



You make **possible**

CISCO *Live!*

Virtual Event APJC • 1-2 April 2020

#CiscoLiveAPJC

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public



Extending the Enterprise

To the IoT Edge

Keith Pereira kpereira@cisco.com

BRKRST-2449 +

Cisco *live!*
June 9-13, 2019 • San Diego, CA

#CLUS



Agenda

- Why Extend the Enterprise?
- Solution Requirements
- Platform Choices
- Extending the Enterprise with Cisco DNA Center
- Cisco SD-WAN for IOT
- Summary and Wrap-Up

Why Extend the Enterprise?

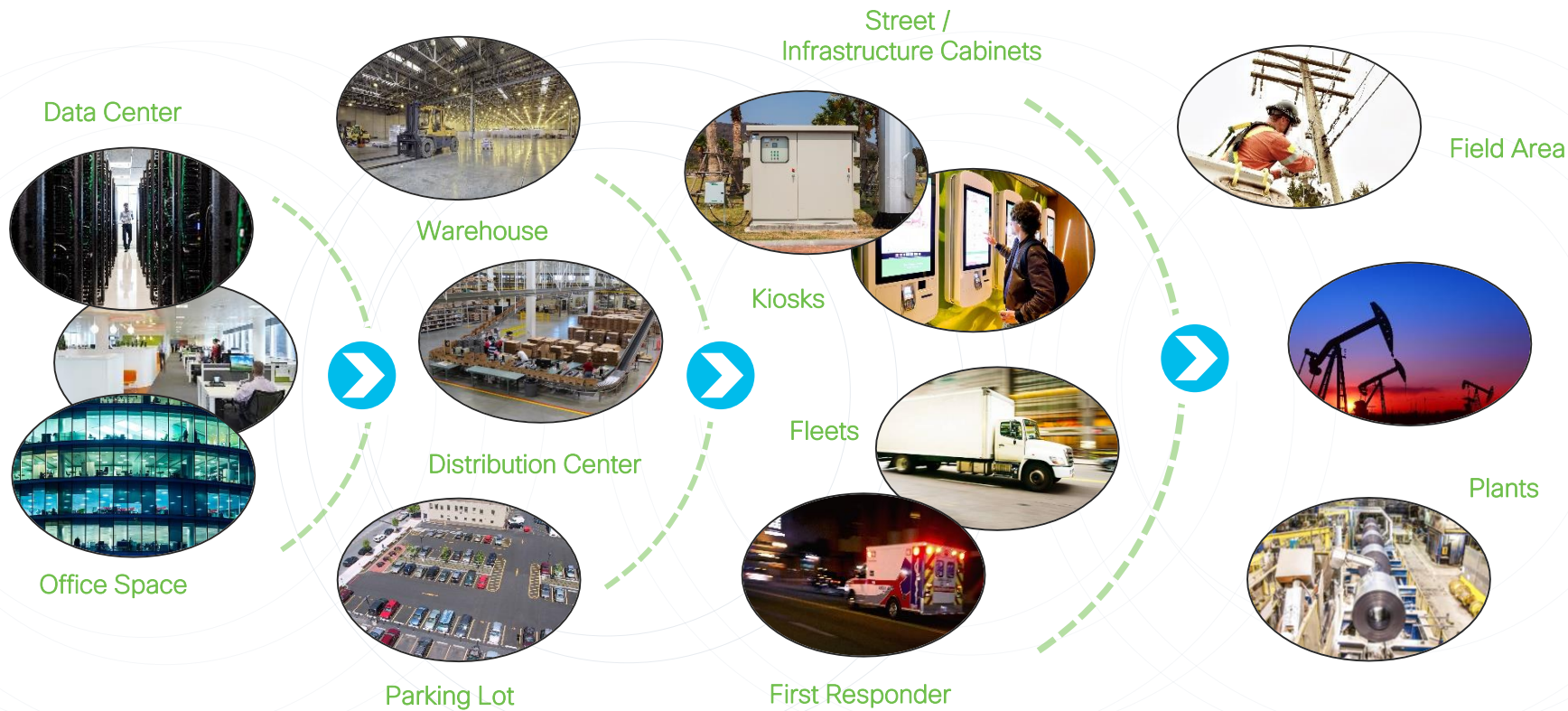


You make networking **possible**

IoT is Digitally Transforming Business



As a Result, the Network Boundary is Being Increasingly Extended

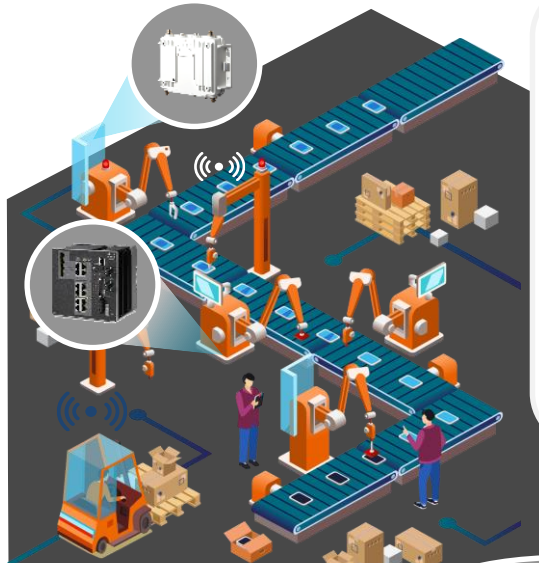


Area of Focus for this Session: The Extended Enterprise



Extended Enterprise Use-Cases

Smart Warehouses and Distribution Centers

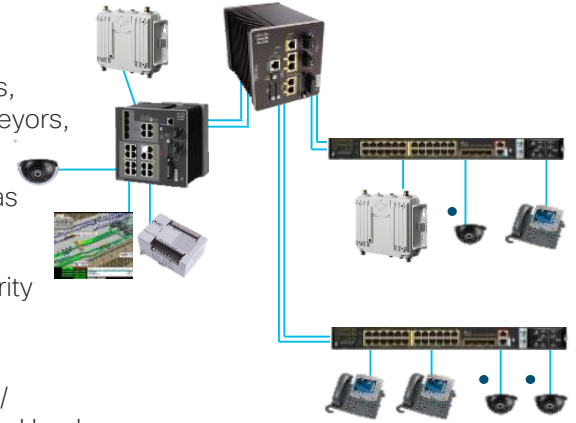


Why?

- Improved inventory management
- Improved safety and productivity of staff
- Increased operational efficiency delivered through real-time process visibility
- Improved security with consistent policies across domains
- Reliable network operations without air-conditioning costs

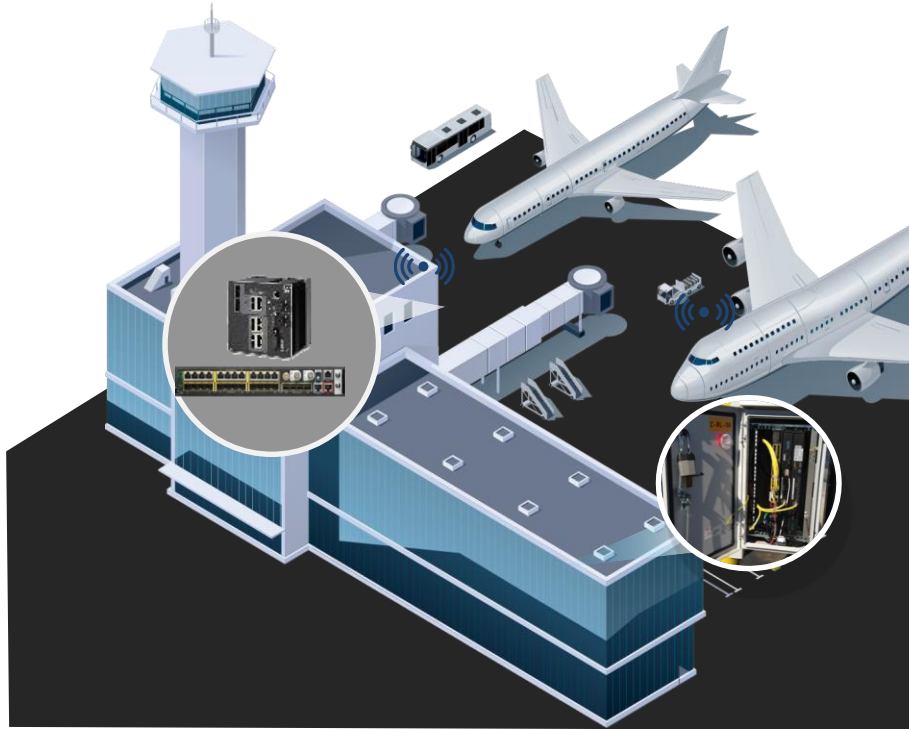
What?

- Tags, Trackers, Sorters, Conveyors, etc.
- Safety cameras
- Wi-Fi APs
- Safety & security systems
- Laptops / Smartphones / Tablets / Other Hand-Held devices



Extended Enterprise Use-Cases

Connected Airports

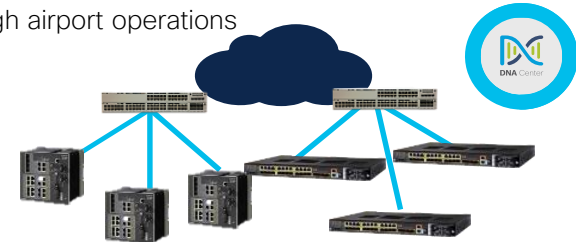


Why?

- Operational efficiency and enhanced passenger experience through
- Reduced lost/ delayed luggage
- Faster flight operations
- Improved turn-around time for planes
- Seamless communications through airport operations

What?

- Video surveillance cameras
- IP phones
- Auxiliary power systems
- Wireless APs for baggage scanning systems



Solution Requirements



You make security **possible**

Extending the Enterprise

Customer Objectives for IOT/OT use cases

Extend
connectivity to
non-IT
environments



Manage
Security Risk



Speed &
Agility



Compliance
and
Regulations



Innovate &
Differentiate



Challenge for IT Network Architects

Which device do I choose for IOT use cases ?

Future Ready



On Time



Within Budget



DNA
Manageable



Best practices



Design Options



Platform Choices



Platform Choices: Why Not use Catalyst?



You make the power of data **possible**

IOT Use Cases Are Different

Choose Hardware to Meet Requirements



Size weight
form-factor



High MTBF resilient
network topologies



Extended
Temperature Range (-
40 – 75°C)
Fanless and Self-
Cooled



Shock and
vibration

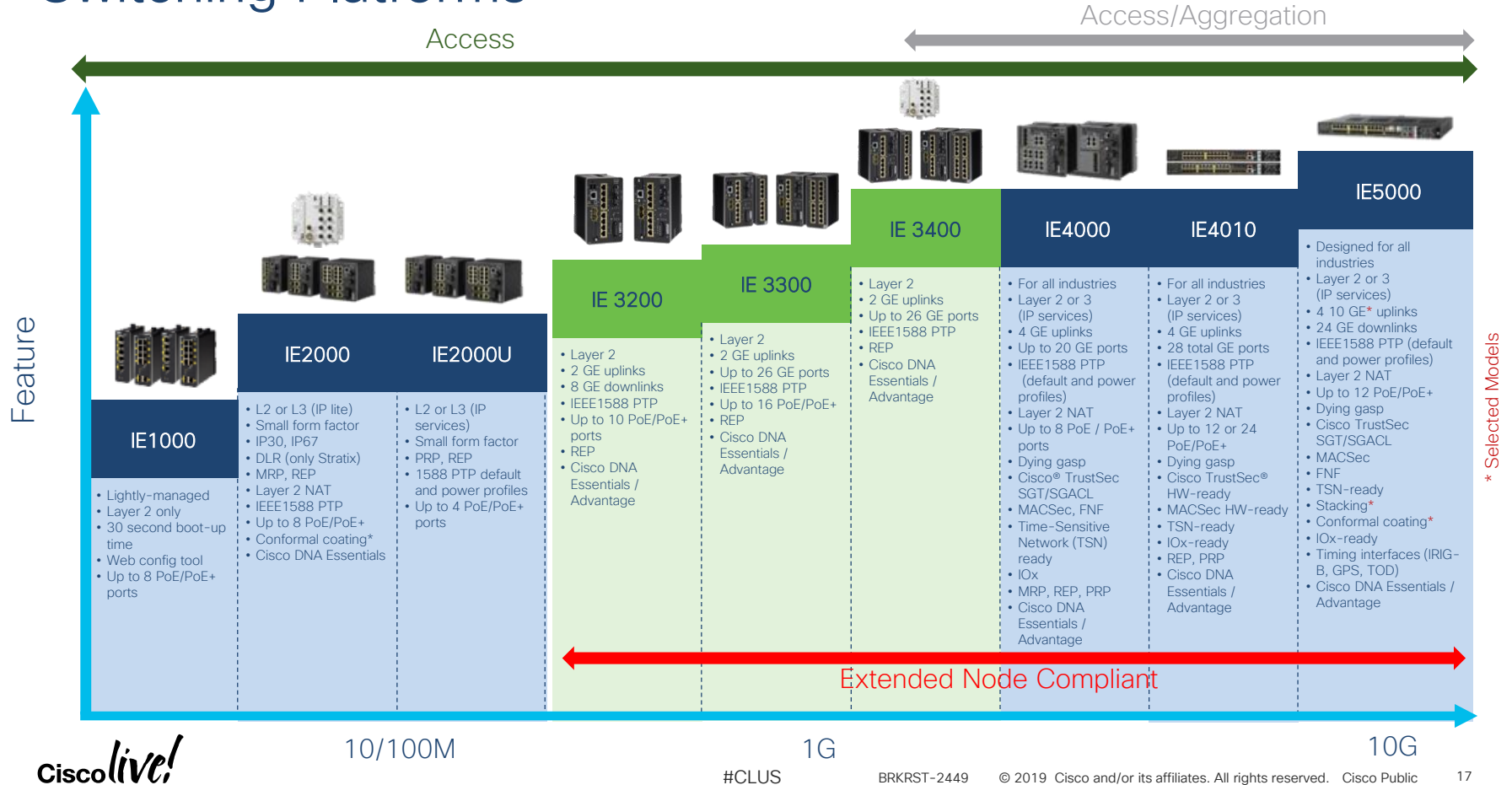


Din-rail or rack
mounts



Industry Safety and
Std's certifications

Extending the Enterprise with Industrial Ethernet Switching Platforms



Extending the Enterprise Platforms

Delivering Intent-Based Networking at the IoT Edge with Industrial Ethernet

Catalyst IE3x00 Rugged Series



IR1101 ISR Rugged



Built for Intent-Based Networking | Powered by IOS XE | Edge Enabled

Proven Cisco Technology

Ruggedized | Built for IoT | Industries Certified



A Modern Modular OS

High Availability | Programmability | Scalability

Managed by Cisco DNA Center

Cisco SD-Access for Extended Network



You make multi-cloud **possible**

Why Cisco SDA for Extended Nodes?

Common workflow, enabling more use cases



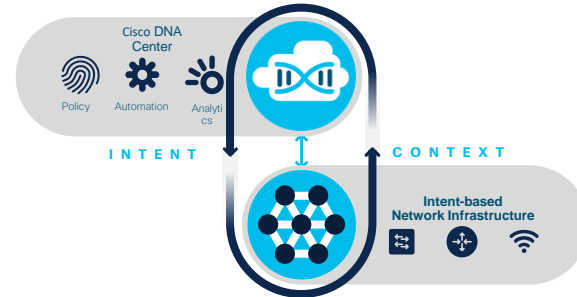
Centralized Management
Automated configuration and
IBN management

Security enforcement at network Edge



Consistent Policy
Macro & Micro segmentation

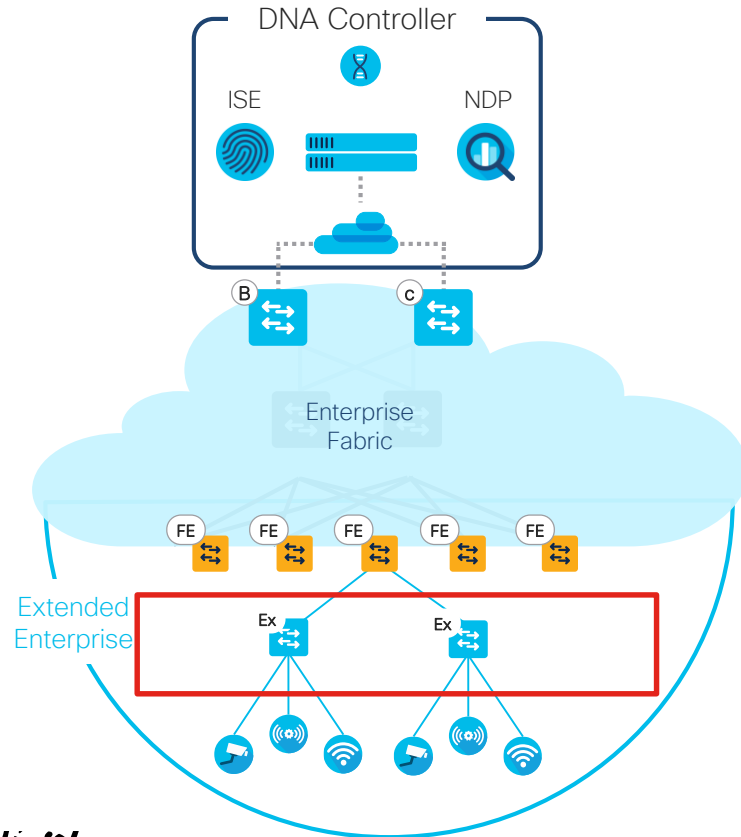
Network Admin focus on 'Intent',
and how to build Policies.



Operational Simplicity

SD – Access Architecture for IoT

Component Roles & Terminology



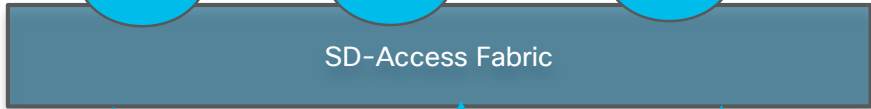
- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context.
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Control Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Extended Nodes** – A Edge access device that connects Wired IoT Endpoints to the SDA Fabric via a Fabric Edge Node

Segmentation Instru FB in Fabric

FE

FB

CP



SD-Access Fabric



Group Based Policy



DNA for Extended Enterprise – Deployment Scenarios

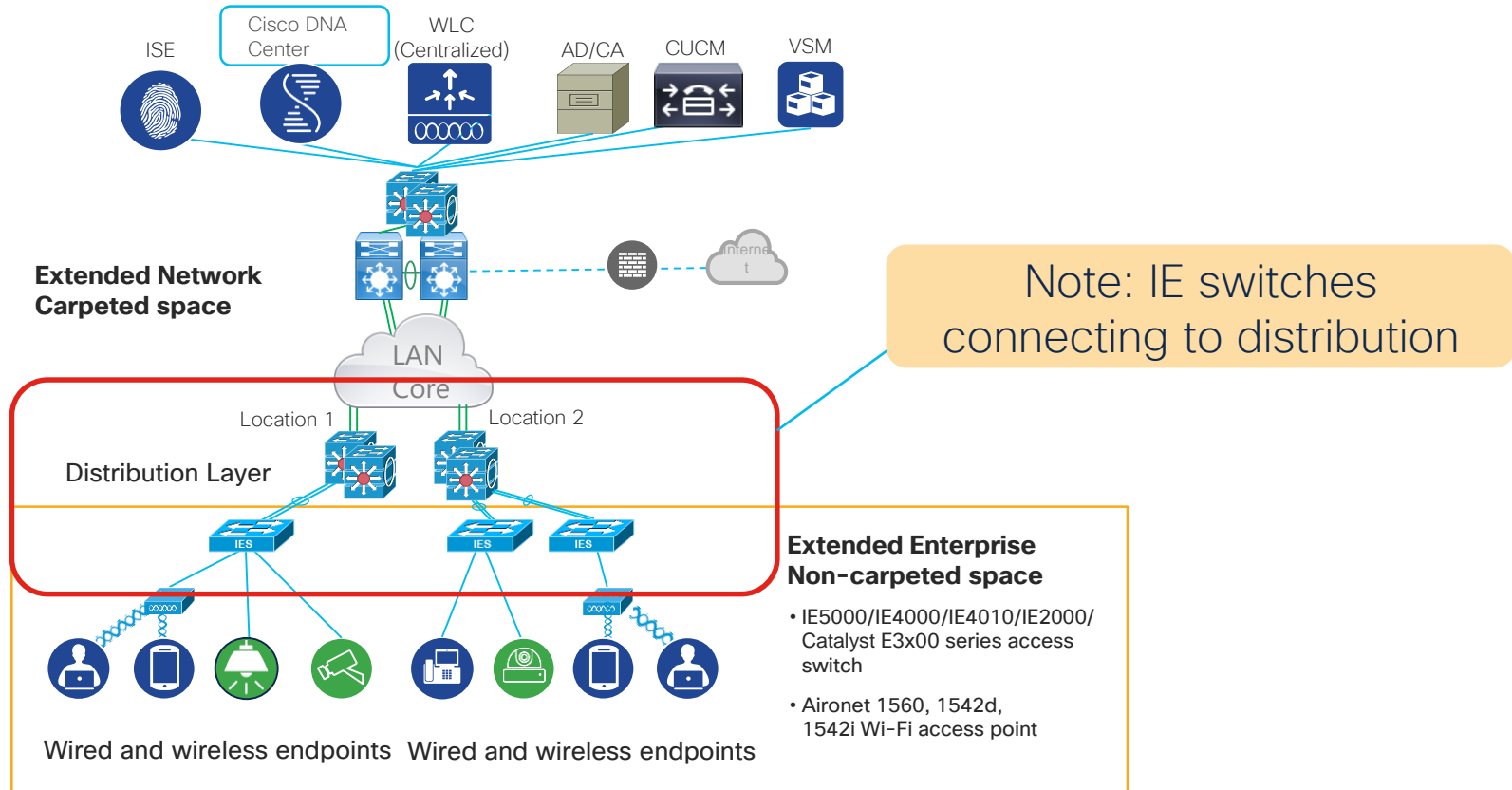
Non-SDA Fabric with Cisco DNA-C

- Traditional Network – Collapsed core or Three layer
 - DNA Centre Appliance and license

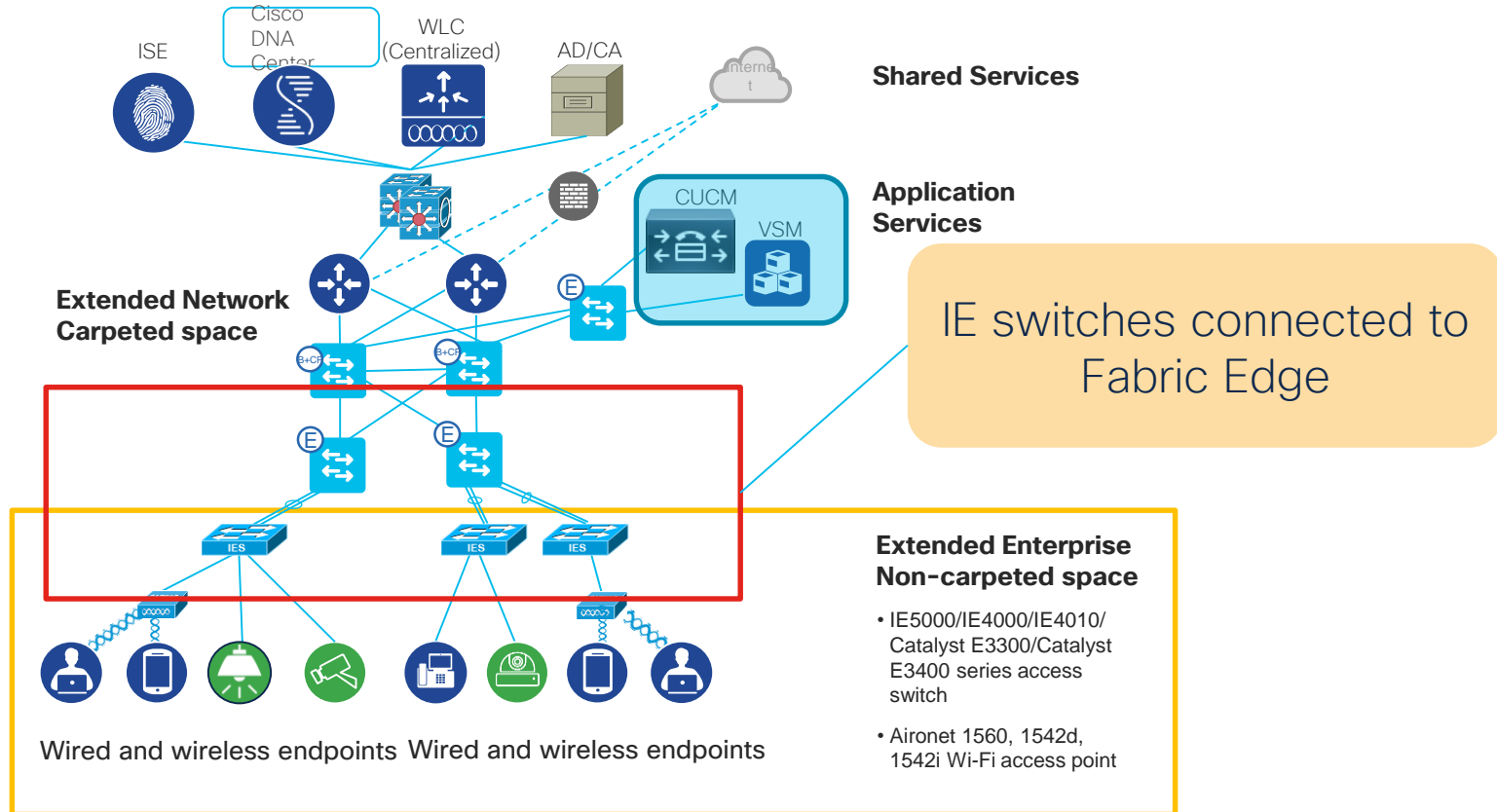
Cisco SD-Access Fabric with Cisco DNA-C

- Cisco SD-Access Fabric with Control, Border and edge nodes
 - DNA Centre Appliance and license

Non-Fabric Extended Enterprise Deployment



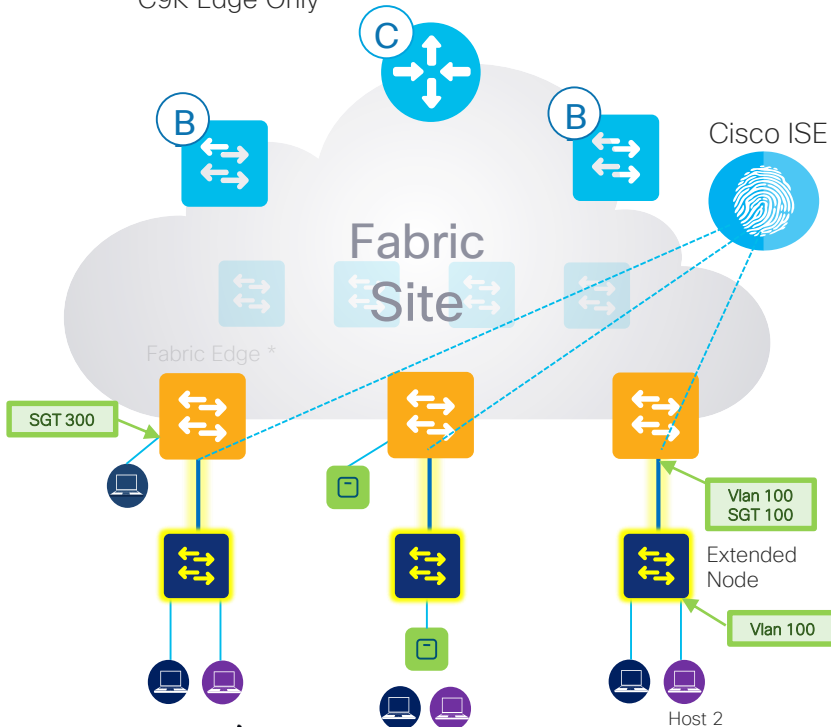
Extended Enterprise SD-Access Deployment



SD-Access Extended Node



* C9K Edge Only



- Extended node connects to a Fabric Edge node using an 802.1Q Trunk port .
- Extended node sets up using DNA-C plug & play (PNP).
- Switch ports on the Extended node are then statically assigned to an appropriate IP Pool or dynamically assigned using authentication via DNA Center.
- Policy tagging is done on the Fabric edge nodes. !!!!
- Group based policy enforcement performed also at the Fabric edge node.
- Extended node puts end devices into default SGT groups mapped to a VLAN at the Fabric edge port. SGT enforcement for Host 2 occurs on the Fabric edge egress port, not on the Ext node.

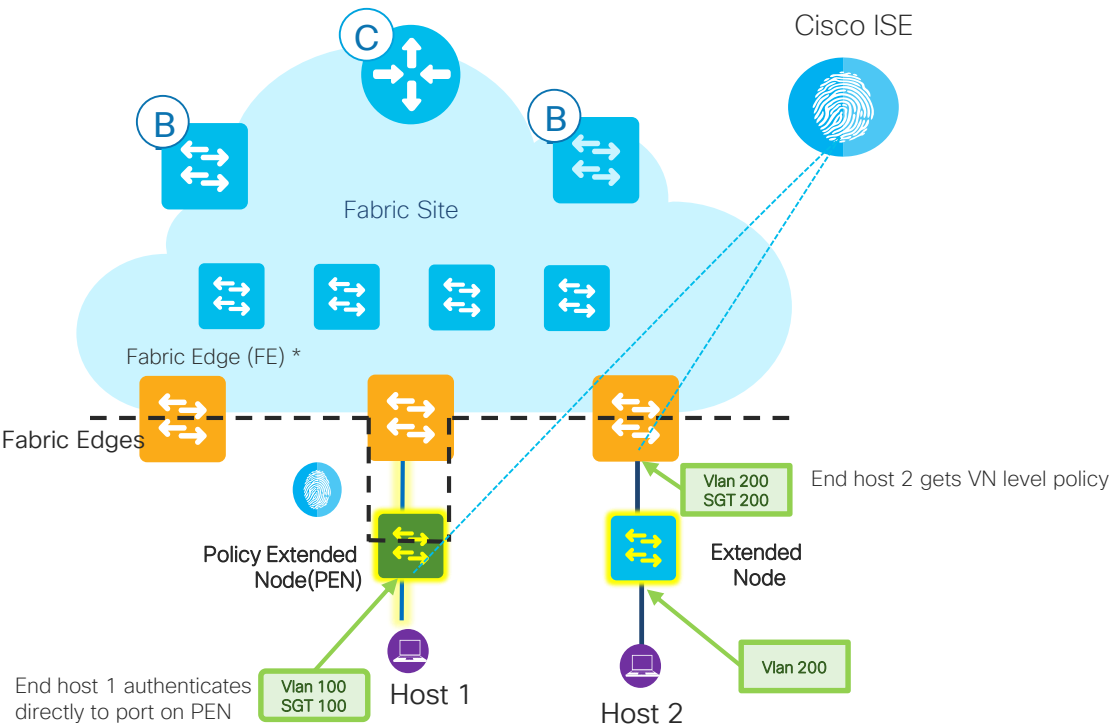
CISCO *Live!*



with Cisco DNA-C 1.3.3



SDA Security with Policy Extended Node



- **Extended Node** puts end devices in default SGT group mapped with VLAN at the FE port. Enforcement for Host 2 on FE egress port.
 - Macro Segmentation
- The *Policy Extended Node* uses 802.1x/MAB Authentication to talk directly to ISE and to download vlan and SGT attributes to the PEN switch ports per DNAC design.
- Policy Extended node performs security (SGACL) enforcement on egress interface.
 - Micro Segmentation
- Policy Extended nodes extend SGT security and L3 capabilities beyond the Fabric edge.



Extending the Enterprise with Cisco DNA Center



You make networking **possible**

Design - Step 1: Configure Global IP Range

Network Hierarchy | **Network Settings** | Image Repository | Network Profiles | Authentication Template

EQ Find Hierarchy

- Global
 - karnataka
 - UnitedStates

Network | Device Credentials | **IP Address Pools** | QoS | Wireless

IP Address Pools (2)

Filter | **Add** | Actions | SUBNET TYPE: All | IPv4 | IPv6

Name	Type	IPv4 Subnet
Global-IP-pool50	Generic	50.0.0.0/8 100% IPs available
Global-IP-pool70	Generic	70.0.0.0/8 100% IPs available

1 Assign unique IP Pool Name

2 Network Range for specific Area

3 Classful Network Mask

4 Gateway IP Address

5 Save to create new entry

Add IP Pool

IP Pool Name*
Global_Extended_Node_Pool

Type*
Generic

IP Address Space
 IPv4 IPv6

IP Subnet*
10.105.199.0

Prefix length
/24 (255.255.255.0)

Gateway IP Address
10.105.199.1

DHCP Server(s)
172.20.10.4

DNS Server(s)

Save

Global IP Pool
IP address repository for multi-function distribution purpose to Area, Site etc.
Reserve IP Pool from Area to automate extended nodes

Design - Step 2: Configure LAN Pool for Site

Find Hierarchy

- Global
 - karnataka
 - UnitedStates
 - SANFRANCISCO
 - SJ-01
 - SJ-10

IP Address Pools (2)

Filter

Reserve

SUBNET TYPE

All

IPv4 only

Dual-Stack

Name	Type	IPv4 Subnet	IPv6 Subnet
SJ-10-ip-pool1	LAN	70.70.70.0/24 63% IPs available	-
SJ-10-ip-pool2	Generic	70.70.71.0/24 0% IPs available	-

Select LAN from menu 2

Select Area Network Range 3

Showing 2 of 2

Assign Prefix 4

5 Click Reserve

Reserve IP Pool

IP Address Pool Name* **1 Assign unique LAN Pool Name**
Extended_Pool_SJ10

Type*
Generic Options

IP Address Space
 IPv4 (Default) IPv6
Check both IPv4 and IPv6 to create a dual-stack pool. If the pool is used for infra VN, or if the fabric contains devices that don't support IPv6, check only IPv4.

IPv4
Global Pool*
10.105.199.0/24 (Global_Extended_Node_Pool)
Tunnel pools are not available for reserving for Site(s).

Prefix length / Number of IP Addresses
 Prefix length Number of IP Addresses
Prefix length*
/24 (255.255.255.0)

IPv4 Subnet
10.105.199.0

Cancel **Reserve**

Provision- Step1:Enabling Fabric Extension

Cisco DNA Center

DESIGN POLICY PROVISION ASSURANCE PLATFORM

Devices ▾ Fabric Services

Fabric-Enabled Sites +

All Fabrics > SJ-10
CVD_AUTOMATION_SITE_10

EQ Find Hierarchy

▼ CVD_AUTOMATION_SITE_10

▼ UnitedStates

▼ SANFRANCISCO

SJ-10

Fabric Infrastructure Host Onboarding

> Authentication Template

▼ Virtual Networks

Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Critical Pool: Not Selected

DEFAULT_VN × INFRA_VN

Select an IP Pool for the INFRA_VN and enable it for Extended Nodes.

Edit Virtual Network: INFRA_VN

< Back

IP Address Pool
Extended_Pool_SJ10 (10.105.199....)

Pool Type ^

AP

Extended

Cancel Add

Select Pool type as Extended

Revision Step 2: Enable Fabric Edge for onboarding



Devices ▾ **Fabric** Services

Fabric-Enabled Sites +

All Fabrics > SJ-01
CVD_AUTOMATION_SITE_01

EQ Find Hierarchy

- ▾ CVD_AUTOMATION_SITE_01
 - ▾ UnitedStates
 - ▾ SANFRANCISCO
 - SJ-01 ⚙️

✔️ Fabric Infrastructure ✔️ **Host Onboarding** Show Task Status

🗑️ Clear 🔄 Refresh **Assign** Save

[A-Z](#) | [Z-A](#) | [Link Status UP](#) | [Link Status DOWN](#)

Opt: Port Channel can be assigned to Extended node

Search

- SN-FOC2330V034
- Switch-50-50-50-65
- Switch-50-50-50-70

Select All

<input type="checkbox"/> AppGigabitEthernet1/1 ↑	<input type="checkbox"/> GigabitEthernet1/1 ↓	<input type="checkbox"/> GigabitEthernet1/2 ↓	<input type="checkbox"/> GigabitEthernet1/3 ↑
<input type="checkbox"/> GigabitEthernet1/4 ↑	<input type="checkbox"/> GigabitEthernet1/5 ↓	<input type="checkbox"/> GigabitEthernet1/6 ↓	<input type="checkbox"/> GigabitEthernet1/8 ↓
<input type="checkbox"/> GigabitEthernet1/9 ↓	<input type="checkbox"/> GigabitEthernet1/10 ↓	<input checked="" type="checkbox"/> Port-channel1 ↑ EXTENDED_NODE	

Port Assignment ✕

Selected Interfaces (1)
Port-channel1

Connected Device Type
Extended Node ⓧ ▾

Description

Extending the Enterprise with Cisco DNA Center

Plug and Play

Cisco DNA Center DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices Fabric

Inventory **Plug and Play**

Plug and Play Devices (18)

Last updated: 1:04 pm Refresh Add

Filter Actions

EQ Find

<input type="checkbox"/>	Name	Serial Number	Product ID	Source	State	Site	Last Contact	
<input type="checkbox"/>	FDO1726T0FC	FDO1726T0FC	IE-2000-16PTC-G-NX	Network	Unclaimed	N/A	05/07/2019 17:04:09 UTC	
<input type="checkbox"/>	FDO2019U0CC	FDO2019U0CC	IE-5000-12S12P-10G	Network	Provisioned	Global/SJC/SJC-Building8	05/07/2019 13:47:18 UTC	
<input type="checkbox"/>	FDO2247J06F	FDO2247J06F	IE-4000-4S8P4G-E	Network	Provisioned	Global/SJC/SJC-Building8	05/07/2019 13:48:07 UTC	
<input type="checkbox"/>	IE4000-BLD12-1	FDO2247J6PB	IE-4000-8GT8GP4G-E	User	Provisioned	Global/SJC/SJC-Building12/SJC-BLD12-F1	05/05/2019 19:01:17 UTC	
<input type="checkbox"/>	IE3300-BLD12-2	FOC2312V0K7	IE-3300-8T2S	User	Provisioned	Global/SJC/SJC-Building12/SJC-BLD12-F1	05/07/2019 16:24:30 UTC	
<input type="checkbox"/>	IE3300-BLD12-1	FOC2310V0P0	IE-3300-8T2S	User	Provisioned	Global/SJC/SJC-Building12/SJC-BLD12-F1	05/07/2019 16:25:30 UTC	

Cisco SD-WAN for Remote Sites

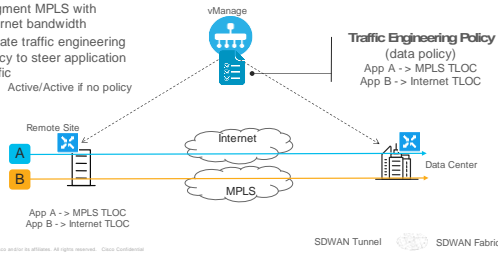


You make networking **possible**

Cisco SD-WAN Use Cases

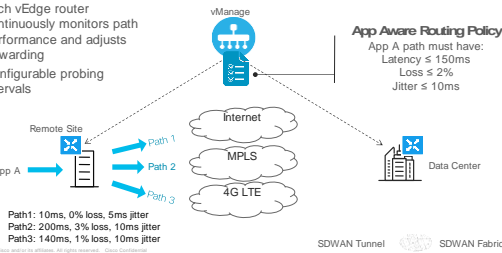
Bandwidth Augmentation

- Augment MPLS with Internet bandwidth
- Create traffic engineering policy to steer application traffic
 - Active/Active if no policy



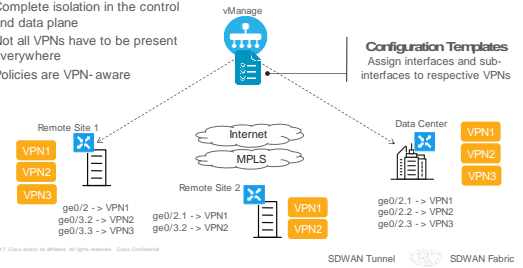
Critical Applications SLA

- Each vEdge router continuously monitors path performance and adjusts forwarding
- Configurable probing intervals



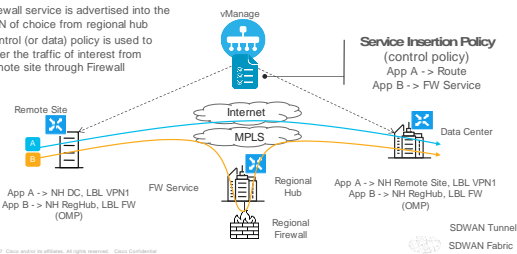
Secure Segmentation

- Complete isolation in the control and data plane
- Not all VPNs have to be present everywhere
- Policies are VPN-aware



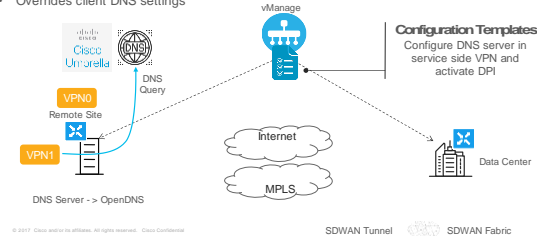
Regional Secure Perimeter

- Firewall service is advertised into the VPN of choice from regional hub
- Control (or data) policy is used to steer the traffic of interest from remote site through Firewall



DIA & DCA

- DNS-based security
- Overrides client DNS settings

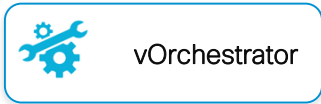


IR1101 – The Next Generation Industrial ISR w SD-WAN



Cisco SDWAN Fabric Overview

Orchestration Plane
assists in the automatic onboarding of the SD-WAN routers into the SD-WAN overlay



vManage v19.2

- centralized network management system
- provides a GUI interface to monitor, configure, and maintain all Cisco SD-WAN devices and links in the underlay and overlay network



Management Plane
(Multi-tenant or Dedicated) for central configuration and monitoring.



vBond Orchestrator

- performs the initial authentication of Edge devices and orchestrates vSmart and Edge connectivity.
- Plays a role in enabling the communication of devices that sit behind NAT



Control Plane
builds and maintains the network topology and makes decisions on where traffic flows



vSmart Controller

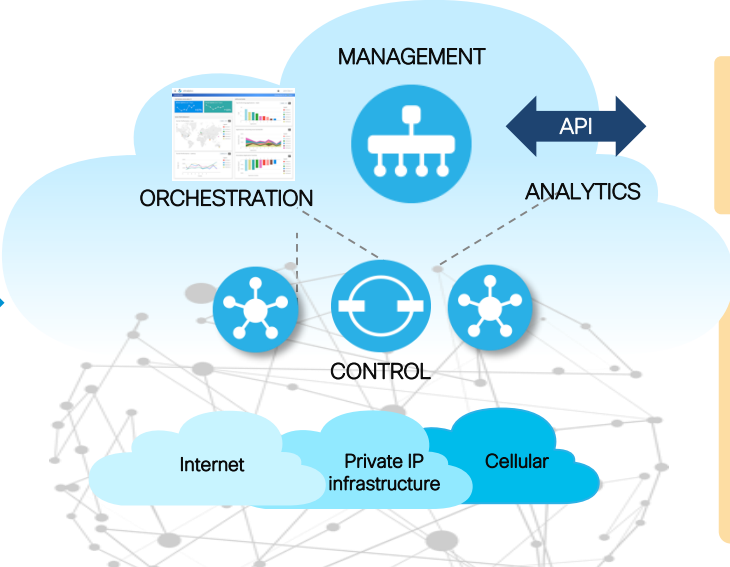
- responsible for the centralized control plane of the SD-WAN network.
- establishes a secure connection to each Edge router and distributes routes and policy information via the Overlay Management Protocol (OMP)
- acts as a route reflector.
- orchestrates the secure data plane connectivity between the Edge routers by distributing crypto key information, allowing for a very scalable, IKE-less architecture



Data Plane
(Physical or Virtual) for forwarding packets based on decisions from the control plane



Data Center ASR1K/ ISR4K/ CSR1Kv #CLUS Campus Cisco ISR 1100 Branch Home Office IOT IR1101 IOS-XE 16.12



Extended Enterprise Cisco Validated Design (CVD) Guide

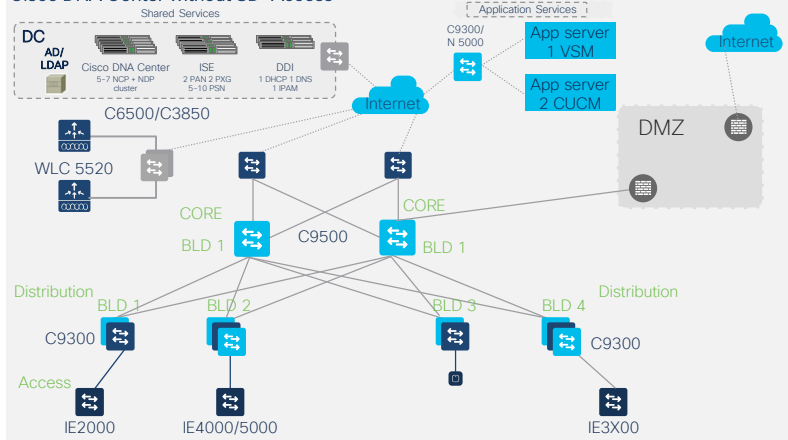


You make multi-cloud **possible**

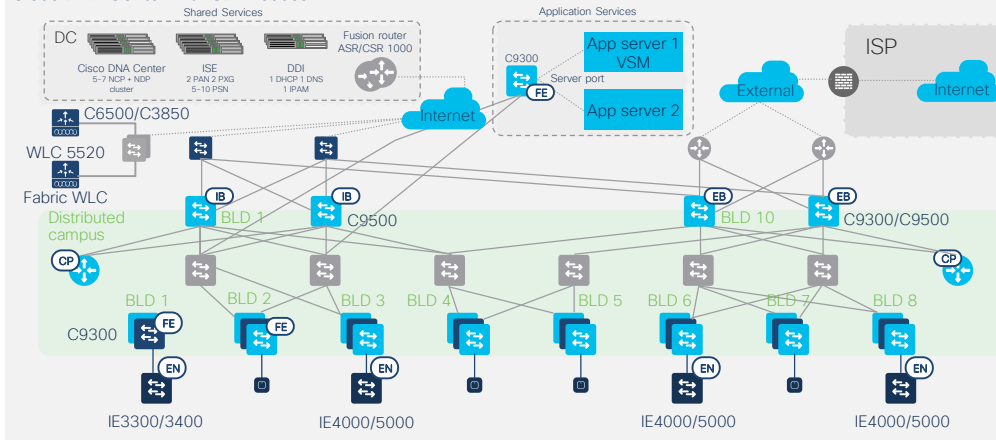
Extended Enterprise CVD

“Connect” with or without SD-Access fabric

Cisco DNA Center without SD-Access



Cisco DNA Center with SD-Access



A Connect design

0 Connect services

- Cisco DNA Center (central management)
- DNS, DHCP, and IPAM
- Shared application services

1 Wired

- Extended access network
- Core, distribution network
- Internet breakout via DMZ

2 Wireless

- Centralized WLC
- Ruggedized access points

3 Scale, redundancy

- Small, medium, large
- Device and link redundancy
- QoS for extended traffic

B Policy design

0 Policy services

- Identity Services Engine
- Outside ID services

1 Identity

- Device profiling
- 802.1X/MAB authentication

2 Segment

- North-south traffic flows
- East-west traffic flows

3 Policy

- Firewall rules
- Access policies
- Application policies

Summary and Key Takeaways



You make networking **possible**

Summary

- There are many business benefits to extending the enterprise
- Non-carpeted environments require purpose-built hardware
- New ruggedized IoT networking platform run on IOS XE
 - Just like other Cisco routers and switches
 - As such, these have compatible features and the same programmable interfaces
- Extended enterprise networks can be managed with the same single pane-of-glass as the enterprise network: Cisco DNA Center
- Cisco provides extensive design guidance to extend your enterprise

