**CCNA Notes**

**Show interfaces command.**

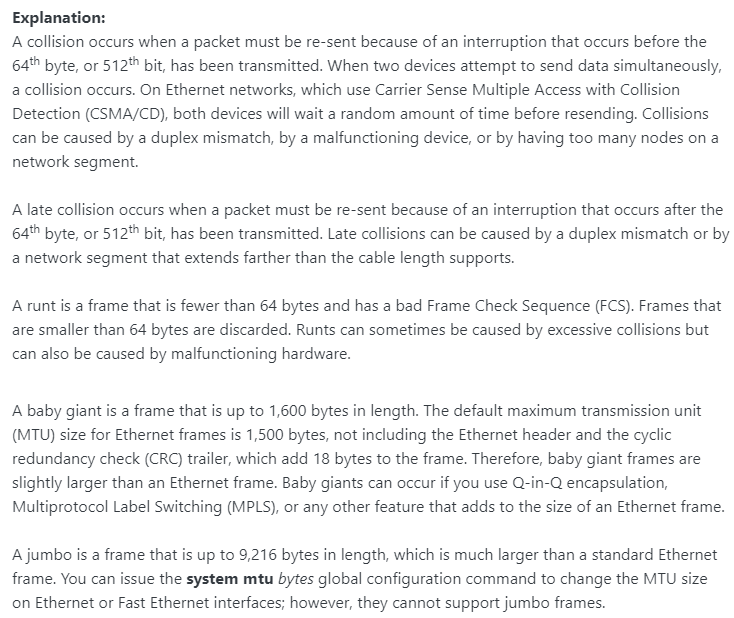
Runt Frames - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts

Giants - Ethernet frames that are longer than the maximum allowed length are called giants.

CRC errors - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or using the incorrect cabling type. If you see many CRC errors, there is too much noise on the link and you should inspect the cable for damage and length. You should also search for and eliminate noise sources, if possible. (the CRC errors grow, but the collisions counters do not, the problem might simply be interference on the cable.)

Collisions - Collisions in half-duplex operations are completely normal and you should not worry about them, as long as you are pleased with half-duplex operations.

Late collisions - A late collision refers to a collision that occurs after 512 bits of the frame (the preamble) have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration.



**802.11 management frame type**

Association request frame – (0x00) Sent from a wireless client, it enables the AP to allocate resources and synchronize. The frame carries information about the wireless connection including supported data rates and SSID of the network to the wireless client that wants to associate. If the request is accepted, the AP reserves memory and establishes an association ID for the device.

Association response frame – (0x01) Sent from an AP to a wireless client containing the acceptance or rejection to an association request. If it is an acceptance, the frame contains information, such as an association ID and supported data rates.

Reassociation request frame – (0x02) A device sends a reassociation request when it drops from range of the currently associated AP and finds another AP with a stronger signal. The new AP coordinates the forwarding of any information that may still be contained in the buffer of the previous AP.

Reassociation response frame – (0x03) Sent from an AP containing the acceptance or rejection to a device reassociation request frame. The frame includes information required for association, such as the association ID and supported data rates.

Probe request frame – (0x04) Sent from a wireless client when it requires information from another wireless client.

Authentication frame – (0x0B) The sending device sends an authentication frame to the AP containing its identity.

**HTTP methods used with REST-Based APIs**

GET: retrieve data

POST: create data

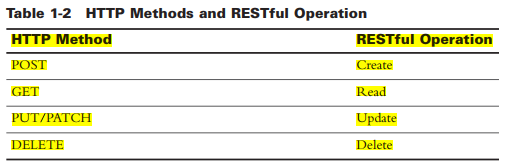
PUT: fully update (i.e., replace) an existing record

PATCH: update part of an existing record

DELETE: delete records

PUT is similar to POST in that it can create resources, but it does so when there is a defined URL wherein PUT replaces the entire resource if it exists or creates new if it does not exist.

Unlike PUT Request, PATCH does partial update. Fields that need to be updated by the client, only that field is updated without modifying the other field.



**Wi-Fi terms**

A Wireless **Distribution System** (WDS) lets you connect multiple access points together. WDS allows the connected access points to communicate with each other via wireless connection. This feature enables clients who roam to have a seamless experience. This makes it easier to manage multiple wireless networks as well as reduces the amount of cables required to connect the networks.

Reference: <https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb2040-connect-multiple-access-points-together-through-wireless-dis.html>

Access Points are limited devices. They can cover a Basic Service Area (BSA) and it is called a Cell. But in many companies network area is very large that only one Access Point can not cover all the area. So, additional Access Points are used to cover all the area. This Access Points are connected through an Ethernet Switch and they become a single continuous and seamless connection from the client perspective. User can go from one cell to another without connection interrupt. So, combining one more Access Point in a switched network is called **Extended Service Set** (ESS).

Reference: <https://ipcisco.com/lesson/wireless-principles/>

**Independent Basic Service Set** (IBSS), as the name suggests, is a service set that allows wireless devices or stations to communicate with each other without any medium or central device. It does not contain or include any AP (Access Point). That’s why it is also known as an ad hoc mode or peer to peer network.

**Extended Service Set** (ESS): uses more than one AP to create a WLAN, allows roaming in a larger area than a single AP.

**Infrastructure mode** is an 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network.

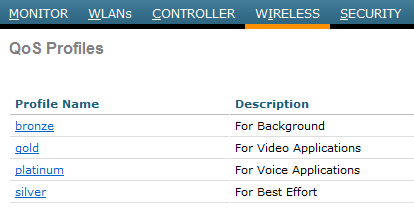
**SNMP fault-management**

+ The network management system launches a preconfigured script to restore functionality: restoration of service  
+ The administrator can manually intervene at the source of the fault: problem resolution  
+ The system identifies performance degradation or service interruption: fault detection  
+ The system groups alarms from related issues: event correlation and aggregation  
+ The system reports on the source of the issue: fault diagnosis and isolation.

**IPv6 DNS Record types**

* [A](https://simpledns.plus/help/a-records) (Host address)
* [AAAA](https://simpledns.plus/help/aaaa-records) (IPv6 host address)
* [ALIAS](https://simpledns.plus/help/alias-records) (Auto resolved alias)
* [CNAME](https://simpledns.plus/help/cname-records) (Canonical name for an alias)
* [MX](https://simpledns.plus/help/mx-records) (Mail eXchange)
* [NS](https://simpledns.plus/help/ns-records) (Name Server)
* [PTR](https://simpledns.plus/help/ptr-records) (Pointer)
* [SOA](https://simpledns.plus/help/soa-records) (Start Of Authority)
* [SRV](https://simpledns.plus/help/srv-records) (location of service)
* [TXT](https://simpledns.plus/help/txt-records) (Descriptive text)

**QoS Levels for Wireless**



**Cisco Unified Wireless Network solution WLANs support four “levels of QoS”:**

Platinum - Voice,

Gold - Video,

Silver - Best Effort (default)

Bronze - Background.

**Table 3-3 Popular Applications and Their Well-Known Port Numbers**

|  |  |  |  |
| --- | --- | --- | --- |
| Port Number(s)  20 | Protocol  TCP | Application  FTP data | access-list Command Keyword ftp-data |
| 21 | TCP | FTP control | ftp |
| 22 | TCP | SSH | — |
| 23 | TCP | Telnet | telnet |
| 25 | TCP | SMTP | smtp |
| 53 | UDP, TCP | DNS | domain |
| 67 | UDP | DHCP Server | bootps |
| 68 | UDP | DHCP Client | bootpc |
| 69 | UDP | TFTP | tftp |
| 80 | TCP | HTTP (WWW) | www |
| 110 | TCP | POP3 | pop3 |
| 161 | UDP | SNMP | snmp |
| 443 | TCP | SSL | — |
| 514 | UDP | Syslog | — |
| 16,384–32,767 | UDP | RTP (voice, video) | — |

**Most Usable AD Values**

Table

Description automatically generated

**Understanding JSON Syntax**

{

"first\_name" : "Sammy",

"last\_name" : "Shark",

"location" : "Ocean",

"online" : true,

"followers" : 987

}

this demonstrates that the format is generally set up with two curly braces (or curly brackets) that are represented with { } on either end of it, and with key-value pairs populating the space between. Most data used in JSON ends up being encapsulated in a JSON object.

Key-value pairs have a colon between them as in "key" : "value". Each key-value pair is separated by a comma, so the middle of a JSON lists as follows: "key" : "value", "key" : "value", "key": "value". In the previous example, the first key-value pair is "first\_name" : "Sammy".

JSON keys are on the left side of the colon. They need to be wrapped in double quotation marks, as in "key", and can be any valid string. Within each object, keys need to be unique. These key strings can include whitespaces, as in "first name", but that can make it harder to access when you’re programming, so it’s best to use underscores, as in "first\_name".

JSON values are found to the right of the colon. At the granular level, these need to be one of following six data types:

* strings
* numbers
* objects
* arrays
* Booleans (true or false)
* null

At the broader level, values can also be made up of the complex data types of JSON object or array, which is discussed in the next section.

Each of the data types that are passed in as values into JSON will maintain their own syntax, meaning strings will be in quotes, but numbers will not be.

With .json files, you’ll typically get a format expanded over multiple lines, but JSON can also be written all in one line, as in the following example:

{ "first\_name" : "Sammy", "last\_name": "Shark", "online" : true, }

This is more common within another file type or when you encounter a JSON string.

Writing the JSON format on multiple lines often makes it much more readable, especially when dealing with a large data set. Because JSON ignores whitespace between its elements, you can space out your colons and key-value pairs in order to make the data even more human readable:

{

"first\_name" : "Sammy",

"last\_name" : "Shark",

"online" : true

}

It is important to keep in mind that though they appear similar, a JSON object is not the same format as a JavaScript object, so though you can use functions within JavaScript objects, you cannot use them as values in JSON. The most important attribute of JSON is that it can be readily transferred between programming languages in a format that all of the participating languages can work with. In contrast, JavaScript objects can only be worked with directly through the JavaScript programming language.

**configuration management terms**

+ easy-to-manage deployment option that may lack scalability: agent  
+ device hardware that runs without embedded management features: agentless  
+ to automatically install or deploy a configuration or update: pull  
+ daemon that determines when the central authority has updates available: provision  
+ model in which the central server sends updates to nodes on an as-needed basis: push

|  |  |
| --- | --- |
| STP Variety | Description |
| STP | This is the original IEEE 802.1D version (802.1D-1998 and earlier) that provides a loop-free topology in a network with redundant links. Also called Common Spanning Tree (CST), it assumes one spanning tree instance for the entire bridged network, regardless of the number of VLANs. |
| PVST+ | Per-VLAN Spanning Tree (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard. |
| RSTP | Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w is an evolution of STP that provides faster convergence than STP. |
| 802.1D-2004 | This is an updated version of the STP standard, incorporating IEEE 802.1w. |
| Rapid PVST+ | This is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. Each separate instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard. |
| MSTP | Multiple Spanning Tree Protocol (MSTP) is an IEEE standard inspired by the earlier Cisco proprietary Multiple Instance STP (MISTP) implementation. MSTP maps multiple VLANs into the same spanning tree instance. |
| MST | Multiple Spanning Tree (MST) is the Cisco implementation of MSTP, which provides up to 16 instances of RSTP and combines many VLANs with the same physical and logical topology into a common RSTP instance. Each instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard. |

**RSTP and STP Port Roles**

RSTP Role STP Role Definition  
**Root port** — Root port A single port on each nonroot switch in which the switch hears the best BPDU out of all the received BPDUs.  
**Designated port** — Designated port Of all switch ports on all switches attached to the same segment/ collision domain, the port that advertises the “best” BPDU.  
**Alternate port** — A port on a switch that receives a suboptimal BPDU.  
**Backup port** — A nondesignated port on a switch that is attached to the same segment/collision domain as another port on the same switch  
**Disabled** — A port that is administratively disabled or that is not capable of working for other reasons

**SLAAC**SLAAC uses **ICMPv6 Router Solicitation (RS) and Router Advertisement (RA) messages to  
provide addressing and other configuration information. A client then uses the RA information  
to build an IPv6 address and verify it with a special type of Neighbor Solicitation (NS) message  
through duplicate address detection (DAD). These three message types—RS, RA, and NS—belong  
to the Neighbor Discovery Protocol**:  
■ **Router Solicitation (RS) message:** When a client is configured to obtain its **addressing  
information automatically using SLAAC**, the client **sends an RS message to the router**.  
The RS message is sent to the IPv6 **all-routers multicast address, FF02::2.**■ **Router Advertisement (RA) message:** A client uses this information to **create its own IPv6  
global unicast address**. A router sends RA messages periodically or in response to RS messages.  
An **RA message includes the prefix and prefix length of the local segment**. By default, Cisco  
routers send RA messages **every 200 seconds**. RA messages are sent to the **IPv6 all-nodes  
multicast address, FF02::1.**  
■ **Neighbor Solicitation (NS) message:** An NS message is normally used to learn the  
data link layer address of a neighbor on the same network. In the **SLAAC process, a host  
uses DAD by inserting its own IPv6 address as the destination address in an NS message.**  
**The NS message is sent out on the network to verify that a newly minted IPv6 address is  
unique. If a Neighbor Advertisement message is received, the host knows that the IPv6 address  
is not unique.**

**An RA message informs a client how to obtain automatic IPv6 addressing: using SLAAC, DHCPv6,  
or a combination of the two.** The RA message contains two flags to indicate the configuration  
option: the **Managed Address Configuration flag (M flag) and the Other Configuration flag (O flag)**.  
The default setting for **these flags is 0, or both bits off**. To the client, this means it is to use the  
SLAAC process exclusively to obtain all of its IPv6 addressing information. If either of these flags is  
set to 1 for some reason, you can use the **no** form of the following **ipv6 nd** commands in interface  
configuration mode to reset them to 0:

**Stateless DHCPv6  
In stateless DHCPv6, the client uses the RA message from the router to generate its global unicast  
address. However, the client then sends a request to the DHCPv6 server to obtain any additional  
information that the RA has not already supplied.** For stateless DHCPv6, **the O flag is set to 1** so that the client is informed that additional configuration information is available from a stateless DHCPv6 server. Use the following command on the interface to modify the RA message:

Router(config-if)# **ipv6 nd other-config-flag**

**Stateful DHCPv6**

For stateful DHCPv6, the RA message tells the client to **obtain all its addressing information from a  
DHCPv6 server.** The M flag must be set on the interface with the following command:

Router(config-if)# **ipv6 nd managed-config-flag**

**Configuring a Router as a Stateless DHCPv6 Server**

To configure R1 as a stateless DHCP server, you need to make sure that **ipv6 unicast-routing  
is enabled**. Then, in global configuration mode, configure the pool name, DNS server, and domain  
name. Finally, enable the DHCPv6 pool on the appropriate interface and **set the O flag** so that clients on that interface know to request DHCPv6 services from the router.

R1(config)# **ipv6 unicast-routing**R1(config)# **ipv6 dhcp pool O-FLAG-SET**R1(config-dhcpv6)# **dns-server 2001:db8:acad:1::5**R1(config-dhcpv6)# **domain-name cisco.com**R1(config-dhcpv6)# **exit**R1(config)# **interface g0/1**R1(config-if)# **ipv6 address 2001:db8:1:1::1/64**R1(config-if)# **ipv6 dhcp server O-FLAG-SET**R1(config-if)# **ipv6 nd other-config-flag**R1(config-if)# **end**R1# **show ipv6 dhcp pool**

To configure a **router interface as a DHCPv6 client, enable IPv6 on the interface and enter the  
ipv6 address autoconfig command**

R3(config)# **interface g0/1**R3(config-if)# **ipv6 enable**R3(config-if)# **ipv6 address autoconfig**R3(config-if)# **end**

**Configuring a Router as a Stateful DHCPv6 Server**

**The main difference between a stateless configuration and a stateful configuration is that a stateful  
server includes IPv6 addressing information and keeps a record of the IPv6 addresses that are leased  
out**. Also, for the **client side, the ipv6 address dhcp** command is used instead of the **ipv6 address  
autoconfig** command

R1(config)# **ipv6 unicast-routing**R1(config)# **ipv6 dhcp pool M-FLAG-SET**R1(config-dhcpv6)# **address prefix 2001:db8:1:1::/64 lifetime infinite infinite**R1(config-dhcpv6)# **dns-server 2001:db8:acad:1::5**R1(config-dhcpv6)# **domain-name cisco.com**R1(config-dhcpv6)# **exit**R1(config)# **interface g0/1**R1(config-if)# **ipv6 address 2001:db8:1:1::1/64**R1(config-if)# **ipv6 nd managed-config-flag**R1(config-if)# **end**

**Table 22-2 Split-MAC Functions of the AP and WLC**

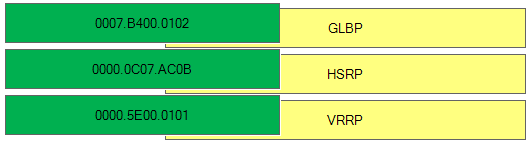
|  |  |
| --- | --- |
| **AP MAC Functions** | **WLC MAC Functions** |
| Beacons and probe | Authentication |
| Packet acknowledgments and retransmissions | Association and re-association of roaming clients |
| Frame queueing and packet prioritization | Frame translation to other protocols |
| MAC layer data encryption and decryption | Termination of 802.11 traffic on a wired interface |

**CAPWAP Operation**The division of labor between the WLC and LAPs is known as *split-MAC architecture*. The LAP must  
interact with wireless clients on some low level, known as the Media Access Control (MAC) layer.  
These functions must stay with the LAP hardware, closest to the clients. The management functions  
are not integral to handling frames but are things that should be centrally administered. Therefore,  
those functions can be moved to a centrally located platform away from the AP. Table 22-2  
summarizes MAC functions of the LAP and WLC.

**HSRP Versions**

|  |  |  |
| --- | --- | --- |
| **HSRP Feature** | **Version 1** | **Version 2** |
| Group numbers supported | 0–255 | 0-4095 |
| Authentication | None | MD5 |
| Multicast addresses | IPv4: 224.0.0.2 | IPv4: 224.0.0.102 IPv6: FF02::66 |
| Virtual MAC ranges | 0000.0C07.AC00 to 0000.0C07.ACFF | IPv4: 0000.0C9F.F000 to 0000.0C9F.FFFF IPv6: 0005.73A0.0000 to 0005.73A0.0FFF |

**HSRP Virtual MAC Address**

****

**HSRP state**

When in operation, HSRP devices are configured into one of many states:  
**Active** – This is the state of the device that is actively forwarding traffic.  
Init or Disabled – This is the state of a device that is not yet ready or able to participate in HSRP.  
**Learn** – 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.  
**Listen** – This is the state of a device that is receiving hello messages.  
**Speak** – This is the state of a device that is sending and receiving hello messages.  
**Standby** – This is the state of a device that is prepared to take over the traffic forwarding duties from the active device.

**elements of a security program**

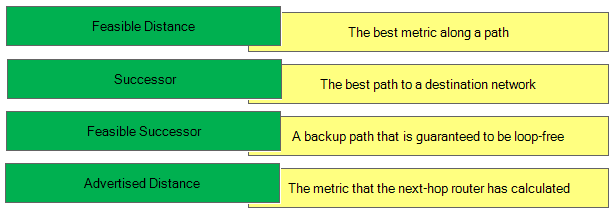
|  |  |
| --- | --- |
| user-awareness learning level that focuses on security practice that all employees must understand and enforce | awareness Correct |
| user-awareness learning level that focuses on learning about topics and practices beyond what is typically required by the user’s job | education Correct |
| tactical document that sets out specific tasks and methods to maintain security | security policy Correct |
| document that outlines an organization’s security goals and practices and the roles and responsibilities of the organization’s personnel | security standard Correct |
| user-awareness learning level that focuses on teaching employees how to perform tasks specifically required by their jobs | training |

**Cisco SDA Terms**

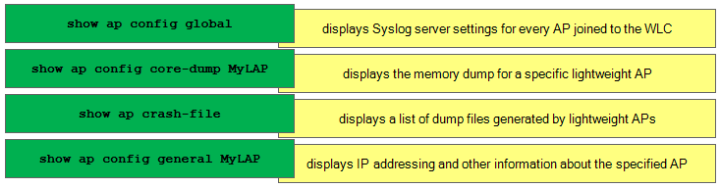
Timeline

Description automatically generated

**EIGRP Terms**



**Wireless LAN Controller CLI Commands**

****

**VTP modes:**

* **VTP client mode** – a 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.
* **VTP server mode** – a 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.
* **VTP transparent mode** – a 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.
* **VTP mode off** – similar to VTP transparent mode, with a difference that a switch using this mode will not forward received VTP updates. This command is supported only in VTP V3.

**Table

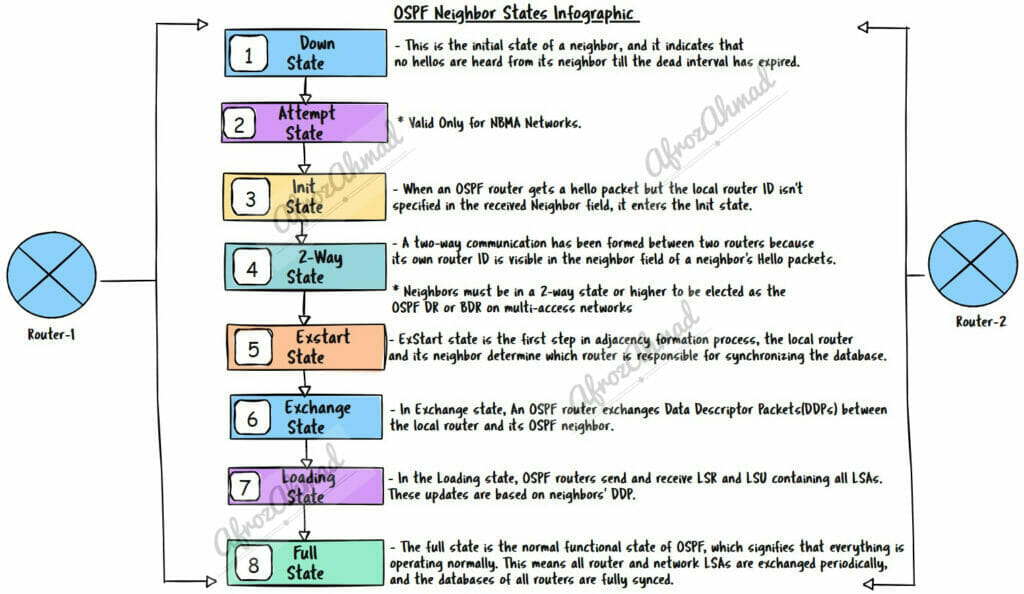
Description automatically generated with medium confidence**

**Table

Description automatically generated**

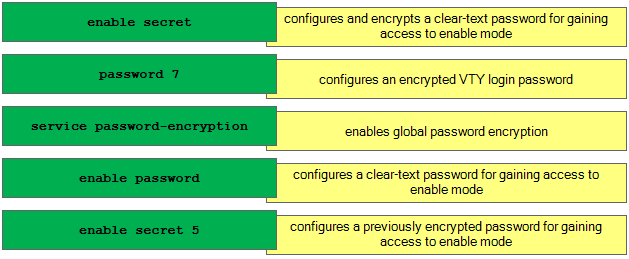
**cloud-provided services**

+ **SaaS** (Software as a Service): SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients’ side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plugins.  
+ **PaaS** (Platform as a Service): are used for applications, and other development, while providing cloud components to software. What developers gain with PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective. With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, networking, and the PaaS software itself. Developers, however, manage the applications.  
+ **IaaS** (Infrastructure as a Service): self-service models for accessing, monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, networking, and networking services (e.g. firewalls). Instead of having to purchase hardware outright, users can purchase IaaS based on consumption, similar to electricity or other utility billing.

**OSPF Neighbor Status**

**SNMP manager and agent identifier commands**

+ show snmp group: displays the SNMP security model in use  
+ show snmp community: displays the SNMP access string  
+ show snmp chassis: displays the SNMP server serial number  
+ show snmp engineID: displays the IP address of the remote SNMP device  
+ show snmp host: displays information about the SNMP recipient

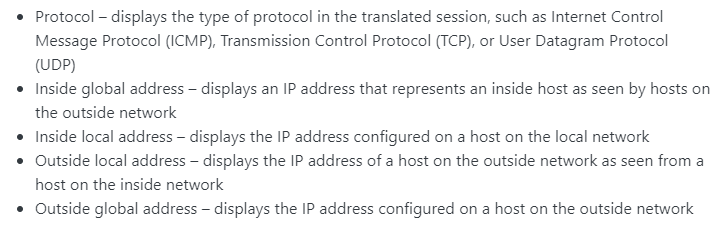
****

**Table

Description automatically generated**

**NAT Terminology**

■ Inside local address: Most likely a private address. In the figure, the IPv4 address 192.168.10.10 assigned to PC1 is an inside local address.  
■ Inside global address: A valid public address that the inside host is given when it exits the NAT router. When traffic from PC1 is destined for the web server at 209.165.201.1, R2 must translate the inside local address to an inside global address, which is 209.165.200.226 in this case.  
■ Outside global address: A reachable IPv4 address assigned to a host on the Internet. For example, the web server can be reached at IPv4 address 209.165.201.1.  
■ Outside local address: The local IPv4 address assigned to a host on the outside network. In most situations, this address is identical to the outside global address of that outside device. (Outside local addresses are beyond the scope of the CCNA.)



Popular Applications and Their Well-Known Port Numbers

|  |  |  |  |
| --- | --- | --- | --- |
| **Port Number(s)** 20 | **Protocol** TCP | **Application** FTP data | **access-list Command Keyword ftp-data** |
| 21 | TCP | FTP control | **ftp** |
| 22 | TCP | SSH | **—** |
| 23 | TCP | Telnet | **telnet** |
| 25 | TCP | SMTP | **smtp** |
| 53 | UDP, TCP | DNS | **domain** |
| 67 | UDP | DHCP Server | **bootps** |
| 68 | UDP | DHCP Client | **bootpc** |
| 69 | UDP | TFTP | **tftp** |
| 80 | TCP | HTTP (WWW) | **www** |
| 110 | TCP | POP3 | **pop3** |
| 161 | UDP | SNMP | **snmp** |
| 443 | TCP | SSL | **—** |
| 514 | UDP | Syslog | **—** |
| 16,384–32,767 | UDP | RTP (voice, video) | **—** |

SNMP consists of 3 items:

+ **SNMP Manager** (sometimes called Network Management System – NMS): a software runs on the device of the network administrator (in most case, a computer) to monitor the network.  
+ **SNMP Agent:** a software runs on network devices that we want to monitor (router, switch, server…)  
+ **Management Information Base** (MIB): is the collection of managed objects. This components makes sure that the data exchange between the manager and the agent remains structured. In other words, MIB contains a set of questions that the SNMP Manager can ask the Agent (and the Agent can understand them). MIB is commonly shared between the Agent and Manager.

Diagram

Description automatically generated

**IPv6 DNS record types**

+ correlates a domain with its authoritative name servers: NS  
+ associates the domain serial number with its owner: SOA  
+ aliases one name to another: CNAME  
+ supports reverse name lookups: PTR  
+ correlates a host name with an IP address:  AAAA

An **AAAA** record maps a domain name to the IP address (Version 6) of the computer hosting the domain. An AAAA record is used to find the IP address of a computer connected to the internet from a name. The AAAA record is conceptually similar to the A record, but it allows you to specify the IPv6 address of the server, rather than the IPv4. An example of AAAA is the ‘www’ of 9tut.com is pointed to 2001:0db8:aaaa:bbbb:cccc:dddd:eeee:ffff.

**NS** (name server) looks like a website URL, but instead of linking to a website, they link to the domain names authoritative nameservers. An example of a NS is ‘ns1.9tut.com’.

The **Canonical Name record (CNAME)** tells anyone visiting that subdomain to use the same DNS records as another domain / subdomain. If you are already using an A or AAAA record for a subdomain you wouldn’t use a CNAME. CNAME records must always point to another domain / subdomain, never directly to an IP address. For example, we can configure the CNAME of www.9tut.com points to 9tut.com so that they use the same IP address.

As opposed to forward DNS resolution (A and AAAA DNS records), the **Reverse-lookup Pointer** (PTR) record is used to look up domain names based on an IP address.

An **SOA** record or start of authority record specifies the DNS server providing authoritative information about an Internet domain, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.

An example of a SOA record is shown below.

; name TTL class rr Nameserver email-address

mydomain.com. 14400 IN SOA ns.mynameserver.com. root.ns.mynameserver.com. (

2004123001 ; Serial number

86000 ; Refresh rate in seconds

7200 ; Update Retry in seconds

3600000 ; Expiry in seconds

600 ; minimum in seconds )

name – mydomain.com is the main name in this zone.

**TTL** – 14400 – TTL defines the duration in seconds that the record may be cached by client side programs. If it is set as 0, it indicates that the record should not be cached. The range is defined to be between 0 to 2147483647 (close to 68 years !) .

**Class** – IN – The class shows the type of record. IN equates to Internet. Other options are all historic. So as long as your DNS is on the Internet or Intranet, you must use IN.

**Nameserver** – ns.nameserver.com. – The nameserver is the server which holds the zone files. It can be either an external server in which case, the entire domain name must be specified followed by a dot. In case it is defined in this zone file, then it can be written as “ns” .  
Email address – root.ns.nameserver.com. – This is the email of the domain name administrator. Now, this is really confusing, because people expect an @ to be in an email address. However in this case, email is sent to root@ns.nameserver.com, but written as root.ns.nameserver.com . And yes, remember to put the dot behind the domain name.

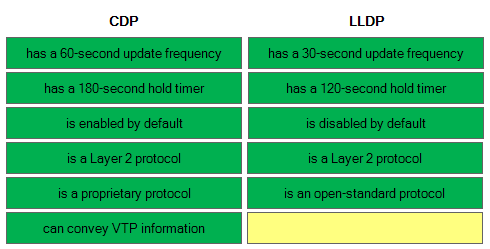
**Serial number** – 2004123001 – This is a sort of a revision numbering system to show the changes made to the DNS Zone. This number has to increment , whenever any change is made to the Zone file. The standard convention is to use the date of update YYYYMMDDnn, where nn is a revision number in case more than one updates are done in a day. So if the first update done today would be 2005301200 and second update would be 2005301201.

**Refresh** – 86000 – This is time(in seconds) when the slave DNS server will refresh from the master. This value represents how often a secondary will poll the primary server to see if the serial number for the zone has increased (so it knows to request a new copy of the data for the zone). It can be written as “23h88M” indicating 23 hours and 88 minutes. If you have a regular Internet server, you can keep it between 6 to 24 hours.

**Retry** – 7200 – Now assume that a slave tried to contact the master server and failed to contact it because it was down. The Retry value (time in seconds) will tell it when to get back. This value is not very important and can be a fraction of the refresh value.

**Expiry** – 3600000 – This is the time (in seconds) that a slave server will keep a cached zone file as valid, if it can’t contact the primary server. If this value were set to say 2 weeks ( in seconds), what it means is that a slave would still be able to give out domain information from its cached zone file for 2 weeks, without anyone knowing the difference. The recommended value is between 2 to 4 weeks.

**Minimum** – 600 – This is the default time(in seconds) that the slave servers should cache the Zone file. This is the most important time field in the SOA Record. If your DNS information keeps changing, keep it down to a day or less. Otherwise if your DNS record doesn’t change regularly, step it up between 1 to 5 days. The benefit of keeping this value high, is that your website speeds increase drastically as a result of reduced lookups. Caching servers around the globe would cache your records and this improves site performance.

****

**QoS congestion management terms**

**First-in, first-out** (FIFO): FIFO entails no concept of priority or classes of traffic. With FIFO, transmission of packets out the interface occurs in the order the packets arrive, which means no QoS  
**Priority Queuing** (PQ): schedules traffic such that the higher-priority queues “always” get serviced first  
**Custom Queuing** (CQ): provide specific traffic guaranteed bandwidth at a potential congestion point, assuring the traffic a fixed portion of available bandwidth and leaving the remaining bandwidth to other traffic.  
**Weighted fair queueing** (WFQ): offers dynamic, fair queuing that divides bandwidth across queues of traffic based on weights. In standard WFQ, packets are classified into flows according to one of four criteria: the source Internet Protocol address (IP address), the destination IP address, the source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, or the destination TCP or UDP port.  
**Class-based weighted fair queueing** (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.  
Once a class has been defined according to its match criteria, you can assign it characteristics. To characterize a class, you assign it bandwidth, weight, and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.

**lightweight access point operation modes**

**Local mode** (default mode): measures noise floor and interference, and scans for intrusion detection (IDS) events every 180 seconds on unused channels

**Sniffer mode**: run as a sniffer and captures and forwards all the packets on a particular channel to a remote machine where you can use protocol analysis tool (Wireshark, Airopeek, etc) to review the packets and diagnose issues.

**Monitor mode**: does not transmit or serve clients at all. It acts like a dedicated sensor for location-based services (LBS), rogue AP detection, and Checks Intrusion Detection System (IDS). In this mode, AP will not broadcast an SSID so clients are unable to connect to it.

**Rogue detector mode**: monitor for rogue APs. It does not handle data at all.

A comparison list of Ansible, Puppet and Chef automation tool:

Table

Description automatically generated