**ITProTV - CCNA**

***IPv4 Addressing (1.6) –***192.168.1 .10

**^Network ID^ ^Host ID^**

**(House Number) (Street Name)**

**Class A =** 1.0.0.1 – 127.255.255.254

Default Subnet: 255.0.0.0

Number of Networks: 127

Number of Hosts Per Network: 16,777,214

Binary: 00000001

**Class B =** 128.0.0.1 – 191.255.255.254

Default Subnet: 255.255.0.0

Number of Networks: 65,636

Number of Hosts Per Network: 65,535

Binary: 10000000

**Class C =** 192.0.0.1 – 255.255.255.254

Default Subnet: 255.255.255.0

Number of Networks: 16,777,216

Number of Hosts Per Network: 254

Binary: 11000000

**Class D =** 224.0.0.1 – 255.255.255.254

Binary: 11100000

The Broadcast Address will always be one higher than the last possible Host ID.

-----------------

***IPv6 (1.9) –***Hexadecimal format (0-9) (A-F = 10-15). Made up of eight 16-bit sections.

Truncate/Truncation: Can truncate (shorten) an IPv6 address by removing leading and continuous zeroes and only keeping the separating colons.

**IPv6 Unicast Addresses –** Meant for IPv6 traffic which only pertains to one sender and one receiver.

Examples:

Unspecified = ::/128 OR :: (Default Routing)

Loopback = ::1/128 (Testing)

**Unique-Local Unicasts =** FC00:: (Like IPv4 Private Address)

**Global Unicasts =** 2000 – 3FFF (Internet Routable)

**Link-Local Unicasts =** FE80::/10 (Neighbor Discovery and Routing Protocols)

**Anycast =** Allows a single router to send out messages to all other connected routers simultaneously. Will never be source addresses, only destination. Doesn’t have a default format, can take on any format it needs to.

**Multicast =** Format is ‘FF00::/12’ Used to send a message to a specified group of devices.

**Modified EUI 64 =** A Unicast type address. Used to ensure uniqueness between addresses. First half of address is network ID, and second half is host ID (like a MAC address).

***Configuring IPv6 –***1) **(config)#***ipv6 unicast-routing* 2) Enter into interface configuration mode and enter: *ipv6 address* “*2001:AC:C8:10::1/64*” 3) Check ipv6 configuration by entering enable mode and enter: *show ipv6 int brief*

--------------------------------------

***Switching Concepts (1.13) –*** Functionality of a switch are three main things: Forwarding, Flooding, and Filtering

**Frame Forwarding =** When a switch refers to its MAC table and distributes frames depending on the known ports/MAC addresses that it has.

**Frame Flooding =** One scenario is if a machine wants to communicate with all other connected machines, it can send a broadcast to achieve this. (Broadcast MAC Address: FFFF.FFFF.FFFF)

Filtering = When a switch detects the same source/destination MAC addresses are designated for the same port, it will simply filter out the frame (essentially cancel it).

Application Specific Integrated Circuit (ASIC): Built into the ports of a switch to properly handle forwarding, filtering, and flooding without having to rely on the switch’s CPU. (provides the high-speed functionality of switches)

----------------------------------

***VLANs (2.1) -*** Can group ports on a switch and assign them to specified VLANs (Marketing, Finance, IT, etc.) VLANs are a Layer 2 technology, subnets are Layer 3. A VLAN can be associated with a specified subnet.

**Access Ports (Voice & Data) –** Data traffic coming from the same port on a switch can be separated by type (Voice & Data). EX: An IP phone can be connected to a PC and both share the same link connecting to the switch. A single port can handle both Voice and Data VLANs, but the same port can’t be part of two different VLANs.

*Configuring VLANs –* **(config)#**vlan 50 **(config)#**name Voice **(config)#**exit **(config)#**vlan 60 **(config)#**name Data **(config)#**exit [specify interface to assign] **(config)#**switchport mode access **(config)#**switchport access vlan 60 **(config)#**switchport voice vlan 50 **(config)#**exit **(config)#**show vlan brief

**Default VLANs =**By default all ports on a switch have access to this vlan (vlan 1). Best configuration practices are to remove all unused ports from this vlan and place them in a separate vlan.

*EX:* **(config)#**vlan 999 **(config)#**name Example **(config)#**exit **(config)#**interface range fa 1/0/1 – 9 **(config)#**switchport mode access **(config)#**switchport access vlan 999 **(config)#**shutdown

**InterVLAN Connectivity =**

-------------------------------------------

***Interswitch Connectivity (2.2) –*** If a VLAN spanned across multiple switches, a link that connected each VLAN across switches would be required for them to communicate. This can be troublesome when dealing with large scales and continuing growth.

**Trunk Ports –**Ports that provide VLAN connectivity between switches, allowing them to communicate over a single link as opposed to requiring a link for each individually separated VLAN.

**802.1Q =**A standard protocol for interconnecting multiple switches & routers and for defining VLAN topologies. A trunking encapsulation method that provides VLAN tags.

**Native VLAN =**A special VLAN whose traffic traverses on the 802.1Q trunk without any VLAN tag. The default Native VLAN ID is always the same and well-known, best practice is to change this. The Native VLAN ID must be the same on all connected switches or an error will occur.

------------------------------------------

***Spanning Tree Protocol*** ***(2.5) –*** Predominantly used to prevent Layer 2 loops (never-ending loop of a frame being sent through a network) and is also used for network redundancy.

BPDU (Bridge Protocol Data Unit) = Used by each connected switch to determine which will be the “king“ of the network. BPDUs contain: Priority ID #, Cost, MAC Address, and a Root/Bridge ID.

**Root Port =** A Port Role which is in a Forwarding state. This port is decided by the lowest costing interface, or the lowest port ID that’s connected to the Root Bridge. Every other port that’s not a Root Port is considered a non-designated port (NDP) and takes a Blocking state.

**Root Bridge (Primary/Secondary) =**“King of the Network” The Root Bridge is the switch with the lowest priority ID or lowest MAC address (if devices have same priority ID). The priority ID of a switch can be changed, you can manually configure whichever device you wish to be the Root Bridge (usually want this to be a centrally located switch not one at the edge of a network).

**Port States (forwarding/blocking) =** States that a port can take, either forwarding/blocking any incoming traffic.

**PortFast =**Can be enabled on a link that connects to a non-switch device (Server, PC) which won’t participate in a Root Bridge Election, meaning those devices won’t send out BPDUs. Enabling PortFast ensures that a switch knows not to expect/receive BPDUs on a particular port, increasing the overall efficiency of all connected switches.

-----------------------------------------------

***Layer 2 Discovery Protocols (2.3) –*** Protocols used to discover where devices in a network are physically located. CDP (Cisco Discovery Protocol) is Cisco proprietary while LLDP (Link Layer Discovery Protocol) is vendor-neutral and more commonly used today.

----------------------------=

***EtherChannel (2.4) –*** Technology used between switches to aggregate multiple links together, making the combined bandwidth available to use and provides fault tolerance if one existing link was to fail. Limited to 8 possible links.

**LACP (Link Aggregation Control Protocol) =** A protocol that supports the exchange of link aggregation information between 2 switches, a switch will dynamically configure port states based on the configurations of the other switch. Can be configured as Layer 2/3 protocol.

-----------------------------------------------

***Cisco Wireless Architecture (2.6) –*** Autonomous AP Architecture – All configuration/management happens directly on the APs. Con is that individual APs can become overwhelmed.

**AP Modes –** Local (Clients), Monitor, FlexConnect (Clients), Sniffer, Rogue Detector (Clients), Bridge/Mesh, Flex Plus Bridge (Clients), SE-Connect

Cloud-Based AP Architecture = Devices are configured with IPs, etc. and then can reach out to the internet and be discovered by an ISP’s cloud. Replaces a physical WLC with ISP’s web portal that handles discovery of APs, licensing, and all management of devices.

Lightweight AP Architecture (LWAPP) = Older architecture that handles direct communication between a WLC and AP.

Split-MAC Architecture (CAPWAP) = Newer architecture that’s similar to LWAPP but uses 2 tunnels: one for control and one for data.

***AP, WLC, Access/Trunk Ports, and LAG (2.7) –***

**WLC =** A Wireless LAN Controller, allows for central management of all connected wireless access points. Usually paired with specialized access points called Lightweight Access Points – these must first be connected to a WLC and configured from there. VLANs can also be connected to and centrally managed by a WLC.

**Access/Trunk Ports =** Ports can be configured as Access ports if only one VLAN’s traffic is traveling across that link. Trunk ports can be configured for AP links that handle multiple VLANs’ traffic.

**Link Aggregation (LAG) =** Allows for configuration of redundancy between WLC and connected Aps as well as load balancing across the WLC>>APs>>Switch.

------------------------------------------------

***Wireless Security Protocols (5.9) –*** WEP (Wired Equivalent Privacy) = 64, 128, and 256-bit static key (Key is easy to discover since its static)

**WPA (Wi-Fi Protected Access) =** Replaces weak protocol and secures wireless per packet instead of using a single static key (Patterns in each packet are easily discoverable/recognized the more they’re watched)

**WPA2 =** AES + CCMP for encryption and authentication

**WPA3 =** Uses Opportunistic Wireless Encryption for open security networks-i.e., Hotspots, Public Wi-Fi, etc. (Uses OWE to securely connect to open networks)

WPA 2 should be the minimum standard for wireless security and the starting point when configuring an AP. If WPA3 is supported, you can configure that instead or if WPA2 isn’t supported, you can move down the protocol list (WPA>>WEP).

---------------------------------------------

***Layer 2 Security Features (5.7) –* DHCP Snooping =** Security technology that monitors for DHCP traffic coming from untrusted ports and drops it

**DAI (Dynamic ARP Inspection) =** Inspects ARP packets on the LAN and uses the info from the DHCP snooping table on the switch to validate ARP packets. IF ARP traffic is received from an unknown source, it is dropped.

**Port Security =** Allows a limited amount of MAC addresses to connect per port. Removing the possibility of a threat actor simply plugging in a rogue device and accessing the network.

----------------------------------------------------------------

***Routers and Layer 2/3 Switches (1.1a + 1.1b) –* Layer 3 Switch (Multilayer) =** Switch that’s added the components of routing into it. Limitations are lack of flexibility, cost, not as efficient as routers when placed at the edge of a network.

------------------------------

***Routing Table (3.1) –*** ‘#show ip route’ = Pulls up the routing table.

**Administrative Distance =** A measure of the trustworthiness of the source of the routing information. The smaller the administrative distance value, the more reliable the protocol.

|  |  |
| --- | --- |
| Connected Interface | 0 |
| Static Route | 1 |
| EIGRP Summary Route | 5 |
| External Border Gateway Protocol (BGP) | 20 |
| Internal EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| RIP | 120 |

**Metric =** If a router learns 2 different paths for the same network from the same routing protocol, it must decide which route is better and will be placed in the routing table. Metric is the measure used to decide which route is better (a lower number is better). Each routing protocol uses its own metric.

**Gateway of Last Resort =** Default route, if a router receives a packet/traffic whose designation is not in the routing table then it should be able to forward it to this particular interface (as long as its set).

-------------------------------------------------

***Router Forwarding Decision (3.2) –* Longest Prefix Match =** Network with the “longest” subnet on a routing table. EX: /29 > /25

If the Prefix Match, Admin Distance, and Metric are all the same for possible destination routes, then a router will equal cost load balance across all those paths.

-----------------------------------------

***Static Routing for IPv4 (3.3) –* Network Route =** The process of selecting a specified path across one or more networks.

**Default Route =** Route that is taken if a routing path isn’t specified in a routing table ‘Gateway of Last Resort’

**Host Route =** A specified route to only one designated IP.

**Floating Static =** Backup route in case a dynamic routing protocol fails, doesn’t actually appear in routing table.

***Static Routing for IPv6 –*** Best practice to always start with ‘**(config)#**ipv6 unicast-routing’ whenever beginning the process of configuring IPv6 addresses.

-------------------------------------

***Single Area OSPFv2 (Open Shortest Path First)(3.4) –*** OSPF is a Link State Protocol (all routers under this protocol will have the same routing table between them). Uses the SPF (shortest path first) algorithm. The Administrative Distance of OSPF is 110. Multicast of 224.0.0.5. All routers under this protocol need to become “neighbors” before they communicate (exchange and agree on information to do this). Routers will send a “hello” message to each other through the multicast to begin the neighbor process.

Wild Card Bits = When selecting networks to configure under OSPF, will be asked to supply the wild card bits of a network. This is essentially the inverse of the network’s subnet mask. EX: /24 = 255.255.255.0 so Wild Card Bits would be 0.0.0.255

Information that OSPF routers must agree on to become neighbors:

* Same subnet/subnet mask
* Same “Hello” Interval—“Keep Alives” (10 sec by default but can be changed)
* Dead Interval (4x Hello Interval)
* Same Area ID (Default Area ID is 0)
* Authentication (Sometimes used/sometimes not)

Once neighbor relationship is established each OSPFv2 Router will build 3 tables:

* Neighbor Table: List of direct OSPF Neighbors
* Topology Table (Link State Database/LSDB): List of subnets, routers, and links
* Routing Table: Router runs Dijkstra against LSDB for best route to each subnet based on “cost”

**Neighbor Adjacencies =** A relationship formed between a router and the designated or backup designated router. For point-to-point networks, no designated or backup designated router is elected. An adjacency must be formed with the neighbor.

**Point-to-point =** A serial link that connects two routers, making them OSPF neighbors.

**Broadcast (DR/BDR selection) =** DR: Designated Router, BDR: Backup Designated Router. Router with the highest Priority ID will become a DR. By default, all routers have a priority of 1. if there is a tie, the router with the highest Router ID wins the election. The router with the second highest Priority ID or Router ID will become a BDR.

**Router ID =** Whichever interface is the highest IP address when OSPF becomes active, that by default becomes the Router ID (ID can also be manually set instead of being the highest IP). EX: 192.168.16.1 > 172.14.0.1, 10.0.12.1 / 192.168.16.1 would be the Router ID

---------------------------------------------------------------

***First Hop Redundancy Protocols (FHRP) (3.5) –*** Prevent a single point of failure. More relevant for small/medium networks with only a single/few APs.

Hot Standby Router Protocol (HSRP) = Cisco Proprietary, requires a group number (should be the same on all connected devices). Main router is the only active one, backup is dormant until its needed. Designed to allow for failover at the first-hop IP router. Determines the active router based on priority number. ‘**#show standby’** to check the protocol configuration.

Virtual Router Redundancy Protocol (VRRP) = Also requires all connected devices to have the same group number. Uses both priority and IP address. ‘**#show vrrp’** to check the protocol configuration.

Gateway Load Balancing Protocol (GLBP) = Cisco proprietary protocol that attempts to overcome the limitations of existing redundant router protocols by adding basic load balancing functionality, protects data traffic from a failed router or circuit. In addition to being able to set priorities on different gateway routers, GLBP allows a weighting parameter to be set. ‘**#show glbp’** to check the protocol configuration.

***Access Control Lists (ACLs) (5.6) –*** Standard ACL (1-99) = Primarily uses source IPs of packets to determine whether to allow/deny access through a router. Implicit deny at end of every ACL (any traffic from a listed ‘deny’ network will be denied, must configure a permit to allow certain hosts if desired and the permit statement should be configured first). Must be applied to interface with direction (inbound/outbound).

Extended ACL (100-199, 2000-2699) = Allows for more granularity in what’s allowed/denied through a router. Defines source/destination of traffic and protocol/port to permit/deny. Implicit deny at end of every ACL. Should be placed as close to the source as possible.

Named ACL = Standard or Extended. Permit/Deny. Implicit deny at end of every ACL. Has to be applied to an interface in a specified direction as well.

-----------------------------------

***Inside Source NAT (4.1) –* Static NAT (1-1) =** One private IP to one public IP. EX: A hosted gaming server that is represented by a private IP inside its network, and is directly connected/associated by a public IP to which others can connect to.

**Pool NAT (Dynamic NAT) (Many-Many) =** Has a range of multiple public IP’s that are associated with a range of internal devices and their respective private IPs. Each public IP can only be occupied by a single device at a time. EX: A network contains 4 devices but is only configured with 3 public IPs, the remaining device would have to wait for a public IP to stop being used by the other devices in order to establish a connection outside the network.

Port Address Translation (PAT) – One public IP that multiple private IPs can translate through and connect to the internet (via specified ports).

Regardless of which NAT type is used, the specified router will need to be assigned with an inside and outside interface/IP. EX: **(config-if)#**ip nat inside (on private side interface) & **(config-if)#**ip nat outside (on public interface) / To verify/show NAT configuration: **#**show ip nat translation

--------------------------------------------------

***Network Time Protocol (NTP) (4.2) –*** Protocol to ensure accurate time synchronization of multiple devices by connecting them to a single time device (server) which controls and implements the correct time to all.

----------------------------

***DHCP & DNS (4.3) –*** Each DNS record has to be manually entered on Cisco routers/switches, if the router/switch is acting as a DNS server.

-------------------------------------------------------------------------

***Simple Network Management Protocol (SNMP) (4.4) –*** Protocol (Versions 1, 2c,3) used to gather hardware information about devices connected on a network. An SNMP server manager is required to gather and access this information. The SNMP manager issues a ping over the broadcast address (uses port 161) to discover all network devices. Each network device is known as an agent when it is connected to the manager and ready to be configured.

***Syslog (4.5) –*** **Facilities =** Also known as Severity, the number by which types of logs are ranked/categorized (0-7).

**Levels =** Name of each log type/category. Emergencies, Alerts, Critical, Error, Warnings, Notification, Information, Debugging

---------------------------------------------------------

***Forwarding Per-Hop Behavior (PHB) (4.7) –* Classification/Marking =** Classifying of network traffic by characteristics and marking of “checkpoints” that ensure proper flow of traffic by data type.

**Queuing =** Directs traffic by designations of each data type/classification. Queuing Types=Real-time traffic (Expedited Forward PHB), Guaranteed bandwidth queue (Assured Forwarding PHB), Default & best effort queue (Default Forwarding PHB), Less than best effort queue (Lower Effort Per-hop Behavior).

CB-WFQ (Class Based Weighted Fair Queuing) = Puts traffic into classifications that can ensures it can use all the bandwidth defined in configuration.

LLQ (Low Latency Queuing) = Instead of setting bandwidth for traffic flow, it sets a priority for the traffic at all times, not just when congested.

**Congestion =** Congestion Avoidance can be used to drop certain packets when a pre-defined limit of bandwidth is set.

WRED (Weighted Random Early Detection) = Only used for some types of queues (not strict-priority, scavenger, and control traffic queues) such as default queues.

**Policing/Shaping =** Policing, unwanted excess traffic is dropped as soon as possible. Shaping, unwanted excess traffic is buffered rather than dropped.

---------------------------------------------

***Configure Remote Access (4.8) –***

-------------------------

***TFTP/FTP (4.9) – T***FTP has speed and ease of set up advantage but doesn’t have any capabilities for checking file corruption while FTP does. FTP requires username and password.

-----------------------------------

***Security Concepts (5.1) –* Threats =** Non-Updated Software, Non-Hardened Server and Simple Passwords

**Vulnerability =** Default Configuration/Passwords, Unsecured Doors, No Antimalware

**Exploit =** Viruses, Malware, Social Engineering

**Mitigation Techniques =** Updating Software, Classification, Server Hardening, Requiring Complex Passwords

***Security Program Elements (5.2) –* User Awareness/Training =** Bringing to the forefront basic security concepts and best practices to meet minimum requirements that satisfy those concepts.

**Physical Access Control =** Locks, Biometrics, Multi-Factor Authentication (Badge + Key)

--------------------------------------------------------------------

***Password Policies Elements & Alternatives (5.4) –* Management =** Passwords can be enabled for multiple CLI modes (User, Privileged, etc.) and access types (SSH, Telnet, etc.). All passwords can be hashed/salted and ensured not to stored in plain text.

**Complexity =** Max password length requirement can be set up to 16, all other password complexity best practices should also be Implemented (special characters, lower/upper case letters, etc.).

**MFA/Certificates/Biometrics =** Digital certificates can be generated and implemented in lieu of passwords.

--------------------------------------------------------------------------

***Authentication, Authorization, and Accounting (5.8) –***  Authentication = Username/Password to validate access.

Authorization = Allowing access to users via specified methods (SSH, Telnet, etc.)

Accounting = Logging of all access validation/attempts.

AAA also provided a separated authenitcatin database that wasn’t simply sotred on a router/switch.

***Device Access Control w/ Local Passwords (5.3) -***

--------------------------------------------

***IPsec & Site-to-Site VPNs (5.5) –*** S2S is a router-to-router encrypted tunnel that remains up as long as traffic is being sent through, doesn’t require a dedicated connection for each individual client (user). Remote Access VPN requires a dedicated connection for each client that needs to access resources remotely, can be cumbersome when many clients require access.

-----------------------------------------------------------

***Automating Network Management (6.1) –*** Scripts can be implemented to routinely handle tasks, save on costs, minimize errors, etc.

***Controller-Based Networking (6.2) -*** Traditional Networking=One Device at a time VS Controller-Based Networking=Configure once, push out to all devices.

---------------------------------------------------------------------------------------

***Controller Based/Software Defined Networks (SDN) (6.3 a/b) –*** Routers/Switches have 3 different operational planes that handle data in certain ways between each of them.

Management Plane = Allows for connection to a device in which they can be programmed/configured.

Control Plane = Handles control traffic such as the routing protocols used to manage incoming data.

Data Plane = Simply the data coming into a device and the attempt to find the path needed to take data out of the device as well.

**Separation of Control/Data Plane –** Control Plane can be moved to a separate device (server/controller) to still configure routers/switches while isolating this plane from the data/management plane.

**Overlay/Underlay =** Underlay is the infrastructure itself. Overlay is the logical network that uses virtualization to build connectivity on top of physical infrastructure using tunneling encapsulations such as VXLAN, IPSec, etc.

**Fabric =** The network topology itself that is built.

**Northbound/Southbound APIs –** Northbound is the interface between the controller and the application (laptop/desktop being used to connect) in a network. Southbound is the interface between the controller and the devices in a network.

------------------------------------------------------------------------------------------------------------

***Campus Device Management VS Cisco DNA Center Device Management (6.4) –*** Traditional device management = SSH (remote access), RDP (Remote Desktop), Console (direct connection to device), Network Monitoring (Visibility)

Cisco DNA Center = Provides all the utilities of traditional remote management types under one umbrella, allowing device management across multiple networks without the need to switch between different interfaces.

----------------------------------

***REST-based APIs (6.5) –*** Allows you to interact with any kind of server over HTTP.

**CRUD (Create Read Update Delete) -** POST = Create: creates new object or resource / GET = Read: retrieves resources / PUT (PATCH)= Update: modifies Large(small) / DELETE = Delete: removes a resource

**HTTP verbs =** A set of request methods to indicate the desired action to be performed for a given resource.

**Data Encoding (Headers) =** The wrapper around the body of an HTTP request/response used to compress the media type. It informs the server which encoding the user will support.

-------------------------------------------------------------------

***Configuration Management Mechanisms (6.6) –*** Helps to control and enforce consistency of multiple systems by using automation instead of manual configuration to provide consistency over a wide scale. Ensuring a proper upkeep of "Desired State" across all devices (Software and version installed, System attributes, Specific configuration).

Idempotent Behavior = Checks to see if state is ok before it needs to be run

|  |  |  |  |
| --- | --- | --- | --- |
|  | Chef | Puppet | Ansible |
| Language | Ruby | Ruby | Python/YAML |
| Configuration Management | Pull | Pull | Push + Pull |
| Architecture | Master-Agent | Master-Agent | Agentless |
| Script Names | Recipe/Cookbooks | Manifest/Modules | Playbooks/Roles |

--------------------------------------------------

***Interpret JSON (JavaScript Object Notation) Encoded Data (6.7) -*** Subset of JavaScript Programming Language used for transferring data between server and client. First format that allowed servers and browsers to communicate without a browser plug-in like Flash or Java.

Value Pair = EX: {“firstName”:”Alan”,

“lastName”:”Tellez”}

JSON Object Rules = Objects use **{}** / Value Pairs use **:** / Between Value Pairs use **,** / Values **“ ”**

JSON Array Rules = Arrays use **[ ]** / Objects use **,** / Value pairs use **:** / Values **“ ”**