, SSH, and SNMP to support traditional networking devices
■ NETCONF and RESTCONF to support newer devices

Cisco DNA Center Network Management Platform
Cisco DNA Center supports the expression of intent for multiple use cases, including basic automation capabilities, fabric provisioning, and policy-based segmentation (SGTs) in the enterprise network. Cisco DNA Center is a network management and command center for provisioning and configuring network devices. It is a hardware and software platform that provides a "single pane of glass"(also called a dashboard) that focuses on assurance, analytics, and automation.

Data Formats
Data formats provide a way to store and exchange data in a structured format.These are some common data formats used in network automation and programmability:
■ JavaScript Object Notation (JSON)
■ Extensible Markup Language (XML)
■ YAML Ain't Markup Language (YAML)

Each data format has specific characteristics:
■ Syntax, which includes the types of brackets used, such as [ ], ( ), and { }, the use of whitespace, indentation, quotes, commas, and more.
■ How objects are represented, such as characters, strings, lists, and arrays.
■ How key/value pairs are represented.The key, which is usually on the left side, identifies or describes the data.The value on the right is the data itself and can be a character, a string, a number, a list, or another type of data.

JSON Data Format
JSON is a human-readable data format used by applications for storing, transferring, and reading data. It is easy to parse and can be used with most modern programming languages, including Python.

JSON Syntax Rules
JSON data is a collection of key:value pairs that follow these rules:
■ Key:value pair: One key:value pair
■ Key: Text inside double quotes and before the colon that is used as the name that references a value
■ Value: The item after the colon that represents the value of the key, which can be
■ Text: Listed in double quotes
■ Numeric: Listed without quotes

■ Array: A list of values enclosed in square brackets [ ]
■ Object: One or more key:value pairs enclosed in braces { }
■ Multiple Pairs: When listing multiple key:value pairs, separate the pairs with a comma at the
end of each pair (except the last one)

RESTful APIs

APIs exist to allow two programs to exchange data. Some APIs are for interprogram communications within a single operating system (OS). Other APIs are available to programs that run on other computers.These APIs must define the networking protocol. Many are based on REST.
REST is an architectural style for designing web service applications. A REST API is an API that works on top of the HTTP protocol. It defines a set of functions developers can use to perform requests and receive responses through HTTP, such as GET and POST. An API can be considered RESTful if it has the following features:
■ Client/server: The client handles the front end, and the server handles the back end. Either can be replaced independently of the other.
■ Stateless: No client data is stored on the server between requests.The session state is stored on the client.
■ Cacheable: Clients can cache responses to improve performance.

RESTful Implementation

A RESTful web service is a collection of resources with four defined aspects:
■ The data format supported by the web service, which is often JSON, XML, or YAML
■ The set of operations supported by the web service using HTTP methods
■ The API, which must be hypertext driven
■ The base uniform resource identifier (URI) for the web service, such as http://example.com/ resources
RESTful APIs use common HTTP methods, including POST, GET, PUT, PATCH, and DELETE.

RESTful API Requests

A RESTful API is requested by using a URI, which is a string of characters that identifies a specific network resource

■ Uniform resource name (URN): Identifies only the namespace of the resource without reference to the protocol.

■ Uniform resource locator (URL): Defines the network location of a specific resource on the network.

■ Protocol/scheme: HTTPS or another protocol, such as FTP, SFTP, mailto, or NNTP
■ Hostname: In this case, www.example.com
■ Path and file name: In this case, /author/book.html
■ Fragment: In this case, #page155
A RESTful API request elicits a response from the API server

These are the different parts of the API request:
■ API server: The URL for the server that answers REST requests.
■ Resources: Specifies the API that is being requested.
■ Query: Specifies the data format and information the client is requesting from the API service. Queries can include
■ Format:This is usually JSON but can beYAML or XML.
■ Key: The key is for authorization, if required.
■ Parameters: Parameters are used to send information pertaining to the request.

#Configuration ManagementTools
A company with one network engineer might be fine managing device configurations, especially
if the configurations do not change often.The manual per-device configuration model makes great sense.With that model, the one network engineer can use the on-device startup-config as the intended ideal configuration, and he or she can make changes as needed. However, this method
does not work as well for larger networks, with hundreds or even thousands of network devices and multiple network engineers. Larger networks typically make use of configuration management tools. Configuration management tools provide different methods to define logic and processes that indicate what changes the tools should make, to which devices, and when. For each tool, engineers use a language of some kind to define the action steps.The language is often a language defined by the company offering the tool, but the tool's language is generally much easier to learn than a programming language.

Configuration tools specified for the CCNA exam are Ansible, Puppet, and Chef.

Ansible
Ansible uses an agentless architecture to manage network devices. Agentless means that the network device does not need code.Ansible uses SSH or NETCONF to make changes and extract informa- tion. Ansible uses a push model

Ansible uses several text files

■ Playbooks: Files with actions and logic about what Ansible should do
■ Inventory: Device hostnames along with information about each device, such as device roles, so Ansible can perform functions for subsets of the inventory
■ Templates: A device configuration with variables
■ Variables: A list of YAML variables that Ansible will substitute into templates

Puppet
Puppet typically uses an agent-based architecture for network device support. Some network devices enable Puppet support through an on-device agent. However, not every Cisco OS supports Puppet agents, and Puppet solves that problem using a proxy agent running on some external host

(called agentless operation).The external agent then uses SSH to communicate with the network device

Puppet uses a pull model to get a configuration to appear in the device

Puppet uses several important text files with different components

■ Manifest: A human-readable text file that defines the desired configuration state of a device
■ Resource, class, and module: Components of the manifest, with the largest component (module) being comprised of smaller classes, which are in turn comprised of resources
■ Template: A file used to create a manifest, with variable names that will be substituted

Chef
Chef, like Puppet, uses an agent-based architecture. Chef uses several important text files:
■ Resource: A configuration object whose state is managed by Chef (for instance, a set of configuration commands for a network device)
■ Recipe: The Chef logic applied to resources to determine when, how, and whether to act against the resources
■ Cookbook: A set of recipes about the same kinds of work, grouped together for easier management and sharing
■ Runlist: An ordered list of recipes that should be run against a given device
Chef requires on-device Chef client code, and many Cisco devices do not support Chef clients, so
you will likely see more use of Ansible and Puppet for Cisco device configuration management.