***The Complete Networking Fundamentals Course – David Bombal***

***Section 4 – TCP/IP Model:***

|  |
| --- |
| 5-7 = Application |
| 4 = Transport |
| 3 = Network |
| 2 = Data Link |
| 1 = Physical |

**OSI** **TCP/IP**

|  |
| --- |
| 7 = Application |
| 6 = Presentation |
| 5 = Session |
| 4 = Transport |
| 3 = Network |
| 2 = Data Link |
| 1 = Physical |

***Section 6 – Hexadecimal:***

Number Systems:

* **Decimal** (Base 10 – Ten numbers)

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

* **Binary** (Base 2 – Two Numbers)

0 or 1

* **Hexadecimal** (Base 16 – Sixteen numbers)

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

|  |  |  |
| --- | --- | --- |
| **Decimal** | **Binary** | **Hexadecimal** |
| 128 | 1000 0000 | 80 |
| 255 | 1111 1111 | FF |
| 224 | 1110 0000 | E0 |
| 240 | 1111 0000 | F0 |

***Section 7 – IP Addressing:***

**IPv4 –** Layer 3 protocol that is connectionless, each packet is treated independently, and each may take different paths depending on Load Balancing, Bandwidth (OSPF), Hop count (RIP).

IP uses best effort delivery, there are no data recovery features, no built-in sessions, no retransmission. Relies on hierarchical protocols (TCP) to handle dropped, corrupted, and misdirected packets.

**Local Loopback Address –** Used to let a system send a message to itself for testing, this is very useful for making sure the TCP/IP stack is correctly installed on a machine. (**EX:** 127.0.0.1)

Routers also have loopback addresses (*int l0*) which are not the same as the local loopback address.

**RFC 1918 Private Addresses –** Non-routable on the internet, **3 blocks of IPs:**

* 10.0.0.0 – 10.255.255.255
* 172.16.0.0 – 172.31.255.255
* 192.168.0.0 – 192.168.255.255

***Section 8 – Initial Device Configuration:***

**On a switch**, all interfaces are disabled at initial boot and must be manually brought up. **Routers are the opposite**; they have all interfaces up at boot.

**VTY Lines –** The Virtual Terminal lines of the router, used solely to control inbound Telnet/SSH connections. They appear in the configuration line as ‘*line vty 0 4*’.

***Section 9 – IP Subnetting:***

**Binary Subnetting Method Rules:**

* **Network/Subnet Address =** Fill the host portion of an address with binary 0’s
* **Broadcast Address =** Fill the host portion of an address with binary 1’s
* **First Host =** Fill the host portion of an address with binary 0’s **except for the last bit**, set to binary 1
* **Last Host =** Fill the host portion of an address with binary 1’s **except for the last bit**, set to binary 0

**Powers of 2 Shortcut Table:**

|  |  |
| --- | --- |
| **21** | 2 |
| **22** | 4 |
| **23** | 8 |
| **24** | 18 |
| **25** | 32 |
| **26** | 64 |
| **27** | 128 |
| **28** | 256 |
| **29** | 512 |
| **210** | 1024 |

***Section 14 – Cabling and Packet Flows:***

**Rollover Cable –** Cable used in Cisco environment to connect to the console port of network devices (**One side is DB9 =** End Devices, **other side is RJ45 =** Network Devices)

**OSI Model Overview:**

* Layer 1 = Physical (RJ-45, Hub, Physical Interfaces)
* Layer 2 = Data Link (MAC Address)
* Layer 3 = Network (IP Address)
* Layer 4 = Transport (TCP/UDP)

***Section 18 – Duplex and Speed Mismatch:***

**Mismatch Duplex –** When one device is configured for full duplex and another is configured with half duplex, the half-duplex side can expect to receive “late collision” errors.

Duplex – Auto configuration for duplex is recommended, if manual settings are required, ensure both sides have matching set configurations.

***Section 20 – TCP/UDP:***

**Socket –** Combination of the IP of a host, port number used, and the transport protocol used.

**TCP Sliding Window –** Controls the flow of data between sender/receiver. If data is being sent too fast for receiver to handle, receiver drops data and requires retransmission.

***Section 23 – VLANs v1:***

**VTP (VLAN Trunking Protocol) –** **Uses MAC =** 01-00-0C-CC-CC-CC. Messages = Summary Advertisements, Subset Ads, Ad Requests.

**VTP Messages:**

* **Summary Ads =** Every 5 mins, or whenever there’s a change. Informs other switches of the current VTP domain and config revision number.
* **Summary Requests =** **3 situations when these messages are used:** switch has been reset, VTP domain name has changed, or if there are several VLANs more than one subset ad may be required.

***Section 27 – DTP:***

**DTP Modes:**

* **Dynamic Desirable –** Switch initiates trunking with connected network devices
* **Dynamic Auto –** Switch doesn’t initiate but will use trunking if other side initiates

It’s **best practice to disable negotiation of trunking and manually configure** preferred trunking mode.

Disable DTP – **(config-if)#**switchport nonegotiate

DTP packets are sent on the Native VLAN through 802.1Q encapsulation, and they’re sent on VLAN 1 through ISL encapsulation.

***Section 29 – Spanning Tree:***

**Bridge Protocol Dat Unit (BPDU) –** 8-byte value unique to a switch (2-byte priority field, 6-byte system ID). Consists of the priority 32,768 by default.

**3 kinds of BPDU:**

* Configuration BPDU – Used to provide info to switches
* Topology Change BPDU – Tells switches of a change
* Acknowledgement BPDU – Confirms the receipt of a topology change in a notification

**STP Link Types:**

* **Shared** (Half-Duplex)
* **P2P** (Full-Duplex)

**Rapid Spanning Tree (RSTP)** Convergence **–** Unlike classic STP, RSTP doesn’t rely on timers to converge port states. Instead, it relies on 2 variables: Edge Ports and Link Types.

***Section 40 – Routing Intro:***

Routed Protocols – Carry user info, each router makes an independent decision in determining path. (EX: IPv4, IPv6, etc.)

Routing Protocols – Communicate info about networks and determine the best route between networks. (EX: EIGRP, OSPF, RIP, etc.)

**AS (Autonomous System) –** Grouping of networks under a single administrative domain.

* **IGPs (Interior Gateway Routing Protocol) –** Routing protocol used within an AS: RIP, EIGRP, OSPF.
* **EGPs (Exterior Gateway Protocols) –** Routing protocol used between AS’s: BGP (Border Gateway Protocol)

*Types of Routing Protocols:*

**Distance Vector –** Routing by rumor, determine the direction and distance to a destination. Routers advertise routes as a vector of distance and direction.

* **Direction =** Next hop address
* **Distance =** Uses a metric such as hop count

**Link State –** Visibility of entire network, can make a much more informed decision about how to get to a destination because the full path is known. Each router originates info about itself, its directly connected links, and the state of those links.

Uses an algorithm called **Shortest Path First (SPF)**. Every router constructs a map of the connectivity to a network in the form of a graph. Routers flood networks with LSAs and populate the topological database.

Link State routing protocols are more difficult to configure and require more memory and processing power.

**EIGRP (Enhanced Interior Gateway Routing Protocol) –** In theory, takes the best of both combined into a single routing protocol and gives you the power of Link State with the ease of Distance Vector. **Cisco Proprietary.**

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

**Administrative Distance –** Tie breaker to determine the best route to a destination that has multiple known routes via different routing protocols. The **lowest admin distance** will be chosen.

**Classful Routing Protocols –** Don’t advertise subnet masks, consistency of subnet masks is assumed.

*VS.*

**Classless Routing Protocols –** Do advertise subnet masks, support VLSM. Summary routes can be manually configured. EX: OSPF, EIGRP, RIPv2

**Longest Prefix Match –** “The rule of specificity”, routers will choose the most specific match (longest matching network prefix) to a destination, even over AD.

**Ex:** 10.1.1.0/24 is a longer match than 10.1.1.0/16 so a router would choose that route when pinging 10.1.1.1, even if the /16 route had a lower AD.

***Section 41 – Static Routing:***

Routing Table: **Directly Connected =** Added to the routing table automatically, directly connected to one of the interfaces on the local router.

**For static routes on Ethernet interfaces**, use the next-hop IP instead of the exit-interface. **Exit-interfaces are specified when** configuring point-to-point connections such as serial interfaces.

***Section 53 – VLSM:***

**Route Summarization Trick** *(If the octets that are different in each IP fall within these binary ranges)*:

* 4 => 7: 4
* 8 => 15: 8
* 16 => 31: 16
* 32 => 63: 32
* 64 => 127: 64

The various network routes can be summarized by rounding down and counting the existing network bits for correct CIDR notation.

**(config-router)#**no auto-summary **–** This command ensures the routing protocol being used is running as Classless. Meaning it supports subnet masks/VLSM within the network in routing advertisements.

Auto summarization takes place by default in: RIPv1/2, EIGRP, IGRP

***Section 54 – Administrative Distance and Route Lengths:***

|  |  |
| --- | --- |
| **Routing Protocol** | **Administrative Distance** |
| Directly Connected | 0 |
| Static Route | 1 |
| eBGP | 20 |
| EIGRP | 90 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| iBGP | 200 |

***Section 59 – Port SPAN (Mirroring):***

**SPAN (Switch Port Analyzer) –** Port Mirroring/Port Monitoring, to configure a switch to make copies of ethernet frames for certain ports/VLANs.

**Remote SPAN –** Copy frames from a local switch to a remote switch.

*SPAN Configuration EX:*

* **(config)#**monitor session 1 source interface g0/0/0 *(rx, tx, both)*
* **(config)#**monitor session 1 destination interface g1/0/0

Ingress Traffic – When SPAN is enabled on a switch, the switch no longer learns MAC addresses on the SPAN destination port and doesn’t allow traffic to be received on that port either.

SPAN Dependencies & Rules – A SPAN destination port can only be used with one SPAN session at a time. A SPAN destination port can also not be a SPAN source port.

***Section 62 – Network Management Fundamentals:***

**2 Main Network Management Protocol Types:**

* Query (Polling)-Based = Network Management Station asks a question from a device (sends a query). This protocol type is reliable, can be scheduled, and can detect problems just by asking for info from a network device (no response=problem). Cons of this protocol type are possibility of large network overhead and storage requirements.
* Event-Based = Network Management Station listens for announcements/events (Syslog based, SNMP trap based, etc.). Cons are less reliability; NMS is passively waiting/listening and can be unaware of a network issue for some time. Pro is that it can react very quickly if an event takes places on the network.

**NMS’s use UDP Port 161** to initiate destinations to monitored devices, this port number can be manually configured.

***Section 65 – MIBs, OIDs, and Performance Counters:***

**MIB (Management Information Database) –** Used for managing larger entities in a network, tree structured database that uses SNMP.

**OID (Object Identifier) –** Included within an MIB, can be used for polling a specific interface.

***Section 67 – Managing Cisco Devices:***

**Config Register Values:**

* 0x2102 = Normal Boot
* 0x2100 = Router will boot into ROMMON (Read-Only Memory Monitor Mode)
* 0x2142 = Bypass startup-config
* 0x2101 = Boot into RXBoot (if supported), or boot using the first OS in flash

***Section 72 – Infrastructure Security:***

**#**show control-plane host open-ports **=** Command lists all enabled services that currently have open ports. Best practice is to disable any unused services on network devices.

**SSH Configuration:**

1. Specify hostname
2. Specify domain name [**(config)#**ip domain-name*domain*]
3. Configure username/password
4. Generate RSA (public/private) keys
5. Enable SSH connection to be allowed on the vty lines [**(config-line)#**transport input ssh]
6. Specify for the local username/password to be required [**(config-line)#**login local]

Banners [**(config)#**banner \_]:

* MOD (Message of the day) banner = Displays a temporary message (maintenance)
* Login banner = Shown before a user logs in
* Exec banner = Displays after login, info that only internal staff should know (physical location of device)

Login banners are shown before username/password authentication, Exec banners are shown after logging in.

***Section 79 – Port Security:***

**Port Security Violation Options:**

* **Protect (No Logging) =** Drops packets with unknown source MAC until a sufficient number of secure MACs (MACs learned and added to the Secure MAC table) are manually removed.
* **Restrict (Logging) =** Drops packets with unknown source MAC until a sufficient number of secure MACs are removed. Causes the security violation counter to increment and log messages to be generated.
* **Shutdown =** Default, puts port into ‘Error-disabled’ mode and sends SNMP Trap notification (if configured).

**Sticky MACs –** When this is enabled, MACs that have been learned and added to the secure MAC table will automatically be added to the running-config of a device (it’ll be kept there and added to the startup-config if memory is saved before reloading).

**Split Horizon –** A method used by distance vector protocols to prevent network routing loops. The basic principle is: A route can't be advertised out of an interface if the next hop for the advertised route is found on that interface.

**Poison Reverse –** Another distance vector method used to prevent routing loops: Routes received via one interface must be advertised back out from that interface with an unreachable metric.

The difference is Split Horizon passively tries to prevent routing loops by not advertising the route out the wrong interface, whereas Poison Reverse actively forbids neighboring routers to use it to reach the networks.

***Section 81 – 802.1x, RADIUS, TACACS and ACS:***

**RADIUS –** Open-standard protocol that uses **UDP** (**ports 1645, 1812**) and combines Authentication/Authorization. Is used for Users, encrypts only passwords.

**TACACS –** Cisco-proprietary protocol that uses **TCP** (**port 49**) and separates Authorization/Accounting. Is used for Network Devices, encrypts entire packets.

***Section 84 – Access Control Lists (ACLs):***

**Standard ACL –** Checks only source IP, permits/denies entire protocol suites. Should be placed as close to the destination as possible.

**Extended ACL –** Checks source and destination addresses, permits/denies specific protocols and apps.

**Wildcard Masks:** **0 in mask =** host bit must match / **1 in mask =** ignore host bit

***Section 88 – NAT:***

**RFC 1918 Private IPv4 Addresses:**

* 10.0.0.0 – 10.255.255.255 (10/8)
* 172.16.0.0 – 172.31.255.255 (172.16/12)
* 192.168.0.0 – 192.168.255.255 (192.168/16)

|  |  |  |  |
| --- | --- | --- | --- |
| **Inside Local** | **Inside Global** | **Outside Local** | **Outside Global** |
| Internal (Private) IP of a device | Public IP of internal devices | IP of an external device that’s seen by the internal network | IP of external device that’s seen publicly on the internet |

**Static NAT –** Maps a private IPv4 address to a public IP (one-to-one mapping). Useful when a device must be accessible from outside a network (web server).

**Dynamic NAT –** Maps a private IP to a group (pool) of public IPs. Not very efficient, should be used only when necessary.

**PAT (Port Address Translation) –** Maps multiple private IPs to a single public IP. That single public IPs then uses port numbers to differentiate between different translations. **AKA** “**NAT Overloading**”.

***Section 95 – QOS:***

**Classification –** Before QoS can be applied to packets, a network device must first know which class the packet belongs to (Platinum, Gold, Silver, Bronze), it can do that by looking at the Marking.

**Marking –** “Ticket” or indicator of the level of service that a packet will receive. 802.1Q is a Layer 2 marking, it has a header which contains a field called the CoS/PCP (Class of Service/Priority Code Point).

**ToS (Type of Service) –** Second byte in an IPv4 packet that can be used for Layer 3 QoS marking. The first 3 bits of the ToS byte are the IPP (IP Precedence) bits, and combined with the next 3 bits, those 6 bits are the DSCP (Differentiated Services Code Point).

*Best practice is to classify and mark as close to the edge of the network as possible.*

**Trust Boundary –** The Trusted Domain is the part of a network that only admins can manage, the Untrusted Domain is the part of a network admins don’t manage (PC’s/printers). The Trust Boundary is where packets are classified and marked. By default, Cisco routers will override any QoS markings they receive on an Untrusted Boundary.

**Policing and Shaping** limit the amount of traffic that can be transmitted by minimum/maximum set bandwidths. Policing will generally drop excess traffic, while Shaping will delay excess traffic.

Policers – Perform checks for traffic violations against a configured rate. Does not delay traffic, either remarks and transmits it or drops it completely. Usually used as ingress tools, traffic is dropped before its processed to avoid wasting resources. Policers can cause TCP retransmissions because it drops packets, inversely it cannot cause Jitter/Delay because of this.

Shapers – Doesn’t drop traffic but smooths it out by delaying it to make sure that it falls within a configured bit rate. Usually used to meet SLA’s (Service Level Agreements). When the traffic spikes above the contracted rate, excess traffic is buffered. This can cause Delay/Jitter but is gentler on traffic.

**Queuing –** Queuing mechanisms manage traffic congestion. They determine the ordering of packets and the output buffers when congestion occurs; Packets are reordered so that high-priority packets can be sent out before lower-priority packets.

**Round Robin Queuing Mechanisms –** All traffic is treated the same way, can result in delay.

**Scheduling –** The process of deciding which packet should be sent out next, occurs regardless of whether there’s congestion on a link.

**Congestion Management Queuing Mechanisms:**

* **FIFO (First In First Out) –** A single queue with packets that are sent in the exact order that they arrived.
* **PQ (Priority Queue) –** Consists of 4 queue’s (high, normal, medium, low) that are served in a strict priority order; the lower priority queues are served only when the higher-priority queues are empty.
* **CQ (Custom Queuing) –** Up to 16 queues serviced in a round-robin fashion. To prevent starvation, it provides traffic guarantees but doesn’t provide strict priority for real-time traffic.
* **WFQ (Weighted Fair Queuing) –** Algorithm that divides ethernet bandwidth by the number of flows (source/destination IP, protocol, port). It provides a good service for real-time traffic, but no bandwidth guarantees for particular flows, this led Cisco to develop CBWFQ.
* **CBWFQ (Class Based Weighted Fair Queuing) –** Guarantees bandwidth to specific classes and provides dynamic fairness of other flows. Allows you to create different classes where minimum bandwidths can be specified for each class. No latency guarantees, suitable only for data networks.
* **LLQ (Low Latency Queuing) –** Essentially is CBWFQ with an added strict priority queue for real-time traffic.

**WRED (Weighted Random Early Detection) –** Way to avoid congestion, randomly drop packets from multiple flows before the queue fills up.

***Section 100 – OSPF:***

**OSPF (Open Shortest Path First) –** Link state routing protocol that resides directly on top of the IP protocol (doesn’t use TCP/UDP) and has an **Ethernet Protocol ID of** 89/0x59. **Uses 224.0.0.5** or unicast messages to create neighbor relationships. Routers will send LSAs by default, every 30 minutes and whenever a link state changes.

***State =*** Description of an interface and its relationship to neighboring routers.

**OSPF Tables:**

* **IP OSPF Neighbor Table (Adjacency Table) =** Neighboring Routers
* **IP OSPF Topology Table (LSDB) =** All routers and attached links in area/network
* **IP Routing Table (Forwarding Table) =** Best routes

**OSPF Packet Types:**

* **Hello =** Dynamically discovers, forms, and maintains neighbors. Has default intervals of 10 seconds (Ethernet) and 30 seconds (Serial). Dead Timer is 4 times the hello interval by default.
* **Database Description (DD/DBD) =** Used to exchange brief versions of each LSA.
* **Link State Request (LSR) =** Request for LSA info.
* **Link State Update (LSU) =** Contains LSAs, typically in response to LSR.
* **Link State Acknowledgement (LSAck) =** Confirm receipt of an LSU message.

**OSPF LSA Types:**

* **LSA Type 1 =** Router LSAs
* **LSA Type 2 =** Network Link LSAs
* **LSA Type 3 =** Summary LSAs
* **LSA Type 4 =** ASBR LSAs
* **LSA Type 5 =** External LSAs

Any area number can be used for OSPF, unless there are multiple areas, then Area 0 must be used.

**Area 0 (Backbone Area)** must then be connected to every area within an Autonomous System. Routers that connect to the backbone area/other areas are = **ABRs (Autonomous Border Routers)**. ABRs allows for the summarization of routes. **ASBRs** are = Routers that connect/border two AS’s.

* **OSPF Internal Router =** Router with interfaces ONLY in an internal area.
* **Intra-Area OSPF =** Routes that exist within an internal OSPF Area.
* **Inter-Area OSPF =** Routes that exist in different OSPF Areas.
* **External OSPF =** Routes that originate from a different routing protocol.

**OSPF Router ID =** By default, is the IP of the Loopback or the highest IP of any active interface when OSPF is enabled.

**OSPF Neighbor Adjacencies Hello Packet =** **All must be the same** for routers to establish OSPF Neighbor Relationships: Hello/Dead Intervals, Area ID (NOT Process ID), Password, and Stub area flag

**Designated Router (DR) –** All routers within an OSPF segment will designate a DR and each form Full relationships with it. **224.0.0.6** is used by the DR to send updates to all subscribed routers. The DR is elected based on highest OSPF priority, which ranges from 0-255 but the default is 1. A **priority of 0 disables a router’s ability to become the DR**. If there is a tie in priority, then the DR is elected based on the highest OSPF Router ID.

**OSPF Cost –** Has a **default reference bandwidth that is = 108 (100,000,000)**. The cost is then calculated by using: 108 / bandwidth in bits per second.

* 1Kbps = 1,000 bps
* 1Mbps = 1,000,000 bps
* 10Mbps = 10,000,000 bps

***EX: 10 Mbps = 100,000,000 / 10,000,000 = OSPF Cost of 10****.*

The OSPF Reference Bandwidth can be changed using: **(config-router)#**auto-cost reference (bandwidth) *value*

The OSPF Cost can be changed using: **(config-router)#**ip ospf cost *value*

***Section 112 – IPv6:***

IPv6 Address = 16 Octets – 128 bits:  
EX: X:X:X:X:X:X:X:X (X=16 bit hex field)

**IPv6 Loopback =** ::1/128

*There’s no need for NAT in IPv6.*

**IPv6 Unicast =** Address for a single interface (several types):

* **IPv6 Global Unicast –** Has a /64 Network Prefix = First 48 bits are the **Global Prefix**, the next 16 bits are the **Subnet ID**. No need for NAT because of Global Unicast, these addresses are the equivalent to Public IPv4 Addresses.
* **Link-Local Unicast –** Used to communicate with nodes on an attached link, these addresses are not forwarded by routers.

**IPv6 Multicast =** One to many.

**IPv6 Anycast =** One to nearest, multiple devices share the same address.

*There’s no Broadcast in IPv6, Multicast is used instead.*

*Every interface within a network has an IPv6 /64 mask.*

**Stateless Address Autoconfiguration (SLAAC) –** Allows devices on a network to automatically configure IPv6 addresses on its interface (using link-local addresses and the interface’s MAC) without a DHCP server. Routers send periodic Router Advertisement messages using a Link-Local address. **Router boots up, sends Router Solicitation to all routers using FF02::2 requesting Router Ads, another router will reply with Router Ads** containing: Network Prefix, Default Route.

**Stateful DHCP (v6) –** More control than Stateless and can be used concurrently with SLAAC. **Can provide IPv6 addresses in the absence of routers and can be used for network renumbering,** automatic domain name registration of hosts **(Dynamic DNS)**. Unlike SLAAC, DHCPv6 is called ‘stateful’ configuration because it keeps track of which hosts have which IP and stores information about them.

**IPv6 Routing Protocols:**

* Static
* RIPng (next generation) = Similar to RIP for IPv4, uses Distance Vector, radius of 15 hops, Split Horizon, Poison Reverse. Updated from other versions of RIP: Uses IPv6 prefix, next hop IPv6 address. Multicast of FF02::9.
* OSPFv3 = Virtually identical to OSPF for IPv4. Router-ID must still be in IPv4 format.
* IS-IS
* MP-BGP4

**IPv6 Default Route** = ::/0.

**IPv6 Ethernet Protocol ID =** 0x86DD

***Section 118 – Wide Area Networks (Point-to-Point):***

Wan Technologies:

* OSI **Physical Layer =** Physical presentation changes in a WAN from what’s seen in an Ethernet environment. **Instead of RJ45 cabling, X.21/V.35 cabling is used** (Channel Service Unit (CSU) or Data Service UNIT (DSU) are used to connect to these WAN Leased Line connections).
* OSI **Data Link Layer = Encapsulations** **used:** Frame Relay, PPP, HDLC, MPLS.

Leased Lines >> Synchronous Serial Communication >> 2 devices will synchronize their clocks:

Alignment/synchronization of clocks is a prerequisite for an agreement on parameters of data transfer.

**CSU DSU –** Provides the clocking and is the “master” for the communication, the router/network device is the “slave”. Before communication can start, 2 devices must align their clocks and agree on the clock intervals.

**DTE (Data Terminal Equipment) –** Router uses external clocking from a **DCE (Data Communication Equipment)**, thus synchronizing its clock with the CSU DSU. (The CSU DSU is the DCE side of the connection.)

**DCE (Data Control Equipment) =** Controls the speed/clocking when a router sends data, configured for the relevant speed of the connection.

**HDLC (High Level Data Link Control) –** Layer 2 encapsulation that’s used across a leased line providing Layer1 service/connectivity from one site to another. Cisco has a proprietary version (CHDLC) that simply adds a *‘Type’* field to an HDLC frame. This added field allows multiple higher layer protocols (IPv4, IPv6) to traverse the link at the same time.

**PPP –** Industry standard version of encapsulation, can be used to configure a leased line (serial) connection between non-Cisco routers.

*HDLC and PPP cannot properly operate across from each other, interfaces must be configured with one encapsulation type or the other, not both.*

***Section 120 – IPv6 Routing (OSPF):***

**OSPF v2 VS. v3:**

**V2 =** IPv4 networks, uses the *“network”* command to enable the routing protocol.

**V3 =** IPv6 networks, the routing protocol is **enabled directly on an interface**. **Neighbor relationships are formed** using IPv6 link local addresses.

*Both versions of OSPF can be used simultaneously but they will keep separate databases, different addresses, and won’t communicate with each other.*

***Section 122 – VPNs:***

**Cryptography Terminology:**

* **Asymmetric** **Algorithm =** Algorithm in which different keys (public and private) are used for encryption and decryption. Public key algorithms are asymmetric.
* **Symmetric Algorithm =** Algorithm in which the same key is used for encryption and decryption. Secret key (AES) algorithms are Symmetric.

**Authentication:**

* **PSK (Pre-Shared Key) –** A secret key value is entered into each peer manually and is used to authenticate the peer.
* **RSA (Digital) Signatures –** Encrypt the hash with a private key. These are harder to implement than PSKs but are more scalable.

**IPSec (IP Security) –** Network layer protocol (suite of protocols) that protects and authenticates IP packets. Framework of open standards that is algorithm independent.

**IPSec Protocols:**

* Internet Key Exchange (IKE) = Provides a framework for negotiating security parameters and establishing authenticated keys.
* Authentication Header (AH) = No encryption but has Authentication and Integrity.
* Encapsulating Security Payload (ESP) = Encryption, Authentication, and Integrity.

**IPSec Modes:**

* **Transport Mode –** The original IP Header of the packet being encrypted is used to transport the packet.
* **Tunnel Mode –** The original IP Header **is not** used to transport the packet; A new IP Header is tagged in front (contains IPs of peer devices).

IPSec Framework (order of operations):

* Choose the IPSec protocol (ESP, AH, or both)
* Choose the IPSec mode (Transport/Tunnel)
* Choose an Encryption algorithm (AES)
* Choose Authentication (MD5/SHA)
* Choose either PSK or Digital Signatures

**Site-to-Site VPN –** Sets up a dedicated secure tunnel between 2 sites/devices. Can be thought of as a virtual leased line that connects the 2 LANs. Can encrypt all high layer protocols.

**Remote Access IPSec VPN –** Set up a secure VPN tunnel between 2 devices (PC & Router). Client installs VPN software that’s used to connect to the VPN client. Can be used by clients while “roaming” or over public wireless networks.

**Remote Access SSL VPN –** Set up a secure VPN tunnel between 2 devices (PC & Router), doesn’t require VPN software to be installed on client device.

***Section 123 – GRE Tunnels:***

**General Routing Encapsulation (GRE) –** Point-to-point tunnel that provides generic routing encapsulation: multiple higher layer protocols (IPv4, IPv6, IPX), Multicast routing protocols. **Does not provide encryption**. GRE tunnels **can be encapsulated within IPSec tunnels** to utilize both the point-to-point link and encryption/authentication. Uses **IP Protocol number** 47. GRE is a protocol that sits next to TCP/UDP in the OSI model.

***Section 128 – Wi-Fi:***

|  |  |
| --- | --- |
| Wi-Fi 1 | 802.11b |
| Wi-Fi 2 | 802.11a |
| Wi-Fi 3 | 802.11g |
| Wi-Fi 4 | 802.11n |
| Wi-Fi 5 | 802.11ac | Doesn’t support 2.4GHZ. |
| Wi-Fi 6 | 802.11ax | Makes more efficient use of available Wi-Fi Channels by essentially dividing them up into sub-channels. |

**802.11 Topologies** (3 types)**:**

* **Independent Basic Service Set (IBSS) = (Ad hoc mode)** Clients connect directly without an AP.
* **Basic Service Set (BSS) – (Infrastructure Mode)** Mobile clients use a single AP.
* **Extended Service Set (ESS) – (Infrastructure Mode)** 2 or more BSSs, connected by a common distribution system.

**WPA-Personal (WPA-PSK) –** Designed for SOHO/home networks, doesn’t require an authentication server.

**WPA-Enterprise (WPA-802.1X) –** Designed for enterprise networks and requires a RADIUS authentication server.

**WLC –** On initial configuration, connect to WLC via HTTP. After that, connections must be made via HTTPS.

**Wi-Fi Channels =** A range of available frequencies.

**Channel Bonding =** Combining multiple channels together to create one with more available throughput.

***Section 131 – Network Automation & Programmability:***

**Separation of Data and Control Plane –** Control plane (Forwarding Plane) is the “brain” which is separated from the Data plane (contains the actual data packets) in controller-based networks.

**Management Plane –** How a device is managed (Telnet, SSH, SNMP, Syslog).

**Ansible vs Puppet vs Chef:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Ansible** | **Puppet** | **Chef** |
| *Term for the File That Lists Actions* | Playbook | Manifest | Recipe, Runlist |
| *Protocol to Network Device* | SSH, NETCONF | HTTP (REST) | HTTP (REST) |
| *User Agent or Agentless* | Agentless | Agent | Agent |
| *Push or Pull Model* | Push | Pull | Pull |

**Overlay Network =** VXLAN Tunnels. Can use a different IP addressing scheme from the Underlay.

**Underlay Network =** Physical devices (routers/switches). Simple configuration and focuses on high speed.

*Think of the Underlay as the internet, and the Overlay network as IPSec/VPN tunnels. The Underlay has no visibility of traffic that’s being encrypted through the IPSec tunnels.*

**SDA (Software Defined Architecture) –** Instead of manually configuring ACLs, Policies can be centrally configured/implemented to entire networks or specific devices through a controller GUI. These Policies are applied through VXLAN tunnels on the overlay network. SDA is an enterprise solution that uses software-defined principles normally used for data centers and applies them to enterprises (Getting rid of STP, instead use routing protocols. Apply policies to manage devices instead of ACLs).

***Section 132 (6.7) – JSON (JavaScript Object Notation):***

**JSON Formatting –** JSON data is written as key(name)/value pairs. A key/value pair consists of a field name (in “”), followed by a colon, followed by a value.

**EX:** “name”:”John”

**JSON Data Types:**

* **Object =** Unordered collection of key:value pairs. Data surrounded by **{}**. Each key/value pair is separated by a comma but no trailing commas are allowed. Use double quotes not single quotes. Boolean values must be lowercase.

**EX:** {“firstName”:”John”, “lastName”:”Doe”}

{

“firstName” : “John”,

“lastName” : “Doe”,

}

* **Array =** Ordered list of values, uses square brackets []. Can store multiple types of JSON data (string, number, Boolean, object, null, or another array). Values must be separated by a comma.

***Section 133 – REST (Representational State Transfer) APIs:***

Applications talk to other apps by using APIs, structured data (JSON, XML, YAML) is needed for the apps to properly share information.

Principles of REST:

* **Client-Server –** By separating user interface concerns from data storage concerns, we improve the portability of the user interface across multiple platforms and improve scalability by simplifying the server components.
* **Stateless –** Each request from client to server must contain all the info necessary to understand the request and can’t take advantage of any stored context on the server. Session state is kept entirely on the client.
* **Cacheable –** Cache constraints require that the data within a response to a request be implicitly or explicitly labeled as cacheable or non-cacheable. If a response is cacheable, then a client cache is given the right to reuse that response data for later, equivalent responses.

CRUD (4 actions performed by an app):

* **Create =** Create new instances of variables and data structures on the server and initialize their values as kept on the server.
* **Read =** Retrieve the current value of variables that exist on the server, storing a copy of the variables, structures, and values on the client.
* **Update =** Change the value of variables that exist on the server.
* **Delete =** Delete from the server different instances of data variables.

REST (HTTP) Verbs:

* **POST =** Create
* **GET =** Read
* **PATCH, PUT =** Update
* **DELETE =** Delete

***Section 139 – SDN (Software-Defined Networking):***

**Open SDN –** Uses the OpenFlow protocol, defined as the physical separation of the network control plane from the forwarding plane and where a control plane controls several devices.

**SDN via Overlays –** An example is NSX (from VMWare), uses the VXLAN protocol. A virtual network overlays (logically sits on top off) physical network devices (underlay). The virtual network can be automatically deployed across the physical network.

**SDN via APIs (REST) –** Rather than being tied to configuring a network device via a command line interface, able to configure network devices through a programmatic interface.