CHAPTER 1

NETWORK FUNDAMENTALS

Cisco Certified Network Associate (200-301 CCNA)

- CHAPTER 1: NETWORK FUNDAMENTALS

- What is a Network?

Also called (Computer Network), it is 2 or more devices needs to/sharing 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 -

Cisco Certified Network Associate (200-301 CCNA)

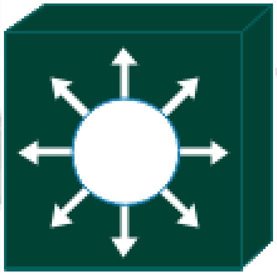
1.1 Network Components:

1 – Routers: Network devices that connect different network domains and routes the IP packets to its correct destinations.

- Each interface is ___________________

2 – Switches: Network devices that connects 2 or more devices in one network domain.

- Then what is a Multi-Layer Switch? , MLS, L3Switch?



3 – Firewalls and Intrusion Prevention Systems:

- Firewalls protects you from the internet Apply some restrictions to your local network

- Intrusion Prevention Systems (IPS) Do deep packet inspection (DPI) Try to spot attacks

*There is a 2 in 1 solution

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

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

5 – Controllers:

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

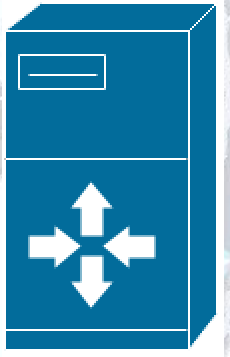
B - Cisco DNA Center: the super powerful, super capable central point of management for??

- Analytics
- Automation
- Using GUI to Design, Display, and Configure

6 – 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.



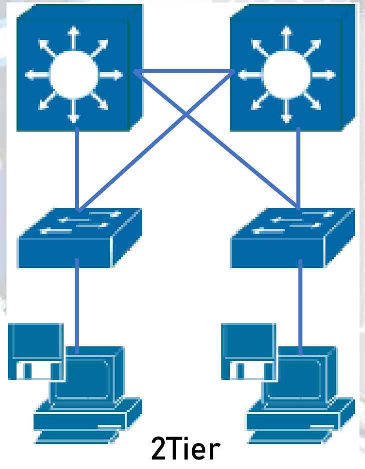
7 – Virtual Machines: ……………………………………………………………………………………………………….

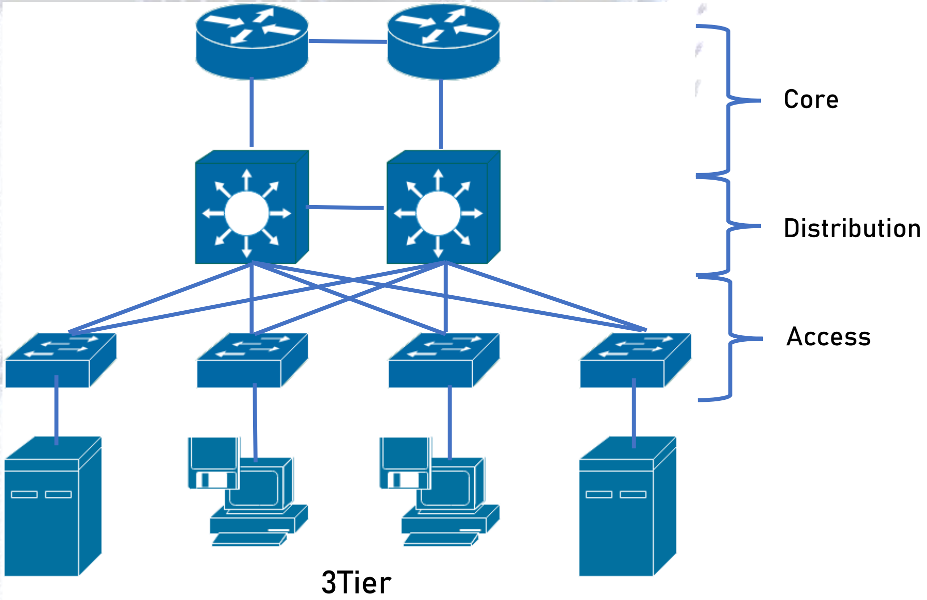
1.2 Network Topologies:

1 – 2Tier & 3Tier: Typical for Enterprise & Campus Networks Which came first? And what is the difference

- Core → Distribution → Access (3 Tier)
- Aggregation → Access (2 Tier)

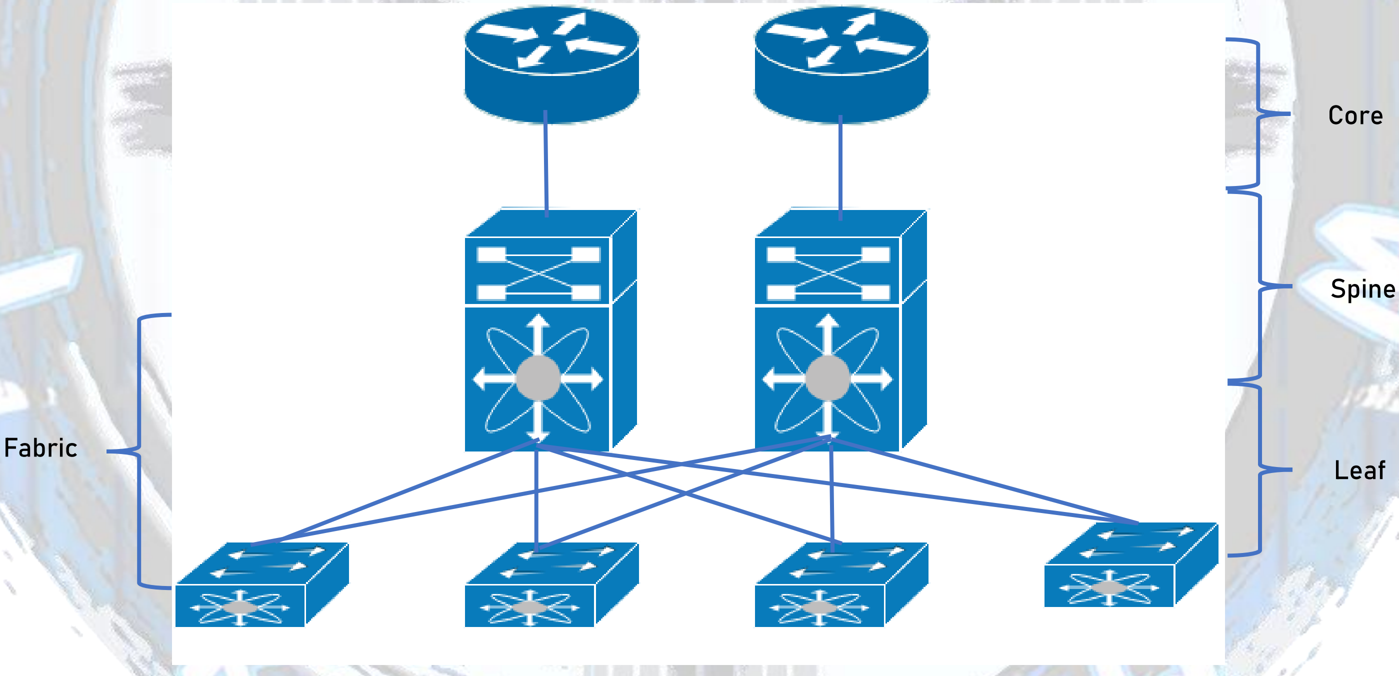
- Access ⇒ Authentication
- Distribution ⇒ Fast Convergence





2 – Spin & Leaf: Especially for Data Centers

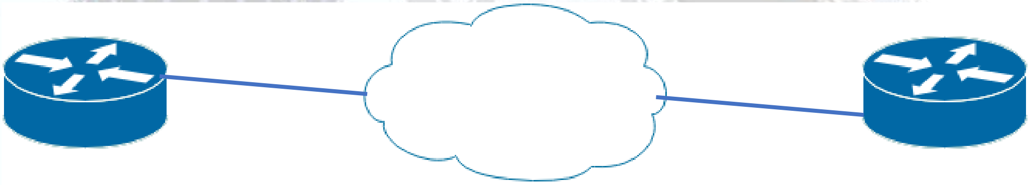
- Special Switches (Nexus)
- Full Redundancy
- NO Outage



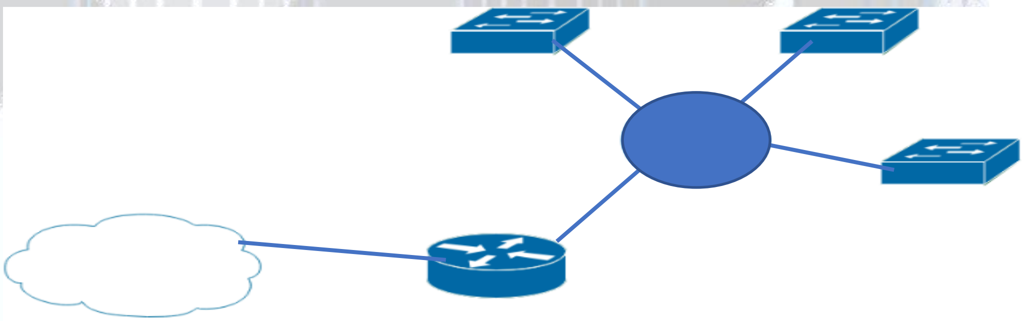
3 – Wide Area Networks Topology (WAN):

- It can be on 3 types:

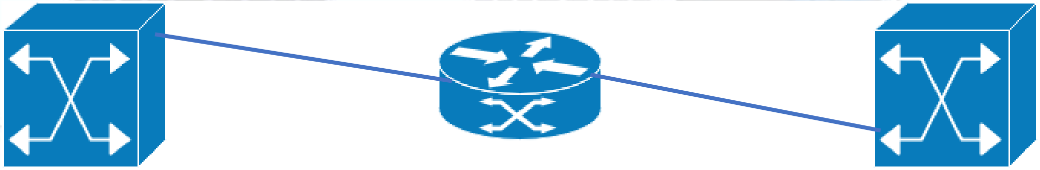
A- Point to Point (P2P)



B – Broadcast (MetroE)

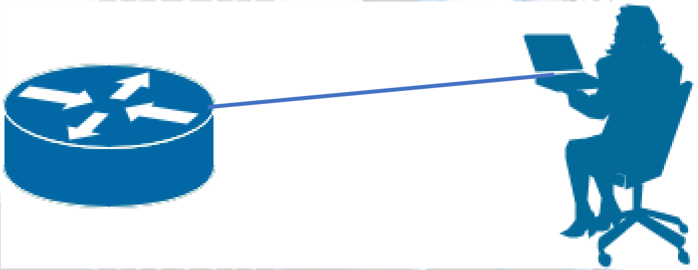


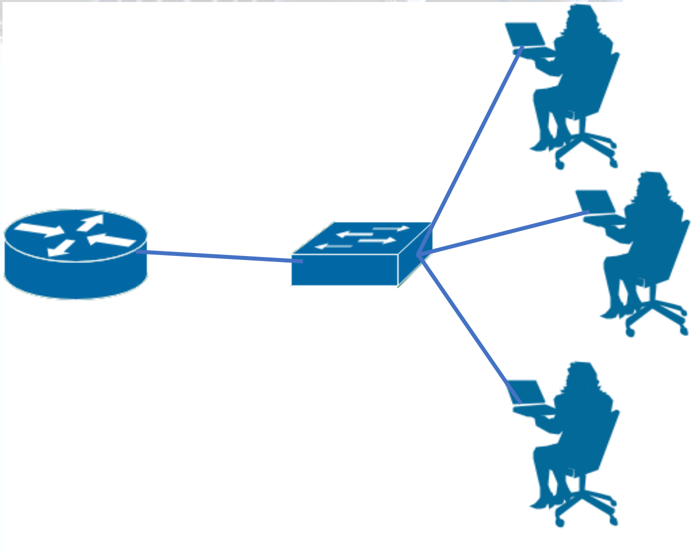
C – Non-Broadcast Multi-Access (NBMA)



4 – Small Office / Home Office (SOHO)

- 2 Terms reflects 2 Network Types
  - Single Router / Switch
  - Few Users
  - Less Concern about? ________
  - SO:
  - HO:





5 – On-Premise & Cloud-Based Networks:

- What is the difference? And which one is the Classic known network?

- On-Premise: everything is in the office, Company, Data Center

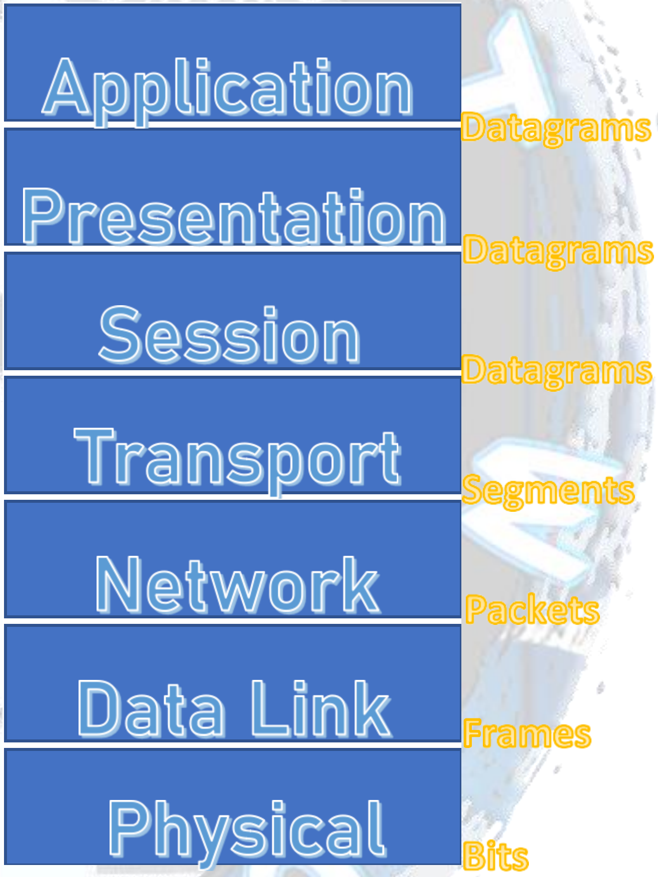
- Cloud-Based: everything is at the Cloud Company (No Headache)

Cisco Certified Network Associate (200-301 CCNA)

1.3 Network Architecture Models:

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

- More specific
- Some layers go through encapsulations & decapsulations
- Makes Troubleshooting Easier



Application — Datagrams

Presentation — Datagrams

Session — Datagrams

Transport — Segments

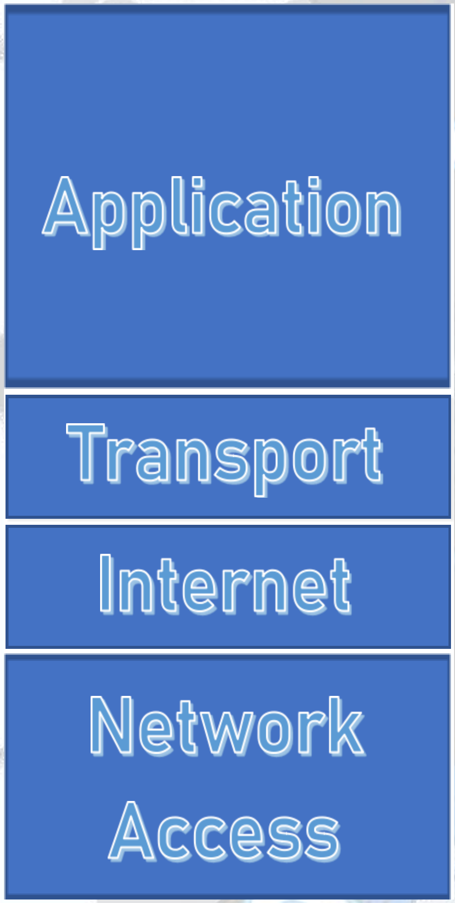
Network — Packets

Data Link — Frames

Physical — Bits

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

- less specific
- Still Some layers go through encapsulations & decapsulations

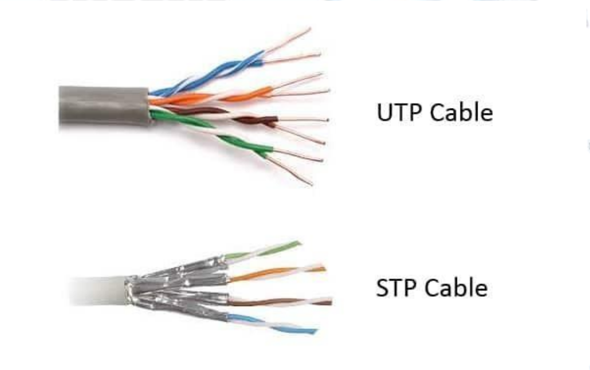


1.4 Layer 1 Technologies

- 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

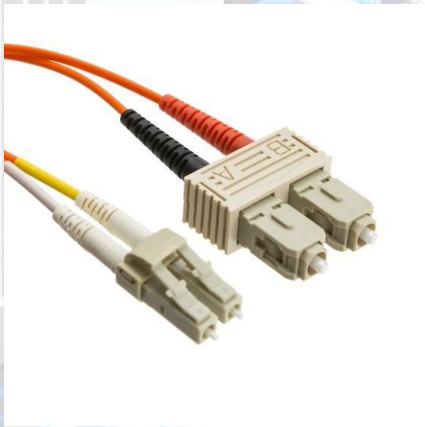


- Shielded and Unshielded
- Connecter: RJ45

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

- 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

1.5 Interfaces and Cables Issues:

- Collisions: more than one device (PC) transmitting at a single time in a shared media
    - Carrier sense multiple access/collision detection, CSMA/CD Solved it!!
- Errors: Cabling Issue, Unsupported SFP
- Duplex Mismatch: Half or Full? MUST MATCH
- Speed: 10/100/1000? MUST MATCH

1.6 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

1.7 Media Access Control Address (MAC Address):

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

1.8 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 = 232 = 4,294,967,296

- 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

- 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

- Classless Inter-Domain Routing (CIDR):
    - The relief of classes and its usage of subnets
    - using VLSM

- 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

1.9 Internet Protocol Version 6 (IPv6):

- Hexa-Decimal Language
- 128 bit length
- 8 parts
- Hosts = **2128** = 340,282,366,920,938,000,000,000,000,000,000,000,000

- Types:

- Global Unicast:	2000::/3	Public
- Unique local:	FC00::/7	Private
- Link local:	FE80::/10	Per-Interface Assigned (MAC Address)
- Anycast:		Can be assigned to multiple node (Nearest)
- Multicast:	FF00::/8	One Source – Multiple Destinations

1.10 Transmission Communication Protocol & User Datagram Protocol

TCP

- Reliable
- Slower
- Three-Way Handshake
- Connection-Oriented
    - HTTP = TCP80
    - HTTPS = TCP443
    - FTP = TCP20, 21
    - SSH = TCP22
    - Telnet = TCP23
    - SMTP = TCP25
    - BGP = TCP179

UDP

- Not-Reliable
- Faster
- No Pre steps performed
- Connection-less
    - SNMP = UDP161
    - TFTP = UDP69
    - DNS = USP53
    - SYSLOG = UDP514

1.11 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

- 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

1.12 Virtualization and Virtual Machines

- 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:

  - Type1:

    - The Native or Bare Metal
    - Runs directly on the HW resources
    - HW --- Hypervisor --- VM

Critix XEN
Oracle VM
Microsoft Hyper-V
VMwares ESX/ESXi

  - Type2:

    - Hosted
    - Runs as a SW besides the OS
    - HW --- OS --- Hypervisor

VMware Workstation

Virtual Box

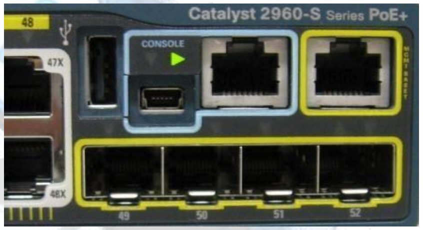
- How to connect all these?
- Virtual Switches:
  - Connects all VMs Together like a Real Switch
  - Assigns a Virtual Network Interface Card (V.NIC) for each VM
  - Exists by default in Hypervisors Type1
  - After Creating a V.Switch & V.NIC, all VMs will automatically get connected together

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

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

- Examples:
  - Microsoft Hyper-V
  - ESXi VSwitch

1.13 Introduction to the Cisco IOS Systems



1- Use the console port/console cable

2 – Access though the COM port using Teraterm/ PuTTY

3 – The IOS system:

- Command Line Interface (CLI)
- User Mode >
- Privilege Mode #
- Global Configuration Mode (Config)#

- Some Common Commands:

```
enable
configure terminal
Interface fa0/0/1
Ip address 192.168.1.1 255.255.255.0
Hostname Router1212
Reload
copy running-config startup-config
write erase
shutdown
no shutdown
```

```
Show ip interface brief
Show interface description
Show version
Show running-config
Show mac address-table
Show interface status
```

CHAPTER 2

NETWORK ACCESS

CHAPTER 2: Network Access

2.1 Switching Concepts

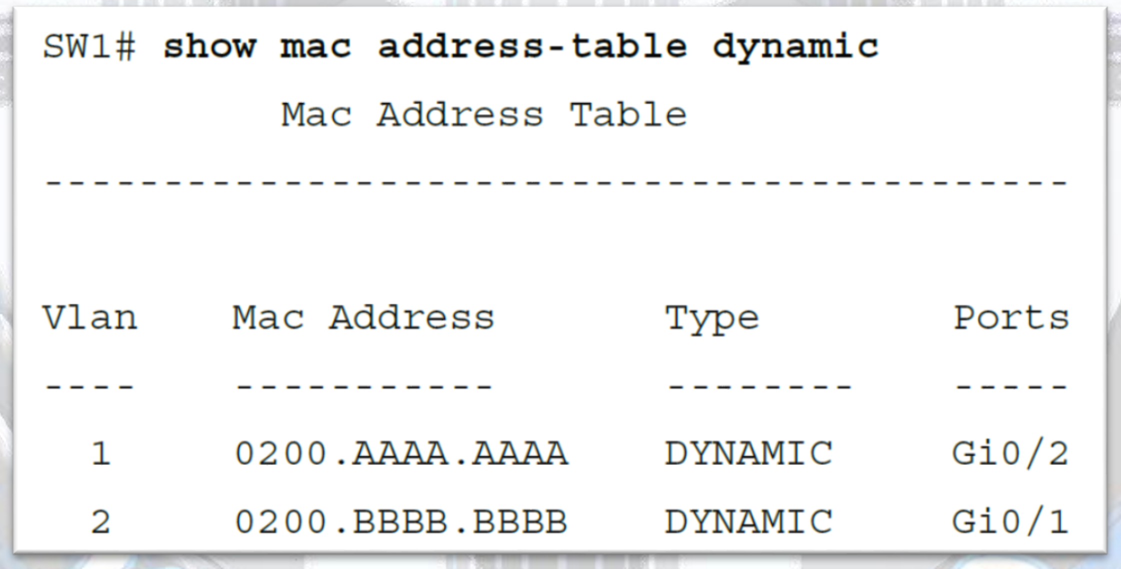
- First were called “Bridges” and had Bridge Tables
- Bridges had low port Density

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?
    - 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
```

2.2 Virtual Local Area Networks

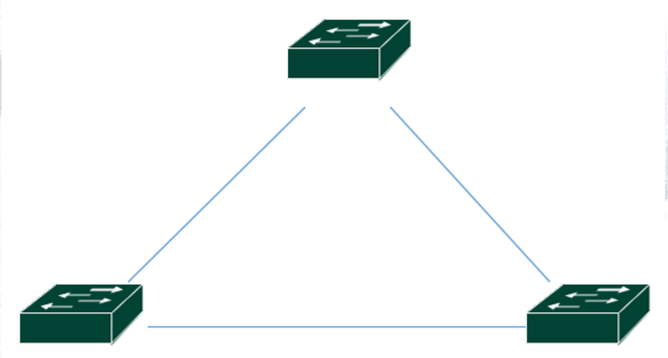
- Can I separate hosts!
- What will each group of them become?
- Every single switch port must become either ________ or ________
- Access Ports: every switch port that is connected to an End device, NO Tags will Cross
- Trunk Ports: every switch port that must carry more than on ________

- VLAN Types:
  - Data VLAN: Ordinary
  - Voice VLAN: Voice data only (higher priority)
  - Default and Native VLAN: NO TAGS, but ____________________

- Trunking: I need more than 1 VLAN to cross a link
  - Done by using encapsulation (DOT1Q)

2.3 Spanning Tree Protocol

- We need redundancy, but there will be a broadcast message!
    - What will happen?
- Then how can we prevent what is called a “LOOP”, AKA “Broadcast Storm”?
- STP requires election to be performed first
- The Winner must be: 1-Lowest Priority, 2-Lowest MAC Address



- After that port roles and states will happen:
    - Designated Port: Forwarding state
    - Root Port: Forwarding State
    - Alternative Port: Blocking State
- The entire process of election takes (30 – 50) Seconds

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

- In order to speed things up:
    - Rapid STP: NO Listening, NO Blocking, only(Discard,Forwarding, Learning)
- Then delay will become = 3 + 3 = 6 Seconds
- What's the BIG benefit of Redundancy then!!!!! If STP is blocking ports
    - There will be a Per-VLAN STP (PVST)
    - Each VLAN can have an ELECTION!!
    - Each VLAN will have its own root!
    - Things are much better now

    - Specially that there is a RPVST+ (faster)!

- Now, Edge ports and Port Fast: what's the cases and differences?

* Don't forget MST

2.4 Cisco Discovery Protocol & Link Layer Discovery Protocol

- Who am I connected to!!
- If it wasn't a Cisco Device, then can I still know who my neighbor is!

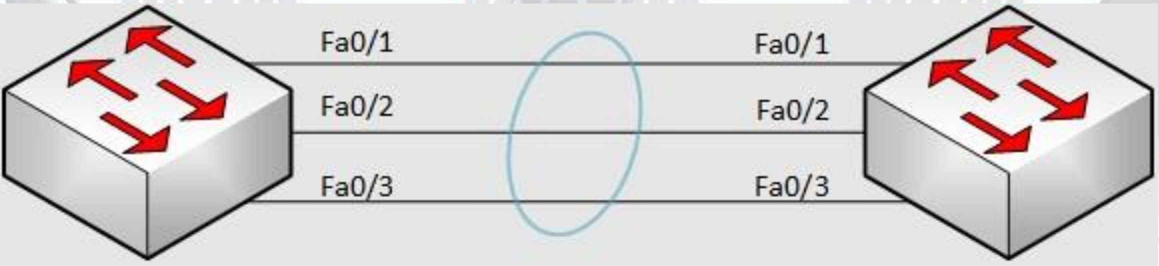
- CDP and LLDP do Discovery negotiations between devices
- Detailed information about the neighbor
    - My port that is connected to it
    - Its port that is connected to me
    - The IP Address of the neighbor device
    - The MAC Address of the neighbor device
    - Port description of the neighbor

2.5 Link Aggregation Control Protocol (LACP)

- What if the bandwidth of an interface is not enough?
- We need bigger bandwidth, but resilient not fixed!

- LACP can Aggregate/Bundle multiple interfaces into a single new interface
- Done by negotiating between the two devices using the LACP protocol and Device Role
- Watch out for both devices, at least one of them must be ACTIVE
- Load Balancing Mechanism: by default = src-dst-mac

- Both Layer2 (Switches) and L3 (Routers) LACP can be done, But in L3: no need for Negotiating and Device Roles 😊



CHAPTER 3

IP CONNECTIVITY

Chapter3: IP Connectivity

3.1 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

3.2 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

3.3 Open Shortest-Path First (OSPF)

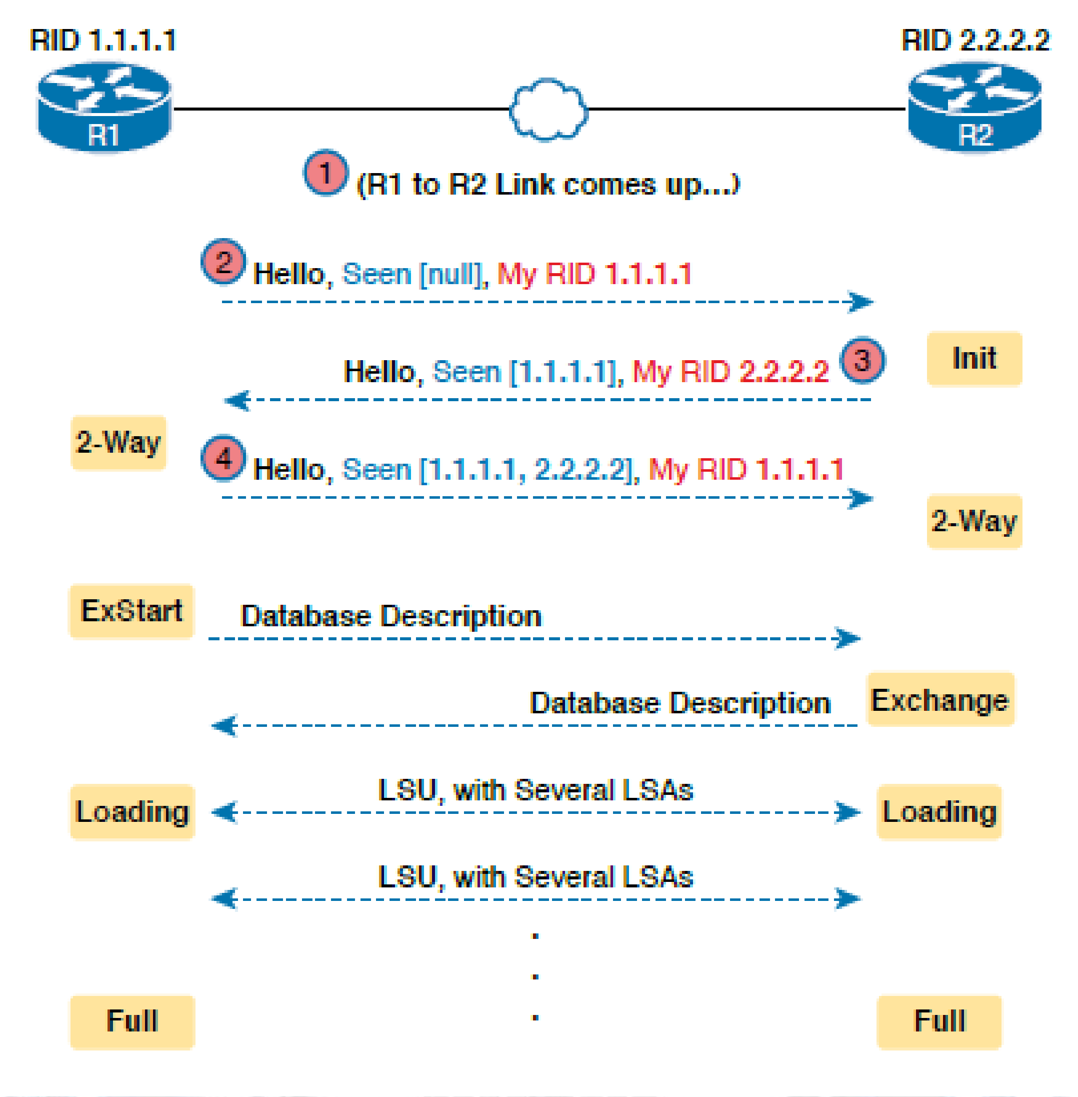
- Dynamic Routing Protocol
- administrative Distance = 110
- Metric = Cost (lesser = Better)
- Dijkstra algorithm
- SPF algorithm for route decision
- Process ID for multiple instances
- Area ID for Data Base isolation

- Link-State Advertisements: negotiation between OSPF Routers
    - it contains: LSRequest: provide the missing Information

      LSUpdate: reply for the LSR

      LSAcknowledgement: reply for the LSU

- Neighboring Process:

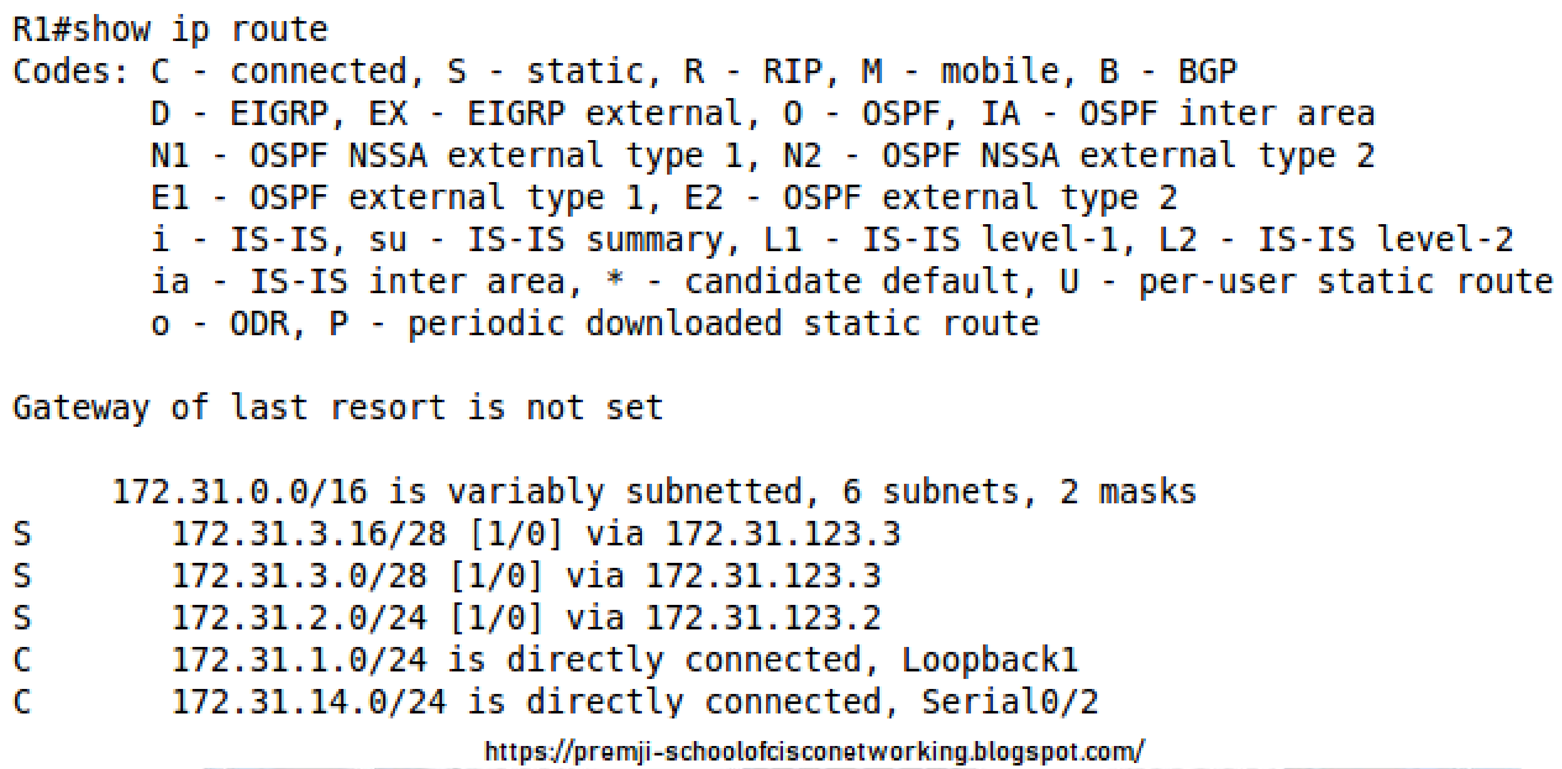


- a Neighboring router can be a P2P neighbor
    - in this case no problems
- or can be connected through a “SWITCH”!!
    - broadcast will happen
    - elections must take place
    - only One router should update the topology (DR)

    - 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)

3.4 The Routing Table



```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/16 is variably subnetted, 6 subnets, 2 masks
S       172.31.3.16/28 [1/0] via 172.31.123.3
S       172.31.3.0/28 [1/0] via 172.31.123.3
S       172.31.2.0/24 [1/0] via 172.31.123.2
C       172.31.1.0/24 is directly connected, Loopback1
C       172.31.14.0/24 is directly connected, Serial0/2
```

https://premji-schoolofcisconetworking.blogspot.com/

CHAPTER 4

IP SERVICES

CHAPTER 4: IP SERVICES

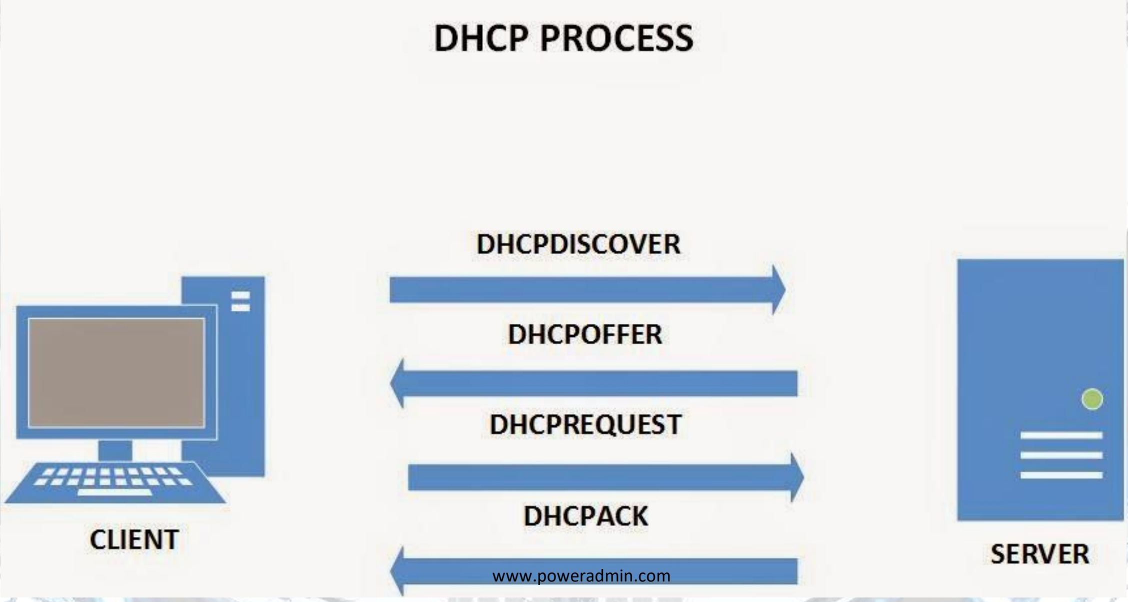
4.1 Dynamic Host-Configuration Protocol (DHCP)

- A Dynamic/Automatic method to assign IP Addresses
- Not only IP Addresses:
    - Subnet Masks
    - Gateways
    - DNS!!

- What's a DNS!?
    - Domain Name Server: resolve a URL to an IP Address and vice-versa
    - works on UDP port 53
    - also, there is a reverse DNS (for that vice-versa thing)

- Again, DHCP's assigns information for all your devices dynamically
- Assignment will be for a specific amount of time (default 24 hrs.)
- after 50% of assignment time begins, some checks will happen for each Client, and again after 87.5% of the assignment time, another check Will take place.

- to achieve DHCP Service, some negotiation will happen:



- what if the first router (Gateway) wasn't a DHCP Server!!??
- there will be a "Helper-Address"
- known as "DHCP Relay"
- help redirecting the broadcast message from the first Gateway to the Correct DHCP Server

4.2 First Hop Redundancy Protocol (FHRP)

- what if the gateway went down!!!!!!!!
- a redundant gateway must be there
- but how to redirect the requests from one to another?
- how many back-ups can there be?
- What protocols will do this:

Hot-Standby Redundancy Protocol (HSRP)

- Cisco Only
- 2 Gateways
- No Load-Balancing

Virtual-Router Redundancy Protocol (VRRP)

- Open Standard
- 2 Gateways
- No Load-Balancing

Gateway Load-Balancing Protocol (GLBP)

- Cisco Only
- 4 Gateways
- Load-Balancing

4.3 Network Address Translation (NAT)

- Private IP Addresses don't carry Internet!
- Public IP Addresses can't be assigned to private devices!
- Then!!!, NAT will translate Private to Public and vice-versa 😊

*NAT is done ONLY ONLY by Routers, no Switches, no MLS's

- it can be:

    Static: one-one translating

    Dynamic: Group-Group Translating

- also, this did not solve everything, IP exhaustion still there
    - so here comes PAT (Port Address Translation)
    - also called NAPT, or NAT-Overload
- PAT will do a one-65535 Translation!!!

4.4 Network Time Protocol (NTP)

- we have to stay synchronized
- give a precise information, with real timing and date
- either by setting an inner clock manually
- or asking someone to inform us about timing
- uses UDP = 123

- each network device can either be a Server or a Client
- Stratum is needed:
    - how preferred and accurate this source is
    - starts from 0 – 15
    - the closest, the better
    - by default: a cisco router = 8

4.5 Simple Network Management Protocol (SNMP)

- Monitor Networks from a single point of view
- Server/Agent Relationship
- uses UDP 161
- the server is thee requester (and recorder)

- at the agent side:
    - MIB Object (The Factory)
    - Agent (The Messenger)
- SNMP versions:
    - v1: obsolete
    - v2c: enhanced
    - v3: supports Authentication & Encryption

4.6 System Loggings (Syslog)

- stay aware of “everything”
- know all what’s happening behind the scenes (or even in front of)
- starts from the obvious information up to “Emergency”
- Server/Client Relationship

- Server can be a Normal Server that collects all the loggings
- Server can use the “Syslog” or “Splunk” Software
- client is the networking device that generates logs

- Quote: “Every Awesome Cisco Engineer Will Need Ice-Cream Daily”

0 = Emergency

1 = Alert

2 = Critical

3 = Error

4 = Warning

5 = Notification

6 = Information

7 = Debug

4.7 Quality of Service (QoS)

- 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 will prefer based on Variety of Factors, some are:

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

- Classification & Marking:

  classifying the traffic according to its importance

  (Very High, High, Med, Low)

- Queueing:
  - giving a specific priority to every type of packet

    (giving the priority of "very high" to the "UDP" traffic)
  - dividing the Transmission capacity with respect to the priority

    (giving 40% to the very high, 20% to the high, etc.)

- Policing & Shaping:
  - Policing is counting the traffic before transmitting it, and limiting it

    (limit the FTP traffic to be transmitted at maximum of only 2Mbps)

    *counting the desired traffic, and dropping all that exceeds
  - Shaping limits the Queued traffic to a certain amount of traffic, and what EXCEEDS, wait at the queue

4.8 Secure Shell (SSH)

- A secured and trusted method to log in a device remotely
- uses TCP 22
- encrypt the transmitted information
- uses the server/client relationship
- a replacement for Telnet
- needs an application for (Microsoft Windows Users)

4.9 File Transfer Protocol (FTP)

- can devices transfer data between them?
- data like Files, Software Images, Configs saved as Texts
- FTP uses TCP 20,21!
- 2 TCP ports for 2 reasons:
    - TCP 21 (Control Channel): to establish connection between Server and Client
    - TCP 20 (Data Channel): to transfer Data between Server and Client

- there is a relative:
    - Trivial FTP (TFTP)
    - uses UDP 69
    - UDP so, unreliable, but still has its uses

CHAPTER 5

SECURITY FUNDAMENTALS

CHAPTER 5: SECURITY FUNDAMENTALS

5.1 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!

- 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)

- Also, 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:

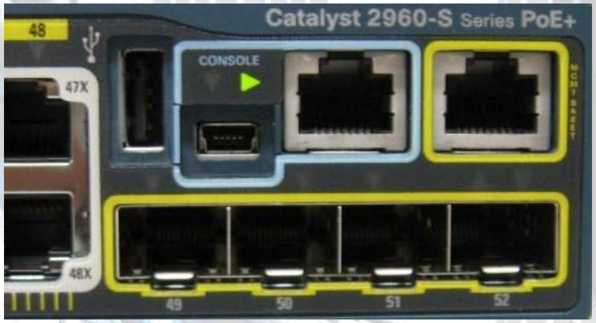
- This is an in-reality protection
    - like securing the devices inside racks
    - racks should have licked metal/glass door
    - all racks should be installed in a secured DC
    - Racks and DCs can be secured using Keys, Cards, Fingerprints

5.2 Device Access Control

- what if the device wasn't locked properly (physically)
- if someone did connect to the Console/AUX ports!!!!

- Console and Auxiliary ports can be protected
  - either by configuring a specified password for each port
  - or by using a local credentials and applying them upon the ports

*even if a user did login to a device, limit his access by assigning "enable secret/password"



5.3 Virtual Private Networks (VPN)

- How Virtual? And How Private?
- Tunnels will be established
- Full separation
- End-to-End Encryption

- Site-to-Site VPN
  - Peer-to-Peer VPN
    - needs and IGP for Routing and Forwarding (Underlay)
    - the IGP will be exchange at the edges with the ISP
  - Overlay VPN
    - obtain a circuit from the ISP
    - IGP will be yours all the way

- Client VPN
    - for an end user
    - requires a software
    - established remotely
    - credentials are needed
    - the Tunnel will be “PC – Router”

5.4 Access Control List (ACL)

- specific permissions for users/ networks
- allow or deny rules only
- allow or deny some hosts/networks from internet

- ACL Types
    - Standard:
        - uses source host/network to decide the permissions
        - range of 1-99
        - NO specific permissions
    - Extended:
        - uses source & destination hosts/networks/ports/services
        - range of 100-199
        - specific in detail permissions
    - Named: A Combination, Hierarchy Mode, Name

5.5 Port Security

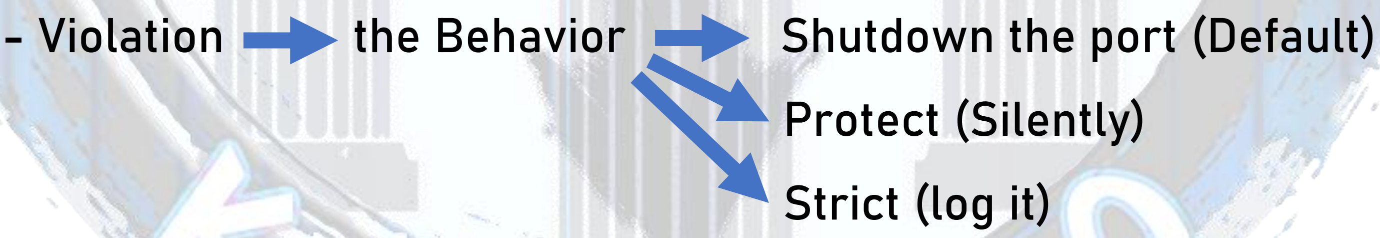
- Switch Ports connects you immediately
- A limitation is needed to the switch ports
- This limitation includes:
    - The No. of learned MAC Addresses
    - Only “Statically” assigned MAC Addresses are allowed to connect
    - A combination of the 2 above

*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 → the Behavior → Shutdown the port (Default)

Protect (Silently)

Strict (log it)

5.6 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

5.7 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, SO!! → Drop the ARP

Or → Trust the Port

↘ Create ARP ACL

5.8 Authentication, Authorization, and Accounting

- AAA are the Security mechanisms for the MGM Plane
- you can control everything about everyone allowed/denied From accessing the Network
- Authentication:
    - Verifies Credentials
    - Contacts the AAA Server to check the eligibility of those Credentials
- Authorization:
    - Determines the Credentials Powers
    - Contacts the AAA Server to check the Privileges of those Credentials
- Accounting:
    - Determines some Limitations
    - Calculates Statistics

CHAPTER 6

WIRELESS NETWORKS FUNDAMENTALS

CHAPTER6: WIRELESS NETWORKS FUNDAMENTALS

6.1 Wireless Principles

- So, what happens in the wireless world?
- 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)
    - will i really get a 14 Gbps!!!! Wirelessly!!!!

- More Details:
    - The Encoder now, the one who 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 to Do so! So, a power source is also needed
    - this power source might be a battery or an AC adapter
    - measuring the power of a frequency is called “Amplitude”

6.2 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)

6.3 Types of Wi-Fi Networks

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

6.4 Wi-Fi Terms

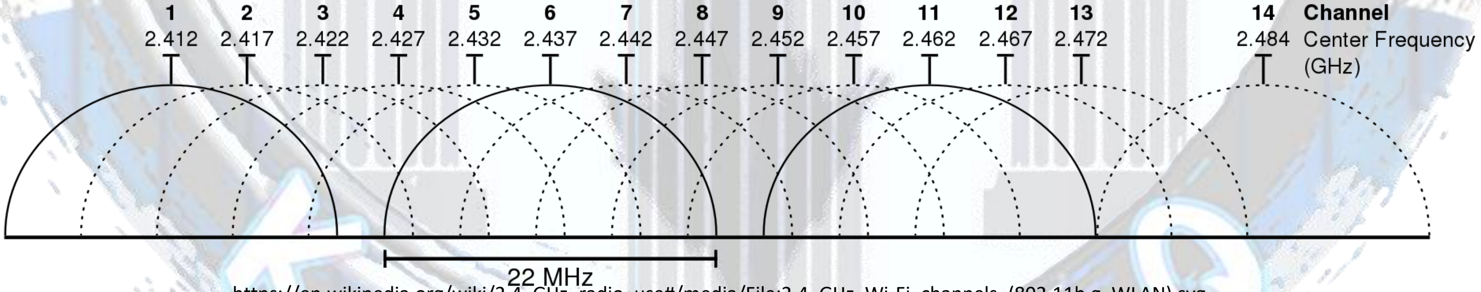
- Basic Service Set (BSS): A single AP and it's coverage area
- Basic Service Set Identifier (BSSID): The MAC address of that AP
- Service Set Identifier (SSID): Name of the WLAN
- Distribution System (DS): The Wired Net. that connects the AP to the LAN
- Extended Service Set (ESS): A collection of APs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

6.5 Wi-Fi Channels

- so, what is happening exactly between the transceivers?
- a group, or a range of Radio Frequencies (RF), are being Established, all are 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 from 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

- 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

6.6 WLAN Architectures

- Autonomous Architecture
    - Autonomous (Independent) Access Points
    - Independent Management (GUI)
    - one or more SSIDs (each = 1 VLAN)

*when having multiple SSIDs, and each will be 1 VLAN, the back link Should be a trunk

*adding a new SSID, requires to login to each AP individually

- Split-MAC Architecture
    - there is a WLC
    - APs now will be called Lightweight APs (LAPs)
    - WLCs will manage (RF, QoS, AAA, Policies)
    - APs will (RF TX/RX of frames, RF Collision Detection, MAC & Data Management)

- Cloud-Based Architecture
    - also, a WLC
    - but remotely (through public cloud, or private cloud)
    - also, LAPs
    - might be a Cisco Meraki (does self-config to the LAPs)
    - or, Cisco Cat. 9800-CL

*when having WLC & LAP scenario, there will be a private tunnel between them, It will encapsulate and transfer all the control and data information between the WLC and LAPs, it's called the "Control and Provisioning of Wireless AP" Or "CAPWAP"

- 2 tunnels (control tunnel = UDP5246, data tunnel = UDP5247)
- control tunnel (encrypted and authenticated)
- data tunnel (not encrypted by default)

6.7 WLC Positioning

- Centralized WLAN Architecture
    - single WLC that controls all the LAPs
    - might be placed in the DC, or near the edge of the network
    - all data must pass through the CAPWAP tunnel to reach the WLC
    - even if the destination is closer than the WLC

    - this can be fixed, using Cisco Flex Connect
    - which is a mode, to be enabled on the LAPs
    - especially if the LAPs like in a branch, and the WLC is in the HQ
    - LAPs can now pass the traffic directly to the LAN
    - LAPs can now authenticate the clients for access
    - LAPs can now work even if the CAPWAP tunnel goes down

- Converged WLAN Architecture
  - connect a WLC and an AP both, to the same switch
  - the access/distribution layer switch
  - now the LAPs are reaching the WLC through the switch
  - multiple WLCs will be needed in such scenario
  - this leads to a shorter distance CAPWAP
  - hence, faster Wi-Fi, less delays

*Cisco Catalyst 9300 series, provides switches, that can have a WLC Integrated inside the switch itself (embedded)

6.8 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
- Monitor Mode
    - generates reports & statistics, send them to the WLC

- Sniffer Mode
  - scan a specific channel
  - send the scanning reports to the WLC

- 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

*a mesh node (MAP), uses adaptive wireless path protocol (AWPP)
To determine the best path to a root node/AP (RAP)

*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

6.9 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

- Encryption:
    - 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

- 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!

- 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

- 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)

- 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

CHAPTER 7

AUTOMATION & PROGRAMMABILITY

CHAPTER 7: AUTOMATION & PROGRAMMABILITY

7.1 Automation

- Traditionally, Network Management is about
    - Installation and initial config
    - modifying and updating the existing config
    - upgrading software
        - all of those were achieved by
            - Console, Telnet, SSH, applying scripts or by copying config
    - and, Monitoring
        - which was achieved through
            - SNMP, and Netflow
    - AND, it was always “Box-by-Box”

Cisco Certified Network Associate (200-301 CCNA)

- With Automation
    - new devices automatically finds an initial configuration
    - automated QoS profiles/config
    - automated AAA profiles/config
    - utilizes scripts/tools
    - standardize some procedures
        - software image per device model
        - and, the upgrade procedure
    - schedule operations
    - sometimes, automated troubleshooting (WoW)
        - which are done through (CLI, SSH, SNMP, NETCONF, RESTCONF)
    - topology visualization and monitoring
        - which are done by using (SNMP Manager, and Netflow Collector)
- So, all of that led to reduce or even eliminate the Box-by-Box, Smaller staff is needed, time saving, and config consistency

7.2 Software-Defined Networking (SDN)

- Automation is achieved by SDN
- where you have a “software” that runs your network
- so, through a “software” you be able to run and administrate

  An entire network, with its different types of devices
- that will definitely need either a “Controller”!!!

  Or, a built-in scripting (Cisco TCL, or Python)

- SDN Controller
  - the big guy that does almost everything in this chapter
  - controls and implement the automation and administration
  - can either be
    - A “software” installed in a server
    - An appliance with a controller inside (Cisco APIC, DNA Center)
    - Or, a remote controller through the cloud
    - and, it uses some tools/apps like (puppet, chef, and ansible)

7.3 SDN Implementation

- Imperative Approach
    - the control plane logic resides completely in the controller
    - the controller has a complete control over programing the 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

7.4 SDN Architecture

- Underlay Network
    - the protocols & features to get reachability
    - all the links must be L3 and P2P
    - open standard protocols (OSPF and IS-IS)

- Overlay Network
    - Virtual Network created on top of the Underlay
    - now the underlay is like a “physical connectivity”
    - some protocols use (VRF, MPLS-VPN, VXLAN)

- SDN Fabric
    - the physical devices used to build the underlay
    - those devices can be controlled by a “Controller”

7.5 SDN Effect upon Planes

- First of all, there are 3 planes in the network devices
  - Control Plane
    - learn information from the protocols
    - downloads them to the Data planes (as Tables)
    - protocols resides here (routing protocols, MAC learning, DHCP, AAA, etc…)
  - Data Plane
    - also known as Forwarding Plane
    - any logical/physical component that controls the frame/packet Forwarding (action)
    - like Tables (MAC Table, Routing Table)
  - Management Plane
    - responsible for AAA (remotely)
    - also, the console port resides in here

- so, the SDN effect upon the Control and the Data plane
  - depends on the implementation approach
  - if it was an Imperative approach
    - also called a "Stateful SDN"
    - the controller will be responsible for learning information
    - and downloading them to the data plane
    - if the devices lost connectivity to the controllers, they Will be powerless

  - if it was a Declarative approach
    - also called a "Stateless SDN"
    - the controller will only declare how it wishes things To go on in the network

- Cisco DNA Center
    - the Digital Network Architecture
    - it is an Appliance (comes in various models)
    - A Central Management, Automation, and Analysis Point
    - gives Intent-Based Networking
    - and that is, controlling a network by a software
    - allows to design and create topology maps
    - design WLAN SSIDs
    - managed through a GUI
    - has a built-in APIC
        - the Application Policy Infrastructure Controller
        - it's controller
    - also has a built-in NDP
        - Network Data Platform
        - analyzes problems, show them, and suggest solutions

7.6 Application Programming Interface

- the transformers that are transforming everything from
  The Application to the controllers, and vice-versa
    - those will be called "Northbound API"
- also transforms everything from the controller to the network
  Devices, and vice-versa
    - the "Southbound API"
- and, transforms data between different controllers of different devices
- so, it's a code
- written by a language
- that language encodes data into an API
- it uses the Server/Client relation
    - in the Northbound (Controller = Server, Application = Client)
    - in the Southbound (Network Device = Server, Controller = Client)

- API types
  - Internal API
    - between applications
    - like transferring data from HTML to PDF
  - Web-Service API
    - exchanging data between remote devices
    - Uses IP address
    - like REST-Based API

*some Southbound APIs (Openflow, Cisco OpFlex, CLI, SNMP, NETCONF)

- Representational State Transfer APIs (REST-Based APIs)
    - the most common type of web-service API
    - mostly found in the Northbound (like a Polar Bear!)
    - utilizes HTTP verbs (GET, PUT, POST, DELETE)
    - while a REST API is in developing, a developer would use A CRUD to develop the API's HTTP verbs
    - CRUD = Create, Read, Update, and Delete
    - most common languages used to encode data in a REST-Based API Are (XML, and JSON)
    - encoding means standardizing a data structure between the app, Controller, and nodes

*Cisco Intent: is a Northbound REST-Based API

7.7 Configuration Management Mechanisms

- the applications that you use to automate
- all of them requires CLI/Scripting
- includes a GUI
  - schedule a task
  - manually instantiate events
- so, a CLI script will give a GUI result
- like (Puppet, Chef, and Ansible)

- Puppet & Chef
    - uses the Master/Agent relation
        - 2 codes
        - one in the server, other in the node
    - uses the Pull Model
        - an agent will periodically ask a master for event and actions, And Pulls the script from it
    - uses the RUBY language

- Ansible
    - Agentless
    - uses the Push Model
        - Master pushes a config to the agent
    - uses the YAML language

7.8 Java-Script Object Notation (JSON)

- a programming language used to create APIs
- used by REST-Based APIs
- human-readable
- lightweight
- the “Object” is about
    - a container that encloses “one-or-more” {name:value} pairs
    - also called a “key-value pairs”

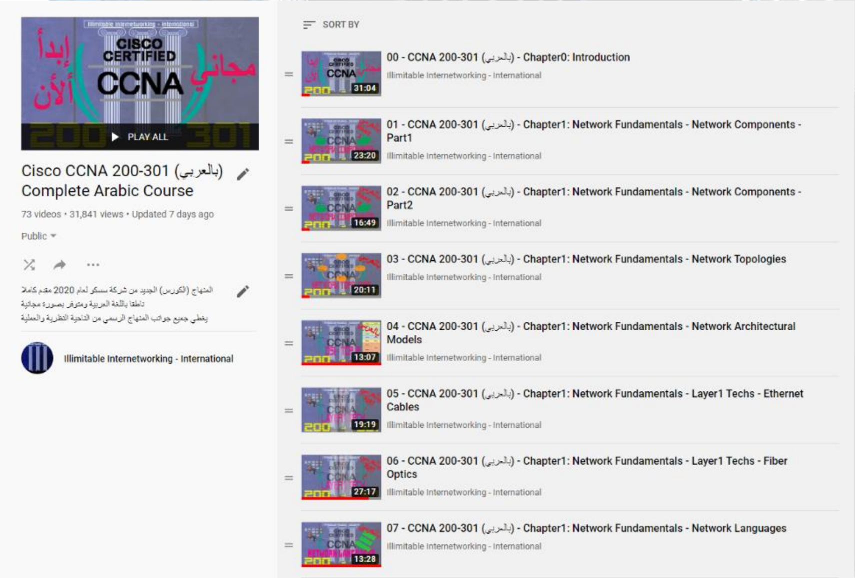
- JSON Values
    - always surrounded by a curly bracket { }
    - name:value pairs
    - a string must be enclosed with double quotes “ ”
    - like = {“name”:”III”, “job”:”channel”, “location”:”YouTube”}

- the pairs values types
  - 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}

*Spaces don’t matter

Cisco Certified Network Associate (200-301 CCNA)

- Thanks a lot for reaching here so far
- Chapter 7 is the final chapter
- CCNA 200-301 Complete Course
- Free and available on YouTube
- Available in 2 Languages (English and Arabic)
- more Courses are coming!
  https://www.youtube.com/channel/UCbXctm6VW2ZZrksHBWAg_tw



Cisco CCNA 200-301 (بالعربي) Complete Arabic Course

73 videos • 31,841 views • Updated 7 days ago

Public

المنهاج (الكورس) الجديد من شركة سسكو لعام 2020 مقدم كاملا
ناطقا باللغة العربية ومتوفر بصورة مجانية
يغطي جميع جوانب المنهاج الرسمي من الناحية النظرية والعملية

Illimitable Internetworking - International

00 - CCNA 200-301 (بالعربي) - Chapter0: Introduction
Illimitable Internetworking - International

01 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Network Components - Part1
Illimitable Internetworking - International

02 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Network Components - Part2
Illimitable Internetworking - International

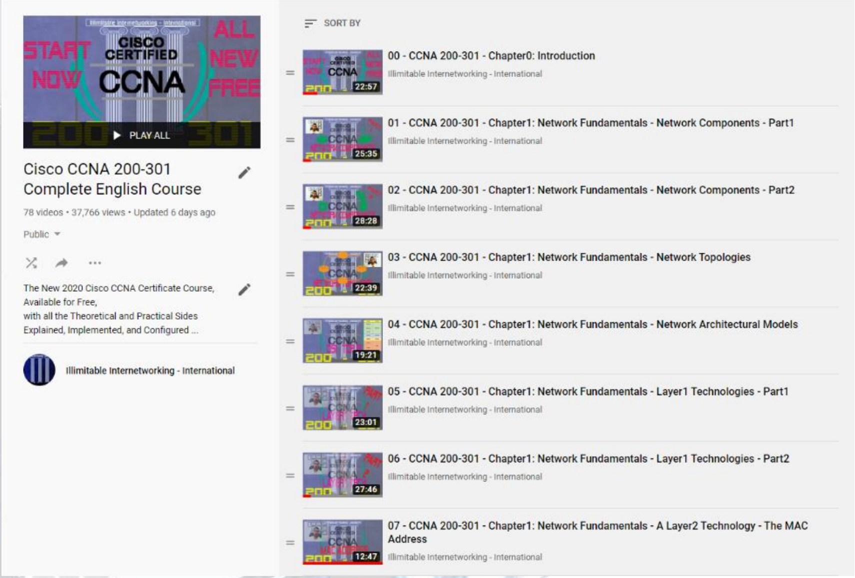
03 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Network Topologies
Illimitable Internetworking - International

04 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Network Architectural Models
Illimitable Internetworking - International

05 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Layer1 Techs - Ethernet Cables
Illimitable Internetworking - International

06 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Layer1 Techs - Fiber Optics
Illimitable Internetworking - International

07 - CCNA 200-301 (بالعربي) - Chapter1: Network Fundamentals - Network Languages
Illimitable Internetworking - International



Cisco CCNA 200-301 Complete English Course

78 videos • 37,766 views • Updated 6 days ago

Public

The New 2020 Cisco CCNA Certificate Course,
Available for Free,
with all the Theoretical and Practical Sides
Explained, Implemented, and Configured ...

Illimitable Internetworking - International

00 - CCNA 200-301 - Chapter0: Introduction
Illimitable Internetworking - International

01 - CCNA 200-301 - Chapter1: Network Fundamentals - Network Components - Part1
Illimitable Internetworking - International

02 - CCNA 200-301 - Chapter1: Network Fundamentals - Network Components - Part2
Illimitable Internetworking - International

03 - CCNA 200-301 - Chapter1: Network Fundamentals - Network Topologies
Illimitable Internetworking - International

04 - CCNA 200-301 - Chapter1: Network Fundamentals - Network Architectural Models
Illimitable Internetworking - International

05 - CCNA 200-301 - Chapter1: Network Fundamentals - Layer1 Technologies - Part1
Illimitable Internetworking - International

06 - CCNA 200-301 - Chapter1: Network Fundamentals - Layer1 Technologies - Part2
Illimitable Internetworking - International

07 - CCNA 200-301 - Chapter1: Network Fundamentals - A Layer2 Technology - The MAC Address
Illimitable Internetworking - International