CISCO Live!

ALL IN

#CiscoLive

The bridge to possible

Extending Your SD-WAN Network to the Great Outdoors

Extending Cisco SD-WAN for Advanced Metering Infrastructure (AMI) , Utilities, Remote and Mobile Assets

Emmanuel Tychon
@ManuNetworking

BRKIOT-2011

Cisco Webex App

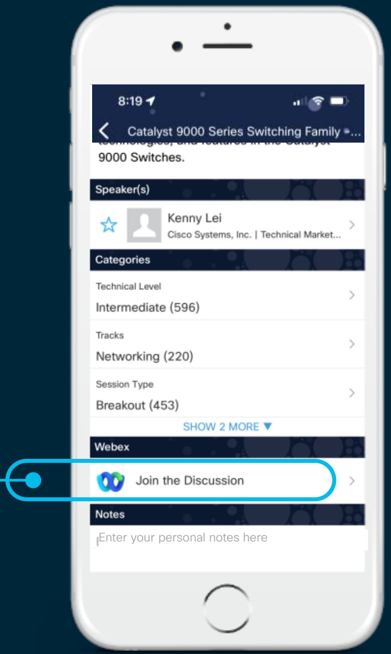
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKIOT-2011

Assumptions for this session

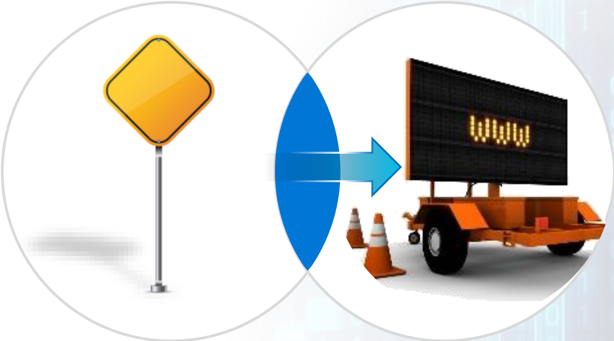
1. You already have an enterprise **SD-WAN** core network in place
2. You want to **extend** this network **outside the carpeted space**
3. Gateways can in the **“great outdoors” over Cellular**
4. You want to use Cisco IoT gateways in **rugged environments**
5. You want to **manage those gateways at scale** (multiple thousands)
6. This session is NOT about outdoor WiFi radio access network

Agenda

1. Use Cases for Extending the Network
2. SD-WAN Challenges outside carpeted spaces
3. Managing IoT Gateways without SD-WAN
4. How to extend the SD-WAN Network?
5. Building Blocks : vManage and FND or IoT OD

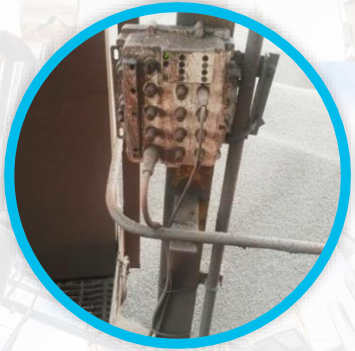
Extending the Network Use Cases

Digitization requires Enterprise Applications to communicate to all assets



Enterprises are converging to an IP / Ethernet / Wireless Networks

Cisco IoT Gateways Purpose-Built for Harsh Environments



1 Size Weight Form-Factor

2 Shock and Vibration

3 High MTBF Resilient Network Topologies

4 Din-Rail or Rack Mounts

5 Fanless -40 to 75°C Self-cooled

6 Industry Certifications

IoT Networking + Security Portfolio

Industrial Switching
1K, 2K, 3200, 3300, 3400, 3400H, 4K, 5K

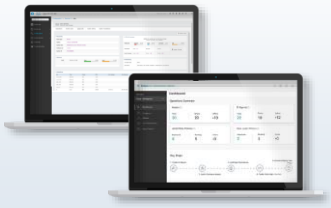
Industrial Routing
IR1101, IR1800, IR8100, IR8300, CGR1120, CGR1240, CGR2010, IoT Gateways (IG21, IG21R, IG31R)

Embedded Networking
ESS, ESR, ESW, Resilient Mesh

Industrial Wireless
Cisco Ultra-Reliable Wireless Backhaul, IW6300, IW3702, IR5XX, IXM Gateway

Industrial Cybersecurity
Cyber Vision, ISA3000 Firewall

Data Control and Exchange
Edge Intelligence, IOx

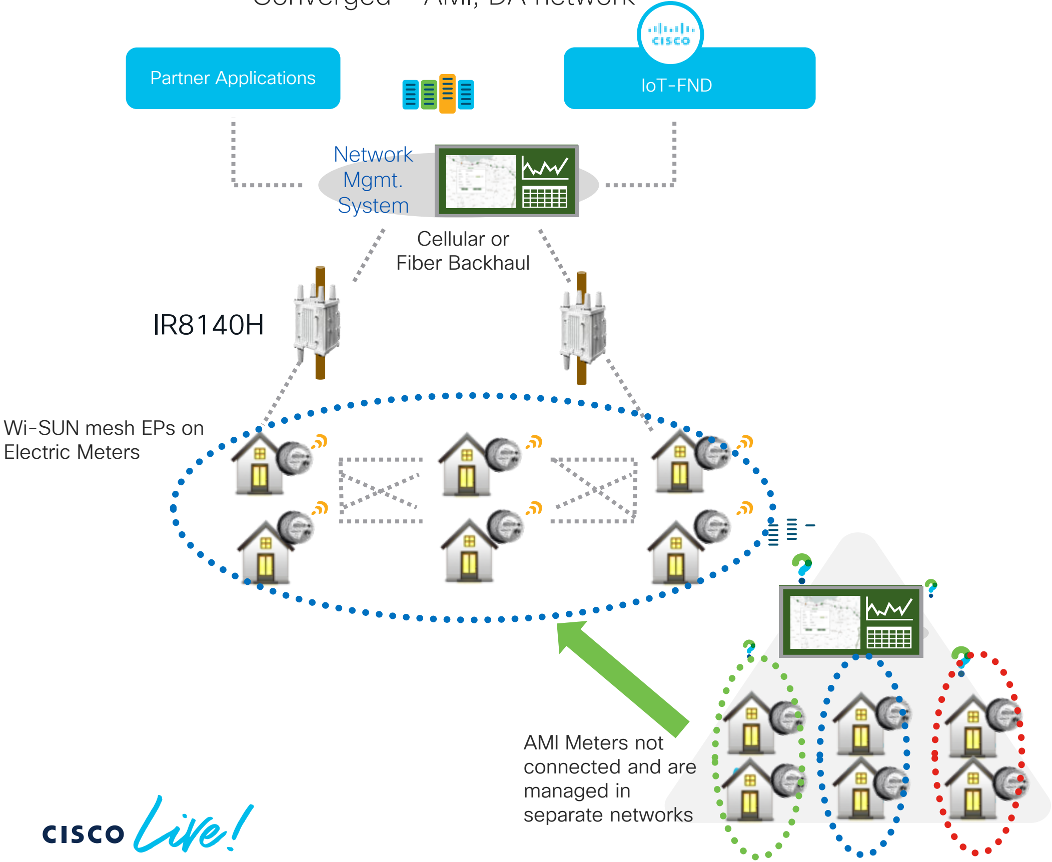


Industrial Sensor Solution
Industrial Asset Vision

Management & Automation
Field Network Director, IoT Operations Dashboard, Cisco DNA Center

Use Case:
Connected Utilities (AMI and DA)

Converged – AMI, DA network


Partner Applications
IoT-FND
Network Mgmt. System
Cellular or Fiber Backhaul
IR8140H
Wi-SUN mesh EPs on Electric Meters
AMI Meters not connected and are managed in separate networks

Challenges

- No real-time visibility and control of the electric grid
- Legacy and disconnected communications paradigms within a vertical - with vendor lock-ins
- Non-secure network with legacy processes to fix vulnerabilities
- No Insights into fluctuating and renewable power sources

Solutions

- Wi-SUN / Cisco resilient mesh converges electric utility assets with an IPv6 mesh network
- Intelligent networked applications provide real-time alerts and metric data
- Ruggedized IP67 platform for outdoor connectivity

Outcomes

- Electric Utility assets become sensors sending metrics and data to the applications
- Faster response to outages and electric grid disruptions through network and application monitoring
- Safer , reliable and more efficient power generation and distribution
- Security at every layer of the network

Connected Remote and Mobile assets

Public Safety Fleets

Location tracking, improve safety & productivity in field. Faster crime detection. Maintenance monitoring.

Service Vehicle Fleets

Monitor driver behavior for safety, liability, and Maintenance monitoring.

Passenger Transit Fleet

Surveillance cameras, passenger Wi-Fi, and more. Maintenance monitoring.

Oil & Gas

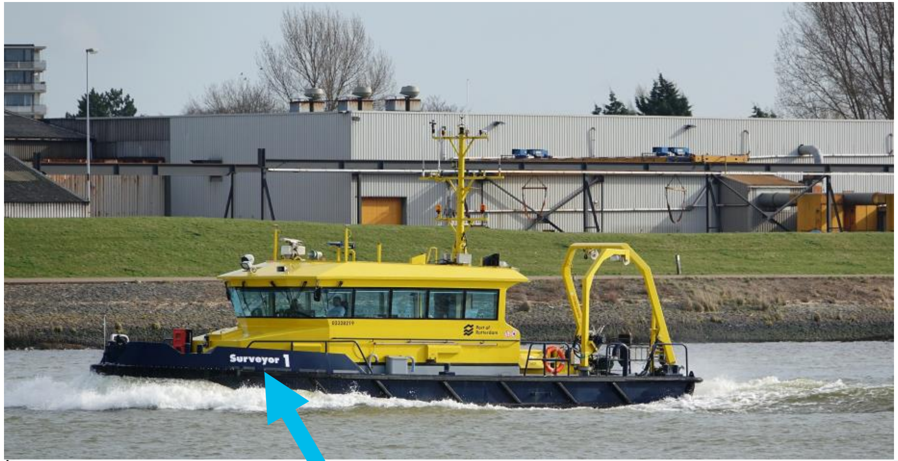
Monitor pipelines, adjust valve pressure, optimize production and prevent unplanned downtime.

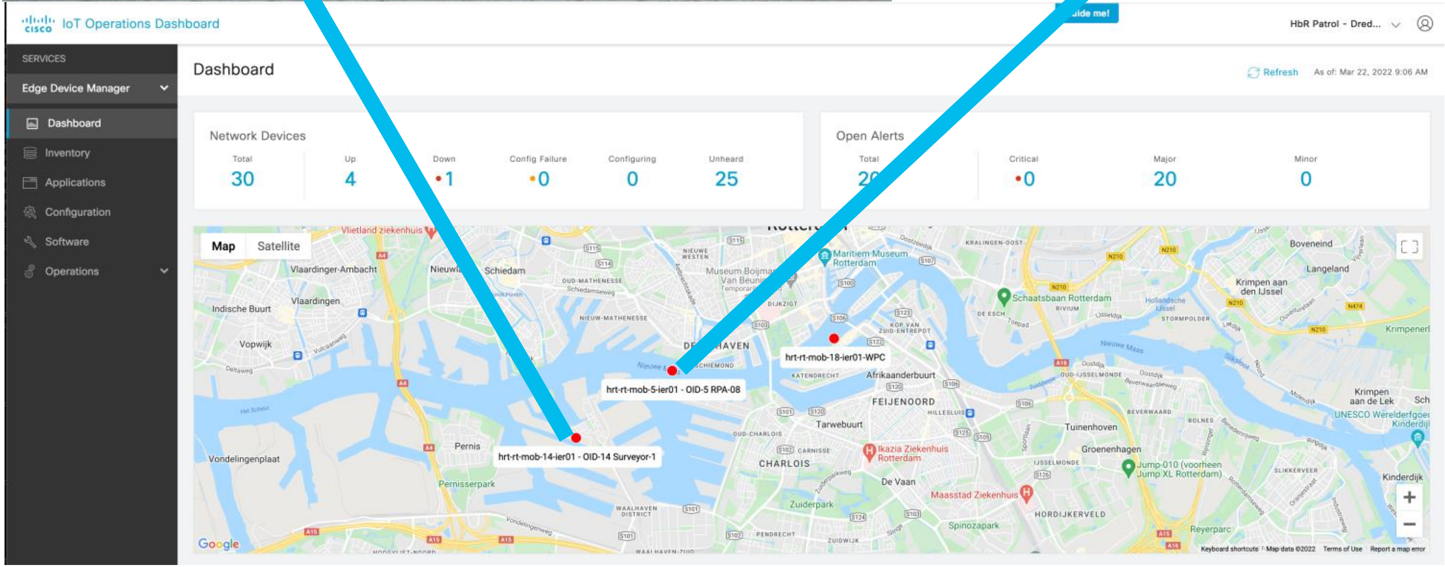
Purpose

- Patrol vessels are scouting the port for **security** and **safety**
- Need **critical access** to information about other vessels and payload
- In case of fire, firefighters can identify potentially dangerous goods

Patrol Vessels

- IR829 **2LTE** in active-active mode with 2 different operators to provide always-on access
- **External AP** in lightweight mode with **CAPWAP**
- All equipment (Ethernet and WiFi) authenticated with **dot1x** and Cisco **ISE**
- Cisco **IoT OD** managing all vessels, all configs, including 3 separate S2S FlexVPN connections per gateway





Dashboard

Refresh As of: Mar 22, 2022 9:06 AM

Network Devices

Total	Up	Down	Config Failure	Configuring	Unheard
30	4	1	0	0	25

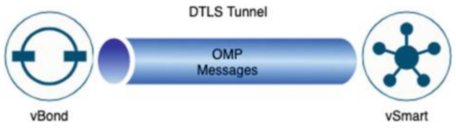
Open Alerts

Total	Critical	Major	Minor
20	0	20	0

hrt-rt-mob-18-ier01-WPC
hrt-rt-mob-5-ier01 - OID-5 RPA-08
hrt-rt-mob-14-ier01 - OID-14 Surveyor-1

SD-WAN Challenges outside carpeted spaces

SD-WAN Recap

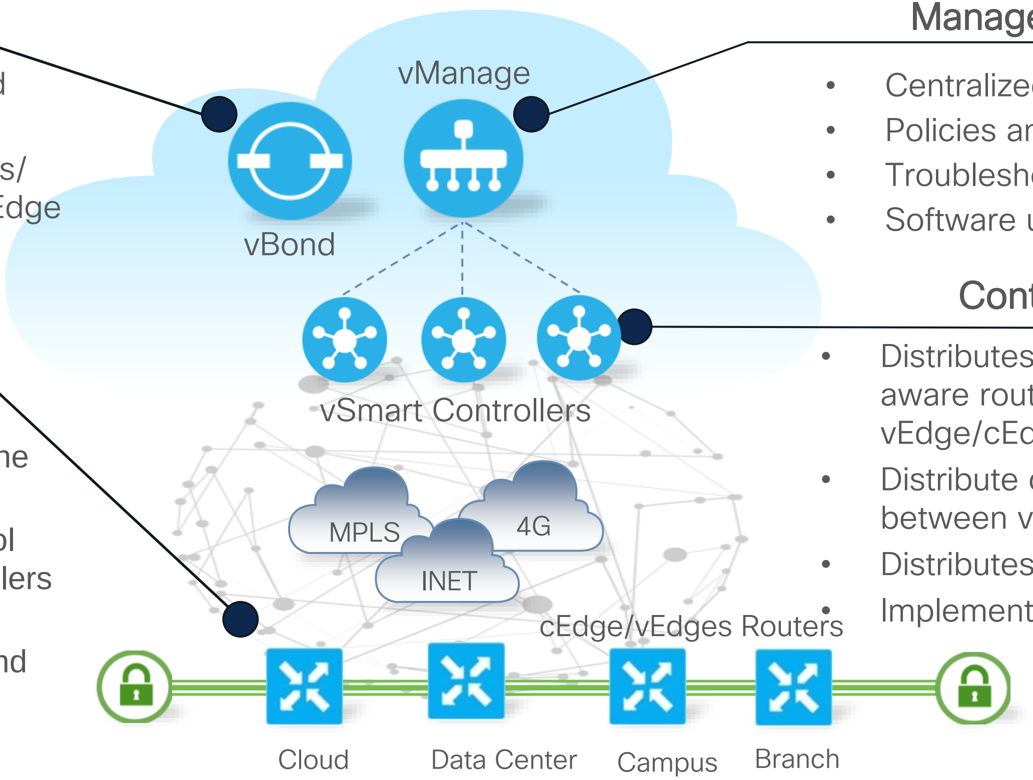


Orchestration Plane

- Orchestrates control and management plane
- Distributes list of vSmarts/ vManage to all vEdge/cEdge routers

Data Plane

- WAN edge router
- Provides secure data plane with remote Edge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies



Management Plane

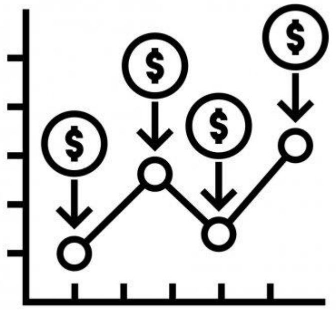
- Centralized provisioning
- Policies and Templates
- Troubleshooting and Monitoring
- Software upgrades/downgrade

Control Plane

- Distributes data plane and app-aware routing policies to the vEdge/cEdge routers
- Distribute control plane information between vEdge/cEdge
- Distributes data plane policies
- Implements control plane policies

SD-WAN Challenges in non-carpeted space

- SD-WAN is **not optimized for data usage**
  - SD-WAN sends BFD ‘hello’ every second to all neighbors
  - Minimum 1.5 GB per month per gateway (single hub)
- In comparison IoT OD consumes about ~ 30MB of data per gateway / per month



SD-WAN Challenges in non-carpeted space

- SD-WAN **does not provide gateway autonomy**
  - Losing access to SD-WAN network will cause the router to stop forwarding traffic after the keys are expired (default: 12 hours)
- No edge compute support for 3rd party **IOx applications on IoT router** which allows the router to take decision at the edge.

SD-WAN Challenges in non-carpeted space

- SD-WAN **is not supported on Classic IOS platforms**
- SD-WAN does not support **switches** or **AP**s.
- SD-WAN will not support millions of End-points and smart devices/assets
  - Maximum 2000 cEdge per vManage instance

Managing IoT Gateways without SD-WAN

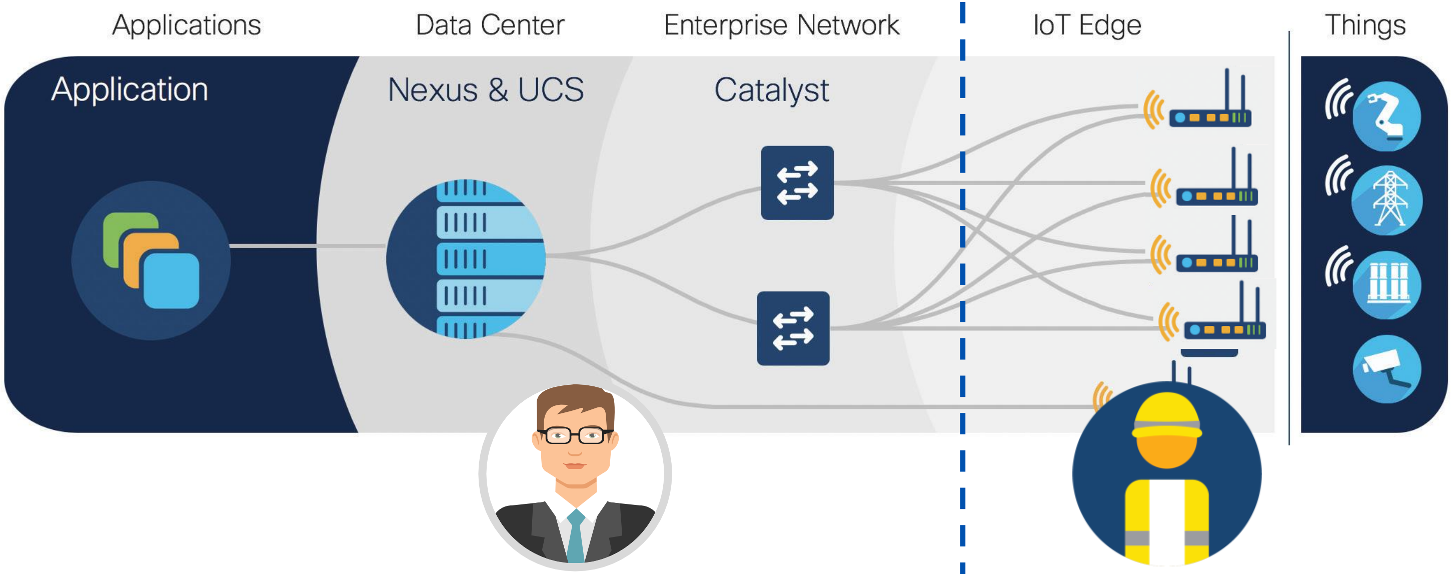
Cisco Management

IoT / Non-carpeted Space

Cisco
APIC

Cisco
SD-WAN (vManage)

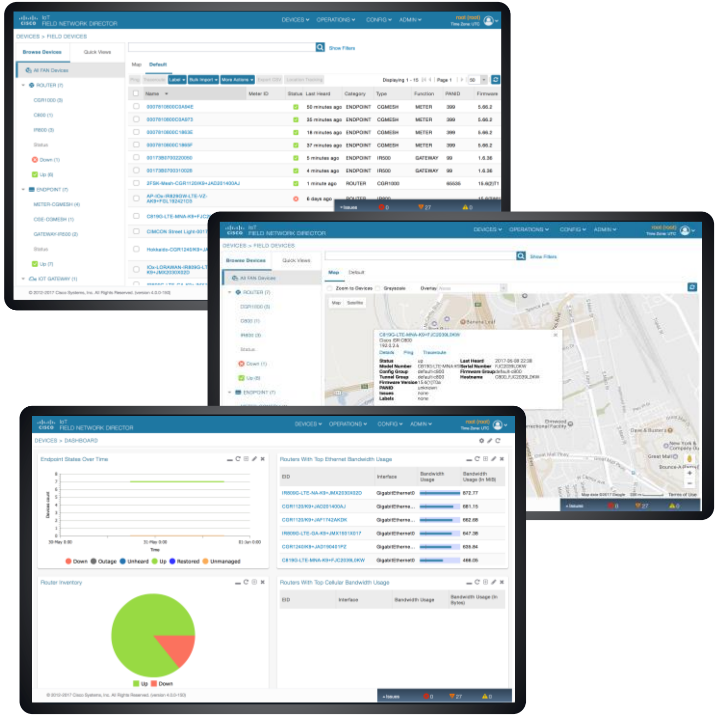
Cisco IoT OD (Cloud)
Cisco FND (OnPrem)



IT Operated

OT Operated

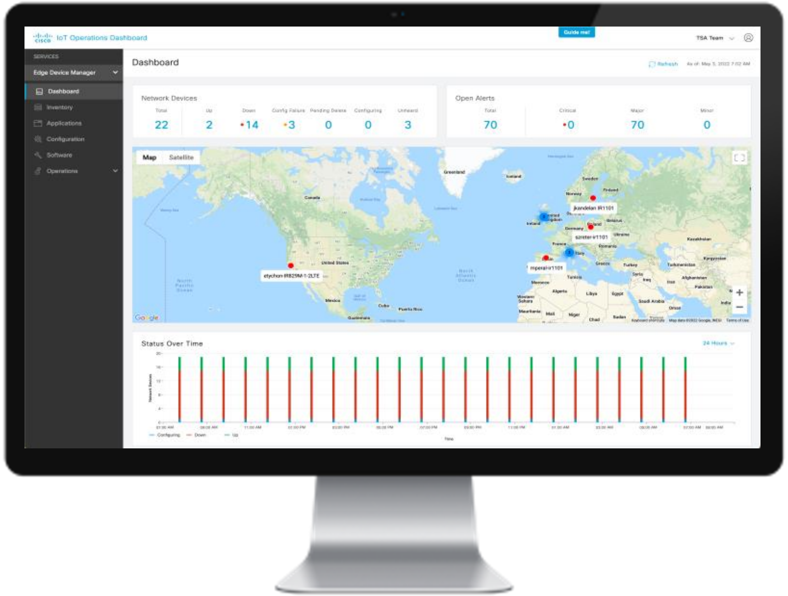
Cisco IoT
Field Network Director


FIELD NETWORK DIRECTOR
DEVICES > FIELD DEVICES
DEVICES > DASHBOARD
Endpoint States Over Time
Routers With Top Ethernet Bandwidth Usage
Router Inventory
Routers With Top Cellular Bandwidth Usage

FND

- **On Prem** Network Management System for the IoT Field Area Network
- Secure zero touch deployment (ZTD) at scale
- Real-time critical infrastructure monitoring
- Geographical visualization of all network assets
- Field device lifecycle management
- Application management
- Multi-tenancy and RBAC support
- Supports FAN solutions: AMI / DA in utilities, and street lighting in cities
- API for 3rd party integration
- Over 8 Million endpoints deployed

Cisco IoT Operations Dashboard



IoT OD

- **Cloud-only** SaaS device Management System for IoT Gateways
- Secure zero touch deployment (ZTD) at scale
- Real-time devices monitoring
- Geographical visualization of all network assets
- IOx Application management
- Multi-tenancy and RBAC support
- API for 3rd party integration
- Remote Secure Equipment Access (SEA)
- Edge Intelligence computing at the edge
- Jasper Control Center Integration
- Secure Device Onboarding (SDO) over cellular
- WiFi Provisioning for IR829 and IR1800
- Single-sign-on Functionality
- Smart Account Integration for easier on-boarding

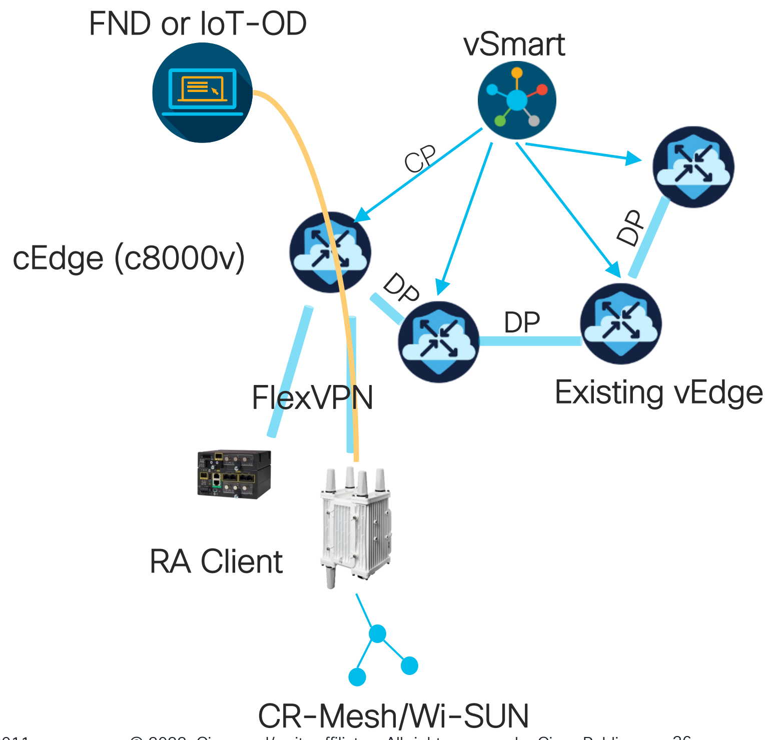
Platform Support

Platform		Cisco SD-WAN	Cisco FND	Cisco IoT OD
IR8140H		✓	✓	✗
IR1101		✓	✓	✓
IR1800		✓	✓	✓
IG21/IR31R		✗	✗	✓
IW9167E		✗	✗	✓

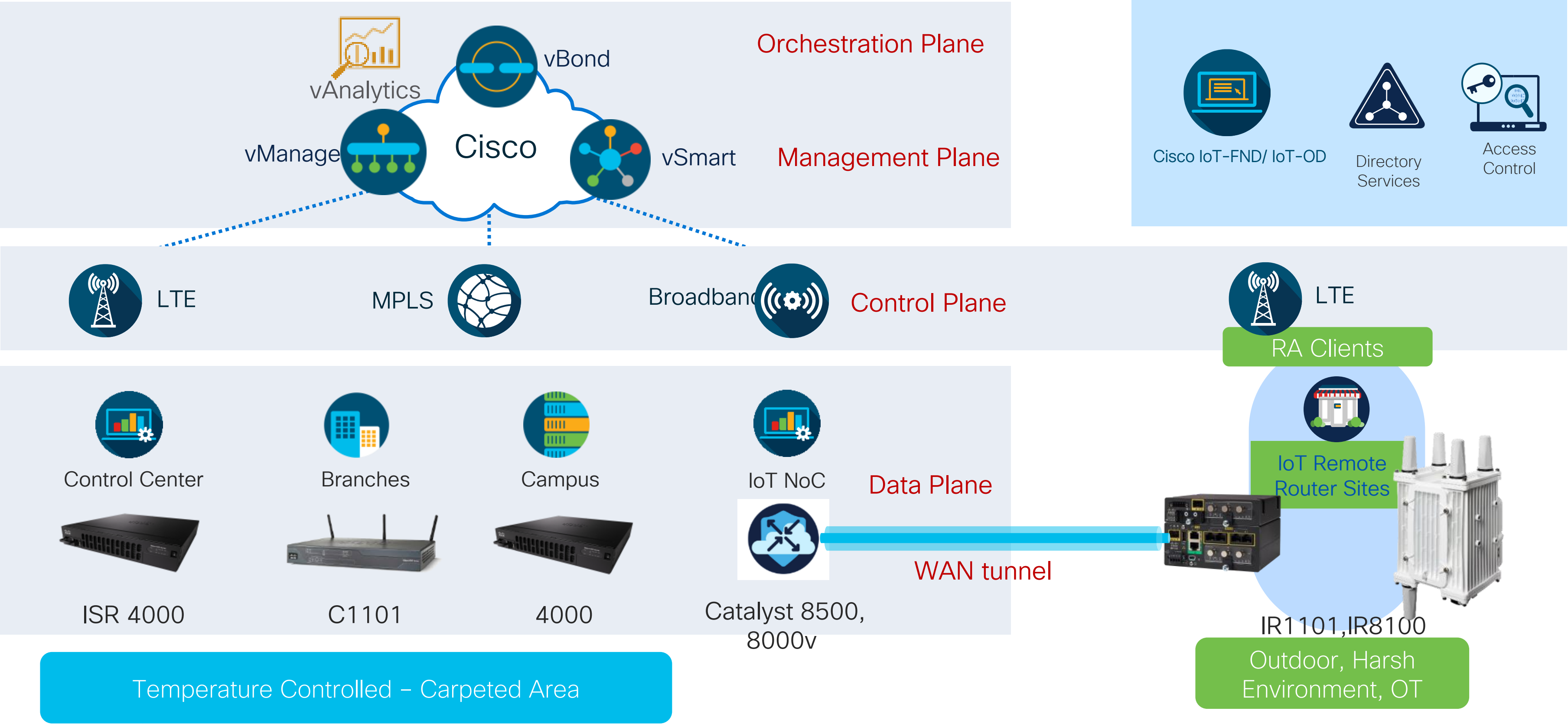
How to extend the SD-WAN Network?

Leverage Cisco SD-WAN Remote Access

- Allows secure access from remote devices
- Extends the network outside carpeted space
- Avoid overhead of running Overlay Management Protocol (OMP) on IoT gateways
- IoT gateways managed with IoT management platforms such as FND or IoT OD

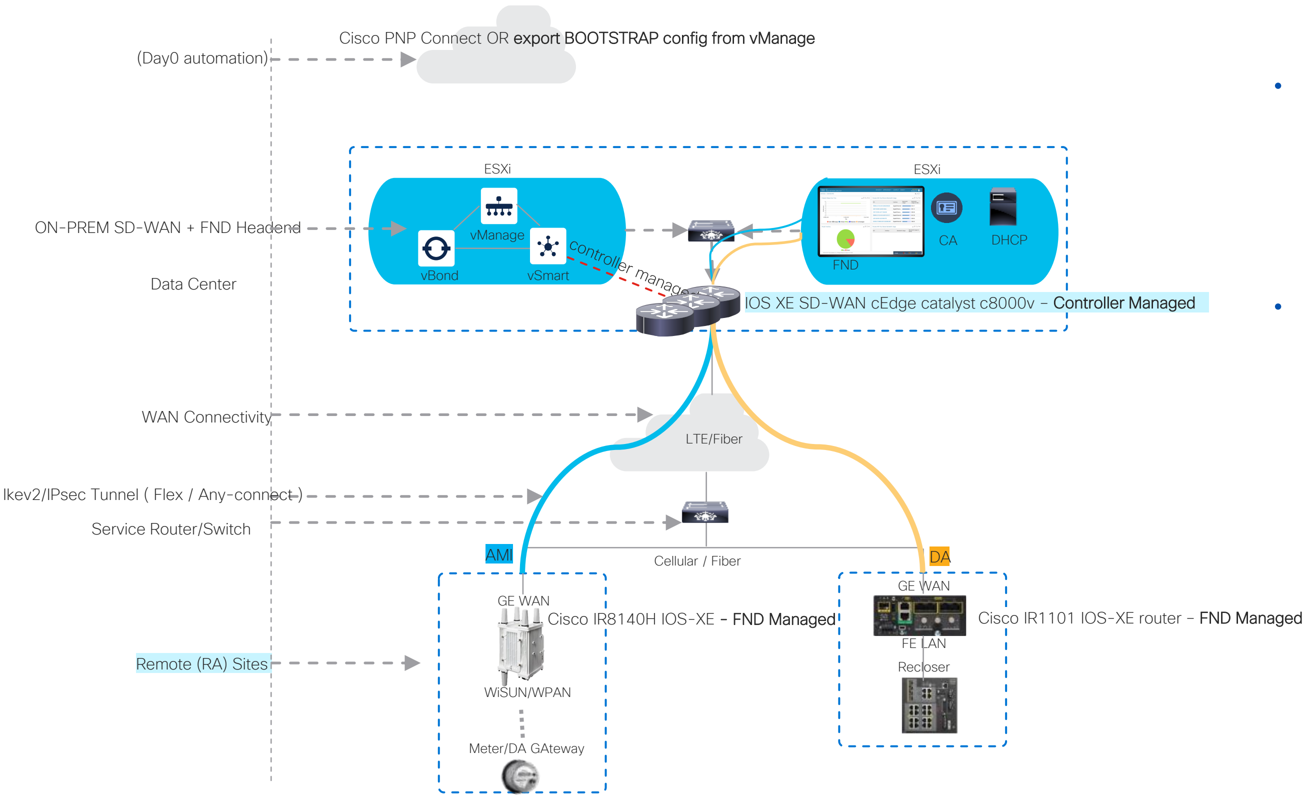


Bringing IT/OT together – Leverage SDWAN - RA



Building Blocks
vManage and FND

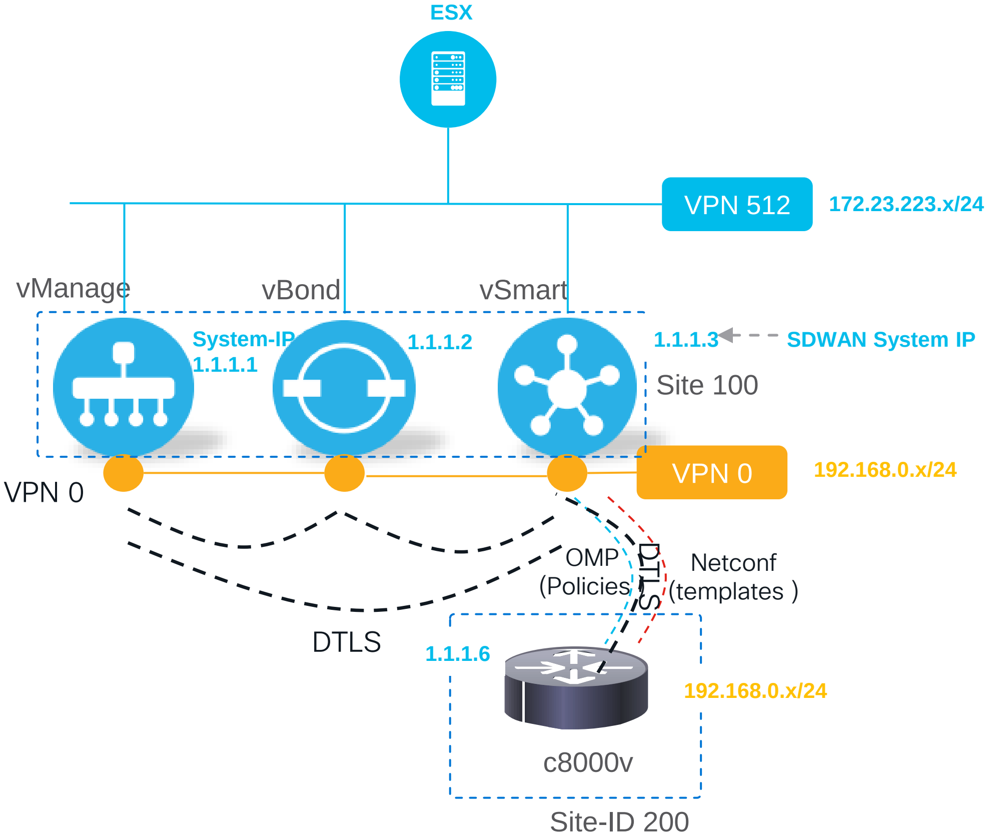
Extended Enterprise SD-WAN and IoT-FND solution (on-prem)


Cisco PNP Connect OR export BOOTSTRAP config from vManage
(Day0 automation)
ON-PREM SD-WAN + FND Headend
Data Center
ESXi
vManage
vBond
vSmart
controller managed
ESXi
CA
DHCP
FND
IOS XE SD-WAN cEdge catalyst c8000v – Controller Managed
WAN Connectivity
LTE/Fiber
Ikev2/IPsec Tunnel (Flex / Any-connect)
Service Router/Switch
AMI
DA
Cellular / Fiber
GE WAN
Cisco IR8140H IOS-XE – FND Managed
WiSUN/WPAN
Meter/DA GAteway
GE WAN
Cisco IR1101 IOS-XE router – FND Managed
FE LAN
Recloser
Remote (RA) Sites

- C8000v / Catalyst 8500 are the **only** edge routers that work as SDWAN managed RA Headend(s) in this solution
- Tunnel can be PSK or PKI based

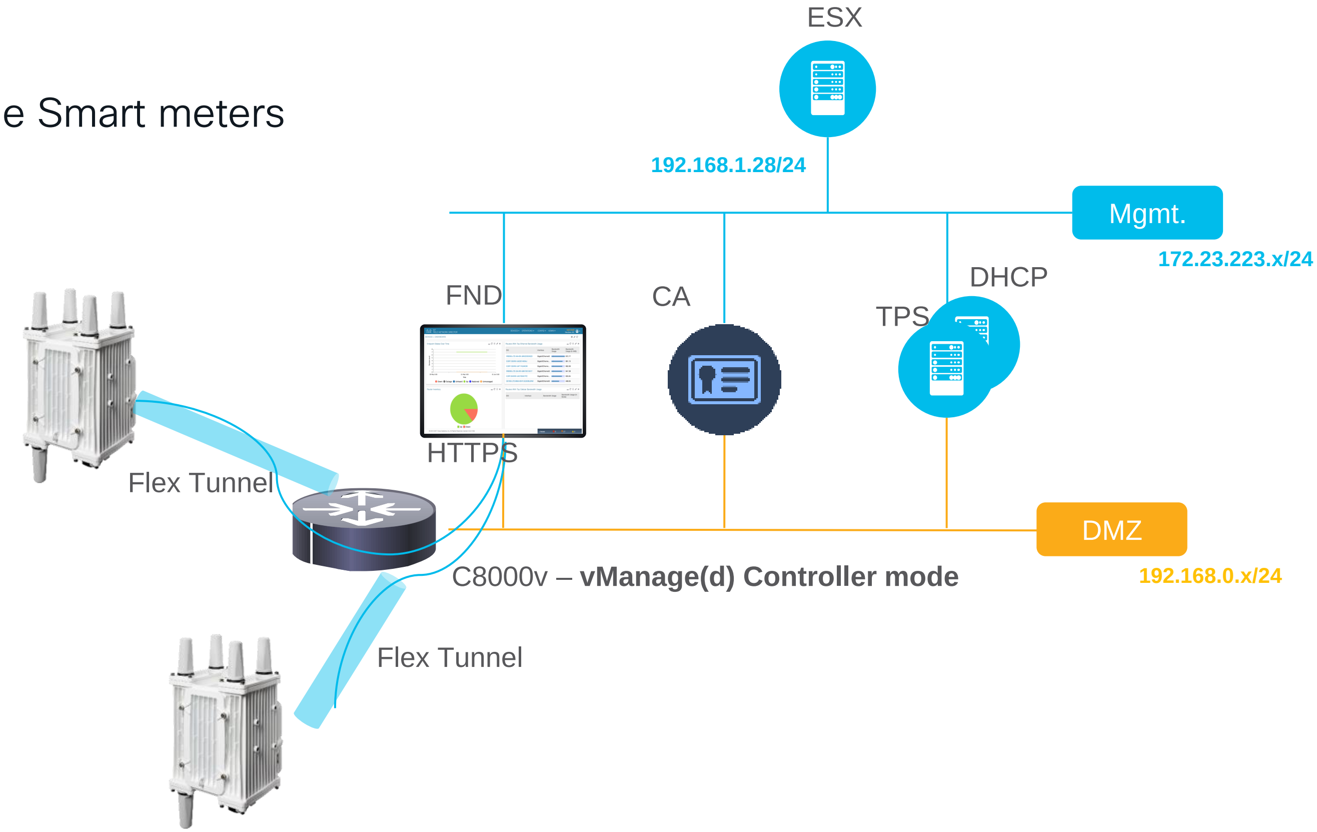
vManage and Headend Connectivity

- VPN 0 is used to establish DTLS connections
- VPN 512 is used as an OOB management for the controllers
- Control Channel (DTLS/TLS) always sourced from VPN 0



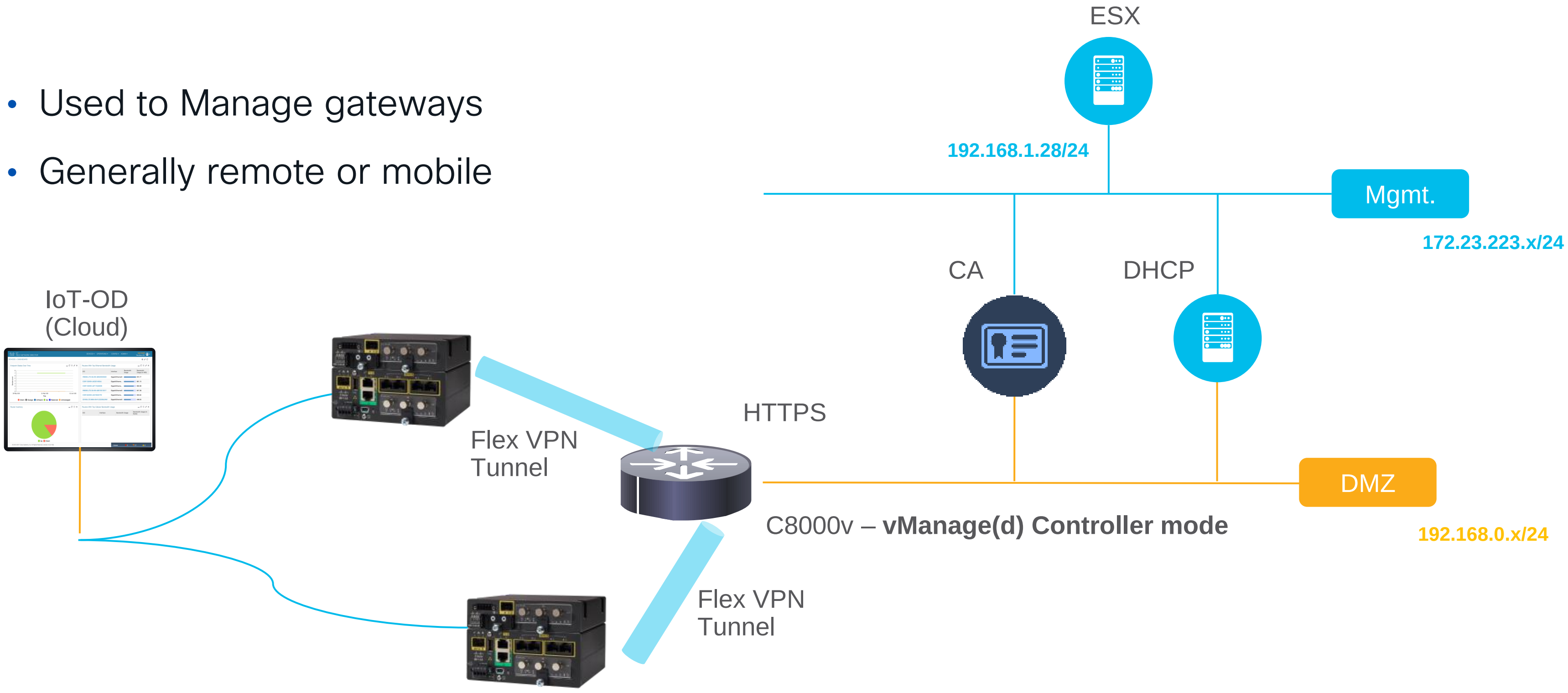
FND – On Prem

- Used to Manage the Smart meters / AMI network only



IoT-OD – Cloud

- Used to Manage gateways
- Generally remote or mobile



Conclusions

Conclusions

- vManage can be used everywhere – core to edge – but with some caveats
- You can also use vManage for Core and Remote Access, IoT OD/FND for edge device management
- Know what you **want** and **need** with regards to scalability, volume, and edge compute needs is key to decide
- Whatever the scenario : Cisco has a flexible and extensive portfolio of products

Other Upcoming Related Sessions

- PSOSPG-1701 : 3 Keys to Succeeding at IoT Scale with Cellular Connectivity Management (Wed, 2PM)
- INTIOT-1300 : Digitizing the Physical World with Mass-scale Industrial IoT to Move Industries Forward (Tue, 3PM)
- BRKIOT-1083 : Cisco Industrial Asset Vision: Simplifying Industrial Sensor Solutions! (Wed, 1PM)

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

CISCO Live!

#CiscoLive

Appendix

2. Prepare vManage for device onboarding

Prepare FND and vManage

1. Prepare FND tunnel template and vManage Configuration templates
2. Export vManage configuration as c8000 cloud_init file
3. Move file to c8000 and reload c8000 in Controller mode
4. Attach c8000 to the vManage group which has the tunnel template configuration
5. Make sure c8000 already has the requisite certificates for TLS handshake with vSmart
6. Once c8000 is up – let it authenticate with vSmart
7. IoT – IR router can now being PnP process
8. IR router will contact PnP server and receive bootstrap configuration
9. It will then receive Tunnel configuration and Tunnel with c8000

1. FND/OD VPN Template : Flex-VPN for RA devices

```
vrf definition 600
 !
 address-family ipv4
 exit-address-family
!
ip vrf forwarding
!
interface Loopback0
 no shutdown
 ip address 30.0.0.1 255.255.255.0
Exit
interface Virtual-Template101 type tunnel
 vrf forwarding 600
 ip unnumbered Loopback0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROFILE ikev2-profile IKEV2_PROFILE
!
aaa authentication enable default enable
aaa authentication login default local
aaa authorization console
aaa authorization exec default local
aaa authorization network Flex_PG local
!
crypto ikev2 authorization policy IKEV2_AUTH
 route set interface
 route set remote ipv4 30.0.0.0 255.255.255.0
 route set access-list IKEV2_ROUTES
exit
no crypto ikev2 diagnose error
crypto ikev2 keyring KEYRING
 peer ANY-PEER
  address 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
 !
!
```

```
crypto ikev2 profile IKEV2_PROFILE
 match identity remote any
 identity local address 192.168.0.202
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list Flex_PG
 virtual-template 101
!
crypto ipsec profile IPSEC_PROFILE
 set ikev2-profile IKEV2_PROFILE
!
no crypto isakmp diagnose error
!
security
 ipsec
  authentication-type ah-sha1-hmac sha1-hmac
  !
!
ip access-list standard IKEV2_ROUTES
 10 permit 0.0.0.0
```

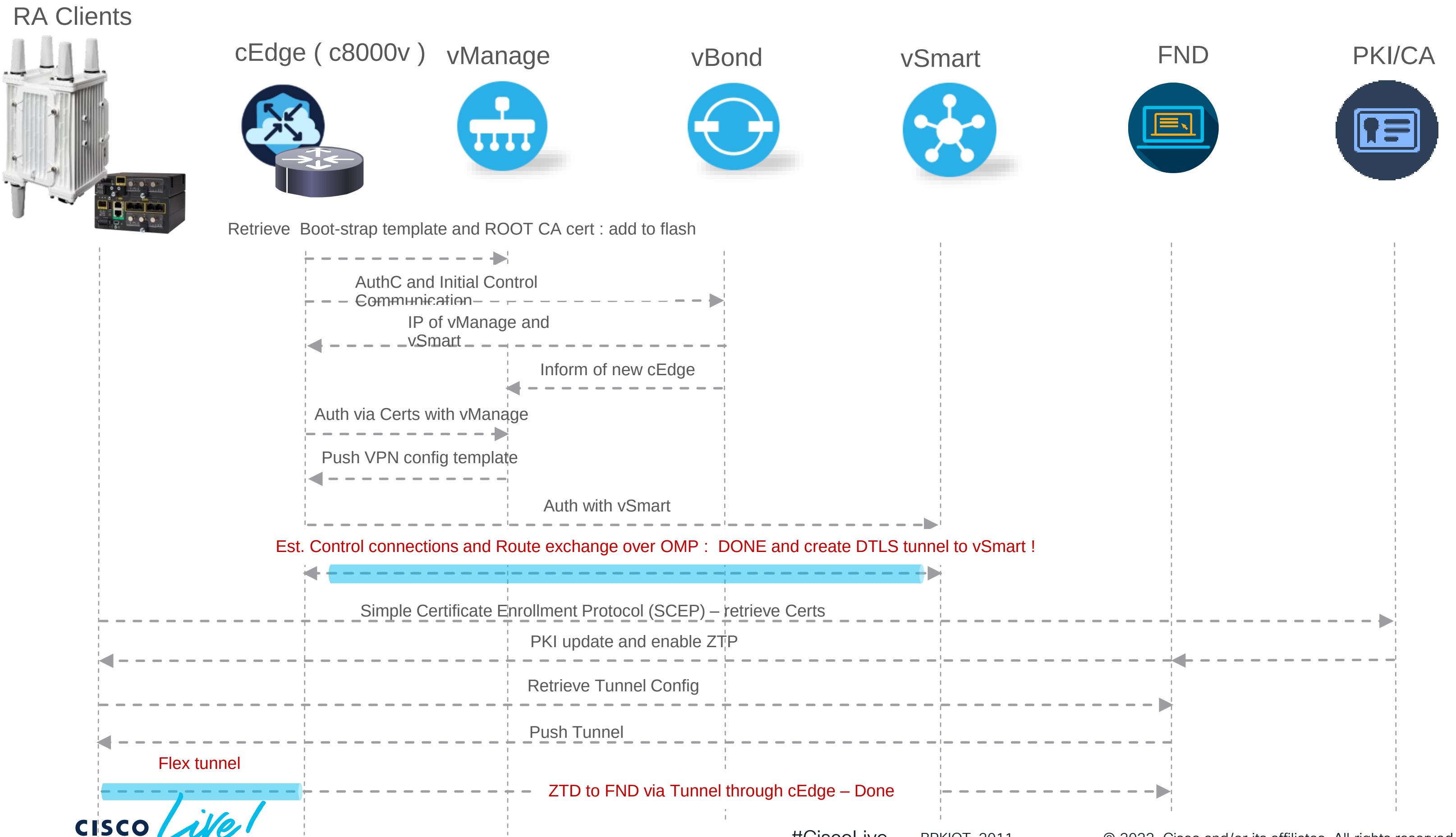
2. SDWAN VPN Template : Flex-VPN for RA devices

```
vrf pre-shared-key local cisco123
  pre-shared-key remote cisco123
 !
!

vrf definition 600
 !
 address-family ipv4
 exit-address-family
!
ip vrf forwarding
!
system
 system-ip             1.1.1.6
 site-id               200
 admin-tech-on-failure
 organization-name     Cisco12345
 vbond 192.168.0.132
!
memory free low-watermark processor 71477
no service tcp-small-servers
no service udp-small-servers
platform console virtual
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname cEdge-csr
username admin privilege 15 secret 5 $1$tZUp$zY91qs8X8OKE.sK5AERL1/
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
no ip dhcp use class
ip route 0.0.0.0 0.0.0.0 192.168.0.1
ip route 10.0.0.0 255.0.0.0 172.23.223.1
ip route 171.0.0.0 255.0.0.0 172.23.223.1
ip route 172.0.0.0 255.0.0.0 172.23.223.1
no ip source-route
ip ssh version 2
no ip http server
ip http secure-server
no ip igmp ssm-map query dns
ip nat settings central-policy
interface GigabitEthernet1
 no shutdown
 ip address 192.168.0.202 255.255.255.0
 no mop enabled
```

4. ZTP

FND + vManage Onboarding (On-Prem)



RA Clients

cEdge (c8000v)

vManage

vBond

vSmart

FND

PKI/CA

Retrieve Boot-strap template and ROOT CA cert : add to flash

AuthC and Initial Control Communication

IP of vManage and vSmart

Inform of new cEdge

Auth via Certs with vManage

Push VPN config template

Auth with vSmart

Est. Control connections and Route exchange over OMP : DONE and create DTLS tunnel to vSmart !

Simple Certificate Enrollment Protocol (SCEP) – retrieve Certs

PKI update and enable ZTP

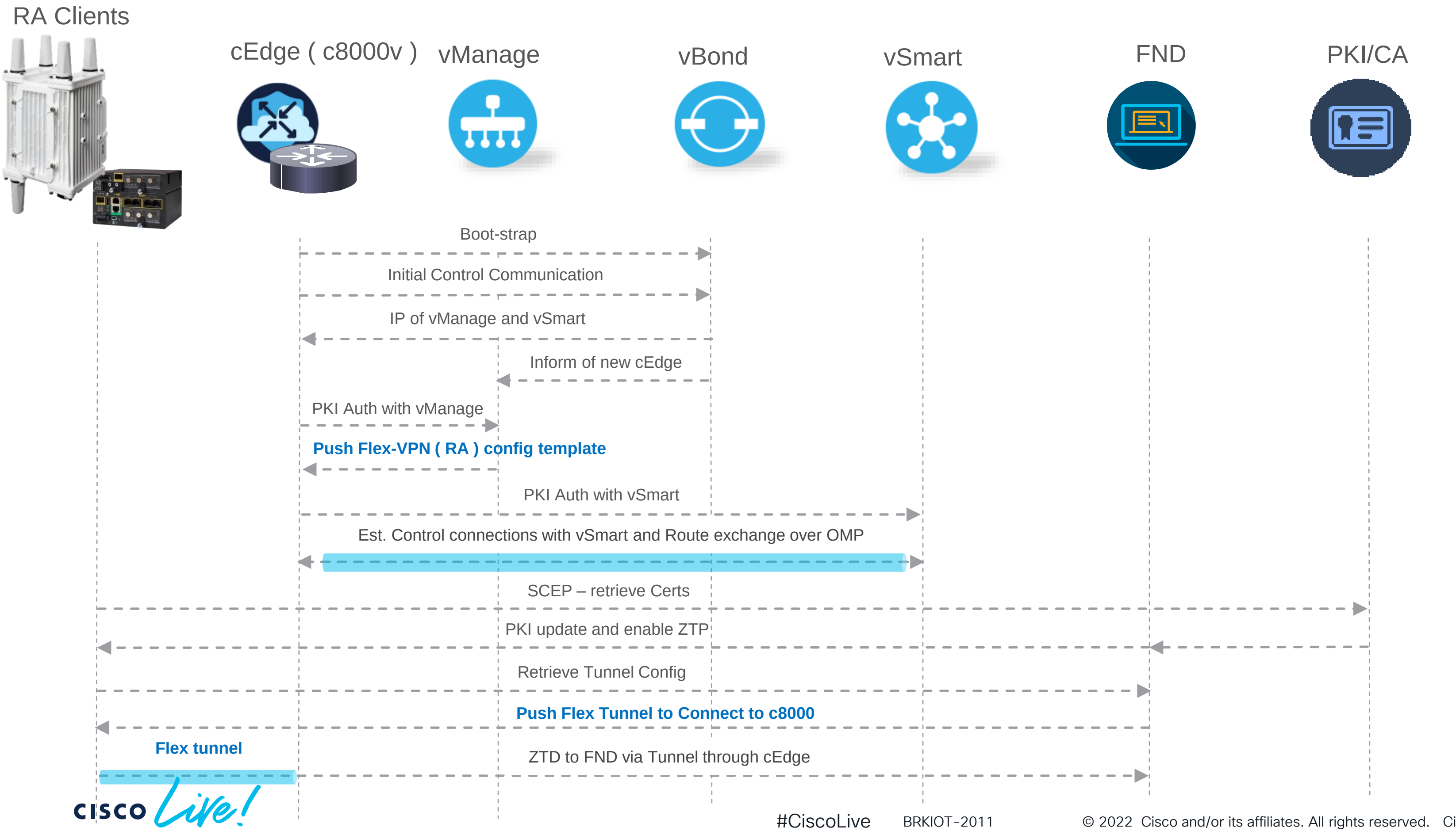
Retrieve Tunnel Config

Push Tunnel

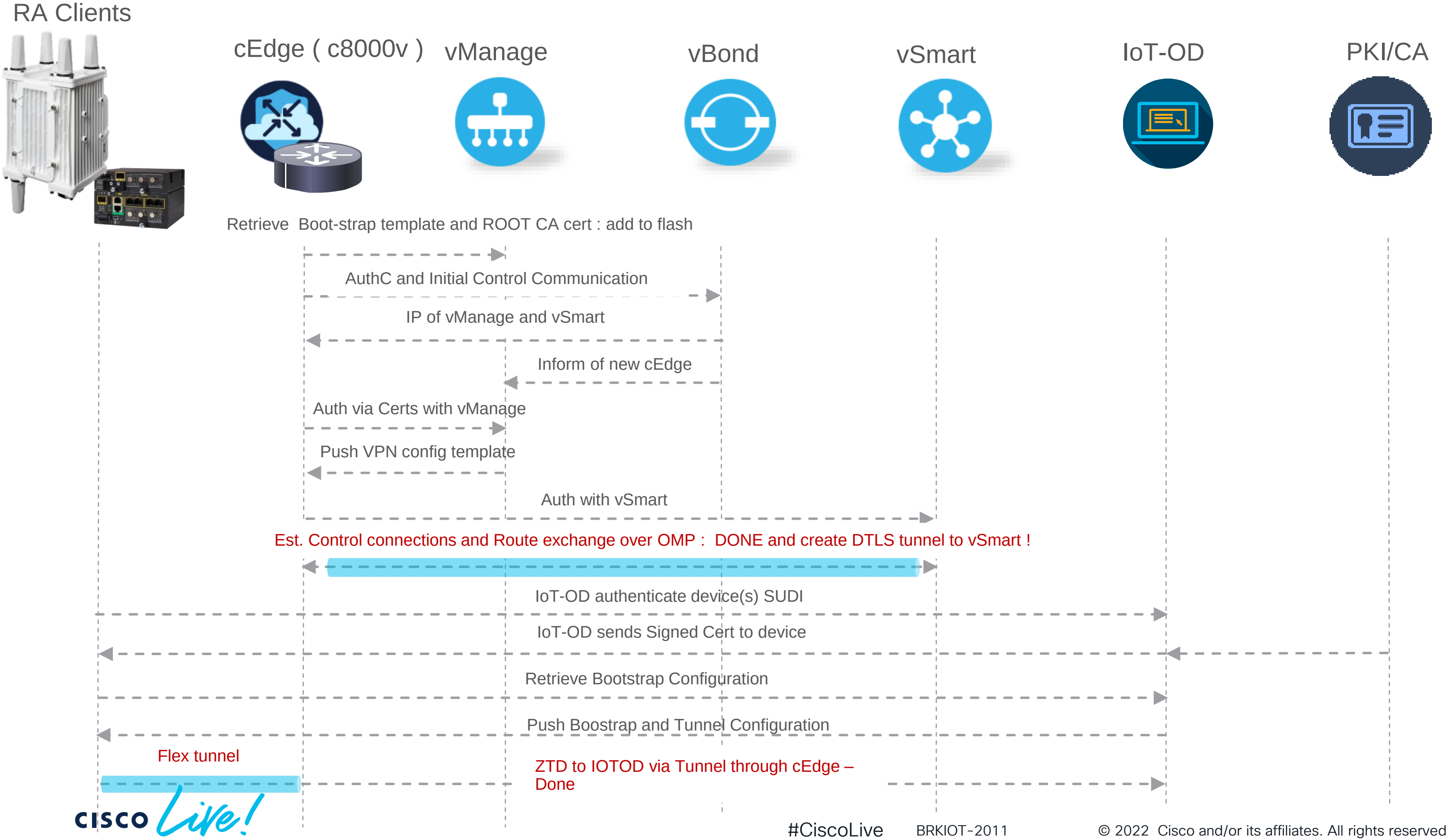
Flex tunnel

ZTD to FND via Tunnel through cEdge – Done

FND + vManage Onboarding (On-Prem)


RA Clients
cEdge (c8000v)
vManage
vBond
vSmart
FND
PKI/CA
Boot-strap
Initial Control Communication
IP of vManage and vSmart
Inform of new cEdge
PKI Auth with vManage
Push Flex-VPN (RA) config template
PKI Auth with vSmart
Est. Control connections with vSmart and Route exchange over OMP
SCEP – retrieve Certs
PKI update and enable ZTP
Retrieve Tunnel Config
Push Flex Tunnel to Connect to c8000
Flex tunnel
ZTD to FND via Tunnel through cEdge

IoT-OD + vManage Onboarding (Cloud)



RA Clients

cEdge (c8000v)

vManage

vBond

vSmart

IoT-OD

PKI/CA

Retrieve Boot-strap template and ROOT CA cert : add to flash

AuthC and Initial Control Communication

IP of vManage and vSmart

Inform of new cEdge

Auth via Certs with vManage

Push VPN config template

Auth with vSmart

Est. Control connections and Route exchange over OMP : DONE and create DTLS tunnel to vSmart !

IoT-OD authenticate device(s) SUDI

IoT-OD sends Signed Cert to device

Retrieve Bootstrap Configuration

Push Boostrap and Tunnel Configuration

Flex tunnel

ZTD to IOTOD via Tunnel through cEdge – Done