CCNA Notes

Some Links:

<https://www.networkworld.com/article/3243262/what-is-a-hypervisor.html>

<https://www.webopedia.com/definitions/802-11/>

Commands to know

* Show IP interface brief – displays a summary of the IP addresses on the interface and the interface’s status
* Show vtp status – display the IP address of the switch that last updated your VLAN database
* Show cdp neighbors detail – determine the hostname associated with this IP address

When selecting cables, the following rules apply

* Router to router -> Crossover cable
* Router to Switch -> Straight-through cable
* Management Station (PC) to router for console session -> rolled (or rollover) cable
* Switch to switch -> Crossover cable
* PC to switch -> Straight-through cable

Full list of message types and their severity levels are in the list below:

|  |  |
| --- | --- |
| Message Name | Severity |
| Emergencies | 0 |
| Alerts | 1 |
| Critical | 2 |
| Errors | 3 |
| Warnings | 4 |
| Notifications | 5 |
| Informational | 6 |
| Debugging | 7 |

Pneumonic: Every Awesome Cisco Engineer Will Need Info Daily

WPA lists

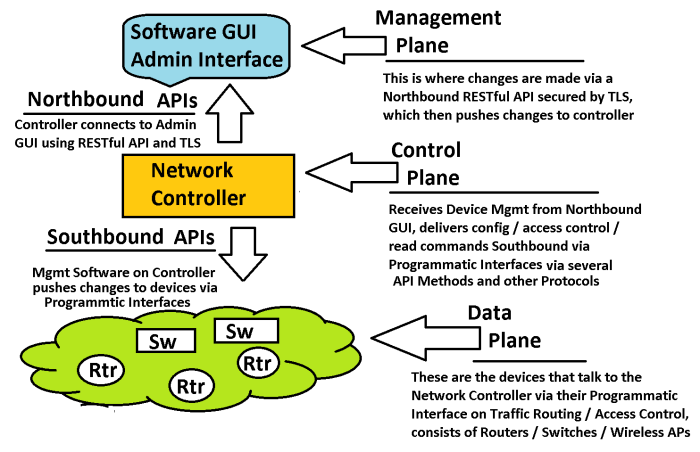
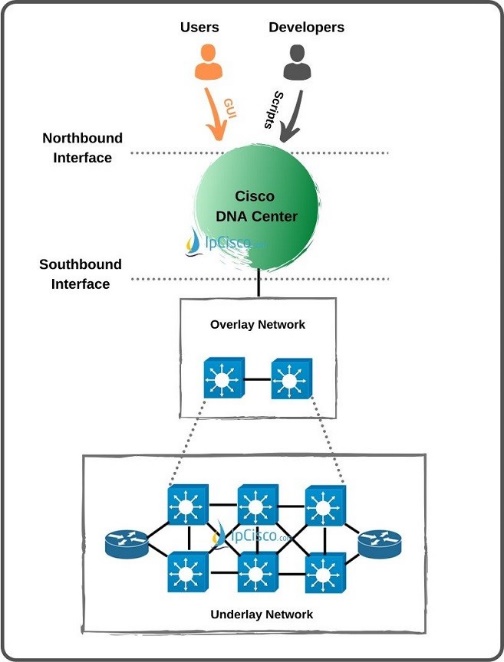
|  |  |
| --- | --- |
| WPA Type | Description |
| WPA-Enterprise | Requires RADIUS authentication server, intended for large networks. Also referred to as WPA-802.1x |
| WPA2 | More secure than WPA. |
| WPA-Pre-shared key (WPA-PSK) also known as WPA-Personnal | For use in home and small office networks.  Works for old and new devices |

For CCNA you need to protect against the following wireless attacks or issues

|  |  |
| --- | --- |
| Attack or Issue | Description |
| Evil Twin | Occurs when a wireless access point that is not under your control is used to perform a hijacking attack. It is set up to look like a valid network including the same Set Service Identifier (SSID) and other settings. |
| Rogue Access Point (AP) | Occurs when a wireless attack that is not under your control is connected to your network. With these devices, they are not set up to look just like your network. This attack preys on users’ failure to ensure that an access point is valid. You can perform site surveys to detect rogue Aps |
| War Driving | Occurs when attackers seek out a Wi-Fi network with a mobile device or laptop while driving a vehicle. You can lower the signal strength to help protect against this attack. You should also turn off the broadcasting of the SSID and use WPA or WPA2 Authentication. |
| War Chalking | Occurs when attackers place Wi-Fi network information on the outside walls of buildings. Keep an eye out for this type of information by periodically inspecting the outside of your facilities |
| Bluejacking | The sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices. Turning off Bluetooth when not in use is the best protection against this |
| Bluesnarfing | The unauthorized access of information from a wireless device through a Bluetooth connection. Once again, turning off Bluetooth when not in use is the best protection against this |
| WPA/WEP/WPS attacks | Any attacks against wireless protocols can usually be prevented by using a higher level of encryption or incorporating RADIUS authentication. Wired Equivalent Privacy (WEP) should be avoided because even its highest level of encryption has been successfully broken. Wi-Fi Protected Setup (WPS) allows users to easily secure a wireless home network but is susceptible to brute force attacks. Wi-Fi Protected Access (WPA) is more secure than WEP and WPS. WPA2 provides better security than WPA. |

Southbound API communicate with data place devices such as routers, switches, and firewalls

THE SDN controller uses the northbound API to communicate with higher level devices such as the network management station. The SDN stack is show below:



|  |  |
| --- | --- |
| Term | Description |
| Northbound API | Enables an SDN controller to communicate with applications in the application plane |
| Southbound API | Enables an SDN controller to communicate with devices in the data plane |
| Overlay | Creates VXLAN tunnels between SDA switches |
| Fabric | Is the entirety of the overlay network and the underlay network |
| Underlay | Is a collection of devices that compromises the IP network that connects to each fabric node |

Default Administrative Distances

|  |  |
| --- | --- |
| Route Source | AD |
| Directly connected route | 0 |
| Static route | 1 |
| EIGRP summary route | 5 |
| eBGP | 20 |
| Internal EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| External IGRP | 170 |
| iBGP | 200 |
| Unknown | 255 |

Calculate OSPF or IS-IS – Cost (calculate cost based on bandwidth)

Calculate EIGRP – Bandwidth & Delay

Calculate RIPv1 & RIPv2 – Hop Count (limit of 15 hops, more than 15 considered unreachable)

Cloud Infrastructure: What is the customer responsible for with each

IaaS Infrastructure as a Service)

* Operating Systems
* Data
* Applications
* Middleware
* Runtime

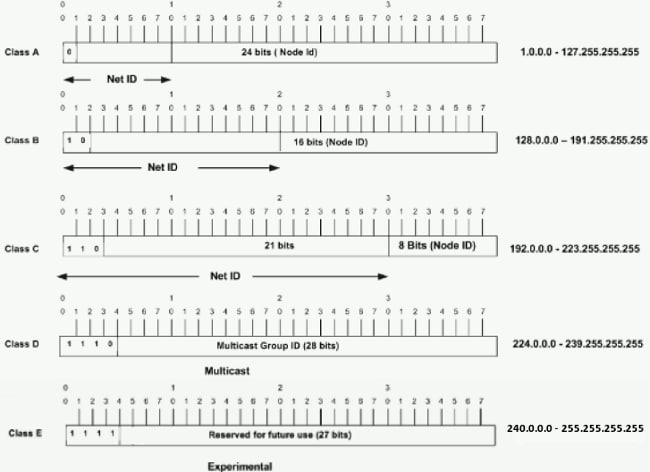
PaaS (Platform as a Service)

* Application
* Data

SaaS (Software as a Service)

* Deployment Only

Different IP address Classes



In a Class A address, the first octet is the network portion, so the Class A example in Figure 1 has a major network address of 1.0.0.0 - 127.255.255.255. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a Class B address, the first two octets are the network portion, so the Class B example in Figure 1 has a major network address of 128.0.0.0 - 191.255.255.255. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses are used for networks that have between 256 and 65534 hosts.

In a Class C address, the first three octets are the network portion. The Class C example in Figure 1 has a major network address of 192.0.0.0 - 223.255.255.255. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

Routing Table, at the beginning of the output will be a legend describing the letters as show below:

|  |  |
| --- | --- |
| I | IGRP |
| R | RIP derived |
| O | OSPF derived |
| C | Connected |
| S | Static |
| E | EGP |
| B | BGP |
| L | Local host route |
| \* | Candidate default route |
| IA | OSPF inter area route |
| i | IS-IS derived |
| ia | IS-IS |
| U | Per-user static route |
| o | On-demand routing |
| M | Mobile |
| P | Periodic downloaded static route |
| D | EIGRP |
| EX | EIGRP external |
| E1 | OSPF external type 1 route |
| E2 | OSPF external type 2 route |
| N1 | OSPF NSSA external type 1 route |
| N2 | OSPF NSSA external type 2 route |

Port Numbers to know

20 FTP  
21 FTP control  
22 SSH  
23 Telnet  
25 SMTP  
53 DNS

67, 68 DHCP  
69 TFTP  
80 HTTP  
110 POP3  
123 NTP

NetBIOS – 137-139  
161/162 SNMP  
443 HTTPS  
1812, 1813 RADIUS

Top of main menu page when setting up WLAN

Configure WPA2 for a specific WLAN -> select WLAN -> blue arrow to right of list

Security -> global security settings including RADIUS settings

Wireless Menu -> load balancing and configuration of frequencies

Controller Menu -> manage interfaces on the controller as well as configure DHCP

802.1 List

802.1x -> Port-Based access control and authentication (requires AAA to be configured on the switch)

802.1d -> standing for spanning tree protocol (STP)

802.1w -> standard for Rapid Spanning Tree Protocol (RSTP).

802.1P -> method for assigning priority traversing a network

802.1Q -> describes VLAN tagging

802.1q -> used to create trunk links for VLANs

802.11 List

|  |  |  |  |
| --- | --- | --- | --- |
| 2.4 GHz WLAN | 802.11b | 802.11n | 802.11g |
| Non-overlapping channels | 3 | 3 | 3 |
| Channels | 1,6,11 | 1,6,11 | 1,6,11 |
| Bandwidth MHz | 22 | 20 | 20 |
|  |  |  |  |

Number of overlapping channels available

802.11a -> 23

802.11b -> 4

802.11n and 802.11g -> 3

|  |  |
| --- | --- |
| Deployment models available for IPv4 to IPv6 migration | |
| IPv6 over IPv4 tunnel | IPv6 traffic is encapsulate into IPV4 packets. Then these packets are transferred over IPv4 WAN. Eliminates the need to create separate circuits to connect to the IPv6 network. Increases protocol overhead because the IPv6 headers required both ends to be capable of both protocols |
| Protocol translation | Method allowing an IPv6 host to communicate with an IPv4 host via Network Address Translation – Protocol Translation (NAT-PT). NAT-PT allows communication between IPv6 hosts and applications, and native IPv4 hosts and applications. |
| IPv6 over dedicated WAN links | Deployment of IPv6 is created. In this model IPv6 hierarchy, addressing, and protocols are used by all noted. Involves cost for creating IPv6 WAN circuits. Not designed for LAN translation but rather translation over WAN links |
| Dual-stack backbones | Hybrid model in which backbone routers have dual-stack functionality, enabling them to route both IPv4 and IPv6 packets. It is suitable for an enterprise that uses both IPv4 and IPv6 applications. Running IPv6 and IPv4 together in a network is known as dual stack routing. |

Show CDP neighbors command Code

R – Router

T – Trans Bridge

B – Source Route Bridge

S – Switch

H – Host

I – IGMP

r – Repeater

|  |  |  |
| --- | --- | --- |
|  | STP 802.1d | RSTP 802.1w |
| Port States |  |  |
| Disabled |  |  |
| Blocking |  |  |
| Discarding |  |  |
| Listening |  |  |
| Learning |  |  |
| Forwarding |  |  |
| Broken |  |  |
| Port Roles |  |  |
| Root (Forwarding) |  |  |
| Designated (Forwarding) |  |  |
| Non-Designated (Blocking) |  |  |
| Alternate (Discarding) |  |  |
| Backup (Discarding |  |  |
| Topology Changes and Convergence |  |  |
| Source: <https://cciethebeginning.wordpress.com/2008/11/20/differences-between-stp-and-rstp/> | | |

Switching processes

Store and forward: waits until the entire frame is received before forwarding to the destination port

Fragment-free: waits to receive first 64 bytes of frame before forwarding

Cut-through: does not require switch to verify the FCS in a frame before forwarding, fast but may forward errors

Metric for routing protocols

EIGRP – Composite metric

OSPF – cost

RIP – hop count

Router looks at AD of each and picks a route if multiple are used. EIGRP is 90 OSPF 110 and RIP is 120

Puppet is deployed in 1 of two architectures

Stand-alone: each note contains the application and its own configuration information

Agent/master: puppet master keeps all the configuration information and controls. Agent nodes pull the config info from the master and configure the nodes using those settings.

Private IP addressing

10.0.0.0 to 10.255.255.255 10.0.0.0/8

172.16.0.0 to 172.31.255.255 172.16.0.0/12

192.168.0.0 to 192.168.255.255 192.186.0.0./16

Public IP addressing

Registered with the Internet Assigned Number Authority (IANA)

Types of IPv6 address – Anycast, Multicast, Unicast

Graphical user interface

Description automatically generated with medium confidence

|  |  |
| --- | --- |
| Classless Routing Protocols | Classful Routing Protocols |
| BGP | IGRP |
| RIPv2 | RIPv1 |
| EIGRP |  |
| OSPF |  |
| IS-IS |  |

Characteristics of classless routing protocols

* Subnet mask is advertised with each route
* Flexible route summarization and super netting (CIDR) are allowed
* Support variable length subnet masks (VLSMs), which allow different subnets of a given IP network to be configured with different subnet masks

Main advantage is its ability to minimize the effects of discontiguous networks. When subnets of the same classful network are separated by anther classful network, the networks are called discontiguous.

|  |  |
| --- | --- |
| Wireless Encryption Protocols | |
| WEP | Uses 40-bit or 104-bit key |
| WPA/WPA2 Personal | Uses 256-bit pre-shared key |
| WPA/WPA2 Enterprise | Requires a RADIUS server |

VM Planes

Management Plane – Used to create, start, and stop VM instances. It also provisions them with proper virtual resources

Control Plane – Processes that control work done by the network device but do not directly impact the forwarding of individual frames or packets.

Data Plane – Actions that devices take to forward data

Storage Pool – Storage media used in virtualization

|  |  |
| --- | --- |
| LAN | WAN |
| CDDI | SONET |
| Token Ring |  |
| FDDI |  |

Configuring SSH on a router requires the minimum of three commands:

|  |  |
| --- | --- |
| Configuring SSH on a router requires the minimum of three commands: | |
| ip domain-name [domain-name] | Configures the DNS of the router (global configuration mode) |
| Crypto key generate rsa | Generates a cryptographic key to be used with SSH (global Configuration Mode) |
| Transport input ssh | Allows SSH connections on the router’s VTY lines (VTY line configuration mode) |

|  |  |
| --- | --- |
| Class IP Addressing | |
| A | * Range from 0.0.0.0 to 127.255.255.255 * Decimal value of the first octet can range from 1 to 126 * The first octet represents the entire network portion of the address * The value of the first binary place in the first octet must be 0 |
| B | * Range from 128.0.0.0 to 191.255.255.255 * Decimal value of the first octet can range from 128 to 191 * The first two octets represent the entire network portion of the address * The value of the first two binary places in the first octet must be 10 |
| C | * Range from 192.0.0.0 to 223.255.255.255 * Decimal value of the first octet can range from 192 to 223 * The first three octets represent the entire network portion of the address * The value of the first two binary places in the first octet must be 11 |

|  |  |  |
| --- | --- | --- |
| **Functions in each layer of the Cisco three-tier architecture** | | |
| **Access Layer** | **Distribution layer** | **Core layer** |
| Port Security | Routing updates | Access-list checking |
| PoE | Route Summaries | Data Encryption |
| Link Aggregation | VLAN traffic | Address Translation |
| QoS | Address Aggregation |  |

The following statements are true of link-state and distance vector routing protocols:

* Packets are routed based upon the shortest path calculated by an algorithm with link-state protocols
* Link-state protocols place a high demand on router resources running the link-state algorithm
* Link-state protocols use hello packets and LSAs from other routers to build and maintain the topological database
* Link-state protocols require a hierarchical IP addressing scheme for optimal functionality
* Distance vector protocols require a hierarchical IP addressing scheme for optimal functionality

|  |  |
| --- | --- |
| Distance Vector | Link State |
| RIP, RIPv2, IGRP, EIGRP | OSPF, ISIS |
| Routers communicate with neighbor routers advertising networks as measures of distance and vector | Routers communicate with all other routers exchanging link-state information to build a topology of the entire network |
| Distance = Metric Vector = Direction (Interface) | Link-state = interface connections or “links” to other routers and networks |
| Best for: - simple, flat design, nonhierarchical networks - minimum administrator knowledge - convergence time is not an issue | Best for:  - large, hierarchical networks  - advanced administrator knowledge  - convergence time is crucial |
| Knowledge of the network from directly connected neighbors | Routers have a complete view of the network, knowledge of the entire topology |
| Send periodic updates of the entire routing table | Send triggered partial updates |

Split horizon is the loop avoidance mechanism that dries the requirement to create subinterfaces for each point-to-point connection in a partially meshed frame relay network.

Frame relay is a non-broadcast multiple access (NBMA) network and obeys the rules of split horizon. This mechanism prohibits a routing protocol from sending updates out the same physical interface on which it was received. When the same physical interface is used to host multiple frame relay connections, this will prevent an update arriving from a remote network on the physical interface from being sent out to another remote network.

By creating subinterfaces for each frame relay connection and assigning IP addresses to the subinterfaces rather than the physical interface, and by placing the subinterfaces into different subnets, split horizon will not see the “virtual” interfaces as the same interface and will allow these routing updates to be sent back out the same physical interface on which they arrived.

* Subinterfaces solve the NBMA split horizon issues
* There should be one IP subnet mapping to each DLCI

Root bridge for SPT

Determined by lowest bridge ID

* Lowest priority number
* Lowest MAC address

OSPF DR and BDR

Two rules

* Router with the highest OSPF priority will become DR. By default all routers have priority of 1
* If tied, a router with highest router ID wins. The router with second highest router ID will become BDR

When a router has been configured with a loopback address the highest IP address assigned to a loopback interface on the router determines the OSPF router ID

How to prevent certain attacks

Brute-force attack – User awareness or training

Social Engineering - User awareness or training

Burglary – Physical access control

Pharming - User awareness or training

Tailgating – Physical access control

IPv6 Prefix:

2000::/3 – global aggregately unicast addresses

FC00::/8 and FD00::/8 – unicast site-local addresses

|  |  |  |
| --- | --- | --- |
| IPv6 Prefixes | | Range |
| 2000::/3 | global aggregately unicast addresses | 2000 - 3FFF |
| FC00::/8 and FD00::/8 | unicast site-local addresses | FC00 – FDFF |
| FF00::/8 | Multicast addresses which are used for one-to-many communications | FF00 – FFFF |
| FF01::/16 | Node-local |  |
| FF02::/16 | Link-local (used to form neighbor adjacencides) |  |
| FF05::/16 | Site-local |  |
| FF08::/16 | Organization-local |  |
| FF0E::/16 | Global |  |
| FE80::/10 | Unicast link-local addresses | FE80 - FEBF |

IPv6 Static Routes

Fully specified static route – Ipv6 static route in which destination network, outbound interface, and next-hop IPv6 address are all configured directly

* IPv6 route 2001:db8:a::/32 fastethernet 0/1 2001:db8:b::1

Directly attached static routes – route specifies the destination IPv6 network and the outbound interface

* IPv6 route 2001:db8:a::/32 fastethernet 0/1

Recursive static routes - specifies the destination IPv6 network and the IPv6 next-hop address only

* IPv6 route 2001db8:a::/32 2001:db8:a::1

Floating static routes – compromised of any of the other three types. Typically used as a backup route. Floating static routes typically are configured with an administrative distance value.

* IPv6 route 2001:db8:a::/32 2001:db8:a::1 5

|  |  |
| --- | --- |
| Application layer protocols which use: | |
| User Datagram Protocol (UDP) | **Transmission Control Protocol (TCP)** |
| SNMP - monitor and manage network devices | Hypertext Transfer Protocol (HTTP) – used to transfer webpages over the internet |
| TFTP – UDP port 69 to transfer files unreliably and without authentication over a network | File Transfer Protocol (FTP) - uses TCP port 20 and 21 to transfer files over a network |
| Dynamic Host Configuration Protocol (DHCP) – used to assign internet protocol (IP) addressing information to clients | Simple Mail Transfer Protocol (SMTP) – used to send email messages |
| Network Time Protocol (NTP) – coordinate time on a network | Post Office Protocol 3 (POP3) – used to retrieve email messages |
| Remote Authentication Dial-in Service (RADIUS) – used to authenticate users | Telnet – Used to manage network devices |

Basic Service Sets (BSS) – a closed group of wireless devices that are dependent on a fixed device

|  |  |
| --- | --- |
| Lightweight APs | Autonomous APs |
|  |  |

Point to point vs point to multipoint

Multiaccess network

Another name for a hypervisor is a Virtual machine monitor (VMM)

A hypervisor is software that can virtualize the physical components of computer hardware. Virtualization enables the creation of multiple VMs that can be configured and run in separate instances on the same hardware.

|  |  |
| --- | --- |
| Type 1 Hypervisor | Type 2 Hypervisor |
| Installed on bare metal server meaning that the hypervisor is also its own operating system (OS). | Applications installed on host OS |
| Perform better than type 2 due to its proximity to the physical hardware | Called hosted hypervisors, use calls to the host OS to translate between guest OSs in VMs and the server hardware |
|  | Easy to deploy and maintain |

Ethernet multicast range of 01-00-5E-00-00-00-00 through 01-00-5E-7F-FF-FF has been allocated for IP multicast use

* The first 24 bits of a 48bit multicast MAC address is always 01-00-5E
* The twenty-fifth bit is always set to 0

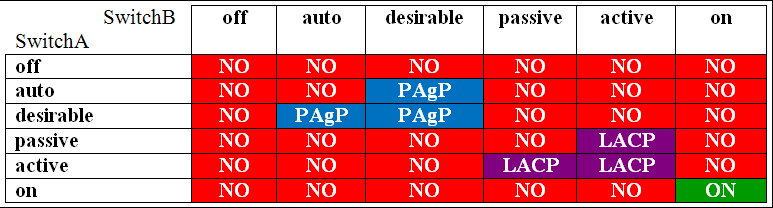
To enable **Secure Shell (SSH) for virtual terminal (VTY) lines** on a Cisco router, you should complete the following steps:

* Configure the router with a host name other than Router by issuing the hostname command
* Configure the router with a domain name by issuing the ip domain-name command
* Generate an RSA key pair for the router by issuing the crypto key generate rsa command
* Configure the VTY lines to use SSH by issuing the transport input ssh command from line configuration mode

Access-class ranges

|  |  |  |
| --- | --- | --- |
| Range | ACL Type | Use |
| 1-99 | Standard | Permit or deny packets based only on the source IPv4 address |
| 100-100 | Extended | Permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more. |

|  |  |  |  |
| --- | --- | --- | --- |
| description | VLAN Trunking Protocol (VTP) | | |
|  | Server | Client | Transparent |
| Creates/modifies/deletes VLANs |  |  |  |
| Synchronizes VTP information |  |  |  |
| Originates VTP Information |  |  |  |
| Forwards VTP Information |  |  |  |
| Stores VLAN information in NVRAM |  |  |  |



|  |  |
| --- | --- |
| API | Use Case |
| Northbound APIs | |
| Representation State Transfer (REST) | Northbound API which uses Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS) to enable external resources to access and make use of programmatic methods that are exposed by the API. REST APIs typically return data in either Extensible Markup Language (XML) or JavaScript Object Notation (JSON) format. |
| Java Open Services Gateway Initiative (OSGi) | A Java-based northbound API framework that is intended to enable the development of modular programs. OSGi also allows the use of the Python programming language as a means of extended controller functions. For transport, OSGi deployments often rely on HTTP. |
| Southbound APIs | |
| Southbound Interface (SBI) | Enables an SDN controller to communicate with devices on the network data plane. NETCONF, OnePL, OpenFlow, and OpFlex are all examples of Southbound APIs |
| NETCONF | Uses Extensible Markup Language (XML) and Remote Procedure Calls (RPCs) to configure network devices. XML is used for both data encoding and protocol messages. NETCONF typically relies on Secure Shell (SSH) for transport. |
| OpFlex | Uses a declarative SDN model in which the instructions that are sent to the controller are not so detailed. The controller allows the devices in the data plane to make more network decisions about how to implement the policy |
| OpenFlow | Uses an imperative SDN model in which detailed instructions are send to the SDN controller when a new policy is to be configured. The SDN controller manages both the network and the polices applied to the devices |
| OnePK | A cisco-proprietary API. Uses Java, C, or Python to configure network devices. It can use either Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt data in transity |

802.11 Frame Format: FC DUR ADD1 ADD2 ADD3 SEQ ADD4 DATA FCS

CDP – advertisement every 60 seconds

LLDP – advertisement every 30 seconds, hold for 120 seconds before discarding, hold time can be set to any integer 0 through 65535

HSRP Version 1 virtual MAC address – ACxx

HSRP Version 2 virtual MAC address - Fxxx

OSPF neighbor states in order: (1) Down (2) Init (3) 2-way (4) Exstart (5) Exchange (6) Loading (7) Full

|  |  |  |
| --- | --- | --- |
| Application Layer Protocols | | |
| TCP | UDP | TCP & UDP |
| FTP 20 / 21 | DHCP 67/68 | DNS 53 |
| HTTP 80 | SNMP 161/162 |  |
| SMTP 25 | TFTP 69 |  |
| POP3 110 | NTP 123 |  |
| Telnet 23 | RADIUS 1812/1813 |  |

TCP – FHSP – Tel

UDP – DSNR - TF

QoS levels priorize different traffics

Gold – Video

Platinum – Voice over Internet Protocol (VoIP)

Silver – default when you configure a WLAN on a cisco WLC. Delivered by using best effort voice and video

Bronze – typically used for guests and provides the lowest bandwidth

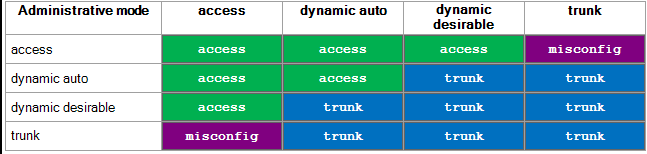
Professor Messer – [Seven Second Subnetting](https://www.youtube.com/watch?v=ZxAwQB8TZsM)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Masks | | | | | Networks | Addresses |
| /1 | /9 | /17 | /25 | 128 | 2 | 128 |
| /2 | /10 | /18 | /26 | 192 | 4 | 64 |
| /3 | /11 | /19 | /27 | 224 | 8 | 32 |
| /4 | /12 | /20 | /28 | 240 | 16 | 16 |
| /5 | /13 | /21 | /29 | 248 | 32 | 8 |
| /6 | /14 | /22 | /30 | 252 | 64 | 4 |
| /7 | /15 | /23 | /31 | 254 | 128 | 2 |
| /8 | /16 | /24 | /32 | 255 | 256 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Addresses |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 128 | 0 | 128 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 64 | 0 | 64 | 128 | 192 |  |  |  |  |  |  |  |  |  |  |  |  |
| 32 | 0 | 32 | 64 | 96 | 128 | 160 | 192 | 224 |  |  |  |  |  |  |  |  |
| 16 | 0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 244 | 240 |
| 8 | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 | 64 | 72 | 80 | 88 | 96 | 104 | 112 | 120… |
| 4 | 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 | 52 | 56 | 60… |

Steps

* Convert address and mask to a decimal
* Calculate the network address
  + If the mask is 255, bring down the address
  + If mask is 0, use the 0
  + For any other number, reference the chart
* Calculate the broadcast address
  + If mask is 255, bring down the address
  + If mask is 0, use 255
  + For any other number, reference the chart
* First IP is network address + 1
* Last IP is broadcast address – 1



|  |  |
| --- | --- |
| Layer 2 Security drop-down list | Layer 3 security drop-down list |
| WPA+WPA2 | IPSec |
| 802.1X | VPN Pass-Through |
| Static WEP | Web Authentication |
| Static WEP + 802.1X | Web Passthrough |
| CKIP |  |
| EAP Passthrough |  |

Timeline

Description automatically generated

Chart, bar chart

Description automatically generated

|  |  |  |
| --- | --- | --- |
| OSPF Network | Interfaces Enabled by default | Timer Hello/Dead Seconds |
| Broadcast [DR/BDR] | FDDI, Ethernet | 10/40 |
| Nonbroadcast [DR/BDR] | Frame Relay, X.25 | 30/120 |
| Point-to-point | HDLC, PPP | 10/40 |
| Point-to-multipoint broadcast |  | 30/120 |
| Point-to-multipoint nonbroadcast |  | 30/120 |

HSRP Version 1 virtual MAC address – ACxx

HSRP Version 2 virtual MAC address - Fxxx

GLBP virtual MAC address – 0102

VRRP Virtual MAC address – 0101

Chart, bar chart

Description automatically generated

Timeline

Description automatically generated

Timeline

Description automatically generated

Table

Description automatically generated

Bar chart

Description automatically generated with medium confidence

