A Central Network Controller for Industrial Automation – What Does It Mean for ODVA Technologies

Paul Didier
Cisco

SW-Defined Network and Centralized Network Control

- Why Centralized Control for the Network
  - Automated
  - Assurance
  - Security & Segmentation
- What is an SDN?
  - Underlay and Overlay
  - SDN architecture and roles
  - Virtual networking concepts: Control, Data and Policy “planes”
  - Segmentation and Zones & Conduits
- What does this mean for ODVA-based technologies?
  - EIP’s IP focus means native integration
  - Dynamic movement of workloads
  - APIs to coordinate network and IACS into a SW-Defined Factory

Why a Centralized Controller & SW-Defined Networking

Benefits of SDN

Enhance Security and Compliance

Deliver consistent Experience

Boost operational effectiveness

Gain network insights

SDN - Interesting features for Industrial Networks

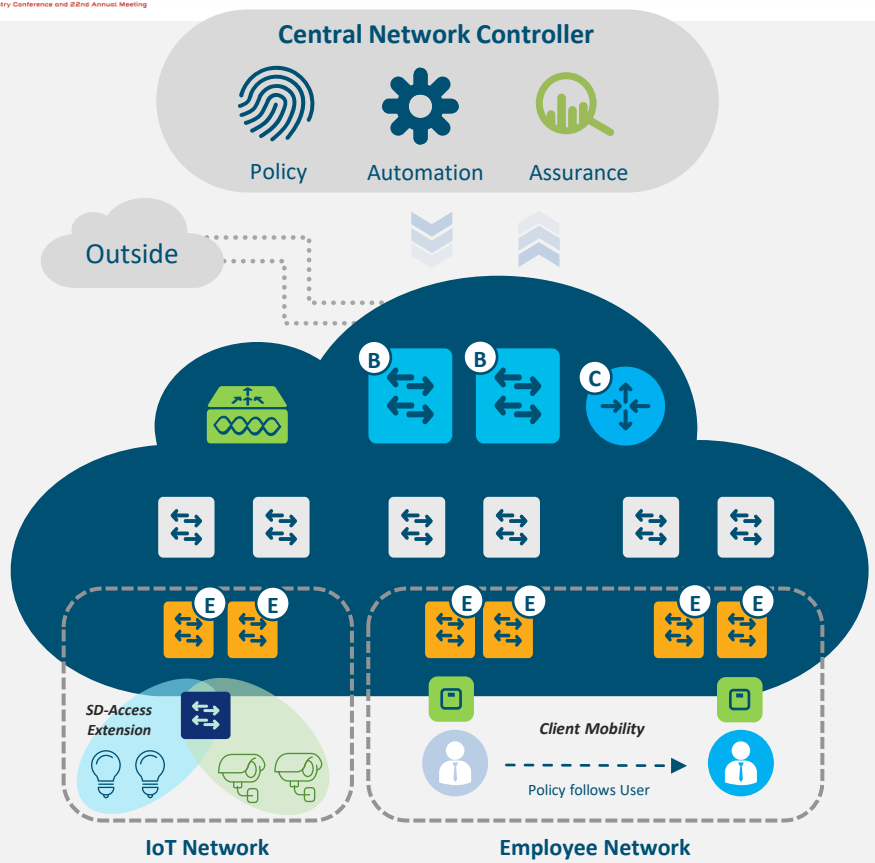
Key advantages for IACS:

- Stretching VLANs to enable asset virtualization: Engineering workstations, HMIs and PLCs
- Limit Spanning Tree impacts
- Easily deploy Zones and Conduits model

Challenges:

- Precision Time requires consistent paths
- Resiliency – recovery from link/switch failures not the same range as the L2 protocols

Software Defined Network – key functions



One Automated Network Fabric

Single fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

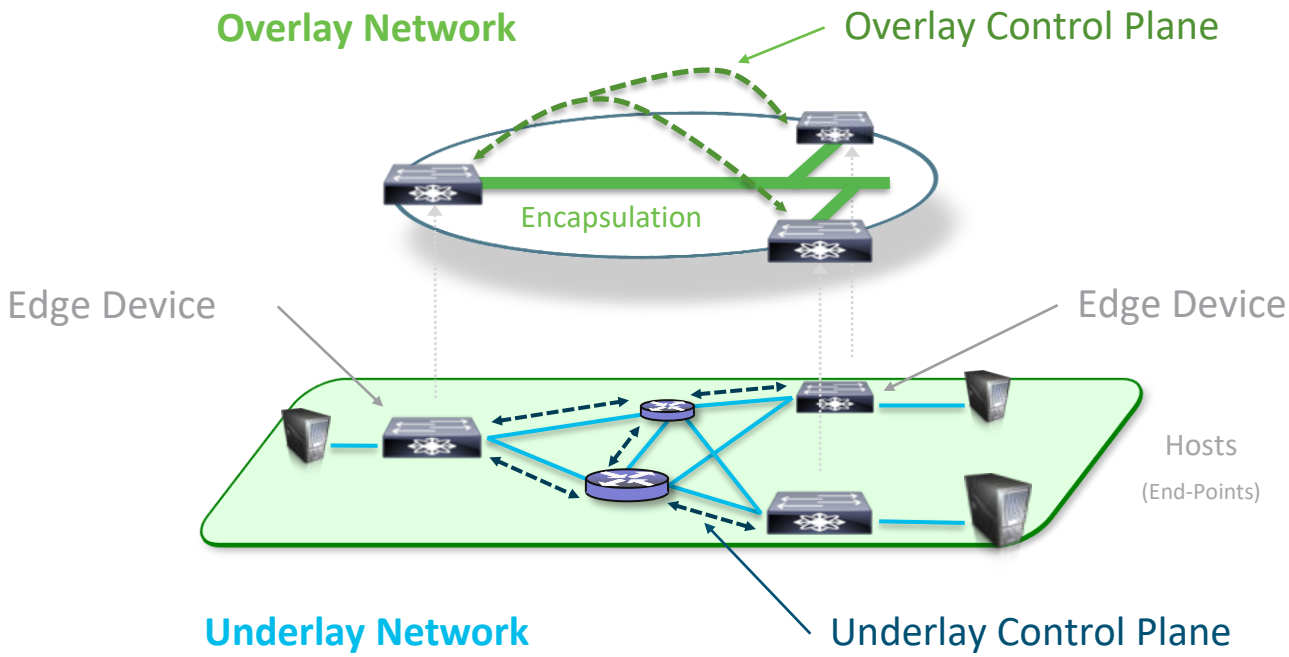
Policy definition decoupled from VLAN and IP address

AI-Driven Insights and Telemetry

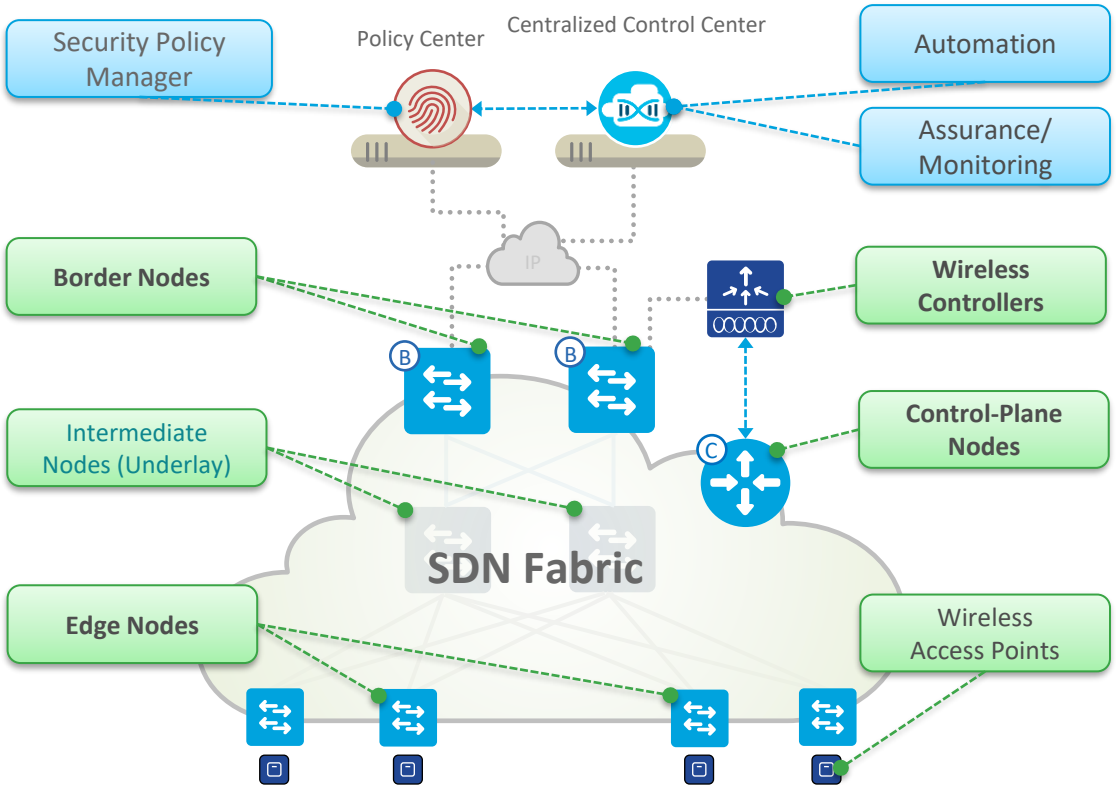
Analytics and visibility into User and Application experience

What is a SW-Defined Network

SW-Defined Network: Virtualizing HW from Network



SW-Defined Network: Roles & Terminology

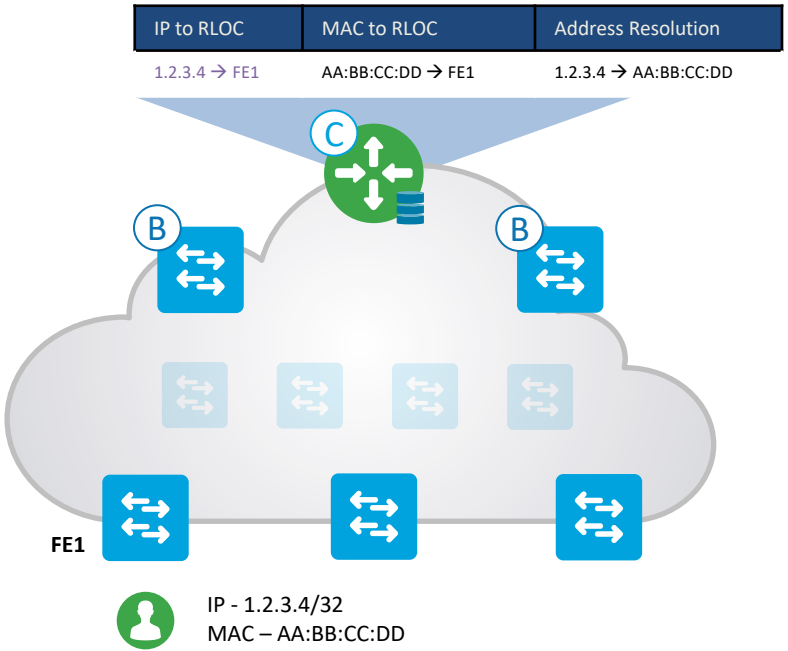


- **Automation** – Simple GUI and APIs for automated deployment, configuration and management of wired and wireless devices
- **Assurance** – Data Collectors analyze Endpoint to Application flows and monitor network/end - device status
- **Security Policy Manager** – Network Access Control & ID Services for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the fabric
- **Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the fabric
- **Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the fabric

SDN – Control Plane Nodes

Control-Plane Node runs a Host Tracking Database to map location information

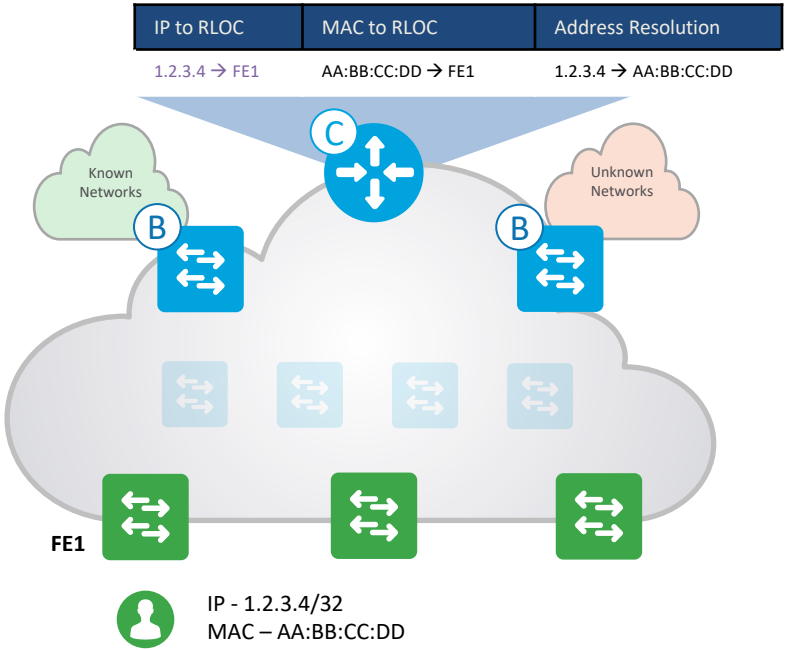
- A simple Host Database that maps Endpoint IDs to a current Location, along with other attributes
- Host Database supports multiple types of Endpoint ID lookup types (IPv4, IPv6 or MAC)
- Receives Endpoint ID map registrations from Edge and/or Border Nodes for “known” IP prefixes
- Resolves lookup requests from Edge and/or Border Nodes, to locate destination Endpoint IDs



SDN – Edge Nodes

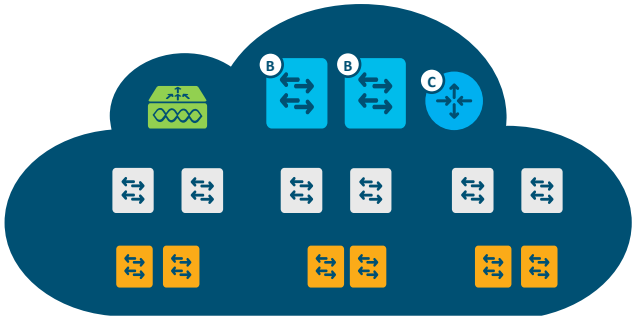
Edge Node provides first-hop services for Users / Devices connected to a Fabric

- Responsible for Identifying and Authenticating Endpoints (e.g. Static, 802.1X, Active Directory)
- Register specific Endpoint ID info (e.g. /32 or /128) with the Control-Plane Node(s)
- Provide an Anycast L3 Gateway for the connected Endpoints (same IP address on all Edge nodes)
- Performs encapsulation / de-encapsulation of data traffic to and from all connected Endpoints



SDN Key Components

1. **Control-Plane** based on **LISP or BGP-EVPN**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **VRFs and SGTs**
4. **Management-Plane**



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)

Why LISP?

Pull Model

- No massive routing tables
- “DNS” for routing
- Conversational learning

Scalability

- Purpose built for scale

Address-Family support

- IPv4, IPv6 and MAC address family

Wired and Wireless unification

- WLC participates in LISP control plane communication
- Wired and Wireless endpoints have policy applied at same point in the network

Host Mobility

- Native support for this capability
- Wired and Wireless

SDN Key Components – LISP
(Locator/ID Separation Protocol)

Control-Plane based on LISP

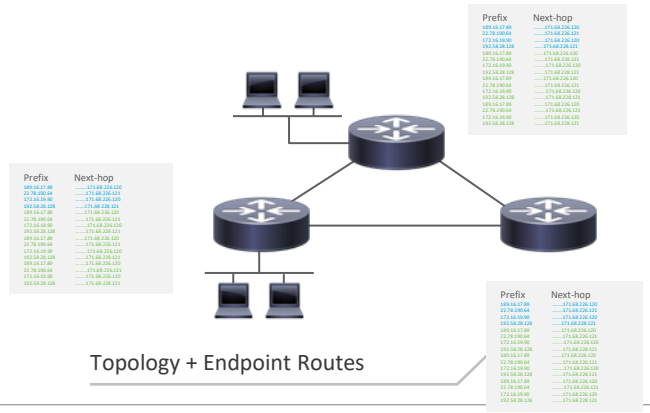
Host Mobility

Routing Protocols = **Big Tables** & **More CPU**
with Local L3 Gateway

LISP DB + Cache = **Small Tables** & **Less CPU**
with Anycast L3 Gateway

BEFORE

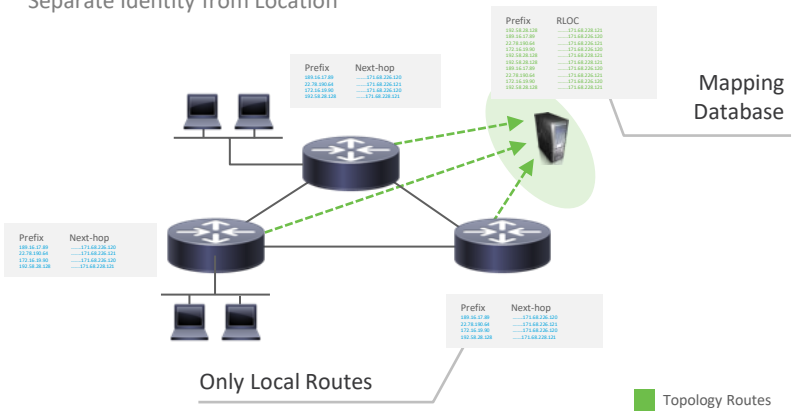
IP Address = Location + Identity



Endpoint Routes are Consolidated to LISP DB

AFTER

Separate Identity from Location



Topology Routes
Endpoint Routes

LISP Operations

Control-Plane Roles & Responsibilities

LISP Map Server / Resolver
(Control-Plane)

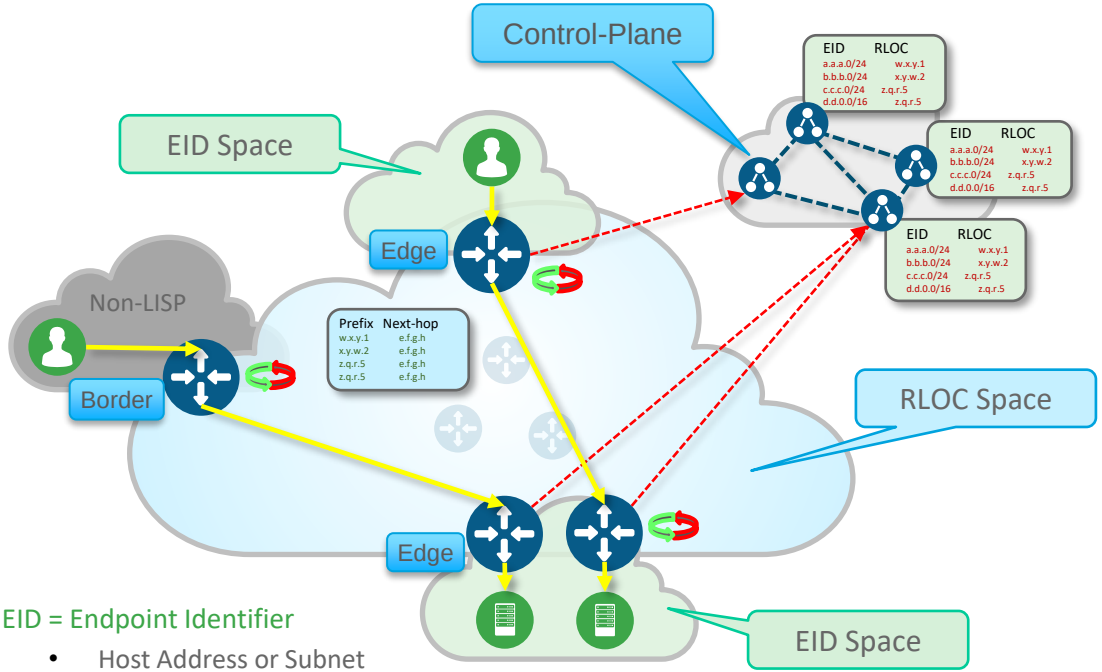
- EID to RLOC mappings
- Can be distributed across multiple LISP devices

LISP Tunnel Router - XTR
(Edge & Internal Border)

- Register EID with Map Server
- Ingress / Egress (ITR / ETR)

LISP Proxy Tunnel Router - PXTR
(External Border)

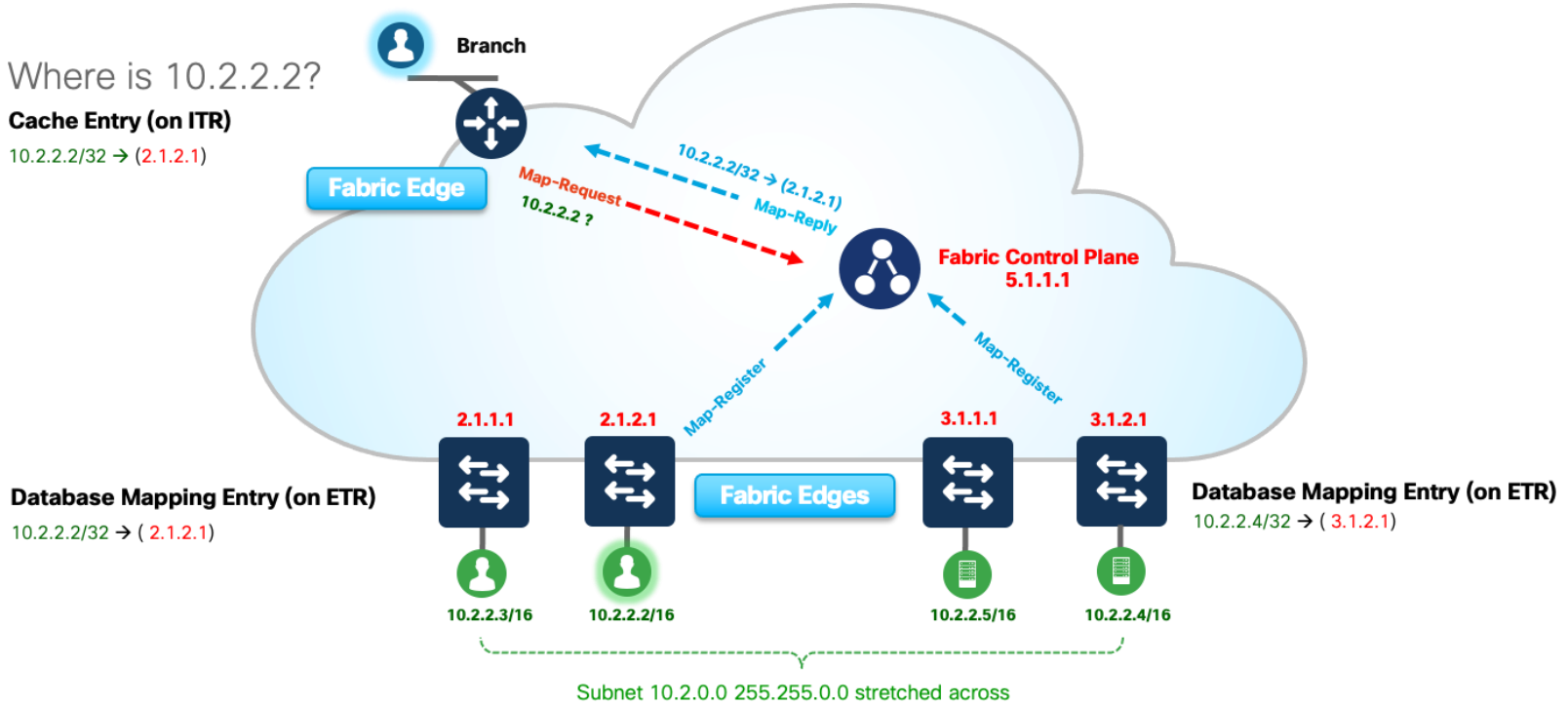
- Provides a Default Gateway when no mapping exists
- Ingress / Egress (PITR / PETR)



- EID = Endpoint Identifier
  - Host Address or Subnet
- RLOC = Routing Locator
  - Local Router Address

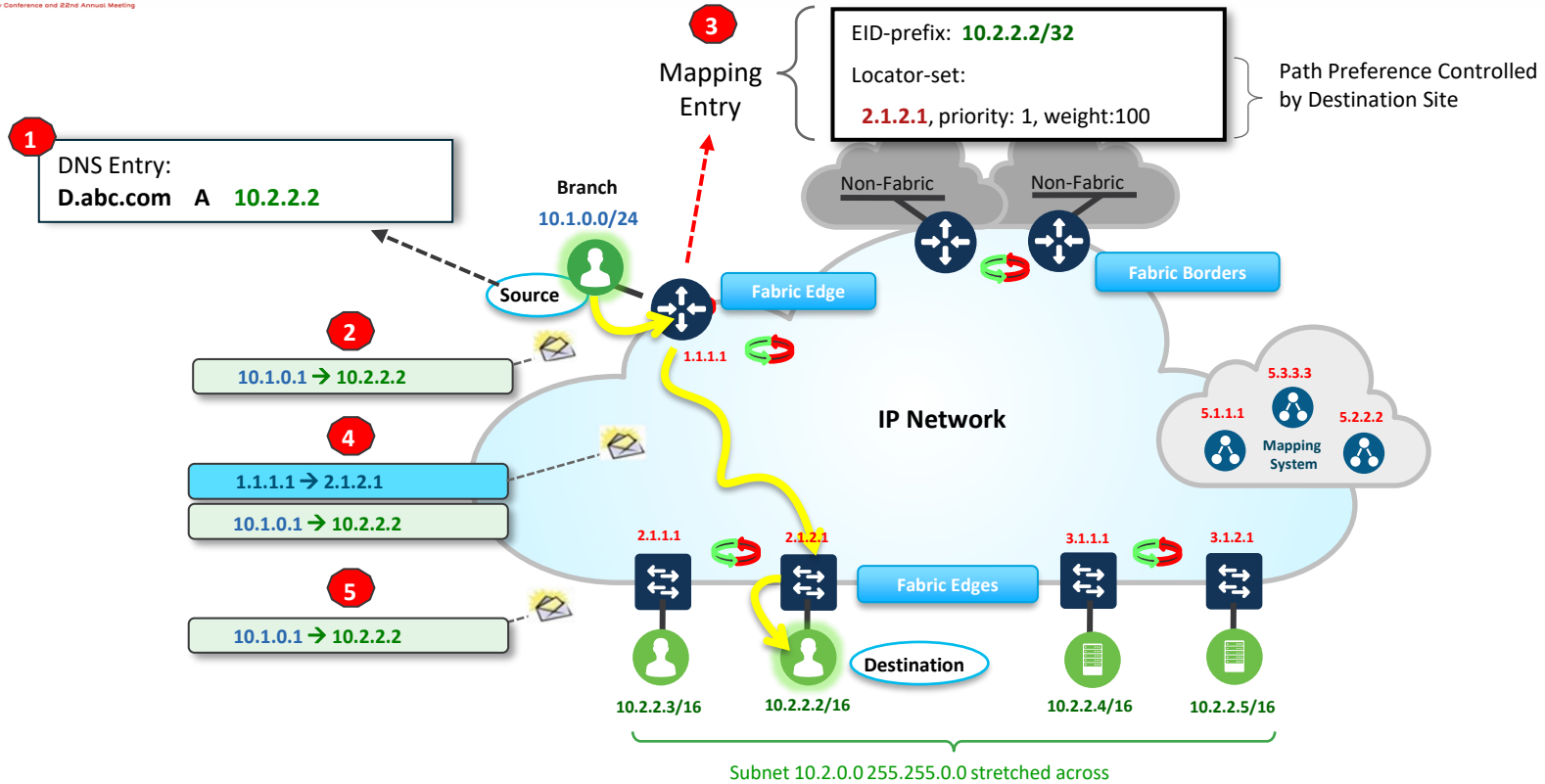
LISP Operations

Control Plane Register & Resolution



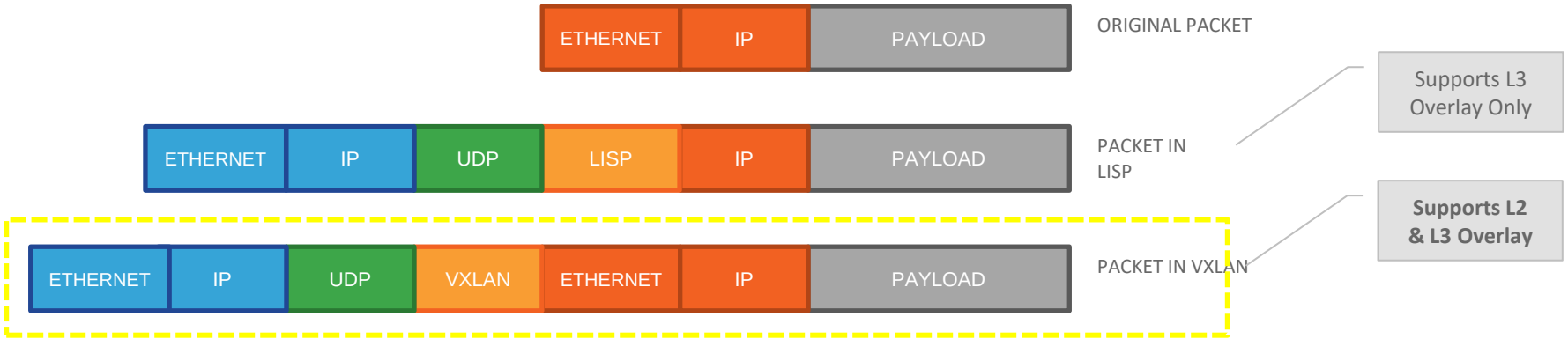
LISP Operations

Fabric Internal Forwarding (Edge to Edge)



SDN Key Components – VXLAN

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



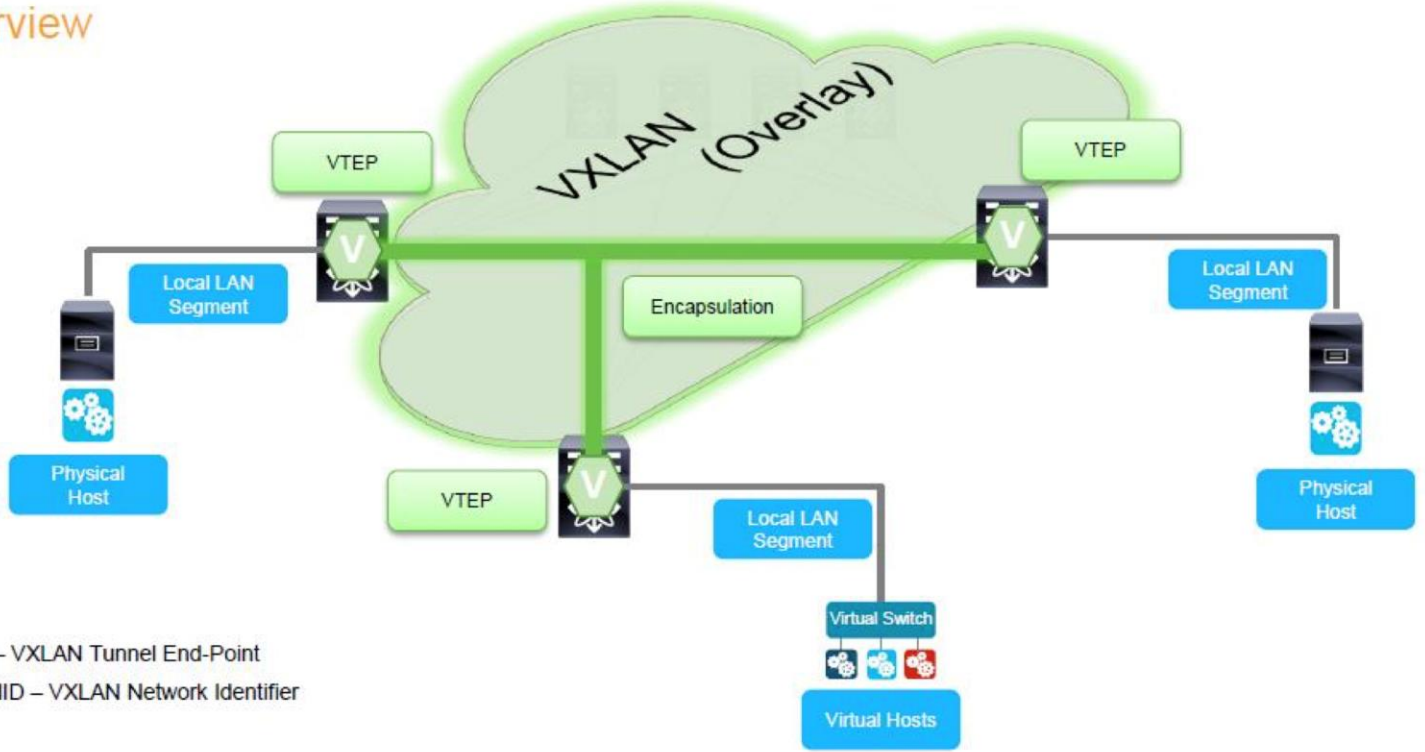
What is VxLAN

VxLAN – Virtual eXtensible Local Area Network is an extension of VLANs created for cloud applications

- Standards based Encapsulation IETF RFC 7348
- Uses UDP-Encapsulation
- Transport Independent
- Layer-3 Transport (Underlay)
- Flexible Namespace
- More VLANs - 24-bit field (VNID) provides ~16M unique identifier
- Allows Segmentations
- Limits the impact of STP
- Adds

VXLAN Overview

Overview

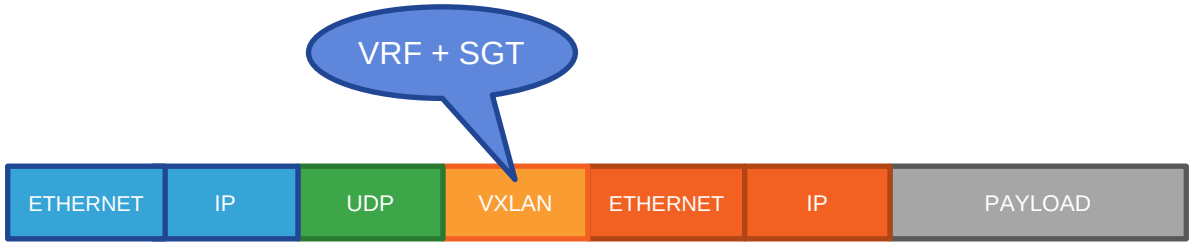


VTEP – VXLAN Tunnel End-Point

VNI/VNID – VXLAN Network Identifier

Key Components – Group Based Policy

1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **VRF and SGT**

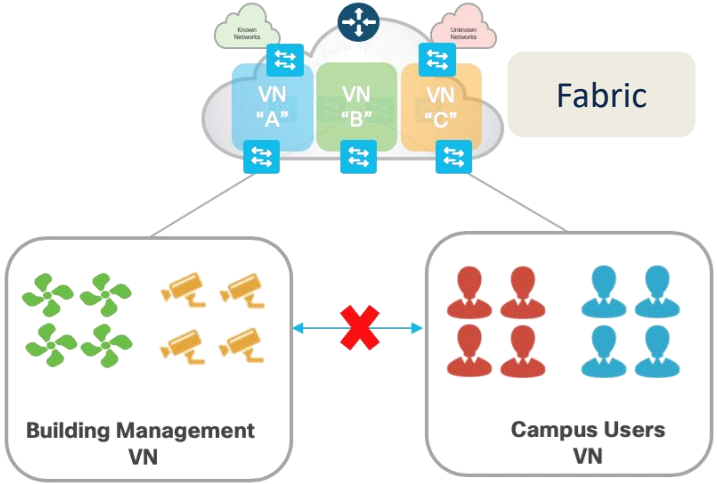


Virtual Routing & Forwarding

Scalable Group Tagging

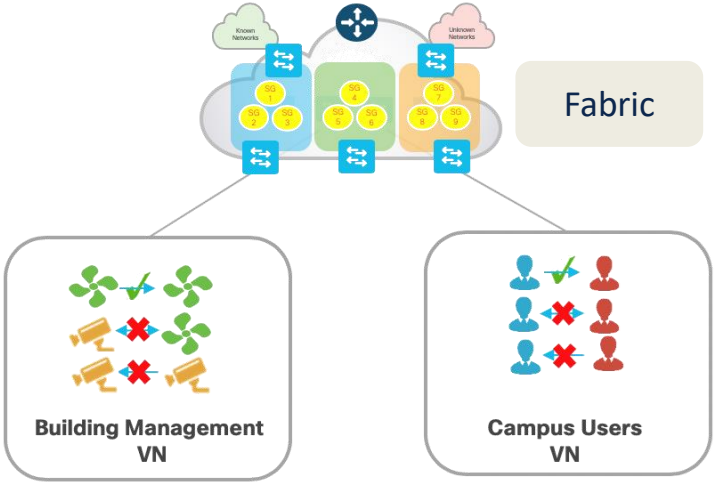
SDN Policy

Two Level Hierarchy – Macro & Micro Segmentation



Virtual Network (VN)

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



Scalable Group (SG)

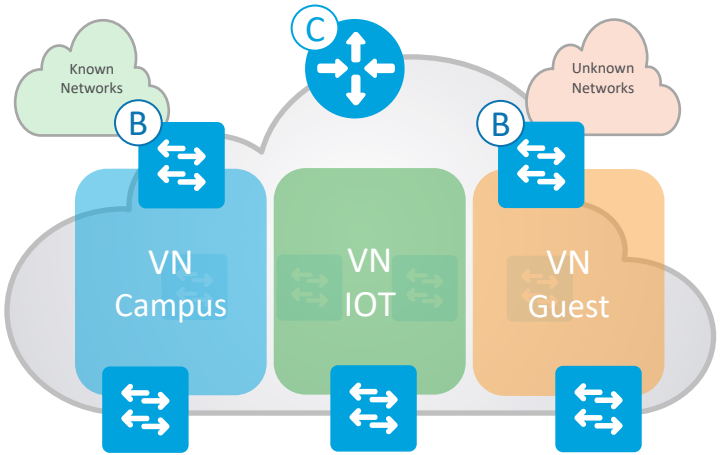
Second-level Segmentation ensures **role-based access control** between groups in a VN. Ability to segment the network into lines of business or functional blocks. Also know as Cisco TrustSec (CTS)

IETF equivalent: https://datatracker.ietf.org/doc/html/draft-smith-kandula-sxp-10

SDN – Macro segmentation

Virtual Network maintains a separate Routing & Switching table for each instance

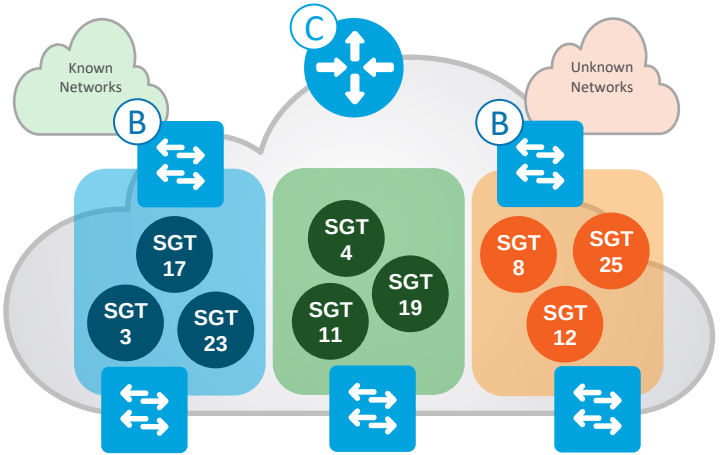
- Control-Plane uses Instance ID to maintain separate VRF (Virtual Routing and Forwarding) topologies (“Default” VRF is Instance ID “4098”)
- Nodes add a VNID to the Fabric encapsulation
- Endpoint ID prefixes (Host Pools) are routed and advertised within a Virtual Network
- Uses standard “vrf definition” configuration, along with RD & RT for remote advertisement (Border Node)



SDN – Micro segmentation

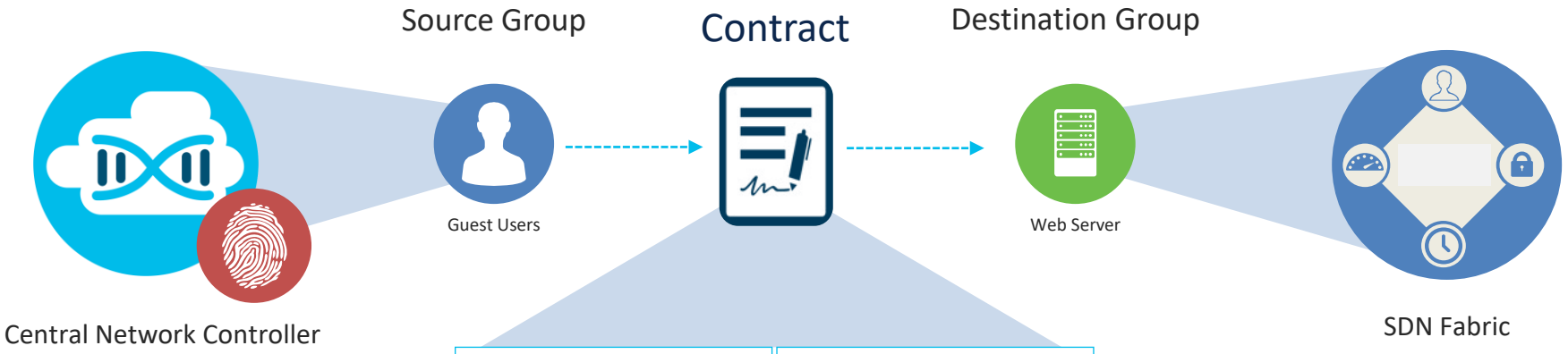
Scalable Group is a logical policy object to "group" Users and/or Devices

- Nodes use "Scalable Groups" to ID and assign a unique Scalable Group Tag (SGT) to Endpoints
- Nodes add a SGT to the Fabric encapsulation
- SGTs are used to manage address-independent "Group-Based Policies"
- Edge or Border Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)



IETF equivalent: https://datatracker.ietf.org/doc/html/draft-smith-kandula-sxp-10

SDN - Access Control Policies



CLASSIFIER: PORT | ACTION: DENY

Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

All groups in a Policy must belong to the same Virtual Network

What Does it Mean for ODVA Technologies?

SDN and ODVA

- EIP based on IP means EIP is ready to be transported natively over SDN networks
  - CIP Sync/Motion - PTP over SDNs needs to be tested and validated
- DetNet (Layer 3 TSN) uses VXLAN
- Virtualize assets that communicate via EIP
- Redundancy protocols apply to networks connected to SDN
  - Redundancy protocols over an SDN has not been tested – not sure it adds value
  - PRP over SDN (2 fabrics) is a consideration
- Application specific configuration data can be used to program the network
  - API's in SDN platforms enable integration with Control applications beyond telemetry


2023
ODVA
Industry Conference and 22nd Annual Meeting