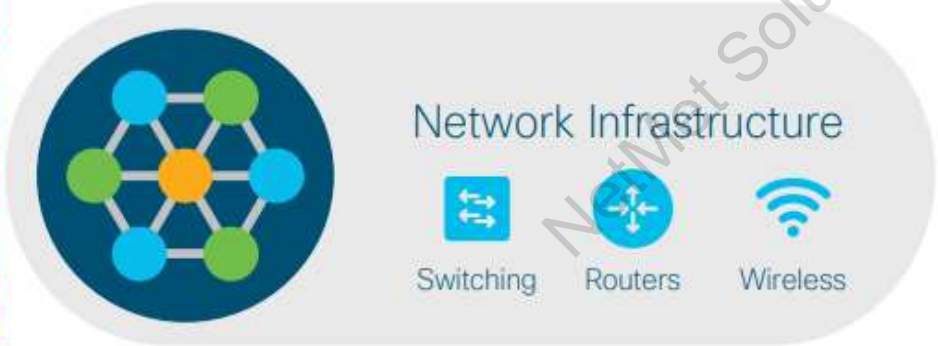
NetMet Solutions
Your Trusted Learning Partner

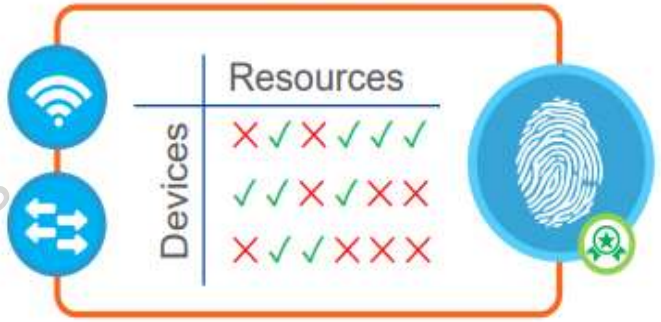
Introduction to DNA Center

Traditional Networking Challenges

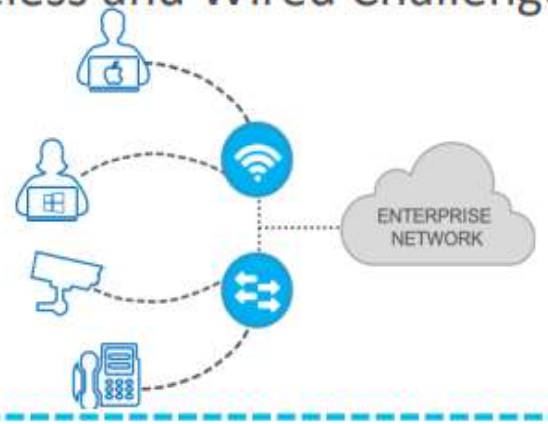
Network Deployment Challenges



Network Security Challenges



Wireless and Wired Challenges

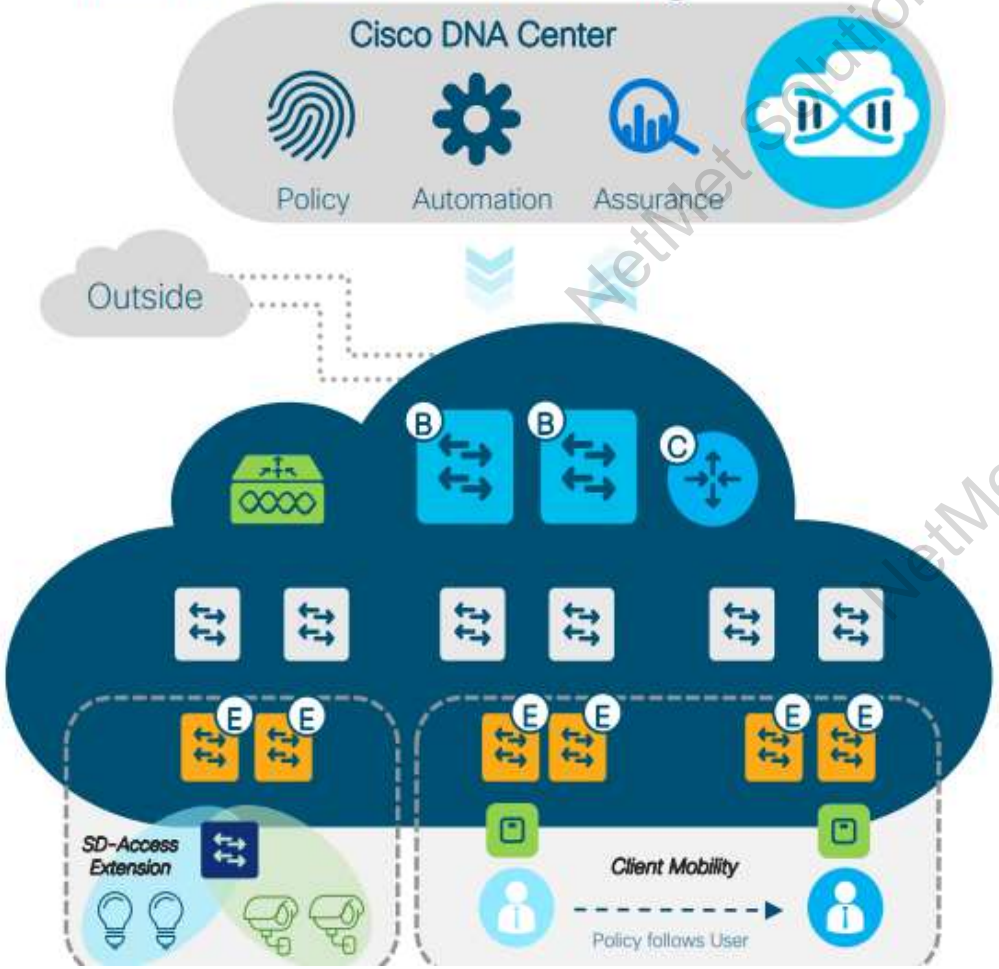


Network Operations Challenges

NetMet Solutions
Your Trusted Learning Partner

Cisco Software-Defined Access

Intent-Based Networking



One Automated Network Fabric

Single fabric for wired and wireless with full automation

Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

AI-Driven Insights and Telemetry

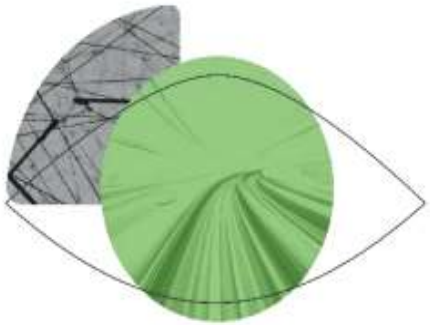
Analytics and visibility into user and application experience

NetMet Solutions
Your Trusted Learning Partner

Cisco Software-Defined Access

Zero Trust for the Workplace

Visibility



Grant the right level of network access to users and devices.

Segmentation

Shrink zones of trust and grant access based on least privilege.

Containment

Automate containment of infected endpoints and revoke network access.

Benefits of Cisco Software-Defined Access

Enhance Security and Compliance

Deliver Consistent Experience

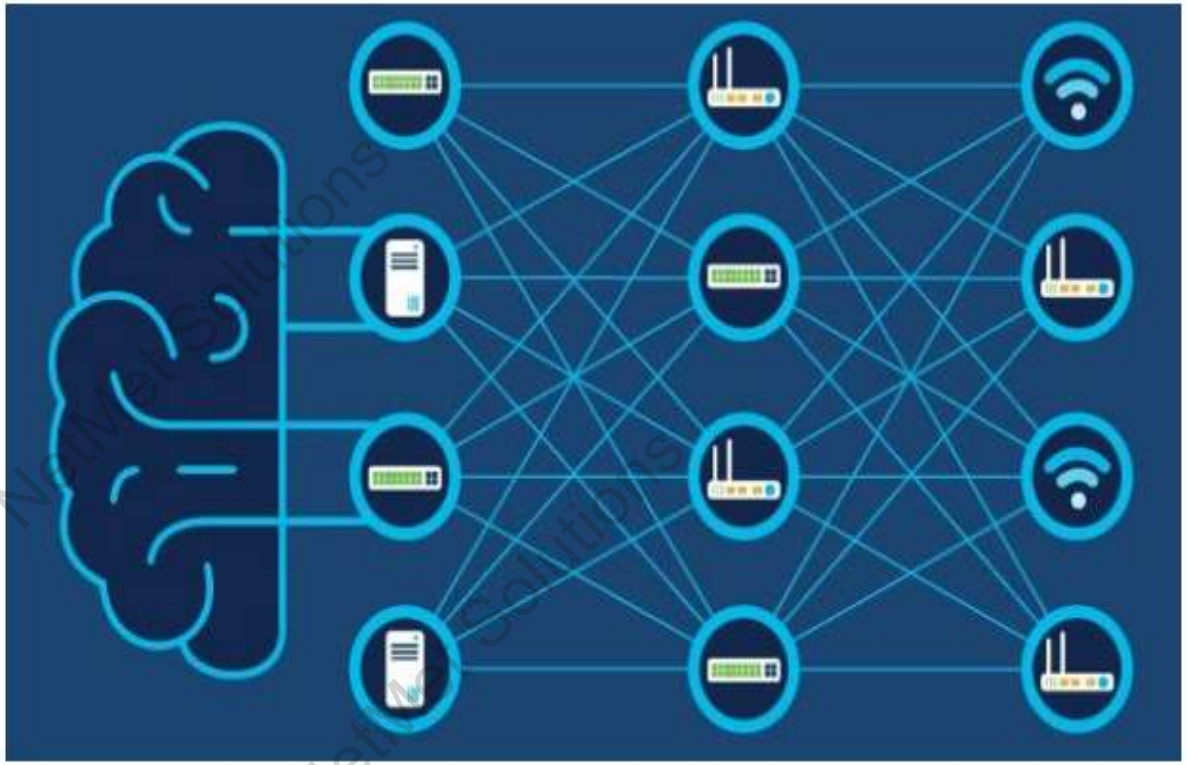
Boost Operational Effectiveness

Gain Network Insights

NetMet Solutions
Your Trusted Learning Partner

What is a Network Fabric?

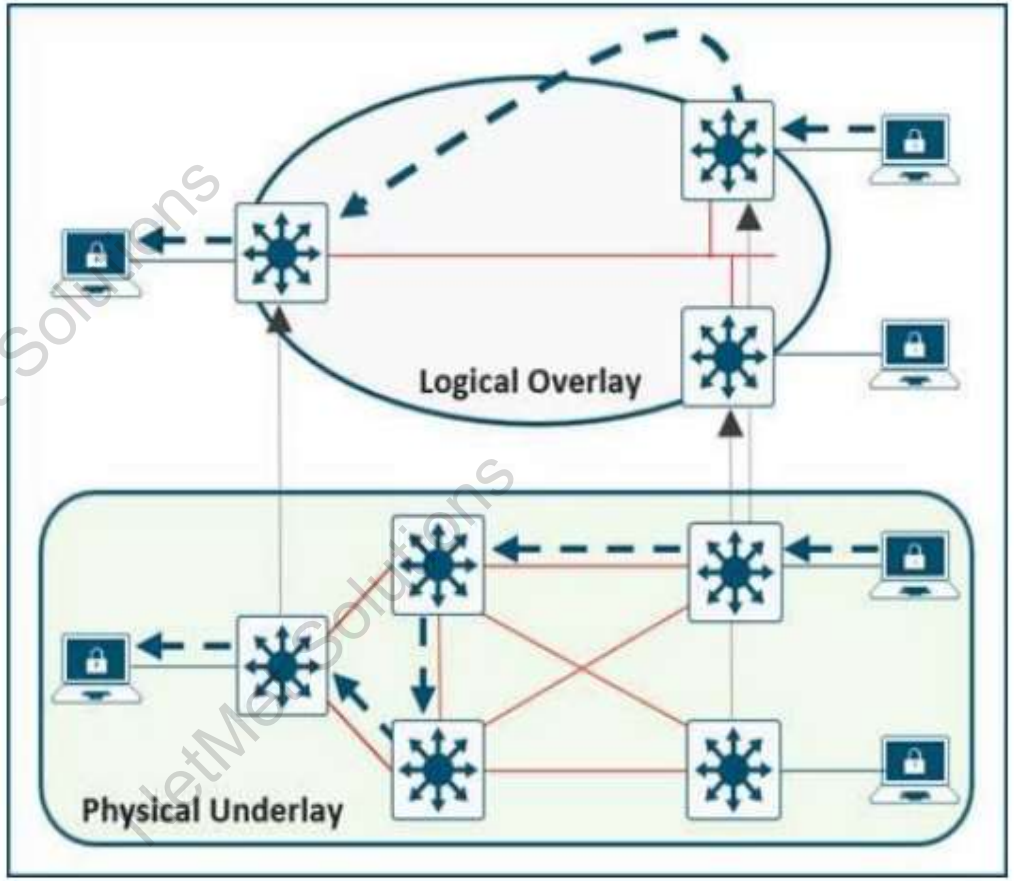
- Mesh of connections between network devices.
- Transports data from source to destination.
- Usually refers to a virtualized, automated lattice of overlay connections.
- May (uncommonly) refer to physical wiring of a network .



NetMet Solutions
Your Trusted Learning Partner

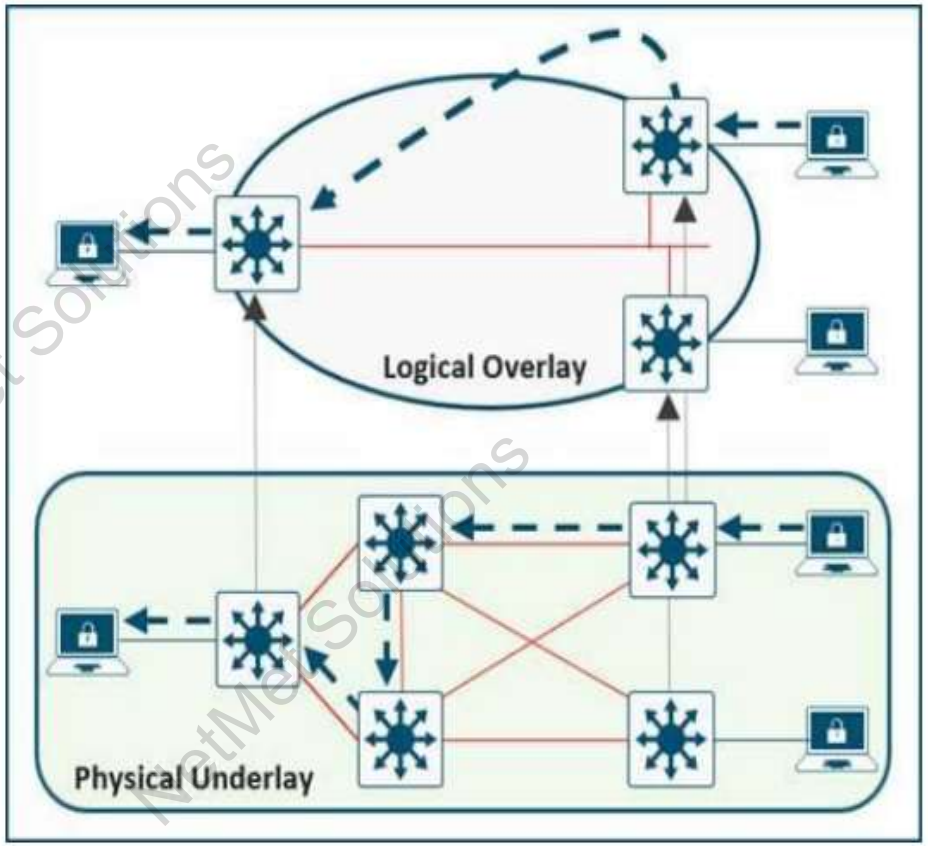
What is an Overlay?

- An Overlay network is a logical topology used to virtually connect devices, built over an arbitrary physical Underlay topology.
- Examples of overlay technologies:
  - GRE
  - MPLS
  - IPsec
  - CAPWAP
  - LISP
  - VXLAN
  - BGP EVPN
  - SD-WAN
  - ACI
  - OTV



Why an Overlay?

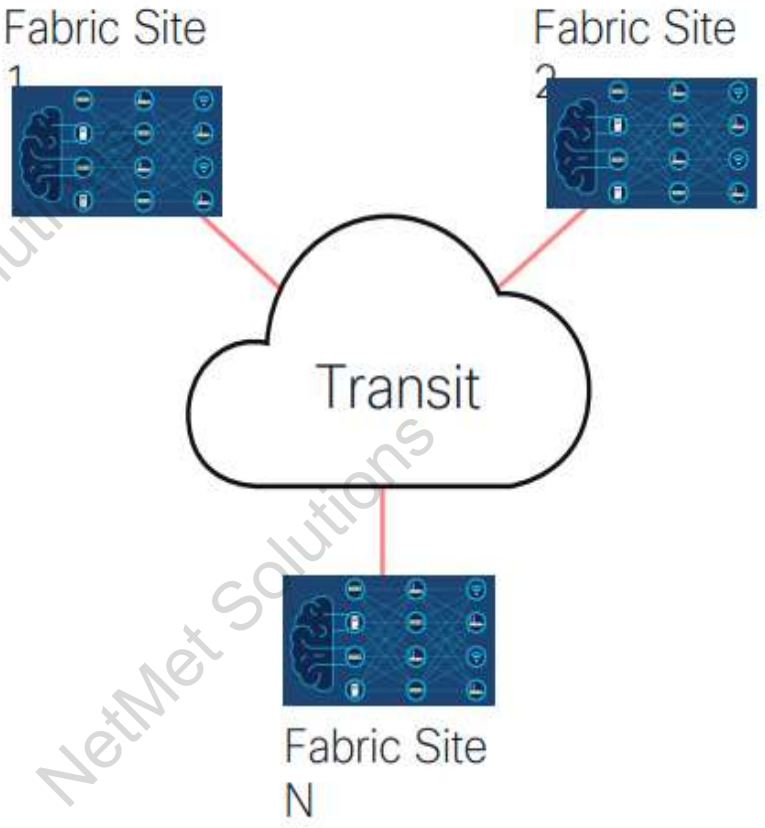
- Services - deliver using overlay.
- Mobility - map endpoints to edges.
- Scalability - reduce protocol state.
- Underlay is simple and manageable.
- Flexible and programmable.
- Maximize network reliability.



NetMet Solutions
Your Trusted Learning Partner

What is Fabric Site?

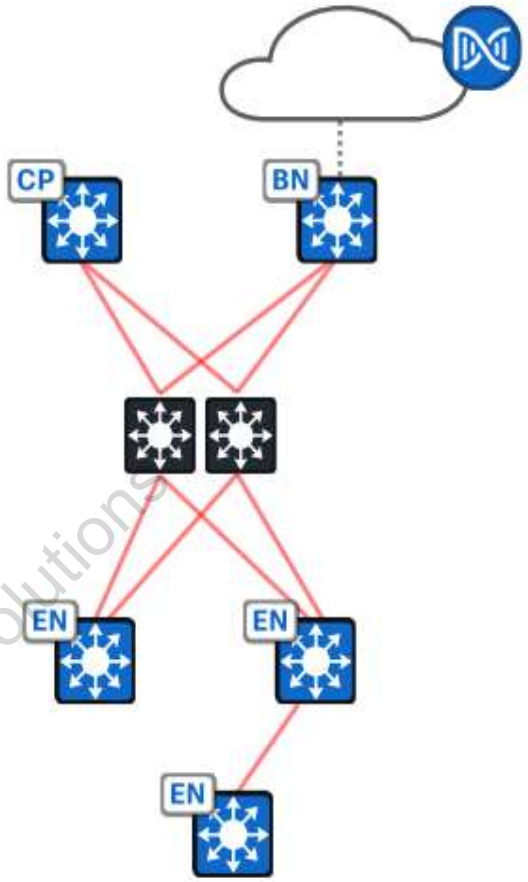
- An instance of an SD-Access Fabric.
- Typically defined by disparate geographical locations, but not always.
- Can also be defined by:
  - Endpoint scale.
  - Failure domain scoping.
  - RTT.
  - Underlay connectivity attributes.
- Typically interconnected by a “Transit”.



Cisco SD-Access Roles

Mandatory Components

- **Cisco DNA Center** – GUI and APIs for intent-based automation of wired and wireless fabric devices.
- **Fabric Border Nodes** – A fabric device that connects external L3 and L2 networks to the Cisco SD-Access fabric.
- **Edge Nodes** – A fabric device that connects wired endpoints to the Cisco SD-Access fabric and optionally enforces micro-segmentation policy.
- **Control Plane Node** – Map System that tracks endpoint to fabric node relationships.

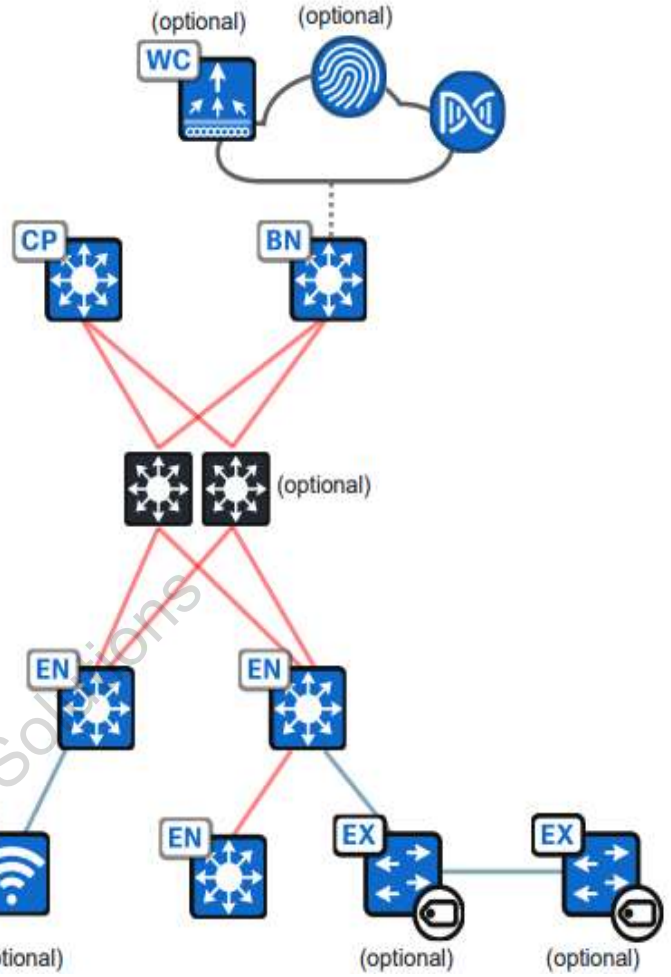


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Roles

Optional Components

- **Identity Services Engine** – Highly recommended. NAC and ID services for dynamic endpoint to Security Group Tag mapping and policy distribution.
- **Fabric Wireless Controller** and **Fabric APs** – Highly recommended. Connects wireless endpoints to the SD-Access fabric.
- **Extended Node** – A switch operating at Layer 2 that extends fabric connectivity and optionally enforces micro-segmentation policy.
- **Intermediate Nodes** – Moves data between fabric nodes. Can be one or many hops.



Cisco SD-Access Roles

Some of the Supported Colocations

Border Node and Control Plane Node.

Border Node, Control Plane Node, and Fabric Edge Node.

Border Node, Control Plane Node, and Embedded Wireless Controller.

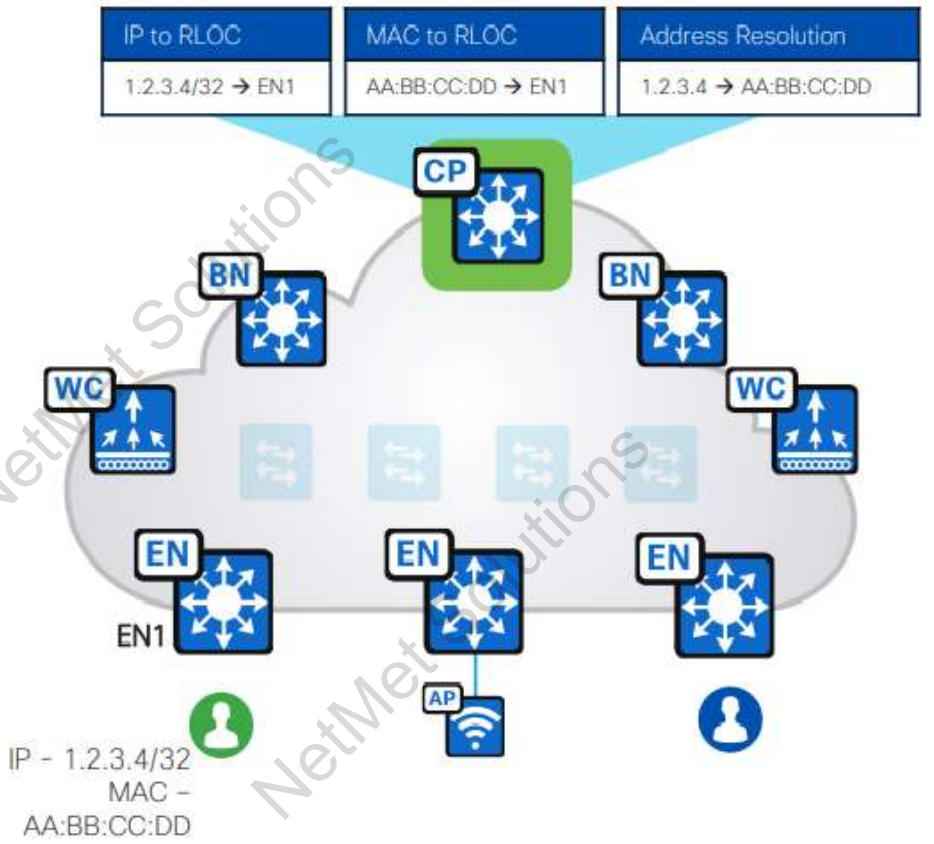
Border Node, Control Plane Node, Fabric Edge Node, and Embedded Wireless Controller.

NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Control Plane Node Maintains a Host Tracking Database to Map Location Information

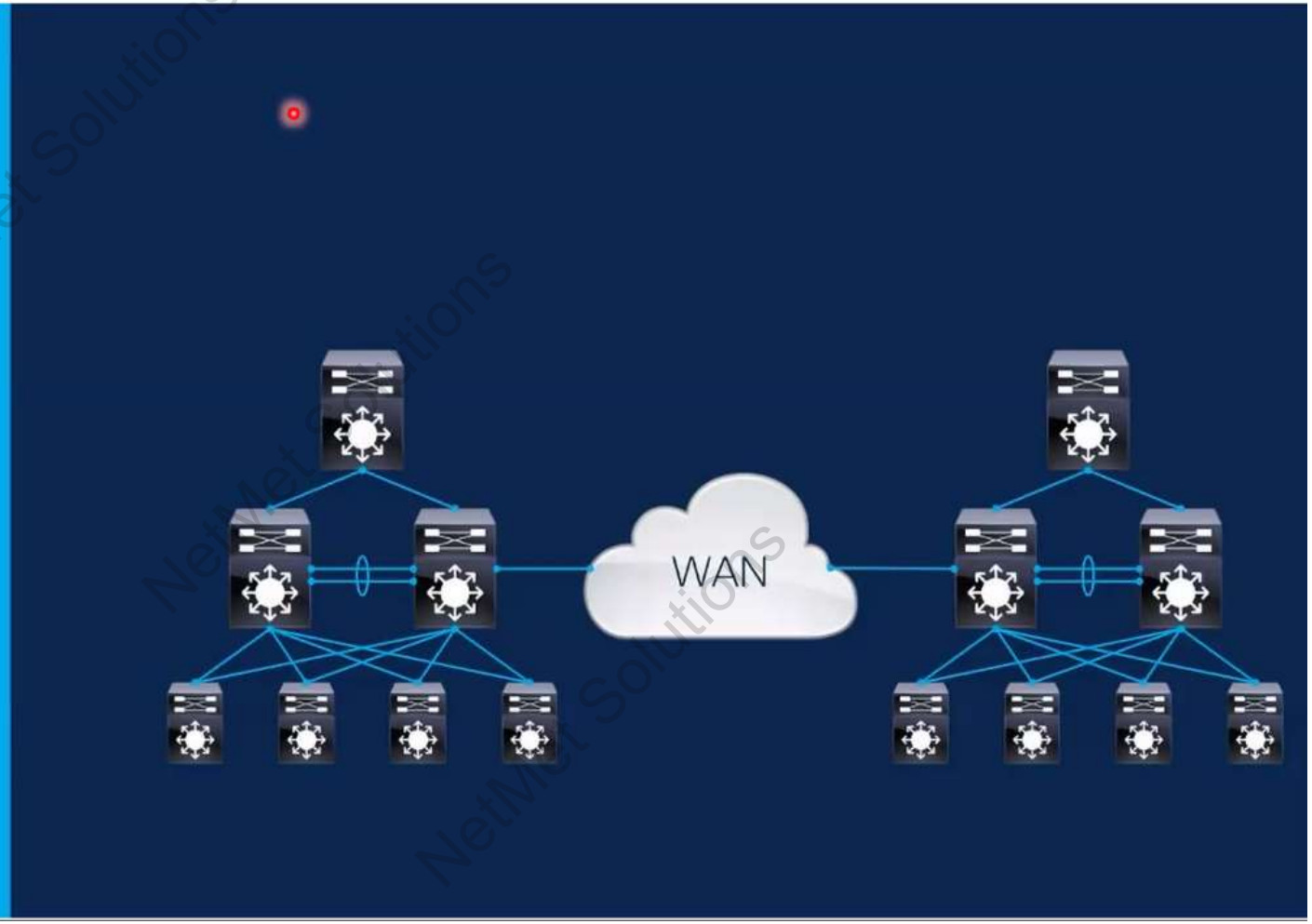
- A simple Host Database that maps Endpoint IDs to locations, along with other attributes.
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC).
- Receives Endpoint ID map registrations from Edge Nodes, Border Nodes and Fabric Wireless LAN Controllers.
- Resolves lookup requests from Edge Nodes and Border Nodes, to locate destination Endpoint IDs.
- Publishes registrations to Subscribers (Border Nodes).



NetMet Solutions
Your Trusted Learning Partner

Traditional Networks

- Hardware Centric
- Manual
- Fragmented in Their Security
- Focused on Network Data

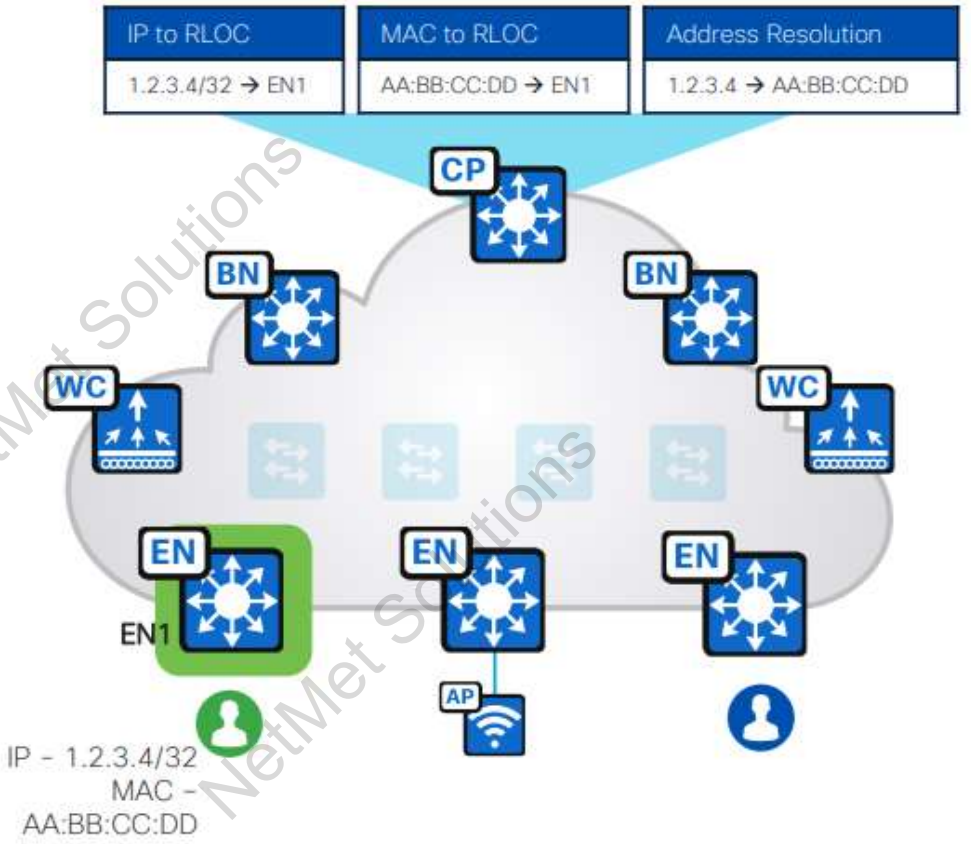


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Edge Node Provides First Hop Services for Endpoints

- Responsible for Authenticating and Authorizing endpoints (e.g. 802.1X, MAB, static) in concert with ISE.
- Register Endpoint IDs (IPv4, IPv6, MAC) with the Control Plane Nodes.
- Provide an Anycast Gateway for the connected wired and wireless endpoints.
- Performs VXLAN encapsulation and decapsulation of traffic to and from all connected wired endpoints.

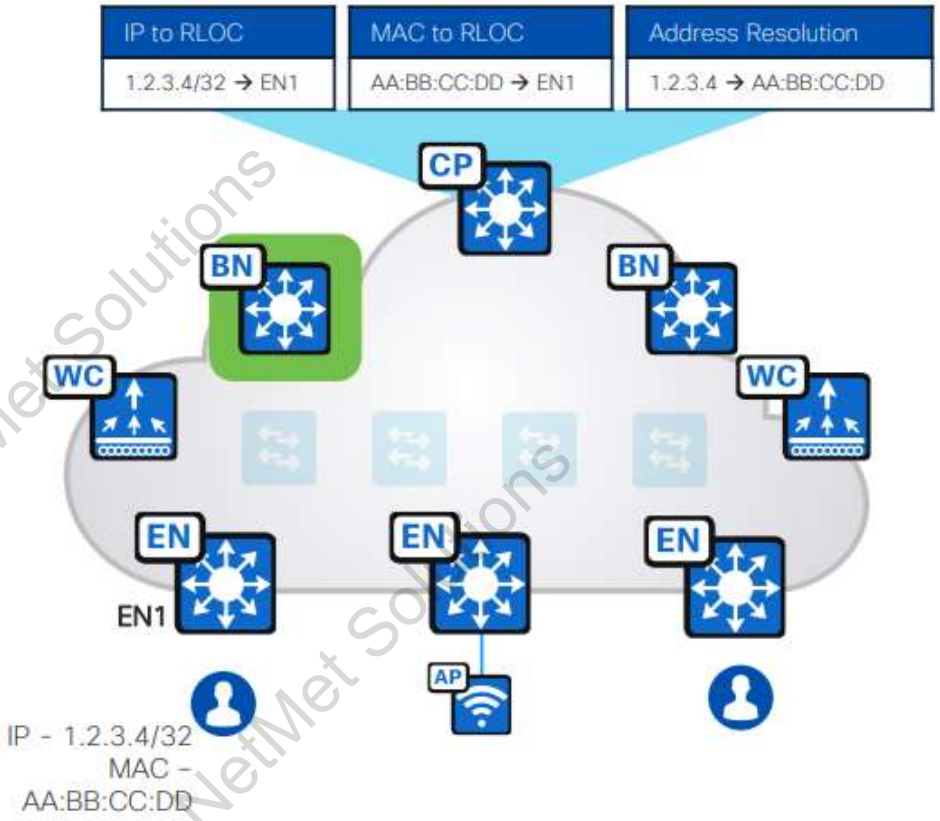


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

- Subscribes to LISP Control Plane Node IPv4 and IPv6 Tables.
- There are 4 types of Border Node:
  - External Border Node.
  - Internal Border Node.
  - Internal + External Border Node.
  - Layer 2 Border Node.

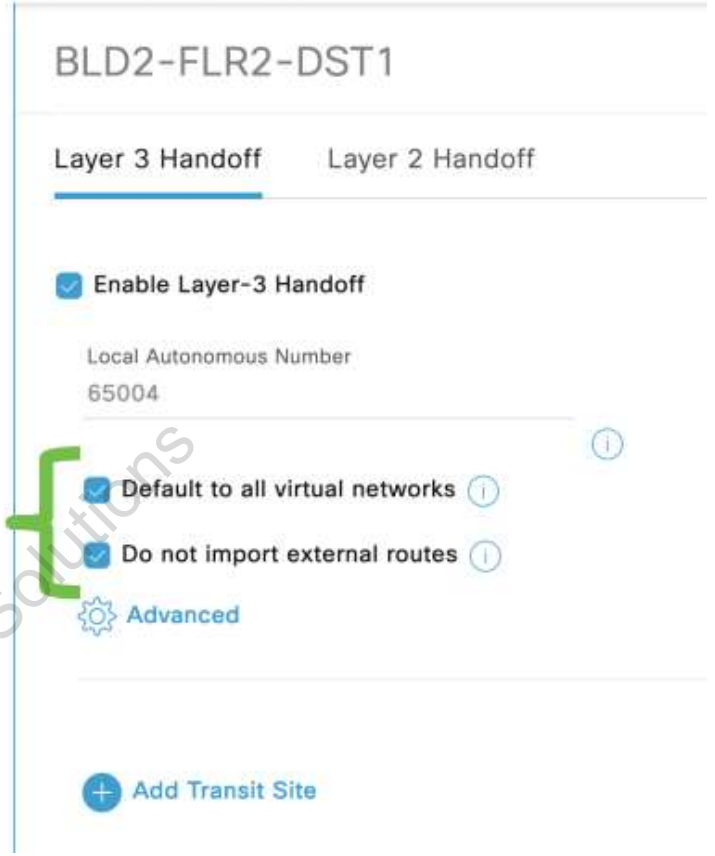


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

- External Border Node:
  - The most common configuration.
  - Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
  - Does not register IP prefixes from outside the Fabric Site into the fabric Control Plane.
  - Acts as a gateway of last resort for the Fabric Site.

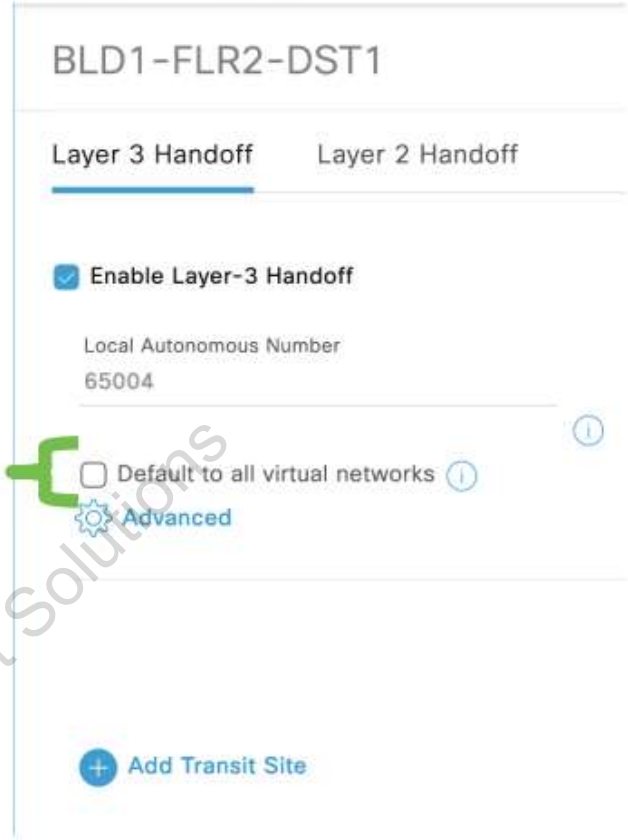


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

- Internal Border Node:
  - Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
  - Imports and registers eBGP-learned IPv4/IPv6 prefixes from outside the Fabric Site, into the fabric Control Plane.
  - Does not act as a gateway of last resort for the Fabric Site.

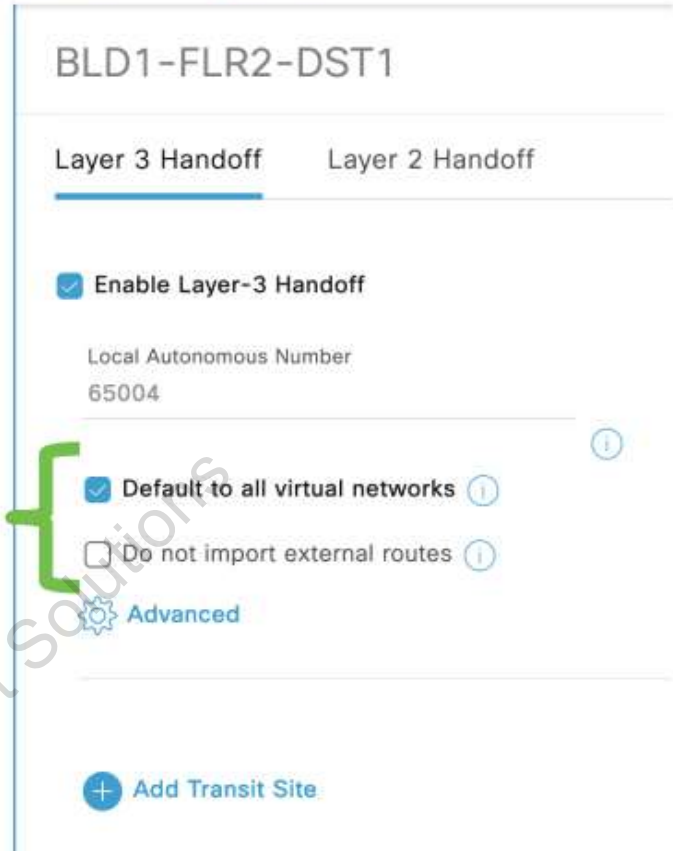


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

- Internal + External Border Node:
  - Exports all fabric subnets to outside the Fabric Site as eBGP summary routes.
  - Imports and registers eBGP-learned IPv4/IPv6 prefixes from outside the Fabric Site, into the fabric Control Plane.
  - Acts as a gateway of last resort for the Fabric Site.



NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Border Node is the Fabric Site Entry and Exit for Network Traffic

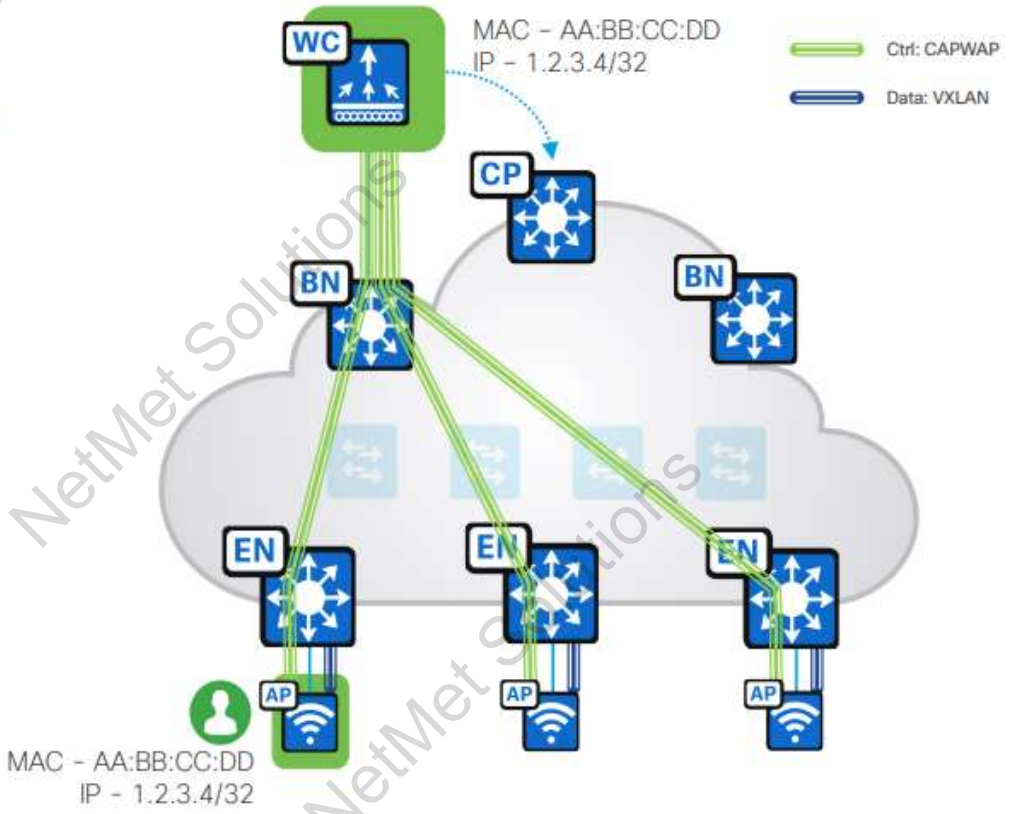
- **Layer 2 Border Node**:
  - Acts as Layer 2 handoff for pure Layer 2 Overlays or Layer 2 + Layer 3 Overlays.
  - Allows VLAN translation between SD-Access network segments and non-fabric VLAN IDs.
  - Dual homing requires link aggregation; STP it not tunneled within the SD-Access Fabric.
  - Ideally should be separate device from the Layer 3 Border Node.

NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Fabric Enabled Wireless Unifies Wired and Wireless Management, Policy and Data Planes

- Fabric WLC accessible though a Fabric Border Node (Underlay). Can be several hops away.
- Fabric Enabled APs reside in a dedicated IP range and communicate with the WLC (CAPWAP Control).
- Fabric WLC registers endpoints with the Control Plane Node.
- Fabric APs switch endpoint traffic to the adjacent Edge Node.
- Wireless endpoints use same data plane and policy plane as wired endpoints.

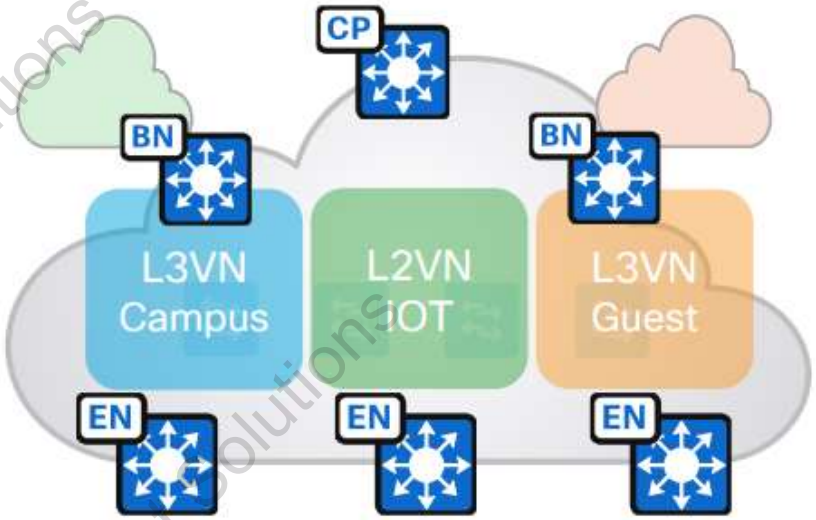


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Virtual Networks

- Layer 3 Virtual Networks use VRFs and LISP Instance IDs to maintain separate routing topologies.
  - Endpoint IDs (IPv4/IPv6 addresses) are routed within an L3VN.
- Layer 2 Virtual Networks use LISP Instance IDs and VLANs to maintain separate switching topologies.
  - Endpoint IDs (MAC addresses) are switched within an L2VN.
- Edge Nodes, Border Nodes and Fabric APs add a VNID (the LISP IID) to the fabric encapsulation.

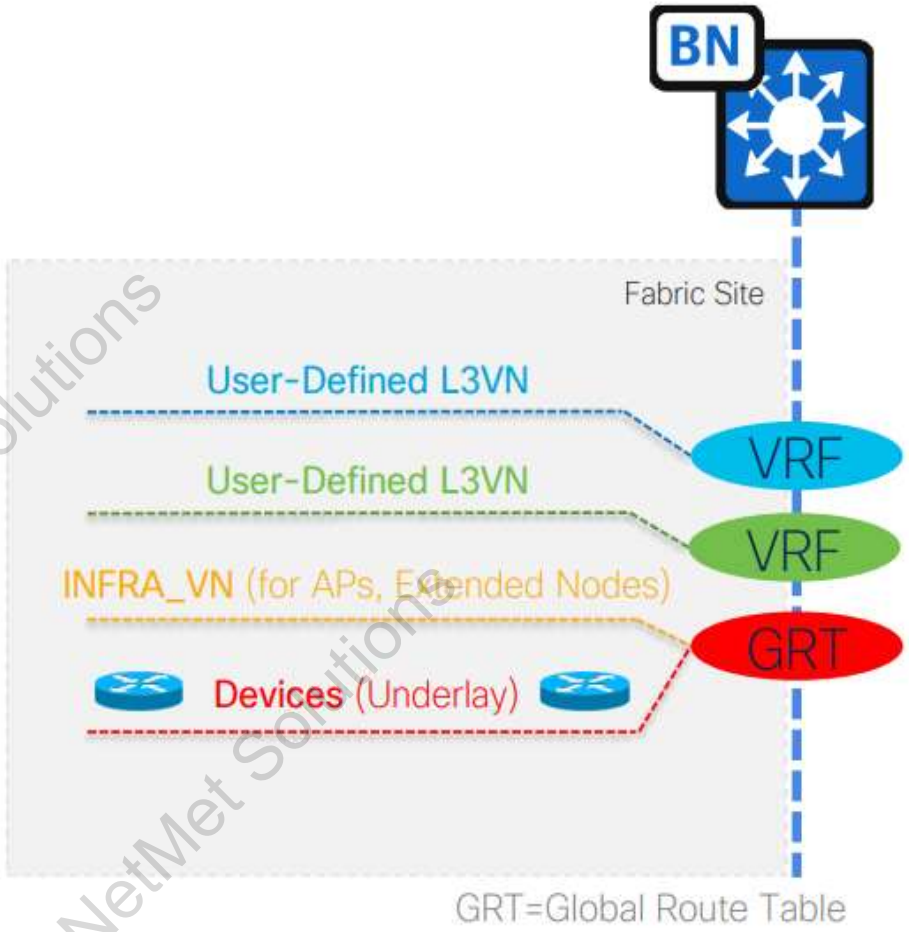


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Layer 3 Virtual Networks

- **Fabric Devices (Underlay)** connectivity is in the Global Routing Table.
- INFRA_VN is only for Fabric Access Points and Extended Nodes in the Global Routing Table.
- User-Defined VNs can be added or removed on demand.
- DEFAULT_VN is the same as a user-defined VN. Present in the SD-Access UI by default. Not deployed to the Fabric Site by default.

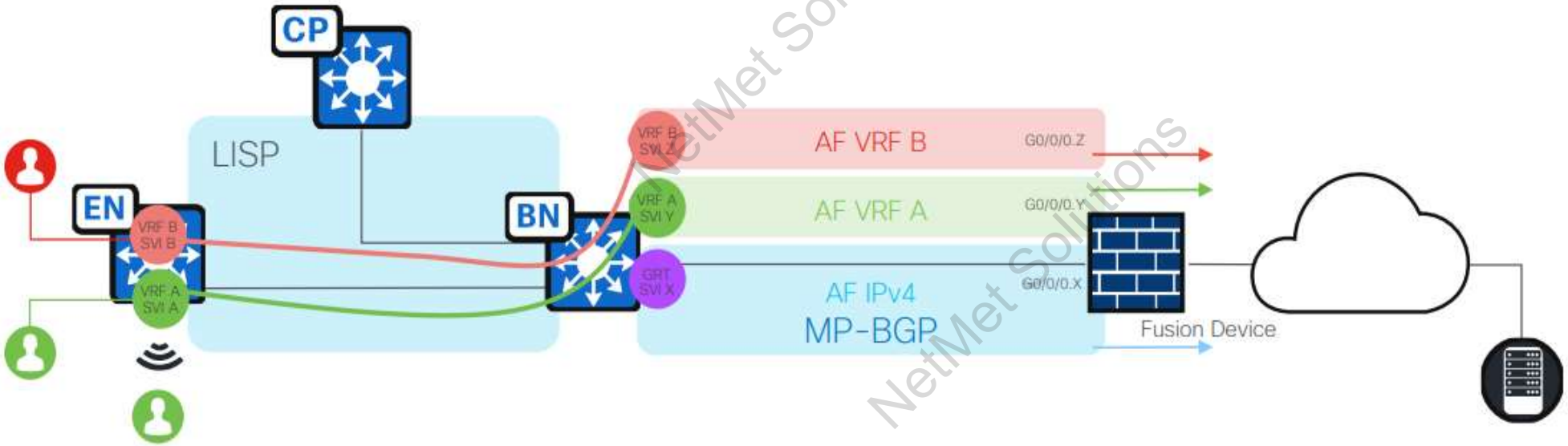


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Per-Layer-3-Virtual-Network Layer 3 Handoff

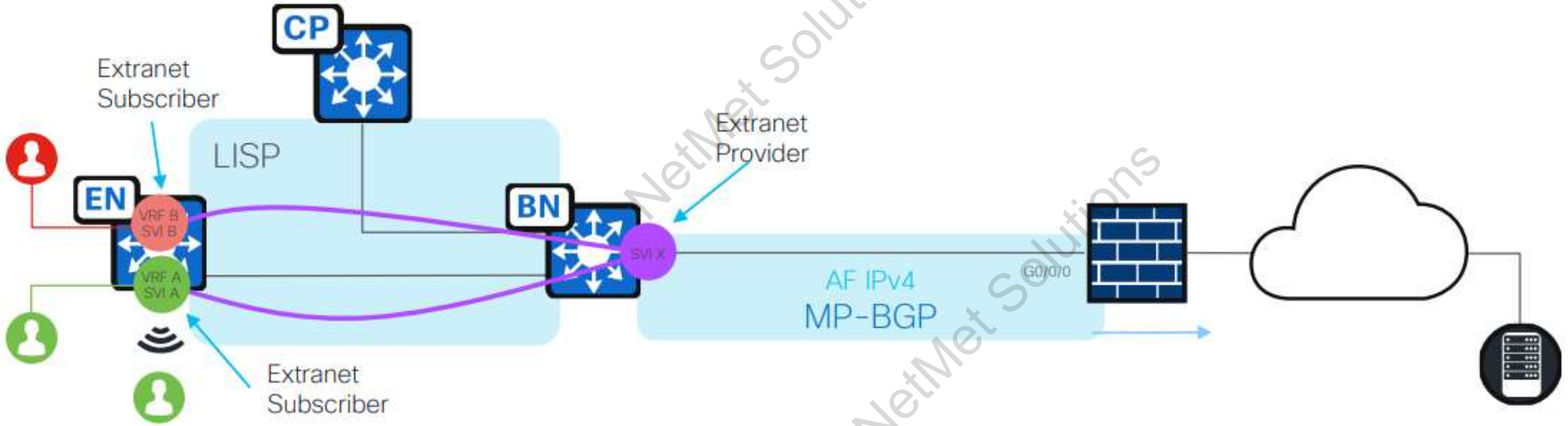
- Use a "Fusion Device" to leak external routes into SD-Access Layer 3 Virtual Networks.
- Alternatively, maintain VRF segmentation outside of the SD-Access Fabric with a VRF-aware external routing domain.
- Fusion Device is outside the fabric. Can be any platform (router, Layer 3 switch, firewall, etc.) with appropriate capabilities.



Cisco SD-Access Fabric

Extranet Provider Virtual Network Layer 3 Handoff

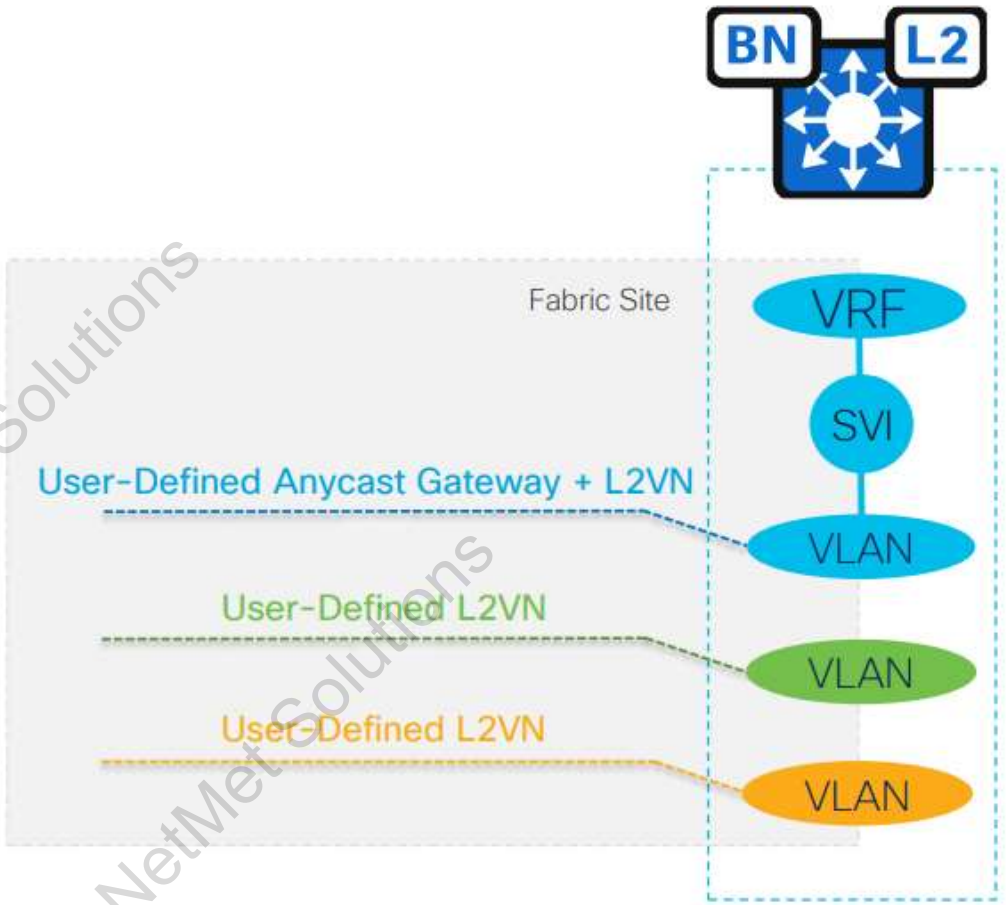
- Use an Extranet Policy to allow communication between one Provider Virtual Network and one or more Subscriber Virtual Networks.
- Extranet Policy is roadmap for SD-Access 2.3.5.0 ETA ~Q2CY23. Requires LISP Pub/Sub Control Plane. Please read the release collateral for details of functionality and design considerations.



Cisco SD-Access Fabric

Layer 2 Handoff

- Ancient wisdom: Route whenever you can, switch when you must.
- Layer 2 Virtual Networks handoff through a user-defined VLAN.
- Layer 2 Virtual Networks may implement BUM flooding. Important to be mindful of loop prevention.

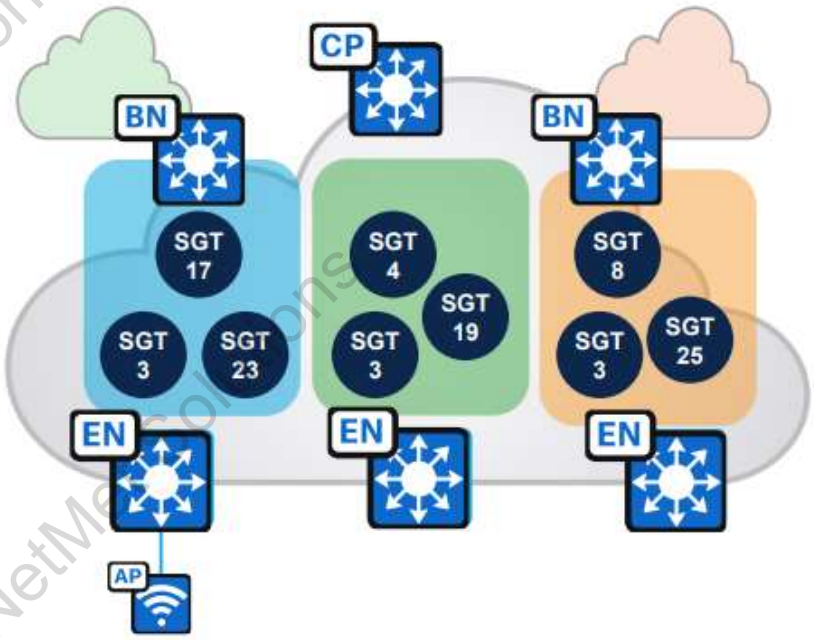


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

A Security Group Tag Assigns a "Group" to Each Endpoint

- Edge Nodes and Fabric APs assign a unique Scalable Group Tag (SGT) to each end endpoint in concert with ISE.
- Edge Nodes and Fabric APs add an SGT to the fabric encapsulation.
- SGTs are used to implement IP-address-independent traffic policies.
- SGTs can be extended to numerous other networking technologies e.g., Cisco Secure Firewall, Cisco SD-WAN, some third-party devices, etc.

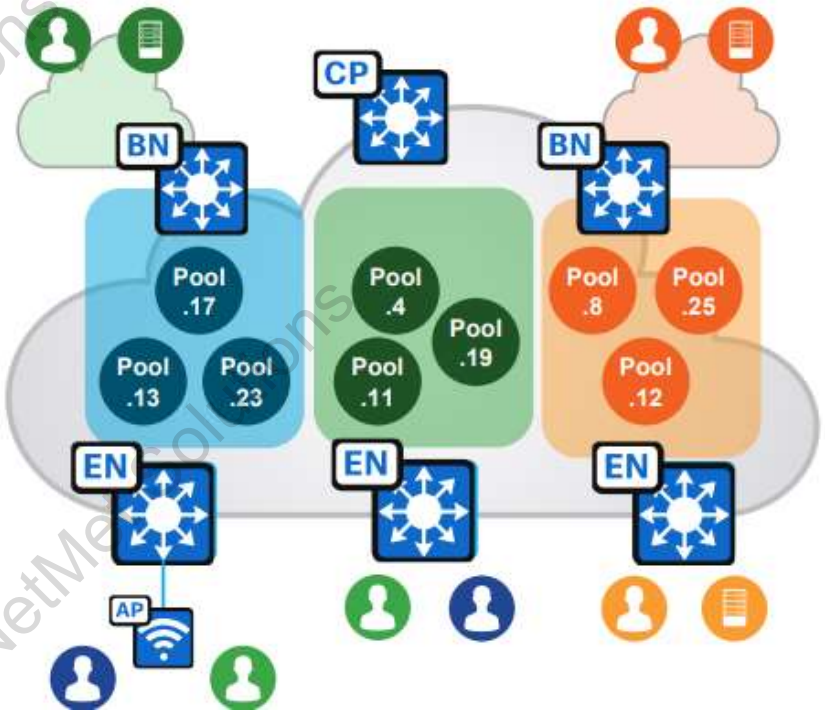


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Host Pools Provide a Default Gateway and Basic IP Services for Endpoints

- Edge Nodes instantiate an access VLAN and a Switched Virtual Interface (SVI) with user-defined IPv4/IPv6 addresses per Host Pool.
- Host Pools assigned to endpoints dynamically by AAA or statically per port.
- Edge Nodes and Fabric WLCs register endpoint IDs (/32, /128 or MAC) with the Control Plane, enabling IP mobility; any IP address anywhere.

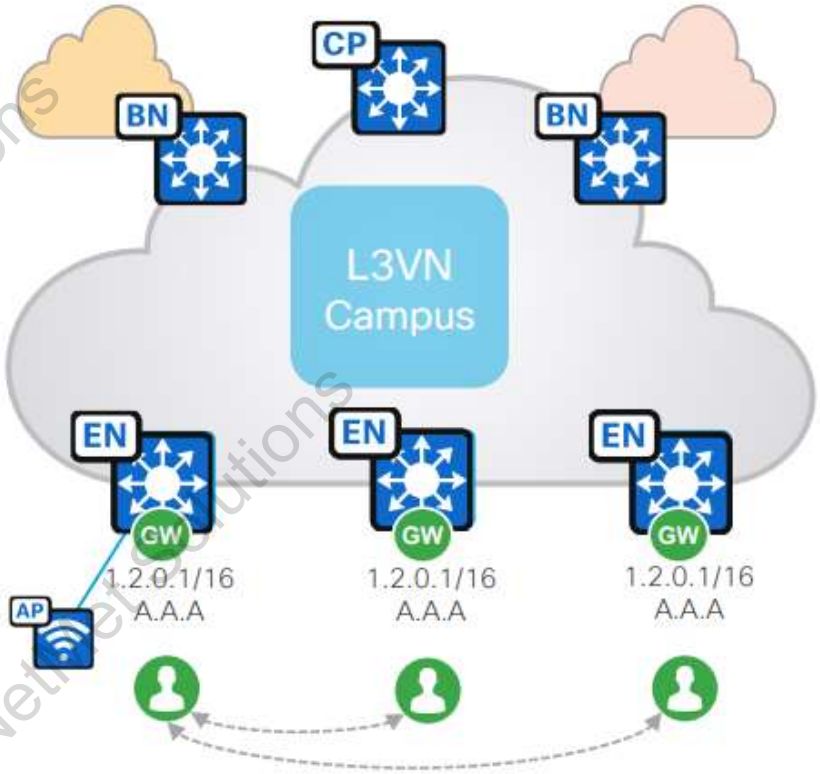


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Anycast Gateway Provides a Default Gateway for IP-Capable Endpoints

- Similar principle and behavior to FHRP with a shared virtual IPv4/IPv6 addresses and MAC address.
- The same Switch Virtual Interface (SVI) is present on all Edge Nodes with the same virtual IP and MAC.
- The wired or wireless endpoint can connect to any switch or AP in the fabric and communicate with the same Anycast Gateway.

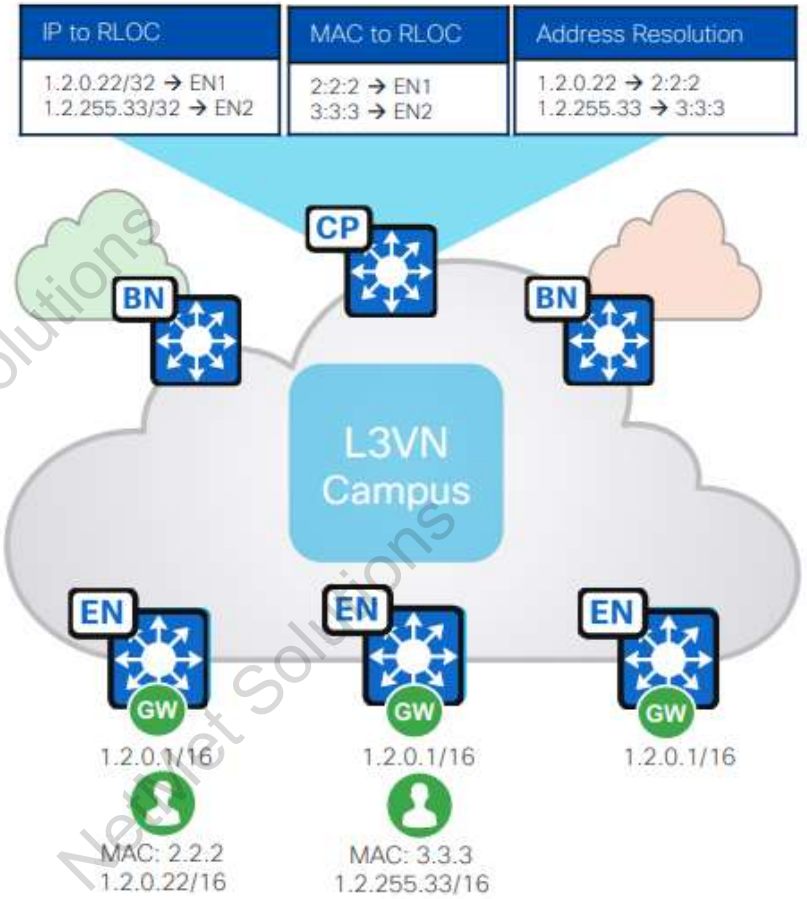


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Host Pools are "stretched" via the Overlay

- Endpoint IPv4/IPv6 traffic arrives on an Edge Node and is then routed or switched by the Edge Node.
- Fabric Dynamic EID mapping allows endpoint-specific (/32, /128, MAC) advertisement and mobility.
- No longer need VLANs to interconnect endpoints across Edge Nodes, this happens in the Overlay without broadcast flooding.

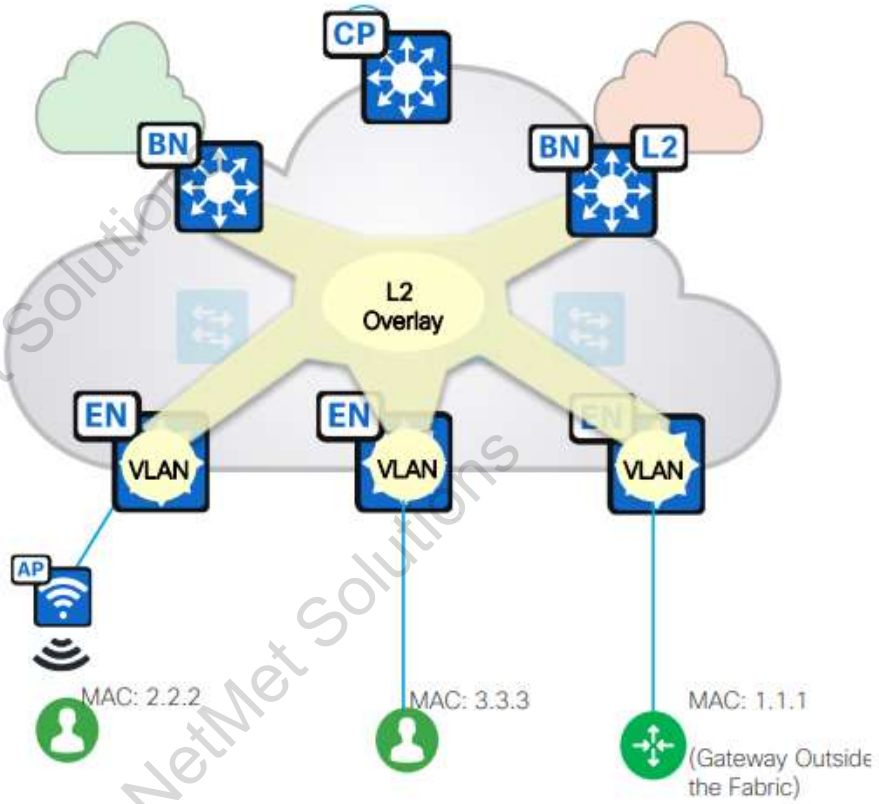


NetMet Solutions
Your Trusted Learning Partner

Cisco SD-Access Fabric

Layer 2 Virtual Networks

- By default, an L2VN is deployed with each Anycast Gateway and Layer 2 Flooding is disabled. Layer 2 Flooding can be enabled, if necessary, to service niche applications.
- L2VN can be deployed without an Anycast Gateway, and Layer 2 Flooding cannot be disabled.
  - Sometimes referred to as "Gateway Outside the Fabric".
- If Layer 2 Flooding is enabled, a Multicast Underlay P2MP tunnel is established between all Fabric Nodes.

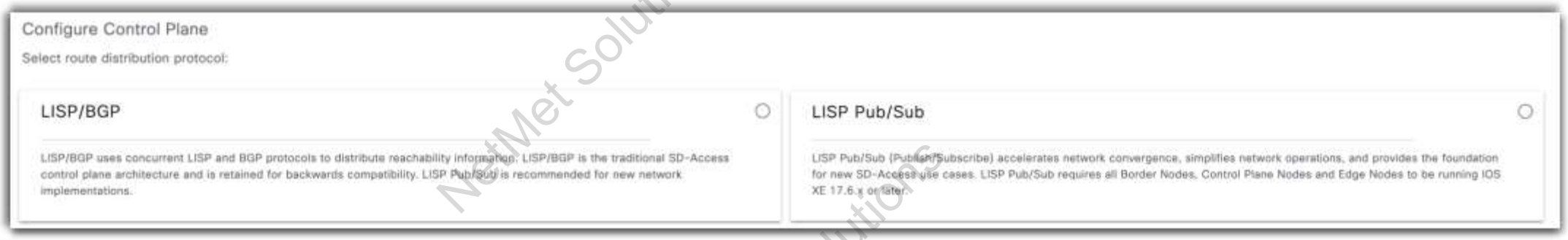


Cisco SD-Access Fabric

- Control Plane: LISP
  - Locator/ID Separation Protocol.
  - IETF Standards Track RFC9300-RFC9305 and Informational RFC9299.

Lightweight, Efficient, Scalable and Extensible

LISP in Cisco SD-Access



LISP/BGP

- Released circa 2017.
- Reliable and stable.
- BGP transport.

LISP Pub/Sub

- Released in 2022 with DNA Center 2.2.3.x.
- Reliable and stable.
- Native LISP transport.
- Less Control Plane load.
- Faster convergence.
- Highly extensible.

NetMet Solutions
Your Trusted Learning Partner

LISP Pub/Sub

A Brief Digression, before you ask...

- No plans to end support for LISP/BGP.
- LISP Pub/Sub is recommended for new deployments.
- In DNA Center 2.2.3.x new Fabric Sites can be configured as LISP/BGP or LISP Pub/Sub. Note minimum IOS XE versions.
- First phase of LISP/BGP to LISP Pub/Sub migration workflow is under development now.
  - Migrate IP-Based Transit Fabric Sites.
  - ETA CY2023.
- Second phase of LISP/BGP to LISP Pub/Sub under planning.
  - Migrate SD-Access Transit Fabric Sites.
- Official release collateral will explain functionality.

NetMet Solutions
Your Trusted Learning Partner

Advantages of LISP

- Optimised resource usage on Edge Nodes:
  - "Pull" only the information needed, like DNS. By comparison BGP pushes all routing information to all Edge Nodes.
- Underlay network is simple and stable:
  - IGP routing from Border Node to Edge Node. Maybe PIM. **No L2, no VLANs, no link bundling, no STP, no MPLS.**
- Unified wired and wireless data plane and policy plane.
  - No wireless concentrator bottleneck = higher throughput.
- Receive future innovations in later SD-Access + IOS XE releases.

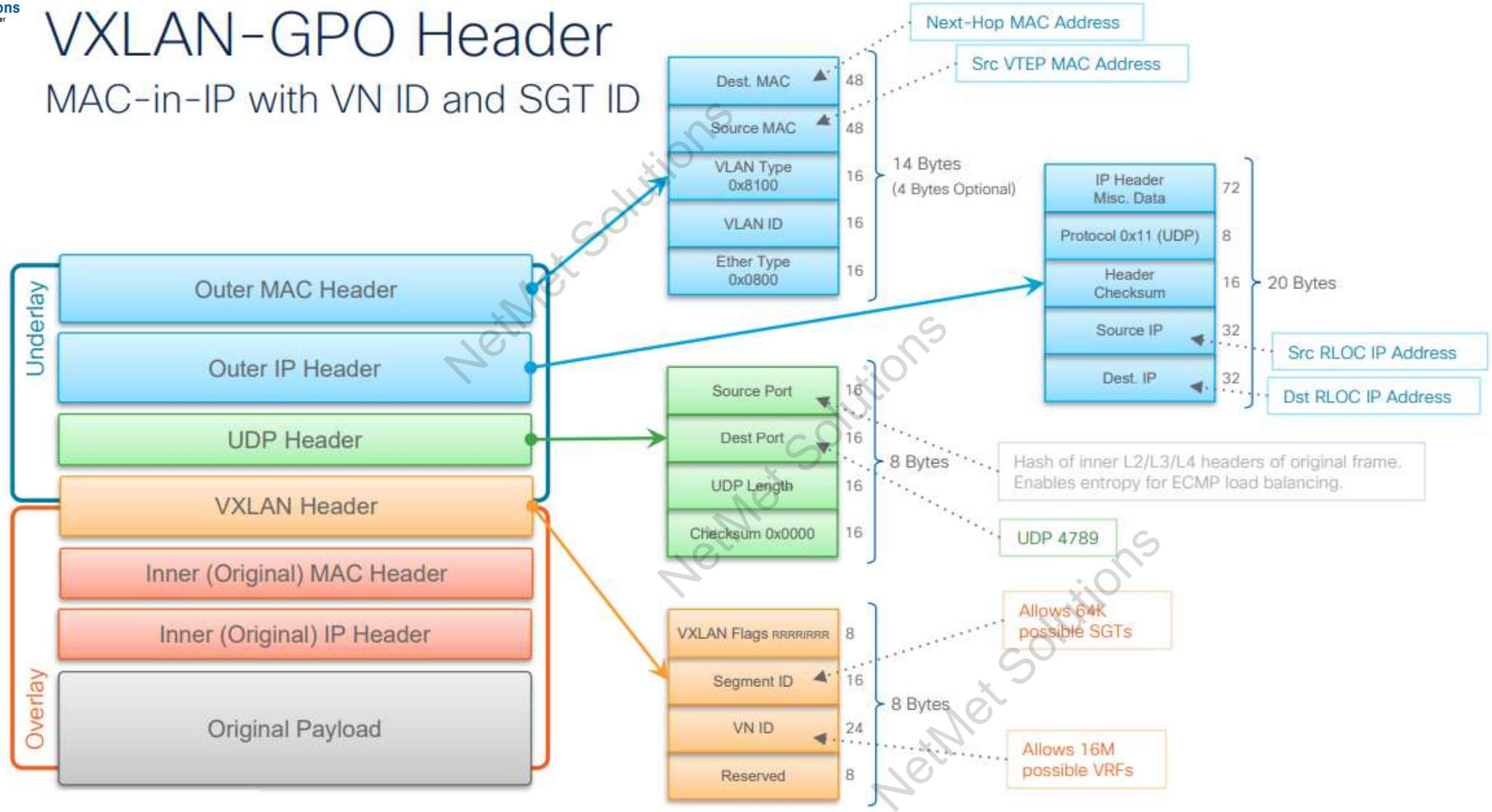
Cisco SD-Access Fabric

1. Control Plane: LISP
2. Data Plane: VXLAN

NetMet Solutions
Your Trusted Learning Partner

VXLAN-GPO Header

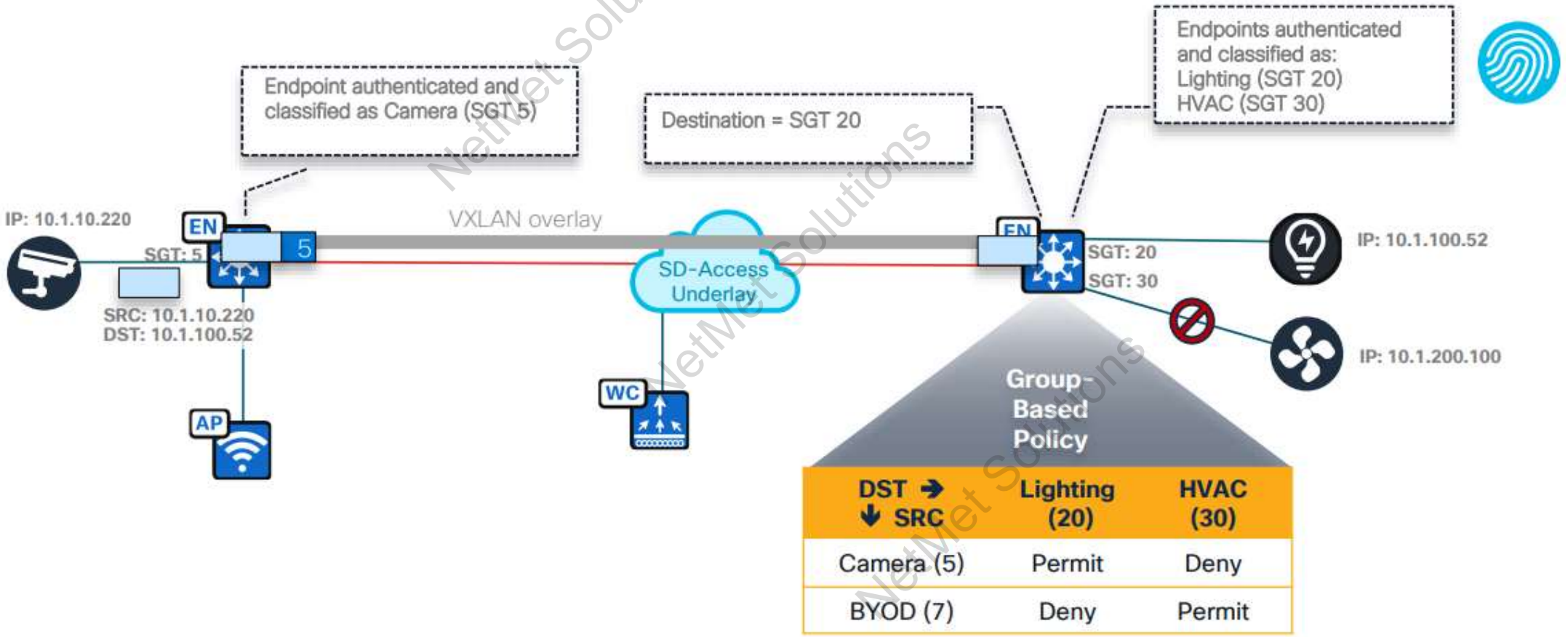
MAC-in-IP with VN ID and SGT ID



Cisco SD-Access Fabric

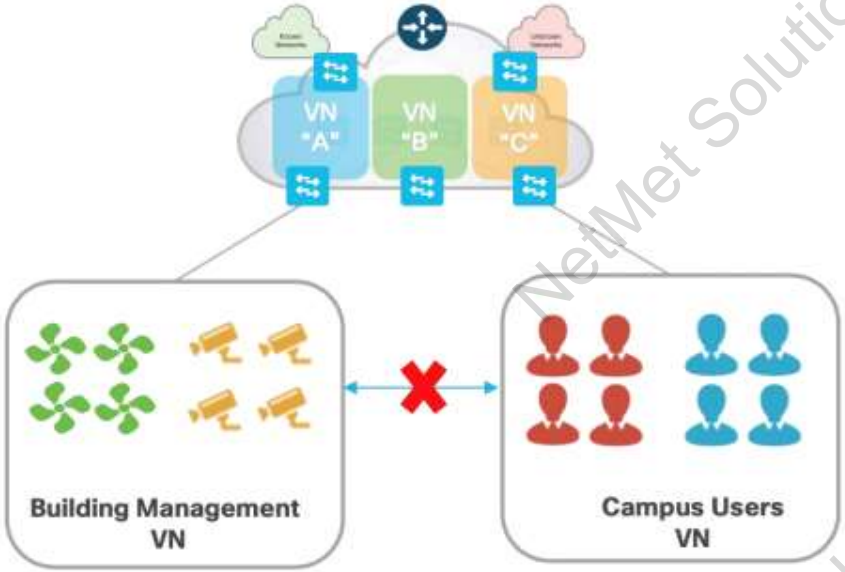
1. Control Plane: LISP
2. Data Plane: VXLAN
3. Policy Plane: Group-Based Policy

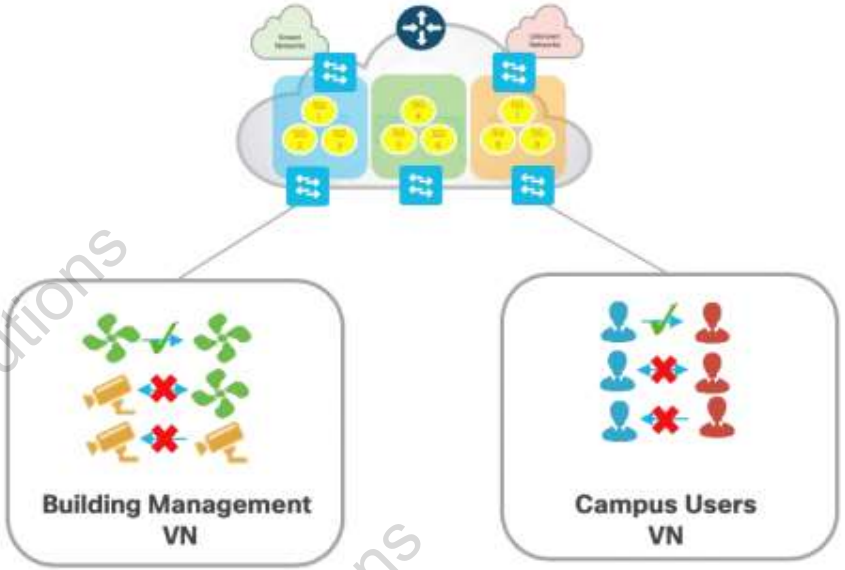
What is Security Group Tag and Group-Based Policy?



SD-Access Policy

Macro-Segmentation and Micro-Segmentation





Virtual Network (VN)

First-level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

Security Group Tag (SGT)

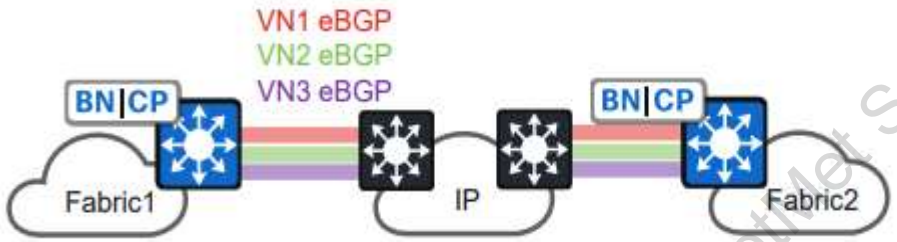
Second-level Segmentation ensures **role-based access control** between groups in a VN. Ability to segment the network into lines of business or functional blocks.

SD-Access Policy

Access Control Policies

NetMet Solutions
Your Trusted Learning Partner

Transits for VN and SGT Preservation

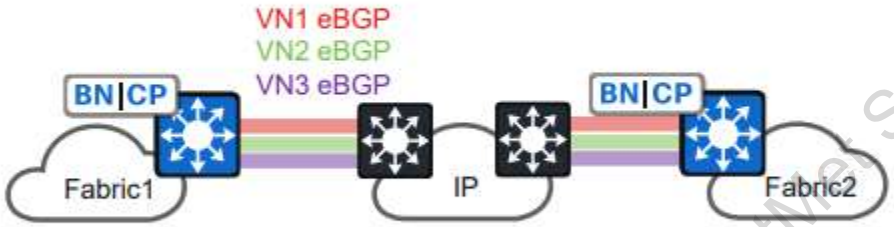


IP-Based Transit

- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.

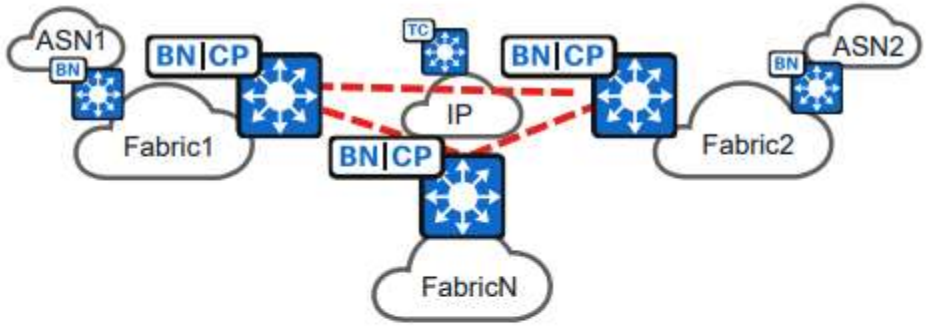
NetMet Solutions
Your Trusted Learning Partner

Transits for VN and SGT Preservation



IP-Based Transit

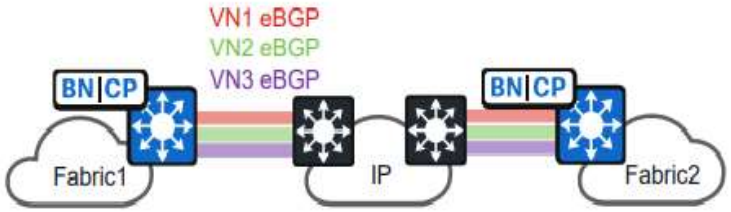
- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.



SD-Access Transit

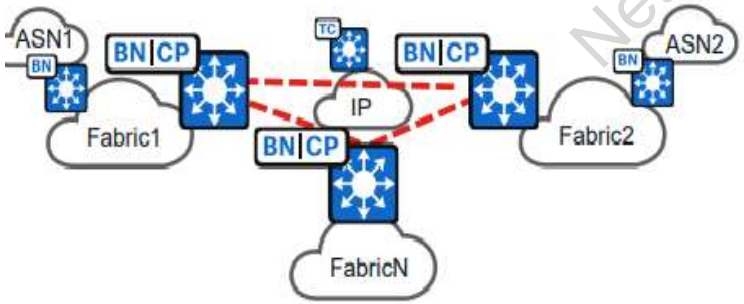
- SD-Access LISP/VXLAN between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGT.
- Fabric as a transit between external routing domains.

Transits for VN and SGT Preservation



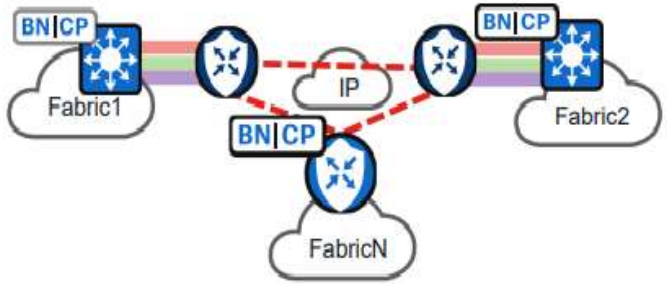
IP-Based Transit

- Per-Layer-3-Virtual-Network eBGP peering to external routing domain, or LISP Extranet Provider VN eBGP peering to external routing domain.
- SGT propagation outside of fabric requires suitable hardware and software.



SD-Access Transit

- SD-Access LISP/VXLAN between Fabric Sites.
- Preserves Layer 3 Virtual Networks and SGT.
- Fabric as a transit between external routing domains.



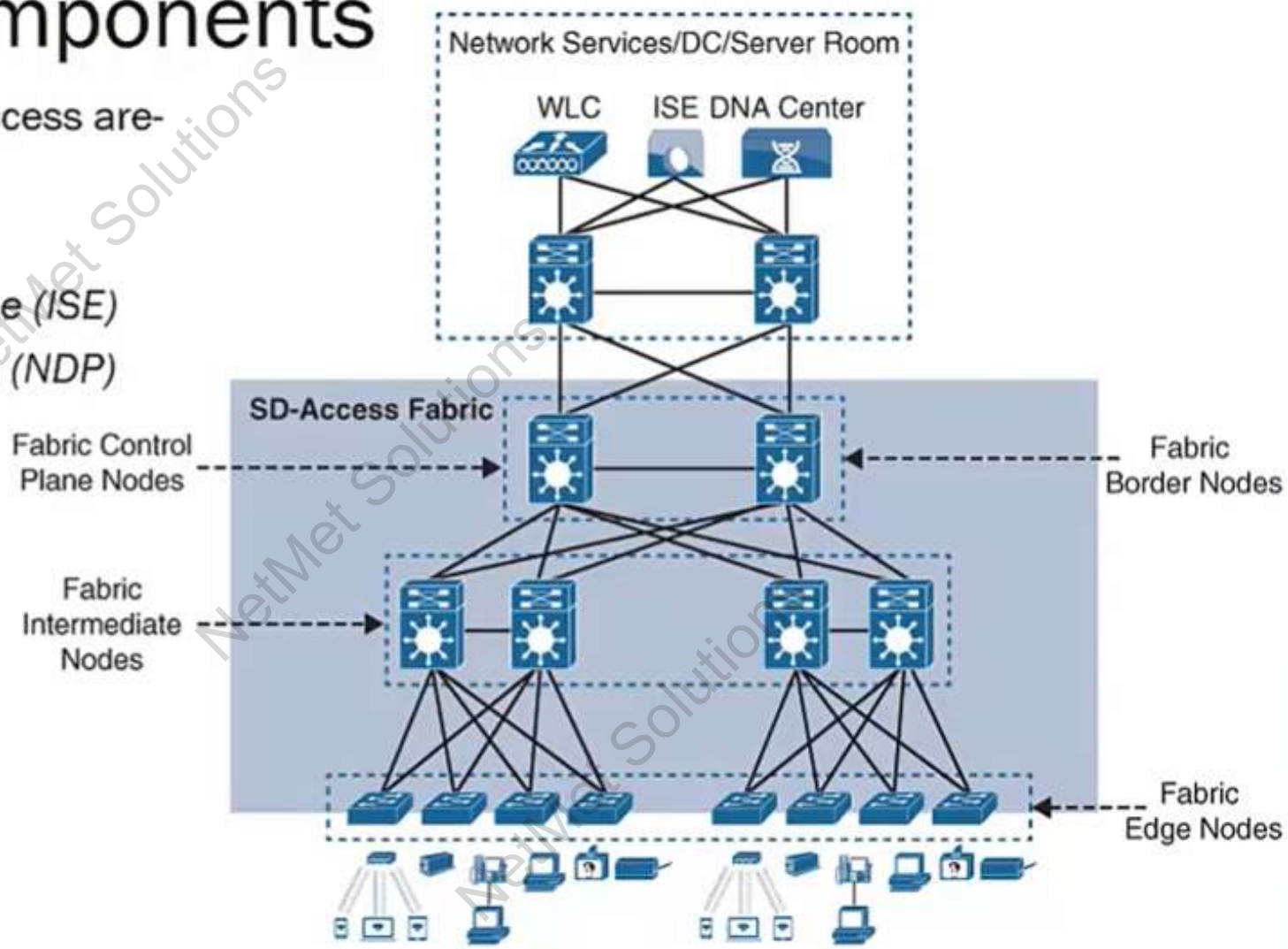
SD-WAN Transit

- Cisco SD-WAN between Fabric Sites.
- Separate SD-WAN Edge for implementation flexibility, Border Node port density and speed. Independent Domains PDG.
- Colocated SDWAN Edge for L3VN-VPN stitching with SGT data plane. IMPORTANT: Read Integrated Domains PDG for functional restrictions.

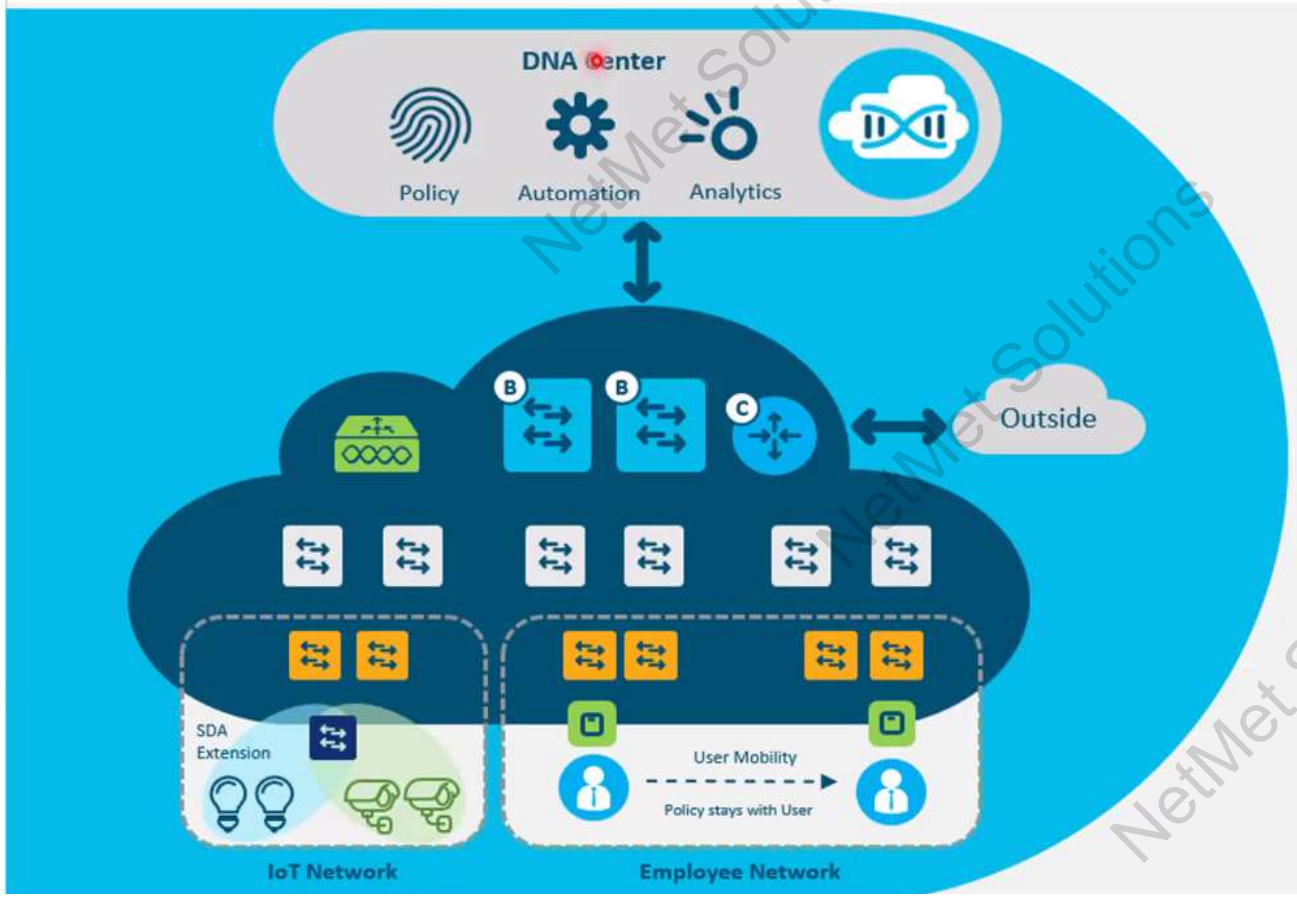
NetMet Solutions
Your Trusted Learning Partner

SD-Access Components

- Major components of SD-Access are-
  - *Fabric*
  - *APIC-EM Controller*
  - *Identity Services Engine (ISE)*
  - *Network Data Platform (NDP)*
  - *DNA Center*



Cisco SD-Access Components and Roles



Automated Network Fabric

Single Fabric for Wired & Wireless with simple Automation

Identity-Based Policy & Segmentation

Decouples Security & QoS from VLAN and IP Address

Insights & Telemetry

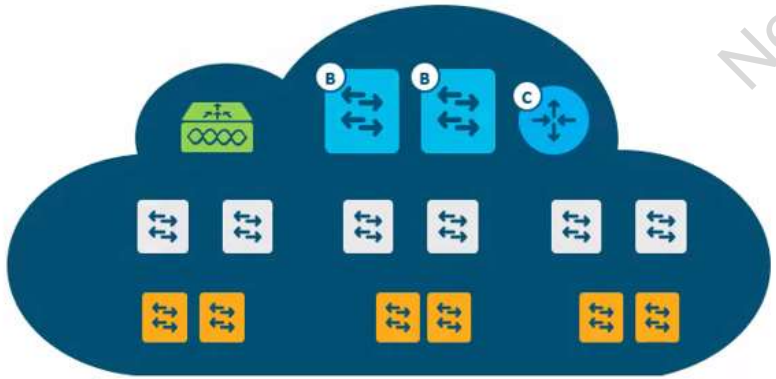
Analytics and Insights into User and Application behavior

NetMet Solutions
Your Trusted Learning Partner

SD-Access

Campus Fabric - Key Components

1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **CTS**

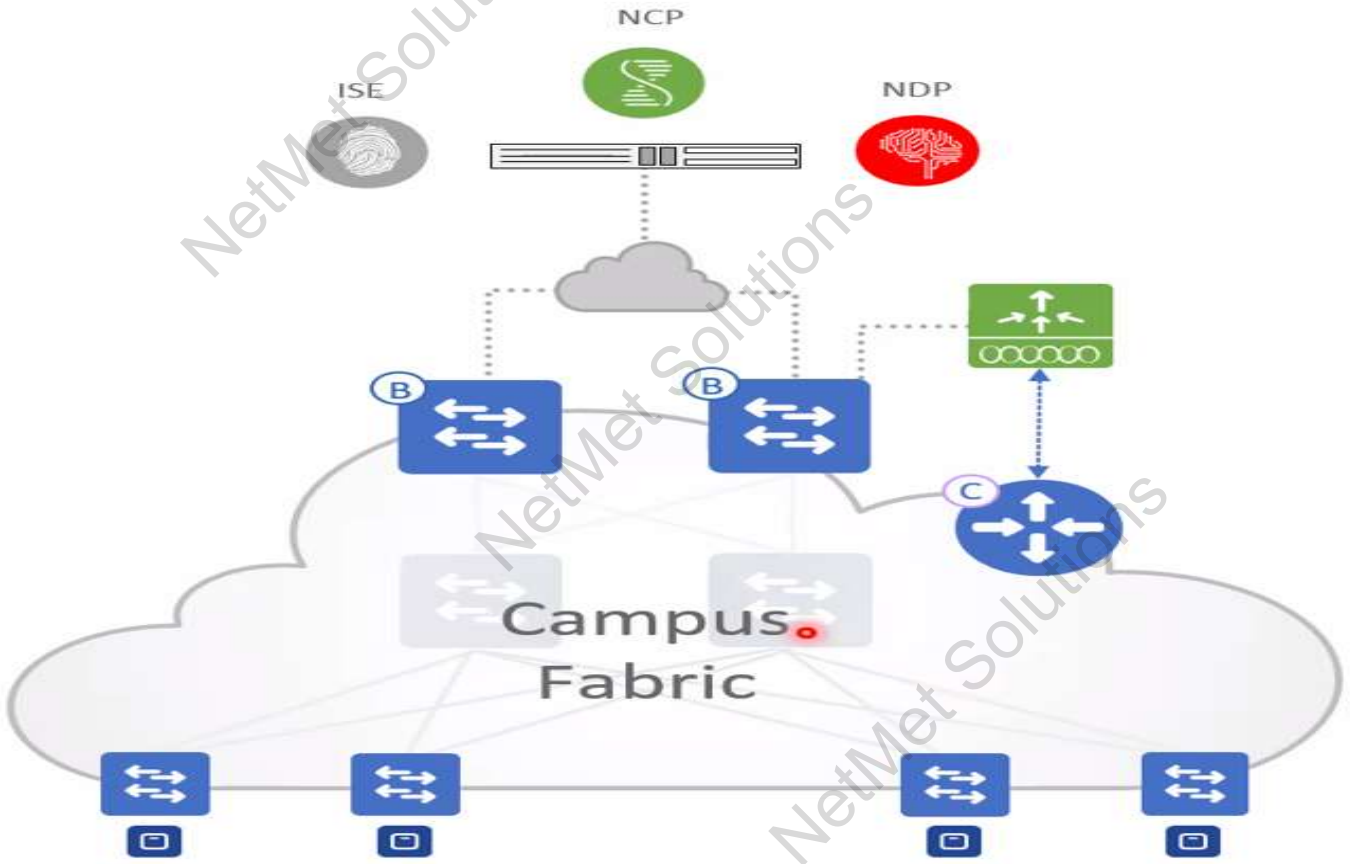


Key Differences
• L2 + L3 Overlay -vs- L2 or L3 Only
• Host Mobility with Anycast Gateway
• Adds VRF + SGT into Data-Plane
• Virtual Tunnel Endpoints (Automatic)
• NO Topology Limitations (Basic IP)

NetMet Solutions
Your Trusted Learning Partner

SD-Access

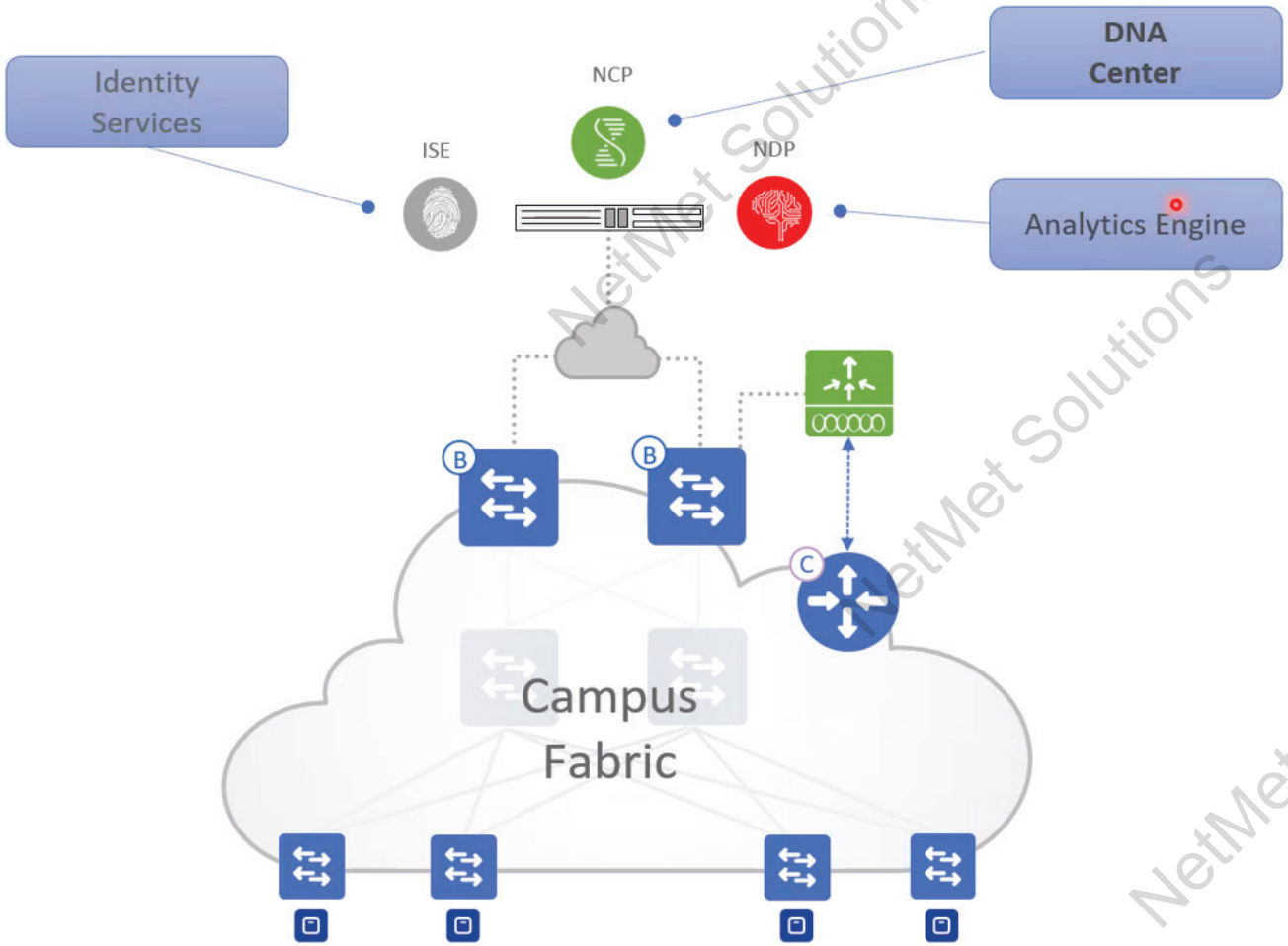
Fabric Roles & Terminology



NetMet Solutions
Your Trusted Learning Partner

SD-Access

Fabric Roles & Terminology



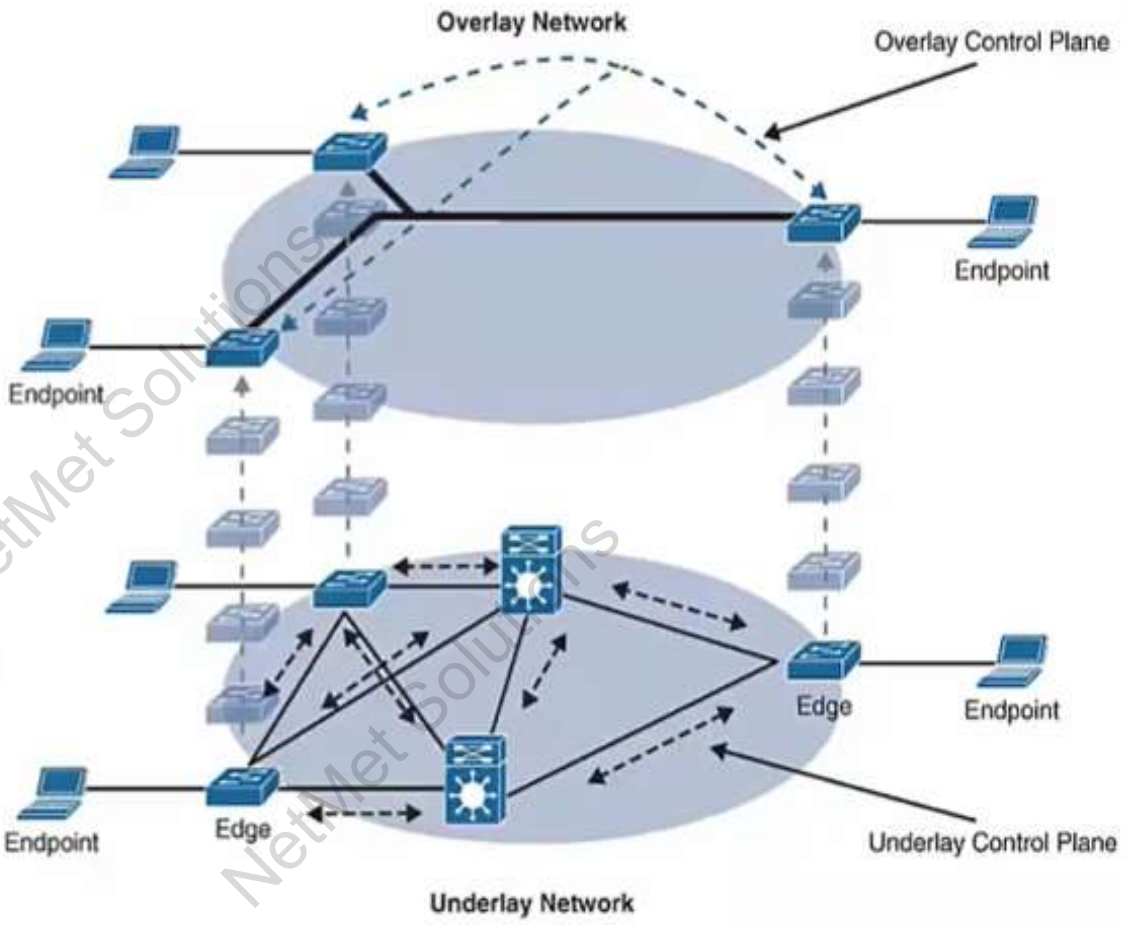
- **DNA Center** – provides simple GUI management and intent based automation (e.g. NCP) and context sharing
- **Identity Services** – NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status

58

NetMet Solutions
Your Trusted Learning Partner

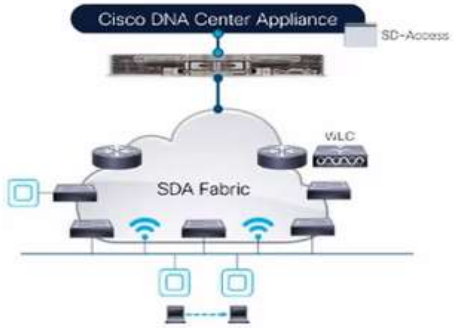
Underlay and Overlay Network

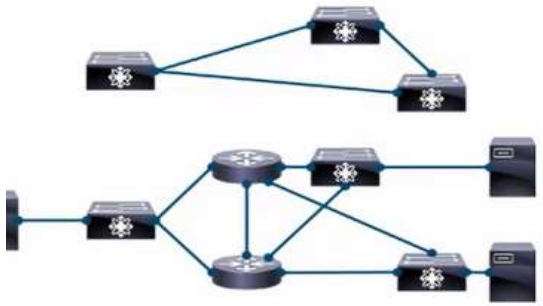
- The underlay network is defined by the physical switches and routers that are used to deploy the SD-Access network.
- All network elements of the underlay must establish IP connectivity via the use of a routing protocol.
- An overlay network is created on top of the underlay network through virtualization.
- The 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.



NetMet Solutions
Your Trusted Learning Partner

isco SD-Access Overview





Data Plane Encapsulation