22-11-2023

Cheat sheet..

1. Where to use subnet mask and wildcard mask

|  |  |
| --- | --- |
| Subnet mask | Wildcard mask |
| Ip add | Ospf & Eigrp |
| Static route | Acl |
| Dhcp server |  |
| Dynamic NAT |  |

1. Standard Vlan (1-1005) & Extended Vlan (1006-4095)
2. Standard ACL (**1-99, 1300-1999**) & Extended ACL (100-199, 2000-2699)
3. CDP timer (60sec) & holdtime (180sec)
4. LLDP timer (30sec) & holdtime (120sec)
5. RIPv2 timer (30sec) & holdtime (180sec) & flush timer (240sec)
6. EIGRP hello interval (5sec) & holdtime (15sec)
7. Ospf hello interval (10sec) & dead interval (40sec) for Broadcast & Point to Point
8. Ospf hello interval (30sec) & dead interval (120sec) for non-broadcast & all other
9. HSRP = Active and Standby router = Hello (3Sec) & Hold time (10Sec)
10. If didn’t receive any update for a port switch will remove MAC address entry after (300sec)
11. STP BPDU - Hello time (2 sec) – Forward Delay (15 sec) – Max Age (20 sec)

|  |  |
| --- | --- |
| Header size in bytes |  |
| L2 | Header 22 bytes Payload 1500 bytes Trailer 4 bytes |
| L3 | IPv4 Header 20 bytes & IPv6 Header 40 bytes |
| L4 | TCP Header 20 bytes & UDP Header 8 bytes |

1. STP port cost

|  |  |
| --- | --- |
| 10G | 2 |
| 1G | 4 |
| 100M | 19 |
| 10M | 100 |

1. Ospf default port cost 1 ie (1-65535) – Lowest is the best
2. Ospf default port priority ie (1-255) – Highest is the best
3. Ospf DR/BDR selection

|  |
| --- |
| 1. Ethernet link will check for Highest port priority = If port priority is the same   The Router with the highest OSPF interface priority on a segment becomes the DR  Router with the next highest OSPF interface priority becomes the BDR.  Setting a OSPF port priority of zero make the router ineligible to become a DR or BDR |
| 1. The router-id <ip-address> config-router command / Manually configured Router ID.  2. If that doesn’t exist, then the highest IP address on a loopback is used.  3. If that doesn’t exist, then the highest IP address on an up physical is used. |

1. OSPF reference bandwidth

|  |
| --- |
| 1. The "auto-cost reference-bandwidth" takes its argument in Mb.  2. The "bandwidth" command takes its argument in Kb.  3. The formula for calculating OSPF cost is = reference bandwidth/interface bandwidth. |
|  |

1. SPT default bridge priority value = (32768) & STP increments priority by 4096
2. DSCP – 46 -EF
3. COS For voice 5
4. QoS For video = Gold
5. Qos For voice = Platinum
6. QoS For Best effort delivery = Silver
7. QoS & COS

A screenshot of a computer

Description automatically generated

1. QoS & DSCP

DSCP(Differentiated Service Code Point) By having generally agreed upon standard markings for different kinds of traffic.

Default Forwarding (DF) - best effort traffic

Expedited Forwarding (EF) - Low losslatency/jitter traffic

Assured Forward Forwarding (AF) -

1. QoS & DSCP

A screenshot of a computer

Description automatically generated

1. QoS

|  |  |
| --- | --- |
| **Traffic Policing** | **Traffic Shaping** |
| 1.Traffic policing is a mechanism which monitors the traffic in any network. | Traffic Shaping is a congestion control mechanism that brings delays in packets. |
| 2.The packets with rates that are greater than the traffic policing rate are discarded. | It buffers the packets with rates that are greater than the traffic shaping rate. |
| 3.Traffic policing doesn’t cause delay. | Traffic shaping causes delay of packets. |
| 4.The token values are calculated in bytes per second. | The token values are calculated in bits per second. |
| 5.In traffic policing queuing of traffic is not performed. | Queuing of traffic is performed in traffic shaping. |
| 6.Traffic policing supports traffic remarking. | Traffic shaping doesn’t supports traffic remarking. |
| 7.Traffic policing can be used to control outbound or inbound traffic. | Traffic policing can used to control outbound traffic only. |
|  |  |

1. Queueing Methods

|  |  |
| --- | --- |
| - First In First Out (FIFO)  - Priority Queueing (PQ)  - Custom Queueing (CQ)  - Weighted Fair Queueing (WFQ)  - Class-Based Weighted Fair Queueing (CBWFQ) - Low Latency Queueing (LLQ) |  |
|  |  |

1. Ipv6 Multicast address

|  |  |
| --- | --- |
| FF02::1 | All nodes |
| FF02::2 | All routers |
|  |  |
|  |  |
|  |  |
|  |  |

1. IPv6 Addressing

|  |  |
| --- | --- |
| Link Local address | FE80::/10 (FE80:: to FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF) |
| Unique Local address | FC00::/7 (FC00:: to FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF) |
| Global Unicast address | 2000::/3 to 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF |
| Multicast address | Interface-local > FF01  Link-local > FF02  Site-local > FF05  Organization-local > FF08  Global > FF0E |
| Anycast Address | In way we can say – It is a Global unicast address depends on the design  One to one of many |
| Extended Unique Identifier  EUI - 64 |  |
|  |  |

1. Hi
2. Hi
3. Security Attacks and solutions/mitigation technic

|  |  |  |
| --- | --- | --- |
| S.no | Security thread | Prevention measure |
| 1 | What is a practice that protects a network from VLAN hopping attacks? | Assign all access ports to VLANs other than the native VLAN  Manually implement trunk ports and disable DTP |
| 1.1 | 802.1q double-tagging VLAN-hopping attack | Configure the native vlan with a nondefault vlan id  Configure a VLAN access control list |
| 1.2 | Switch-spoofing vlan hopping attack | Disable DTP |
| 2 | Rogue server that spoofs IP configuration | Ip source guard |
| 3 | Rogue clients on the network  ARP snooping | Dynamic Arp inspection |
| 4 | Flood attacks | Storm control |
| 5 | Cache poisoning | DHCP snooping |
| 5.1 | Mac flooding attack | Configure DHCP snooping |
| 6 | Man-in-the-middle spoofing attack | Configure 802.1 authentication |
| 7 | Unwanted superior BPDUs | Configure the root guard feature |
| 8 | Unwanted BPDUs on port fast enabled interface | Configure the BPDU guard feature |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. IEEE standards

\*\*\*\*2.4G means 3 non overlapping channel\*\*\*\*

\*\*\*\*5G means 23 non overlapping channel\*\*\*\*

|  |  |
| --- | --- |
| 802.11 | Wifi0 - 2.4G |
| 802.11b | Wifi1 - 2.4G |
| 802.11a | Wifi2 - 5G |
| 802.11g | Wifi3 - 2.4G |
| 802.11n | Wifi4 - 2.4G and 5G |
| 802.11ac | Wifi5 - 2.4G and 5G |
| 802.11ax | Wifi6 - 2.4G, 5G & 6G |
| 802.11be | Wifi6 - 2.4G, 5G & 6G |
|  |  |
| 802.1x | Wifi protected access & authentication method  EAP – Extensible Authentication Protocol |
|  |  |
| 802.1ab | LLDP |
|  |  |
| 802.1q | Vlan tagging – Trunking |
| 802.1d | STP |
| 802.1w | RSTP |
| 802.1s | MSTP |
|  |  |
| 802.3 | Wired Ethernet standard |
| 802.3ad | Wired EtherChannel - LACP |
| 802.3bt | 90watts 10/100/1000mbps – 100m PoE |
| 802.3bz | 90watts 2.5/5gbps – 100m PoE+ |
|  |  |
| 802.11k = Assisted Roaming | The list will provide it with information regarding neighbouring APs and their channels |
| 802.11r = Fast Transmission | Fast Basic Service Set Transition (FT) to allow encryption keys to be stored on all of the APs in a network |
| 802.11v = Power saving | Helps clients to improve battery life by enabling them to sleep longer.  Enables the WLAN to send messages to associated clients, for better APs to associate with clients. This is useful for both load balancing and in directing poorly connected clients |
| 802.11w = Management Frame Protection | Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames |
|  |  |

1. FHRP

|  |  |
| --- | --- |
| HSRP = Cisco | 224.0.0.2 = 0000.0c07.acxx  224.0.0.102 = 0000.0c9f.fyyy |
| VRRP = Open | 224.0.0.18 = 0000.5e00.01xx |
| GLBP = Cisco | 224.0.0.102 = 0000.5e00.yyxx  0007.b400.xxyy |
|  |  |

1. FHRP

|  |  |
| --- | --- |
| State | Function |
| active | is forwarding packets |
| standby | is ready to forward packets if the device that is currently forwarding packets fails |
| listen | has heard from the neighbor device and is receiving hello packets |
| learn | - is waiting to hear from the neighbor device  - This is the state of a device that has not yet determined the virtual IP address and has not yet seen a hello message from an active device. |
| speak | is transmitting and receiving hello packets |
|  |  |

1. Routing Table selection process

|  |
| --- |
| Longest prefix length |
| Smaller AD |
| Smaller metrix/cost |

1. OSPF Router ID election process

|  |
| --- |
| Manually configured has higher priority |
| Highest loopback ip address |
| Highest interface ip address |

1. STP Bridge ID & Root Bridge election process

|  |
| --- |
| By default – Lowest MAC address switch become --- Root Bridge of the network |
| Bridge ID = Bridge Priority + Switch Port MAC address  Default Bridge priority is 32768 --- increments of 4096 |

1. Root Port Selection

|  |
| --- |
| Lowest root cost |
| Lowest neighbour bridge ID |
| Lowest neighbour port ID – will be affected by individual port priority in STP |

1. DR and BDR selection

|  |
| --- |
| Router is highest OSPF port priority will become DR & router with second-highest port priority will become DBR |
| If the ospf port priority same then, Router with highest router ID is selected as DR second highest will be BDR |
| To Setup OSPF port priority  #int g0/0  #ip ospf priority (0-255) |
|  |
|  |

1. AD

|  |  |
| --- | --- |
| Directly connected/linked | 0 |
| Static route | 1 |
| eBgp | 20 |
| Eigrp | 90 |
| iGrp internal | 100 |
| Ospf | 110 |
| Isis | 115 |
| Rip | 120 |
| iGrp external | 170 |
| iBgp | 200 |
| Wouldn’t shown in the table | 255 |

1. Sys log ------------- What type of syslog under these category

|  |  |  |
| --- | --- | --- |
| Emergency | 0 | Hardware or software problem within the device |
| Alert | 1 | Hardware or software problem within the device |
| Critical | 2 | Indicate something that might impact the device |
| Error | 3 | Interface up/down state |
| Warning | 4 | Indicate something that might impact the device |
| Notification | 5 | Route Flaps/Neighbour adjacencies/interface protocol up/down |
| Information | 6 | Routine messages |
| Debug | 7 | Show debug command output - \*\*no debug all\*\* to stop after the troubleshoot |
|  |  |  |
|  |  |  |
| Emergency | 0 | Emergencies System shutting down due to missing fan tray |
| Alert | 1 | Alerts Temperature limit exceeded |
| Critical | 2 | Critical Memory allocation failures |
| Error | 3 | Errors Interface Up/Down messages |
| Warning | 4 | Warnings Configuration file written to server, via SNMP request |
| Notification | 5 | Notifications Line protocol Up/Down \* A routing instance has flapped\* |
| Information | 6 | Information Access-list violation logging |
| Debug | 7 | Debugging Debug messages |
|  |  |  |

1. Network Architecture

3-Tier

|  |  |
| --- | --- |
| Core L3 Router | Doing high speed transfer/backbone/redundancy |
| Aggregation L3 Switch | Doing routing/filtering/qos |
| Access L2 Switch | Doing connecting end devices |

2-Tier

|  |  |
| --- | --- |
| Collapsed Core L3 Switch | Doing high speed transfer/backbone/redundancy/ routing/filtering/qos |
| Access L2 Switch | Doing connecting end devices |

2-Tier Spine Leaf

|  |  |
| --- | --- |
| Core L3 Router | Doing high speed transfer/backbone/redundancy |
| Aggregation L3 Switch | -Doing routing/filtering/qos & Mostly server end device connectivity  - Avoid STP  - Higher East-West traffic  - No downtime while changing device  - Reduced hop count better performance |

1. Well known ports

|  |  |
| --- | --- |
| TCP |  |
| FTP | 20-data, 21-control |
| Ssh / Ansible | 22 |
| Telnet | 23 |
| SMTP | 25 |
| TACACS | 49 |
| http/https | 80/443 |
| POP3 | 110 |
| Puppet | 8140 |
| Chef | 10002 |
|  |  |
|  |  |
|  |  |
| UDP |  |
| DHCP | 67-server / 68-client |
| TFTP | 69 |
| NTP | 123 |
| SNMP | 161-agent / 162-manager /  Management Information Base (MIB)  Network Management System (NMS) |
| Syslog | UDP: 514 ……………. TCP: 6514 |
| RTP/VoIP/Video | 16384-32767 |
| RADIUS | 1812/1813 |
| CAPWAP Control/Data | 5246/5247 |
|  |  |
| TCP/UDP |  |
| DNS | 53 |

1. SNMP

|  |  |  |
| --- | --- | --- |
| V1 | V2C | V3 |
| Operations  Get  GetNext  Set  Trap  **Community Strings** | Operations  Get  GetNext  Set  Trap  **Getbulk**  **Inform** | Operations  Get  GetNext  Set  Trap  **Getbulk**  **Inform**  **Message Authentication**  **Message Encryption** |
| Plain Text Community String |  |  |
| 32 bit Counter  No security | 64 bit Counter | 64 bit Counter  Has Authentication and Encryption |
|  |  |  |

1. Ji
2. Available Password types

|  |  |
| --- | --- |
| TYPE 0 | Not in use – Clear text |
| TYPE 4 | Not in use |
| TYPE 5 | MD5 – If the device is too old recommand to use |
| TYPE 6 | Not in use |
| TYPE 7 | Not in use |
| TYPE 8 | Not in use |
| TYPE 9 | Algorithm Script – Best practice  80-bit salt hashing |

1. TCP Vs UDP

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| **Connection-oriented**: TCP establishes a connection before transmitting data, ensuring that the communication link is reliable. | **Connectionless**: UDP does not establish a connection before sending data, making it faster but less reliable. |
| **Reliable**: TCP ensures that all data packets are delivered in the correct order. It uses acknowledgments (ACKs) and retransmissions for lost packets. | **Unreliable**: UDP does not guarantee the delivery of data packets. Packets may be lost, duplicated, or arrive out of order. |
| **Flow Control**: TCP uses flow control mechanisms to avoid overwhelming the receiver with too much data at once. | **No Flow Control**: UDP does not have flow control mechanisms, which can result in the receiver being overwhelmed with data. |
| **Error Checking**: TCP includes error-checking mechanisms to detect corrupted data packets. | **Minimal Error Checking**: UDP includes a simple checksum for error checking but does not provide mechanisms for retransmission. |
| **Congestion Control**: TCP has congestion control mechanisms to avoid network congestion. | **No Congestion Control**: UDP does not have built-in congestion control mechanisms. |

1. Automation Port Info

|  |  |
| --- | --- |
| Ansible (TCP) | Port 22 > ssh to push config file > Python > Open source > YAML for fundamental config |
| Puppet (TCP) | Port 8140 > Pull > Ruby > Proprietary |
| Chef (TCP) | Port 10002 > Pull > DSL based on Ruby > Open source > Port 443 also use > Manifest |

1. Non-Overlapping 2.4G channels

|  |
| --- |
| 1,6,11 |

1. North Bound Interface & South Bound Interface

|  |  |
| --- | --- |
| SBI | NBI |
| OpenFlow - imperative SDN | REST API   * uses HTTP messages to transfer data to applications residing on different hosts |
| OpFlex – declarative SDN |  |
| Cisco onePK – cisco - Java,c,python – ssl & tls |  |
| NETCONF – Use XML, SSH |  |

1. South Bound interface

|  |  |
| --- | --- |
| OpenFlow | OpenFlow is a well-known southbound API. OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements. |
| OpFlex | An open-standard, distributed control system. It send ג€summary policyג€ to network elements. |
| onePK | a Cisco proprietary SBI to inspect or modify the network element configuration without hardware upgrades. |
| The Network Configuration Protocol (NetConf) | uses Extensible Markup Language (XML) to install, manipulate and delete configuration to network devices. |

1. Your summary of HTTP status codes

|  |
| --- |
| 1xx-informational, the request was received.  2xx-Successful, request successfully received.  3xx-Redirection, further action need to be taken.  4xx-Client error, syntax error.  5xx-Server error, server failed. |

1. HTTP methods used in REST API

|  |  |
| --- | --- |
| GET: retrieve data |  |
| POST: create data |  |
| PUT: fully update (i.e. replace) an existing record |  |
| PATCH: update part of an existing record |  |
| DELETE: delete record |  |

1. Non-idempotent HTTP methods Vs Idempotent HTTP methods

|  |  |
| --- | --- |
| **Non-Idempotent Methods**: | **Idempotent Methods**: |
| A non-idempotent operation refers to a command or action that, when executed multiple times, **does not produce the same result each time** | Focus on networking commands and configurations that **yield the same result when applied multiple times** |
| POST | GET |
|  | PUT |
|  | DELETE |
|  | HEAD |

1. SOAP vs REST
2. SOAP vs REST
3. SOAP vs REST
4. SOAP vs REST

A table with text and images

Description automatically generated

1. AAA – Accounting/Authentication/Authorization

|  |
| --- |
| AAA stands for Authentication, Authorization and Accounting. ✑ Authentication: Specify who you are (usually via login username & password) ✑ Authorization: Specify what actions you can do, what resource you can access ✑ Accounting: Monitor what you do, how long you do it (can be used for billing and auditing) |

1. AAA – Accounting/Authentication/Authorization

|  |  |
| --- | --- |
| Authentication | Process > verifying a user’s identity = finger pattern/password |
| Authorization | Process > level access configured for a user = allowing to access a file |
| Accounting | Process > recording the use of resources |

1. RADIUS & TACACS+

A white sheet with black text

Description automatically generated

ACS – Access control server

ISE – Identity services engine

1. Security - CIA

|  |  |
| --- | --- |
| Confidentiality |  |
| Integrity |  |
| Availability |  |

1. Etherchannel

|  |  |  |
| --- | --- | --- |
| Static | LACP | PAgP |
| Mode on | Mode active/passive | Mode auto/desirable |
|  | Open Standard | Cisco Proprietary |
|  |  |  |

1. FlexConnect ACL

|  |  |
| --- | --- |
| FlexConnect ACL | Cisco Traditional ACL |
| -Only applied to Native Vlan  -Not possible when inherited from a flexconnect group |  |
| -applied per AP, per VLAN |  |
| -All the rules only can apply inbound or outbound | -per rule can specify the direction |
| -By default, implicit deny rule | -By default, implicit deny rule |

1. MAC

|  |
| --- |
| Multicast |
| Broadcast |
|  |
|  |

1. Security Violation mode

|  |  |
| --- | --- |
| Shutdown | Err-disabled, one time = Generate syslog, Increment violation counter once |
| Restrict | Discards traffic from unauthorized MAC, interface isn’t disabled, each time send syslog, each time increment violation counter |
| Protect | Discards traffic from unauthorized MAC, interface isn’t disabled, doesn’t send syslog, doesn’t increment violation counter |

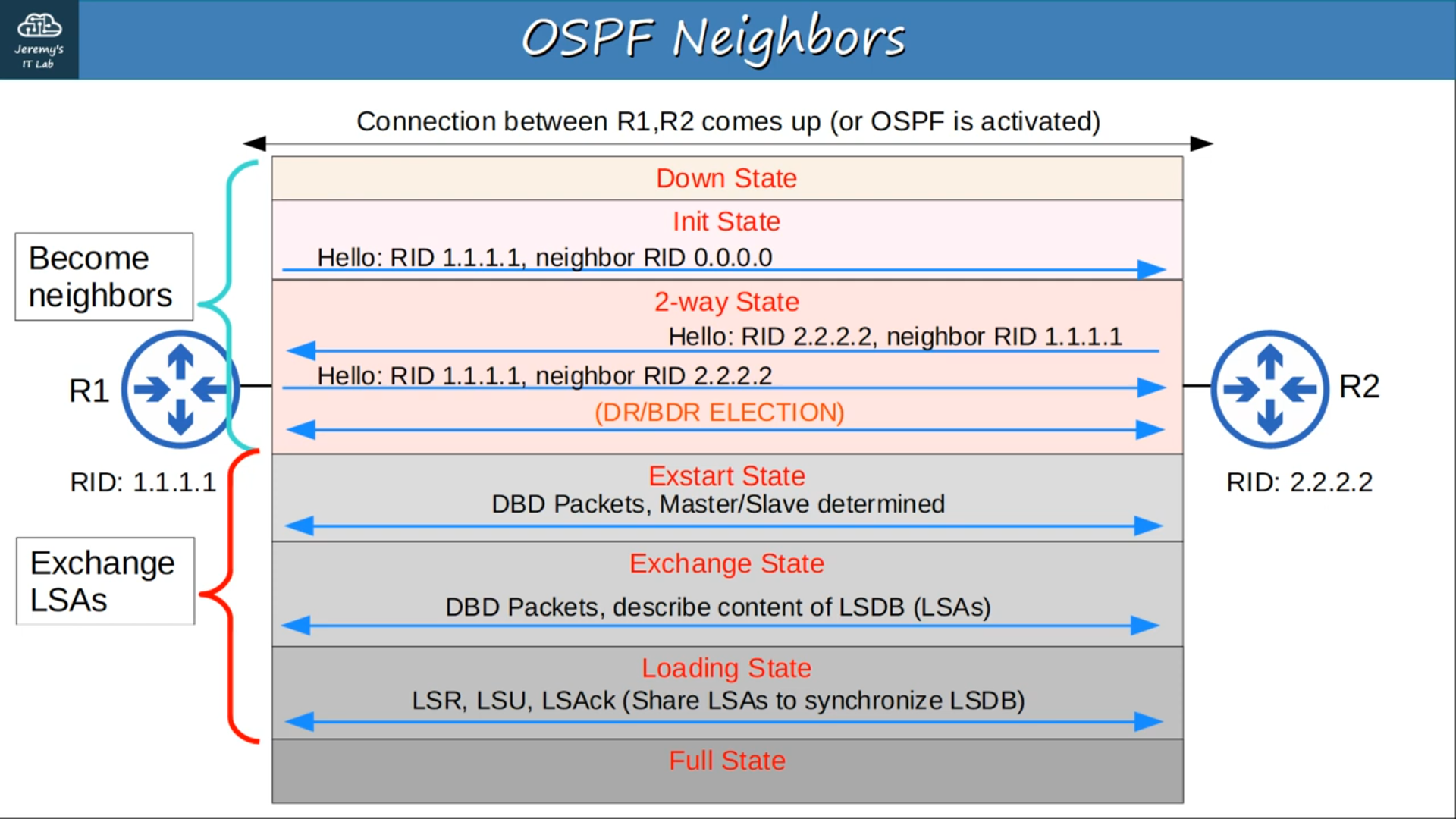
1. Abbreviation

|  |  |
| --- | --- |
| WRED  RED | Weighted Random Early Detection  Random Early Detection |
| DSCP | Differentiated Services Code Point |
| TACACS | Terminal Access Controller Access-Control System |
| RADIUS | Remote Authentication Dial-In User Service |
| RC4 | Rivest Cipher 4 |
| TKIP |  |
| CCMP |  |
| GCMP |  |
| ACS | Access control server – cisco – TACAS+ - TCP – 49 |
| ISE | Identity service engine – RADIUS – UDP - 1812,1813 - |
| SAE | Simultaneous Authentication of Equals |
| PFS | Perfect Forward Secrecy |
| OWE | Opportunistic Wireless Encryption |
| IPsec over GRE | Generic Routing Encapsulation |
| PKI | public key infrastructure |
| CA |  |
| CRL |  |
| AH | Authentication Header |
| ESP | Encapsulating Security Payload |
| JWT | JSON Web Token |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. OSPF Network type

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | DR and BDR election | Hello/Dead | Neighbour cmd | Interface |
| Broadcast | Performed | 10/40 | Not Required | Ethernet/FDDI = Fiber distributed data interface |
| Non-Broadcast | Performed | 30/120 | Required | Frame Relay/x.25 |
| Point to Point | Not Performed | 10/40 | Not Required | PPP/HDLC = High level data link control |
| Point to Multipoint Broadcast | Not Performed | 30/120 | Not Required | na |
| Point to Multipoint  Non-Broadcast | Not Performed | 30/120 | Required | na |

1. OSPF Neighbour selection process & 7 Steps



1. Split MAC Address

|  |  |
| --- | --- |
| WLC | LAP |
| Authentication | Beacon and probe |
| Roaming reauthorization | Encryption and decryption |
| switch between protocol | packet ack and retransmission |
| converting to wired network | Queueing and priority |
|  |  |

1. Wireless Security

Authentication Method = 1) Open system authentication, 2) Psk – Pre-Shared Key

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication Method | Encryption Method | Description |  |
| WEP | RC4 | Key never change when exchanging |  |
| WAP | TKIP | Encrypt L2 Payload with TKIP  also do MIC |  |
| WAP2 | AES - CCMP | Destination Host will determine.  if the encrypted and non-encrypted bits have been altered | AES – 128  Encryption  CCMP is an encryption protocol based on the Advanced Encryption Standard (AES) algorithm. It provides both encryption and data integrity by combining the Counter Mode (CTR) for encryption and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for data integrity.  WPA3 (Wi-Fi Protected Access 3) and WPA2 (Wi-Fi Protected Access 2) are the latest and most commonly used wireless security standards. Both WPA3 and WPA2 support the use of CCMP as the encryption and integrity protocol for securing wireless communications. |
| WAP3 | GCMP = Galois Mode Protocol  pre-shared key or 802.1x authentication, GCMP, SAE, and forward secrecy. | More efficient than CCMP  Simultaneous Authentication of Equals (SAE) A strong authentication method used in WPA3 to authenticate wireless clients and APs and to prevent dictionary attacks for discovering pre-shared keys. | WPA3 – Enterprise GCMP – 256  Encryption  WPA3 – Personal  CCMP128  Encryption  WPA3 is the wireless security protocol that relies on Perfect Forward Secrecy (PFS). It uses the Simultaneous Authentication of Equals (SAE) protocol, also known as Dragonfly, to provide PFS for each Wi-Fi session, making it much more secure than its predecessors (WPA2 and WPA) in terms of key management and encryption. |

1. WPA 2 and WPA 3

|  |  |  |
| --- | --- | --- |
| WPA | WPA 2 | WPA 3 |
| WPA has two modes of operation:  **Personal mode**  **Enterprise mode.** | WPA2 uses 128-bit key encryption with AES | while WPA3 supports 128-bit and 192-bit key encryption with AES and the new SAE protocol for key establishment. |
| **WPA-Personal mode** uses PSK authentication, WPA-PSK (Pre-Shared Key),  **WPA-Enterprise mode** uses RADIUS server authentication  WPA-EAP (Extensible Authentication Protocol | **AES-CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)** with a 128-bit key. Therefore, the key length for AES in WPA2 is **128 bits**. | GCMP-256 (Galois/Counter Mode Protocol) cipher suite, which uses a 256-bit encryption key |
|  |  |  |
|  |  |  |
|  |  |  |

1. WLAN QoS Profile

|  |  |
| --- | --- |
| Profile Name | Description |
| Bronze | For Background |
| Gold | For Video Applications |
| Platinum | For Voice Applications |
| Silver | For Best Effort |

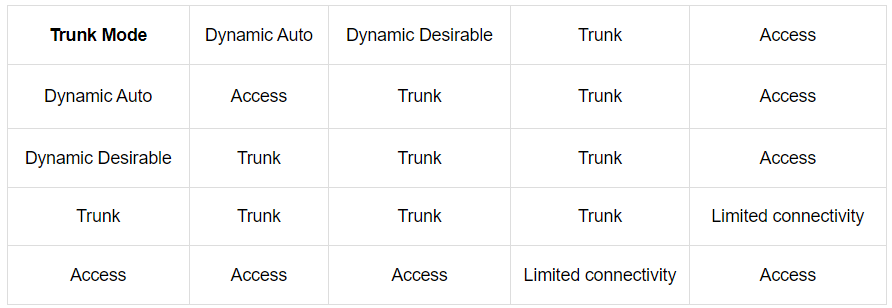
1. Automation network management tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tool | Push/Pull model | Client Agent | Port/Protocol | Description |
| Ansible | Push | No need | 22/SSH or NETCONF | 1)Playbook  2)Inventory  3)Templates  4)Variables |
| Puppet | Pull | -Client Agent based  -Proxy server agent = helping with agentless device with ssh login | HTTP(REST)  TCP = 8140 | 1)Manifest  2)Resource, Class, Module  3)Template |
| Chef | Pull | Agent based | HTTP(REST)  TCP = 10002 | 1)Resource  2)Recipe  3)Cookbook  4)Run list |

1. Ansible

|  |  |
| --- | --- |
| Control Node: | device with Ansible installed that manages target devices. |
| Inventory: | Ansible file that defines the target devices upon which commands and tasks can be executed. |
| Managed Node: | network device, without Ansible installed, upon which commands can be executed. |
| Module: | specific action to be performed on one or more target devices. |
| Playbook: | collection of actions to perform on target devices, expressed in YAML format. |
| Task: | While the description provided seems to indicate a Python code unit, in Ansible's context, a task should be a directive within a playbook that tells Ansible to execute a module with specific parameters. There's a mismatch in the description here, as Ansible tasks are not standalone Python code units. |
|  |  |

1. DTP



1. VTP

|  |  |  |
| --- | --- | --- |
| VTP client | VTP server | VTP transparent |
| Switch using this mode can’t change its VLAN configuration.  That means that a VTP client switch cannot create or delete VLANs.  However, received VTP updates are processed and forwarded | Switch using this mode can create and delete VLANs.  A VTP server switch will propagate VLAN changes.  This is the default mode for Cisco switches. | Switch using this mode doesn’t share its VLAN database, but it forwards received VTP advertisements.  You can create and delete VLANs on a VTP transparent switch, but these changes will not be sent to other switches |

1. VTP

A white background with black text

Description automatically generated

1. Input error counter = show interface g0/0

|  |  |
| --- | --- |
| Input errors | total of many counters, including all below |
| Frame = Illegal formatting | Frames on illegal format. Can be caused by collisions |
| Giants = > 1518byte of data | Frames that exceeded the maximum size (1518 bytes) |
| CRC = FCS failure | Received frames that did not pass the FCS math |
| Runts = <64byte of data | Frames that did not meet the minimum size (64 bytes). Can be caused by collisions |

1. Input error.

|  |  |
| --- | --- |
|  | Physical cable fault |
|  | Speed mismatch / duplex |
|  | High bandwidth usage |
|  | Cable is too long |
|  |  |

1. Output error counter.

|  |  |
| --- | --- |
| Output errors |  |
| Late collisions | Collision comes to know after 64bytes of data transfer |
|  |  |

1. 802.11 Frame type

|  |  |
| --- | --- |
| Management frame | Association Request/Response  Reassociation Request/Response  Probe Request/Response  Action/Reserved  Authentication/ DE authentication  Beacon |
| Control frame | Request to Send – RTS  Clear to Send – CTS  ACK  PS-Poll  Block ACK/Block ACK Request  Beamforming Report Poll  VHT/HE NDP Announcement – Null Data  Control Wrapper  Control Frame Extension |
| Data frame | Data  null  QoS data  QoS null  Reserved |

1. WLC Layer 2 and Layer 3 Security Mechanism
2. PoE port over draw power form the port.

|  |
| --- |
| A syslog message is issued |
| Monitored port is shut down and err-disabled |
| The allocated power is freed |

1. PoE Switch Port modes

|  |  |
| --- | --- |
| Auto | Automatically detect the poe device and ensure the power delivery |
| Dynamic | Automatically detect the poe device and negotiate with power delivery as per availability and requirements from device |
| Static | This port will delivery the configure power to the port regardless of connection to the port (device connected or device doesn’t connected) |

1. Point to Point = Private WAN connection AT&T USA = T1,T2,,T3,T4 & Europe E0,E1,E2,E3,E4,E5

A white paper with black text and numbers

Description automatically generated

E1 = 2.048Mbps

E3 = 34.368Mbps

1. Subnetting Mastery

A white rectangular object with black numbers

Description automatically generated

1. Ethernet Standards

SFP-10G-SR 850 nm Multimode 300 m Duplex LC 10GBASE-SR

SFP-10G-LR 1310 nm Singlemode 10 km Duplex LC 10GBASE-LR

1. Fiber Multimode cables

|  |  |
| --- | --- |
| OM1 |  Core diameter: 62.5 micrometers   Maximum distance for 10GbE: 33 meters   Uses: Suitable for lower speed, short-distance applications (up to 1 Gb/s for 300 meters). |
| OM2 |  Core diameter: 50 micrometers   Maximum distance for 10GbE: 82 meters   Uses: Suitable for higher-speed applications than OM1, up to 1 Gb/s for 550 meters. |
| OM3 |  Core diameter: 50 micrometers   Maximum distance for 10GbE: 300 meters   Uses: Optimized for 10 Gb/s transmission, can also support 40 GbE and 100 GbE over shorter distances (up to 100 meters). |
| OM4 |  Core diameter: 50 micrometers   Maximum distance for 10GbE: 400 meters   Uses: Enhanced version of OM3, supports 10 Gb/s up to 550 meters, and can handle 40 GbE and 100 GbE over longer distances (up to 150 meters). |

1. DAGFAD
2. ADFSAF
3. WLC Component

|  |  |
| --- | --- |
| access point = | proved wireless device with connection to the wired network |
| WLC = | Manage access point |
| Service port = | out of band management of WLC |
| virtual interface = | mobility management WLC  used for guest authentication  802.1x |
| Dynamic interface = | Applied to the WLAN for wireless client communicate  Maps WLANs to VLANs and provides IP addressing |

WLC dynamic interface vs virtual interface

A screenshot of a computer

Description automatically generated

1. WLC management option.

|  |  |
| --- | --- |
| GUI Management | Secure Web interface |
| Out Of Band Management | No Regular Traffic  Dedicated service port, Console Port |
| Secure In Band connectivity | With regular traffic – with secure protocols  SSH, HTTPS |
| Unencrypted in Band connectivity | With regular traffic – without secure  Telnet, http |
|  |  |
|  |  |

1. Interface counter = show interface g0/0
2. Access Points

|  |  |  |
| --- | --- | --- |
| Autonomous AP | Lightweight AP | Cloud Based AP |
| Requires a management IP address | Configured and managed by WLC | Managed from a web-based dashboard |
| Accessible for management via telnet,ssh, web gui | Supports different operational modes | Supports automatic deployment |
|  |  |  |

1. WLC AP or LightWeight AP Operational modes

|  |  |
| --- | --- |
| Client – Serving Cisco AP mode | Network Management Cisco AP mode |
| 1. Local mode – when it is in standby (no client using it) , It scan for interference & match against it | 1] Monitor mode – doesn’t broadcast SSID, act as a sensor, only absorb and monitor the wifi channel |
| 1. Flexconnect mode – when wlc is down, it allow ap to work as standalone share traffic between ssid and vlans | 2] Rogue Detector mode – Broadcast ssid, also detect rogue device on wired and wireless network |
| 1. Bridge mode or Mesh mode | 3] SE – connect mode – analysis & collect the data about all wireless channels to discover source of interference |
| 1. Flex+bridge mode | 4] Sniffer mode – doesn’t broadcast ssid, collect the wifi signal data and store it, for later wireshark analysis |
|  |  |
|  |  |

1. SPT vs RSTP vs MSTP

|  |  |  |
| --- | --- | --- |
| Difference between Spanning Tree versions: MSTP vs RSTP vs STP vs PVSTP | | |
| **STP** | **RSTP (Rapid Per-Vlan Spanning Tree)** | **MSTP** |
| Its IEEE standard is 802.1D. | Its IEEE standard is 802.1W. | Its IEEE standard is 802.1S. |
| IEEE 802.1D is the first child of the STP family. | IEEE 802.1W is the successor and an improved version of STP. | IEEE 802.1S is built on top of RSTP to group VLANs into instancesfor scalability, ease of management, security, etc. |
| STP results in slower network convergence and not so robust when compared to RSTP and MSTP.  It will take 30 to 50 Seconds | On the other hand, RSTP significantly accelerates network convergence and is more robust than STP. | RSTP is the underlying protocol for MSTP, and that is why it also provides faster convergence similar to RSTP.But it has more features than RSTP. |
| Deployment of STP is more straightforward than RSTP and MSTP. | RSTP deployment is easier when compared to MSTP. | MSTP needs a proper understanding of STP and additional MSTP concepts before deployment.Which makes it harder to deploy and the reason sometimes network engineers opt for RSTP instead. |
|  | Cisco proprietary, limited to Cisco equipment. |  |
| STP has three port functions:-  Root PortDesignated PortBlocked Port | RSTP utilises four ports:-Root PortDesignated Port,Alternate PortBackup Port | MSTP has five-port roles:-Root PortDesignated PortAlternate port,Backup PortMaster port |
| STP supports five different port states:-  Forwarding  Learning  Listening  Blocking  Disabled | RSTP is composed of three-port states:-  Forwarding  Learning  Discarding  (It replaces Forwarding, Learning, and Listening for fast convergence.) | Since MSTP is built on top of RSTP, it has the same three port states:-  Forwarding  Learning  Discarding |
| It lacks all link types. | It supports two types of links: shared links and point-to-point links. | It also has two link types, i.e., Shared link and Point to point link. |
| STP use only 2 bits from the flag octet:Bit 7: Topology Change Acknowledgment.Bit 0: Topology Change | In RSTP, the following flag bits are used:Bit 0 for TCNBit 1 for ProposalBits 2 and 3 for Port roleBit 4 for LearningBit 5 for forwardingBit 6 for AgreementBit 7 for TCN | Same as RSTP. |
| In STP, the root bridge is the only one that sends BPDUs.Others then transfer BPDUs (Bridge protocol data units). | All bridges in RSTP are capable of forwarding BPDUs. | In MSTP, all bridges can forward BPDUs. |
| In the Spanning Tree Protocol, when a bridge detects a change in the network,it notifies the root, who then notifies all others via BPDU with the TCA bit set,instructing them to clear their database entries when the "short-timer" (Forward delay) expires. | In RSTP, TC (Topology change) is flooded throughout the network;each bridge generates TC (Topology change) and notifies its neighborswhen a topology change occurs, immediately deleting old database entries. | Same as RSTP. |
| If a non-root bridge does not receive Hello after 10\*Hello (advertised from the root),the non-root bridge should begin claiming the root role by generating its own Hello. | On the other hand, RSTP does not act untilit receives 3\*Hello on a root port (advertised from the root). | Same as RSTP. |
| STP waits until all TC have reached the root and the short timer (Forward delay)has expired before flashing all root database entries. | RSTP immediately deletes all local databases except forthe MAC of the port receiving the topology changes (proposal) | Same as RSTP. |
| STP is compatible with RSTP and MSTP. But it is always advisable to check with thedevice vendor before deploying more than one Spanning tree Protocol type in your network. | Rapid Spanning Tree Protocol is backward compatible with STP. | MSTP has CST (Common Spanning Tree) Instance, which is backward compatible with the RSTP and STP. |
| Load balancing or utilizing multiple physical paths in the network is not possible with STP.All VLANs have to follow the same Spanning Tree path. | Same as STP. | Contrary to STP and RSTP, with MSTP, you can group VLANs into separate MST Instances and canutilize multiple physical paths. |
| Ports connected to endpoints (laptops, computers, printers, etc.) cannot be configured as anedge port for fast transition. There is no concept of edge ports in STP. | When connected to endpoints while in RSTP, these ports can be configuredas edge, ports to allow for rapid changes in the forwarding state. | Boundary ports are ports at the edge of an MST region that are connected to eitheran STP or RSTP bridge or an endpoint. |

1. STP VS Rapid PVST VS Rapid PVST+

|  |  |  |
| --- | --- | --- |
| SPT | Rapid PVST | Rapid PVST+ |
| Blocking  Forwarding  Listening  Learning | Discarding  Learning  Forwarding | Blocking  Learning  Forwarding  Disabled |
|  |  |  |
|  |  |  |
|  |  |  |

1. Domain name configure

|  |  |
| --- | --- |
| DNS domain name configure – While doing ssh server | (config)#ip domain-name example.com |
| VTP domain name configure | (config)#vtp domain EXAMPLE |
| DHCP dns server ip configure | (dhcp-config)#dns-server 8.8.8.8 |
|  |  |
|  |  |
|  |  |

1. Latency Vs Jitter

|  |  |
| --- | --- |
| Latency | Jitter |
| TCP | UDP |
| 30 – 40 ms best | Below 30ms is best |
| Ping test  ICMP  Sender to receiver then receiver to sender one hole round | NTP  Calculated based on time different between sender to receiver |

1. ADGADF
2. RGAG
3. SFGSFH
4. SRHFSRHF
5. Guhiu

Port Security

Interface config mode

#no switchport port-security mac-address sticky

>en

#sh interface g0/1 switchport

#sh interface g0/1

POE

Sh power inline

show power inline police

int g0/0

power inline police action (log | errdisable)

IPSec tunnel mode vs IPSec transport mode

IPsec over GRE

* IPsec over GRE (Generic Routing Encapsulation) is a mechanism that can be used to carry multicast traffic between remote sites and supports encryption. It combines the functionality of both IPsec and GRE to provide secure and efficient communication between sites.
* With IPsec over GRE, the multicast traffic is encapsulated inside a GRE tunnel, and the tunnel is then protected using IPsec encryption.
* This allows the multicast traffic to be securely transmitted over the public internet or other untrusted networks.

IPSec - IPsec (Internet Protocol Security)

ipsec suit

|  |  |
| --- | --- |
| Authentication Header (AH): | Encapsulating Security Payload (ESP): |
|  |  |
|  |  |

Cisco VPN technology for Multiple branch office

|  |  |
| --- | --- |
| GETVPN | DMVPN |
| GETVPN (Group Encrypted Transport VPN): GETVPN is a Cisco VPN technology that provides secure and scalable VPN connectivity for multiple branch offices and large-scale deployments. It uses a group-based encryption mechanism to encrypt traffic between sites, allowing for efficient and scalable encryption across the network. GETVPN is particularly suitable for deployments with high bandwidth requirements and complex routing environments. | DMVPN (Dynamic Multipoint VPN): DMVPN is another Cisco VPN technology designed for scalable and dynamic VPN deployments. It allows for the creation of secure overlay networks over public or private WAN connections. DMVPN provides efficient and scalable connectivity between multiple branch offices by using a combination of IPsec, GRE (Generic Routing Encapsulation), and NHRP (Next Hop Resolution Protocol). It simplifies the configuration and management of VPN connections, making it well-suited for large-scale deployments. |

Dhcp snooping

* Prevent >> Man in the middle >>> Dhcp starvation.
* By doing Trusted and untrusted ports
* Check the untrusted port dhcp offer message and drop it
* DHCP messages DHCPACK, DHCPNAK, DHCPOFFER originating from a DHCP server that is not trusted

Dynamic arp inspection

* Prevent >>> Man in the middle >>> Arp snooping.
* Attacker will copy Gateway MAC and act as a Rouge Gateway
* Attacker will copy client mac and act as a client.
* Trusted and untrusted Port
* In untrusted Port
* checks dst mac is match with target mac or not
* Match equal forward
* Unmatch equal drop
* check for dst mac in dhcp snooping table
* If found Matching entry equal forward
* Unmatch equal drop

Wireless Topology

1) Infrastructure

2) Adhock

3) Mesh

AP Architecture

1) Autonomous AP

2) Cloud Based AP

3) Lightweight AP

Lightweight AP

LAP – Lightweight Access Point

WLC – Wireless Lan Controller

LWAPP – Lightweight Access Point Protocol

CAPWAP – Control and Provisioning Wireless Access Points

UDP 5246 Control

UDP 5247 Data

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Monitor | Sensor | Sniffer |  |  |  |
| Analyzes wireless frames on a remote device | Wireless performance Tesing | Real-time wifi client troubleshoot when network engineers are offsite |  |  |  |
| RFID-tag Location tracking | Can capture the packets on a specific wireless  channel | Air-quality data and interference detection across all enabled channels |  |  |  |
|  |  |  |  |  |  |

Split MAC Address

LAP

1) Becon and probe

2) Encryption and decryption

3) packet ack and retransmission

4) Queueing and priority

WLC

1) Authentication

2) Roaming reauthorization

3) switch between protocol

4) converting to wired network

24-02-2024

Arp ACL and Dynamic arp inspection.

device# configure terminal

device(config)# arp access-list host2

device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0000.0011.0022

device# configure terminal

device(config)# arp access-list arp\_acl\_1

device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222

device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223

device(config-arp-acl)# exit

device(config)# vlan 200

device(config-vlan-200)# ip arp inspection filter arp\_acl\_1

device(conf-vlan-200)# ip arp inspection

device# configure terminal

device(config)# arp access-list arp\_acl\_2

device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222

device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223

device(config-arp-acl)# exit

device(config)# interface ethernet 1/2

device(conf-if-eth-1/2)# switchport

device(conf-if-eth-1/2)# ip arp inspection filter arp\_acl\_2

27-02-2024

NTP

1)Server Mode

2)Server/Client Mode

3)Client Mode

1)Server Mode

Router(config)#ntp master [stratum level] #### Default value is 7 ####

Router(config)#ntp source [Interface / IP address of NTP Source]

By Default router comes up with server/client to restrict to act as a server only - Will act only as a server

Router(config-if)#ntp broadcast

2)Server/Client Mode

Router(config)#ntp server [NTP Source IP Address]

R2(config)#ntp server 100.0.0.1

3)Client Mode

Router(config)#ntp server [NTP Server IP address]

Router(config-if)#ntp broadcast client

To Update time from Internet

#conf t

#clock timezone SGT +8

#ntp server time.google.com

#ntp server 8.8.8.8

#show clock

#show clock details

#show ntp status

#show ntp aasociations

03-04-2024

spanning-tree vlan 750 primary 0

Spanning-tree vlan 750 Root primary

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

Lldp tlv-select

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