III-Networking

introduces

Cisco Certified Network Associate

By: Sajjad Ghaffoori

iiinetworking.com

Our Website

YouTube.com/@iiinetworking

Arabic IT Courses/Content

Page: Facebook.com/iiinetworking
Group: Facebook.com/groups/iiinetworking

Technical Discussion and Sharing

@III_Networking

Entertaining IT Content

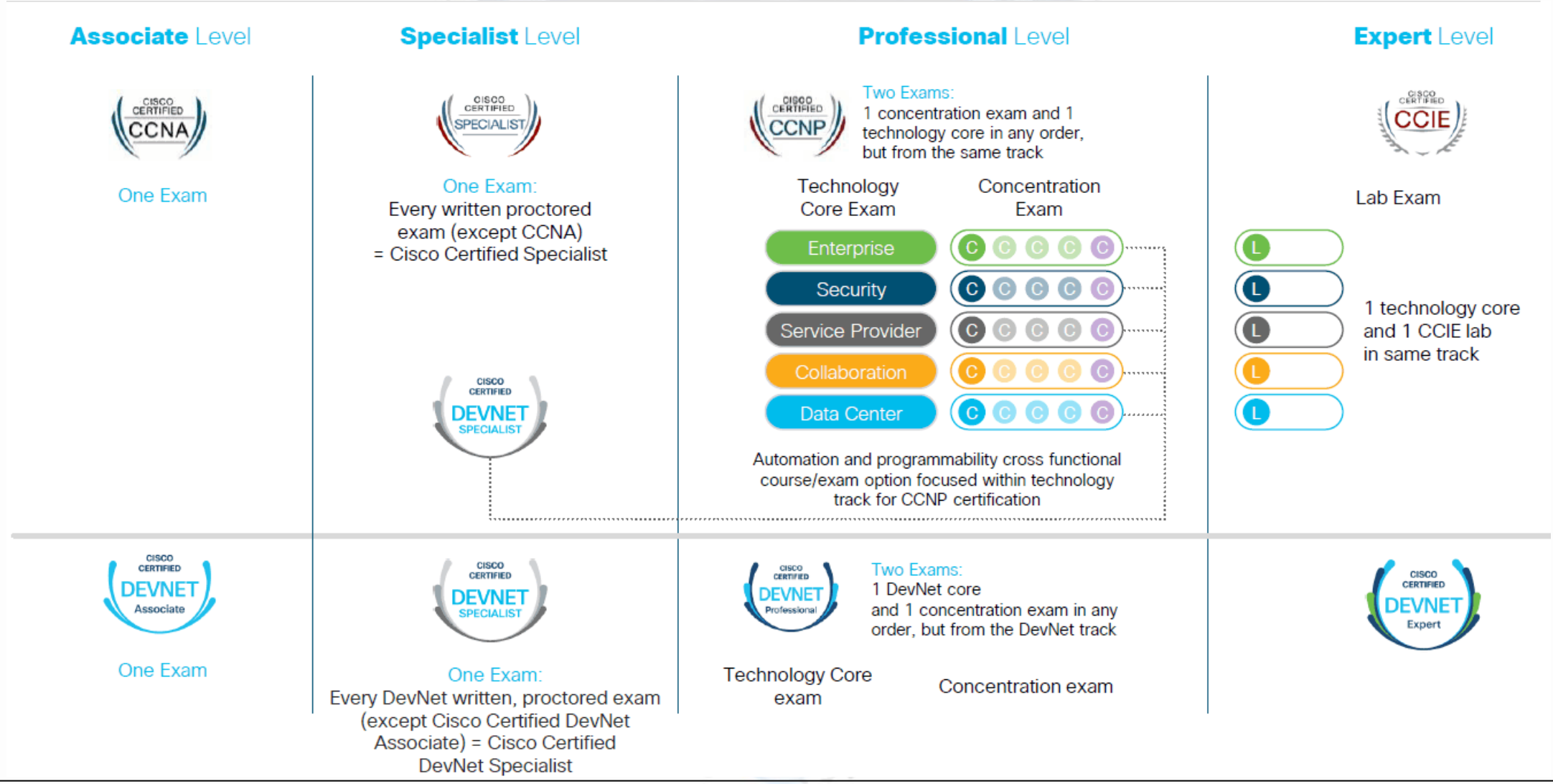
Linkedin.com/in/ sajjad-ghaffoori-6b4674134
Linkedin.com/company/iii-networking

Direct Connection

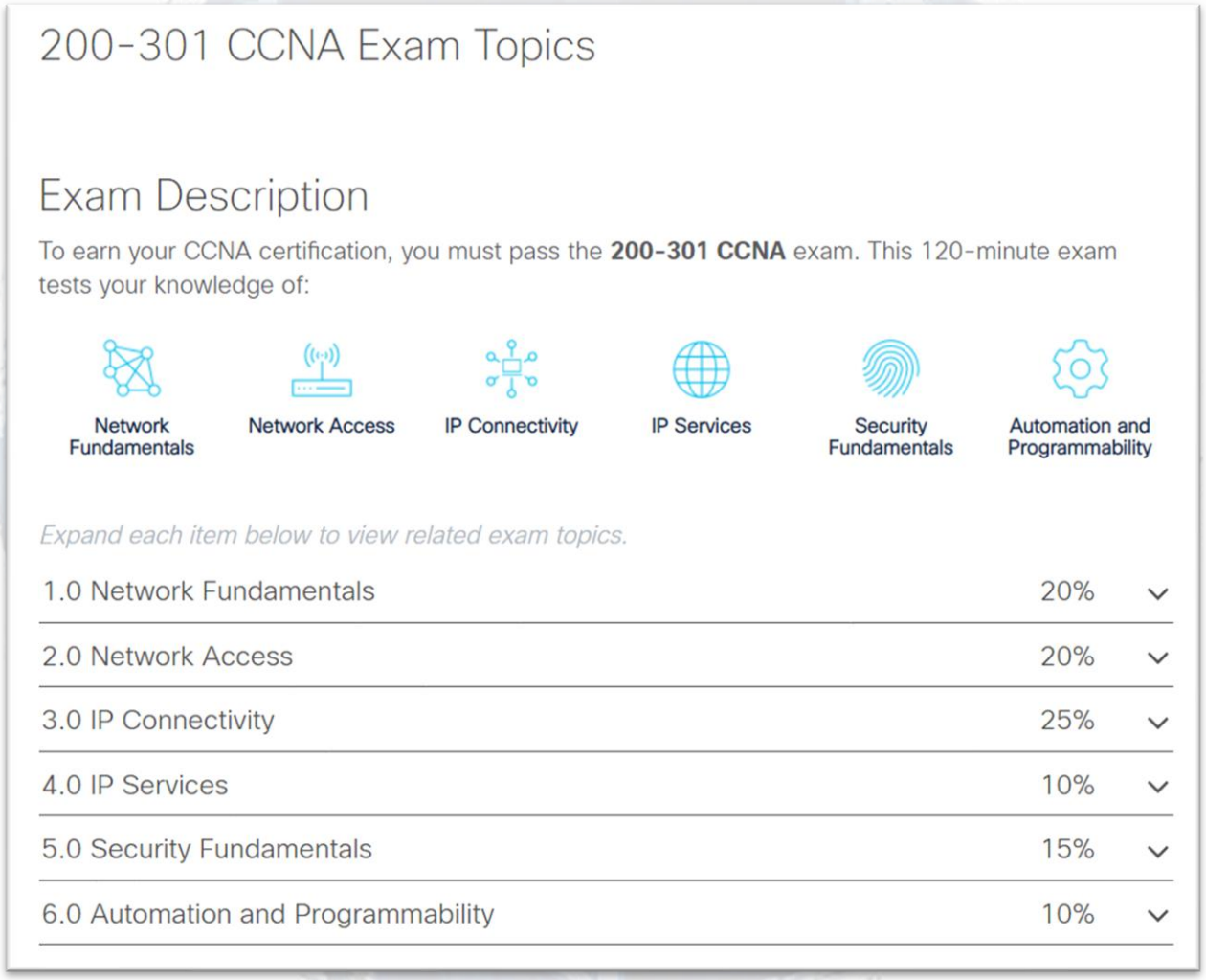
https://t.me/+yDloeSbd-3EwYzA0

Courses Channel

- Cisco Exams Roadmap



- CCNA Exam Topics



200-301 CCNA Exam Topics

Exam Description

To earn your CCNA certification, you must pass the **200-301 CCNA** exam. This 120-minute exam tests your knowledge of:

Network Fundamentals | Network Access | IP Connectivity | IP Services | Security Fundamentals | Automation and Programmability

Expand each item below to view related exam topics.

1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%
5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%

- CCNA Exam Information

- Cisco Certified Network Associate 200-301
- Exam questions: 93-103
- Questions Types: MCQ, DnD, and LAB Sims
- Exam duration: 120 minutes
- Exam Engine: PearsonVue
- Exam Passing Score: 825/1000
- English Course to prepare for CCNA
    - https://youtu.be/eF8iET38RYc?si=AjeYWPkE1Eb_DUHA
- Arabic Course to prepare for CCNA (منهاج عربي)
    - https://www.youtube.com/playlist?list=PLAqaqJU4wzYXBeFUFYs4qQ2qnWm_28xBV

- Module-1: Network Fundamentals

1.1 Explain the role and function of network components
- 1.1.a Routers
- 1.1.b Layer 2 and Layer 3 switches
- 1.1.c Next-generation firewalls and IPS
- 1.1.d Access points
- 1.1.e Controllers (Cisco DNA Center and WLC)
- 1.1.f Endpoints
- 1.1.g Servers
- 1.1.h PoE

1.2 Describe characteristics of network topology architectures
- 1.2.a Two-tier
- 1.2.b Three-tier
- 1.2.c Spine-leaf
- 1.2.d WAN
- 1.2.e Small office/home office (SOHO)
- 1.2.f On-premise and cloud

1.3 Compare physical interface and cabling types
- 1.3.a Single-mode fiber, multimode fiber, copper
- 1.3.b Connections (Ethernet shared media and point-to-point)

1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

1.5 Compare TCP to UDP

1.6 Configure and verify IPv4 addressing and subnetting

1.7 Describe the need for private IPv4 addressing

1.8 Configure and verify IPv6 addressing and prefix

1.9 Describe IPv6 address types
- 1.9.a Unicast (global, unique local, and link local)
- 1.9.b Anycast
- 1.9.c Multicast
- 1.9.d Modified EUI 64

1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)

1.11 Describe wireless principles
- 1.11.a Nonoverlapping Wi-Fi channels
- 1.11.b SSID
- 1.11.c RF
- 1.11.d Encryption

1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)

1.13 Describe switching concepts

1.14 MAC learning and aging

1.15 Frame switching

1.16 Frame flooding

1.17 MAC address table

- What is a Network?

- Also called (Computer Network), it is 2 or more devices needs to share information between them.
    - To do that, they will need a common media between them to share that information.

- Network Types (sizes):
    - some users in the same room/department connected using a switch device
    - Or: some users in different rooms/department connected using a router and some switches.

Local Area Network - LAN -

    - Users connected globally through the Internet,
        - Service Providers will be needed
        - A group of devices (Routers, Switches, & other devices) will be needed

Wide Area Network -WAN -

- Network Components

- Routers: Network devices that connect different network domains
  and routes the IP packets to its correct destinations.
  - Each interface is a broadcast domain
- Switches: Network devices that connects 2 or more devices in one network domain.
  - Then what is a Multi-Layer Switch? , MLS, L3Switch?
- Firewalls and Intrusion Prevention Systems
  - Firewalls protects you from the internet
  - Apply some restrictions to your local network
  - Intrusion Prevention Systems (IPS) performs deep packet inspection (DPI)
  - Try to spot attacks

*There is a 2 in 1 solution

  - Next-Generation Firewalls (NGFW) = FW + IPS

– Network Components

– Access Points: like switches, APs are the (wireless) destination for a host to communicate with other hosts

- Controllers:

    A - Wireless Controllers: a central management point for multiple APs,

    B - Cisco DNA Center: the super powerful, super capable central point of management for??

        - Analytics

        - Automation

        - Using GUI to Design, Display, and Configure

– Servers: a device, storing common data for users (clients) to make use of:

    - As a hardware matter, it is a computer! but with _____

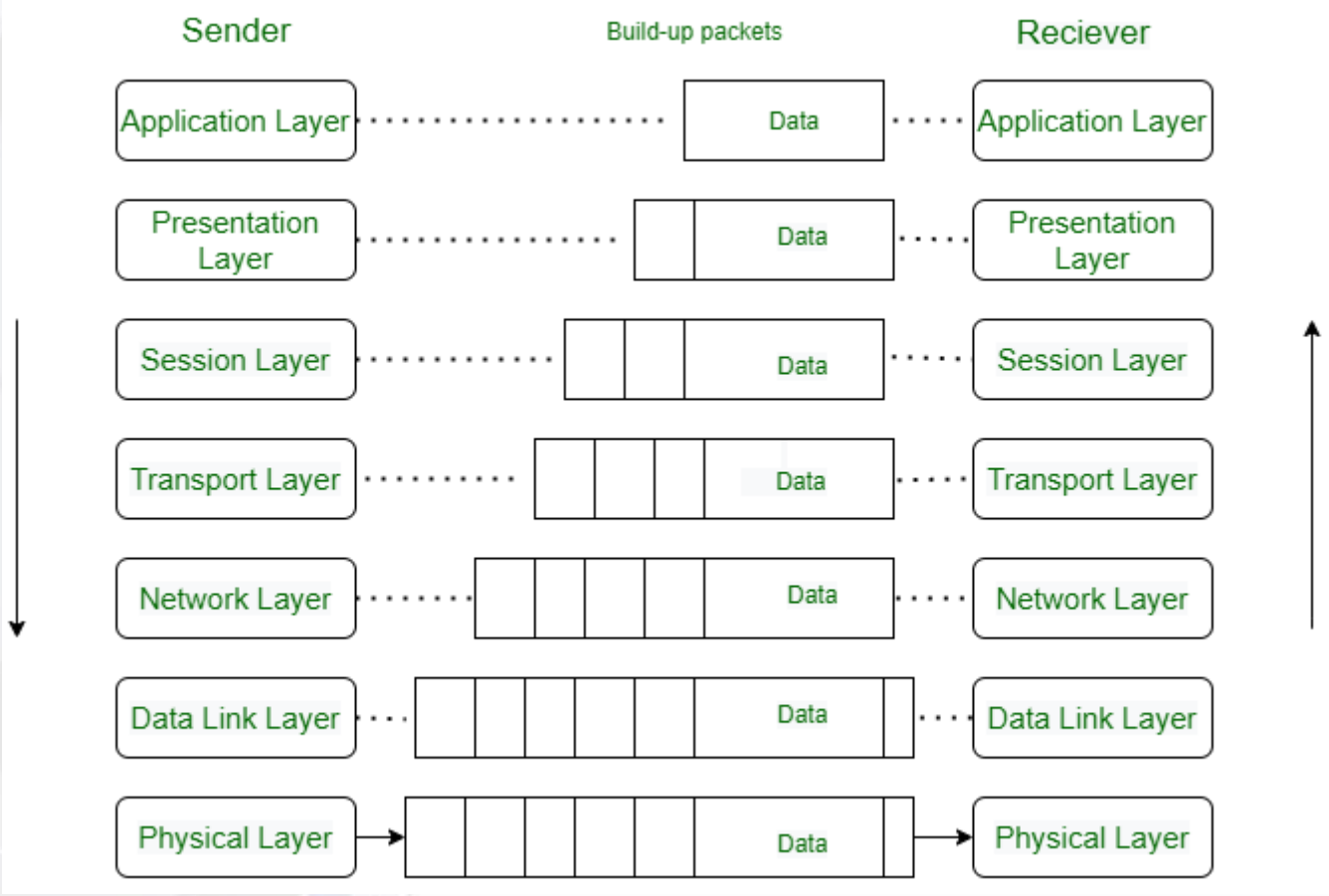
    - While clients, are the end devices that consumes OR generates new data.

– Virtual Machines: ……..

– Network Architecture Models

A – The Open Systems Interconnection model (OSI model):

- 1st model out
- 7 specified layers of tech.
- carries the Ethernet 802.3
- many old/ & legacy protocols
- were and still using it

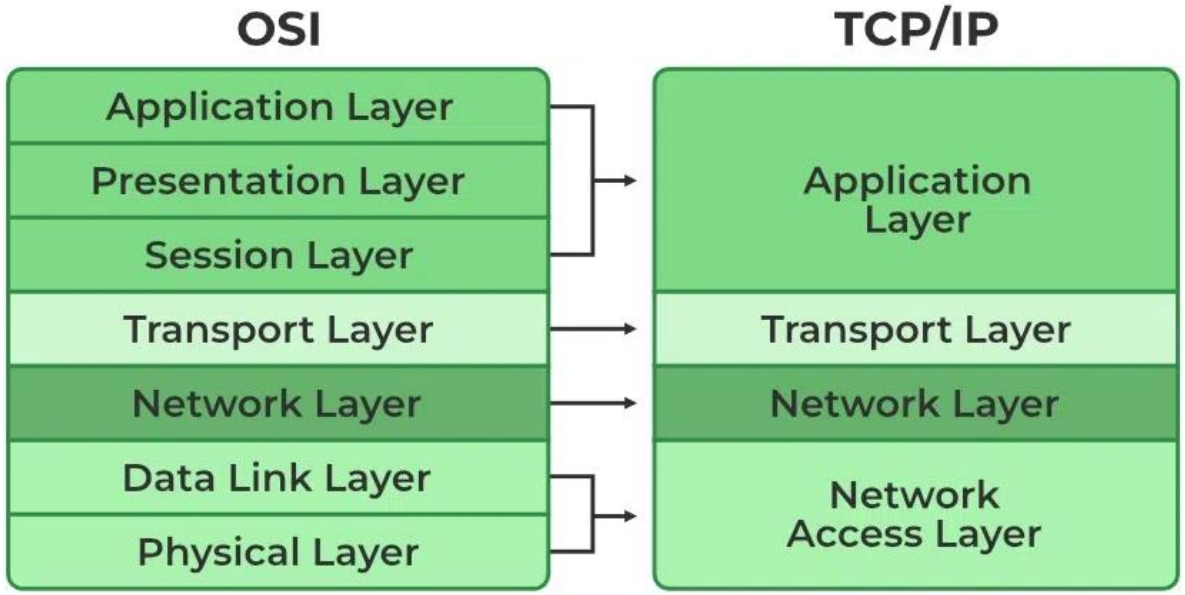


https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/

– Network Architecture Models

B – The Transmission Communication Protocol/Internet Protocol Model (TCP/IP Model)

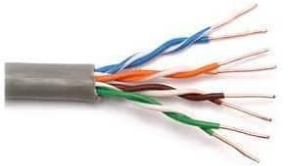
- 2nd model announced
- less specific
- deals with Ethernet II
- many modern and current protocol depends on it within the networks



https://www.geeksforgeeks.org/tcp-ip-model/

- Layer 1 Technologies

- Physical Links/Connections
    - A – Copper (Ethernet): the oldest, variety in speeds, developed through time
        - 4 pairs of “Copper”
        - Functions in a matter of Electric Circuit
        - 2 pairs for 100 Mbps
        - 4 pairs for the 1000 Mbps
    - Shielded and Unshielded
    - Connecter: RJ45



UTP Cable

STP Cable

- Layer 1 Technologies

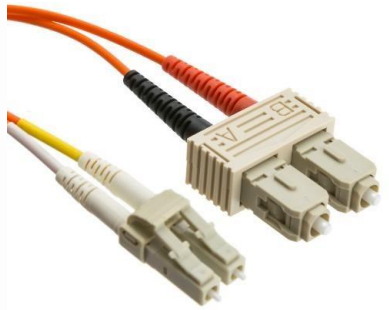
B – Optical Fibers: New. Already in High Speeds, even more Speed!

- Single fiber is enough
- Starts with 1 Gbps, up to Tens of Gbps
- Either light or laser

- 2 Types of Transmission media is used, either light or laser
  - Multimode (MM): light is used in the case of short distances
  - Single Mode (SM): laser is used in the case of long distances

- How do the devices understand light signals?!?!
- How do light become limited to a certain speed?!?!
- Connectors: on the end of each Fiber Optic cable,

  LC, SC, FC, ST, MTP/MPO



- Layer 1 Technologies

- Point to Point & Shared Media
    - Point to Point (P2P): directly connected, nothing in the way
    - Shared Media: Broadcast, a layer 2 device in the way

- Power over Ethernet (PoE):
    - Carrying Power over 2 pairs of Copper Cables (enough to power up some network devices)
    - Can replace an AC adapter
    - PoE Terms:
        - PSE: Power Sourcing Equipment (Switches, Power Injectors)
        - PD: Powered Device (PCs, IP Phones, IP Cameras)
    - Negotiation happens between the PSE & PD before/after starting Suppling
    - Power Suppling over PoE can be from 15 – 95 Watts (Total)
    - UPoE+: Universal PoE make use of all the 4pair to carry both Data & Power

- Layer 1 Technologies

- Collisions
    - more than one device (PC) transmitting at a single time, in a shared media
    - causes collisions and data loss
    - to avoid collisions:
        - Carrier sense multiple access/collision detection, CSMA/CD
            - listen for TX and wait for your turn
            - the Half-Duplex
        - Bidirectional Transmission by buffering and transmitting
            - the Full-Duplex
    - Errors: Cabling Issue, Unsupported SFP
    - Duplex Mismatch: Half or Full? MUST MATCH
    - Speed: 10/100/1000? MUST MATCH

- Wireless Principles

- Mimic the Signaling in Wired-Medium
    - Electro-Magnetic field to encode data (0,1)
    - Encoding will be done by changing the frequency of a wave
    - that is measured by Hertz
    - and Hertz: the change in frequency/second
    - then, Modulation will express the Zeros and Ones
- there are Wi-Fi generations (like Ethernet Categories)
    - starts from 802.11a (2 Mbps) – 802.11ax (14 Gbps)

- Wireless Principles

- The Encoder that turns the Zeros and Ones to that “Electro-Magnetic” field
- is called a Trans/ceiver
    - The more transceivers available, the more data encoded
    - Then, a transceiver, will push the field, through an Antenna

    *also, the more antennas, the more data
- To generate and push data through the air, there must a power source
- to do so, a power source is needed
    - this power source might be a battery or an AC adapter
    - measuring the power of a frequency is called “Amplitude”

- Wireless Network Components

- Wi-Fi Client (End Point): also called a “Station”
    - Generates/Consumes Data
    - Have Transceivers (to encode data)
    - Have Antennas (to push the data)
    - It will need Power
- Wi-Fi Access Points (AP)
    - GW for the stations
    - Stations talks through the AP
    - also have Transceivers
    - also have Antennas
- Wi-Fi Controllers
    - Controls APs (central point of management)
    - Controls Access for clients (AAA)

- Wireless Modes/Terms

- Ad-Hoc: Point to Point (NO APs)
- Infrastructure: AP between stations
- Mesh: APs talking together (Wirelessly)

- Basic Service Set (BSS): A single AP and it's coverage area
- Basic Service Set Identifier (BSSID): The MAC address of that AP
- Service Set Identifier (SSID): Name of the WLAN
- Distribution System (DS): The Wired Net. that connects the AP to the LAN
- Extended Service Set (ESS): A collection of APs connected to the same
    - DS, offering the same WLAN & SSID (like hotels, hotspot)

- Wireless Modes/Terms

- Radio Frequency power
    - the amount of power an antenna will receive
    - to convert it to electric power
    - measured in either watts, or deciBills x MilliWatts (dBm)
    - affected by barriers in the way, and get attenuated
    - decremented by cable length (transceiver to antenna), incremented by antenna gain
    - RF power affects signal strength
    - important for “Design”, to measure, how many AP we need to maintain signal strength
    - important for “Troubleshooting, slow internet
- RSSI
    - received signal strength indicator
    - an indicator for the quality of all the broadcasting SSID's nearby
- Noise Floor and Interference
        - other electro-magnetic fields roaming in the space
        - conflict signals will cause interference

- Wireless Modes/Terms

- SNR
    - signal to noise ratio
    - the difference (-) between received signal and noise floor
    - Signal (-) Noise
    - higher = better
- Client Devices Capabilities
    - a client device that receives a signal and data
    - should have an approximate power compared to the transmitter
    - download data will be transmitted from the AP to the client
    - acknowledgments, upload data, and other communications
    - will be transmitted from the client
    - thus, capabilities should be approximate
    - to avoid exchanging mismatch

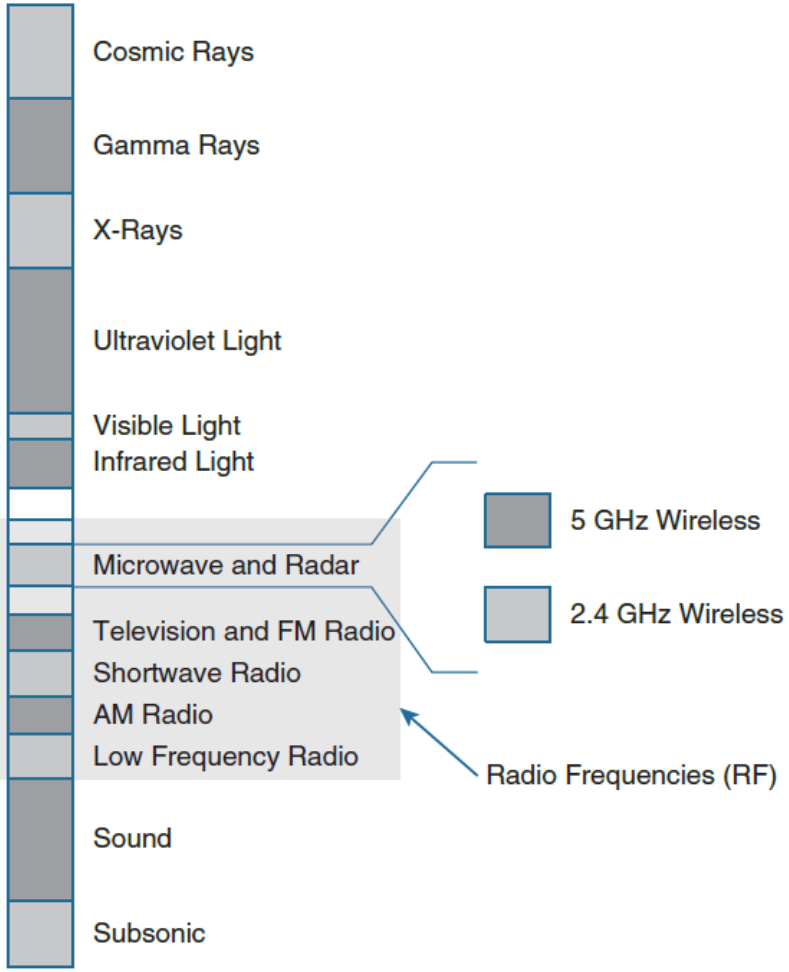
- Wireless Frequency

- Starting a wireless signal from a point
- and meeting back that point
- equals a frequency!
- the opportunity of having a frequency or more
- happening in 1 second (period of time)
- is measured in Hertz

- frequencies can be grouped in bonds
- like 2.4 and 5 GHz bonds
- their levels are of different uses
- and designed to be on international standards

CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

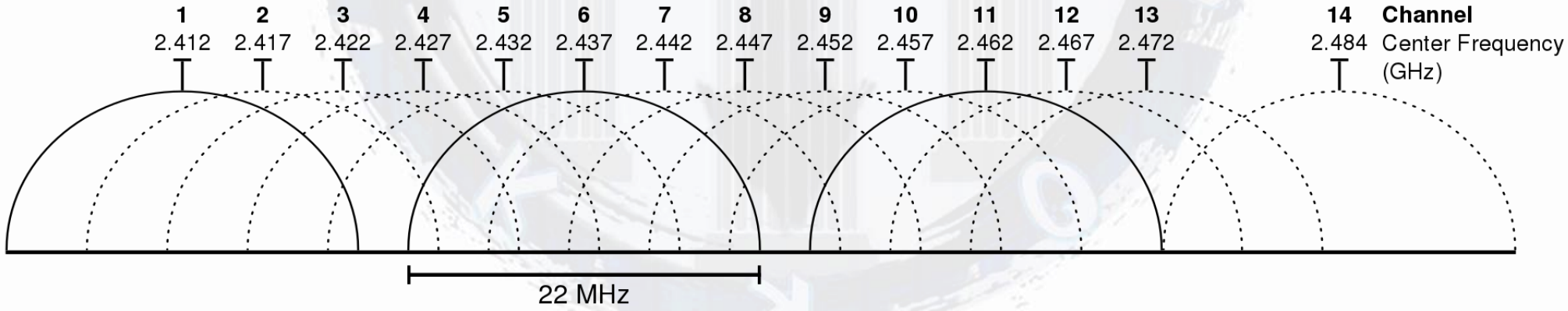
Frequency (Hz)	Frequency Notation
10^{22}	
10^{21}	
10^{20}	
10^{19}	
10^{18}	
10^{17}	
10^{16}	
10^{15}	
10^{14}	
10^{13}	
10^{12}	100 GHz
10^{10}	10 GHz
10^{9}	1 GHz
10^{8}	100 MHz
10^{7}	10 MHz
10^{6}	1 MHz
10^{5}	100 kHz
10^{4}	10 kHz
10^{3}	1 kHz
10^{2}	100 Hz
10^{1}	10 Hz
0	0 Hz



– Wireless Channels

- A set, or a range of Radio Frequencies (RF)
- established together, all encoding and transmitting data
- each frequency can be modulated differently (for more encoding)
- the total RF bandwidth is then called (Channel Bandwidth)
- channels include Frequencies, either from the 2.4 GHz range, or the 5 GHz range

*channel bandwidth: the total bandwidth of the involved frequencies



https://en.wikipedia.org/wiki/2.4_GHz_radio_use#/media/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg

- Wireless Channels

- if 2 channels were close enough
- streaming some common frequencies, overlapping will happen
    - unless, they were far enough
    - this is with 2.4 GHz channels only (which comes in 20 MHz width)
    - with 5 GHz channels, a new channel, start with a frequency
    - right after the last channel's frequency ended
    - so, overlap won't happen
    - the 5 GHz channels support from 20 MHz width, up to 160 MHz!

*more channel width, means more frequencies included, thus, more data can be encoded

– Networking Languages

A – The Binary Language

- Only 2 digits: 0 & 1
- Everything is Binary
- Each digit = 1 bit
- Zeros are low Electric pulse, low frequency light wave, Once are the opposite

B – The Decimal Language

- 10 digits: 0 – 9
- Value: 0 – 255
- NO Number “10”
- For humans, ease

C - The Hexa-Decimal Language

- 16 digit: 0 – 9, A – F
- 0 = smallest value, F = biggest value

- Media Access Control Address

- The MAC Address
    - Layer 2 Technology
    - Hexa-Decimal Language
    - Physical Address
    - Constant and Unique
    - 48 Bit length
    - Half for the Organization, half for the product

- Internet Protocol Version 4 (IPv4)

- Layer 3 Technology
    - Decimal Language (and Binary)
    - Logical Address
    - Variable, based on the need
    - 32 Bit length
    - Part for the Network, Part for the Hosts
    - 4 Octets, each =?
- Addressing:
    - convert from binary to decimal, and vice versa
    - What defines network octets from hosts octets?
    - Total Hosts = 2^{32} = 4,294,967,296

- Internet Protocol Version 4 (IPv4)

- Subnetting
    - form 8 – 32
    - The smallest, the bigger
    - /XX or XXX.XXX.XXX.XXX like the IP address
- Variable-Length Subnet Mask (VLSM)
    - The opposite of Subnetting
    - Much more economic for the use of subnetting
    - Can obtain
        - Network ID
        - Network Addresses Range Network
        - Broadcast ID

- Internet Protocol Version 4 (IPv4)

- IPv4 Classes:
  - What defines the class?

- Class A: /8	1.0.0.0	---	126.255.255.255
- Class B: /16	128.0.0.0	---	191.255.255.255
- Class C: /24	192.0.0.0	---	223.255.255.255
- Class D: /8	224.0.0.0	---	239.255.255.255
- Class E: /8	240.0.0.0	---	255.255.255.255

- Internet Protocol Version 4 (IPv4)

- Private vs. Public IPv4 Addresses
    - Avoid duplication
    - Private: available and free
    - Public: reserved (costs money)
- Private Addresses:
    - 10.0.0.0 – 10.255.255.255 /XX
    - 172.16.0.0 – 172.31.255.255/XX
    - 192.168.0.0 – 192.168.255.255 /XX

- Internet Protocol Version 4 (IPv4)

- Classless Inter-Domain Routing (CIDR)
    - design a “subnet mask”
    - based on the need
        - need for amount of address space
        - factor of safety (future growth)
        - appropriate isolation
        - careful with summarization
    - based on the number of the hosts
        - get ID’s
        - amount of useable addresses
        - which mask will identify this subnet
- extract 4 subnets based on the needs of 4 different design (50, 150, 300, 600)

- Internet Protocol Version 6 (IPv6)

- relevant to IPv4
- based on 128 bits in total length
- leads to 340 undecillion address
- an IPv6 packet has a header of 40 bytes
- many new field added, others removed instead
    - version: 6 (0110)
    - traffic class & flow label: QoS
    - payload length: just the length of the payload
    - next header: replaces protocol number
    - hop limit: replaces TTL
    - Src. & Dst. Addresses

- Internet Protocol Version 6 (IPv6)

- And thus, it can be written as
    - 2001:db80:0000:0000:0000:0000:0000:0001
    - 8 total parts
    - 16 each / 4 digits
    - it can be simpler
        - 2001:db80:0000:0000:0000:0000:0000:0001
        - 2001:db80:0:0:0:0:0:0001
        - 2001:db80:0:0:0:0:0:1
        - 2001:db80::0001
        - 2001:db8::1

- Internet Protocol Version 6 (IPv6)

- Different types are supported
- to help with the private/public addressing

    - ::1/8 loopback address
    - 2000::/3 global unicast address
    - FC00::/7 unique local unicast address
    - FE80::/10 link-local unicast address
    - FF00::/8 multicast address

- IPv6 supports
    - Unicast (one-to-one)
    - Multicast (one-to-many)
    - Anycast (one-to-nearest)

- Internet Protocol Version 6 (IPv6)

- IPv6 Unicast Addresses
    - Global Unicast
        - for public connection
        - can be reached from the internet
        - can be assigned per hosts
        - the address structure represents many details
            - the company
            - the subnet
            - the specific interface assigned with this address
                - interface ID is derived from the MAC
                - from the modified EUI-64

- Internet Protocol Version 6 (IPv6)

- IPv6 Unicast Addresses
    - Link-Local
        - internal used only
        - within the domain/segment
        - between the interfaces
            - starts with FE80
            - 24 bits of the MAC
            - FFFE
            - 24 bits of the MAC
        - requires the modified EUI-64

- Internet Protocol Version 6 (IPv6)

- IPv6 Unicast Addresses
    - Unique Local
        - for internal use
        - within the network
        - not routed to the internet
            - starts with FC00
            - global ID
            - subnet ID
            - interface ID
    - which is of the modified EUI-64

- Internet Protocol Version 6 (IPv6)

- IPv6 Anycast Address
    - a global address
    - that will be used multiple times
    - on multiple distributed nodes
    - at the same time
    - each one will serve the nearest
- IPv6 Multicast Address
    - to many destinations
        - how many?
            - from 2 to all (all?)
            - which makes it a broadcast
    - it will be achieved (multi-destinations)
    - by assigning a group ID instead of an interface ID

- Internet Protocol Version 6 (IPv6)

- IPv6 Assignment Methods
    - as IPv6 is not that simple or short to be assigned
    - for every needing node in the environment
    - many methods can support granting IPv6 addresses
    - including
        - Manual: go and assign based on the design
        - SLAAC:
            - stateless and automatic
            - if the requesting interface found out an appropriate
            - global IPv6 address on the opposing end
            - it will request an address for itself, from that subnet
            - OR, if non were available
            - Link-Local would occur

- Transmission at Layer 4

- Transmission Communication Protocol & User Datagram Protocol
- Multiplexing at layer 4
- for multi-transmission of different techs. At the same time
- protocols can be
    - Reliable, connection-oriented, perform the 3-way handshake
        - TCP
    - Unreliable, connection-less, direct transmission
        - UDP
- some technologies considers the same port of both the protocols
- which by most, are taken from the well-known domain (0-1023)

TCP

HTTP = TCP80

HTTPS = TCP443

FTP = TCP20, 21

SSH = TCP22

Telnet = TCP23

SMTP = TCP25

BGP = TCP179

UDP

SNMP = UDP161

TFTP = UDP69

DNS = USP53

SYSLOG = UDP514

- Enterprise Networks Design

- Simplify Scaling & Troubleshooting
- Technologies should be distributed well, based on layers/tiers
- Depends on your networks size, and future growing

- Tier 2 will be for Small/Mid networks
    - One building network
    - only 2 Tiers (Access and Aggregation)
    - Access:
        - The first layer facies/authenticates endpoint devices
        - Connects the endpoints to their gateways (aggregation)
    - Aggregation:
        - Aggregates/Communicates all the access layers
        - Runs both Layer2 and Layer3 Techs. and Protocols
        - Run in pair-devices mode (SSO)

- Enterprise Networks Design

- Tier 3 for Mid/Large Enterprises
    - Multiple Buildings
    - More East-West traffic
    - Future scaling (Horizontally)
    - 3 Tiers (Access, Distribution, and CORE)
    - Core:
        - Aggregate multiple networks
        - High speed/convergence
        - Runs in pair-devices mode
        - Runs at Layer 3
        - Connects to the WAN/Internet
        - Connects to servers and other Data Centers

*Fabric Capacity Planning

- Enterprise Networks Design

- Spine and Leaf
    - Data Center networks connect and interconnect
    - considering the CLOS architecture
    - where leaves don't directly connect, neither spines
    - yet every leaf should have a direct link to every available spine
    - simply, the 3-Stage CLOS, super spines can lead to 5-Stage CLOS
- End Points will have
    - Layer 2 gateways (leaves)
    - Layer 3 gateways (spines)
    - VXLAN tunnels between the VTEPs (L2GWs)

- Enterprise Networks Design

- WAN
    - LANs connected/interconnected together
    - over an uncontrolled infrastructure
    - transported data should be
        - isolated, virtualized, and secured
    - VPN is the responsible technology
        - MPLS L3 VPN (MP-BGP, SR-MPLS, and others)
        - MPLS L2 VPN (L2VPN, L2Circuits, VPLS, EVPN)
- SOHO
    - Small size, small footprint, local connection
    - serves small offices (one or few broadcast domains)
    - serves home offices (one domain, with a possible VPN connection)

- IP Parameters for Client/End Device OS

- Useful Tools:
    - Ping: Availability Check
    - Traceroute: IP's in the Way
    - FTP: Data Transporting
    - SCP: Secure Data Transporting
    - Telnet: Remote Access
    - SSH: Secure Remote Access
    - Ipconfig: End Device IP Assignment
- PING:
    - Windows: Terminal --- Ping X.X.X.X
    - Mac OS: Terminal --- Ping X.X.X.X
    - Linux: Terminal --- Ping X.X.X.X

- IP Parameters for Client/End Device OS

- Traceroute:
    - Windows: Terminal (CMD) --- Tracert/Tracert –d X.X.X.X
    - Mac OS: Network Utility --- X.X.X.X --- Trace
    - Linux: Terminal --- Traceroute X.X.X.X
- Telnet & SSH:
    - Windows:
        - Telnet: Terminal --- Telnet X.X.X.X
        - SSH: Software (SecureCRT, PuTTY)
    - Mac OS:
        - Telnet: install Homebrew --- Terminal--- Telnet X.X.X.X
        - SSH: Terminal --- ssh X.X.X.X
    - Linux:
        - Telnet/SSH: Terminal --- Telnet/SSH X.X.X.X

- Device Virtualization

- Just Networks, BUT in Virtualized Environment
- Multiple Devices inside One
- Ease of Management

- The Hypervisor: The new Mediator between SW/HW
- Load the Hypervisor on the Physical HW, after that install OS on the Hypervisor
- Now the Hypervisor = Host, and the OS = Virtual Machines = Guest

- Hypervisors:
    - Schedules the VMs requests to the HW
    - Distributes the HW resources between the VMs

- Hypervisors Types

- Type-1 Hypervisors
    - The Native or Bare Metal
    - Runs directly on the HW resources
    - HW ---Hypervisor --- VM
    - Oracle VM, MS Hyper-V, WMWare ESXI
- Type-2 Hypervisors
    - Hosted
    - Runs as a SW besides the OS
    - HW --- OS --- Hypervisor
    - Virtual Box, VMWare Workstation

- Virtual Switches

- Connects all VMs Together like a Real Switch
- Assigns a Virtual Network Interface Card (V.NIC) for each VM
- Exists by default in Hypervisors Type1
- After Creating a vSwitch & vNIC, all VMs will automatically get connected together

*also, can create Port Group for Complete Isolating (like VLANs)

*there is another V.NIC for each VM (for Internet)

- Microsoft Hyper-V
- ESXi VSwitch

- Module-2: Network Access

2.1 Configure and verify VLANs (normal range) spanning multiple switches

2.1.a Access ports (data and voice)

2.1.b Default VLAN

2.1.c InterVLAN connectivity

2.2 Configure and verify interswitch connectivity

2.2.a Trunk ports

2.2.b 802.1Q

2.2.c Native VLAN

2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations

2.5.a Root port, root bridge (primary/secondary), and other port names

2.5.b Port states (forwarding/blocking)

2.5.c PortFast benefits

2.6 Compare Cisco Wireless Architectures and AP modes

2.7 Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)

2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)

2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

– Switching Concepts

- First were called “Bridges” and had Bridge Tables
- Bridges had low port Density

Then Switches came:

- Have MAC Learning based on the Device port
- Have MAC Tables
- Forwards Frames based on the MAC Table
- Have a Look-up Engine
- Look-up one frame only at a time (How fast?)
- Do Schedule Frame forwarding

- MAC Table

- Filled (learned) based on the Source MAC (The Dynamic Entry)
- Decision is taken, based on the Destination MAC
- Aging Time! What for? How often?
- Number of Entries per table
- What will happen if Destination MAC is unknown
    - “FLOODING

```
SW1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  1     0200.AAAA.AAAA    DYNAMIC     Gi0/2
  2     0200.BBBB.BBBB    DYNAMIC     Gi0/1
```

- ARP Table

- Since it is all about destination MAC's
- and since it is always local (elaborate!)
- then a mechanism should help to cooperate with IP Addresses

- ARP will bind a destination IP (local or remote) with a
- Destination MAC (local)
- for local switching to happen and deliver the frame with its packet

Address	Age	Hardware Addr	State	Type	Interface
10.4.1.1	-	000c.cfe6.3336	Interface	ARPA	GigabitEthernet0/3/1/3
10.4.1.2	01:37:50	0000.c004.0102	Dynamic	ARPA	GigabitEthernet0/3/1/3
10.1.4.2	-	000c.cfe6.33b5	Interface	ARPA	FastEthernet0/3/3/4
10.1.0.2	-	000c.cfe6.33b1	Interface	ARPA	FastEthernet0/3/3/0
10.1.0.1	00:37:56	000a.8b08.857a	Dynamic	ARPA	FastEthernet0/3/3/0
10.1.4.1	01:37:51	000a.8b08.857e	Dynamic	ARPA	FastEthernet0/3/3/4
10.11.1.1	-	000c.cfe6.32fa	Interface	ARPA	FastEthernet0/3/0/6
10.1.5.2	-	000c.cfe6.33b6	Interface	ARPA	FastEthernet0/3/3/5
10.1.1.2	-	000c.cfe6.33b2	Interface	ARPA	FastEthernet0/3/3/1
10.1.1.1	01:37:51	000a.8b08.857b	Dynamic	ARPA	FastEthernet0/3/3/1
10.1.5.1	01:37:50	000a.8b08.857f	Dynamic	ARPA	FastEthernet0/3/3/5

- Virtual Local Area Networks

- Can I separate hosts!
- What will each group of them become?
- Every single switch port must become either _____ or _____
- Access Ports
    - every switch port that is connected to an End device
    - NO Tags will be sent to the endpoints
    - tags will start from the access ports towards the switch internally
    - double tags can happen (Q-in-Q)
    - an access port can have 2 VLANs at the same time
        - one tagged (voice traffic)
        - one untagged (data traffic)

- VLAN Types

- Data VLAN: Ordinary
    - standard range: 1-1001
    - reserved range: 1002-1005
    - extended range: 1006-4096
- Voice VLAN: Voice data only (higher priority)
    - tagged and passed over access ports
    - one port for 2 VLANs (physically towards an IP Phone)
- Default VLAN: out-of-box operation
    - all the ports will be accessed to that VLAN (by default)
    - Tag ID = 1 (by default)
- Native VLAN: passes with no Tags
    - carries switches BPDU's even through pruning
    - VLAN reserved = 1 (by default)

- Static and Dynamic 802.1Q Trunking

- Trunk Ports: for switch ports that must carry more than one _____
    - Done by using encapsulation (802.1Q)

- Dynamic (enabled by default)
    - only requires one side to start negotiations
    - to cooperate and form Trunking between 2 opposite ports
    - negotiations can be “Disabled”
    - port roles are either “Dynamic Desirable” or “Dynamic Auto”
    - SLOW AND TAKES TIME !
- Static is to configure one or both ports
    - to become statically trunks using 802.1Q
    - no negotiations, no port roles

– VLAN’s Workorder

- *VLAN Creation*
  - *(config)#vlan <vlan-id>*
  - *(config-vlan)#name <value>*
- *Access Ports*
  - *(config-if)#switchport mode access*
  - *(config-if)#switchport access vlan <vlan-id>*
- *Trunk Ports (Static Trunking)*
  - *(config-if)#switchport mode trunk || modern switches*
  - *(config-if)#switchport trunk encapsulation dot1q || legacy switches*
- *Trunk Ports (Dynamic Trunking)*
  - *(config-if)#switchport mode dynamic desirable || start negotiations*
  - *(config-if)#switchport mode dynamic auto || listen for negotiations*
- *Native VLAN*
  - *(config-if)#switchport trunk native vlan <vlan-id>*

– VLAN’s Workorder

- *VLAN Pruning*
  - *(config-if)#switchport trunk allowed vlan <value/s> || first entry / overwrite*
  - *(config-if)#switchport trunk allowed vlan add <value/s> || add an entry*
  - *(config-if)#switchport trunk allowed vlan remove <value/s> || remove an entry*
  - *(config-if)#switchport trunk allowed vlan except <value/s> || except an entry*
- *Voice VLAN*
  - *(config-if)#switchport mode access*
  - *(config-if)#switchport voice vlan <vlan-id>*

- Spanning Tree Protocol

- We need redundancy and high availability
- but there will be a broadcast message, What will happen?
    - a “LOOP”, AKA “Broadcast Storm”
- STP / 802.1D operates at the control plane level
    - requires election to be performed first
    - The Winner must have the
        - Lowest Bridge ID
            - Lowest Bridge Priority.Lowest MAC Address
    - After that port roles and states will happen
        - Designated Port: Forwarding state D/F
        - Root Port: Forwarding State R/F
        - Alternative Port: Blocking State A/B

- Spanning Tree Protocol

- The entire process of election takes (30 – 50) Seconds

    Max Age = 20 + (Forwarding Delay = 15) + (Learning Delay = 15) = 50 Seconds

        - when it is an indirect link failure

    - Process = 30 Seconds (NO MAX AGE)

        - when it is a direct link failure!

- The matter is to keep eliminating the ports that should stay
- until the least needed port is determined

    - then, Alternative/Blocking

- in cases of >= 2 links between 2 adjacent switches

    - lowest port ID of the designated devise wins

*Designated devices (Root Bridges) sends superior BPDU's

*others will have an inferior BPDU's

*going through a pause or a cutout of receiving S.BPDU's will start generating them 😵

– STP Workorder

- *STP Root Bridge Setting*
  - *(config-)#spanning-tree vlan <vlan-id> priority <value>*
- *STP Port Cost Setting*
  - *(config-if)#spanning-tree vlan <vlan-id> cost <value>*

Port speed	Pre-802.1D-1998 Cost	802.1D-1998 Cost	802.1D-2004 Cost
10 Mbps	100	100	2000000
100 Mbps	10	19	200000
1 Gbps	1	4	20000
10 Gbps	1	2	2000

- Rapid Spanning Tree Protocol

- In order to speed things up:
    - Rapid STP / 802.1W: NO Listening, NO Blocking
    - only (Discard, Forwarding, Learning)
    - delay will become = 3 + 3 = 6 Seconds
    - proposal and agreement is a series of
    - superior and inferior BPDUs
    - starting from 1st to assume itself as a root bridge
    - until reaching an edge port

        Make it Deterministic

    - STP Loop Guard is absent here
    - S.BPDU's are automatically ignored on D/F ports of a Root Bridge

- Furthermore in STP

- What's the BIG benefit of Redundancy If STP is blocking ports
    - in cases of many VLANs all consuming the same D/F
    - There will be a Per-VLAN STP (PVST) / (RPVST+)
    - Each VLAN can have an ELECTION
    - Each VLAN will have its own root
    - Multiple different logical topologies
- Multiple Spanning Tree Protocol (MST) / 802.1S
    - Instances (Groups) that requires domain names/revision numbers
    - each instance will have its own tree
    - design practice: 150-250 VLANs should be per instance
    - the default, non-erasable instance 0 is the
        - shelter for those who doesn't have an instance assigned
        - the general root bridge of all the regions

- Neighbor Discovery

- Cisco Discovery Protocol & Link Layer Discovery Protocol

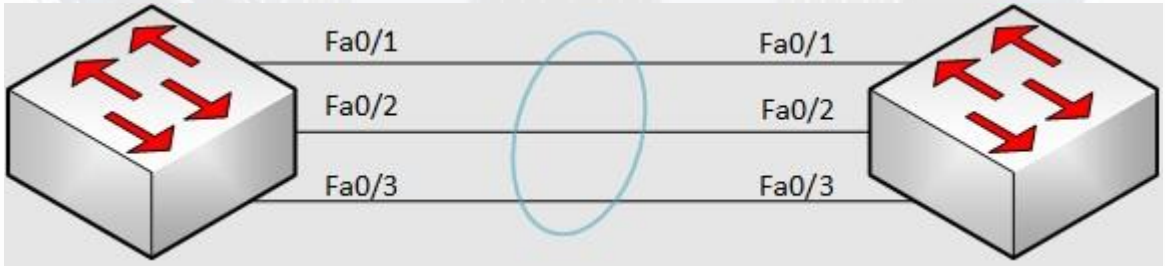
- Who am I connected to
- can depend on the protocol and the version
- CDP and LLDP do Discovery negotiations between devices

- Detailed information about the neighbor
    - My port that is connected to it
    - Its port that is connected to me
    - The IP Address of the neighbor device
    - The MAC Address of the neighbor device
    - Port description of the neighbor
- LLDP-MED is the highest flexible and useful one, carrying TLV's

– Link Aggregation (LAG)

- load balancing (distributing) the traffic flow
- among more than one link (if available)
- flow will be reordered and sent over multiple paths (per packet)
- LAG does not split a packet and consumes the bundle as a total

- Flow can be distributed per:
    - Basic Flow: MAC-to-MAC
      IP-to-IP
    - Micro Flow: L4-to-L4 port/protocol



- Static and Dynamic EtherChannels

- EtherChannels are supported on Cisco switches
- supporting both LACP and PAgP negotiations protocols
- it can be negotiation based (for L2)
- it can be static and fast (for L2 and L3)

- LACP uses:
    - Active: initiates bundling negotiations
    - Passive: waits for other side to initiate
- PAgP uses:
    - Desirable: initiates bundling negotiations
    - Auto: waits for other side to initiate
- Static:
    - Mode ON: no negotiations, direct bundling

– PO Workorder

- *Members bundling*
  - *(config-if)#channel-group <id> mode desirable* || *PAgP Negotiator*
  - *(config-if)#channel-group <id> mode auto* || *PAgP Listener*
  - *(config-if)#channel-group <id> mode Active* || *LACP Negotiator*
  - *(config-if)#channel-group <id> mode Passive* || *LACP Listener*
  - *(config-if)#channel-group <id> mode on* || *Static*

- AP Modes

- AP Modes
    - Local Mode
        - the default of a LAP
        - CAPWAP to the WLC
        - everything passes through the CAPWAP
        - if the CAPWAP fails, all clients will be disconnected
- Bridged Mode
    - allows an Autonomous AP to connect as a client to the LAP
- Flex Connect Mode
    - a hybrid Cisco solution for LAP's
- Monitor Mode
    - generates reports & statistics, send them to the WLC
- Sniffer Mode
    - scan a specific channel
    - send the scanning reports to the WLC

- AP Modes

- Sensor Mode
    - perform SSID tests
    - send test report to the DNA Center
- Mesh Mode
    - a frame might travel multiple mesh nodes
    - before reaching the LAN
    - uses adaptive wireless path protocol (AWPP)
    - to determine the best path to a root node/AP (RAP)

- AP Management

- some APs have a PoE & AUX ports in the back
- these 2 can be bundled/aggregated to form a higher bandwidth data interface
- WLCs have a Service/Management port, can have an IP address assigned to, for GUI access

- to bundle/aggregate ports:
    - WLC: use “channel-group mode on” on the switch, as it doesn’t support LACP/PAgP
    - AP: either using “ON” or “LACP”, BUT, only with “local” APs, not the “Autonomous” APs
- APs and WLCs are just like other networking devices
- they can be managed by CLI (console, telnet, ssh) and GUI (http and https)
- Authorization access can also be done using AAA

- Antenna Types

- Dipole Antenna
    - ordinary in Home-Routers
    - omnidirectional
    - low power gain
    - horizontal streaming only
- Yagi Antenna
    - linear in shape and in transmitting
    - sends in only one way!!
- Patch Antenna
    - also linear
    - but wider than Yagi
- Parabolic-Dish Antenna
    - outdoor, long distance
    - very high power gain
    - P2P connections
- Hidden Antenna (inside client devices)

- Module-3: IP Connectivity

3.1 Interpret the components of routing table

- 3.1.a Routing protocol code
- 3.1.b Prefix
- 3.1.c Network mask
- 3.1.d Next hop
- 3.1.e Administrative distance
- 3.1.f Metric
- 3.1.g Gateway of last resort

3.2 Determine how a router makes a forwarding decision by default

- 3.2.a Longest match
- 3.2.b Administrative distance
- 3.2.c Routing protocol metric

3.3 Configure and verify IPv4 and IPv6 static routing

- 3.3.a Default route
- 3.3.b Network route
- 3.3.c Host route
- 3.3.d Floating static

3.4 Configure and verify single area OSPFv2

- 3.4.a Neighbor adjacencies
- 3.4.b Point-to-point
- 3.4.c Broadcast (DR/BDR selection)
- 3.4.d Router ID

3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols

- The Forwarding Decision

- as a Router, I do separate Broadcast Domains
    - when receiving a packet, it stops at the Interface
    - Routing will decide how to Forward/Route the Packet

    - in the matter of:
        - first let us check the longest match for this prefix
        - then decide which routing protocol should handle this task
        - finally, the desired protocol will submit its own “Rules” (Metrics) to route the packet

- Static Route

- the only method of manually routing a specific packet to a specific route
    - the first next-hop can either be the egress interface Port ID
    - Or, the next reachable IP Address
    - Available for IPv4 & IPv6
    - can route a host or an entire network

- Static Route Flavors:
    - Default Route: every un-mentioned subnet to be routed here also, can be a default Gateway
    - Floating Static: a hidden back-up plan

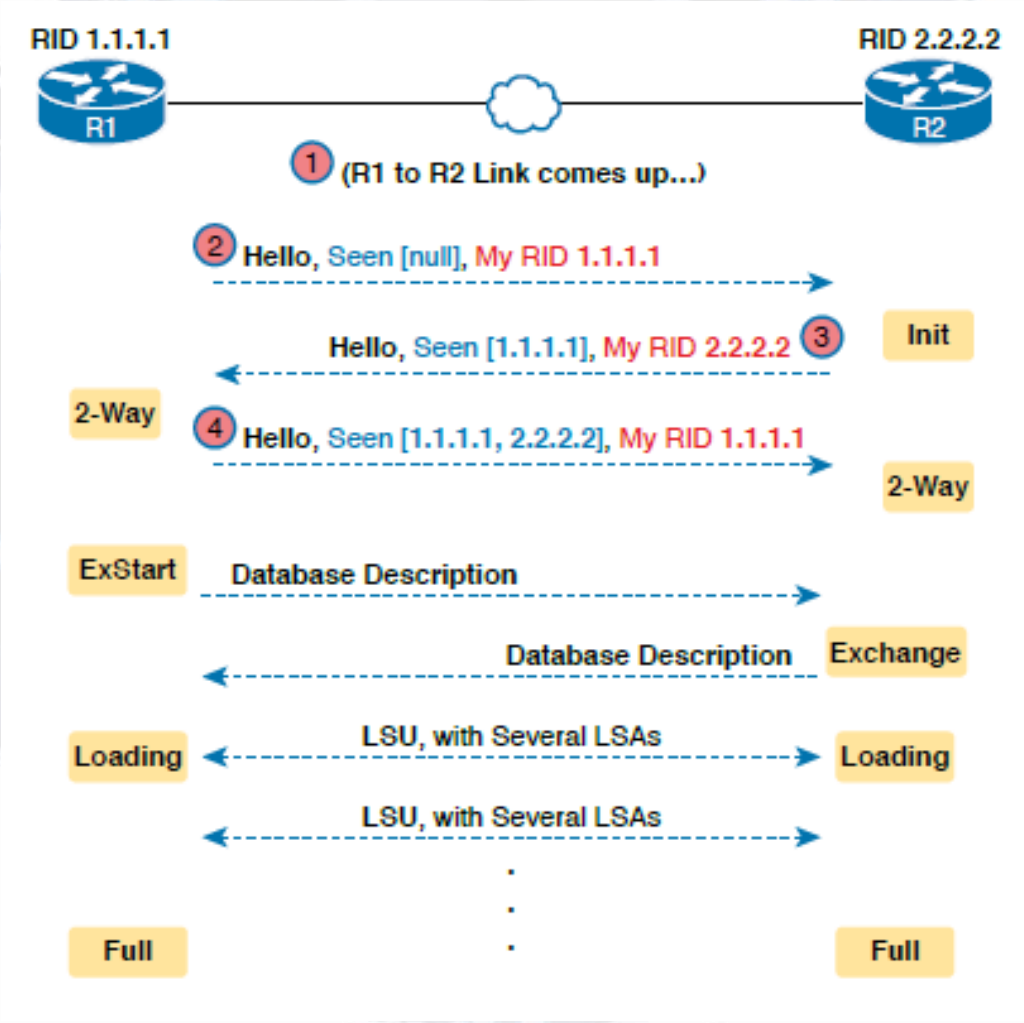
- Static Route Workorder

- Static Route
    - Router(config)#ip router <prefix> <prefix-length> <next-hop>
- Static Host Route
    - Router(config)#ip router <prefix> 255.255.255.255 <next-hop>
- Static Default Route
    - Router(config)#ip router 0.0.0.0 0.0.0.0 <next-hop>
- Floating Static Route
    - Router(config)#ip router <prefix> <prefix-length> <next-hop> <Higher AD Value>
- IPv6 Static Route
    - Router(config)# ipv6 route <prefix/length> <next-hop-egress-interface-name>
    - Router(config)# ipv6 route <prefix/length> <next-hop-address>
    - Router(config)# ipv6 route <::/0> <next-hop-address>

- Open Shortest-Path First (OSPF)

- Link State Protocol
- Dijkstra algorithm
    - SPF algorithm for route decision
    - AD = 110
- Metric = Cost (lesser = Better)
    - Process ID for multiple instances
    - Area ID for Data Base isolation
- Link-State Advertisements: negotiation between OSPF Routers
    - it contains:
        - LSRequest: provide the missing Information
        - LSUpdate: reply for the LSR
        - LSAcknowledgement: reply for the LSU

- OSPF Neighboring Process



- OSPF LSA's

- Link State Advertisements (LSA's)
    - multiple types
    - depends on the advertisement they are doing
        - LSA Type.1 (Router LSA): investigates local OSPF connections
        - LSA Type.2 (Network LSA): investigates local OSPF connections for a DR
        - LSA Type.3 (Network Summary LSA): for ABR to reach links in Areas
        - LSA Type.4 (ASBR Summary LSA): for ABR to reach ASBR's
        - LSA Type.5 (External LSA): for ASBR redistribution
        - LSA Type.7 (NSSA External LSA): for ASBR NSSA

- OSPF Neighbor Types

- A Neighboring router can be a P2P neighbor
    - in this case no problems
- or can be connected through a “SWITCH”!!
    - broadcast will happen
    - elections must take place
    - only One router should update the topology (DR)

- a DR (Designated Router): Highest Router Priority (0-255), Def=128
    - Or Highest Router ID
        - Router ID (R.ID): 32-bit Address
    - DR needs BDR (second best of everything)

- OSPF Routers Types

- Internal
    - participate only in a non-backbone area
    - generates Type-1 & Type-2 LSA's
- Backbone
    - participate only in a backbone area || area 0
    - generates Type-1 & Type-2 LSA's
- ABR
    - connects Backbone Area with any other Area
    - regenerates Type-1 LSA's into Type-3 LSA's and floods them
- ASBR
    - connects an OSPF to a non-OSPF network
    - floods Type-4 LSA's

- OSPF Workorder

- Router(config)#router ospf <process-id>
- Router(config-router)#router-id <32-bit value>
- Router(config-router)#network <prefix> <wild-card mask> <area-id>

OR

- Router(config)#interface <interface-name>
- Router(config-if)#ip ospf <process-id> <area-id>

- Verification
    - Router#show ip ospf database
    - Router#show ip ospf neighbors
    - Router#show ip ospf interfaces brief
    - Router#show ip ospf border-routers
    - Router#show ip route ospf
    - Router#show ip protocols

- First Hop Redundancy Protocol

- Establishes a virtual gateway between a router and its redundancies
- Virtual IP and Virtual MAC will be assigned
    - one vMAC means one GW at a time (Active/Standby)
    - multiple vMACs means multiple GWs at the same time (Active/Active)
- can be tracked and manipulated upon events
- protocols including “HSRP, VRRP, and GLBP”

HSRP
- Cisco Proprietary
- One vMAC
- MAC address range
0000.0C9F.F000 - 0000.0C9F.FFFF
- last 3 digits for group No.

VRRP
- Open Standard
- One vMAC
- MAC Address
00-00-5E-00-01-{VRID}
- in hex in internet standard bit-order
- preemption is enabled by default

GLBP
- Cisco Proprietary
- up to 4 vMACs
- MAC Addresses
0007.b400.XXYY
- where X = GLBP group number
- and Y = AVF number

- FHRP Workorders

- HSRP
    - Router(config-if)#standby <group-number> ip <virtual-address>
    - Router(config-if)#standby <group-number> priority <value>
    - Router(config-if)#standby <group-number> <preempt>
    - Router(config-if)#standby <group-number> track <track-id> decrement <priority-value>
    - Router(config-if)#standby <group-number> authentication md5 key-string <password>
- VRRP
    - Router(config-if)#vrrp <group-number> ip <virtual-address>
    - Router(config-if)#vrrp <group-number> priority <value>
    - Router(config-if)#vrrp <group-number> track <track-id> decrement <priority-value>
    - Router(config-if)#vrrp <group-number> authentication md5 key-string <password>

- Module-4: IP Services

4.1 Configure and verify inside source NAT using static and pools

4.2 Configure and verify NTP operating in a client and server mode

4.3 Explain the role of DHCP and DNS within the network

4.4 Explain the function of SNMP in network operations

4.5 Describe the use of syslog features including facilities and levels

4.6 Configure and verify DHCP client and relay

4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping

4.8 Configure network devices for remote access using SSH

4.9 Describe the capabilities and function of TFTP/FTP in the network

- Network Address Translation

- Maintain the privacy of the RFC1819 block
- Avoid address duplication possibility
- by translating private addresses to public ones
- also supports private to private translation (Carrier-Grade NAT)

- used to exhaust efforts and public address with
    - Static (one-to-one) and Dynamic (range-to-pool) NATs
- till the NAT Overload suggested to consider ports with translating
    - allowed for a public address to be consumed in thousands of operations
    - using different port numbers for each packet flow
    - up to 65,536 port
    - also known as the NAPT, and PAT

- NAT Workorder

- Static NAT
    - Router(config)# interface <global-network-facing-interface>
    - Router(config-if)# ip nat outside
    - Router(config)# interface <local-network-facing-interface>
    - Router(config-if)# ip nat inside
    - Router(config)# ip nat inside source static <inside-local-ip> <inside-global-ip>
- Dynamic NAT
    - Router(config)# ip access-list standard <acl-name>
    - Router(config-std-nacl)# permit <prefix> <wild-card-mask>
    - Router(config)# interface <global-network-facing-interface>
    - Router(config-if)# ip nat outside
    - Router(config)# interface <local-network-facing-interface>
    - Router(config-if)# ip nat inside
    - Router(config)# ip nat pool <pool-name> <first-address> <last-address> prefix-length <SM>
    - Router(config)# ip nat inside source list <list-name> pool <pool-name>

- NAT Workorder

- PAT
    - Router(config)# ip access-list standard <acl-name>
    - Router(config-std-nacl)# permit <prefix> <wild-card-mask>
    - Router(config)# interface <global-network-facing-interface>
    - Router(config-if)# ip nat outside
    - Router(config)# interface <local-network-facing-interface>
    - Router(config-if)# ip nat inside
    - Router(config)# ip nat source list <acl-name> interface <global-network-facing-interface> overload

– Network Time Protocol

- synchronizes nodes time with a timing source (NTP Server)
- based on UDP 123
- in Cisco systems, a node can be an: NTP Server, NTP Client
    - it can have an internal clock (not recommended)
- time is synchronized in a server/client relation
- a server should be directly attached to a timing source (Atomic Clock)
- to guarantee proper synchronization of communication between them
- stratum count should be in consideration
    - number of L3 hops to the NTP Server (Cisco Node attached to a clock)
    - if multiple were available, the lowest wins
    - max. of 16 supported
    - counted cumulatively (elaborate)

*NTP clients can behave as NTP servers to other nodes, after the synchronize with a server first

*this will cumulatively increase the stratum number

- NTP Workorders

- NTP Server
    - Router(config)#clock timezone <zone>
    - Router#clock set <clock> <date>
    - Router(config)#ntp master <stratum level>
    - Router(config)#ntp source <source-interface>
- NTP Client
    - Router(config)#ntp server <server-address>
    - Router(config)#ntp server <server-address> source <source-address>
- Router#show ntp status
- Router#show ntp associations

- Dynamic Host Configuration Protocols

- Dynamically (Automatically) check for who's asking for an IP address
- and assign based on the available pool (IPv6 supported)
- assignment can include
    - IP address
    - Subnet mask
    - Gateway
    - DNS server (main and backup)
    - predefined features (leased time)
- considers the DORA process
    - Discover (broadcast message to whomever might reply
    - Offer (unicast message back to the requester)
    - Request message (broadcast again to acquire the pack)
    - Acknowledge (unicast message to the server after installing the pack)

*IP Forwarding can translate a broadcast request to unicast and push it to a remote server (DHCP Relay)

- DHCP Workorder

- DHCP Server
    - Router(config)#ip dhcp excluded-address <single-address>
    - Router(config)#ip dhcp excluded-address <first-address-in-a-range> <last-address>
    - Router(config)#ip dhcp pool <pool-name>
    - Router(dhcp-config)#network <network-id> <subnet-mask>
    - Router(dhcp-config)#default-router <default-gateway-to-assign>
    - Router(dhcp-config)#dns-server <primary-server-address> <secondary-server-address>
- DHCP Relay
    - Router(config-if)#ip helper-address <destination-address-to-forward-to>

- Domain Name Server

- DNS ease the process of accessing services
- memorize the name of the domain instead of the IP address!
- solving and translating a request to a domain before pushing to the network
- maintaining the communication to always be per IP technology

- reverse DNS can resolve an IP address to its registered domain!
- DNS did reserve both TCP and UDP port number 53
- you would see UDP at most

- DNS server can have a private or a public address
- private is inside the network
- public is on the internet

- Simple Network Management Protocol

- Formally, a configuration transportation protocol
- currently, traps and notification (status) transportation protocol
- operates in the Server/Agent way
- a server would first request an agent to provide the latest updates on its status
    - it can include
        - device reachability
        - system and health status
        - interfaces status and current bandwidth
        - environmental parameters (depends on the agent)
- and agent has 2 components to reply to the server
    - MIB Object (generator of elements)
    - Agent (contact the server
- SNMP uses UDP 161/162 and it is recommended to deploy only SNMPv3

- System Loggings

- all what the system is recording about its operations
- classified and categorized per
    - level of severity
    - type of message
- normally it would show by default on the screen (Cisco Systems)
- from the Level 6 (information) up to Level 0 (emergency)
- except for the debug to be manually enabled
- as it is resources consuming
- Syslog has a server/client relation
- and uses UDP port number 514
- reporting can be to a remote server as well

0 = Emergency
1 = Alert
2 = Critical
3 = Error
4 = Warning
5 = Notification
6 = Information
7 = Debug

- Syslog Logging Types

- Console Logging: show logs to the console user
- Terminal Logging: show logs to Line VTY user
- Buffered Logging: store some logs in the RAM
- Remote Logging:
    - collect and send Syslog messages to a remote server
    - remote server must be reachable via an interface
    - remote server must have a Syslog Application
- monitoring will occur from the server side
- *Syslog Workorder:*

    Router(config)#logging host x.x.x.x

    Router(config)#logging traps (0 1 2 3 4 5, etc.)

    Router(config)#logging source-interface Loopback0

- SNMP & Syslog Workorders

- SNMP
    - Router(config)#snmp-server community <community-name> <ro>
    - Router(config)#snmp-server community <community-name> <rw>
    - Router(config)#snmp-server community <public> <rw>
    - Router(config)#snmp-server host <server-address> <community-name>
- Syslog
    - Router(config)#logging <server-address>
    - Router(config)#logging on
    - Router(config)#logging trap <severity-level>
    - Router(config)#logging trap <server-address> transport <protocol> port <destination-port>
    - Router(config)#logging source-interface <interface-name>

– Quality of Service

- if traffic was more than bandwidth!
- if congestion WILL happen, can some traffic be more preferred than another!?
- Generally, UDP will be preferred over TCP (TCP will automatically do A retransmission)
- QoS Tools that will do the specific desired “Preferring”:

(Classification & Marking, Policing, Shaping, Queuing, and Scheduling)

- QoS Components

- Classification & Marking
    - for the Ingress traffic/interface
    - Classification first, please classify this type of traffic, like: “UDP=High, Mail=Low”
    - Then, Marking, “Marks” the classified traffics to identify them uniquely in the network

*Classification usually happens by matching port numbers
    - if further recognizing is needed
    - Network-Based Application Recognition (NBAR)
    - recognized, identifies, and classifies a traffic
    - based on multiple variety of things
    - Word, Phrase, URL!!

- QoS Components

- Policing & Shaping
    - The Provider – Client Relation
    - Policing:
        - From the Provider side
        - Drop the exceeding ingress (Coming) traffic
        - or mark-down that traffic, to be dropped later in the network
    - Shaping:
        - From the Client side
        - To avoid misunderstanding, or unwanted behavior with the provide
        - Queues the excess egress (Outgoing) traffic in the “Egress Queue”
        - This is called “Queuing”

- QoS Components

- Queuing:
    - Dividing the Egress Queue, to multiple sub-queues
    - Each, is differentiated by “Priority”
    - To deal with classified packets

- Scheduling:
    - How to empty the sub-queues, by which criteria

- Congestion Management:
    - Tools for Queuing and Scheduling
    - Emptying the Queued traffic in the egress queue
    - WFQ, CBWFQ, PQ, LLQ, WRR, SRR, Shaping

- QoS Components

- Congestion Avoidance:
    - Tools to avoid congestion
    - Before even happening
    - At the ingress interface/s (receiving queue)
    - RED, WRED, WTD, Policing

- QoS Application in a Network
    - Integrated Services
        - unified settings all the way
        - uses The Resource Reservation Protocol (RSVP)
    - Differentiated Services
        - each hop has its unique settings
        - uses “Per-Hop Behavior” (PHB)

- QoS Polices

- Modular QoS Command-Line (MQC)
    - applying the QoS tools globally
    - multiple tools will be available for multiple ports/uses
    - requires 3 components to operate
        - Class-Maps
        - Policy-Maps
        - Service-Polices

- Class-Maps
    - create a list, that identifies/matches some characteristics of a traffic
    - classify those “matched” traffic
    - to provoke this list to operate, we will need a “Policy-Map”

- QoS Polices

- Policy-Maps
    - MATCH a Class-Map
    - to apply a specific action to its traffic (queue it, shape it, police it…)
    - the same Class-Map can be matched multiple time on multiple interfaces
    - each time, a different “action” will be taken!
    - to apply a “Policy-Map” to an interface/s
    - we will need a “Service-Policy”

- Service-Policy
    - apply a “Policy-Map” to an interface
    - either “INBOUND” or “OUTBOUND”

- Secure SHell

- An out-of-band (OOB) management protocol
- should target the management plane, and can target the data plane as well
- access a node remotely through Line VTY
- recommended after Telnet
- to use reliable transport protocol (TCP 22)
- alongside with encryption to protect the transported data
- requires hostname, domain-name, RSA keypair, and credentials to access
- recommended to use version 2
- and can support access-lists to match who’s allowed to access

- SSH Workorder

- Router(config)#hostname <name>
- Router(config)#ip domain-name <name>
- Router(config)#username <user> password <value>
- Router(config)#crypto key generate rsa
- Router(config)#ip ssh version 2

- Router(config)#line vty 0 4
- Router(config-line)#transport input ssh
- Router(config-line)#login local

- Data Transfer Protocols

- Volumes of data to be transferred remotely
- requires internal and/or external connection
- a server can host files for reference
- a transfer protocol can import and export files from and to the server

- File Transfer Protocol (FTP)
    - Reliable on TCP 20/21
    - supports authentication
    - no encryption (no security!)
- Trivial FTP (TFTP
    - Unreliable on UDP 69
    - no authentication
    - no encryption!

- FTP/TFTP Workorder

- FTP/TFTP Import
    - Router(config)#ip ftp username <server-username>
    - Router(config)#ip ftp password <server-password>
    - Router(config)#copy ftp://<server-address> <destination-directory>: <destination-filename>
- FTP/TFTP Export
    - Router(config)#ip ftp username <server-username>
    - Router(config)#ip ftp password <server-password>
    - Router(config)#copy <source-directory>:<filename> ftp://<server-address>

- Module-5: Security Fundamentals

5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

5.2 Describe security program elements (user awareness, training, and physical access control)

5.3 Configure and verify device access control using local passwords

5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

5.5. Describe IPsec remote access and site-to-site VPNs

5.6 Configure and verify access control lists

5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

5.8 Differentiate authentication, authorization, and accounting concepts

5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

5.10 Configure WLAN using WPA2 PSK using the GUI

- Security Concepts & Programs

- What do I have? And should I care about?
    - Asset: everything valuable (Docs, Info's, etc.)
    - Threat: Danger to Asset (Hacker, SW BUG, Environmental Disaster)
    - Vulnerability: Weakness (old Bug, missing Patch)
- Then we should consider Mitigation:
    - it has 3 types
    - Type 1: Technical/Logical Mitigation
        - Choosing the Correct Firewall
        - Choosing the Correct IPS
        - Choosing the Correct Design!

- Security Concepts & Programs

- Type 2: Administrative
- Things that you (The Network Admin.) decides and consider
- Like Policies & Procedures (The company agreed policies & procedures)
    - Written documents
    - Background check for new employees
    - Security awareness/periodically (remind them from time to time)
- And Password of course
    - Length (characters)
    - Complexity (Upper/Lower case, Numbers, Symbols)
    - Age (Minimum/Maximum Age for changing the Password)

- Security Concepts & Programs

- there are some Alternatives
    - 2 Factor/Multi-Factor Authentication
    - Done by using some biometrics and certificates
    - Besides passwords
    - Can be Physical Card (Identity Card)
    - One-Time Password (Mobile phone App)
    - Iris Scan, Fingerprints, Face recognition
- Type 3: Physical
    - This is an in-reality protection
    - like securing the devices inside racks
    - racks should have licked metal/glass door
    - all racks should be installed in a secured DC
    - Racks and DCs can be secured using Keys, Cards, Fingerprints

- Lines and password protection

- there are multiple ways to access a device
    - Line Console
        - through console port
        - can be accessed directly, no protection
        - can be protected by
            - assigning a login password
            - login password can/can't be encrypted
            - a second step of protection can be applied
            - the "enable password" method
            - will not work if the password is fully privileged
    - Line Aux
        - same as Line Console
        - through AUX port

- Lines and password protection

- Line VTY
    - for remote access
    - requires a remote session to be established
    - either by Telnet or SSH
    - multiple session can be established at the same time
    - through multiple lines
    - protection can also be by
        - login password
        - enable password
        - full privilege

- Lines Workorders

- Lines Password Protection
    - Router(config)#line con <0>
    - Router(config-line)#password <password>
    - Router(config-line)#login
    - Router(config)#line aux <0>
    - Router(config-line)#password <password>
    - Router(config-line)#login
    - Router(config)#line vty <0 4>
    - Router(config-line)#password <password>
    - Router(config-line)#login

- Lines Workorders

- Lines Credentials Protection
    - Router(config)#username <user> privilege <privilege-level> password <type> <password>
    - Router(config)#line con <0>
    - Router(config-line)#login local

    - Router(config)#line aux <0>
    - Router(config-line)#login local

    - Router(config)#line vty <0 4>
    - Router(config-line)#transport input <protocol/s>
    - Router(config-line)#login local
    - Router(config-line)#access-class <acl-number> <in>

- Generic Route Encapsulation

- Virtually create a P2P path
- adding an extra IPv4 header to the packet
- Virtually isolate some traffic in a path
- Across multiple hops
- Data will be “Encapsulated” at L3
- Source and Destination ports should be specified
- Virtual ports will be created on Tunnel ends

*NOT SECURED

*IPSec can help (GRE over IPSec, or IPSec over GRE)

*Site-to-Site VPN

- Internet Protocol Security

- packets travels unsecured
- any sniffer, analyzer, can read your data!
- IPSec is a set of tools
    - pick the set you like to secure your data
    - Confidentiality: Encrypt the data all the way
    - Data Integrity: Guarantees delivering original data
    - Authentication: only the trusted ends can communicate
    - Anti-Replay: only regenerated or duplicated packets
- To provide and establish all the CIA and R
    - Security Associations (SA) will be exchanged between the peers
    - things like (tools, algorithms, protocols, and keys) will be discussed

- Security Associations Parameters

- hashing: redistributing data by using an algorithm (MD5, SHA)
- encryption: locking data by using a 2-way algorithm
- shared passwords
- all of the above is either statically configured, or dynamically (IKE)

- Dynamic (Internet Key Exchange, IKE)
    - a group of SA's
    - end tunnels will negotiate their accepted SA's
    - IKE has versions 1 and 2
    - IKEv1 creates 2 Tunnels (in 2 phases):

- IKE Phases

- Phase1: establish an authenticated tunnel, it requires:
    - authentication (PSK or PKI)
        - PSK easier, PKI requires official certificate authorizer
    - encryption (DES, 3DES, or AES)
        - Cisco recommends ONLY AES
    - hash (SHA or MD5)
        - Cisco recommends ONLY SHA
    - DH group
        - Cisco recommends Group 19
    - lifetime (optional)
- Phase2: negotiates SA's between end points
    - (Destination, Data, and Transport Method)

*PSK requires Password

- GRE over IPSec Workorder

- GRE
    - Router(config)#interface Tunnel <id>
    - Router(config-if)#bandwidth <value>
    - Router(config-if)#ip address <address> <subnet-mask>
    - Router(config-if)#ip mtu <value>
    - Router(config-if)#Keepalive <period> <retries>
    - Router(config-if)#tunnel source <interface-name>
    - Router(config-if)#tunnel destination <vtep-destination-address>
- IPSec IKEv2 Phase-1
    - Router(config)#crypto isakmp policy <priority>
    - Router(config-isakmp)#authentication <pre-share>
    - Router(config-isakmp)#hash <sha256>
    - Router(config-isakmp)#encryption <aes>
    - Router(config-isakmp)#group <19>
    - Router(config)#crypto isakmp key <key-string> address <peer-physical-interface-address>

- GRE over IPSec Workorder

- IPSec IKEv2 Phase-2
    - Router(config)#crypto ipsec transform-set <set-name> <esp-aes> <esp-sha-hmac>
    - Router(cfg-crypto-trans)#mode <transport>
    - Router(config)#ip access-list extended <acl-name>
    - Router(config-ext-nacl)#permit gre host <source-peer-address> host <destination-peer-address>
    - Router(config)#crypto map <map-name> <priority> <ipsec-isakmp>
    - Router(config-crypto-map)#match address <acl-name>
    - Router(config-crypto-map)#set transform <set-name>
    - Router(config-crypto-map)#set peer <destination-peer-address>
    - Router(config)#interface <source-peer-physical-interface>
    - Router(config-if)#crypto map <map-name>

- Access Control List

- specific permissions for users/ networks
- limits reachability and access
- by using allow/deny rules
- ACL Types
    - Standard
        - based on source host/network
        - range of 1-99
        - NO specific permissions
    - Extended
        - based on source & destination hosts/networks/ports/services
        - range of 100-199
        - specific in detail permissions (L4 & L5 perimeters)
    - Named: A Combination, Hierarchy Mode, Name for each list

- ACL Workorders

- Standard Numbered ACL
    - Router(config)# access-list <Number> <deny/permit> <prefix> <wild-card-mask>
    - Router(config)# access-list <Number> <deny/permit> host <host-address>
    - Router(config)# access-list <Number> <deny/permit> any
    - Router(config)# interface <interface-name>
    - Router(config-if)# ip access-group <Number> <in/out>
- Extended Numbered ACL
    - Router(config)# access-list <Number> <deny/permit> <protocol> any any eq <port-number>
    - Router(config)# access-list <Number> <deny/permit> <protocol> any any
    - Router(config)# access-list <Number> <deny/permit> <prefix> <wild-card-mask>
    - Router(config)# access-list <Number> <deny/permit> host <src-host-address> host <dst-host-address>
    - Router(config)# access-list <Number> <deny/permit> <protocol> any
    - Router(config)# interface <interface-name>
    - Router(config-if)# ip access-group <Number> <in/out>

- ACL Workorders

- Named Standard/Extended ACL
    - Router(config)#ip access-list extended <acl-name>
    - Router(config-ext-nacl)#<deny/permit> <protocol> any any
    - Router(config-ext-nacl)#<deny/permit> <prefix> <wild-card-mask>
    - Router(config-ext-nacl)#<deny/permit> <protocol> any
    - Router(config)# interface <interface-name>
    - Router(config-if)# ip access-group <acl-name> <in/out>
- Time-Based ACL
    - Router(config)# clock set <clock-time> <calendar-date>
    - Router(config)# time-range <range-name>
    - Router(config)#periodic <type> <time-period>
    - Router(config)# ip access-list extended <acl-name>
    - Router(config-ext-nacl)#<deny/permit> <protocol> any time-range <range-name>
    - Router(config)# interface <interface-name>
    - Router(config-if)# ip access-group <acl-name> <in/out>

- ACL Workorders

- VLAN ACL
    - Switch(config)# ip access-list extended <acl1-name>
    - Switch(config-ext-nacl)#<deny/permit> <prefix> <wild-card-mask>
    - Switch(config)# ip access-list extended <acl2-name>
    - Switch(config-ext-nacl)#<deny/permit> <protocol> any any
    - Switch(config)# vlan access-map <map-name> <sequence-number>
    - Switch(config-access-map)# match ip address <acl1-name>
    - Switch(config-access-map)# action <forward/drop/log>
    - Switch(config)# vlan access-map <map-name> <sequence-number>
    - Switch(config-access-map)# match ip address <acl2-name>
    - Switch(config-access-map)# action <forward/drop/log>
    - Switch(config)# vlan filter <map-name> vlan-list <vlan-id/s>

- Port Security

- Switch Ports connects you immediately
- A limitation is needed to the switch ports
- This limitation includes
    - The No. of learned MAC Addresses
    - Only “Statically” assigned MAC Addresses are allowed to connect
    - A combination of the 2 above

*All Cisco Switch Ports are “Dynamic” by Default, Make them Access

*Static Ports DON’T have timers, assign timers

*Those “Statically” assigned MACs are called “Sticky”

- What will be the reaction when an unallowed MAC/s hits?
    - Violation
        - Shutdown the port (Default)
        - Protect (Silently)
        - Strict (log it)

- Port Security Workorder

- Switch(config)#interface <interface-name>
- Switch(config-if)#switchport port-security
- Switch(config-if)#switchport port-security maximum <max-number-of-learned-macs>
- Switch(config-if)#switchport port-security mac-address <mac-address>

- DHCP Snooping

- Rouge DHCP Servers will respond to your “Discovery” message
- Computers will take/accept the first offer they receive

- Snooping will trust an interface to make it the
    - Only interface allowed to receive Broadcast Messages
- Applied on a specific VLAN

*Rouge Servers will Act as a “Man in the Middle”, which is an attack

– Dynamic ARP Inspection

- First, what is ARP
    - Address Resolution Protocol: Binds an IP Address to Its Source MAC Address
    - so, if a binding is missing, an ARP will handle it
    - but ARP is a Broadcast, thus, everyone will know about you trying to Reach your GW for any purpose
    - Someone might manipulate you and claim that he is the GW!
        *Man in the Middle detected
    - DAI will allow only trusted interfaces to receive and forward Broadcast
    - It will cooperate with the DHCP Snooping DB to perform
    - After inspecting, it will either Forward the ARP, or Drop it (LOG)

    *Static IPs don't use DHCP
        - Drop the ARP
        - or, Trust the Port
        - Create ARP ACL

- DHCP Snooping & DAI Workorders

- DHCP Snooping
    - Switch(config)#ip dhcp snooping
    - Switch(config)#interface <trusted-interface-name>
    - Switch(config-if-range)#ip dhcp snooping trust
    - Switch (config)#ip dhcp snooping vlan <vlan-to-protect>
    - Switch(config)#no ip dhcp snooping information option

* After DHCP Snooping
- Dynamic ARP Inspection
    - Switch(config)#ip arp inspection vlan <vlan-to-inspect>
- Static ARP Inspection
    - Switch(config)#arp access-list <acl-name>
    - Switch(config-arp-nacl)#permit ip host <host-ip> mac host <host-mac>
    - Switch(config)#ip arp inspection filter <acl-name> vlan <vlan-assigned-to-host>

- Authentication & Authorization using AAA

- Using the 3 farmwork protocol AAA
- Authentication, Authorization, and Accounting
- the framework requires a carrier protocol such as
    - RADIUS: best for secure network access
        - supports EAP
    - TACACS+: best for network device access
        - supports flexible authorization

CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide

Component	RADIUS	TACACS+
Protocol and port(s) used	Cisco's implementation: ■ UDP: port 1645 (authentication and authorization) ■ UDP: port 1646 (accounting) Industry standard: ■ UDP: port 1812 (authentication and authorization) ■ UDP: port 1813 (accounting)	TCP: port 49
Encryption	■ Encrypts only the password field ■ Supports EAP for 802.1x authentication	■ Encrypts the entire payload ■ Does not support EAP
Authentication and authorization	■ Combines authentication and authorization ■ Cannot be used to authorize which CLI commands can be executed individually	■ Separates authentication and authorization ■ Can be used for CLI command authorization
Accounting	Does not support network device CLI command accounting	Supports network device CLI command accounting
Primary use	Secure network access	Network device access control

- AAA Notes

- Remotely
    - by AAA server
    - uses either RADUIS or TACACS+ protocols
    - all the profiles will be created in the server
    - for every login session, the node will ask the server
    - for all the AAA perimeters
    - losing the connection to the server, with no local model
    - will lose access to the node
- Privilege Levels
    - privilege level 0—Includes the disable, enable, exit, help, and logout commands
    - privilege level 1—Includes all user-level commands at the router> prompt
    - privilege level 15—Includes all enable-level commands at the router> prompt

*default privilege for Line VTY = 1

*default privilege for Line Console 0 = 15

- AAA Workorders

```
aaa new-model
tacacs server <server-name>
  address <server-address>
  key <server-key>
tacacs server <server2-name>
  address <server2-address>
  key <server2-key>
aaa group server tacacs+ <group-name>
  server name <server-name>
  server name <server2-name>
```

- AAA Workorders

aaa authentication login default group <group-name> local

aaa authentication login <custom-list-name> local line enable

aaa authentication enable default group <group-name> enable

aaa authorization exec default group <group-name> if-authenticated

aaa authorization exec <custom-list-name> none

aaa authorization commands 0 <custom-list-name> none

aaa authorization commands 1 <custom-list-name> none

aaa authorization commands 15 <custom-list-name> none

aaa authorization commands 0 default group <group-name> if-authenticated

aaa authorization commands 1 default group <group-name> if-authenticated

aaa authorization commands 15 default group <group-name> if-authenticated

aaa authorization console

aaa authorization config-commands

- AAA Workorders

aaa accounting exec default start-stop group <group-name>

aaa accounting commands 0 default start-stop group <group-name>

aaa accounting commands 1 default start-stop group <group-name>

aaa accounting commands 15 default start-stop group <group-name>

line con 0

authorization commands 0 <custom-list-name>

authorization commands 1 <custom-list-name>

authorization commands 15 <custom-list-name>

authorization exec <custom-list-name>

privilege level 15

login authentication <custom-list-name>

line vty 0 4

<uses default method-lists for AAA>

- Wi-Fi Security

- Unsecured WLANs are the once with no password, free, and public
    - Secured WLANs might have:
        - hidden SSID
        - Authentication
        - Encrypt Data (from the client to the AP)
- Authentication can be done by:
    - authenticating the user's credentials
    - authenticating a device's MAC Address
    - captive portal

- Wi-Fi Security

- Extensible Authentication Protocol (EAP)
    - transport protocol
    - carries authentication information
    - can not travel directly in the network
    - must be encapsulated before injected in the media
        - 802.1x (Client – WLC)
        - RADIUS (WLC – AAA Server)
- Web Authentication (WebAuth)
    - applied and enabled on a WLC
    - to authenticate through a Web Browser
    - carried by HTTP
    - also requires 802.1X to be activated on the authenticator
    - supports Pre-shared Key to encrypt user data
- Pre-Shared Key
    - used to encrypt data between client and AP
    - same PSK can be used with all the clients connecting to the same AP
    - derived from the Passphrase

- Encryption in Wireless Networks

- for data frames only
    - Management frames won't get encrypted
    - happens between client and AP only
    - what's beyond AP (the LAN) is not encrypted
    - to have an end to end encryption:
        - use HTTPS
        - that will send a digital certificate between the src and dst
        - thus, the entire path will be encrypted

- Encryption in Wireless Networks

- Wi-Fi Protected Access (WPA)
    - has 2 types (Personal and Enterprise)
    - Personal:
        - uses a passphrase (statically assigned password in the AP)
        - uses a 256-bit pre-shared key for encryption
        - this pre-shared key is derived mathematically from the passphrase
        - this pre-shared key utilizes RC4 + TKIP, and MIC for generating the pre-shared key
        - TKIP every packet with a unique key

- Encryption in Wireless Networks

- WPA in Enterprise
    - uses 802.1X (supplicant, authenticator, authentication Server)
    - packets carried by EAP
    - 802.1X will happen only between the supplicant and the authenticator
    - the rest (authenticator, to the authentication server) will be RADIUS
    - after the authentication is done, comes the encryption
    - encryption is done by the authentication server
    - which will give each client, a unique key

- Encryption in Wireless Networks

- WPA2
    - also have a personal and enterprise modes
    - now it uses AES-CCMP instead of RC4+TKIP
    - Personal:
        - also, uses passphrase
        - also, the pre-shared key is derived from the passphrase
        - also, encryption happens from the client to the AP
        - supports AES-CCMP, and, RC4+TKIP
    - Enterprise:
        - 802.1X in Ad-Hoc mode (ignore that)
        - 802.1X supports re-authentication (faster)

- Encryption in Wireless Networks

- WPA3
    - personal and enterprise modes are here
    - it supports “Enhanced Open” Wi-Fi (like airports)
    - it supports “Wi-Fi Easy Connect” (for IoT)
    - Personal:
        - no pre-shared key
        - SAE instead
        - the derived key now is not related to the passphrase
        - protects against offline dictionary attacks
        - uses “Protocol Management Frame” (PMF)
            - encrypt some Management Frames
    - Enterprise
        - uses PMF
        - uses 192-bit minimum cryptographic security suite

- Module-6: Automation & Programmability

6.1 Explain how automation impacts network management

6.2 Compare traditional networks with controller-based networking

6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)

- 6.3.a Separation of control plane and data plane
- 6.3.b North-bound and south-bound APIs

6.4 Compare traditional campus device management with Cisco DNA Center enabled device management

6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible

6.7 Interpret JSON encoded data

- The Automation Impact

- Network automation is a scheme that can be achieved in ways of
    - preparing a script to accomplish a task instead of typing the commands one by one
    - using tools to generate scripts in different structuring languages
    - using platforms to push scripts to multiple nodes automatically
    - running persistent scripts to troubleshoot an issue in a network and understand its nature
    - all of which can be built-in, or manually/automatically pushed to nodes from outside controller
- Automation impact
    - shorter period of time for configuring nodes
    - less chances of human-mistakes while configuring
    - preparing a pre-defined stable and tested templates of scripts and policies
    - using data modeling to have general raw modules that can automate over different platforms
    - having the possibility to manage nodes from a single login point of control

- Traditional vs Controller-based Networks

- Traditional Networks
    - Each network device has its own control plane
    - Configuring, modifying, upgrading, and Monitoring is done “Box-by-Box”
    - Automation is more difficult
    - New Installation requires “from scratch” efforts

- Controller-Based Networks
    - Centralized Management
    - Through a “software” you be able to run and administrate an entire network
    - Automation is easy (API)
    - New devices automatically finds an initial configuration (ZTP)

- What is SDN?

- where a “software” runs a network
- and the software will have discovering features to
    - analyze, visualize, troubleshoot, maintain, and monitor the network
    - through a single pane-of-glass
- that will need either a “Controller”
- for example
    - Cisco SDA using DNA for Enterprise Networks
    - Cisco Viptela SD-WAN for WAN Edge-to-Edge Networks

- SDN Implementation & Effect upon planes

- Imperative Approach
    - the control plane logic resides completely in the controller
    - the controller has a complete control over programing the
        - forwarding decisions of the networking devices
    - devices then will ask the controllers before any forwarding or routing action

- Declarative Approach
    - the control plane resides within the network device (just like before)
    - the controller will declare the requirements of the all the
        - forwarding/routing decisions to the networking devices
    - the network devices will then decide how to translate the controller instructions into actions

- Application Programming Interfaces

- APIs are the carriers of instructions between 2 components of a network
    - components can be internal within a node
    - or external between nodes
- an API requires careful structuring to build and test before launching
- API components to construct are
    - Methods: HTTP methods to cooperate with a device and express the intended operation
        - HTTP Methods: GET, PUT, POST, and DELETE
    - Objects: the requested information with its description (address)
        - to inform the target about what do the API seek here
    - Format: the proper encoding language used to construct the request and/or reply of the API
        - represents the “body” of the API
        - can be in XML or JSON

- API Types per Region

- Northbound APIs
    - orchestrator to controller, and controller to orchestrator
    - mostly, and heavily mostly a REST-BASED APIs
    - instructions about investigations, analyzing, monitoring, inventory management,
    - topology discovering, maintaining and managing network nodes
    - all in the northbound section of an SDN network
    - occasionally it happens between internal component of a solution (Cisco DNA)
- Southbound APIs
    - upon generating instructions from an orchestrator
    - specific instructions meant to visit the networking nodes (routers, switches, etc…)
    - the controller would generate a southbound api and push it southbound!
    - a reply back from the nodes should be converted to northbound and reported to the orchestrator
    - within that area, SSH/SNMP/NETCONF are used to login and push to the nodes

- Software-Defined Access

- An SDN solution from Cisco
- for Cisco Enterprise networks to get
    - onboarded
    - tunneled
    - controlled and automated
    - visualized and policed
- by changing the concept of networking layers and planes to
    - Physical layer (Cisco and Cisco supported nodes)
    - Network Layer (migrate the Access-to-Core infrastructure to L3 underlay/overlay)
    - Controller Layer (integrate Cisco DNA & Cisco ISE with the infrastructure)
    - Management Layer (start implementing underlay, overlay, and policing services from GUI)

- Software-Defined Access

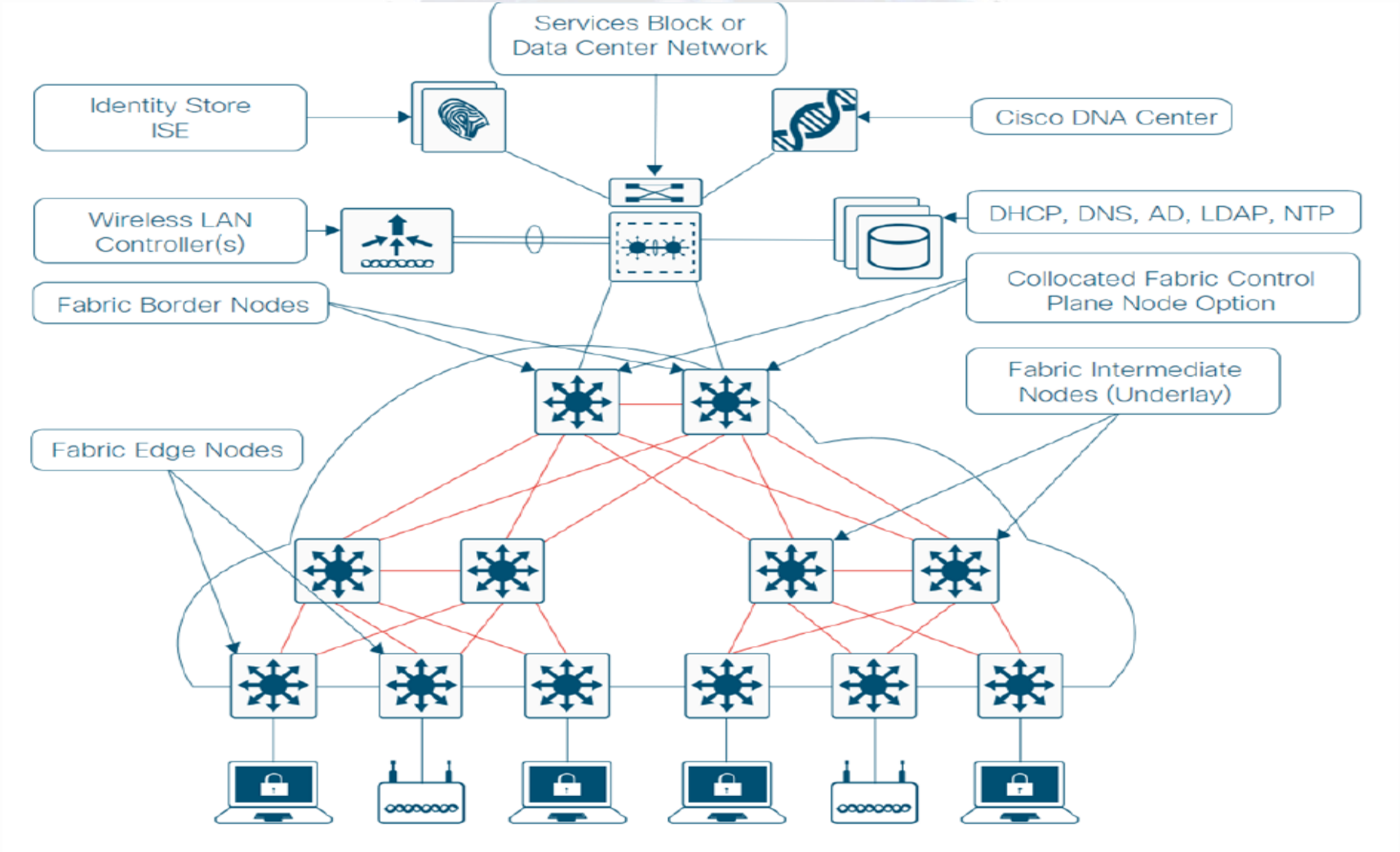
- Cisco SDA is where:
    - Access-to-Core will deal in L3 fashion only
    - routing will be underlay, tunneling will be overlay
    - LISP and VXLAN will route and forward packet between
        - Fabric Edge Nodes (Access-Layer-Switches)
        - Fabric Border Nodes (Core-Layer-Routers)
    - tunnels will assure these VTEPs will see each other directly
    - through the Fabric Intermediate Nodes (Distribution-Layer-Switches)
    - TrustSec (Security Group Tags, GPO) will manage security policing

*All devices participating in the SDA Fabric are named “Fabric Nodes”

- this can include Routers, Switches, Firewalls, WLCs, and APs

*devices that do not operate under the DNA control but connect to the fabric are “extension nodes”

- Software-Defined Access



http://cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.pdf

- Encoding Languages

- Structuring information into format
- using XML, JSON, YAML
- can be converted to and from python for integration
- JSON forms the vast-majority of REST-API's requests data
- Postman is a FREE solution to push and pull REST-API's containing JSON data format
- JavaScript Object Notation (JSON)
    - simple, human-readable encoding language
    - using curly braces { } and square brackets [ ]
    - depending on the key:value pairs
- JSON Values
    - always surrounded by a curly bracket { }
    - name:value pairs
    - a string must be enclosed with double quotes " "
    - like = {"name":"III", "job":"channel", "location":"YouTube"}

- JSON Encoding

- String:String
    - the name is a string, also the value is a string
    - {“name”:”III”}
- String:Number
    - the value won’t need a double quote
    - {“Count”:10}
- String:Arrays
    - for a range of values
    - {“Class”:[A, B, C, D]}
- String:Booleans
    - True/False case
    - the value won’t need a double quote
    - {“Direct”:False}
- Null
    - {“Route”:Null}

- HTTP Response Parts

- for every successful attempt of an API request
- a response is expected to return
- containing the following
    - Response Code
        - first indicator of the API health
        - 1XX:Informational | 2XX: success | 3XX: redirection | 4XX: client-side issue | 5XX: server-side error
    - Header
        - brief info. About the type and content of the API coming
        - also carries info. About Authentication, Authorization, and others…
    - Body
        - the requested information are included there
        - written by XML, or JSON

- HTTP Response Codes

Code	Label	Reason
100	Continue	The server received the request and is in the process of giving the response.
200	OK	The request is fulfilled
201	Created	Request was fulfilled and the requested resource was created
202	Accepted	Request has been accepted for processing, but not completed
301	Move permanently	The resource requested has been permanently moved to a new location.
400	Bad Request	The server could not interpret or understand the request
401	Unauthorized	The requested resource is protected and requires the client's credentials
403	Forbidden	The server refuses to supply the resource, regardless of the identity of the client
404	Not Found	The requested resource cannot be found on the server
500	Internal Server Error	The server might have an error in the server-side program responding to the request
502	Bad Gateway	The proxy or gateway indicates that it received a bad response from the upstream server
503	Service Unreachable	The server cannot respond due to overloading or maintenance.

- REST API Security

- The most common type of web-service API
- utilizes HTTP verbs (GET, PUT, POST, DELETE)
- any person is allowed and able to use it
- by using any types of service that is carried by HTTP/HTTPs

- securing the API's is important
- meaning securing the content sent and the content received
- authentication and authorization are required to limit privileges
- encryption is mandatory whenever possible (API Keys)
- secure the encoding "JSON" by using JSON Web Token (JWT)
- secured Certificates are needed, use HTTPs
- better to start the limitation of privileges by:
    - denying everything from everyone
    - start giving permissions based on real privileges

- Orchestration Tools

- Automation and Scripting Programs
- can be installed on a server already operating an OS
- login and automate config on devices
- can store the config and push it later
    - either scripts, IOS, YAML, Ruby, or GUI

- Master/Agent Relation
    - each component should be installed on its side
    - agent mostly is built-in
    - some programs are agentless
    - just directly pushes the config to the nodes
        - push, to send immediately or at a schedule
        - pull, a client asks if there is a change periodically

- Orchestration Tools

- Puppet and Chef uses the “Pull” model
    - utilizes Ruby language
    - Agents
    - config file of puppet is named "Manifest"
    - config file of chef is a per vendor
        - cookbooks that include recipes
- Ansible uses the “Push” model
    - An Open-Source Orchestration tool
    - utilizes YAML language
    - considers the “Push” model
        - where the clients stay calmly still
        - till Ansible push to the something new
    - it is Agentless by default
    - Ansible can SSH to the nodes and push the script
    - config file of Ansible is a playbook.yaml
        - inside the playbook, there are some plays
        - each play contains a group of tasks (to perform)

- Orchestration Tools

- Saltstack
    - Agent mode and Server Mode
        - utilizes YAML language
        - Python is an option as well
        - The relationship is a “master – minion” relation
    - internal components:
        - reactors: resides in the master, synchs with the nodes
        - beacons: resides in the minions, synchs with the server
        - this process = remote execution system
    - SaltStack is fast, secured, compatible,
    - no plugins required, but utilizes more resources
    - SaltStack SSH (Server-Only Mode): minion-less mode, SSH directly