Software Defined Network
SDN

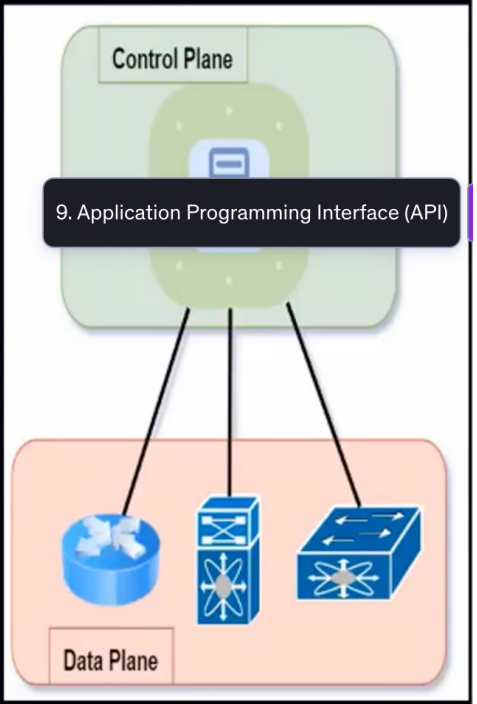
Ch 11

SD-Access

What is SDN (Software Defined Networking)

SDN

- A network driven by software/policy/program/application/template.
- SDN is an architecture designed to make a network more flexible and easier to manage.
- Larger network are hard to manage so centralized management was required.
- In traditional networking we used distributed control plane in which every device manage its own control plane.
- SDN decouple control plane from data plane.
- SDN use the concept of centralized control plane which is provided by Central Controller.
- SDN use API (Application programing interface).



Benefits of SDN

- **Centralized Provisioning** : All devices can be configured from one place.
- **Scalability** : Change your network infrastructure at will and in a moment's notice.
- **Security** : Centralized location for the administrator to control the entire security of the network.
- **PnP**: plug and play or zero touch provisioning
- **Reduced human error**

Disadvantage of SDN

- controller acts as a single point of failure , if the controller is down downstream devices will be in trouble. for this reason SDN controllers deployed in cluster.

Cisco SDN Solutions

ACI
Application Centric Infrastructure

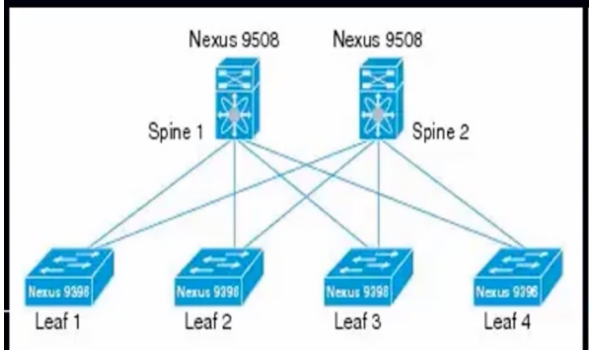
- Cisco SDN Data center solution
- 2-layer, Sine-Leaf Architecture
- Controller(Mgmt Plane) – APIC
- Control-Plane - Spine
- Control-Plane Protocol – IS-IS, COOP (Registration)
- Data-Plane Protocol - VXLAN
- Avoids STP loops, switches connected via L3.
- Underlay routing protocol –ISIS (can't change)
- Spine : NX9500, NX9300
- Leaf: NX9300

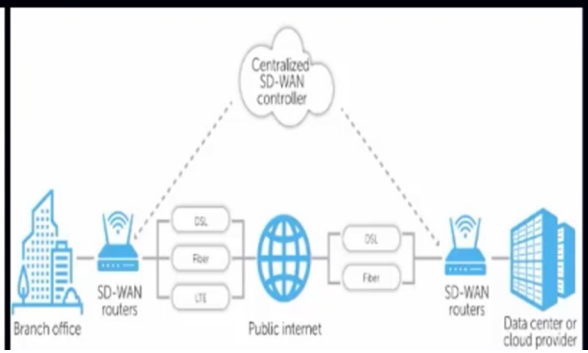
SD-WAN
Software - Defined WAN

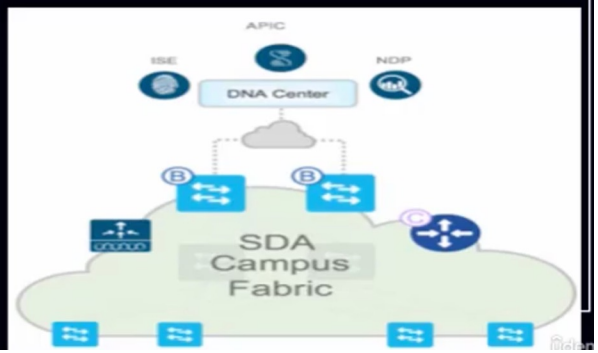
- Cisco SDN WAN solution
- Acquired company called Viptela
- Controller(Mgmt Plane) – vManage
- Control Plane – vSmart
- Data Plane – Wan Edges
- Authentication & Security – vBond
- Control-Plane protocol – OMP
- Data-Plane Protocol - IPSEC

SDA
Software - Defined Access

- Cisco SDN Campus Solution
- Controller(Mgmt Plane) – DNAC
- Control Plane – CP Node
- Data Plane – FEN Nodes
- Policy Plane – ISE
- Control-Plane protocol – any IGP, LISP(Registration)
- Data-Plane Protocol - VXLAN
- Underlay routing protocol –ISIS by default , any IGP
- Underlay switches : Any switches , high port BW
- FEN: catalyst 3850, 9300, 9400
- BEN: catalyst 3850, 9500, NX7700
- CP Node: catalyst 3850, 9500, NX7700







Cisco Software-Defined Access

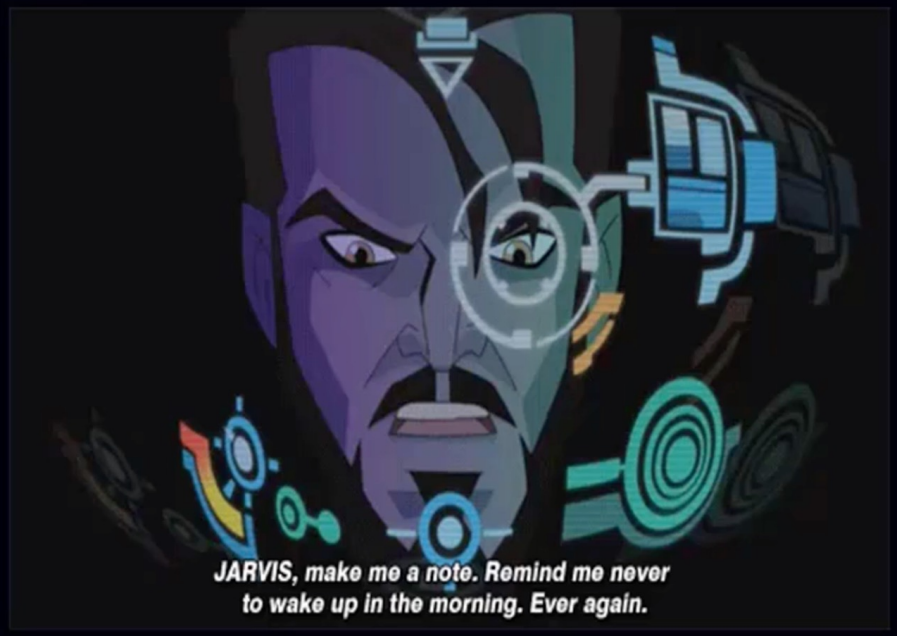
Cisco Software-Defined Access

- Cisco SDN Solution for Campus Networks.
- Cisco SD-Access helps transform traditional campus LAN designs to intent-driven, programmable networks.
- Main components of Cisco SD-Access are Cisco Campus Fabric and Cisco non fabric elements/components (DNAC, ISE)
- DNAC Center offers automation and assurance to create and monitor the Cisco Campus Fabric.

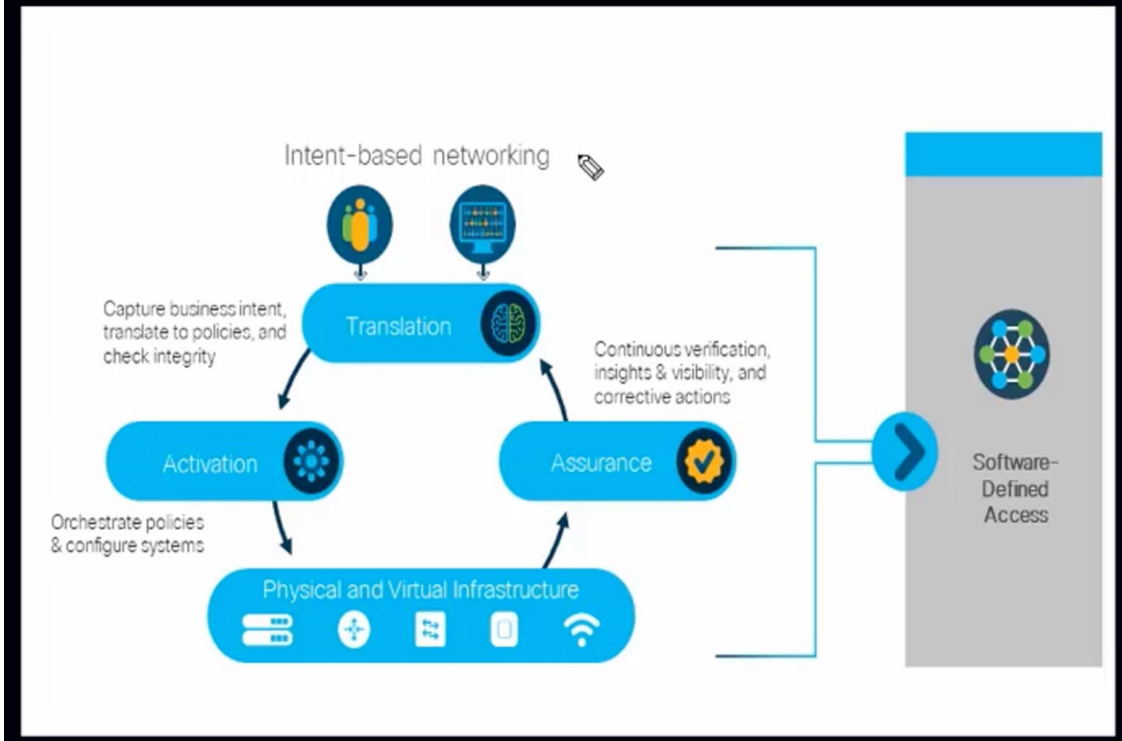
Intent-Based Networking

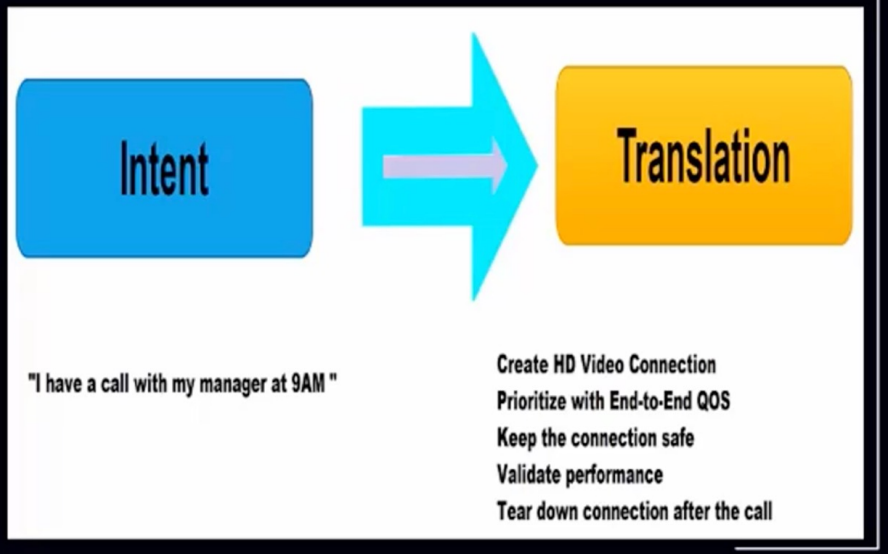
Intent-Based Networking

- Also known as Intent-Driven Networking
- In traditional networking admin manage the network by cli but this way of networking is not scalable, in IBN network admin simply tells the network what their intent is, and network implements it.

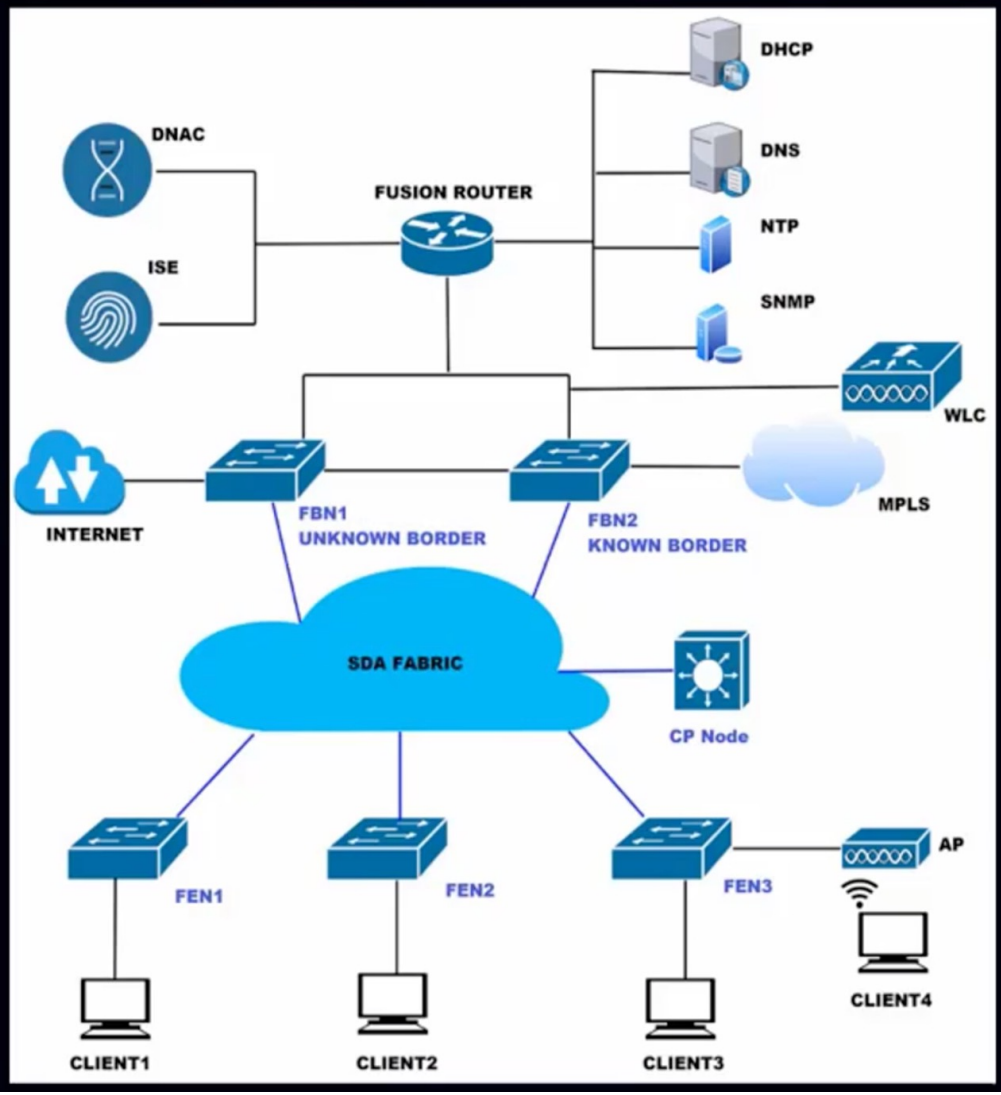


Intent-Based Networking





Cisco Software-Defined Access



Cisco SD-Access: 4 Planes & 4 Layers

1. Control Plane

Control Plane is build using Locator ID Separation Protocol (LISP)
LISP separates identity and location.
Endpoint Identifier (EID) represents identity of client.
Routing Locators (RLOC) represents location of client.
Map-Server (MS) manage mapping database which has EID-RLOC mapping.

2. Data Plane

VXLAN is an encapsulation technique for data packets.
VXLAN is used for data forwarding.
VXLAN builds tunnel between FEN/FBN data forwarding.

3. Management Plane

Orchestration, assurance, visibility, and management.
Cisco DNA Centre (DNAC) controller manage the management plane.
DNAC controller provides Automation which helps deploy fabric devices.
DNAC controller provides Assurance which provides proactive monitoring.

4. Policy Plane

Used for security and segmentation.
Cisco TrustSec (CTS) assign an SGT value to the packet at its ingress point into the network.
An access policy elsewhere in the network is then enforced based on this tag information.

Cisco SD-Access: 4 Planes & 4 Layers

1.Physical Layer

FEN, FBN, CPN, FWLC

All Febric Networkig devices

2.Network Layer

Control Plane : LISP
Data Plane : VXLAN
Policy Plane: CTS

3 Planes resides inside this Layer

3.Controller Layer

DNAC, ISE

StandAlone : 1
Cluster : 3

4.Management Layer

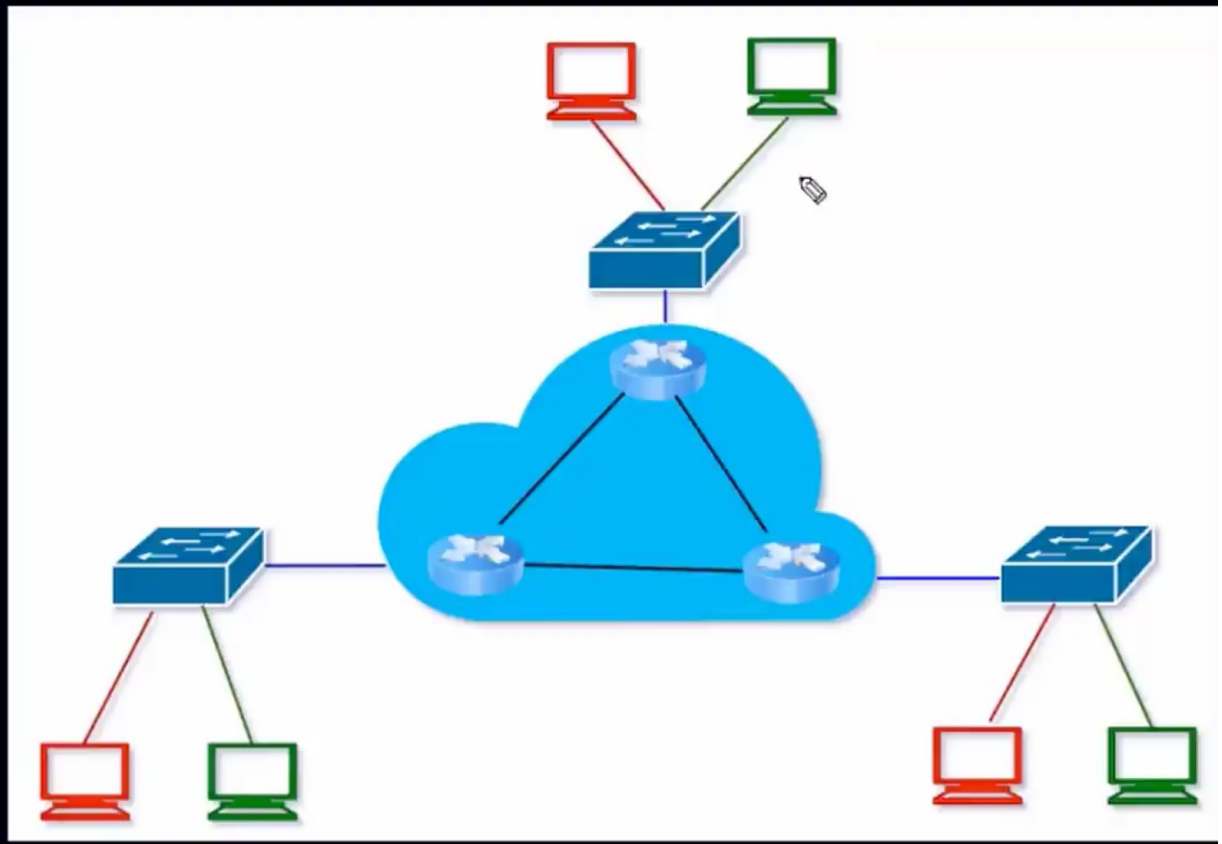
Is Managed using GUI
Management Plane: DNAC

Use of REST-API for gui access

AnyCast Gateway

Anycast Gateway

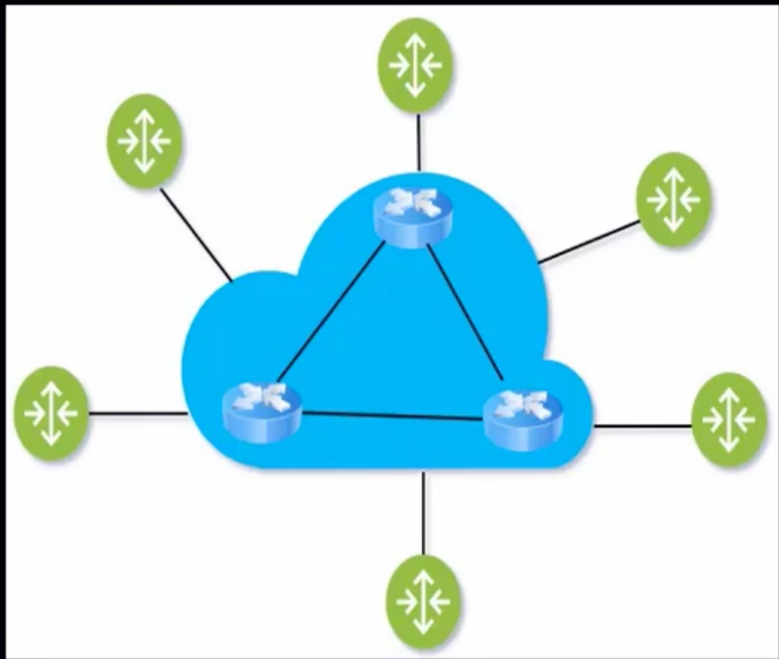
- Inefficient forwarding / traffic flow
  In traditional networking.
- Can't have default gateway in underlay.
- Client subnets not advertised in underlay.
- An address which can reside on multiple devices at the same time.
- Local endpoints/clients use local SVI .
- No duplicate IP problem because SVI are local to switches.
- SVI are only used for local communication not for other purposes like telnet / ssh etc.
- No FHRP required.



Locator Identifier Separation Protocol (LISP)

Locator Identifier Separation Protocol (LISP)

- Mapping and Encapsulation Protocol.
- Originally designed for the Internet but nowadays, used in data centers, Cisco SD-Access.
- IP address has 2 functions :
  - **Identity**: Identify the device.
  - **Location**: Location of the device in the network, used for routing.

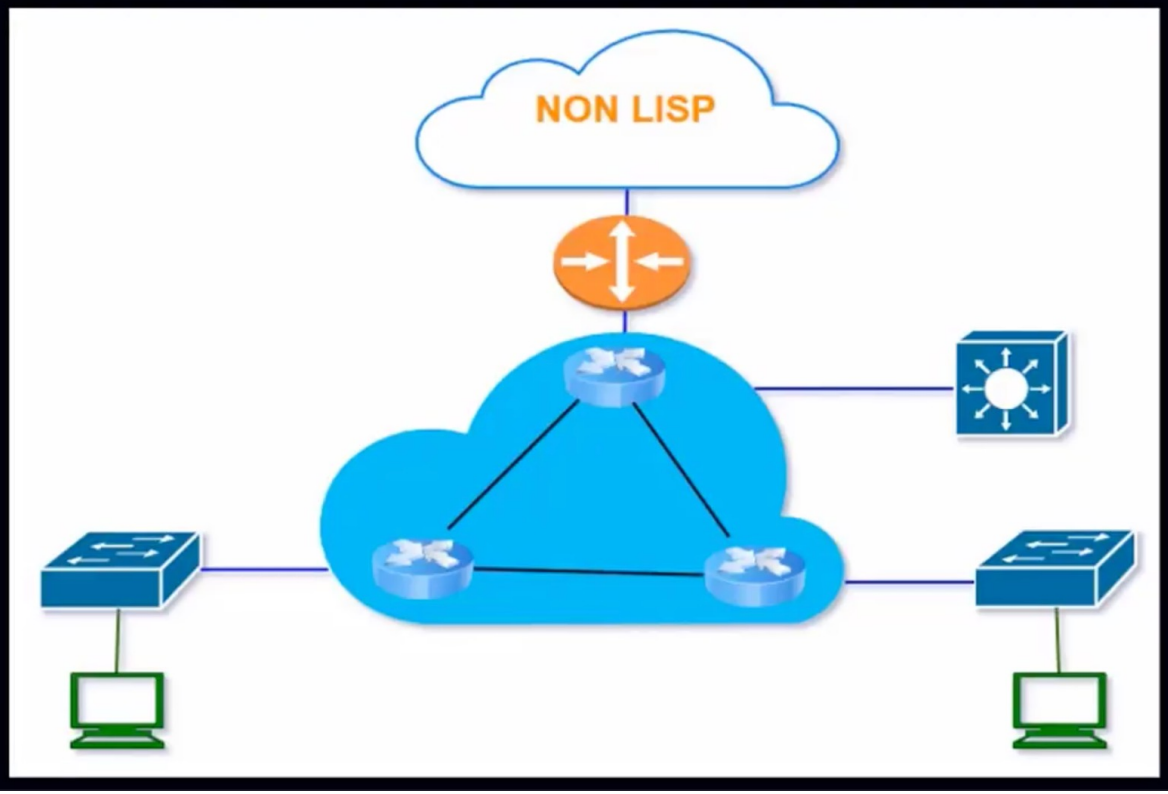


- LISP separates these 2 functions of an IP address into 2 separate functions:
  - **Endpoint Identifier (EID)**: Assigned to clients like computers, laptops, printers, etc.
  - **Routing Locators (RLOC)**: Assigned to routers. We use the RLOC address to reach EIDs.
- In LISP, IP only tells about identity and for location we use the concept of RLOC.
- While protocols like OSPF/EIGRP use PUSH model, LISP is based on a PULL model.

Locator Identifier Separation Protocol (LISP) Control Plane

LISP Control Plane

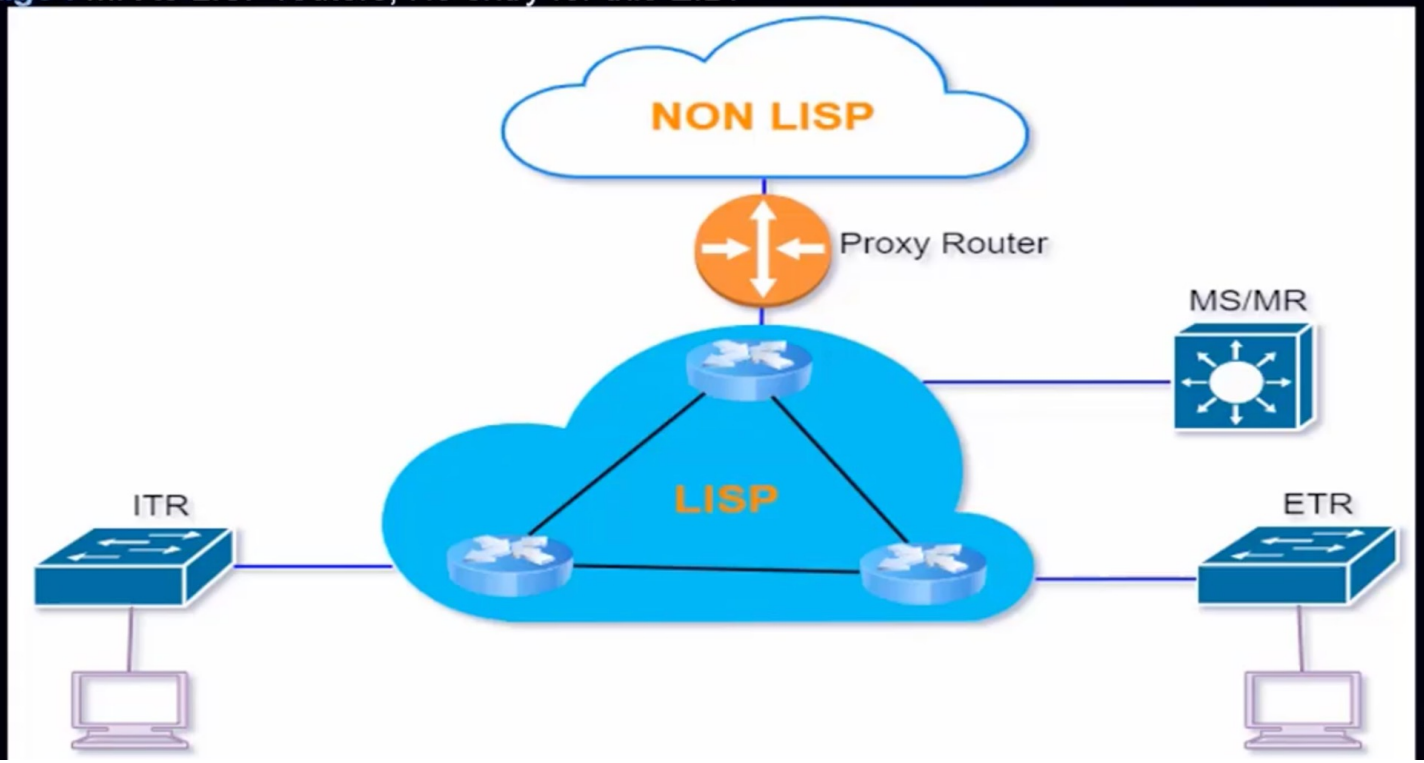
- Map-Server (MS) manage mapping database which has EID-RLOC mapping.
- MAP-Resolver (MR) shares the EID-RLOC mapping information with the LISP routers on request.
- LISP routers has local Map-Cache which it shares with Map-Server, life of Map-Cache entry is 24 hrs.
- MS and MR can be combined to single device for smaller network.
- Think of LISP as DNS ,DNS resolves a hostname to an IP address, LISP resolves an EID to an RLOC.
- LISP is based on a PULL model.



Locator Identifier Separation Protocol (LISP) Message Types

LISP Message

Map-Register Message : LISP routers to MS to update the EID-RLOC mapping.
Map-Notify Message : MS to LISP routers, ack of Map-register msg.
Map-Request Message : LISP routers to MR, to know about EID-RLOC mapping.
Map-Reply Message : MR to LISP routers, as a response of Map-request msg.
Negative-Map Reply Message : MR to LISP routers, No entry for this EID.

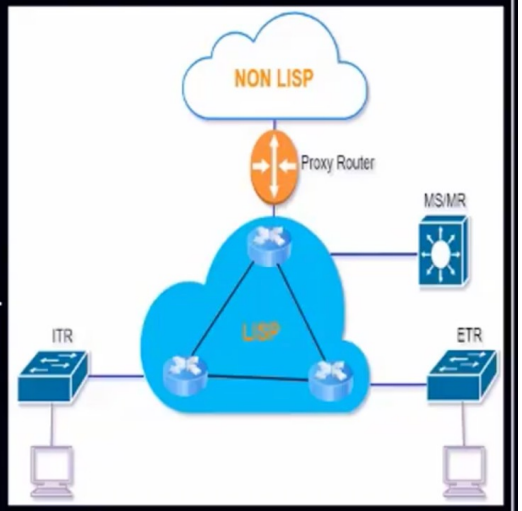


Locator Identifier Separation Protocol (LISP) Data Plane

LISP Data Plane

- L3 Tunneling
- UDP destination port is 4341, source port is random

- **Ingress Tunnel Router (ITR):** Encapsulates IP packets.
- **Egress Tunnel Router (ETR):** De-encapsulates LISP encapsulated IP packets.
- **Tunnel Router (xTR):** Both the ITR and ETR functions , depends on direction of traffic flow.



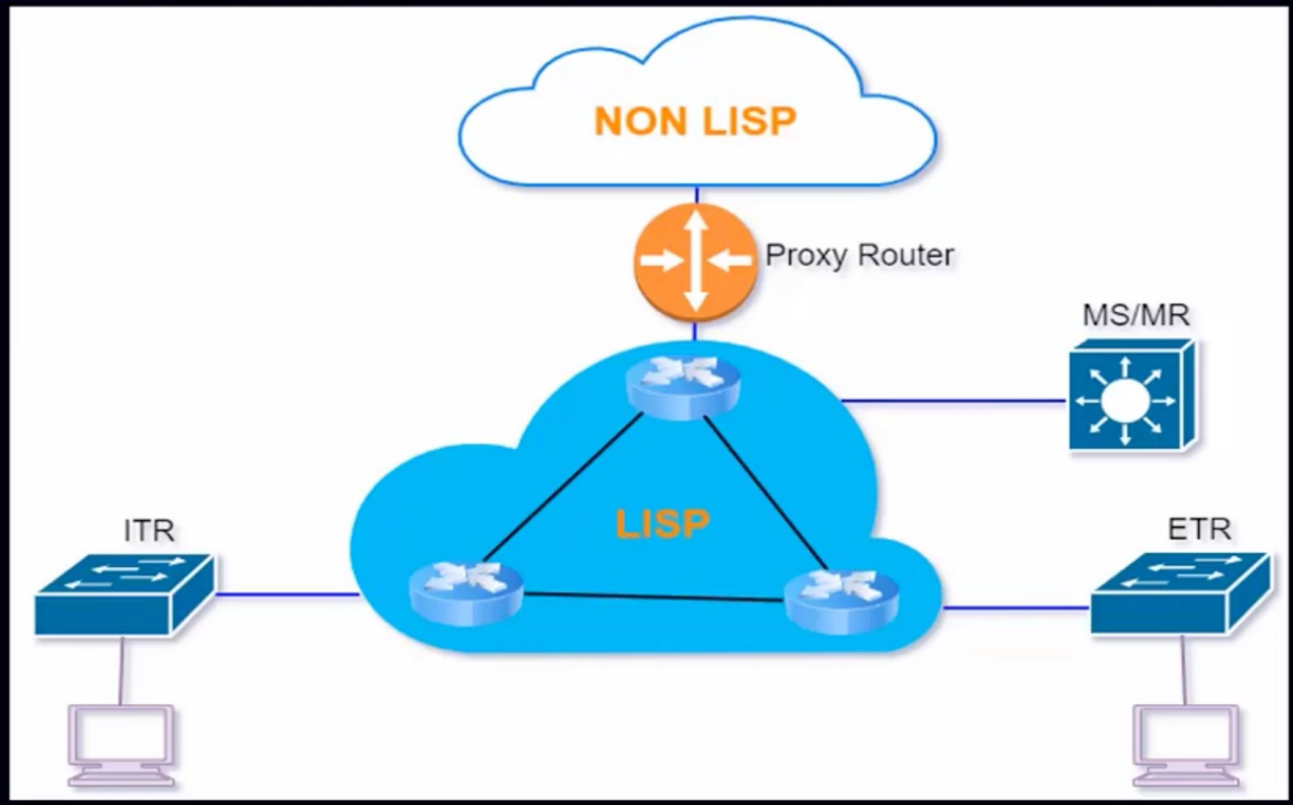
- **Proxy Router (PITR/PETR/PXTR) :** Border router which sits between LISP and non-LISP environment.
- PXTR don't send MAP-register msg to MS.
- Used as default router if MS has no mapping for any given subnet MS send that query to PXTR.

Source IP (ITR)	Destination IP (ETR)	Source UDP port	Destination UDP Port (4341)	LISP Header	Source IP (EID)	Destination IP (EID)	DATA

- Instead of LISP we use VXLAN for SDA data plane because LISP use L3 tunneling and can't share L2 information while VXLAN use L2 tunneling.

Locator Identifier Separation Protocol (LISP) Data Plane

LISP Data Plane

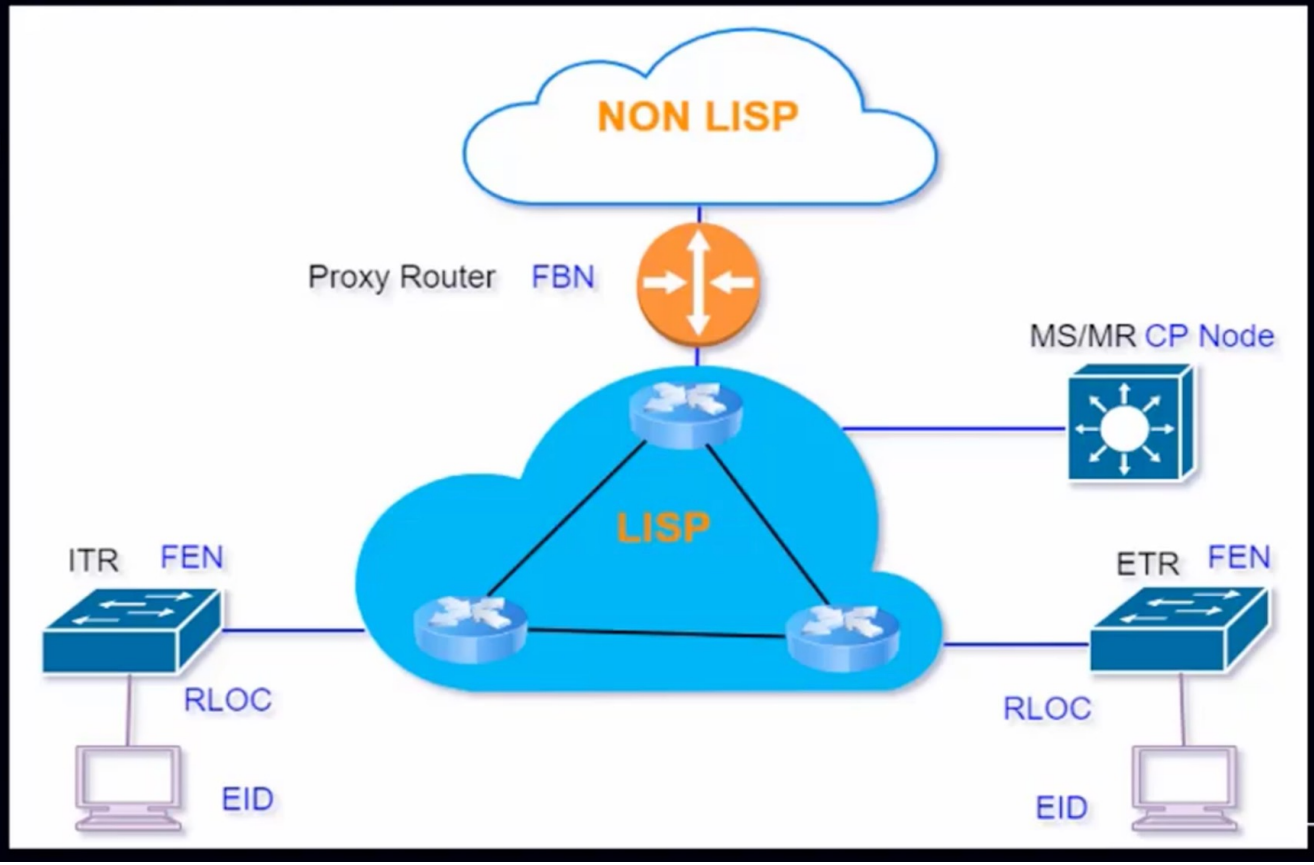


Source IP (ITR)	Destination IP (ETR)	Source UDP port	Destination UDP Port (4341)	LISP Header	Source IP (EID)	Destination IP (EID)	DATA

Locator Identifier Separation Protocol (LISP) in SDA

LISP in Software-Defined Access

- Tunnel Router (xTR) become Fabric Edge Node (FEN)
- Map-Server (MS)/MAP-Resolver (MR) becomes Control Plane Node (CP Node)
- Proxy Router (PXTR) becomes Fabric Border Node (FBN)
- LISP used for Control plane
- VXLAN used for Data plane
- EID IP address of Client
- RLOC Loopback IP address of FEN



Why Virtual Extensible LAN (VXLAN) is Required in SDA?

Why Underlay is Layer3 based (Problems with Layer2 underlay)

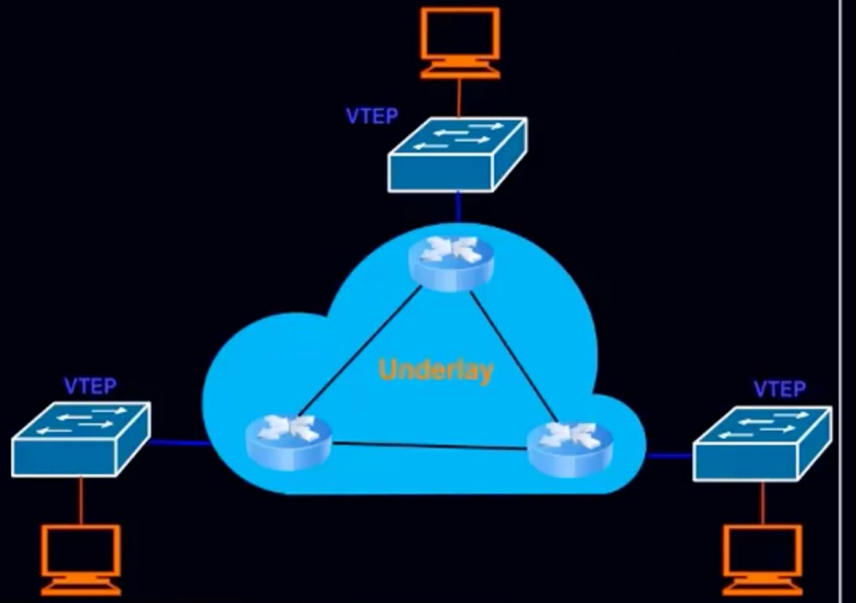
- Spanning Tree
- Limited Number of VLANs , VLAN ID size 16 bits
- Large Broadcast Domain and Large MAC address table

Why Overlay is Layer2 based (Problems with Layer3 overlay)

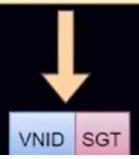
- No subnets and VLAN info sharing across the network

How VXLAN solves the Problem

- VXLAN allows sharing of subnets/VLAN info across L3 boundaries.
- VNID size is 24 bits, so we got 16 Million VNID numbers.
- 1 VNID has 4094 VLAN capability
- Each VNID is assigned per customer , which keep traffic separate.
- With VXLAN MTU is increased by 50-54 Byte, 1550 to 1554Byte total.



Source MAC 6 Bytes	Destination MAC 6 Bytes	802.1Q Tag 2 Bytes	Source IP (VTEP) 20	Destination IP (VTEP) Bytes	Source UDP port 8	Destination UDP Port (4789) Bytes	VXLAN Header 8 Bytes	Source IP (EID)	Destination IP (EID)	DATA



Virtual Extensible LAN (VXLAN)

Virtual Extensible LAN (VXLAN)

- VXLAN used in Data plane for data forwarding in SDA.
- VXLAN is a tunneling protocol that using L2 Tunnels extends Layer2 networks/VLANs across layer 3 network boundaries.
- VXLAN encapsulates the packet using VXLAN header.
- These Layer 2 Tunnels are known as Overlay network which are build over underlay physical network which is Layer 3.
- LISP use L3 tunneling that is why VXLAN is used because it use L2 tunneling.
- VXLAN has both L2 and L3 tunneling capability, but we use L2 Tunneling in SDA.
- VXLAN L2 Tunneling is UDP based, Port number 4789.

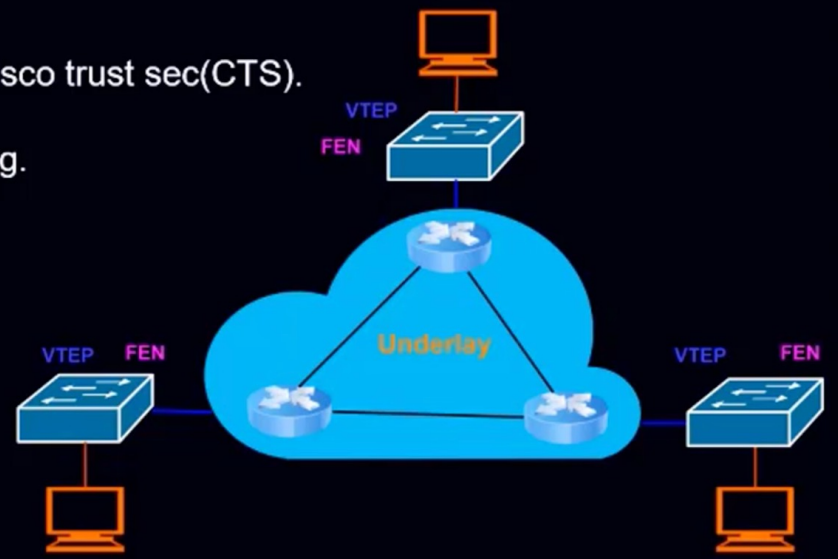
- Think of all this ~~underlay~~ as big L2 switch, FEN are connected via Layer2, clients are connected on different ports of FEN switch.

OVERLAY

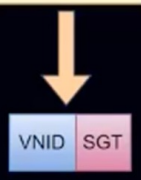
VXLAN in SDA

VXLAN in Software-Defined Access (SDA)

- VXLAN Tunnel end point (VTEP) becomes Fabric Edge Node (FEN).
- VXLAN group policy option (VXLAN-GPO) used in SDA.
- VXLAN header carry scalable group tag(SGT) which are managed by cisco trust sec(CTS).
- VXLAN uses LISP for control plane.
- All FEN form point-to-point L2 Tunnel with each other for data forwarding.



Source MAC 6 Bytes	Destination MAC 6 Bytes	802.1Q Tag 2 Bytes	Source IP (VTEP) 20	Destination IP (VTEP) Bytes	Source UDP port 8	Destination UDP Port (4789) Bytes	VXLAN Header 8 Bytes	Source IP (EID)	Destination IP (EID)	DATA



Protocols Used in Cisco Campus Fabric

Cisco TrustSec (CTS)
- Responsible for security in SDA environment.
- Makes Network Segmentation easier by assigning Tags to traffic, treat the traffic based on Tags rather then IP.

Access Control List (ACL)
- ACL depends on IP address and this the problem

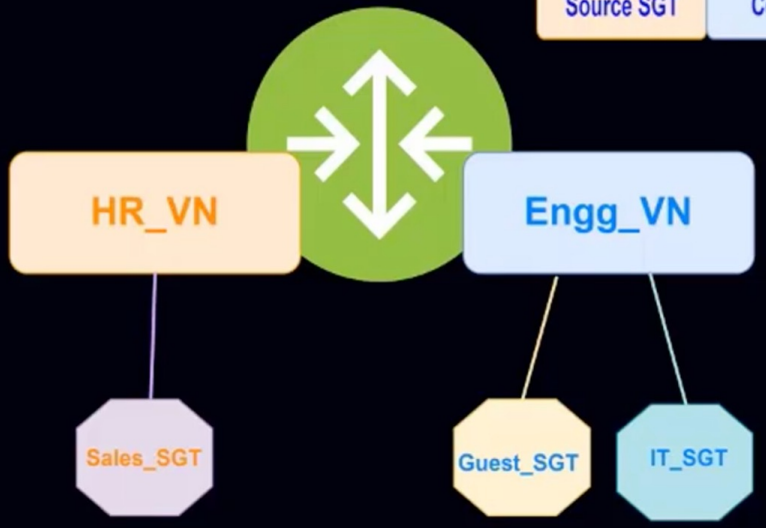
Source IP	Permit/Deny	Destination IP	ACL Name

Types of Segmentation :

➢ **Macro segmentation (InterVN segregation)**
- Traffic segregation between VN (virtual network)
- Similar to VRF

➢ **Micro segmentation (IntraVN segregation)**
- Traffic segregation within VN (virtual network)
- Use Scalable group Tag (SGT)

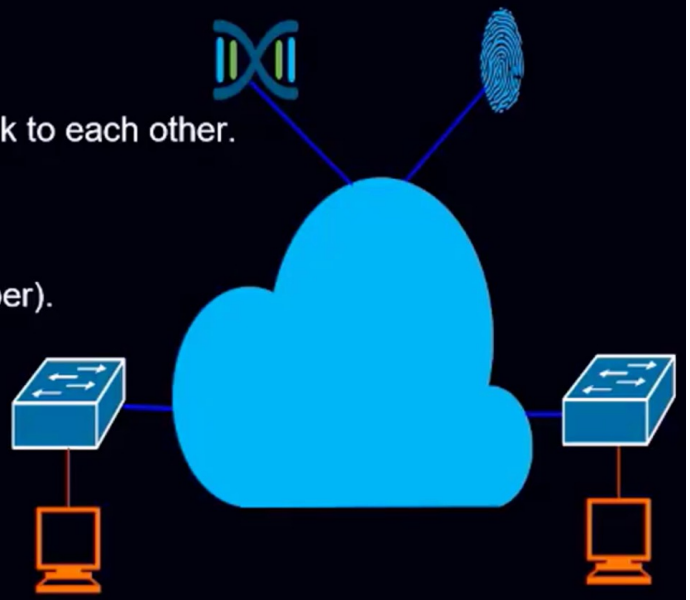
Source SGT	Contract	Destination SGT	Policy Name



Virtual Network (VN) and Scalable Group Tags (SGT)

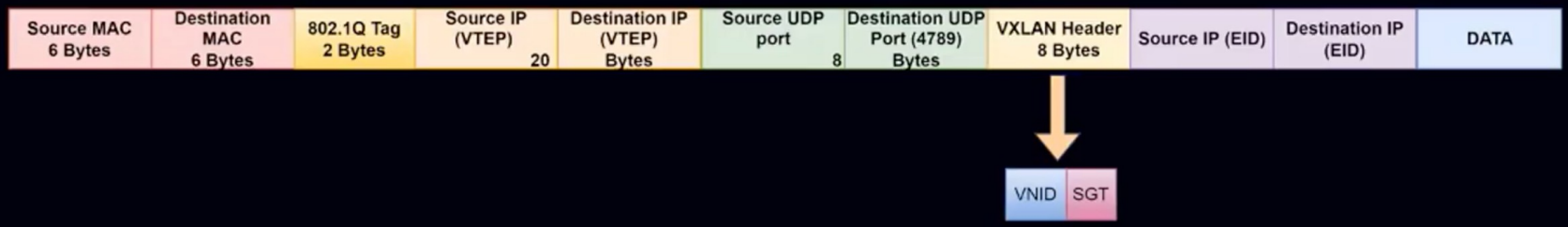
Virtual Network (VN) & Virtual Network Identifier (VNID)

- VN is the name which has a unique VNID.
- Think of VN as VRF.
- Organizations are assigned a VN and by default client of 2 different VN can't talk to each other.
- Initially all SG are part of DEFAULT_VN.



Scalable Group (SG) & Scalable Group Tag (SGT)

- SGT (Scalable Group Tag) is the name given to the tags, has a tag value (number).
- In DNAC, Scalable group tag (SGT)
- In ISE, Security Group Tag (SGT)
- When DNAC and ISE integrated, SGT are copied from ISE to DNAC.
- After Integration, SGT configured on DNAC but applied by ISE on devices.
- Policies are now applied to SGTs instead of IP addresses.
- Both SGT and VNID are part of VXLAN.
- SGT information is contained in the VXLAN-GPO header.
- Within VXLAN header, if group-based policy bit is set to 1, the SGT is carried, if it's 0, the SGT is not carried.



Protocols Used in Cisco Campus Fabric

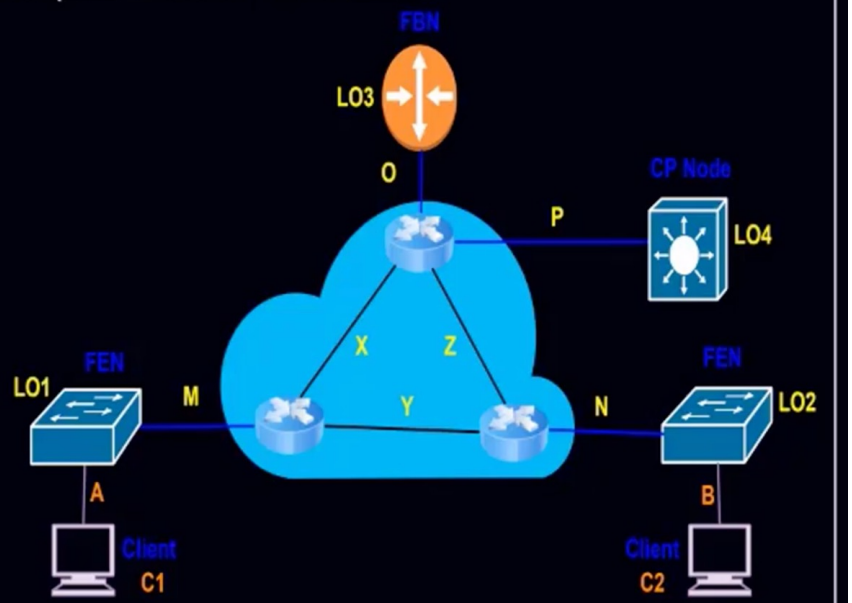
Protocols used in Cisco Campus Fabric

- Routing Protocol for Underlay (ISIS, OSPF, EIGRP)
- Anycast
- Locator Identifier Separation Protocol (LISP)
- Virtual Extensible LAN (VXLAN)
- Cisco TrustSec (CTS)

Routing Protocols for Underlay in SDA

Routing Protocol for Underlay (ISIS, OSPF, EIGRP)

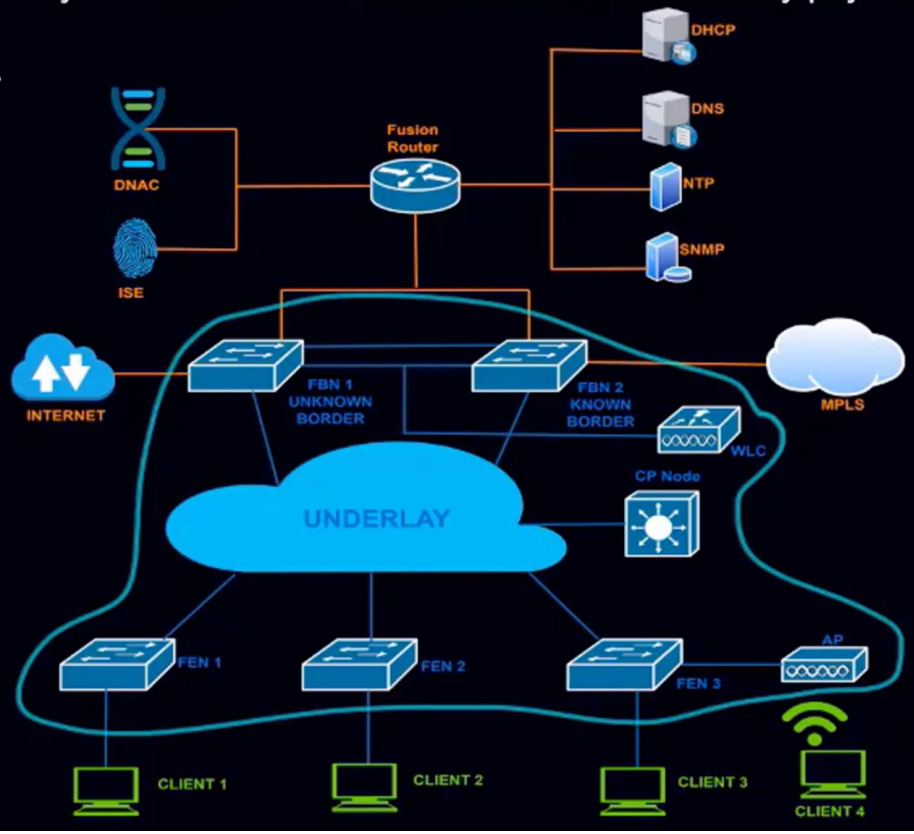
- Any IGP can be used as an underlay routing protocol, like OSPF, EIGRP, ISIS (cisco recommended).
- IGP can be configured, Manual or Automated using DNAC (using PNP).
- Only underlay subnets/L3 and Loopback of FEN/BEN/CP advertised using IGP.
- Purpose is to have loopback-to-loopback reachability. (which builds a solid foundation for LISP and VXLAN)
- Client subnets are not advertised using underlay routing protocol.
- Every underlay router and FEN/BEN/CPN have routing table which has loopback info of each other.



What is Cisco SDA Campus Fabric?

Cisco SDA Fabric

- A fabric is simply an overlay network.
- All the devices together forms the Fabric.
- An overlay network creates a logical topology used to virtually connect devices that are built over an arbitrary physical underlay topology.
- Overlay (or tunnel) provides logical full-mesh connection.
- Think of a cloth where everything is connected together.



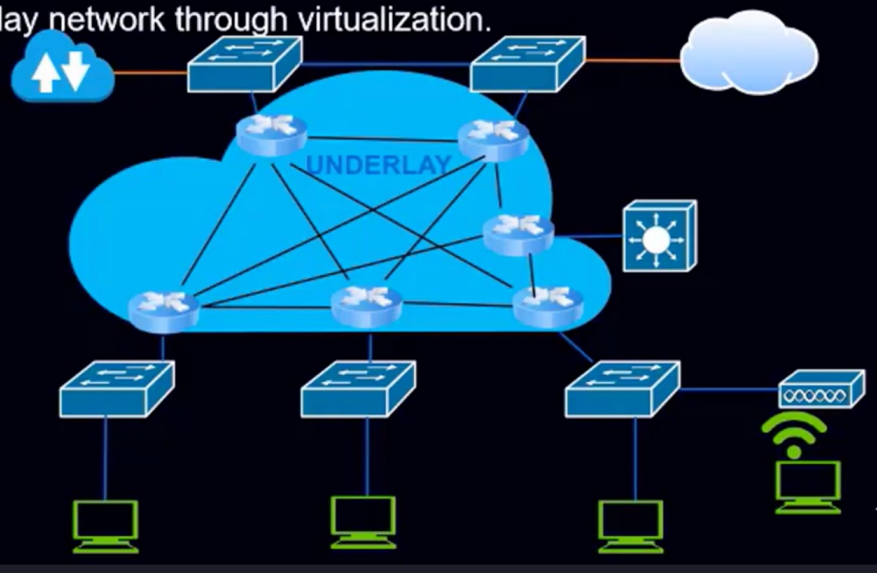
Underlay & Overlay (Network and devices)

Underlay Network

- Underlay network is defined by physical switches and routers that are used to deploy the sd-access network.
- All devices of underlay must establish IP connectivity via the use of a routing protocol.
- End-user subnets are not advertised in underlay network.

Overlay Network

- An overlay network is created on top of the underlay network.
- Data plane traffic and control plane signaling are contained within each virtualized network maintaining isolation among the networks and an independence from the underlay network.
- Multiple overlay networks can run across the same underlay network through virtualization.
- End-user subnets are advertised using overlay network.



Fabric Edge Node (FEN)

Fabric Edge Node (FEN)

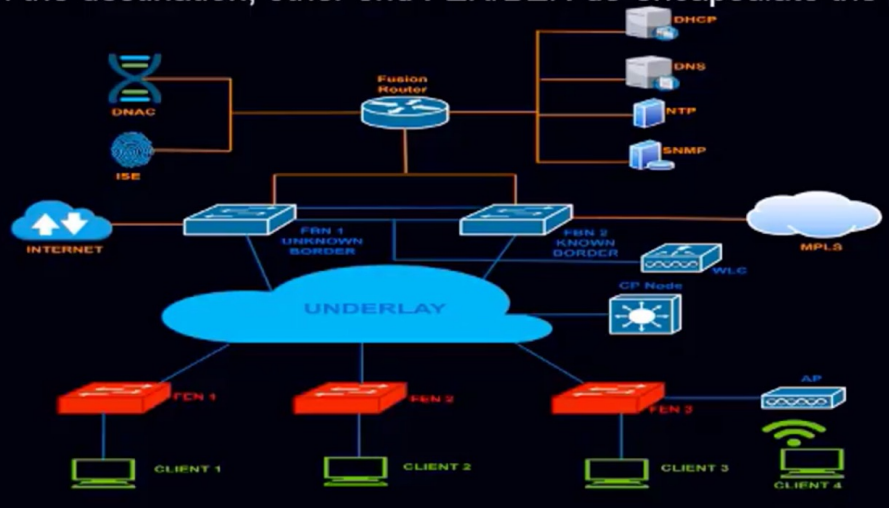
- Equivalent of an access layer switch in a traditional campus LAN design.
- Equivalent of an XTR in LISP.
- Equivalent of an VTEP in VXLAN.

Functions of FEN

- **Endpoint Registration:** Shares local database/EID-table with CP Node via LISP map-register message.
- **Anycast Layer 3 gateway:** A common gateway/SVI is configured on all FEN to avoid Inefficient forwarding/ traffic flow.
- **Mapping of user to virtual network:** Endpoints are placed into virtual networks.
- **AAA Authenticator:** Collects authentication credentials from endpoint, relays that to the Authentication Server.
- **VXLAN encapsulation/de-encapsulation:** Packets are encapsulated in fabric VXLAN and forwarded across the overlay, either sent to another FEN or to the BEN , depending on the destination, other end FEN/BEN de-encapsulate the packet

Models

Catalyst 9000-series: 9200, 9300, 9400, 9500
Catalyst 3850 and 3650
Catalyst 4500E: Sup 8-E, 9-E



Fabric Border Node (FBN)

Fabric Border Node (FBN)

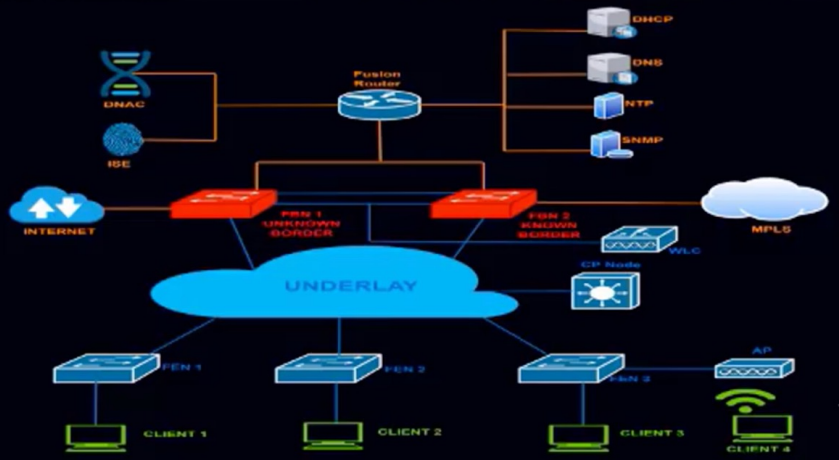
- Serves as the gateway between the SD-Access fabric site and the networks external to the fabric.
- Responsible for network virtualization interworking and SGT propagation from the fabric to the rest of the network.
- Equivalent of an PXTR in LISP.
- **Known Border Node (Internal Border Node):** Known subnets (Like DC).
- **Unknown Border Node (External Border Node):** Unknown subnets (Default Route 0.0.0.0/0).
- **Hybrid Border Node (Anywhere Border Node):** Known Border + Unknown Border

Functions of FBN

- **Advertisement of EID subnets:** Advertise endpoint prefix to outside the fabric.
- **Fabric site exit point:** Gateway of last resort for the fabric edge nodes.
- **Policy mapping:** Maps SGT information from within the fabric to be appropriately maintained when exiting that fabric.
- **VXLAN encapsulation/de-encapsulation:** Packets received from outside the fabric and destined for an endpoint inside of the fabric are encapsulated in fabric VXLAN by the border node. Packets sourced from inside the fabric and destined outside of the fabric are de-encapsulated by the border node.

Models

Catalyst 9000-series: 9300, 9400, 9500, 9600
Catalyst 3850
Catalyst 6840-X, 6880-X
Nexus 7700: Sup 2-E, 3-E
ISR 4300, 4400
ASR 1000-X, 1000-HX



Control Plane Node (CPN)

Control Plane Node (CP Node)

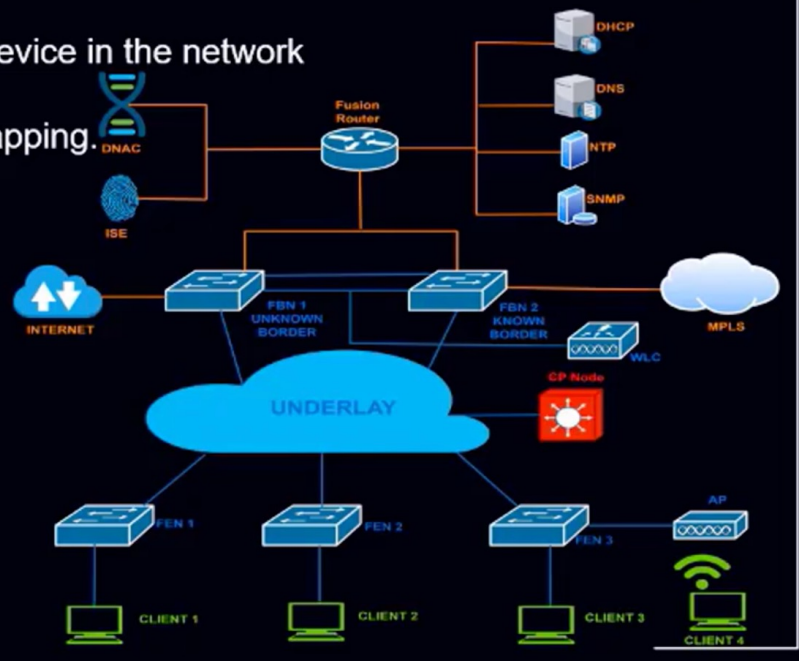
- Manages Control Plane of SDA Fabric devices, Brain of the fabric.
- Maintains EID-to-RLOC database, Keeps track of all endpoints in the fabric site with associated FEN.
- Equivalent to LISP Map-Server and Map-Resolver

Functions of CP Node

- **Host tracking database:** Host tracking database (HTDB) is a central repository of Endpoint ID to Routing Locator (EID-to-RLOC) bindings.
- **Endpoint identifiers (EID):** An address used for identifying an endpoint device in the network
- **Map-Server:** Receives EID-to-RLOC from FEN.
- **Map-resolver:** Responds to queries from FEN regarding EID-to-RLOC mapping.

Models

Catalyst 9000-series: 9300, 9400, 9500, 9600
Catalyst 3850
Catalyst 6840-X, 6880-X
Nexus 7700: Sup 2-E, 3-E
ISR 4300, 4400
ASR 1000-X, 1000-HX



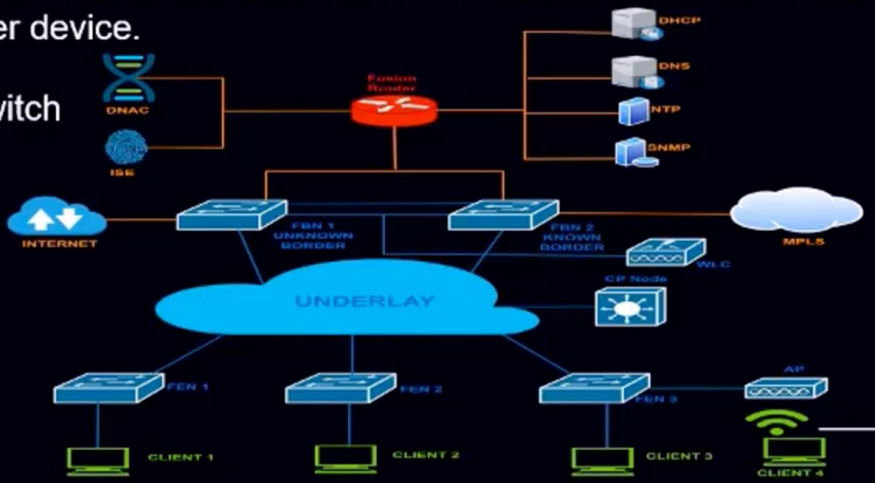
Fusion Device/Router

Fusion Device/Router

- Provides access to shared services for the endpoints in the fabric.
- Not managed by DNAC, configure it manually, not part of SDA fabric.
- Fusion Router required for inter-VN communication.
- Fusion router will have ebgp/ibgp with FBN & ebgp/ibgp/igp with shared services.
- Fusion router shares/redistribute subnets with FBN.
- 2 ways to Provide shared services access, depending on how the shared services are deployed. Both require the fusion device to be VRF-aware.
- **Route Leaking:** Used when the shared services routes are in the GRT of fusion device.
- **VRF Leaking:** Used when shared services are deployed in a dedicated VRF on the fusion device.

Functions of Fusion Device/Router

- **Multiple VRFs:** Multiple VRFs are needed for the VRF-Aware peer model. For each VN that is handed off on the border node, a corresponding VN and interface is configured on the peer device.
- **Sub-interfaces:** When Fusion device is a Routers or Firewall
- **Switched Virtual Interfaces:** When Fusion device is a Layer 3 switch
- **Support IGP, BGP, MPBGP**



Models

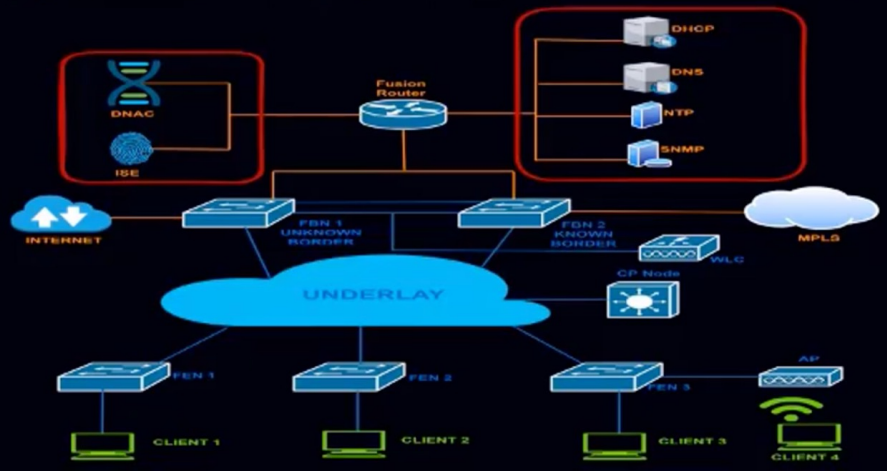
Any L3 Device with Support for Inter-VRF leaking.

Shared Services

Shared Services

- Any services that are common to the enterprise and typically live outside of the Cisco SD-Access fabric but still need to communicate with hosts in the fabric on all virtual networks (VNs).
- Consist of DHCP,DNS,NTP,SNMP,WLC,ISE,DNAC components which must be made available to other virtual networks (VN's) in the campus.
- Fusion Router directly attached outside of the fabric provides a mechanism for route leaking of shared services prefixes across multiple VN.

Dynamic Host Configuration Protocol (DHCP): Provides IP addresses and other settings to hosts in a network
Domain Name System (DNS): Provides name-resolution services to hosts in a network
Network Time Protocol (NTP): Provides accurate time information for hosts and network devices to synchronize their system clocks.
Simple Network Management Protocol (SNMP): Provides monitoring services to devices in a network.



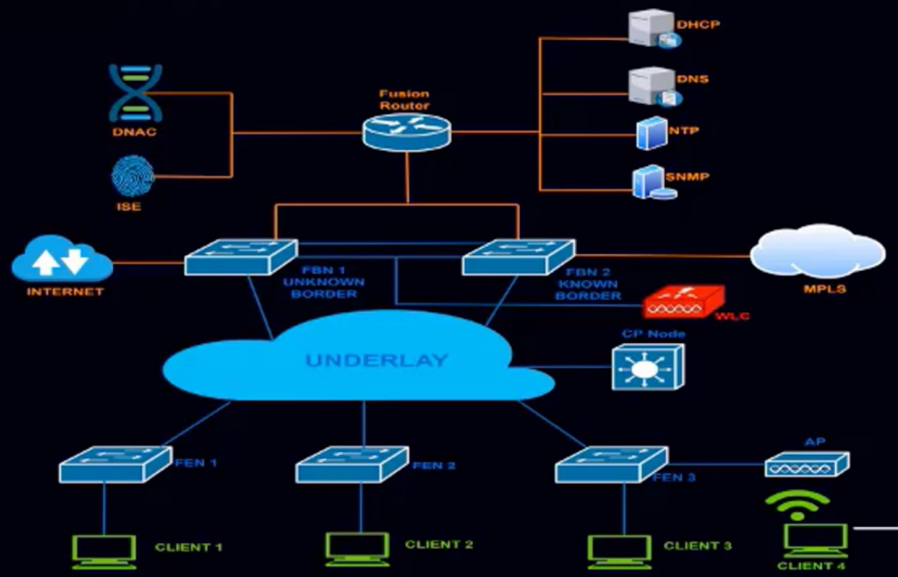
Fabric WLC

Fabric WLC

- Fabric-enabled AP connect to FEN switches and use the underlay to establish a CAPWAP tunnel with the WLC. This tunnel carries control channel information, including wireless host reachability information, from the APs to the WLC, which is in turn advertised to the fabric control plane node in the fabric.
- Data plane traffic is sent directly from the AP to the FEN switch so that traffic stays local to the fabric, where it is subject to the same policy and flow as applied to wired endpoint traffic.
- This increases the efficiency and performance of wired-to-wireless communication, because wireless traffic is no longer centralized at the WLC as it is in traditional wireless environments. (Traffic from AP is de-capsulated on the edge switch without tunneling it up to its WLC).
- Fabric access points and WLCs can also run in hybrid configurations, supporting both fabric-enabled SSIDs and traditional centralized SSIDs on the same hardware.

Models

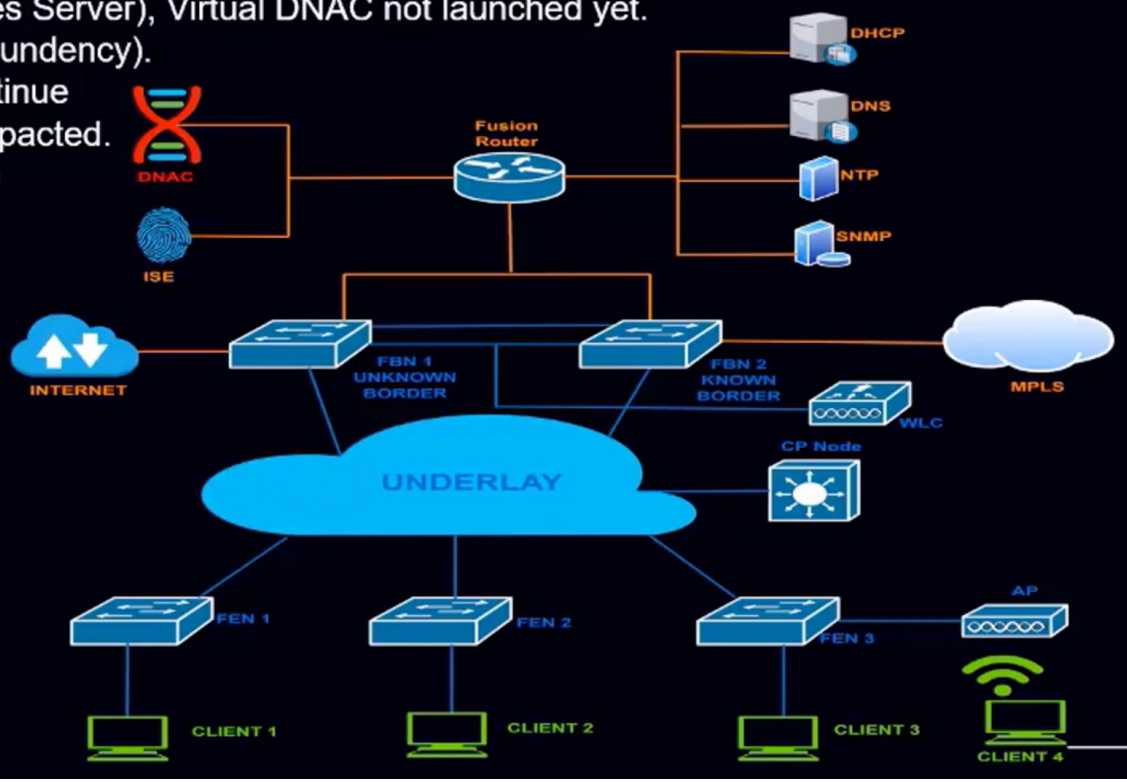
Catalyst 9800 Wireless Controller: 9800-40, 9800-80, 9800-CL
Wi-Fi 6 APs: Catalyst 9115AX, 9117AX and 9120AX
Wave 2 APs: Aironet 1800, 2800 and 3800



Digital Network Architecture Center Controller (DNAC Controller)

Digital Network Architecture Center Controller (DNAC Controller)

- Physical appliance that controls the configuration of SDA Based Network.
- Responsible for Discovery & Configuration of the SDA Devices. (manual discovery or PnP/Lan automation)
- Responsible for Config & Maintenance & Mgmt of all the devices in SDA Fabric.
- DNAC Manage Management Plane of SDA devices, Control Plane managed by CPNode.
- Hardware Based Appliance (Cisco UCS C-series Server), Virtual DNAC not launched yet.
- Deployed as standalone or cluster of 3 (for Redundency).
- If DNC Becomes Unavailable Fabric would continue to function,but automatic provisioning will be impacted. (won't be able to make chnages in our network)
- Manual config is prone to error, DNAC provide automatic provisioning.
- Devices can be accessed with a single click.



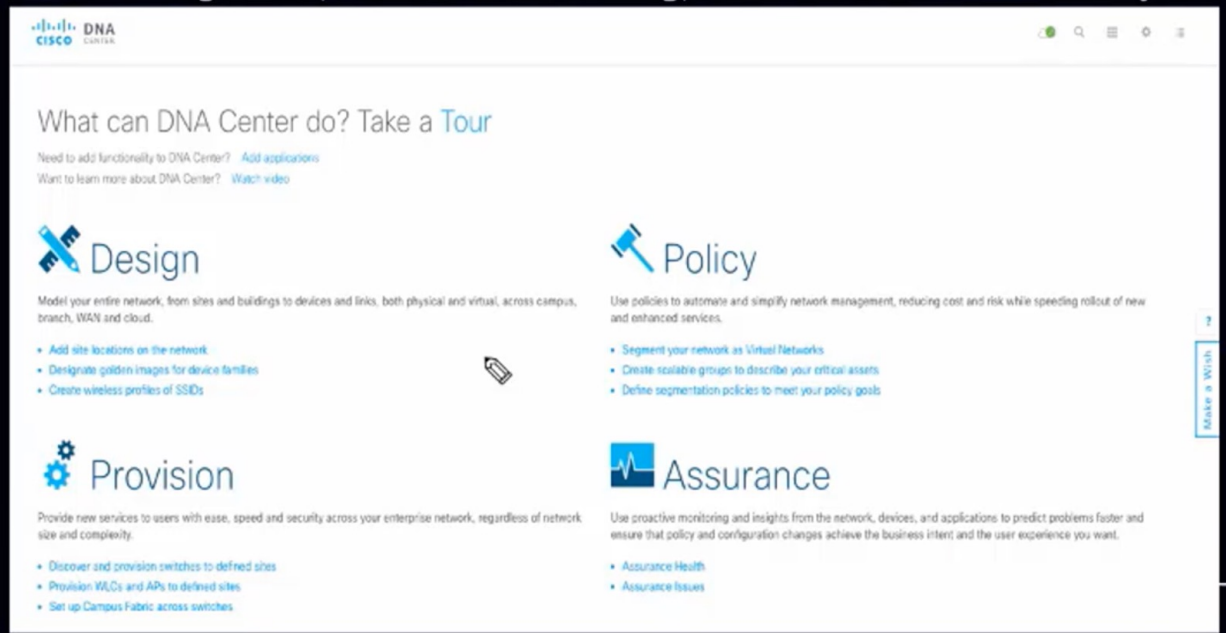
Digital Network Architecture Center Controller (DNAC)

Functions of DNAC

- **Design:** Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, device templates and telemetry configurations such as Syslog, SNMP, and NetFlow.
- **Policy:** Defines business intent including creation of virtual networks, assignment of endpoints to virtual networks, policy contract definitions for groups, and configures application policies (QoS).
- **Provision:** Provisions devices and adds them to inventory for management, supports Cisco Plug and Play, creates fabric sites along with other SD-Access components, and provides service catalogs such as Stealth watch Security Analytics and Application Hosting on the Cisco Catalyst 9000 Series Switches.
- **Assurance:** Enables proactive monitoring and insights to confirm user experience meets configured intent, using network, client, and application health dashboards, issue management, sensor-driven testing, and Cisco AI Network Analytics.

Models

- DN2-HW-APL (1000 Devices)
- DN2-HW-APL-L (2000 Devices)
- DN2-HW-APL-XL (5000 Devices)



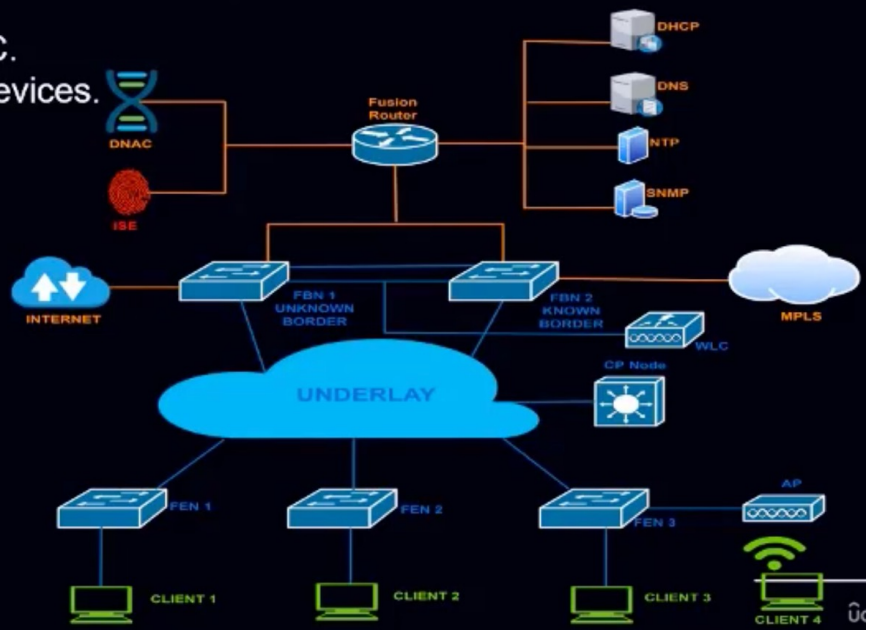
Identity Services Engine (ISE)

Identity Services Engine (ISE)

- Cisco Identity Services Engine (ISE) provides identity services for the SDA solution.
- Cisco TrustSec (CTS) applies Security Group Tags (SGTs) on the traffic based on the identity. These tags can be used to perform filtering using SGT-based access-lists.
- Cisco ISE integrates with DNA Center using REST API and PXGrid. DNA uses REST API to automate policy configuration on ISE and PXGrid is used for endpoint information exchange.
- ISE performs policy implementation, enabling dynamic mapping of users and devices to scalable groups and simplifying end-to-end security policy enforcement.
- Cisco DNAC pushes policies to ISE, endpoints are authenticated and authorized by ISE and as a part of authorization an SGT is assigned to the endpoints.
- When DNAC and ISE integrated, SGT are copied from ISE to DNAC.
- After Integration, SGT configured on DNAC but applied by ISE on devices.
- ISE is available as a virtual and physical appliance.

Models

- SNS-3515, SNS-3595, R-ISE-VMS, R-ISE-VMM, R-ISE-VML



Miscellaneous Components

Fabric in a Box

- Fabric in a Box is an SD-Access construct where the FBN, CPNode, and FEN are running on the same fabric node.
- This may be a single switch, a switch with hardware stacking, or a StackWise Virtual deployment.
- There is no Underlay network in this deployment.

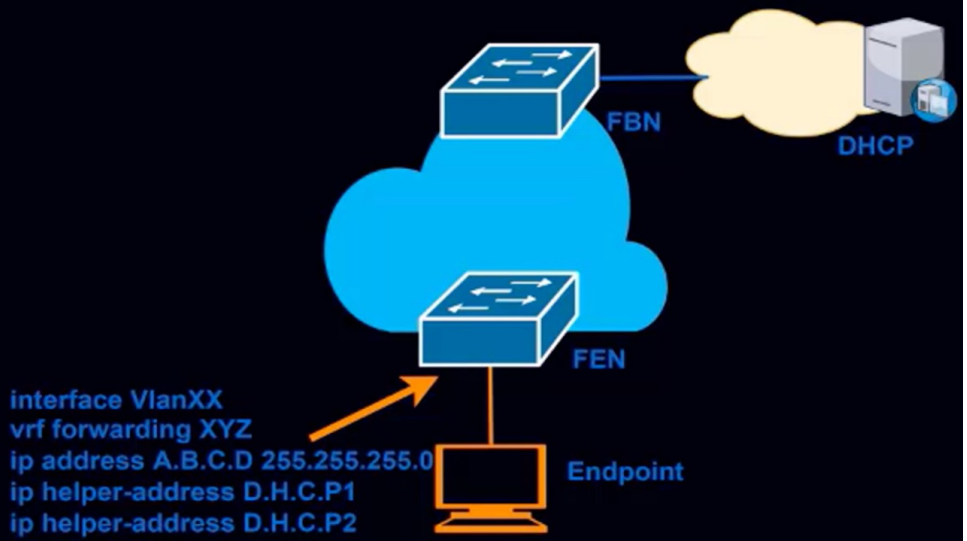
Intermediate Nodes

- Part of the Layer 3 network used for interconnections among the devices operating in a fabric role such as the interconnections between border nodes and edge nodes.
- These interconnections are created in the Global Routing Table on the devices and is also known as the underlay network.
- Intermediate nodes simply route and transport IP traffic between the devices operating in fabric roles.

DHCP in SD-Access

DHCP in SD-Access

- After endpoint authentication, Cisco ISE instructs FEN to place the switch interface connected to the endpoint onto a VLAN and tag each packet from the endpoint with a specific SGT.
- If clients are not given Static IP, they broadcast DHCP request packet in order to get an IP address from the DHCP server.
- In Cisco SD-Access, an anycast gateway(SVI) encapsulates all DHCP requests and unicasts them to a DHCP server in the network with anycast gateway(SVI) as a source and DHCP server as destination.
- FEN act as DHCP relay agent which use DHCP Option 82 field which helps fabric to locate the source of the DHCP request when the DHCP server replies.

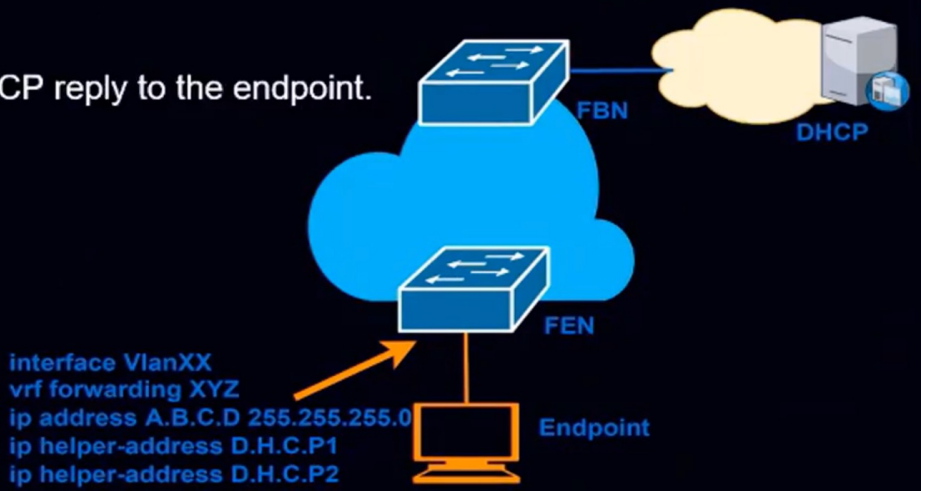


DHCP in SD-Access

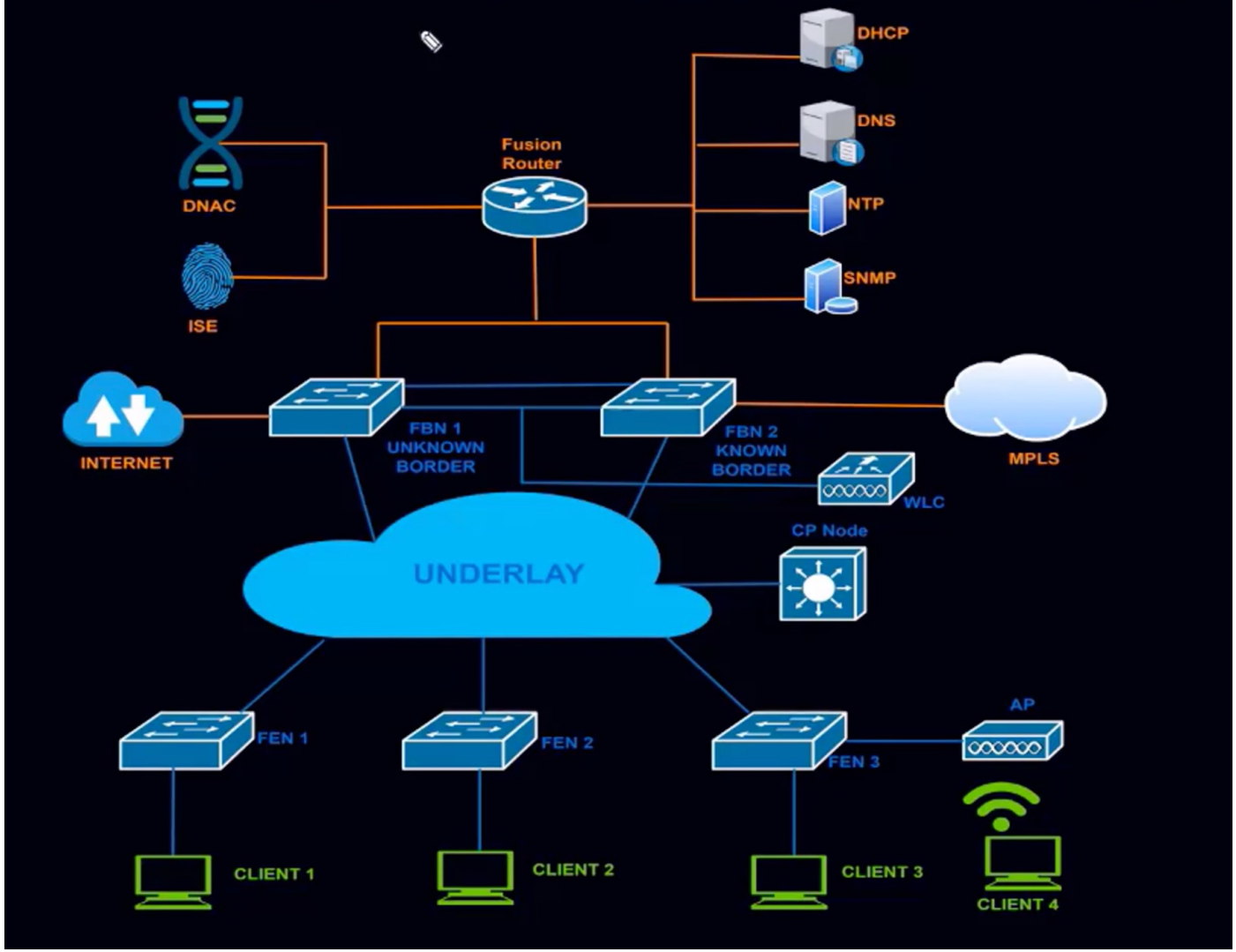
DHCP Request Process in SD-Access

- The client sends a broadcast DHCP request packet.
- FEN adds DHCP Option 82 , which contains VNID , RLOC of FEN.
- FEN encapsulates the request into a unicast packet with the IP address of the SVI/anycast gateway as source and the DHCP server IP address as the destination.
- Packet is routed and sent via the FBN to the DHCP server outside of the fabric.

- The DHCP reply is received by the fabric border.
- Anycast gateway(SVI) could be configured on multiple routers so, Anycast gateway(SVI) can't be used as destination.
- FBN read Option 82, which contains VNID , RLOC of FEN.
- FBN Sends DHCP response to FEN (RLOC of FEN).
- FEN receives the reply, de-encapsulates the packet, forward DHCP reply to the endpoint.



SDA Packet Flow : Endpoints belong to same subnet



SDA Packet Flow

Endpoints belong to same subnet

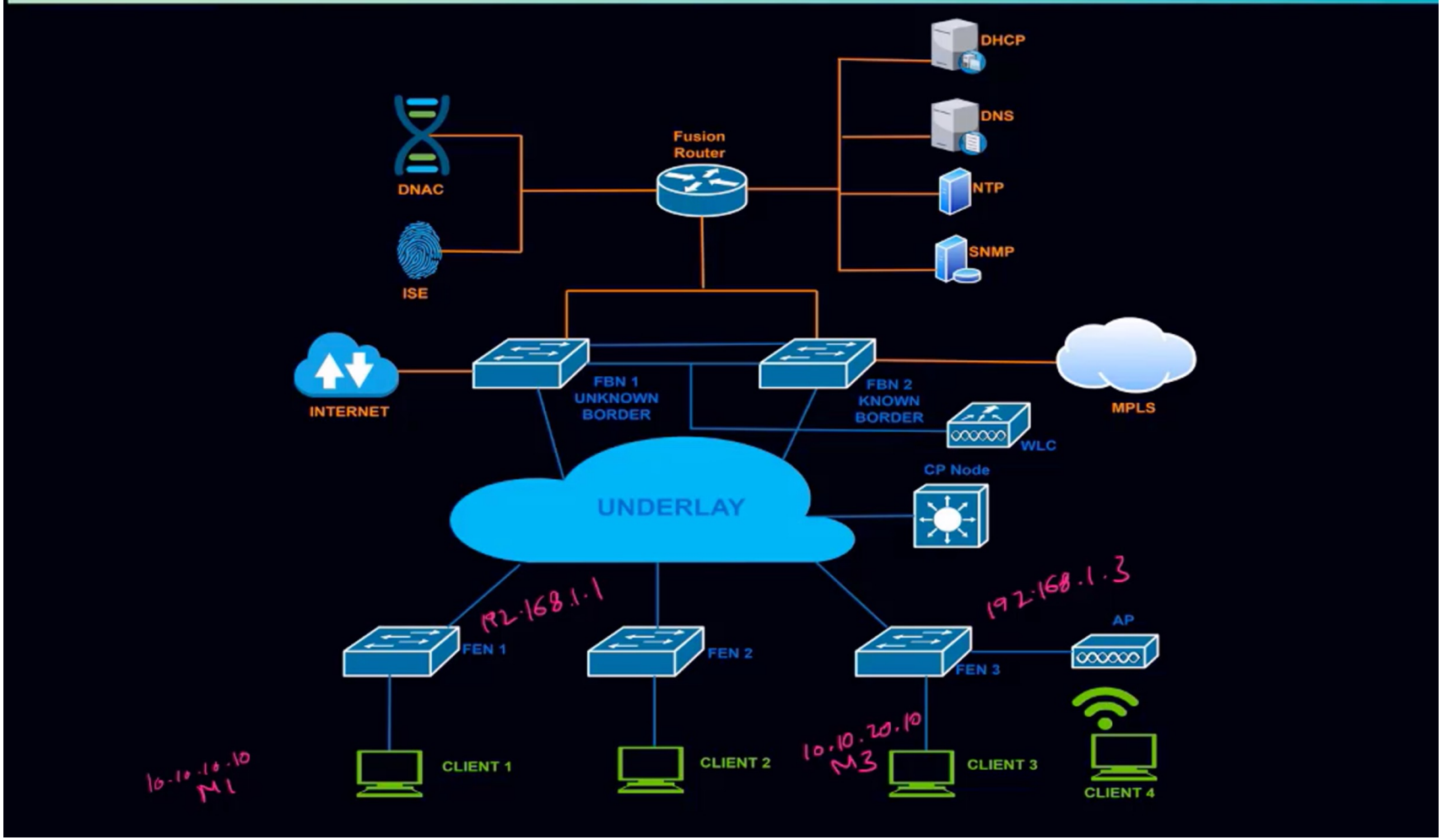
1. Client1 & Client2 belongs to same subnet , Client1(10.10.10.10) need MAC address of Clinet2(10.10.10.11) to start the communication.
2. Client1(10.10.10.10) send ARP request for Client2 (10.10.10.11).
3. FEN1 intercepts the ARP request and sends a LISP ARP request to the CPNode.
4. CPNode replies with Client2(M2) MAC entry from its LISP ARP table. (CPNode has EID-to-MAC-to-RLOC mapping of all the endpoints in SDA fabric)
5. FEN1 saves this mapping in its ARP cache, also shares this information with Client1(10.10.10.10).
6. FEN1 send MAP-Request to CPNode for the location of Clinet2(10.10.10.11) IP/MAC address.
7. CPNode replies with MAP-Response to FEN1(192.168.1.1) with RLOC for Clinet2(10.10.10.11) which is FEN2(192.168.1.2).
8. Now, Clinet1(10.10.10.10) sends packet towards FEN1(192.168.1.1) which is for destination Clinet2(10.10.10.11).
9. FEN1(192.168.1.1) check its local-cache and finds an EID-to-RLOC entry for Clinet2(10.10.10.11), which is via RLOC FEN2(192.168.1.2).
10. FEN1(192.168.1.1) encapsulate the packet using VXLAN, which has Source RLOC FEN1(192.168.1.1), Destination RLOC FEN2(192.168.1.2) and VXLAN header that has VNID & SGT tags.

Source IP	Destination IP
Client1(10.10.10.10)	Clinet2(10.10.10.11)

Source IP	Destination IP	VXLAN Header		Source IP	Destination IP
RLOC FEN1(192.168.1.1)	RLOC FEN2(192.168.1.2)	VNID	SGT	Client1(10.10.10.10)	Clinet2(10.10.10.11)

11. FEN1(192.168.1.1) send this VXLAN encapsulated packet towards the SDA fabric which is for RLOC destination FEN2(192.168.1.2).
12. Inside Fabric, underlay devices will route the VXLAN packet, based on destination RLOC FEN2(192.168.1.2).
13. VXLAN encapsulated packet received at FEN2(192.168.1.2), FEN2(192.168.1.2) deencapsulate the packet, remove the VXLAN header and inspect the SGT and VNID and Client1(10.10.10.10) IP address.
14. If VNID is same for Client1(10.10.10.10) and Client2 (10.10.10.11) traffic accepted. Else, traffic dropped. (Macro-segmentation)
15. Now SGT checked , if communication between SGT is allowed as per the access-policy configured on DNAC traffic will be allowed else dropped. (Micro-segmentation)
16. Return traffic will follow the same procedure.

SDA Packet Flow: Endpoints belong to different subnet & subnet behind known Border Node



SDA Packet Flow

Endpoints belong to different subnet & subnet behind known Border Node

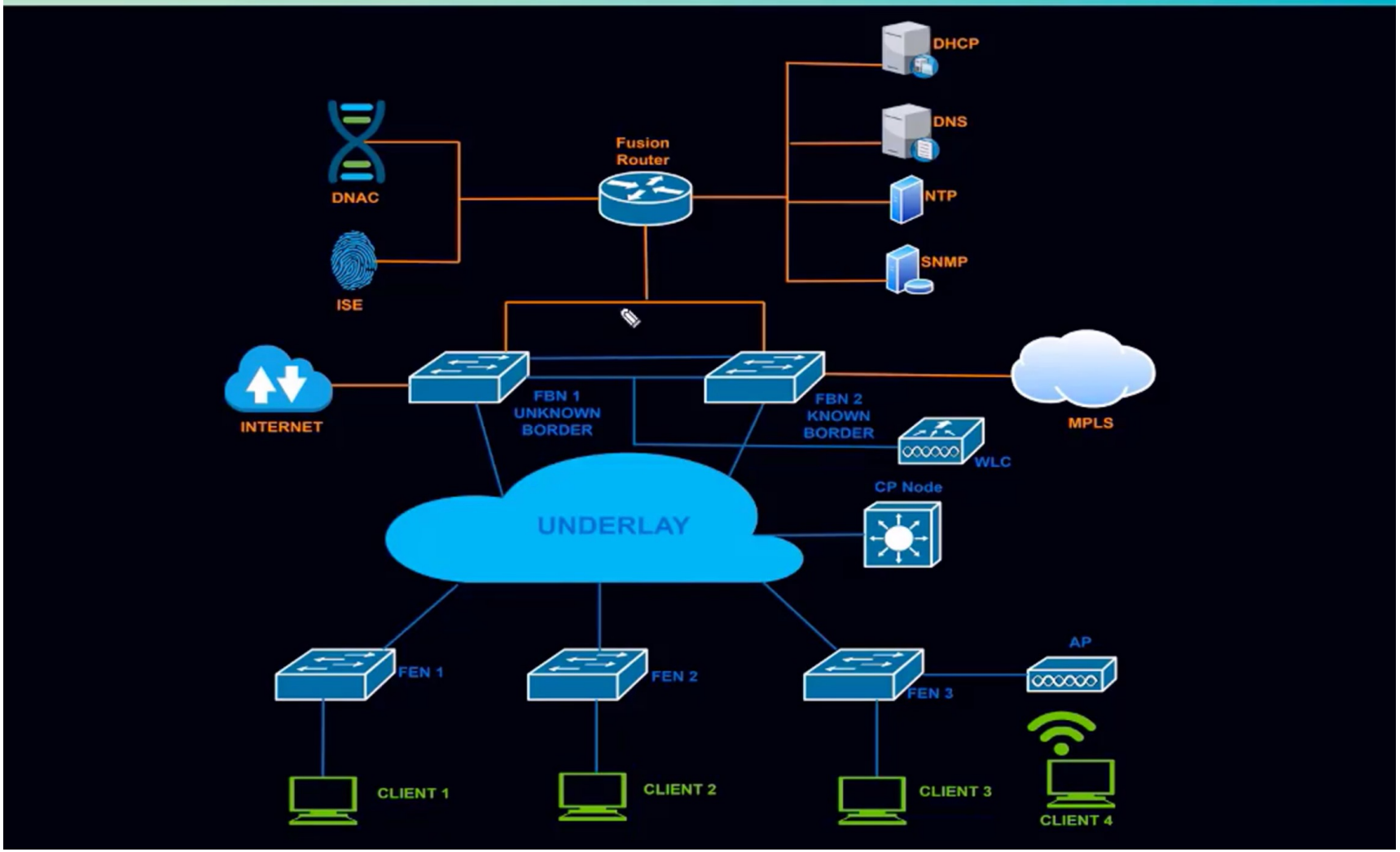
Source IP	Destination IP
Client1(10.10.10.10)	Clinet3(10.10.20.10)

1. Clinet1(10.10.10.10) and Clinet3(10.10.20.10) are in different subnet.
2. Clinet1(10.10.10.10) will send the ARP request for DGW(Anycast Gateway), which is local on FEN1.
3. Clinet1(10.10.10.10) send packet towards FEN1 which is for destination Clinet3(10.10.20.10).
4. FEN1 check its local-cache for EID-to-RLOC entry for Clinet3(10.10.20.10).
5. FEN1 send MAP-Request to CPNode for location (RLOC) of Clinet3(10.10.20.10).
6. CPNode replies with MAP-Reply to FEN1(192.168.1.1) with RLOC for Clinet3(10.10.20.10) which is FEN3(192.168.1.3).
7. FEN1(192.168.1.1) encapsulate the packet using VXLAN, which has Source RLOC FEN1(192.168.1.1), Destination RLOC FEN3(192.168.1.3) and VXLAN header that has VNID & SGT tags.

Destination IP	VXLAN Header		Source IP	Destination IP
RLOC FEN3(192.168.1.3)	VNID	SGT	Client1(10.10.10.10)	Clinet3(10.10.20.10)

8. FEN1(192.168.1.1) send this VXLAN encapsulated packet towards the SDA fabric which is for RLOC destination FEN3(192.168.1.3).
9. Inside Fabric, underlay devices will route the VXLAN packet, based on destination RLOC FEN3(192.168.1.3).
10. VXLAN encapsulated packet received at FEN3(192.168.1.3), FEN3(192.168.1.3) deencapsulate the packet, remove the VXLAN header and inspect the SGT and VNID and Client1(10.10.10.10) IP address.
11. If VNID is same for Client1(10.10.10.10) and Clinet3(10.10.20.10) traffic accepted. Else, traffic dropped. (Macro-segmentation)
12. Now SGT checked , if communication between SGT is allowed as per the access-policy configured on DNAC traffic will be allowed else dropped. (Micro-segmentation)
13. Return traffic will follow the same procedure.

SDA Packet Flow: Endpoint communication with unknown destination / Border Node



SDA Packet Flow

Endpoint communication with unknown destination / Border Node

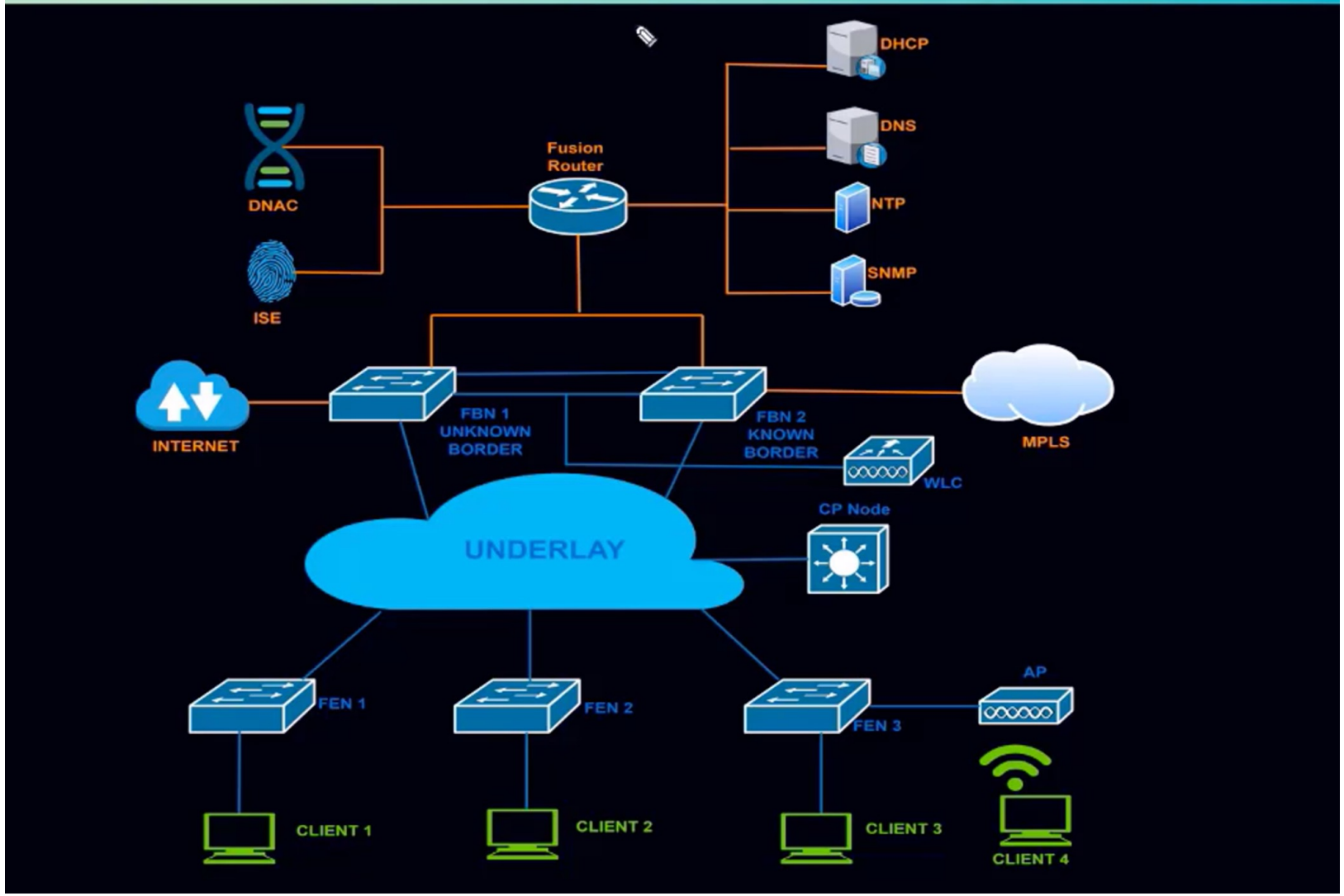
1. Clinet1(10.10.10.10) wants to communicate with 4.4.4.4/32.
2. Clinet1(10.10.10.10) will send the ARP request for DGW(anycast gateway), which is local on FEN1.
3. Clinet1(10.10.10.10) send packet towards FEN1 which is for destination 4.4.4.4 .
4. FEN1 check its local-cache for EID-to-RLOC entry for 4.4.4.4 .
5. FEN1 send MAP-Request to CPNode for location (RLOC) of 4.4.4.4 (unknown destination).
6. CPNode replies with negative map-reply (NMR) to FEN1(192.168.1.1) .
7. CPNode tells FEN1(192.168.1.1) to send the traffic to external border router/unknown border node (192.168.1.6) for 4.4.4.4 (unknown destination).
8. FEN1(192.168.1.1) encapsulate the packet using VXLAN, which has Source RLOC FEN1(192.168.1.1), Destination RLOC unknown FBN (192.168.1.6).

Source IP	Destination IP
Client1(10.10.10.10)	4.4.4.4

Source IP	Destination IP	VXLAN Header		Source IP	Destination IP
RLOC FEN1(192.168.1.1)	RLOC UNKNOWN FBN(192.168.1.6)	VNID	SGT	Client1(10.10.10.10)	4.4.4.4

9. FEN1(192.168.1.1) send this VXLAN encapsulated packet towards the SDA fabric which is for RLOC destination unknown FBN (192.168.1.6).
10. Inside Fabric, underlay devices will route the VXLAN packet, based on destination RLOC unknown FBN (192.168.1.6).
11. VXLAN encapsulated packet received at unknown FBN (192.168.1.6), FBN (192.168.1.6) deencapsulate the packet, remove the VXLAN header.
12. Deencapsulated packet is sent externally towards to internet (towards destination 4.4.4.4)
13. Return traffic will follow the same procedure.

SDA Packet Flow: Endpoint Communication with shared subnets



SDA Packet Flow

Endpoint Communication with shared subnets behind Fusion routers

1. DHCP/DNS/NTP/SNMP/ISE are part of shared subnet.
2. Every host should be able to communicate with these subnets.
3. Shared subnets are hosted behind Fusion Router.
4. Fusion Router Used if we want communication between different VN.
5. Fusion Router let all VN use shared services.
6. Manual config is done on FR no auto-config from DNAC as its not part of SDA fabric.
7. Fusion Router Behaves like a Router on a stick.
8. Fusion Router runs ebgp/ibgp with FBN and igp/bgp with shared services.
9. Fusion Router shares/redistribute shared subnet with FBN.
10. Clients need access to DHCP to get IP address, DNS for name to IP resolution, NTP for time sync, SNMP for monitoring, ISE for authentication & authorization.

1. When Client1(10.10.10.10) wants to communicate with any IP of shared services it forms VXLAN tunnel with known FBN.
2. FEN sends encapsulated packet towards known FBN.
3. FBN decapsulates the packet and as per VNID tagging place the packet in appropriate VRF and send it towards Fusion router.
4. Fusin Router use the concept of route leaking and let Client1(10.10.10.10) communicate with shared services (either in GRT or specific VRF).
5. Return traffic will follow the same procedure.

Link เพิ่มเติม

- https://www.ablenet.co.th/2023/05/02/cisco_dnac/
- https://www.ablenet.co.th/2023/06/17/overlay_underlay_network/
- https://www.ablenet.co.th/2024/08/03/vxlan-cisco-nexus/
- https://www.ablenet.co.th/2024/10/01/vpc-component/
- https://th.opticomfiber.com/info/what-is-nvgre-and-vxlan-52922555.html
- Link Video ที่ควรดู
  - https://www.youtube.com/watch?v=MGfuDIXq4sY&ab_channel=ChaiwatAmornhirunwong
  - https://www.youtube.com/watch?v=quHP4gGl95A&ab_channel=ChaiwatAmornhirunwong
  - https://www.youtube.com/watch?v=QDC_5yAkTRM&ab_channel=UniNet
  - https://www.youtube.com/watch?v=_7Ts0M7P2PU&t=1s&ab_channel=UniNet