© 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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

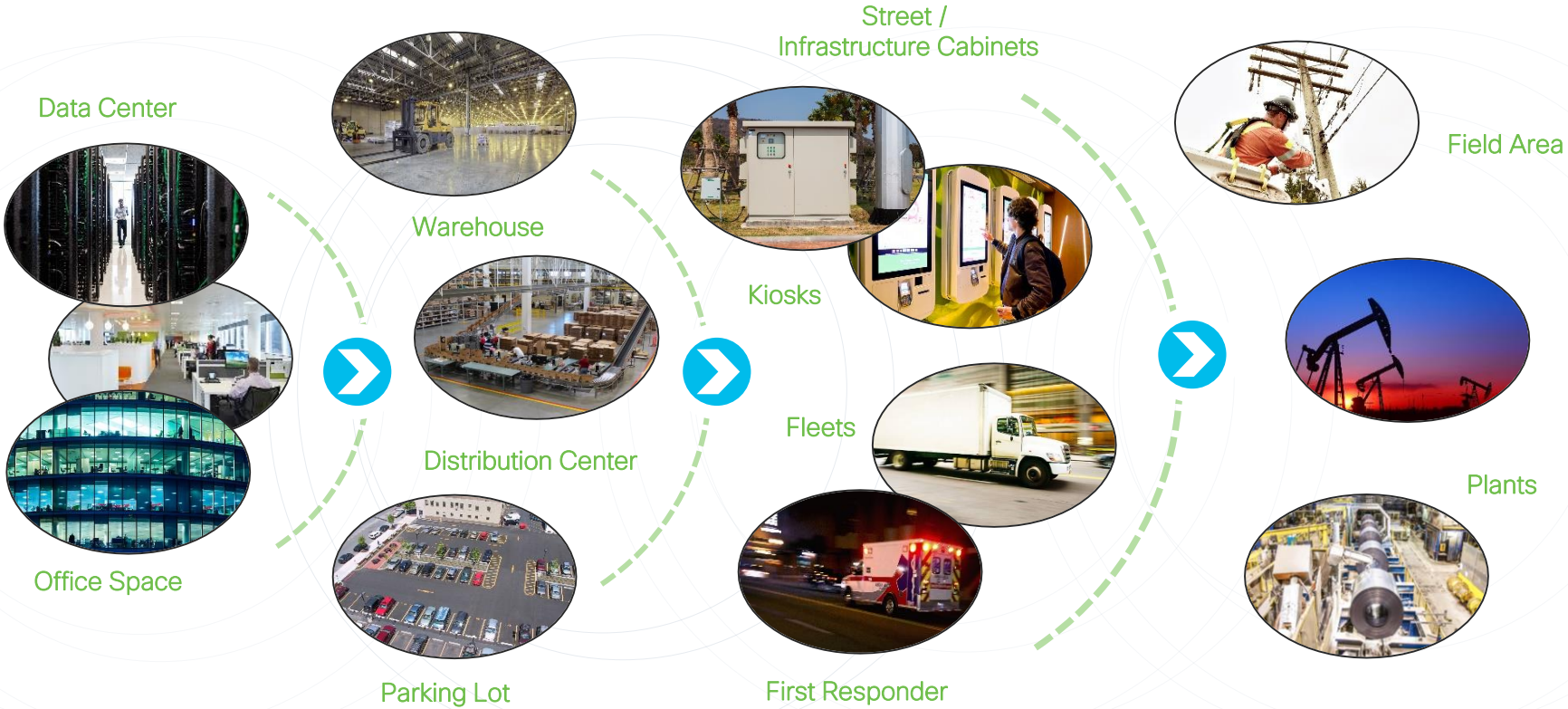
Why Extend the Enterprise?

You make networking **possible**

IoT is Digitally Transforming Business

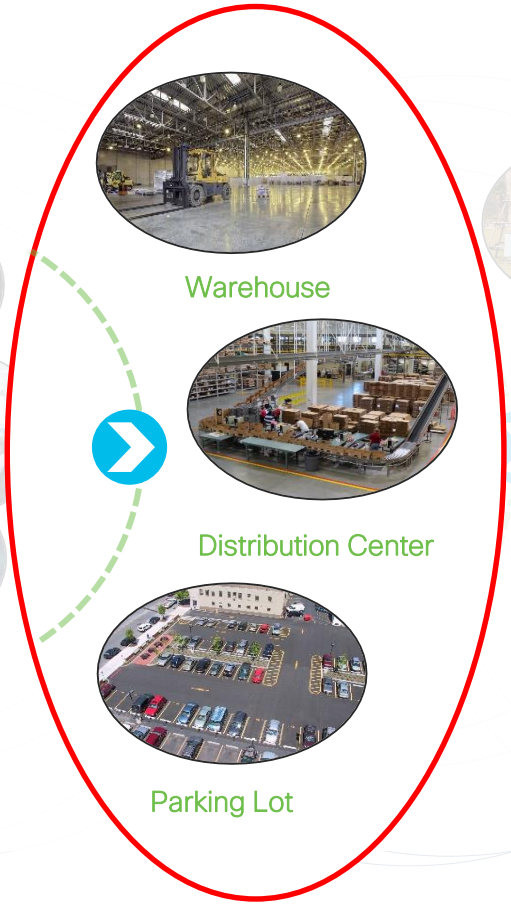
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

As a Result, the Network Boundary is Being Increasingly Extended



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

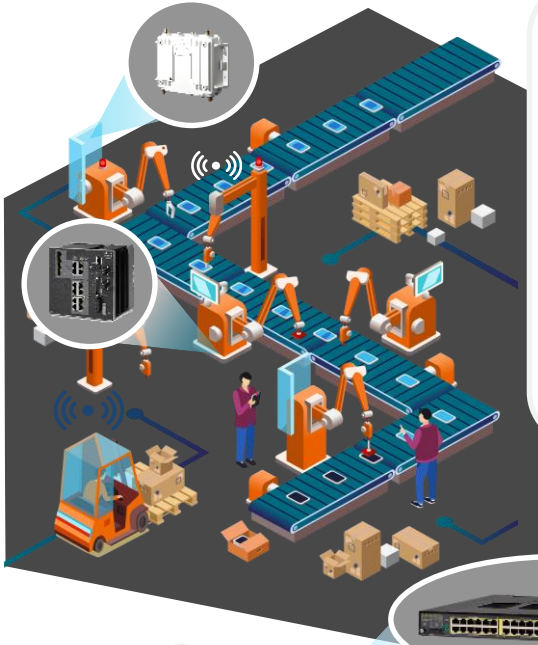
Area of Focus for this Session: The Extended Enterprise



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extended Enterprise Use-Cases

Smart Warehouses and Distribution Centers

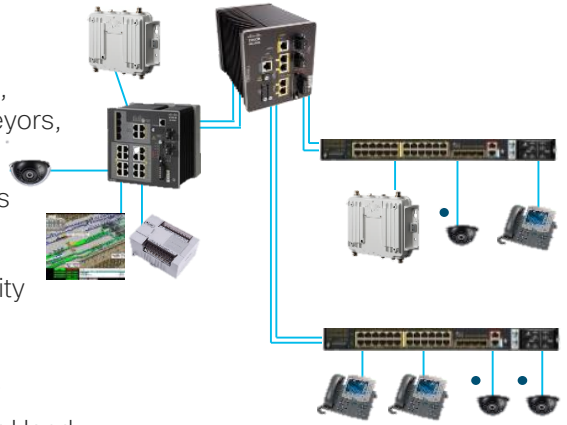


Why?

- 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?

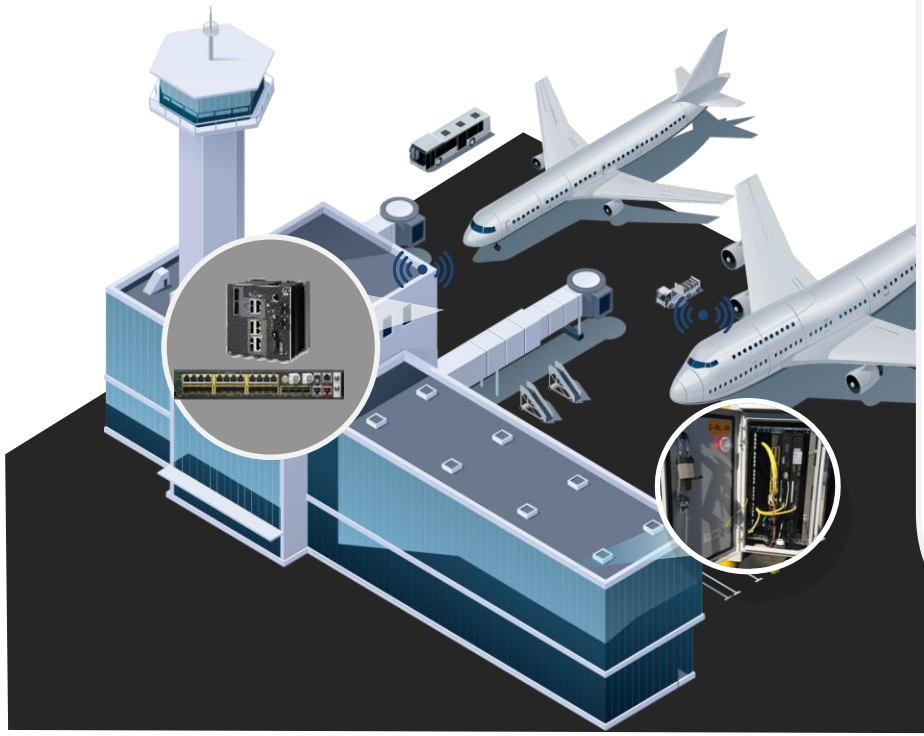
- Tags, Trackers, Sorters, Conveyors, etc.
- Safety cameras
- Wi-Fi APs
- Safety & security systems
- Laptops / Smartphones / Tablets / Other Hand-Held devices



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extended Enterprise Use-Cases

Connected Airports

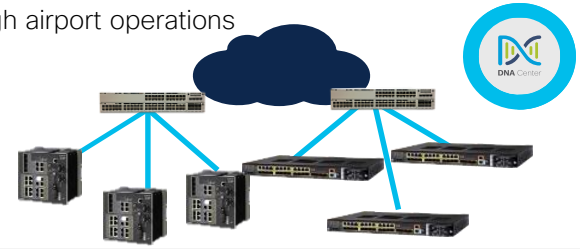


Why?

- 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



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Platform Choices: Why Not use Catalyst?

You make the power of data **possible**

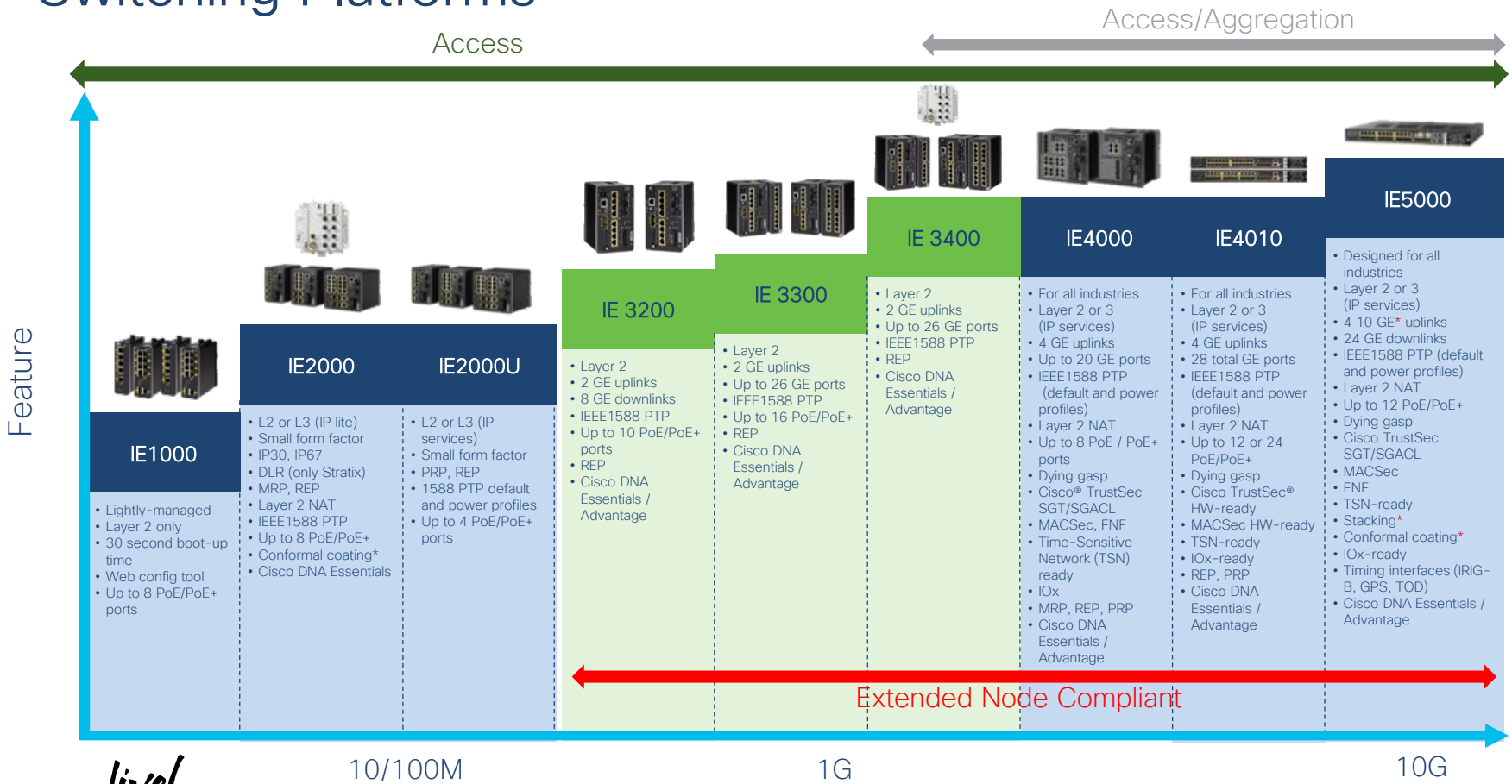
IOT Use Cases Are Different

Choose Hardware to Meet Requirements

- Size weight form-factor
- Shock and vibration
- High MTBF resilient network topologies
- Din-rail or rack mounts
- Extended Temperature Range (-40 – 75℃) Fanless and Self-Cooled
- Industry Safety and Stds certifications

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extending the Enterprise with Industrial Ethernet Switching Platforms



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-Access for Extended Network

You make multi-cloud **possible**

Cisco live!

Why Cisco SDA for Extended Nodes?

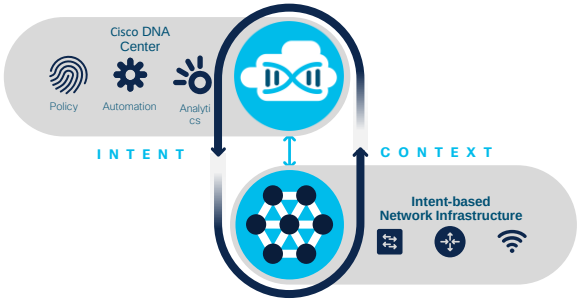
Common workflow, enabling more use cases

Centralized Management
Automated configuration and IBN management

Security enforcement at network Edge

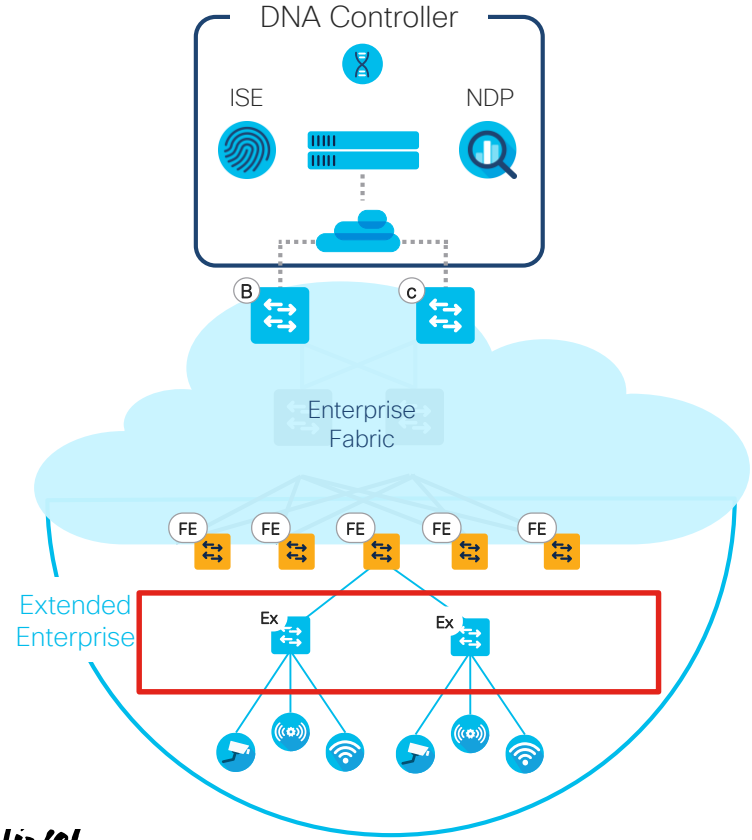
Consistent Policy
Macro & Micro segmentation

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



Operational Simplicity

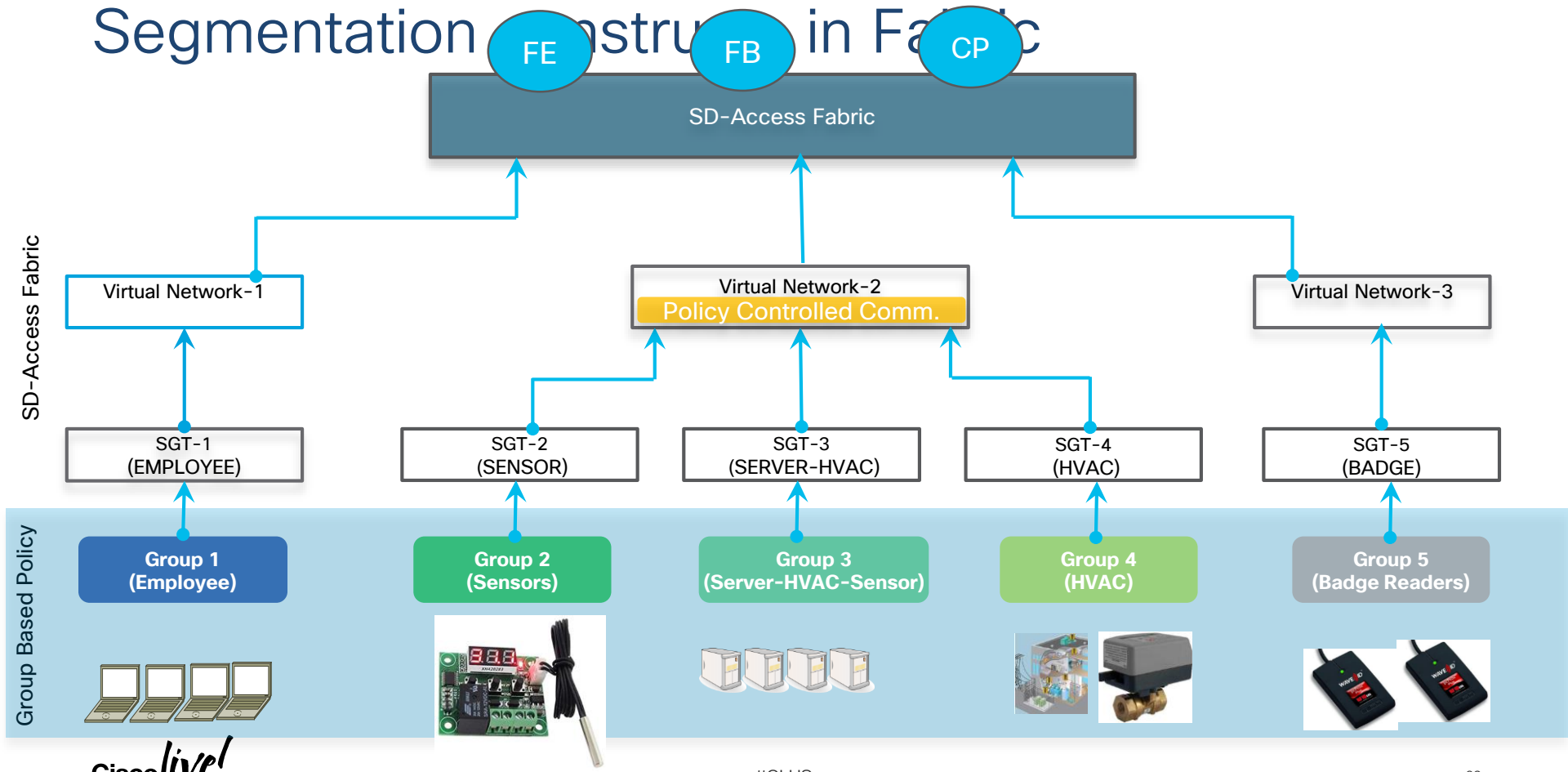
SD – Access Architecture for IoT
Component Roles & Terminology



- **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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Segmentation Constructs in Fabric



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

DNA for Extended Enterprise – Deployment Scenarios

Non-SDA Fabric with Cisco DNA-C

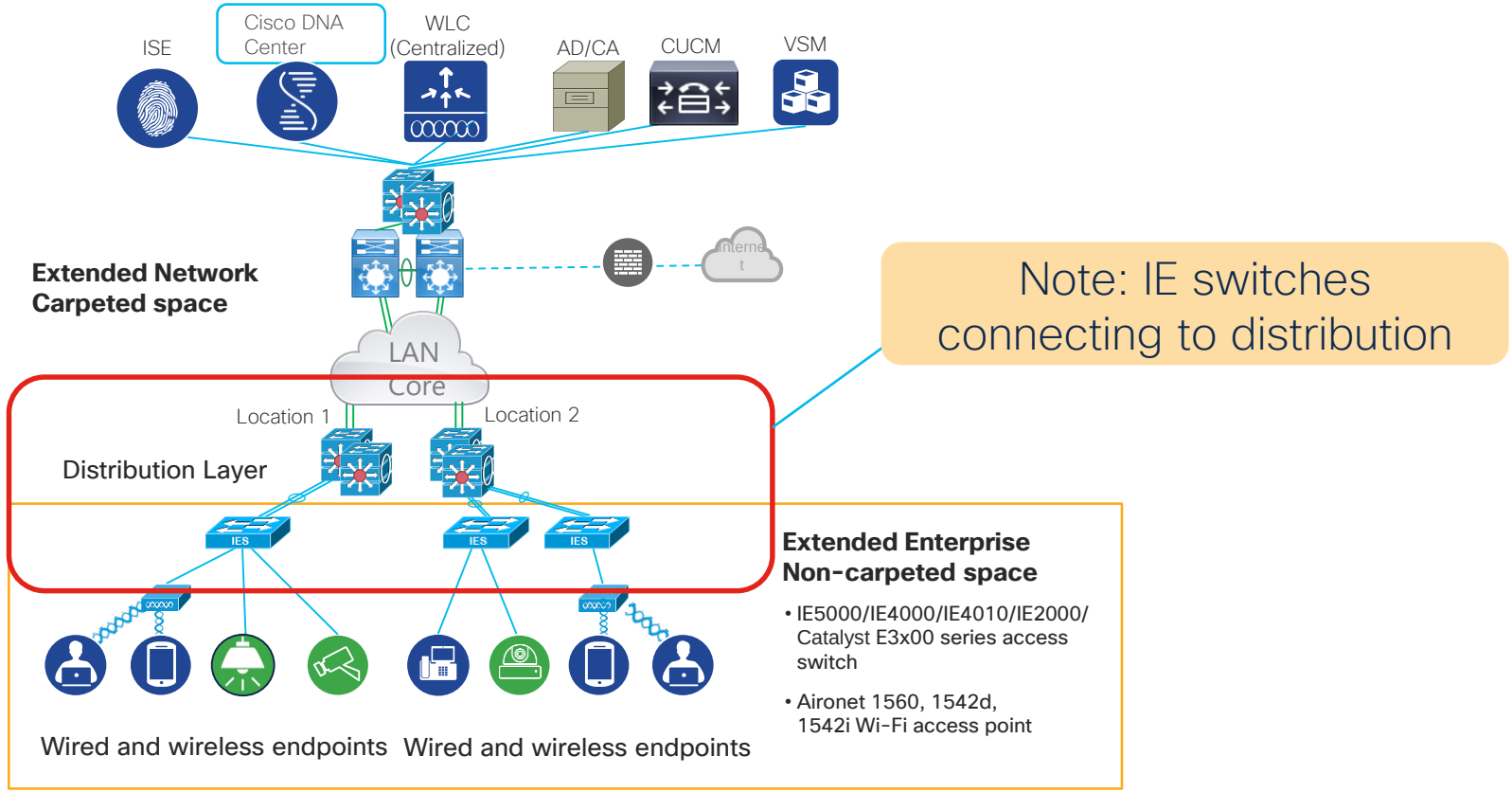
- Traditional Network – Collapsed core or Three layer
- DNA Centre Appliance and license

Cisco SD-Access Fabric with Cisco DNA-C

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

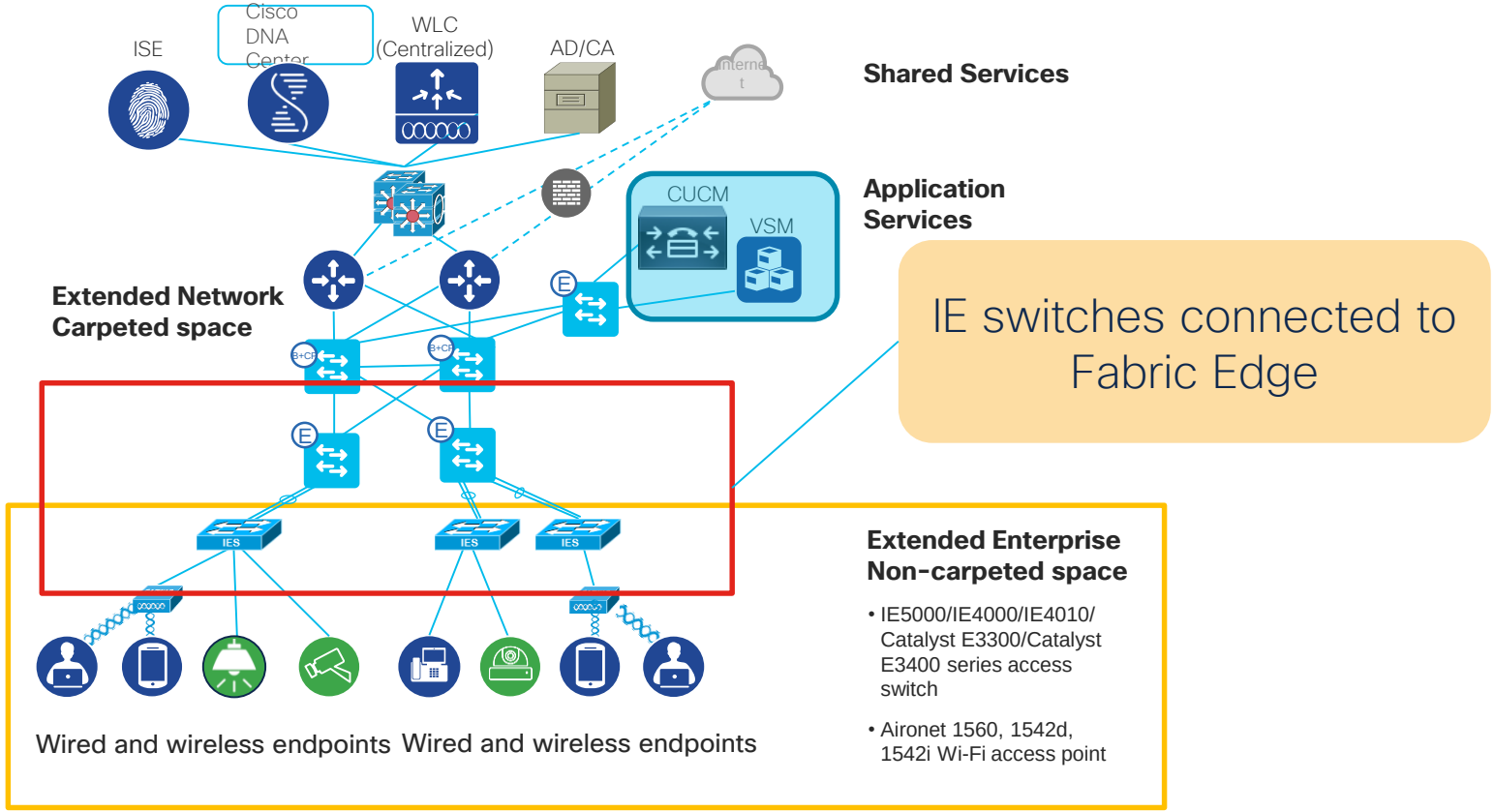
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Non-Fabric Extended Enterprise Deployment



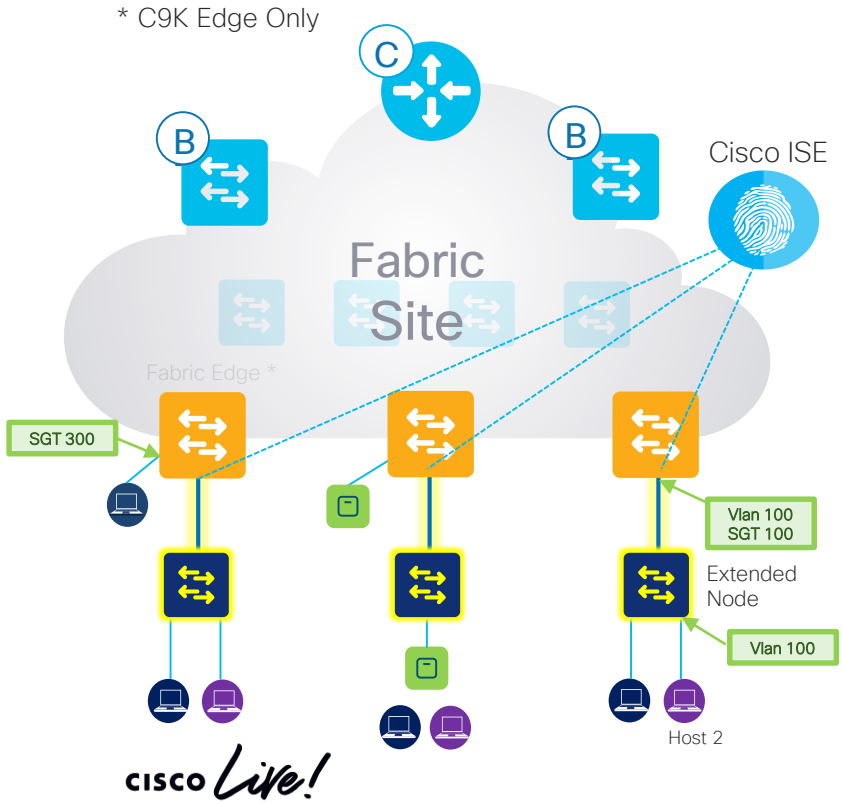
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extended Enterprise SD-Access Deployment



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-Access Extended Node



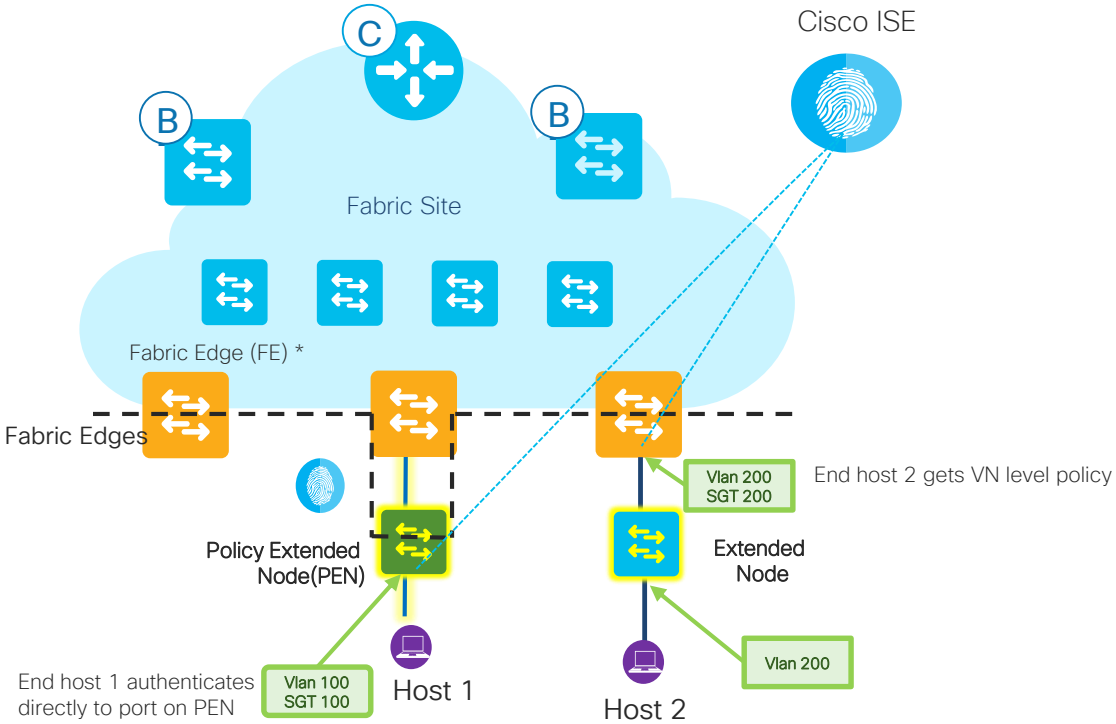
- Extended node connects to a Fabric Edge node using an 802.1Q Trunk port .
- Extended node sets up using DNA-C plug & play (PNP).
- Switch ports on the Extended node are then statically assigned to an appropriate IP Pool or dynamically assigned using authentication via DNA Center.
- Policy tagging is 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.

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

NEW

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.

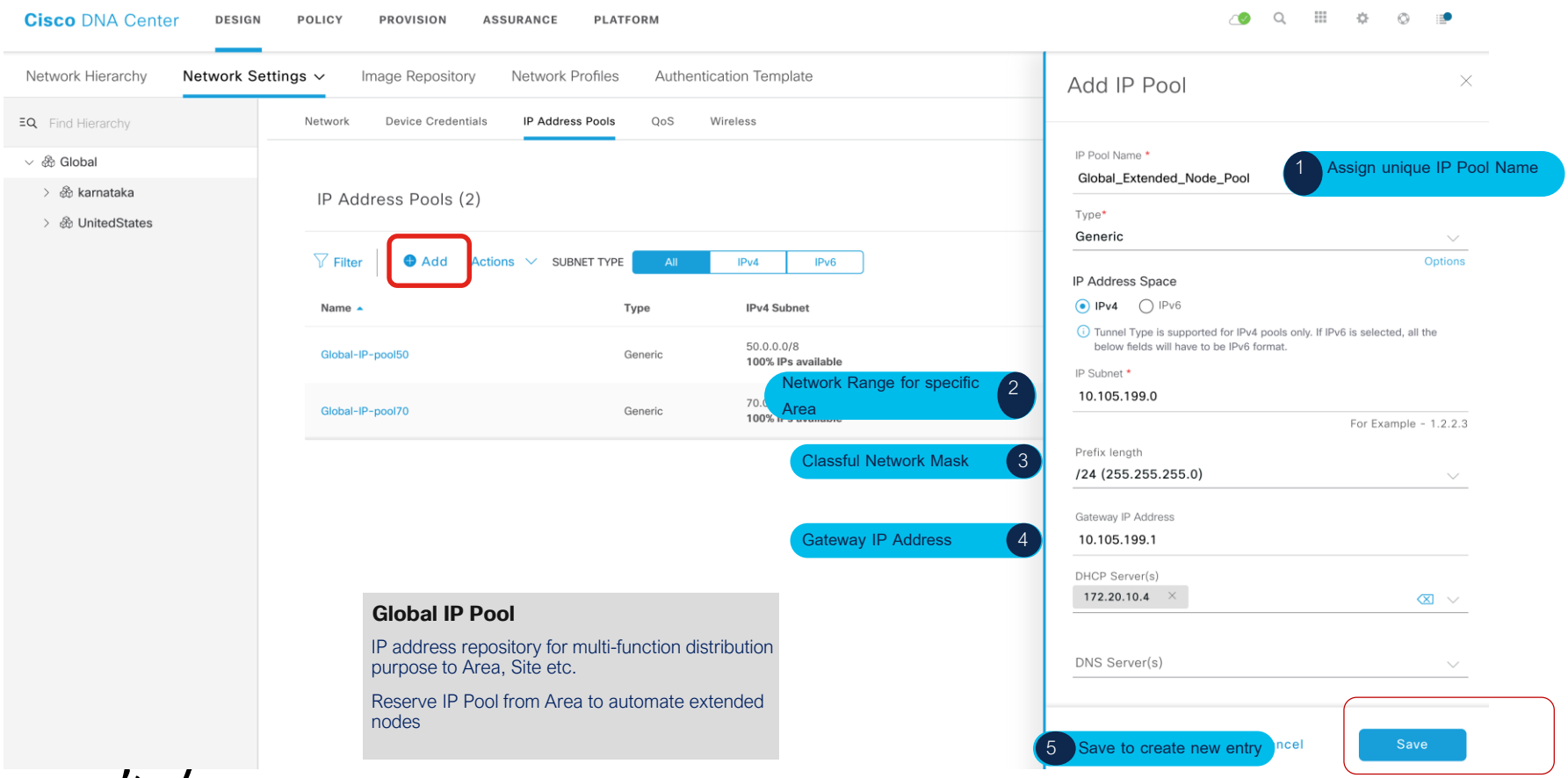
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extending the Enterprise with Cisco DNA Center

You make networking **possible**

Cisco live!

Design –Step1: Configure Global IP Range



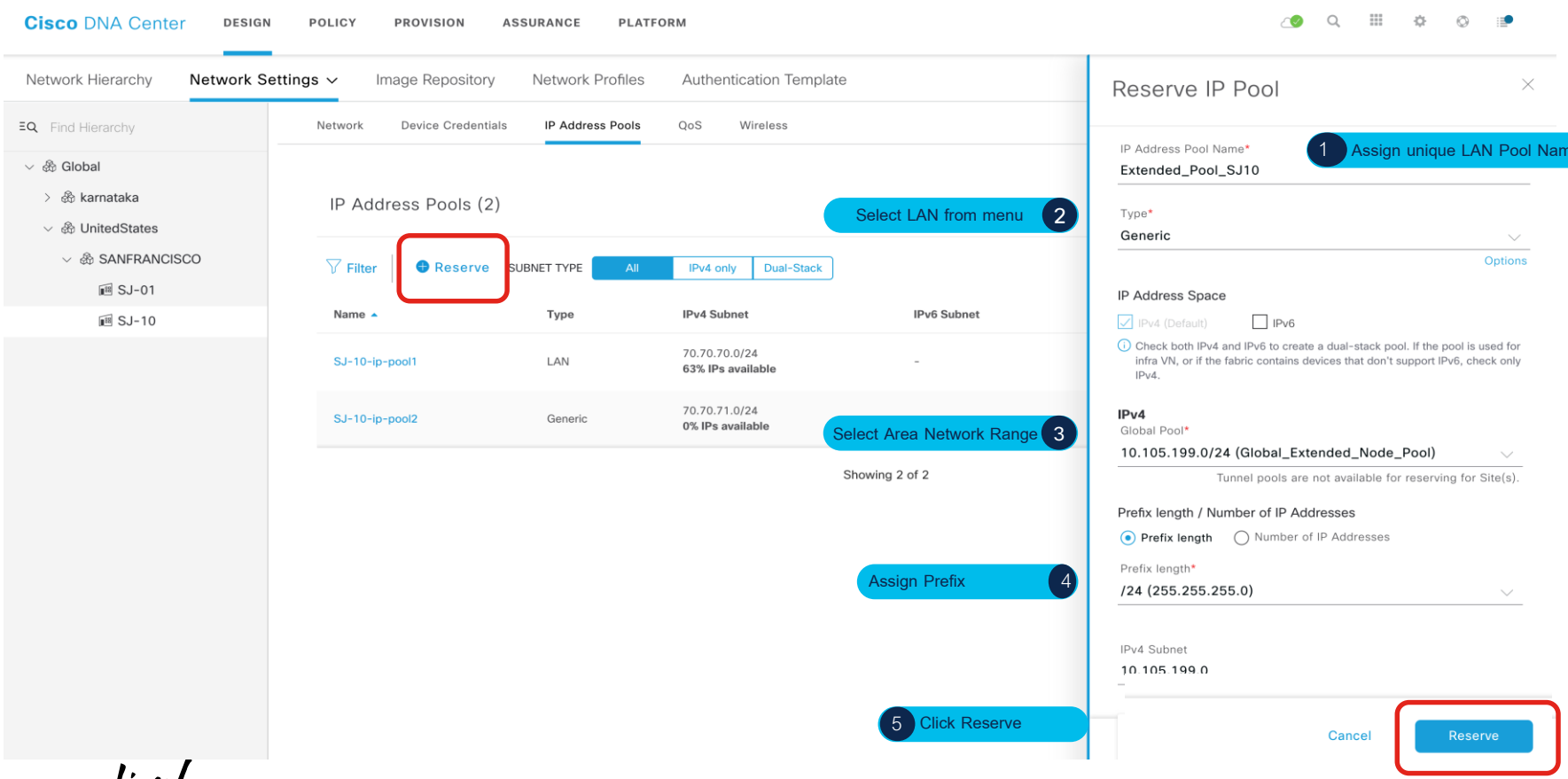
Global IP Pool

IP address repository for multi-function distribution purpose to Area, Site etc.

Reserve IP Pool from Area to automate extended nodes

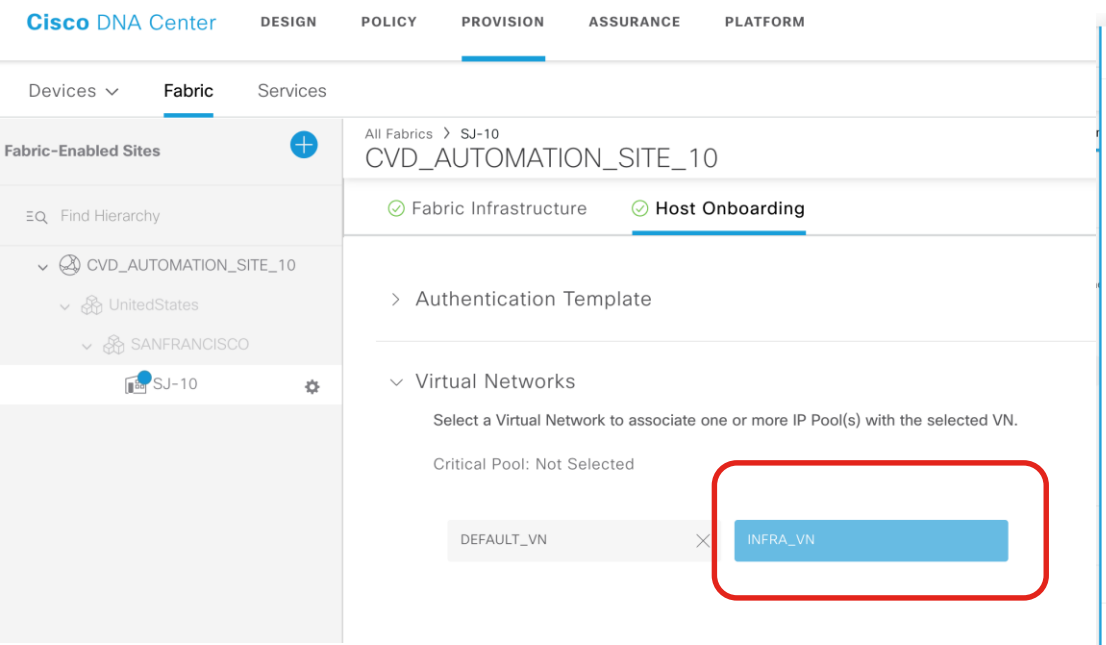
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

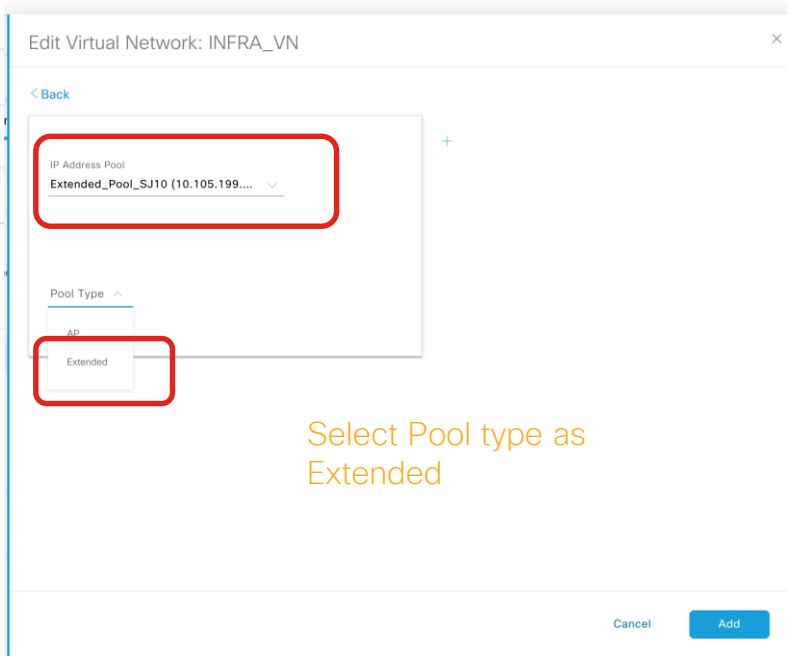
Design –Step2: Configure LAN Pool for Site



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Provision- Step1:Enabling Fabric Extension



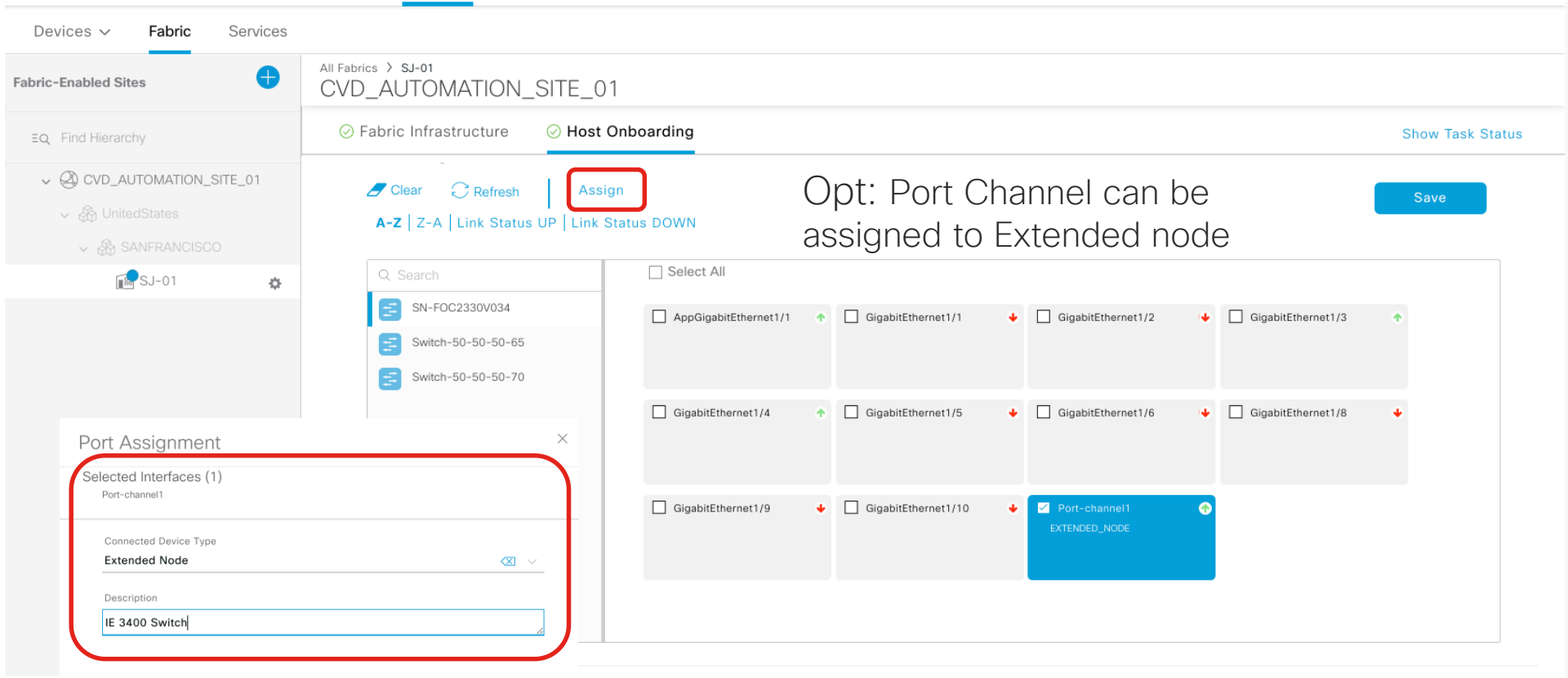


Select Pool type as Extended

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

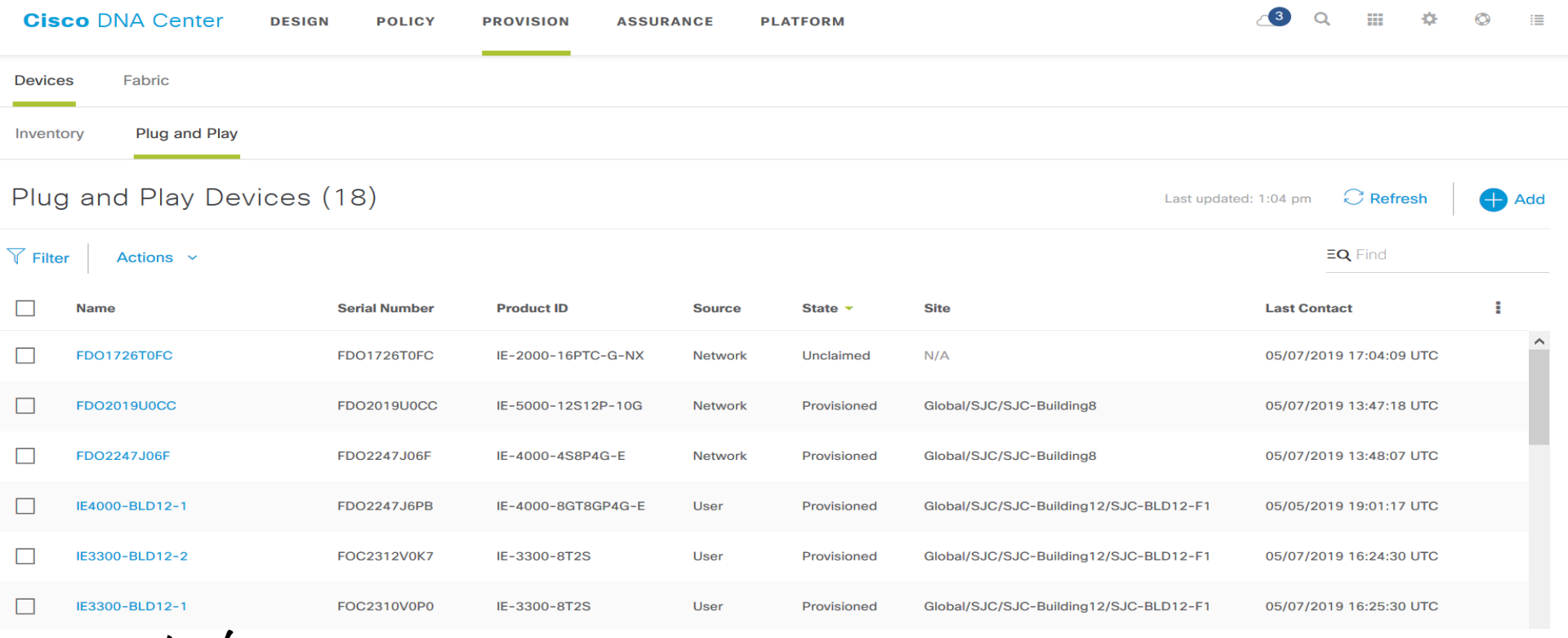
Provision - Step2: Enable Fabric Edge for on boarding



 © 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extending the Enterprise with Cisco DNA Center

Plug and Play



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco SD-WAN for Remote Sites

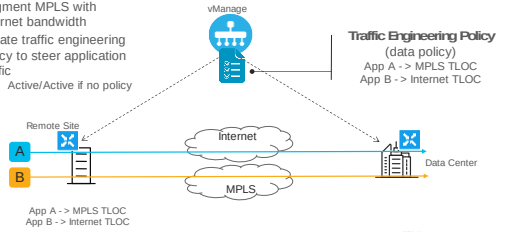
You make networking **possible**

Cisco live!

Cisco SD-WAN Use Cases

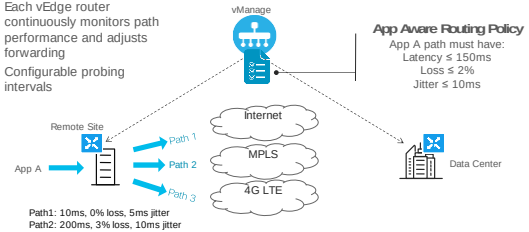
Bandwidth Augmentation

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



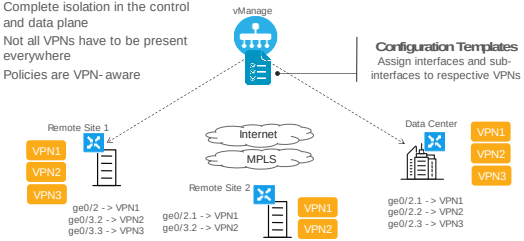
Critical Applications SLA

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



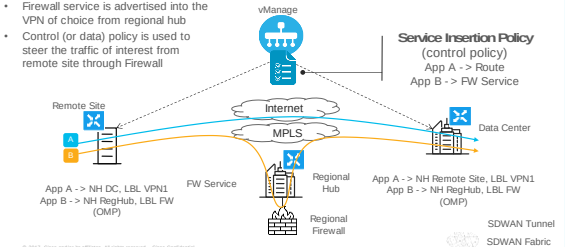
Secure Segmentation

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



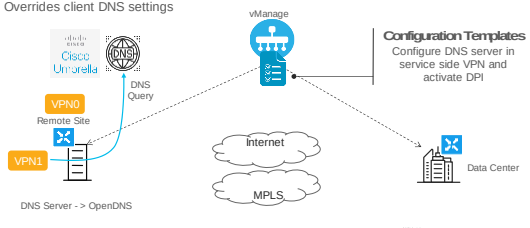
Regional Secure Perimeter

- 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



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IR1101 – The Next Generation Industrial ISR w SD-WAN

Expansion modules for more interfaces

First IoT Router with IOS XE
High-end security Programmability

Modular LTE & 5G Ready

Edge computing enabled

Low average Power consumption of only 10W

SD-WAN Shipping NOW

Compact form factor for cabinet installations

Investment protection

Lower TCO

Extended product life time

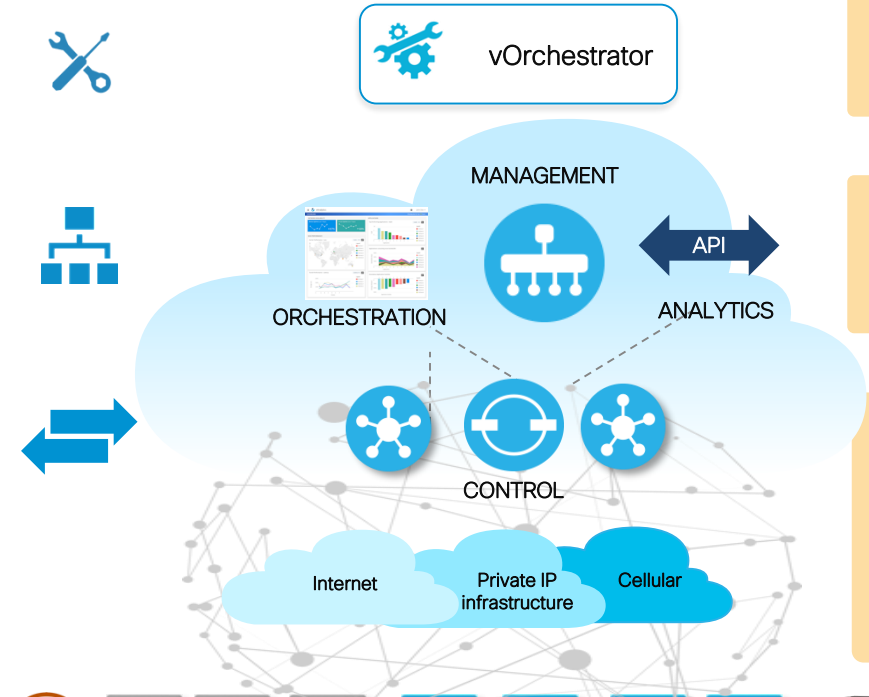
Cisco SDWAN Fabric Overview

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

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

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

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



Data Center
ASR1K/ ISR4K/ CSR1Kv

Campus

Branch
Cisco ISR 1100

Home Office

IOT
IR1101 IOS-XE 16.12

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

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

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

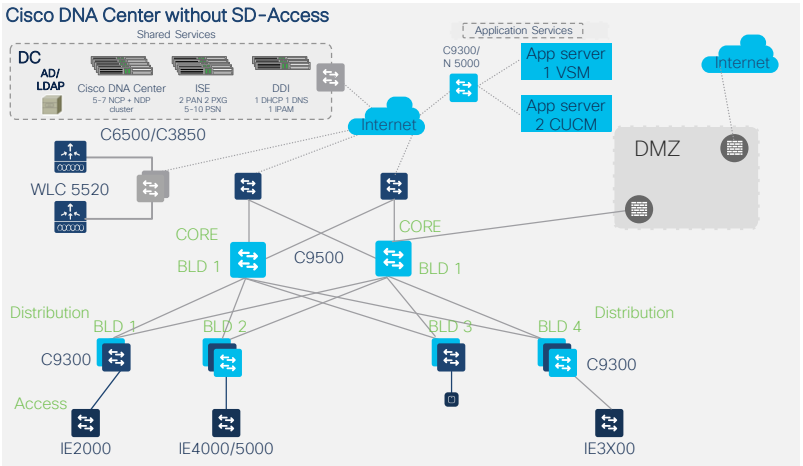
Extended Enterprise Cisco Validated Design (CVD) Guide

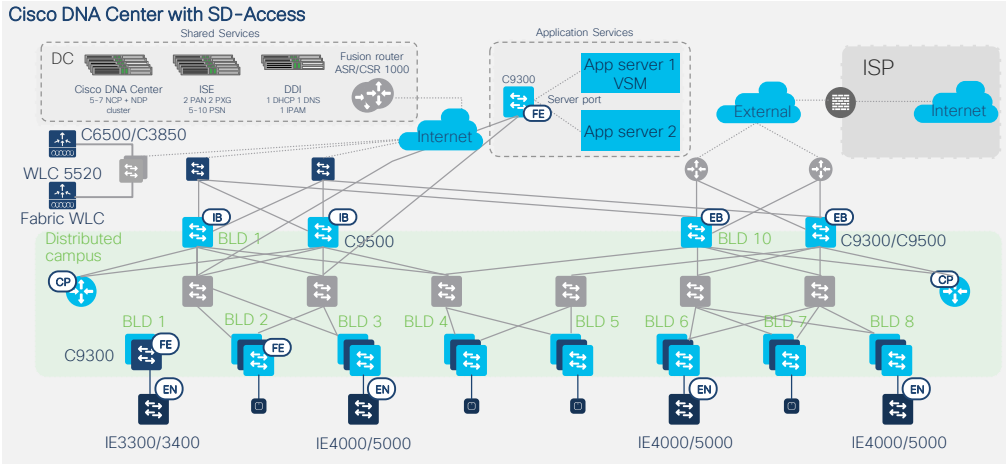
You make multi-cloud **possible**

Cisco live!

Extended Enterprise CVD

"Connect" with or without SD-Access fabric





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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public


CISCO