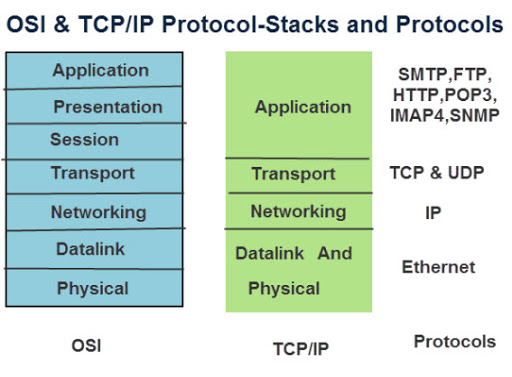
**CCNA 200-301 NOTES**

**INTRODUCTION TO TCP/IP NETWORKING OVERVIEW**

* TCP/IP is a model that defines and references a large collection of protocols that allow computers to communicate. It is commonly known as TCP/IP because the fundamental protocols in the suite are Transmission Control Protocol and Internet Protocol. Before TCP/IP each vendor had their own proprietary networking model, making it difficult for different types of computers to communicate. TCP/IP is a set of rules that allow us to take a computer out of the box and start connecting to a network. Each vendor that creates the OS, Ethernet card, Software apps etc. has implemented TCP/IP so that it is ready to go. OSI is also a good model for reference but is rarely used today.



* **Application Layer** – The protocols in this layer provide services to the application running on a computer. In short, these services provide an interface between the software and the network. For example, web browsers use HTTP to get web pages from servers. The browser would send a packet with an HTTP header ‘get’ request (Protocols generally use headers to put info used by that protocol) and the server would respond with a code such as 100 ‘ok’ or 404 ‘not found’ then return the data.
* **Transport Layer** – provides services to the above application layer using either TCP or UDP. TCP provides error recovery to applications by using numbered sequence (1, 2, 3, etc.) so that if a packet is lost, it knows to resend that packet with the missing header. UDP is ‘connectionless’ and does not provide error recovery. UDP is suitable when using time sensitive applications and correction is not necessary such as when streaming video because UDP uses less overhead and is faster. Uses PDU’s.
* **Network Layer** – Uses 1 main protocol IP, which provides the means to send packets from a source to a destination host. IP addressing is like another addressing and routing system: The Postal Service. Creates headers with source and destination IP’s and routers make decisions on where to send the packet next. This is a small overview.
* **Data Link and Physical Layers** – These two layers work together very closely; some models show this as 1 layer. It defines the protocols and hardware required to deliver data across a physical network. The datalink layer encapsulates the packet adding a header and a trailer creating a Frame that provides the necessary function/information to transfer the data over a physical medium (Ethernet, Wireless, etc). Physical layer is all cabling or wireless.
* **Conclusion** – Each layer asks for services from the next lower layer. To provide services, each layer makes use of a header and possible a trailer then encapsulates the data and is sent to the next layer. This is how data is transferred in networking. Routers operate on Layer 3 while switches and access points work on layer 2. Hubs are like switches but work in half duplex and forward packets to every port despite what’s in the header causing packet collisions. Switches use CSMA/ CD aka collision detection to prevent collisions or sending packets at the same time to cause network interruptions.

**FUNDEMENTALS OF ETHERNET LANs**

* Think of basic cabling / layer 1 stuff, cable speeds (Fast ethenet, gigabit ethernet), ethernet frames, cable pinouts.
* **Cable Speeds** – 1000Mb = Gigabit ethernet. 100Mb = Fast ethernet. Connection speeds must match on the sending / receiving port to work.
* The term Ethernet refers to a family of LAN standards that together define the physical and data-link layers to deliver ethernet frames from host to host. For ethernet cables, the connected cables create an electrical circuit and use an encoding scheme, a set of rules for communication, and the transmitting node changes the electrical signal over time and the receiver interprets these changes as 1’s and 0’s. The following is a short read on how a computer translates binary to data: <https://www.bbc.co.uk/bitesize/guides/zwsbwmn/revision/1#:~:text=The%20digits%201%20and%200,off%20states%20of%20a%20transistor.&text=Each%20instruction%20is%20translated%20into,that%20the%20processor%20can%20execute%20> . Fiber optic cables use light pulses to send data. MM used LEAD based and SM uses laser based SFP modules. MM uses multiple light beams at different angles making it cheaper than SM but cannot travel as far as SM which uses one straight light beam.
* Each wire or pinout within an Ethernet cable either transmits or receives therefore different device connection require either a crossover or a straight through cable. The key is to know whether a device acts like a PC NIC, transmitting at pins 1 and 2 or like a switch, transmitting at pins 3 and 6. Then just apply the following logic:
* **Crossover Cable:** If the endpoints transmit on the same pin pair.
* **Straight Through Cable:** If the endpoints transmit on a different pin pair.

However nowadays most Cisco switches have a feature called auto-mdix which detects the cable and if the wrong one is used; the switch will change its logic to make it work.

|  |  |
| --- | --- |
| * Transmits on pins 1 & 2 | * Transmits on pins 3 &6 |
| * PC’s | * Hubs |
| * Routers | * Switches |
| * Access Points |  |

* An ethernet frame contains a header with several pieces of information, including the destination and source mac address. The frame also has a trailer, which has FCS that detects if the frame had any transmission errors but does not recover the frame like TCP does instead just drops it. Each layer provides a service to the layer below.

**FUNDAMENTALS OF WANS AND IP ROUTING**

* **Leased Lines** – WANs are a collection of LANs that are all connected using routers. These connections between LANs are usually established with Leased Lines from a teleco. company. These Leased Lines provide a layer 1 service however do not provide a Data Link protocol, which controls the correct delivery of data over a physical link of a particular type. The 2 main ones used to encapsulate data are: HDLC & PPP. HDLC protocol has less work to do than Ethernet frames because of the simple point-to-point topology of a leased line. When sending over a Leased Line the data only has one place to go.
* **Learn the 802. Standards**
* **Ethernet as a WAN technology** – Ethernet can be used as a LAN and WAN technology and is more practical for WANs now thanks to Fiber’s long-distance capabilities, Fiber uses Ethernet data link frames. Ethernet WAN services logically behave like a point to point connection and physically behave as if a fiber ethernet link existed between two routers, This Ethernet WAN service is called EoMPLS. Leased Lines and Ethernet WAN services act similar but use different physical connection types and different data link protocols and frames to encapsulate the data.
* **IP Routing** – is used at the Network Layer and focuses on the job of routing data in the form of packets from a source to destination host using either IPv4 or IPv6 protocol. IP concerns itself with the logical details of how to deliver packets not the physical details like the lower layers, in short, the network layer thinks about the bigger picture of sending data.
* LANs are connected using routers and use the same general process of routing packets. Routers have Routing Tables, a list of know networks and lists with the associated interface. When receiving a packet, routers check the frame and if it is directed at them, they process it, discarding the frame and checking the IP packet header destination address to its own routing table, finding the network and forwarding the packet out the proper interface. But first, Router must encapsulate the data in a Layer 2 frame. If it cannot find a match on its routing table or if the host is on a different subnet, it forwards the packet to the default route or default gateway. Routing protocols share known routes with neighbor routers to their routing table. Routers need to include the MAC address when creating frames to send to the next hop, they learn each devices MAC for an associated IP by using ARP, If a device is trying to reach a host via IP and does not know a route to a certain host, they will send an ARP request that goes to every device on the LAN to find the route and populate it’s ARP table. Routers de-encapsulate packets, removing the ethernet frame and then re-encapsulates the packet, adding a new frame.
* Cisco IOS CLI command basics

**ANALYZING ETHERNET LAN SWITCHING**

* **LAN Switching Logic** – The role of a switch is to forward or filter out Layer 2 Ethernet frames on a LAN based on the destination MAC address. Switches use MAC address tables to make these decisions. MAC Address Tables or CAM tables, are created by listening to incoming frames, examining the source MAC, and noting which interface it came from. If it receives with a destination MAC it does not know, the switch Floods the frame out all interfaces in the same VLAN except the one it was received on just like a broadcast message, switches can only learn MAC addresses of devices on the same LAN or subnet. This can also cause loops sometimes, switches use STP to prevent loops by causing some interfaces to block, meaning that they do not forward frames. \*\*Review show mac address-table commands\*\*\*. These tables clear entries of inactive addresses. Each frame uses a destination MAC address of a device on the same LAN or broadcast domain. Destination MAC addresses only change in the frame if the packet travels across a router. PC’s will determine if a host is on a different subnet and send that packet with a destination MAC of the default gateway.
* Placing an IP address on an interface on a switch has nothing to do with how Ethernet frames are forwarded on the device. Certain types of switches can operate on both Layer 2 & 3.
* Configuring Basic Switch Management \*\*\*\*learn ssh commands remote management commands\*\*\* chapter 6
* Switch ports will auto negotiate speeds and duplex by default but can be manually changed. Fast ethernet = 100 mbs, Gigabit ethernet = 1000Mbs or 1Gb. Having a mismatch of speed and duplex on directly connected devices can cause issues. If the duplex is mismatched on each end of the switch it may be hard to tell because the int status will still show as up/ up but packet collisions will occur because full duplex does not use CSMA/CD. The “show interface” command will show several attributes that you can check if collisions are happening, a bad cable might affect these attributes. A switchport mode (access, trunk) mismatch could also cause a up/up result but not forward packets.
* Practice using CISCO IOS CLI
* Do online labs

**ETHERNET VLANs**

* LAN Switches create broadcast domains however configuring VLANs on switches can also break up the broadcast domains on the LAN to reduce traffic, bandwidth, and for security so that hosts are receiving unnecessary packets. A Voice VLAN is a command to use when connected VOIP phones, this type of VLAN kind of acts like a trunk but not quite, it can be used on access ports. Native VLAN is the vlan that untagged traffic will be put into once received on a trunk port. This makes it possible for your VLAN to support legacy devices that don’t tag traffic. With default configuration, all interfaces are added to the native vlan, until you specify a vlan for that port. A native VLAN mismatch on neighboring switches can cause VLAN hopping.
* **Trunking** – Trunk ports are used to allow all switches to forward frames from multiple VLANs over a single link by tagging a small header to the ethernet frame with the VLAN ID. Trunks ports by default use the ‘switchport mode dynamic auto” which does not initiate a trunk connection, use either ‘switchport mode trunk’ or ‘desirable’ modes along with auto or with each other to create a trunk link. “show int status ‘int’ switchport” or “show int trunk” command shows trunking and access info on ports.

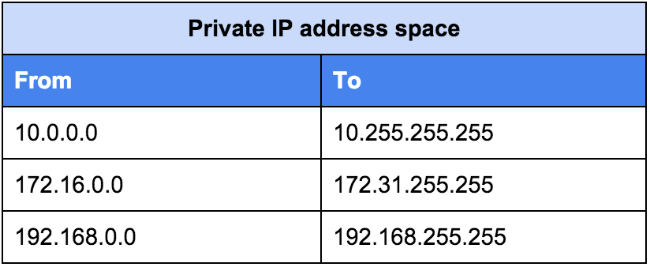
**Spanning Tree Protocol Concepts** – Redundant links in a network can cause frames to indefinitely loop and create broadcast storms that congest the network and confuse MAC tables / applications. STP/RSTP can stop these loops by either forwarding or blocking certain interfaces. STP/RSTP elects a root switch and does not block any ports on that switch. Non root switches keep directly connected links to the root switch enabled also known as their root port. Each non root switch considers one of its ports to have the least root cost between itself and the root then enables that port, this is the designated port. Ports on the non-root switches that are not root ports or designated ports get disabled. To determine the root switch each switch sends each other BPDU messages with BID information and the lowest priority device becomes the root based on speed and mac and other factors, then the other 2 switches communicate their root cost to each other to determine the DP. Endpoints become designated ports but stay enabled because pc’s will ignore BPDU messages because the do not use STP. Root cost depends on the speed of the link. Bridge mac address and priority to determine Bridge ID and elect root.

* **RSTP VS STP** – RSTP is newer and faster but both use similar convergence methods to detect network topology changes. Root Switches are constantly sending BPDU hello messages but if a switch stops receiving these messages it determines that a network change has happened and restarts the Spanning tree process of determining roots etc and flushing MAC tables. And will basically enable the redundancy link on the switch that stopped receiving messages. STP uses timers before enabling disabled ports which is a slow process. RSTP does not use timers and immediately sends BPDU messages to each switch with network updates, clearing MAC tables and enables the Alternate link. STP can use EtherChannel when there are two links between each pair of switches that logically act like 1 link. STP does not need to use convergence because the traffic can immediately fail over to the other cable/ link. This can reduce the time of convergence. Portfast can be configured on host ports to allow a for end-user device connections. Which bypasses the learning/ listening state and automatically starts forwarding traffic. BPDU guard config can be used to make sure to prevent BPDU messages for security reasons on access ports and detects devices that could cause problems on portfast enabled ports and will shut the port down if a BPDU message is received.
* **Cisco Versions of STP and RSTP** – Cisco is compatible with STP and RSTP but only use their own proprietary version of these protocols. PVST, Rapid-PVST, each acting just like STP and RSTP but these protocols only create 1 tree in the entire LAN, the cisco version of each creates 1 tree per VLAN and also can use MSTP that creates multiple trees per VLAN. These protocols use BID differently to choose priority and set roots of switches, instead they use a priority field + SID with VLAN info and then the MAC address to create a BID. You can use commands “switch priority” , “spanning-tree vlan x root primary | secondary” & “spanning-tree {vlan x} cost y” to change roots and priorities on specific vlans.
* **EtherChannel** – 2 neighboring switches can treat multiple parallel links between each other as a single logical link called etherchannel, applying all the same logic as STP to group the ports as one entity. If you were instead using STP on each link, then only one link would be enabled therefore load balancing is not an option. “channel group x mode on” command” manually adds interfaces to a channel and LACP and PAGP desirable and passive can be used to auto negotiate just like trunk modes. All ports must have the exact same setting to work though. Load balancing methods can vary such as src-mac, dst-ip etc. but the algorithms share common goals. Load balancing associates MAC addresses to Port channel int’s instead of physical ports. Cisco switches use an algorithm for LB, the algorithm examines some fields in the various headers, so messages that have the same values in those fields always flow over the same link in a particular etherchannel. It does not break frames down into smaller ones or use a round robin approach or does not examine link utilization when making the choice.

**OVERVIEW of IP SUBNETTING**

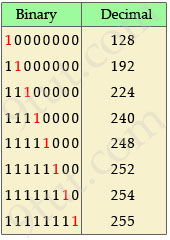
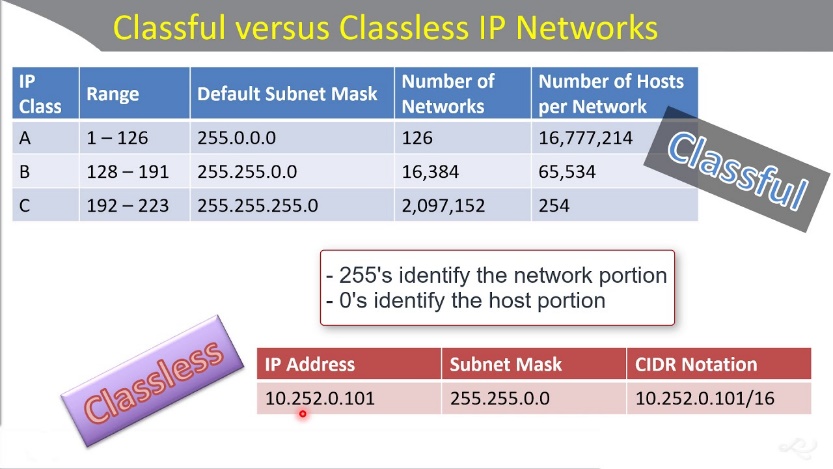
* A subnet is simply a subset of a Class A, B, or C network. Every device that connects to an IP network needs an IP address. Hosts in the same LAN should be on the same subnet. Ip addresses must be assigned according to some basic rules:
* Addresses in the same subnet are not separated by a router
* Addresses in different subnets are separated by at least one router
* WAN links connected on routers need to be in the same subnet
* One subnet for every VLAN
* A Subnet Mask defines the size of a subnet by setting aside a number of host bits whose purpose is to number different host IP addresses in that subnet. The number of hosts in a subnet can be determined by 2H and the mask defines the host bits, of course subtracting to from the total for the broadcast and network address of the subnet (first & last ip). The mask must provide enough host IP addresses to support the largest subnet. VLSM can be used in the same network to create different sizes of subnets to prevent wasting IP’s.

**NAT** – The original design of the Internet requires that companies must use registered classful public IP addresses to connect to the internet. If you want to connect to the internet then you have to have a public IP address. Some networks do not need to reach the internet and can just use private IP’s. Each public IP has to be unique therefore we have ran out of available IPv4 addresses. IPv6, Classless Interdomain Routing (CIDR), and NAT help solve this issue. With NAT, each network uses 1 unique public IP to connect to the network and then assign private IP’s inside that network that get translated when connecting with the network.



**Choosing Subnet Masks** – When creating a network, you must determine subnets by dividing a classful network into different subnets. When subnetting a classful network, you must determine how many subnets are needed and how many hosts are needed per subnet. The Class network determine how many network and host bits are on a network, then you can borrow host bits to subnet the network. The subnet bits or borrowed bits determine how many networks there can be by using 2SB with each subnet bit and hosts by 2HB . A network address is 32 bits. Each 1 in the mask is the network portion and 0’s are the host portion. Use math to determine what your networks are by designating the first IP of every network as the IP, adding the number of host and adding the broadcast address to determine the subnets.

* Work on subnetting and check if above is correct
* Hosts in the same subnet have the same subnet mask and divides the prefix value of 1’s from the host portion of 0’s
* When subnetting with classful IP’s, you can think of IP addresses having 3 parts, the network part as defined by the classes. Ex class A has 8 network bits and 24 host bits. The subnet potion which is defined by the CIDR notation is part with the classful portion in mind and the host portion. Example. A 10.5.1.1 / 24 address, classful rules state that the first octet is the network portion but CIDR states the subnet mask is 24, so the subnet portion is an additional 16 bits. So the host portion is 8 bits long. The network portion + subnet portion define the subnet mask.



Memorize these tables for subnetting

The above table is different for counting the number of networks and hosts of each network. Use 2Subnetbits and 2hostbits to find # of networks and hosts in an address. And use the above table just for subnet mask numbers.

**How to Calculate Subnets and IP’s and Hosts etc**

* First determine the Class of address as defined by the first octet then define the default network mask of that class by memorizing the above table. Look at the subnet mask and determine the number of bits just in the subnet portion by subtracting the subnet bits from that classes defined network bits. Ex. 10.0.0.0 address has 8 default network bits but if the subnet is listed as /24 then there are 16 subnet bits, these are added together to define the subnet mask. Then use use 2Subnetbits and 2hostbits – 2. to find # of networks and hosts in an address.

**Analyzing existing subnets** – Learn the magic number system to calculate the network ID, first, last, and broadcast addresses of a given IP and subnet mask. Subnet masks of 255 or 0 are ‘easy’ masks, for example a 10.0.0.1 /24 or 255.255.255.0 subnet is easy to determine this. Use the same ip for the 255 portion and 0 for the 0 portion of the subnet. However, if the subnet mask has an octet that does not end in 0 or 255, some math is involved. Use the magic number system for this. If a subnet mask of a given Ip address is 255.255.192.0 or /18 let’s say for a 10.12.95.210 ip address. Then first, determine the magic number by subtracting 256 from the 3rd octet, which is 64, 64 is the magic number. Then use multiple of 64 to find the clostest multiple to the number in the original ip which is 95 without going over 95. 64 is the closest multiple, so the Network ID in this case is 10.12.64.0 with the first available IP being 10.12.64.1. To find the broadcast ID, use the next multiple for the third octet minus 1, which is 10.12.127.255, with 10.12.127.254 being the last available IP. Add to the same interesting octet where the subnetting happens to find the network range.

Look up magic number system for the shortcut of finding id’s and broadcasts on companion website but it helps to learn the logic like above.

* Magic number is 256 – difficult mask. Use the magic number multiple that is closest to the address (not greater than) to find subnet ID and use the broadcast is the next magic multiple minus 1. Use the magic number.

**IP ROUTING AND CONFIGURING CISCO ROUTERS**

* When sending data to a destination hosts, the source host determine if the hosts IP address is within their same subnet using the ARP table. If it is in the same LAN they create a layer 2 frame using information from its MAC table to send the packet. If the destination host is not in the same LAN the source sends the frame to the default gateway with the destination MAC of that interface. The router processes the frame if it is addressed to it and re-encapsulates with the correct destination MAC and uses information in its routing table to forward the IP packet. Router interfaces must be configured with an IP address to forward IP packets. Routers must know paths to route packets unless a default route is configured which works like a default gateway and uses a /0 mask. Routers learn paths by the below tactics.
* **Types of Routes**
* **Local routes and Connected Routes** – After configuring a router interface with an IP address, the router adds that route as a connected route. in routing tables only store subnet ID’s and subnet masks for one route, usually the interface ip of how to reach that subnet. The router then learns paths to the rest of the hosts by using ARP. A local route defines a specific host on the connected route with a /32 IP.
* **Static Routes** – are manually configured by telling the router how to forward certain packets. Using the “ip route” command, then listing the destination host or network followed by the mask, then which interface or ip to forward those packets to. There must also be a known route to the next hop. Host static routes use a /32 mask. Floating static routes are used for backup links with manually set with a higher admin distance of the other link. The next hop address should be on a neighboring router.
* **Dynamic routes** – are automatically learned by neighboring routers sharing routing info with each other. If multiple routes exist to a destination, the router uses the route with the lowest administrative distance or most specific route (highest subnet mask route).
* Learn more and practice this more

**IP ROUTING IN THE LAN**

* To route IP packets in and out of subnets and VLANs, layer 3 switches or routers need to have an IP address in each subnet and have a connected route to each of those subnets. Then the IP on the router can serve as the default gateway in that subnet.
* **Router on a stick** works by having one physical trunk port that connects multiple VLANs together. However, each VLAN needs an interface connected to a VLAN, Cisco sovles this problem by creating multiple virtual router interfaces (subinterfaces), one associated with each VLAN on that trunk. Use ‘interface g 0/0.10’ for example, you also must use the encapsulation command for every interface to define a trunk and the VLANS frames that are to be forwarded and received on the interface, i.e. ‘encapsulation dot1q 10’ and then assign the subinterface an ip address. If you do not specify the native VLAN on the router then it assumes the physical interface to be using the native VLAN.
* **Layer 3 switches** are another way to route between VLANs within a LAN. Layer 3 switches use switch virtual interfaces (SVI) that are connected to each VLAN. Use ‘interface vlan *vlanID* ‘along with an ip address to configure this. Layer 2 switches cannot route traffic between different VLANs. The VLAN interface is a switches Layer 3 interface connected to the VLAN. When using SVI’s the physical ports on switches still act like layer 2 switches forwarding ethernet frames, to perform routing a frame is forwarded to one of the SVI mac addresses, then stripping the headers and making a routing decision. Routed ports can be setup though on layer 3 switches, this is useful when the L3 switch needs a L3 interface connected to a subnet and only one physical interface connects to that subnet, use ‘no switchport’ command it then acts just like a router interface. Use for a point to point link between 2 devices. Use SVI’s when you have multiple access and trunk ports all connected to a single switch. No switchport commands turns the interface into a layer 3 int.
* **Layer 3 EtherChannels** can be configured when multiple links between routed ports act as 1 link and load balance traffic using port-channel commands. Learn the commands to configure this. Show ip route – command to view a routers routing table.

-Extended ping command tests a ping from a specific interface on the router side to a destination host.

- Use ip route 0.0.0.0 0.0.0.0 *next hop address* command to configure a default route

**ROUTING PROTOCOL OSPF**

* Routers create their routing tables via connected routes, static routes, and dynamic routing protocols. Dynamic routing protocols advertise their routing information to neighboring routers and if multiple routes exist for a destination, they use the lowest metric to determine which path to take. OSPF uses bandwidth of links to determine its “cost” metric and considers the costs of the outgoing interfaces in each route to make decisions. They ignore switches when analyzing cost. RIP uses hop count. OSPF is a link state protocol and floods a LSA to every router in the network to add routes to the neighboring router and that neighbor in turn sends LSA’s to its neighbor, until all routers have an identical copy of the LSDB. The routers use an algorithm to determine which routes to add and which is the best path to a destination. Each neighbor is constantly sending hellos to each other and if a link is determined down, the router will re-calculate routes and flood LSA’s again. OSPF can use different network types and can have one router behave as a Broadcast Designated Router, and one backup DR. This can be more efficient because all router do not have to constantly send LSA’s to each other, instead the BDR can send one message designated to all other routers. Then only the BDR and DR are the routers’ neighbor, every other router is an adjacent neighbor but not fully adjascent.
* **OSPF Areas** - All routers within the same area will share LSDB’s with each other. With a lot of routers in one area, this can use require a lot of memory and CPU on the routers. Routers in the same area only share LSDB with routers in that same area, reducing overhead. These LSDB’s still have information about subnets on all other areas but does not include topology info. A backbone area is the area in which all other areas must connect. ABR’s connect to the backbone and other non-backbone areas. You can break OSPF into different areas to mitigate this, but when creating these and using ABR’s, the non-backbone area must have a path to the backbone by placing the ABR interface that connects to the backbone in the same backbone area. OSPF sends hello packets to a multi cast address of 224.0.0.5 . LSA type 1 send information that describe a router, LSA type 2 describes a network where a DR resides, each of these LSA’s describe topology info in that area.

**IMPLEMENTING OSPF**

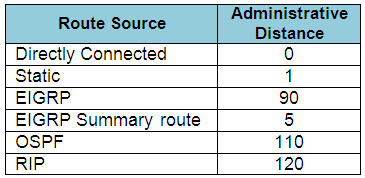
* Learn OSPF commands. Show commands and configuration commands. Show ip ospf neighbor, show ip ospf database.
* To configure OSPF, use the ‘router ospf *process-id*’ global command, that puts you in ospf config mode. Then use ‘network *ip-address wildcard-mask’* command to assign the interfaces. Wildcard masks use the 0 portion to define which octets to match and 255 to define which octets to ignore, so a wildcard mask of 0.0.255.255 defines the first 2 octets that must match then the last 2 octets can be whatever numbers and assigns all interfaces that match the first 2 octets. WC masks are used to configure ranges of ip addresses. Or you can configure ospf on each interface in interface config mode using ‘ip ospf *process-id* area *area-id*’ commands to assign interfaces to use OSPF.
* Passive-interface command can be used to stop trying to form ospf neighbors by stopping hello messages, but the router continues to advertise about the subnet that is connected to the interface.
* You can manipulate routes by manually assigning interfaces different costs, learn these commands such as ip ospf cost x. or different bandwidth commands.
* Default-information originate command advertises the default route
* Learn costs and admin costs for each bandwidth and different protocols

**OSPF NETWORK TYPES** –

* **Broadcast vs Point to Point**. With broadcast, a designated DR and BDR are selected to share LSDA’s with neighbors, every other router becomes a neighbor with each other but is a DRother, ready to become a BDR if the DR fails. You can set the priority for each ospf if not the highest router ID will be chosen, OSPF selects the highest priority as well not the lowest like switches. Broadcast works best when several routers are on an area together because just the DR is advertising not every router, reducing bandwidth. Use ip ospf network broadcast command or point-to-point command. Serial links cannot use broadcast protocols. Point-to-point ospf network types works best when there are just two routers connected on a link or point to point link. Interfaces must have the same settings to become ospf neighbors. Broadcast network type is used by default.

**IPv6**

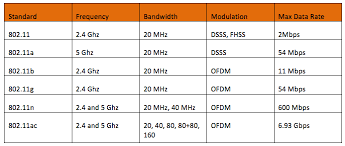
* IPv6 uses the same routing logic as IPv4. Most protocols have created an updated version to support IPv6. IPv6 uses a hexadecimal 128 bit address vs IPv4 32 bit. Use the mask divided by 4 to determine the number of hex bits is the prefix and add 0’s to the host portion (works for masks that are multiples of 4). IPv6 addresses can be abbreviated. Learn to count in hexadecimal.
* **Global unicast** – works like IPv4 public addresses where each organization is assigned one IPv6 block used for connecting to the internet and you can divide that address into subnets. Uses NAT. Usually begin with 2 or 3.
* **Unique local** – works like private IPv4 addresses. Usually begin with FD. Multicast FF and link local FE80. Attach FD: to the global unicast when assigning these addresses hosts. Routers can use EUI-64 to automatically assign unique local addresses if you specify just the prefix, it creates these addresses using devices’ MAC addresses and FFFE in between. Use ‘eui-64’ at the end of the ‘ipv6 address’ command. Learn how they do this and an EUI address based on the MAC. The 7th bit is flipped.
* **Subnetting** has the same concept as IPv4, except you are normally assigned a /32 or /48 global unicast or prefix and you subnet the rest to make a /64 mask. Using 2subnetbits as the number of subnets. The subnet ID’s for each subnet can be all possible combinations of the subnet portion to create different subnets, each combination can be a subnet.
* Learn ‘show ipv4 int brief’ and other ipv6 commands. Learn hex tables to be able to convert hex to binary. Uses the same logic, the subnet mask is what separates / defines the network and host portion.
* **Link Local** addresses are used for overhead protocols and next hop destinations and default gateways in IPv6 networks. Are automatically generated on each interface that is assigned an IPv6 address. Starts with FE80:: . learn ipv6 enable command.
* **Multicast** addresses are used for a lot of protocols and begin with FF, also anycast addresses. Routers will create a solicited-node multicast address for every unicast address on its interface. The abbreviation used to create these addresses is FF02::1:FF\_\_.\_\_\_\_ (the last 24 bits of the unicast address) . Therefore, FF02::1:FF00:1 is a solicited address.
* Learn ipv6 commands
* **IPv6 routing** works just like IPv4. The router creates a connected route for a subnet based on the unicast address of that interface and creates a local route for a specific host with /128 mask. Configuring static routes works the same way too, using ‘ipv6 route’ then listing the subnet ID and mask then specifying the next hop address or outgoing interface to send the packet. Link locals address can be used to route packets to directly connected router but must also list the outgoing interface in the same command. When using ethernet links, you must specify the next hop address, cannot use only the outgoing interface. Can use floating static route as a backup link when multiple routes are present and manually specify an admin distance. :: /0 is used to defines all traffic and is used for static routes.

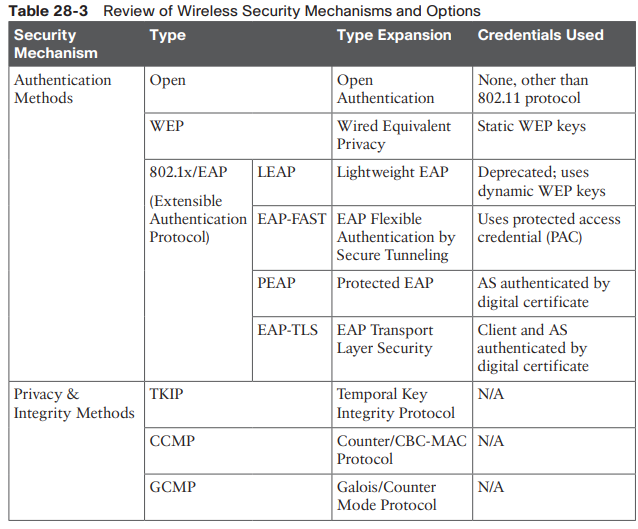
**NDP** is just like ARP for IPv4 and learns a MAC address associated to an IPv6 address. NDP has other uses as well, see below. Sends an NS message with a solicitated node multicast address and then that node replies with a NA message. RS/RA messages are used to find link local addresses.

**SLAAC** IPv6 supports an alternative method besides DHCP for hosts to choose an ip addresses. Hosts learn the IPv6 prefix using NDP RS/RA messages and then use eui-64 to assign their IP. They also use DAD to make sure that no other host is already using that same address using NA/NS messages. Uses command ‘ipv6 address autoconfig’ command.

**WIRELESS NETWORKING**

* Uses 802.11 IEEE standards, ethernet uses. Wi-Fi transmits data using radio waves, must use half duplex to avoid collisions. A wireless LAN is a BSS, every device that connects to must the AP’s settings and use the same channel and SSID. Ad Hoc wireless network is an independent BSS and allows wireless communication without authenticating to a production network. Bridges can be used to connect a wireless network to a wired network, or 2 wireless networks together. Frequency is often measured in hertz and is the number of times the signal makes one complete up and down cycle. 2.4 ghz & 5 ghz are used for wireless networks. Use non overlapping channels when using 2.4 ghz 1,6, & 11. Managing lots of AP’s can be difficult because each work independently, it is best to centrally manage AP’s using WLC controllers that centrally manage AP’s and offer a few different services. Learn AP modes and architectures.



* To control access, wireless networks can authenticate the client devices before they can associate to an AP. Data privacy can also be protected using encryption and integrity. Learn the different authentication and encryption algorithms. Authentication and encryption methods are constantly being upgraded due to hardware changes and vulnerabilities being found. WPA, WPA2, & WPA3 are standards that simplify & define which suite of algorithms are used/ compatible for a devices wireless security. 802.1x protocol defines a supplicant client, an authenticator AP, and an authentication server usually radius. Study this more.
* LAG bundles WLC’s logical ports in an AP kind of like an EtherChannel for redundancy, load balancing etc.
* WLC’s and AP’s have several interfaces that need to be configured to manage, send traffic etc. Learn how to configure WLC’s and AP’s and the logic. AP’s can only have a max. of 16 WLANs configured and 512 on WLC’s. Distribution ports forward user traffic to the wired network. A tunnel connection is used to forward traffic between the AP’s and the WLC.

**TCP/ IP TRANSPORT & APPLICATION LAYERS**

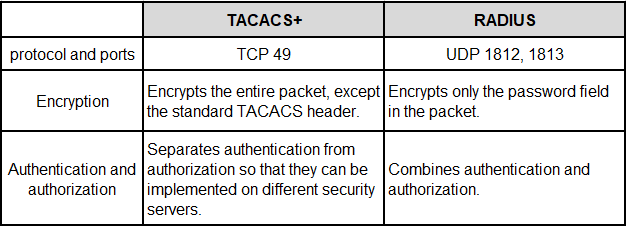
* Layer 4 of the OSI or top 2 layers of the TCP/IP model use either TCP or UDP. Each TCP/IP application chooses to use either TCP or UDP based on the application requirements. TCP requires more bandwidth and overhead processing to deliver error recovery, flow control, and connection based syn, syn ack, ack; before the server starts sending data. Therefore, it takes more time. UDP is faster and requires less overhead for time sensitive apps like video conferencing or voice.
* **Multiplexing** used by both TCP and UDP which use port numbers to keep track of different sessions and which app to send the segment. Relies on sockets, 3 main parts of socket are ip address, transport protocol (tcp or udp) and port number.
* **TCP** uses a 3-way handshake to establish a tcp connection. It also uses windowing and sequence numbers for flow control and to recover packets with lost sequence numbers. Ack messages have sequence numbers in the messages.
* **UDP** is used for time sensitive apps such as streaming when error recovery is not needed or required. Such as DNS. UDP is connectionless meaning no handshake.

**Access Control Lists**

* Access Control lists act as a packet filter to block traffic on interfaces. To filter a packet, you must enable an ACL on an interface that processes the packet, in the same direction the packet flows through the interface. ACL can also be used to match packets for applying QoS features. ACL’s use first-match logic. Once a packet matches one line in the ACL, the router takes the action listed in that line of the ACL and stops looking further in the ACL. ACL’s have an implicit deny all, but it is not listed in the config, you can also configure ACL’s to use the permit any command. There are different types of ACL’s. Learn how to configure wildcard masks to match a particular subnet by subtracting the subnet masks from 255.255.255.255, using the result as the WC mask. And learn how to calculate the range of addresses that are configured, the range begins with the ip address defined and end with the sum of the ip address defined plus the wildcard mask in the command. ACL’s can be configured to filter inbound or outbound traffic on interfaces. Place standards’ on the closest destination router and Extended’s closest to the source. Access-lists can use sequence numbers to edit and manipulate the lists. You can configure ACL’s from a single line command in global config or use the ip access-list {standard or extended} *name* command to enter ACL config to use sequence numbers and config the list. You the keyword *host* in commands when specify a specific host ip.
* **Standard ACL** – An access-list that is developed solely using the source IP address. These access control lists allow or block the entire protocol suite. They do not differentiate between IP traffic such as UDP, TCP, and HTTPS. They use access-group numbers 1-99 or 1300-1999 so the router can recognize the address as the source IP address. Standard ACL’s use the following global command: access-list {1-99 or 1300 - 1999} {permit or deny} *matching parameters*. Use the command: ip access-group *number* {in or out} on an interface to enable it. Use the global command to define the access-list.
* **Extended ACL** – An access-list that is widely used as it can differentiate IP traffic. It uses both source and destination IP addresses and port numbers to make sense of IP traffic. All 3 of these parameters must match. You can also specify which IP traffic should be allowed or denied. They use the numbers 100-199 and 2000-2699. Standard ACL’s can only match packets using source ip addresses not the destination while extended lists match a variety of packet header fields to match / filter traffic Commands that include either the tcp or udp keyword can optionally reference application port numbers. Ex: access-list 110 permit tcp 92.128.2.0 0.0.0.255 eq 80 any. Define the operator and port before the destination address to stop inbound traffic and conversely, define these parameters after the source address to stop inbound traffic from going to the source’s port.

**SECURITY ARCHITECTURES**

* Learn different attacks. Exploits, vulnerabilities, and threats etc.



**Firewalls** protect the network from different kinds of issues by deciding which packets should be forwarded or filtered. Firewalls do the same kinds of work that routers do with ACL’s, but firewalls can perform that packet-filtering with many more options. Stateful firewalls keep track of sessions to detect unusual activity.

**IPS** filters traffic based on a database of known exploits.

**DHCP, DNS** DHCP snooping to filter DHCP traffic and ARP inspection to filter arp messages to secure attacks. Using trusted and untrusted ports on interfaces to filter traffic interfaces are untrusted by default. Enable these security commands on untrusted ports. DCHP snooping feature builds a binding table with a hosts ip address and its related mac address and ARP inspection checks for a match of incoming arp messages to prevent attacks. Routers work at layer 3 and do not have the dhcp snooping feature.

**Logging and NTP** CDP **and LLDP** – Understand their purpose and how to configure / troubleshoot these features.

**NAT CIDR PRIVATE IP’S PAT** learn more about how to configure this.

**QoS** prioritizes packets to give some traffic better service than others, QoS tools focus on managing bandwidth, delay, jitter, and loss. Some applications require better service than others such as voice and video. Routers classify and mark packets for other QoS tools to use. If a network device needs to send packets but does not have enough bandwidth, the device que’s up the packets waiting and prioritizes traffic based on its classification. Policing can be used to used discard or remark traffic from que’s that are hogging too much bandwidth. The shaping feature can que traffic before it is sent to a policer to avoid getting discarded, Shaping can be used to match a CIR, Committed information rate.

**Miscellaneous IP Services**

* **HSRP** – when two are more routers connect to the same LAN subnet you can configure redundant links to the WAN. HSRP can be configured to provide redundancy of the hosts’ default routes. The redundant routers share a virtual ip and mac address that the hosts send traffic too. Can be used for load balancing.
* **SNMP** - is a protocol for collecting and modifying information on a network device. Consists of agents and managers and use a few different types of SNMP messages such as get and set messages. SNMP exposes management data in the form of variables on the managed systems organized in a MIB, which describe the status and config of the system.
* **FTP, FTPS, TFTP** – are used for transferring files over the network. FTP and FTPS use TCP port 20 or 21 and FTPS encrypts data and password while TFTP is least secure using UDP port 69. Can be used to update Cisco IOS images by copying and loading new images to flash memory.

**WAN ARCHITECTURE**

* A customer might need to use a private WAN service provider to connect different sites that are not geographically close to each other to your enterprise network. Learn WAN topologies and technologies. The combination of ISP networks and customer networks create the world wide web.
* **Metro Ethernet** SP WAN acts as a Layer 2 switch and devices connected through the WAN function logically as a point to point ethernet connection. Use E-LINE, E-LAN, and E-TREE.
* **MPLS** Is a WAN Layer 3 routing protocol that routes packets between customer sites. The SP creates an IP network that spans over a large geographical network that connects to the customer edge routers. MPLS supports all data link protocols. Since many different customers on the SP network will most likely be using a lot of the same private addresses, MPLS uses tags between the frame and header to organize different customers traffic and make routing decisions, this creates a MPLS VPN for each customer. CE and PE routers exchange information between the different IGPs and EGPs running on the routers, route redistribution is used to convert routes from one protocol to another on the PE.
* **VPNs** compared to a private WANs the internet or public WAN does not provide for a secure environment that protects the privacy of an enterprise’s data. Internet VPNs can provide important security features such as: Confidentiality, Authentication, Data integrity, and Anti-replay. To accomplish this, 2 devices near the edge of the internet create a tunnel. IPsec defines how two devices both of which connect to the internet can establish a VPN connection, IPsec encryption uses a shared key to encrypt data. While IPsec works well for site-to-site VPNs sometimes you may not always be somewhere that provides a permanent site-to-site VPN. VPNs with TLS work well for remote access VPN’s. an example of this is HTTPS web browser secure connection. TLS requires each device to create their own VPN tunnel instead of IPsec sharing one tunnel for all devices.

**CLOUD ARCHITECTURE**

* VM’s, the cloud definition, hypervisor. Private & public cloud.

**CONTROLLER-BASED NETWORKING**

* Software defined networks are a way to re-image your network vs traditional networks for simplicity, scalability, and easier management.
* The most notable difference between SDN and traditional networking is that SDN is software-based while traditional networking is usually hardware-based. Because it’s software-based, SDN is more flexible, allowing users greater control and ease for managing resources virtually throughout the control plane. Inversely, traditional networks use switches, routers and other physical infrastructure to create connections and run the network.
* SDN controllers feature a northbound interface that communicates with APIs. Because of this communication, application developers can directly program the network, as opposed to using the protocols required by traditional networking.
* API – software that allows applications to communicate over a network.
* Data Plane, Control Plane, Management Plane.
* ASIC is a special purpose chip for processing the data plane.
* Controllers do much of the work needed for the control plane in a centralized control model. It gathers all sorts of useful information about the network and create a centralized repository. Controllers use API’s at the northbound (host end) and the southbound (network devices) interfaces.
* SDN models, ACI use APIC controllers for network programmability or control plane centralization.
* SDN is used as a WAN technology here but SDA defines how the access devices get involved.

**SOFTWARE DEFINES ACCESS**

* Used on controllers to configure the network devices.
* Underlay- network devices, Overlay – forwarding logic, tunnels.
* SDA uses a router access layer design which causes all switches to act as layer 3 switches that use IS-IS routing protocol for this.
* SDA uses VXLAN to create tunnels used by SDA. The underlay needs to use its own subnet on fabric edge routers.
* SDA’s use a LISP map server to dynamically learn paths to host instead of the traditional method. Each device uses the LISP central map server to learn destinations. Each access switch or device that connects to the endpoints become that endpoints default gateway.
* DNA center vs traditional management. Uses ISE to scale ACL’s using logical groups (STGs) instead of regular ACL logic to reduce difficulty when ACLs are to large.

**REST APIs & JSON**

* Applications use APIs to communicate on different computers. To do so, one program can learn the variables and data structures used by another program, making logic choices based on those values, changing values of those variables, created new ones, or deleting variables.
* CRUD, http verbs, data encoding. Create, Read, Update, Delete.
* Data serialization is the representation of data by the server API, so the REST client can read them, there are lots of serialization programming languages such as JSON.

1. Server gives internal data to API
2. API converts internal data to data model
3. Server sends data model in JSON
4. REST client converts JSON formatted data into its native format

* Learn Ansible, Puppet, and Chef configuration management tools.

**EXTRAS**

* TCP 3 WAY HANDSHAKE – SYN → SYNC, ACK → ACK and then the data is sent. Sync and acknowledgement messages use sequence numbers to keep track of data .
* Diagram

  Description automatically generated