

CISCO *Live!*



#CiscoLive



The bridge to possible

# The New Digital Substation

Substation Automation Cisco Validated Design

Paul Didier, IoT Solution Manager  
BRKIOT-2015



#CiscoLive

# Cisco Webex App

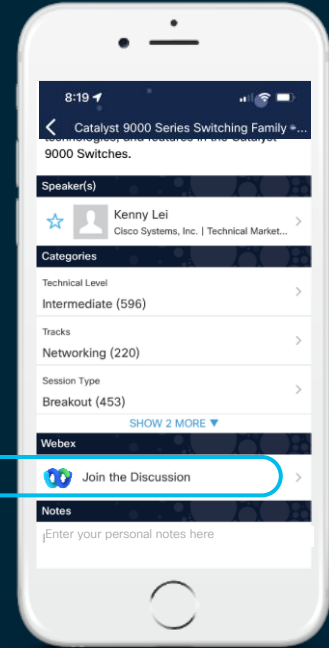
## Questions?

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.



<https://cicolive.ciscoevents.com/cicolivebot/#BRKIOT-2015>



# Agenda

- Utility & Substation Operations Challenges
- Digital Substation Automation Solution
- Securing the Substation
- More Capability, smaller footprint
- Automated deployment and management
- Conclusion

# Substations face unique challenges

The need for agility is accelerating their digitization



Integrate new energy sources

Grid resiliency

Meet security and compliance regulations

Improve grid efficiency and safety





# New demands on the network

## Digitization isn't easy

Visibility of all networked equipment



Cyber security standards



More Devices, Data & Bandwidth



More capabilities in a smaller footprint



Highly resilient networks



IEC 61850 & Precision timing

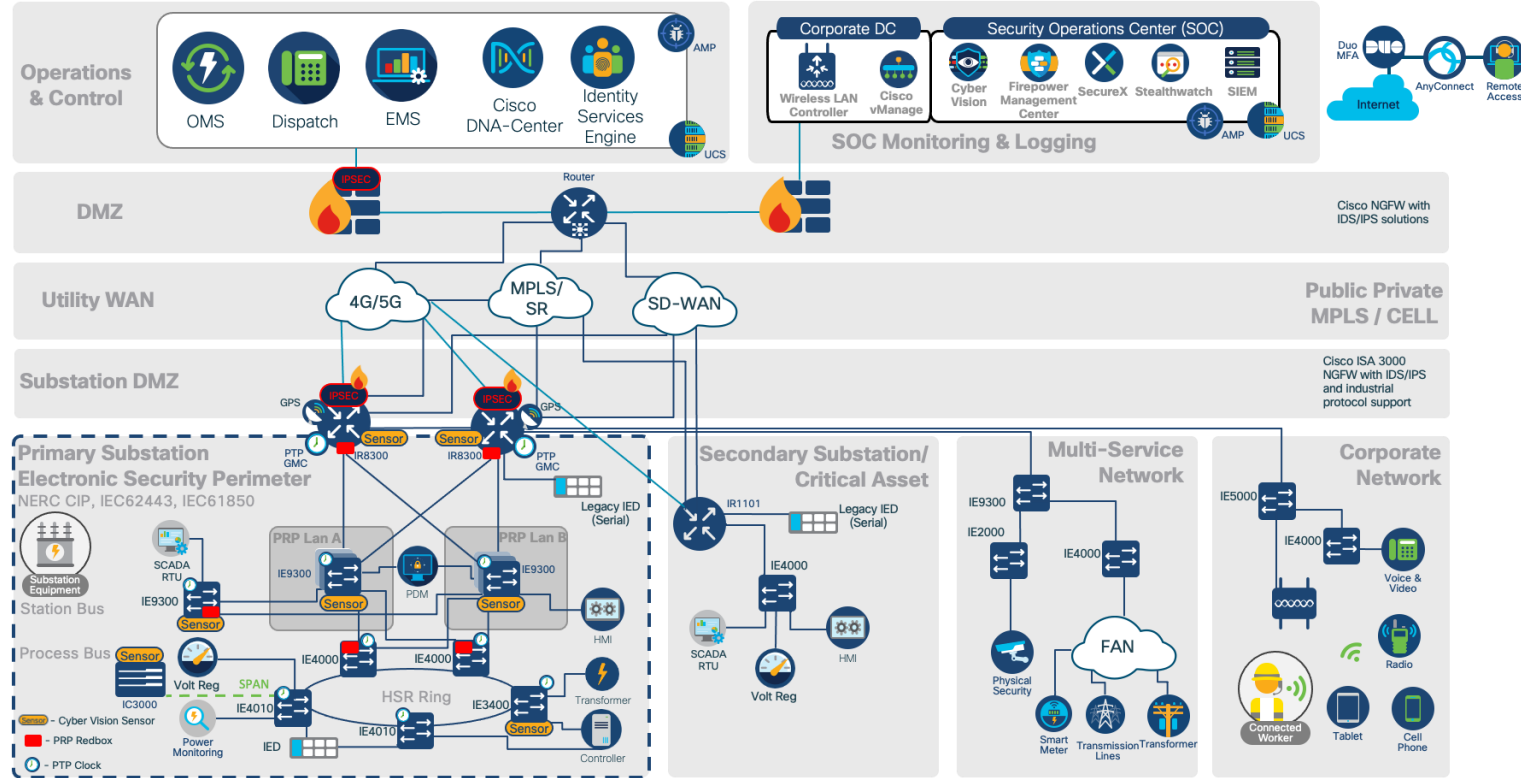


# The New Digital Substation

## Substation Automation Cisco Validated Design

# Substation Automation

## Modernize Grid operations



Proven to work with:



SCHWEITZER  
ENGINEERING  
LABORATORIES

SIEMENS

Schneider  
Electric

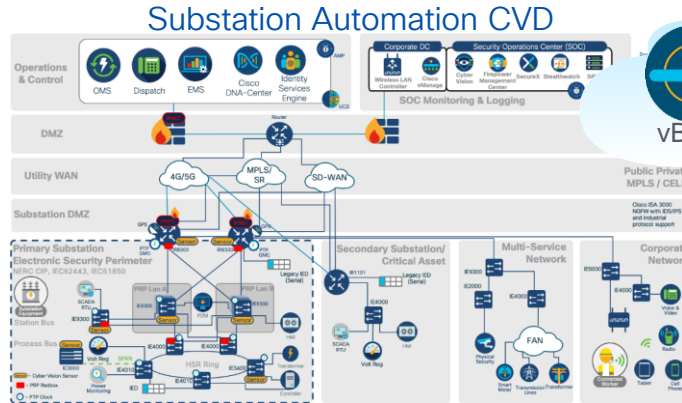


# What's new

NEW



Cisco DNA Center  
& ISE



NEW



vBond

vManage



Cisco SD-WAN



vAnalytics

vSmart Controllers



NEW

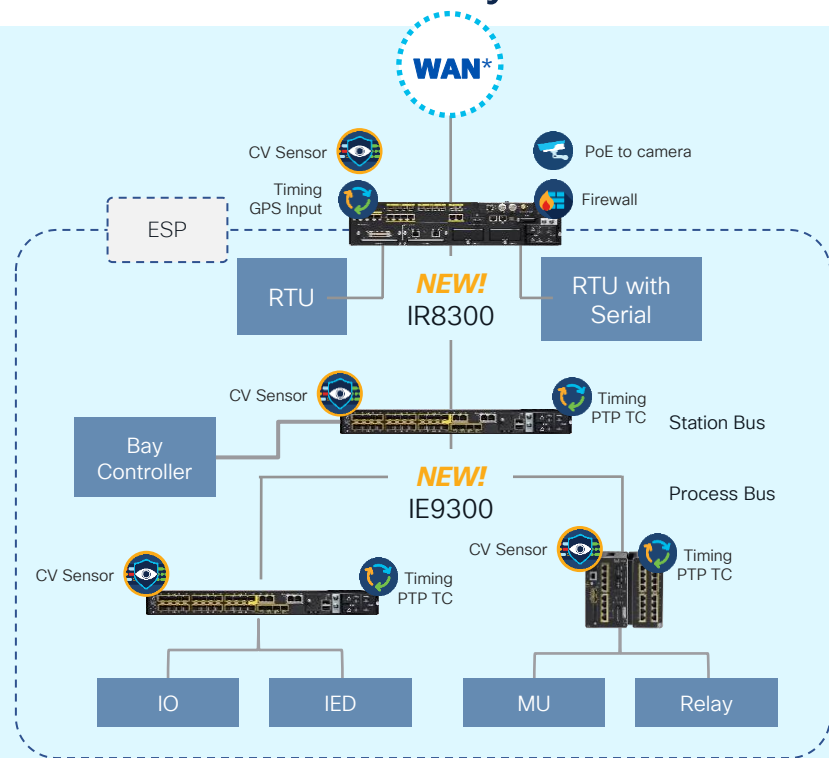
Catalyst IE9300 Rugged  
Series Switch



NEW

Catalyst IR8300 Rugged  
Series Router

# Secure turnkey communications for Digital Substations



Security

Routing

Switching

- High performance substation 5G/FirstNet router
  - Integrated switching, routing, and security
  - PTP Grandmaster with GPS Input
  - Zone-based firewall for Electronic Security Perimeter
  - Cyber Vision sensor for endpoint visibility & security posture
  - Secure VPN transport from substation to control center
  - IOx edge compute to run applications at the edge
- 
- High performance substation LAN switch
  - 8x switch stacking for high port density and reliability
  - High precision PTP with 50ns accuracy
  - MACsec 256 for point-to-point Ethernet link encryption
  - Cyber Vision sensor for endpoint visibility & security posture
  - HSR, PRP redundancy for lossless convergence
  - IOx edge compute to run applications at the edge



Cisco UADP ASIC



Cisco IOS-XE OS



Cisco DNA Center/SD-WAN

# Industrial Cybersecurity

## Protecting the Substation operations

# Industrial Security Framework



## Visibility & Posture



Cyber Vision  
(Industrial Assets)



Secure Endpoint  
(Workstations, Compute, Tablets)



Secure X  
(SOC Integration)



Secure Network Analytics  
(Netflow)



## Segment & Protect



Secure Firewall  
(IDMZ, App Segmentation)



Identity Services Engine  
(User/Device Segmentation)



Secure Access by Duo  
(Multi-Factor Authentication)



## Threat Detection & Response



Secure Firewall  
(Intrusion Prevention)



Secure Endpoint  
(Malware Protection)



Secure X  
(Incident Investigation & Response)



Secure Network Analytics  
(Behavioral Modeling &  
Encrypted Traffic Analytics)



Managed Secure Network Infrastructure  
(Built-In Visibility & Enforcement)



IEC 62443-4-1 certified

Secure Supply Chain

Secure Trustworthy Technologies

Network Access Control

CSDL

Validated Designs

Powered by Talos Threat Intelligence



## Visibility

Asset inventory  
Communication patterns



## Security Posture

Device vulnerabilities  
Risk scoring

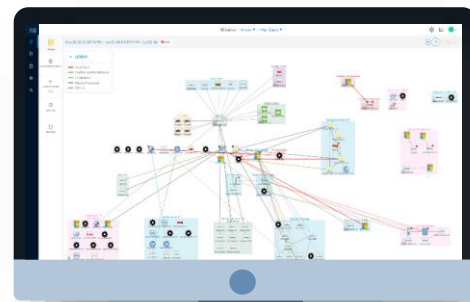


## Operational Insights

Track process/device modifications  
Record control system events

Cisco substation LAN switches and WAN routers **see everything** that attaches to them so you can gain **visibility at scale**

## Cyber Vision Center



1 0 0 1  
0 0 1

Cyber Vision  
Sensor

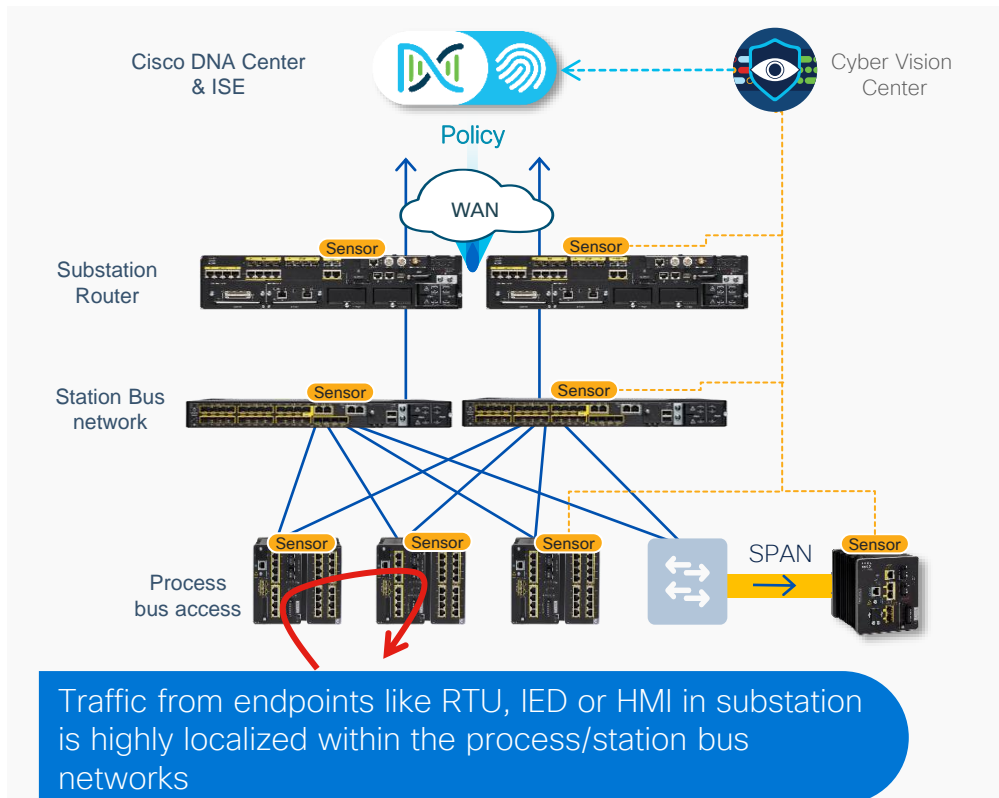
Application Flow  
Metadata

0 0  
1 1 0



Deep Packet Inspection & Active Discovery  
built into your network infrastructure

# DNAC Enables Visualization of Security Policy

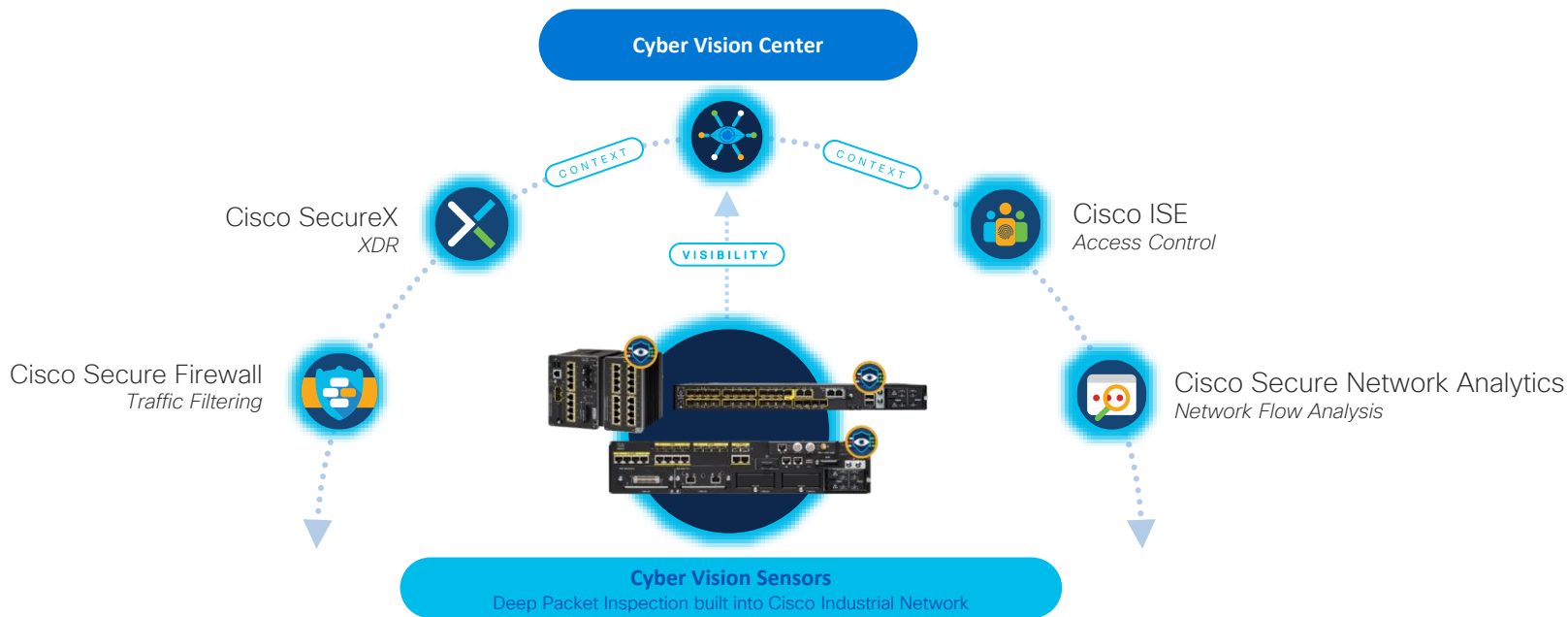


1. Discover endpoints and visualize application relationships in **Cyber Vision** to help create TrustSec group-based segmentation policies in **DNAC Access Control Application**
2. Endpoint grouping in Cyber Vision triggers pxGrid updates and results in dynamic assignment of SGTs in **ISE**
3. Visualize group-based network behavior using NetFlow traffic in **DNAC Policy Analytics**
4. Deploy segmentation policy with confidence using **DNAC Day-n templates** once you are comfortable with the observed network behavior



# Industry-leading security built-in, not bolted-on

## Operational security features with visibility across the enterprise



Unmatched enterprise-to-edge security • Powered by Talos Threat Intelligence

More capability, smaller footprint.  
Switching & Routing upgrade



# Cisco Catalyst IE9300 Switch

## Unleashing enterprise features at the industrial edge

### IE-9310-26S2C

26 SFP • 2 Combo ports  
Redundant power supplies



### IE-9320-26S2C

26 SFP • 2 Combo ports  
Redundant power supplies  
Backplane stacking



Unrivaled  
performance at scale



Unprecedented  
visibility of assets



Industry leading  
cyber security



- Up to 100 Gbps switching capacity
- 8x density with backplane stacking
- Unrivaled timing and synchronization: 50ns per hop PTP accuracy
- Better throughput: 5K TCAM entries

- Endpoint and application visibility with Cyber Vision and NBAR2
- Better assurance: Full Flexible NetFlow and IOS-XE telemetry

- Operational vulnerability and security posture with Cyber Vision
- MACsec 256
- SD-Access fabric Edge and group-based policy (TrustSec)

# IE 9300 Differences Between Models



IE9300 Models	PTP	L2NAT	PRP	HSR	Dying Gasp	Cyber Vision	SDA Fabric Edge	Vertical Stacking	Uplink SFP (Mbps)
IE-9310-26S2C 	✓	✓	--	--	✓	✓	✓	--	1000
IE-9320-26S2C 	✓	✓	✓	✓	✓	✓	✓	✓	100/1000

- Both models have the same scale and performance capabilities
- IE9320 has an FPGA that allows for PRP and HSR functionality
- IE9320 extends its backplane for stacking through its UADP ASIC

✓ at FCS  
✓ post-FCS

# Cisco Catalyst IR8300 Router

## Unleashing enterprise features at the industrial edge



### IR8340

4 copper • 4 combo • 4 SFP • 2 combo WAN ports  
4 expansion slots  
5G • SD-WAN  
Redundant power supplies  
20x increased encryption\*



Unrivaled  
performance at scale



Unprecedented  
visibility of assets



Industry leading  
cyber security

- Single integrated platform for routing, switching and security
- Easier to manage: One control plane for Layer 2 and Layer 3
- Full MPLS Layer 3 support

- DNA-Center and SD-WAN
- 8 core processor for dispersed workloads
- PoE, PoE+ and UPoE
- Backwards compatible with Serial
- Only Cisco router that converts GNSS time to NTP, PTP, SyncE

- Security and visibility with Cyber Vision
- Hardware based MACSec LAN and WAN
- IPSEC - DMVPN, FlexVPN, IKEv1, IKEv2
- URL filtering, Cisco AMP, Snort (IPS/IDS)
- Group based policy (TrustSec)
- Policy edge node support (DNA Center)
- Zone based firewall

\* Encrypted throughput vs. previous generation

# Automated deployment and management Cisco DNA-Center & SD-WAN



# Network Management for Utilities

## Substation Automation



### DNA-Center

#### Substation LAN

Switches, Routers, Wi-Fi  
Infrastructure

For IT/OT

On-premises

Up front initial  
investment for HW and  
SW



### SD-WAN

(vManage)

#### Utility WAN

Routers

For IT

On-premises or cloud

Subscription based on  
usage for cloud

## Field Area & Distribution Automation



### Field Network Director

#### Field Area, Distributed Automation & Secondary Substation Networks

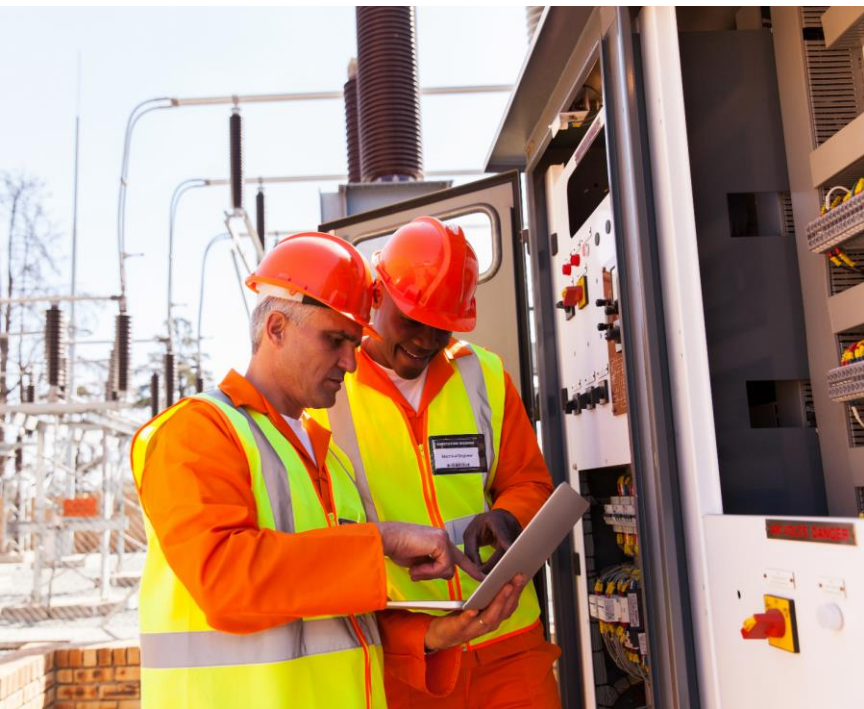
Automated Meters and Industrial Routers

For OT

On-premises

Up front initial  
investment for HW and  
SW

# The **Network is integral** to modern automation & control



Digitization requires Enterprise Applications to communicate with all assets

**Network uptime** is critical to increasing production, reducing costs, and improving quality

# Predictive Maintenance for your industrial network – proactively identify and mitigate connectivity issues

Before → After

Hours spent fixing  
network faults

Resolve issues  
with a single  
module click

Automatically detect and prioritize issues  
AI/ML-driven remediation for quick resolution  
Improve network performance

Cisco DNA Center **Assurance**



Constant monitor of network and devices for up-to-date visibility



AI/ML and machine reasoning for root cause analysis, to find anomalies instantly



Correlated insights, with telemetry data to accurately pinpoint root cause



Guided remediation allows for single-click resolution, allowing machine reasoning automation to close the loop

# Cisco DNA Center Network Automation to drive operational efficiency and streamline maintenance

Base  
Automation

Before → After

Manual device  
configuration

Simple automated  
workflows

Workflows to do in seconds what used to take hours / days

Lower cost of network operations

Bridge the IT skill gap and save time

Cisco DNA Center Base  
**Automation**



Zero-touch provisioning speeds and simplifies adding new devices ( PNP, RMA)



Software image management (SWIM) provides consistency for better network performance



Machine reasoning (MR/ML) workflows automate complex tasks into the simple push of a button

# Compliance Checks to ensure changes made to the network are consistent with your standards

Network  
Compliance

Before → After

Discrepancy  
between As-Built  
vs As-Is network

Insights on  
deviations to  
ensure compliance

Continuous monitoring for network changes

Audit logging to track who (and what/when) made changes

Cisco Product Security Incident Response Team Alerts

Cisco DNA Center **Compliance**

CISCO *Live!*

## Configuration Drifts

Compliance Summary > Startup vs Running Configuration

Change History



Startup Config (375 Lines) - July 27, 2021 01:24 PM

Running Config (374 Lines) - July 27, 2021 01:24 PM

16	aaa authorization network cts-list group ISE	16	aaa authorization network cts-list group ISE
17	aaa authorization auth-proxy default group ISE	17	aaa authorization auth-proxy default group ISE
18	aaa server radius dynamic-author	18	aaa server radius dynamic-author
19	client 10.13.48.184	19	server-key ***** 070C705F4D06485744
20	server-key ***** 070C705F4D06485744	20	aaa session-id common
21	aaa session-id common	21	clock timezone EST -5 0
22	clock timezone EST -5 0		



“Golden Image” confirmation for all network devices



Critical Security Advisories – “Psirts”



## Network Management made easy with **Cisco DNA Center**

**CISCO** *Live!*

#CiscoLive

BRKIOT-2015



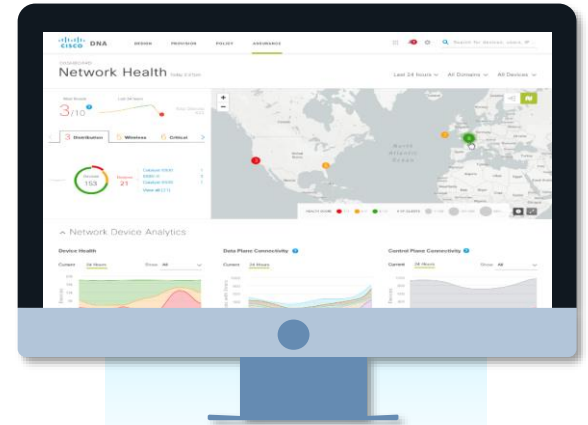
Reduce  
Downtime



Increase  
Efficiency



Stay  
Compliant





# Introducing Cisco SD-WAN

## Summary of Basic SD-WAN Capabilities\*

Circuit Load Balancing  
Direct Internet Access  
Centralized Management & Orchestration  
Circuit Cost Savings



## Cisco SD-WAN extended capabilities

### Multi-layered Security



Security & Segmentation



Analytics & Visibility

### Application Optimization



Voice Optimization



SaaS/IaaS Optimization



App Aware Dynamic Routing

### Enterprise Scale



Open and Programmable

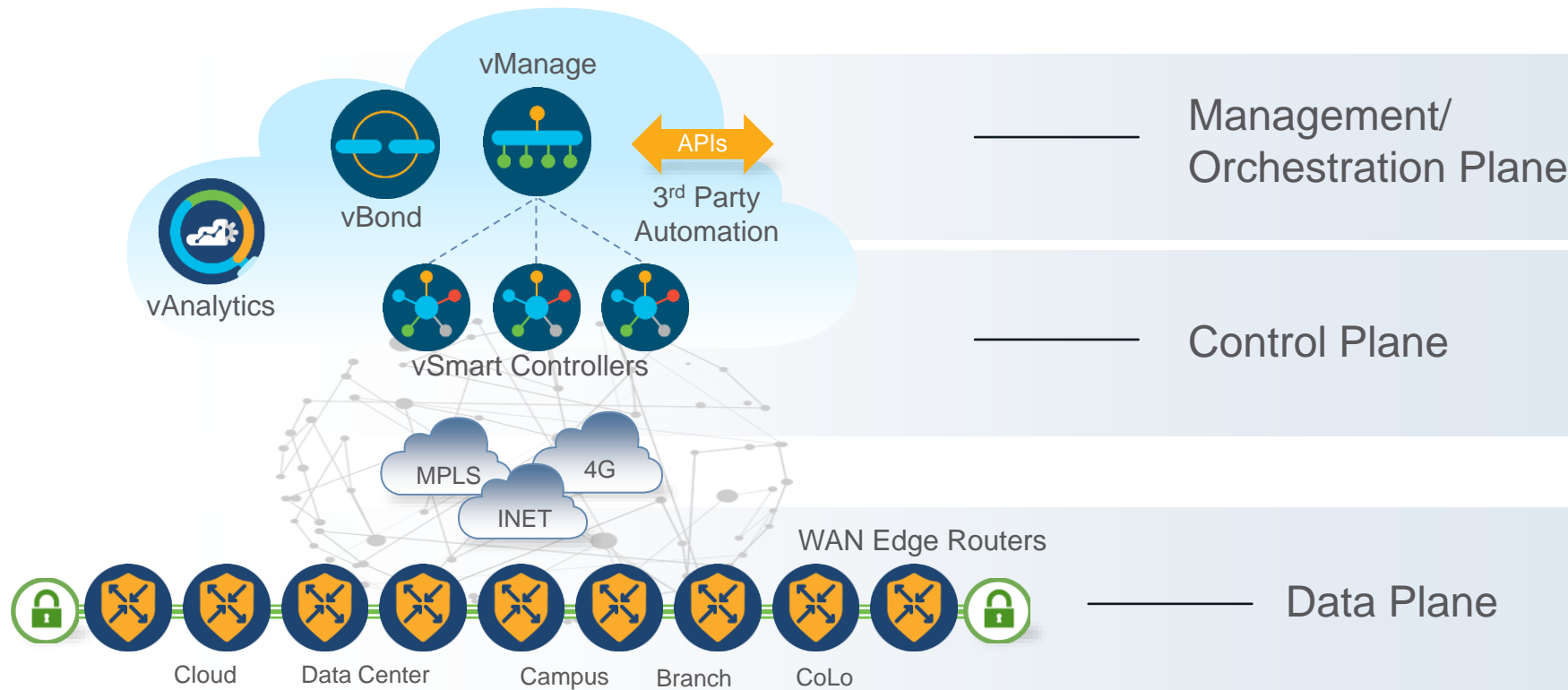


Multi-Tenant/  
Multi-Domain

\*Gartner Critical Capabilities for WAN Edge Infrastructure, December 2018

# Cisco SD-WAN Solution Overview

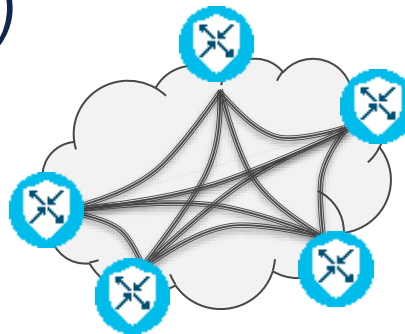
Applying SDN Principles Onto The Wide Area Network



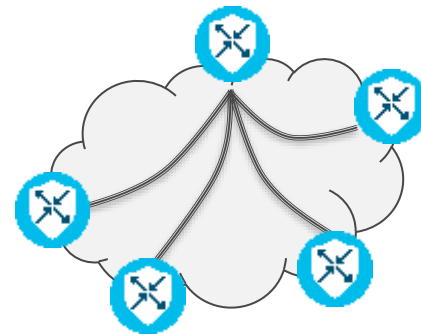
# Build topologies (per VPN)

## Using centralized policy

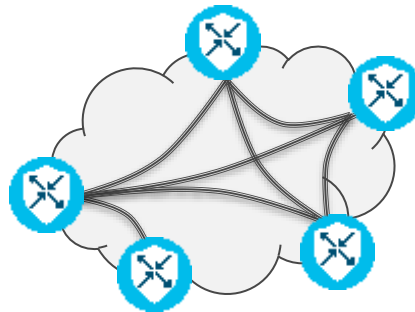
- Each Service VPN can have its own topology
  - Full-mesh, hub-and-spoke, partial-mesh, point-to-point, etc.
- Operator can build their VPN topologies using centralized policies
- Applications can benefit from shortest path, e.g. voice uses a full-mesh topology
- Security compliance can benefit from controlled connectivity topology, e.g. PCI data takes hub-and-spoke topology



VPN 1  
Full-Mesh



VPN 2  
Hub-and-Spoke



VPN 3  
Partial Mesh



VPN 4  
Point-to-Point

# Benefits of Cisco SD-WAN

Predictable app  
experience



Support for evolving  
business application  
strategy

Cloud OnRamp for IaaS,  
SaaS and Colocation

Right security, right place



Secure segmentation across  
entire network stack

Full edge security stack from  
branch to cloud and  
colocations

Enterprise grade,  
simplified



Intent-based networking  
with multi-domain policy

Proven deployments to  
over 10,000+ sites

One user interface for security and SD-WAN across branch, cloud, and colocation

# Cisco next generation substation architecture delivers

Digitization isn't easy



Cisco DNA Center  
& ISE



Cisco SD-WAN



Catalyst IE9300 Rugged  
Series Switch



Catalyst IR8300 Rugged  
Series Router

Visibility of all networked equipment



Cyber security standards



More Devices, Data & Bandwidth



More capabilities in a smaller footprint



Highly resilient networks



IEC 61850 & Precision timing



# Only Cisco can support IT and Operations

Accelerate industrial digitization



## Best of enterprise and industrial networks

- Single architecture
- IT teams - support operations without retraining
- Ruggedized for any environment



## Market leading industry expertise

- #1 in market share across enterprise and industrial networking
- Decades of experience



## Resources to ensure success

- Cisco Validated Designs
- Award-winning dev program
- CX services
- 330 specialized partnerships globally



# 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.



# Continue your education

- 1 Industrial Zero Trust: Opportunities and Realities ([BRKIOT-2012](#))
- 2 Leveraging Visibility to drive Zero Trust for Industrial Security ([BRKIOT-2353](#))
- 3 Securing Industrial Networks: Where do I start? ([BRKSEC-2077](#))
- 4 Extending Cisco Cyber Vision capabilities by using REST API ([DEVNET-1818](#))
- 5 Cisco's IoT Switching Portfolio ([PSO-IOT2007](#))

# 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](https://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](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*



#CiscoLive