Enterprise Network Design Considerations

3 tier architecture

- Access Layer: End devices are connected.
- Distribution layer: interconnecting access layer switches.
- Core layer: Distribution switches are connected. Main concern is speed. Maybe connected to internet.
- Hybrid topology cause it has mesh & star topologies

Collapsed core

- Access layer & collapsed core.
- Another example is leaf spine design in Data centers.

On-premise vs Cloud

- With cloud environment, we don't have to worry about the infra.
- Cloud Is pay as you use.
- On-prem is good for meeting compliance requirements.
- Hybrid uses on-prem and cloud.
- Intercloud exchange can move your data from one cloud provider to the other. The inter cloud exchange provider takes care of it.

Redundant Design

- Redundant components: dual power supply to racks, UPS, FHRP, server clusters, NIC Bonding, load balancer, etc.
- Will increase costs. One needs to justify the increase in cost in incremental uptime & improvement.
- Disaster recovery is critical part of redundant design: Full back up, Differential Backup(less costly), incremental backup, snapshot(backs up entire sever including state)
- Natural disaster: cold site(less expensive. Power, floor). Warm site(we are ready with power, floor, hardware). Hot site(everything warm site plus synchronised data)
- SLA(Service level agreement) :- promise you make to users how long a system will be down in the event of a disaster.
    - RTO(Recovery Time Objective) :- the maximum amount of time a system will be offline after a disaster.
    - RPO (Recovery point objective) :- maximum amount of data that can be lost due to a disaster.
    - MTBF(mean time between failures) :- The average amount of time before a product fails.
    - MTTR(mean time to repair) :- average amount of time to repair a failed product.

FHRP(First Hop redundancy protocol)

- HSRP(cisco propriety protocol) : Hello packets 3 secs. Holdtimer 10 secs.
- VRRP(vendor neutral): advertisement interval 1 sec.
- GLBP: redundancy plus load balancing: Active virtual gateway. Active virtual forwarder. Max 4 routers can be part of GLBP. AVG replies to ARP broadcast in round robin fashion to load balance give MAC of each router for each ARP request. Other than round robin, we can also use Host-dependent and weighted.

Stateful Switchover(SSO)

- Config and state information exchanged between primary and secondary route processor. Packets are dropped until the forwarding table is built.
- NSF makes routing information maintained by CEF available to the back up route processor so there would be no packet drops.

Wireless LAN(WLAN) Design Considerations

WLAN Deployment options

- Controller-less APs: Autonomous APs.
- Controller-based APs: Lightweight APs.
    - WLAN Controller
    - Traffic flows from one AP to the WLAN controller and to the egress AP.
    - AP to Controller protocol used is CAPWAP (control and provisioning of wireless access points).
- Distributed WLC deployment.
- Centralised WLC deployment. Data centre to building. WLC can be a physical or a virtual machine. It can be on a cloud, cloud WLC.
- Remote branch WLC deployment.
    - Cisco flex connect: local switched: APs smart enough to end user traffic within the branch office.control and management traffic still sent to the data centre WLC.

Location Services

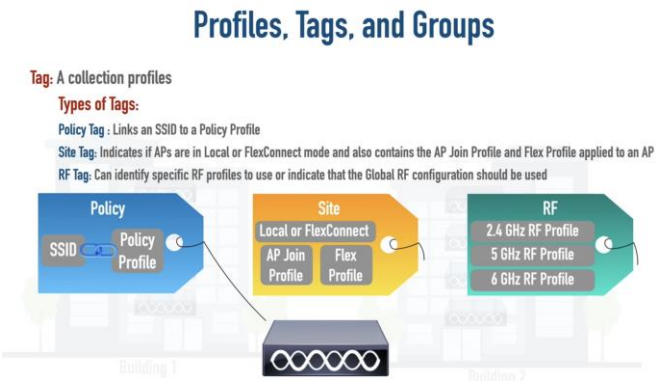
- RSS (received signal strength) : used in location based advertising. Ads sent based on the location.
- Cisco provides RTLS (Real-time location services): DNA Spaces & Cisco Meraki platform.

Client Density Considerations

- Number of clients we need to service within a wireless coverage area.
- More clients added the slice of the bandwidth pie available to each wireless client is going to decrease.
- More Non overlapping channels
- Selecting number of APs
    - The specs of the AP.
    - Wireless standards. More non overlapping channels using 6 ghz band offered by wifi 6E compared 6.
    - Simultaneous communication streams.
    - Bandwidth demand.
- Increasing density of APs
    - Increasing number of APs.
    - Reduce Tx power of APs.
    - Reducing number of bonded channels.
    - Using wifi 6E.

Wireless network segmentation

- Segment using profiles, tags, and groups.
- Profile: characteristics of each wireless LAN:
    - WLAN Profile: SSIDs, authentication settings(PSK, 802.1x, webauth).
    - Policy Profile: policy information such as VLAn & QOS.
    - AP join Profile: includes settings such as CAPWAP Parameters & PoE settings.
    - Flex profile: local authentication.
    - RF profile: parameters such as supported channels and transmitted power.
- Tags:
    - Policy Tag: links an SSID to a policy profile.
    - Site tag
    - RF tag.



- Group: collection of APs sharing a common set of tags.

SD-WAN

SD-WAN implementation

- Cisco SD-WAN implementation is based on Viptela recommended to be used with Cisco DNA centre to leverage automation and virtualisation capabilities.
- Data plane, control plane, management plane, orchestration plane.
- Vmanage: configuration, monitoring and provisioning.
- Vbond: orchestration and provisioning. ZTP.
- Smart: brain of SD_WAN.OMP. enforcement of the policies.
- Data plane: Vedge can be physical or virtual. Reposible for establishing network and forwarding traffic.

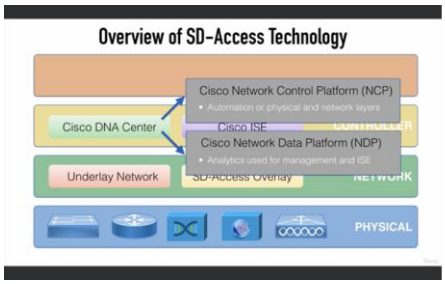
SD-Access

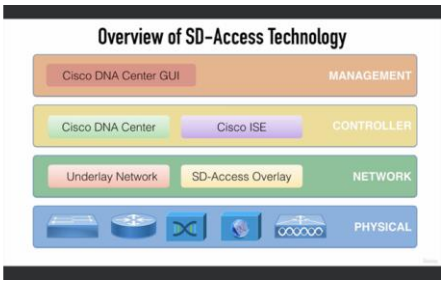
Cisco DNA Center

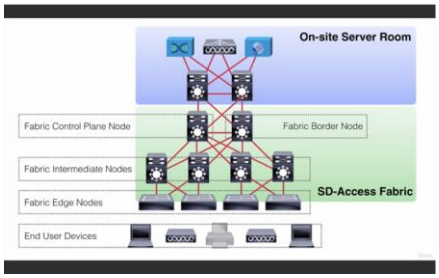
- Central point of management.
- Automate device deployment and configuration.
- Simplifies network maintenance and set-up.

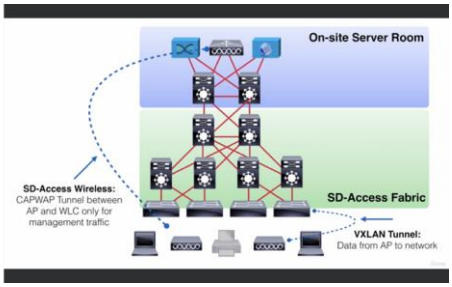
SD-Access advantages/Architecture

- SD-Access uses next gen policy enforcement.
- Security group access control lists.
- Secure network segmentation.
- Virtualisation of physical network.
- Separate virtual networks can have separate policies.
- SD-Access solution: DNA Center & Campus Fabric(overlay network) can be managed via DNAC or NETCONF/YANG
- SD-Access = Campus fabric + DNAC.
- Control(LISP encapsulation and simplified routing), Data(VXLAN Tunneling and Virtual networks), and policy plane(Cisco trustsec and security groupings).





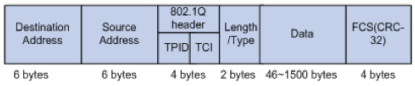


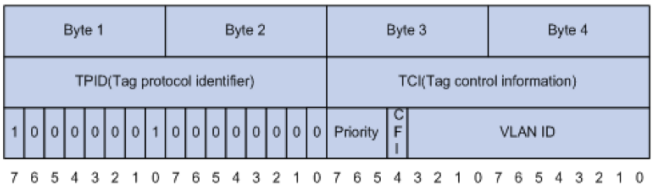


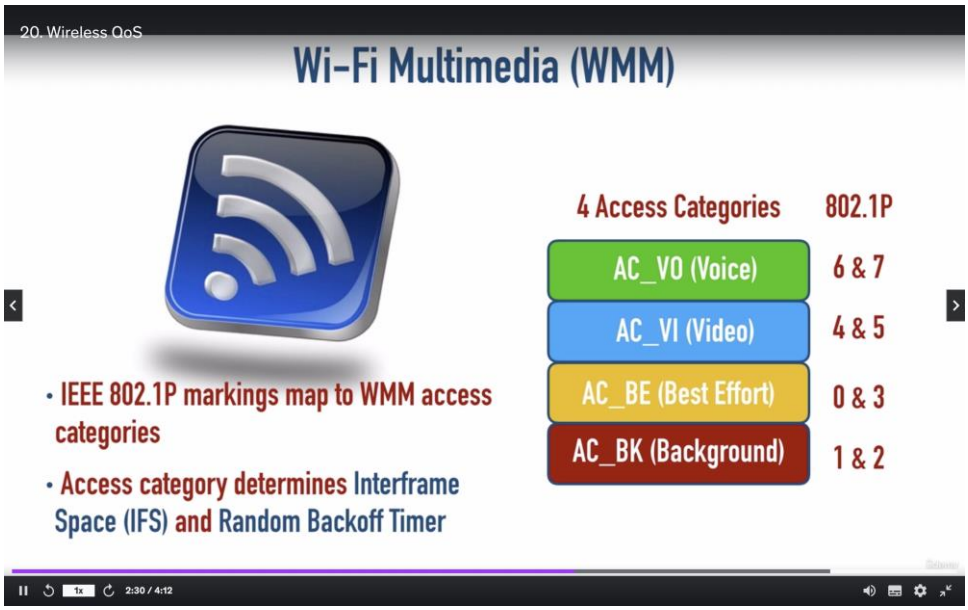
QOS Mechanism

- QOS is good for periodic congestion.
- Best effort is FIFO. Diffserv is based on DSCP markings. Intserv is the strict QOS method uses Resource reservation protocol, bandwidth is reserved.

- Classification and marking is done at as close to the source as possible.
- Queuing is congestion management. CBWFQ, LLQ, etc. no more than 11 sub queues.
- Congestion avoidance: causes TCP slow start. Sliding window decreases substantially.Tcp global synchronisation. WRED.
- Policing and shaping: Policing drops above CIR. Shaping delays the traffic when it exceeds the CIR.
- Link efficiency use it only when your link speed is less than 2mbps for voice and video.
- Wifi QOS based on 802.1P marking which is 3 bit layer 2 marking







Switching Mechanism

Process switching

- Slowest of all. Processor does all the forwarding of every single packet.
- Debugging uses process switching.
- No ip route-cache this will make it process switching.
- Debug ip packet detail —>simple imp debug.

Cisco Express Forwarding

- Less cpu intensive cached.
- dCEF each line card does the forwarding.
- CEF uses FIB and Adjacency table.
- FIB is a replica of routing table with outgoing interface
- Adjacent table is used for constructing l2 header. Directly connected devices.
- Show ip cef
- Sh adjacency table
- If a packet cant be processed by cef it is punted is next fastest switching method.order is dCEF—-CEF—process switching. Fragmented packets.

CAM vs TCAM

- CAM: Arrival port number, Source MAC address, arrival timestamp. Removed after ager timer expires. Default time is 5 minutes.
- Mac address-table aging timer <seconds>
- CAM table stores most recent entries when it gets duplicate entries.
- During lookup it will be 1 or 0.

- TCAM multilayer switches.
- L2 switches uses TCAM for QOS.
- ACLs uses TCAM.
- TCAM returns True 1, False 0, or Do not care value X.
- TCAM uses Value, mask, and result.
- Value = Ip address, protocol ports, etc.
- Mask = mask bits associated with matching values.
- Result = action which should be taken; result, deny, QOS Policing, etc.
- Show platform tcam utilised.
- A L2 or multi layer switch is determined by the availability of TCAM table(some L2 uses it for QOS).

FIB vs RIB

- FIB: next hop and interface number for each destination prefix.
- Direct copy of the routing table.
- More fib entries more time consumed for route lookup. Not an issue with modern ASIC which provides line rate.
- dCEF offloads the CEF to line cards.

- Used by all routing protocols.
- Unreachable routes removed and RIB updated.
- Dynamic, static, and directly connected routes.
- Each routing protocol has its own structures.
- Best path based on best path selection algorithm and inserted to RIB IP routing table.