



Cisco Community Community Live event

May the SD-WAN Force Be With You

Juan Flores, Technical Consulting Engineer

Juan Rangel, Technical Consulting Engineer, CCIE #62667

January 19th 2021

News & Upcoming events



Ask Me Anything following the event



Now through Friday January 29, 2021

May the SD-WAN force be with you
With Juan Flores and Juan Rangel

Participate: <http://bit.ly/AMA-cl19thjan>



Juan Flores
Technical Consulting Engineer

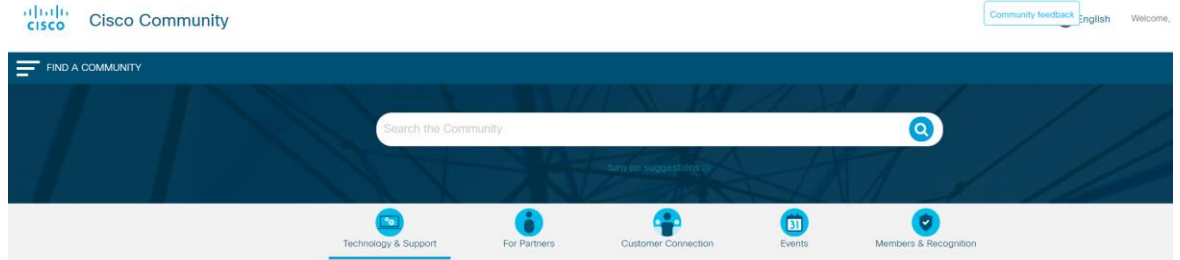


Juan Rangel
Technical Consulting Engineer

Become an event Top Contributor!

Participate in Live Interactive Technical Events and much more

<http://bit.ly/EventTopContributors>



Cisco Community / Events Top Contributors

Events Top Contributors



This program recognizes Cisco experts in the Cisco Community (CSC) that host technical events (Webcasts, Ask the Experts, Tech Talks, and Facebook Forums.) With this program, Cisco recognizes the positive, valuable influence that our top Cisco experts exert on the communities. To learn more, please visit our [FAQs](#)

2014 2013



Julio Carvajal



Ryota Takao



Cisco Designated VIPs

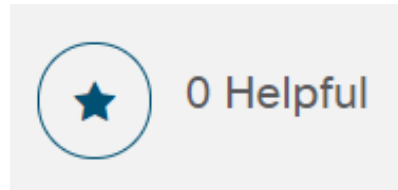


The Cisco Designated VIP program recognizes the top external individual contributors in Cisco's online communities, including the Cisco Support Community (CSC), Cisco Learning Network (CLN) and the Cisco Developers Network (CDN). Cisco Designated VIPs are recognized by their peers for their expertise and tireless contributions, and their abundant participation is vital to community success. With this program, Cisco formally recognizes the positive, valuable influence our top individual members exert on the communities overall. [FAQs](#)

Rate content at the Cisco Community

Help us to recognize the quality content in the community

Rate documents,
Videos & blogs!



Encourage and acknowledge people who
generously share their
time and expertise



Cisco Community Experts



Juan Rangel
Technical Consulting Engineer



Juan Flores
Technical Consulting Engineer

Thank You For
Joining Us Today!



Download Today's Presentation
<http://bit.ly/cl-SlidesJan19th>

Submit Your Questions Now!

Use the **Q&A** panel to submit your questions and the panel of experts will respond.

They will be answered eventually



Please take a moment to complete the survey at the end of the event



Community Live

May the SDWAN force be with you

Juan Flores

Technical Consulting Engineer

Juan Carlos Rangel/ CCIE R&S#62667

Technical Consulting Engineer

January 19, 2021

Description

- In this session, attendees will learn about, SD-WAN Introduction, the importance of control connections.
- How to configure devices using Templates (Device/Feature) and the importance of OMP Protocol with a Live demo during the event to provide a practical overview about the protocol and it's capabilities

Agenda

- Introduction to SDWAN
- Control connections
- SDWAN Templates (Device/Feature)
- OMP (overlay management protocol)
- Live Demo: OMP

Polling Question 1

Have you migrated your traditional network to SD-WAN?

- A. Yes
- B. No

Introduction to SDWAN

What is the benefice of SDWAN over traditional networks?

In the Cisco SD-WAN vManage console, you can easily automate virtual private gateway deployment in IaaS and PaaS environments

Cisco SD-WAN can transform your Cisco routers into advanced, multilayered security devices with an application-aware enterprise firewall, IPS, URL filter, and continuous DNS monitoring.



SD-WAN

Cisco SD-WAN is a secure, cloud-scale architecture that is open, programmable, and scalable. Through the Cisco vManage console, you can quickly establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and colocation facilities to improve network speed, security, and efficiency.



SD-WAN

- ✓ Any Deployment
- ✓ Any Service
- ✓ Any Transport
- ✓ Any Location



Cisco SD-WAN



Cisco vManage

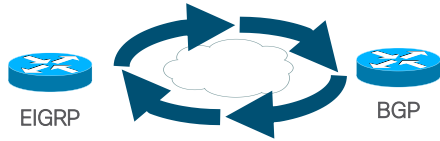
Username

Password

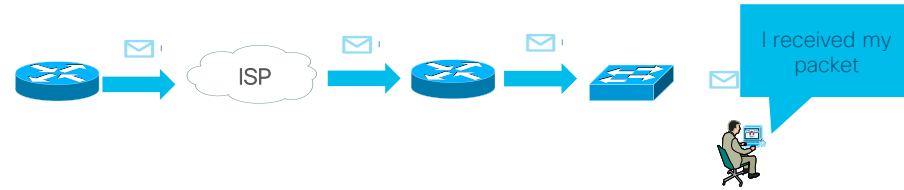
Log In

Before we continue, lets talk about fundamental definitions

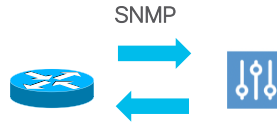
- Control plane



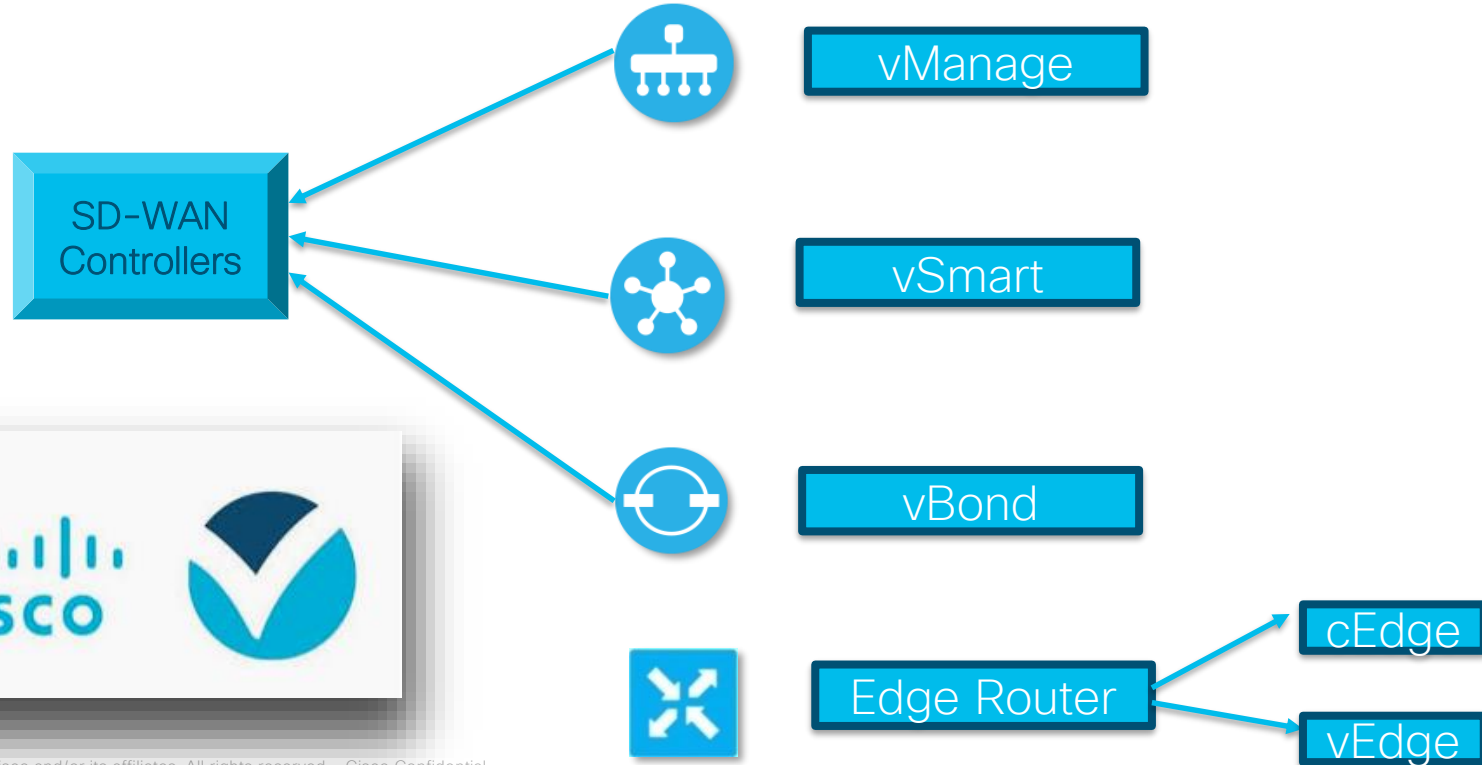
- Data plane



- Management plane



SD-WAN Components



cEdge & vEdge

Branch Services

ISR 1000



Next-gen
Performance
flexibility

ISR 4000



Modular
Integrated
service
containers

ASR 1000



High-performance
HW & SW
redundancy

SD-WAN

vEdge 100



100 Mbps
4G LTE & WiFi

vEdge 1000



Up to 1 Gbps
Fixed

vEdge 2000



10 Gbps
Modular

vEdge 5000



20 Gbps, Modular

Virtualization

ENCS 5100



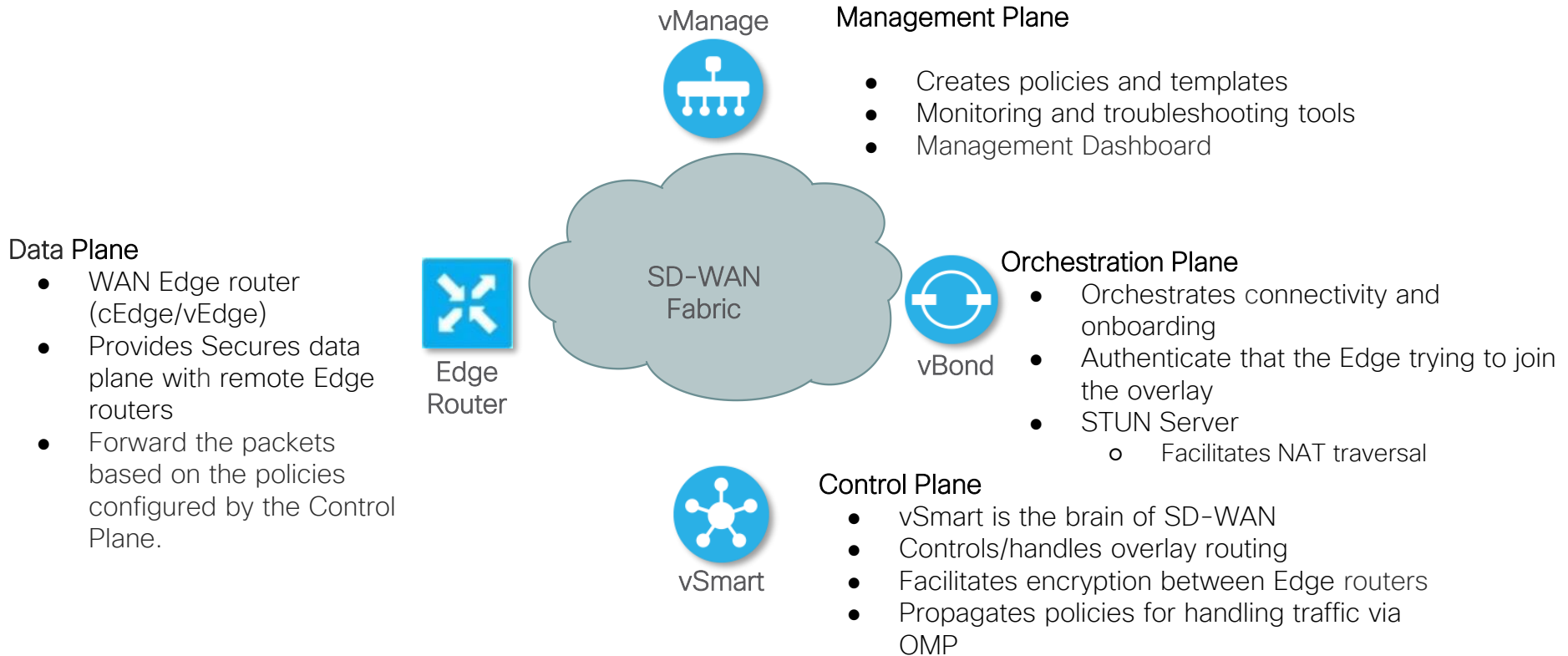
ENCS 5400



Public Cloud



What is the function of the components?



Polling Question 2

May I convert my traditional cisco router into SDWAN?

- A. Yes
- B. No
- C. I don't know

SD-WAN important concepts

- ✓ **Overlay Management Protocol**

Control plane protocol distributing reachability, security and policies throughout the fabric

- ✓ **Transport Locator (TLOC)**

A TLOC, or Transport Location, is the attachment point where a WAN Edge router connects to the WAN transport network.

- ✓ **Color**

The color attribute applies to WAN Edge routers or vManage and vSmart controllers and helps to identify an individual TLOC;

- ✓ **Site ID**

Is a unique identifier of a site in the SD-WAN overlay network with a numeric value 1 through 4294967295

- ✓ **System IP**

A System IP is a persistent, system-level IPv4 address that uniquely identifies the device independently of any interface addresses.

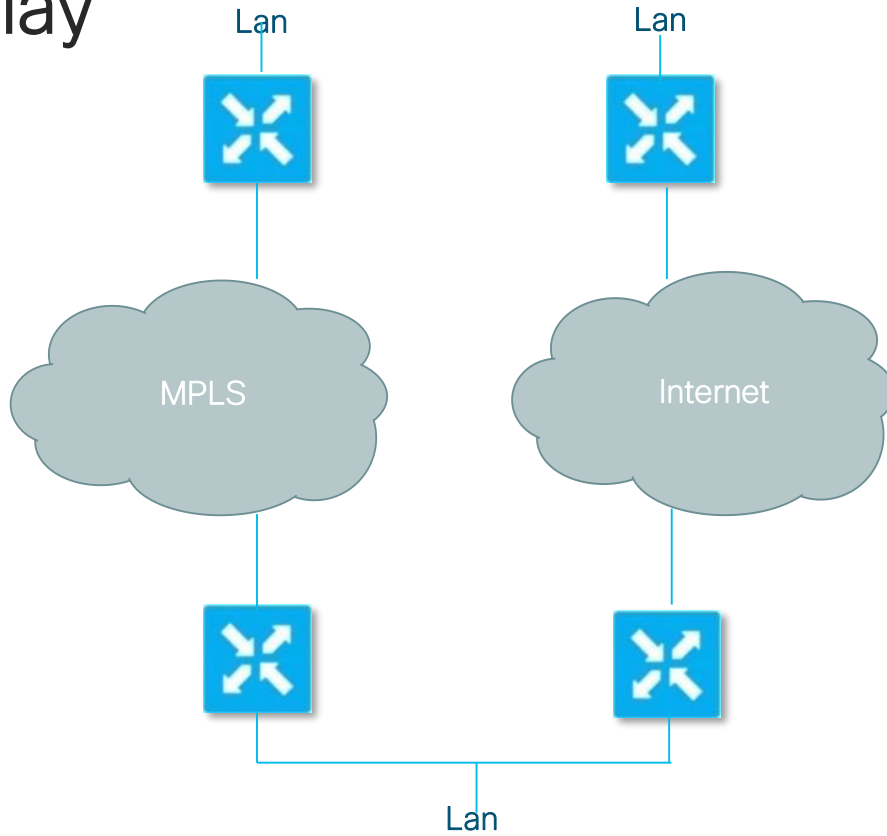
- ✓ **Organization Name**

Is a name that is assigned to the SD-WAN overlay.

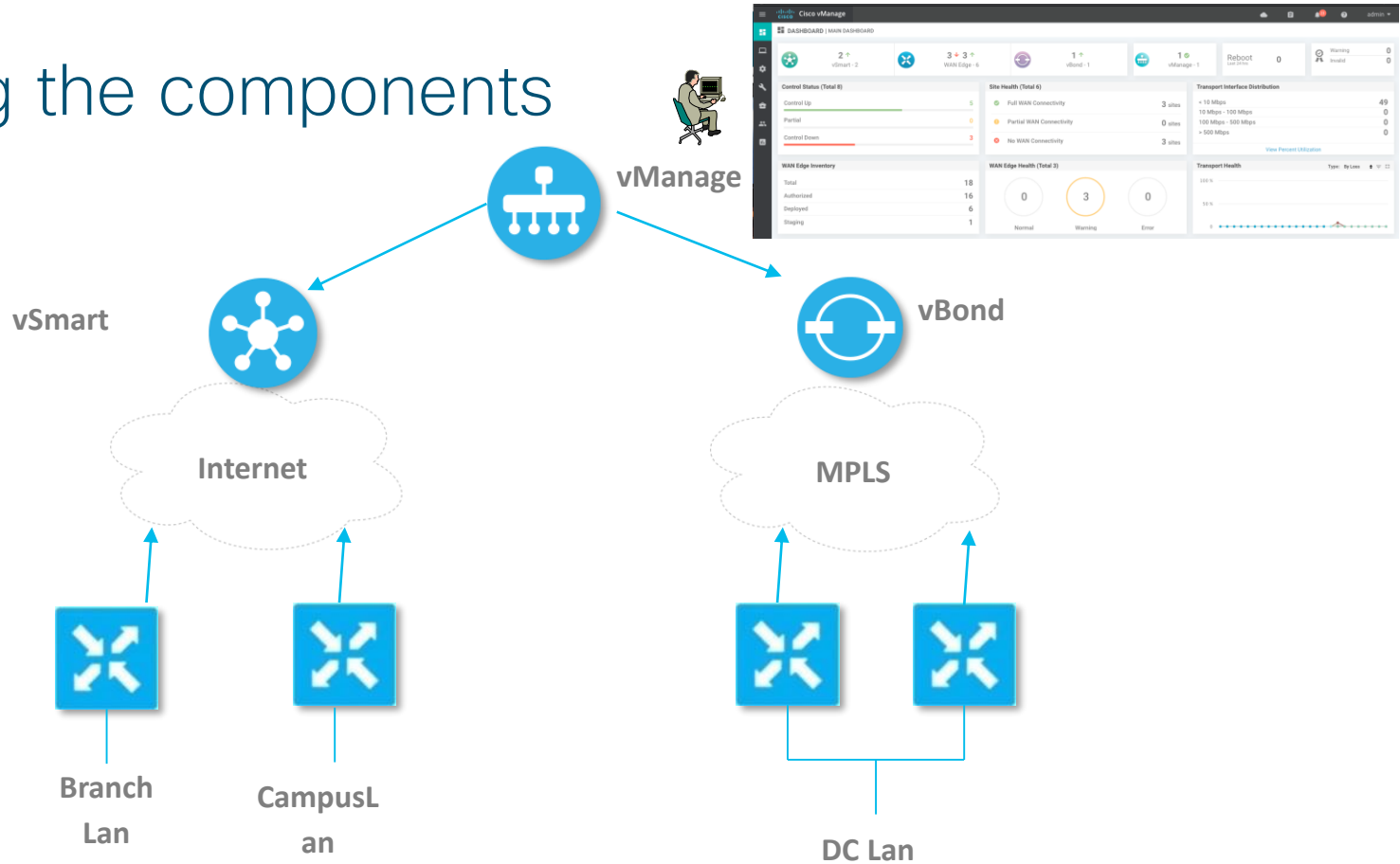
- ✓ **VPN**

(VPNs) provide segmentation, much like Virtual Routing and Forwarding instances (VRFs)

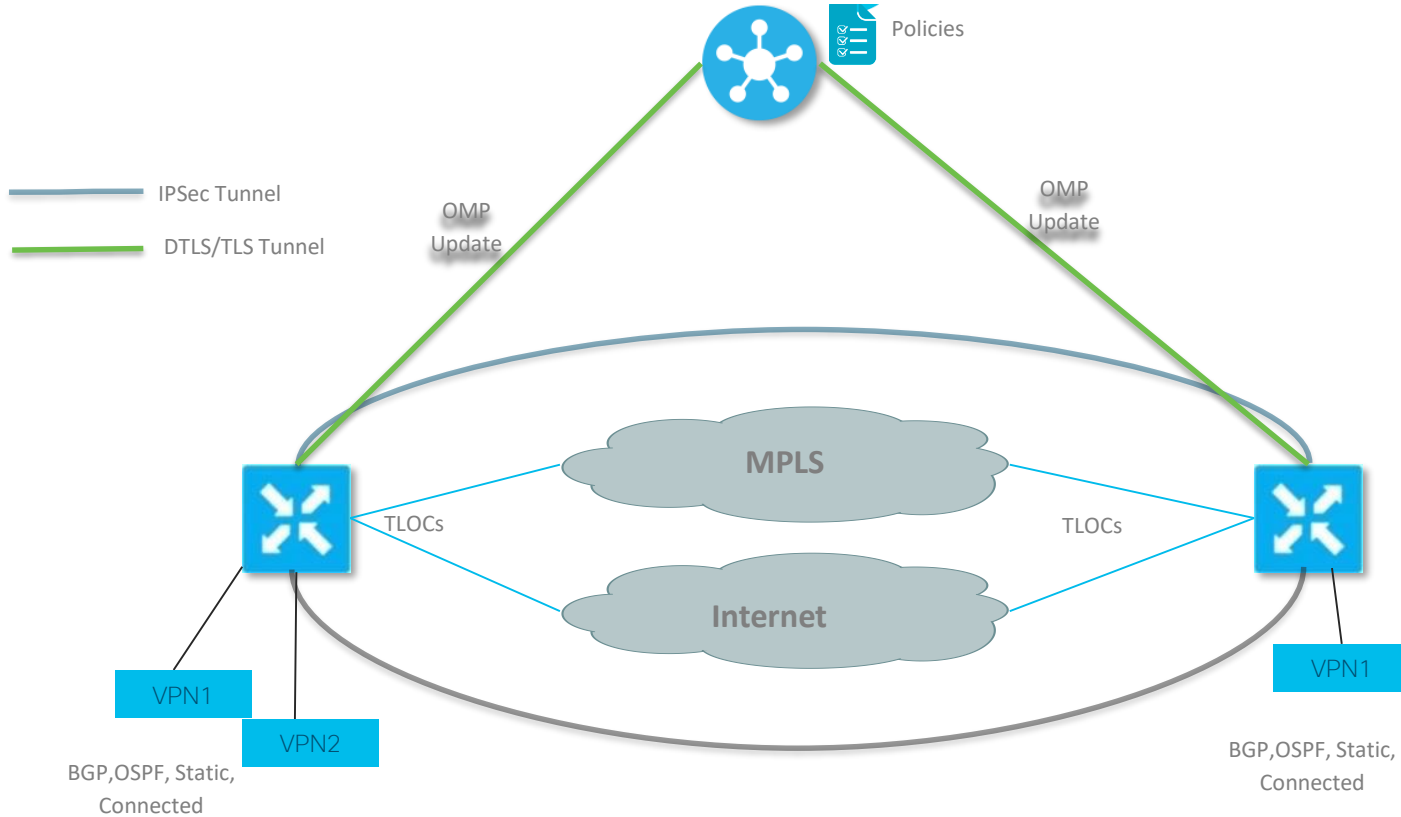
Underlay



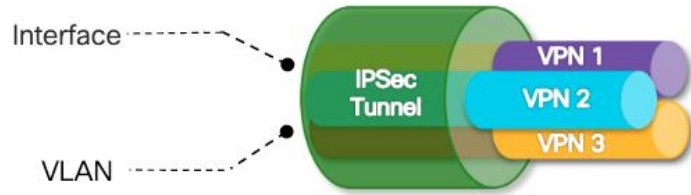
Adding the components



SD-WAN Fabric Operation



Traffic Secure



VPN Topology

Full Mesh

Hub and Spoke

Partial Mesh

Point to Point





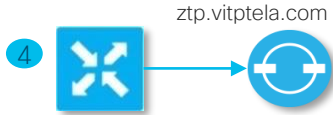
vEdge Powers up!



vEdge gets ip from DHCP



vEdge resolves ztp.viptela.com



vEdge gets verified by ZTP



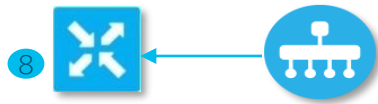
ZTP provides the Org vBond



vEdge gets verified and connects to Org vBond



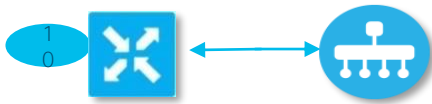
vEdge gets verified and connects to vManage



vManage provides system IP



vEdge connects to vBond



vEdge connects to vManage and receives its full configuration



vEdge joins the Overlay



Polling Question 3

Do you know on which transport I can deploy SD-WAN

- A. Yes
- B. No

Control Connections

Control Connections

The SD-WAN Control Connections (CC) are DTLS sessions established between different nodes (controllers and edge routers)

Basic components

System-ip

Site-id

Org-name

vBond

Vpn0

Interface

Tunnel-interface

Default-route

Lets validate basic configuration on vEdge

It is Important to have the Certificate valid

```
vEdge100B-01-0246AE6# show control local-properties
personality                                vedge
sp-organization-name                      LAB_SD-WAN_20-x
organization-name                         LAB_SD-WAN_20-x
root-ca-chain-status                      Installed

certificate-status                        Installed
certificate-validity                       Valid
certificate-not-valid-before              May 12 05:45:08 2013 GMT
certificate-not-valid-after               Jan 19 03:14:07 2038 GMT

enterprise-cert-status                    Not-Applicable
enterprise-cert-validity                  Not Applicable
enterprise-cert-not-valid-before          Not Applicable
enterprise-cert-not-valid-after           Not Applicable

dns-name                                  192.168.255.2
site-id                                   210161071
domain-id                                 1
protocol                                  dtls
tls-port                                  0
system-ip                                 2.46.6.107
```

How I can validate my transport interfaces?

```
vEdge100B-01-0246AE6# show control local-properties wan-interface-list
```

```
NAT TYPE: E -- indicates End-point independent mapping
A -- indicates Address-port dependent mapping
N -- indicates Not learned
Note: Requires minimum two vbonds to learn the NAT type
```

RESTRICT/ CONTROL/ INTERFACE	LAST PUBLIC LAST IPv4	SPI TIME PORT	VM		PRIVATE IPv6	PRIVATE PORT	VS/VM COLOR	STATE	CNTR MAX
			PUBLIC PRIVATE	NAT CON					
ge0/0.850	172.16.107.1	12366	172.16.107.1	::	12366	1/0	mpls	up	2
no/yes/no	No/No	0:00:00:02	0:02:57:43	N	5				
ge0/0.855	210.16.107.1	12366	210.16.107.1	::	12366	1/1	biz-internet	up	2
no/yes/no	No/No	0:00:00:16	0:02:57:44	N	5				

What colors do we have and how many transports?

Control Connections

By default, all Cisco vEdge devices use base port 12346 for establishing the connections that handle control and traffic in the overlay network. Each device uses this port when establishing connections with other Cisco vEdge devices.

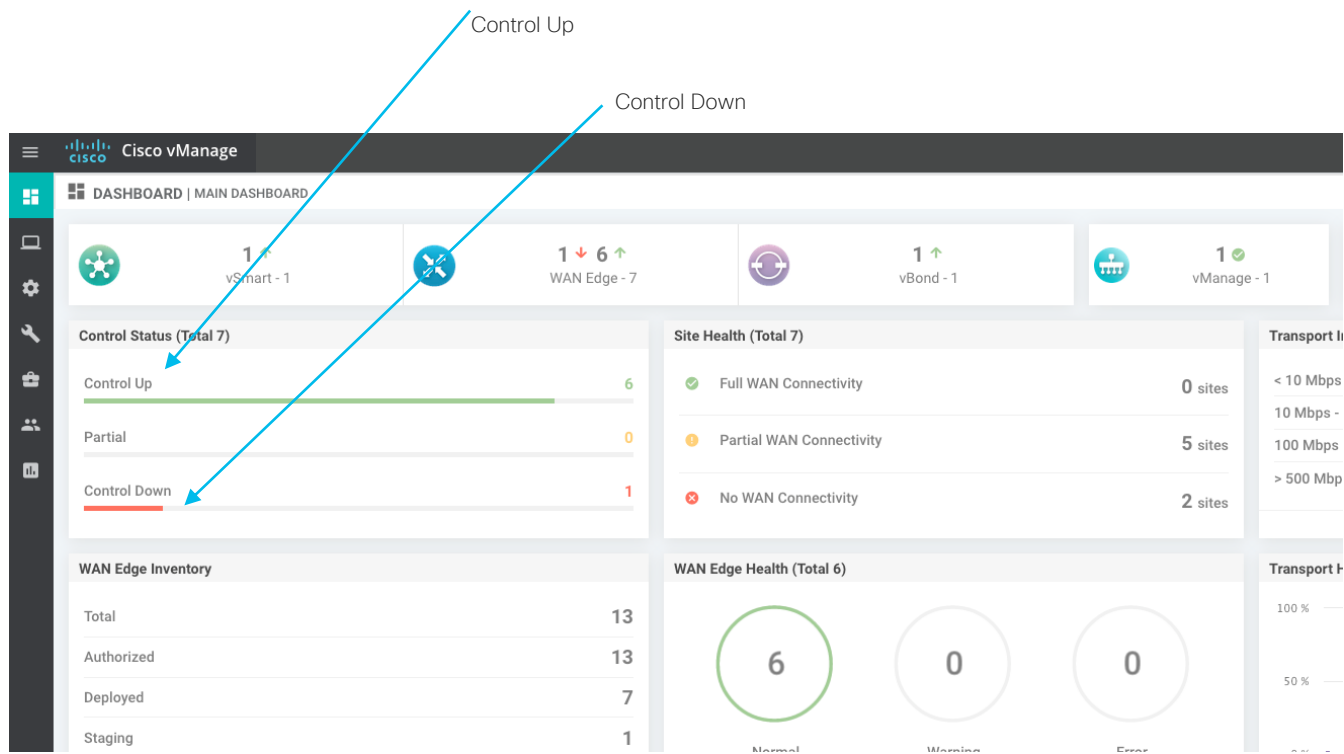
I need to validate the control connections status



```
vEdge100B-01-0246AE6# show control connections
```

PEER	PEER	PEER	CONTROLLER			PEER		PEER	
			SITE	DOMAIN	PEER	PRIV	PEER	PUB	
TYPE	PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	PORT	LOCAL
COLOR	PROXY	STATE	UPTIME	ID					
vsmart	dtls	1.1.1.3	1	1	192.168.255.3	12346	192.168.255.3	12346	mpls
	No	up	22:21:02:20	0					
vsmart	dtls	1.1.1.3	1	1	192.168.255.3	12346	192.168.255.3	12346	biz-in
	No	up	22:21:02:07	0					
ternet	dtls	0.0.0.0	0	0	192.168.255.2	12346	192.168.255.2	12346	mpls
	-	up	22:21:02:32	0					
vbond	dtls	0.0.0.0	0	0	192.168.255.2	12346	192.168.255.2	12346	biz-in
	-	up	22:21:02:25	0					
vmanage	dtls	1.1.1.1	1	0	192.168.255.1	12346	192.168.255.1	12346	biz-in
ternet	No	up	0:11:12:06	0					

Control connections status on vManage



Verify Control connections for one device

Device Dashboard

The screenshot displays the Cisco vManage interface for a vEdge Cloud device. The breadcrumb navigation shows 'MONITOR Network > Control Connections'. The device details are 'vEdge20 | 1.1.1.254', 'Site ID: 254', and 'Device Model: vEdge Cloud'. The status indicates 'vSmart Control Connections (Expected: 1 | Actual: 1)'. A diagram shows a central 'private1' node connected to 'vSmart 1/1' and 'vManage 1/1'. Below the diagram is a table of connections.

Peer Type	Peer System IP	Peer Protocol	Private Port	Public Port	Controller Group ID	Last Updated
private1	--	--	--	--	--	--
vmanage	1.1.1.1	dtls	12546	12546	0	13 Jan 2021 1:20:26 PM CST
vsmart	1.1.1.3	dtls	12346	12346	0	13 Jan 2021 1:20:41 PM CST

Real time commands

MONITOR Network > Real Time

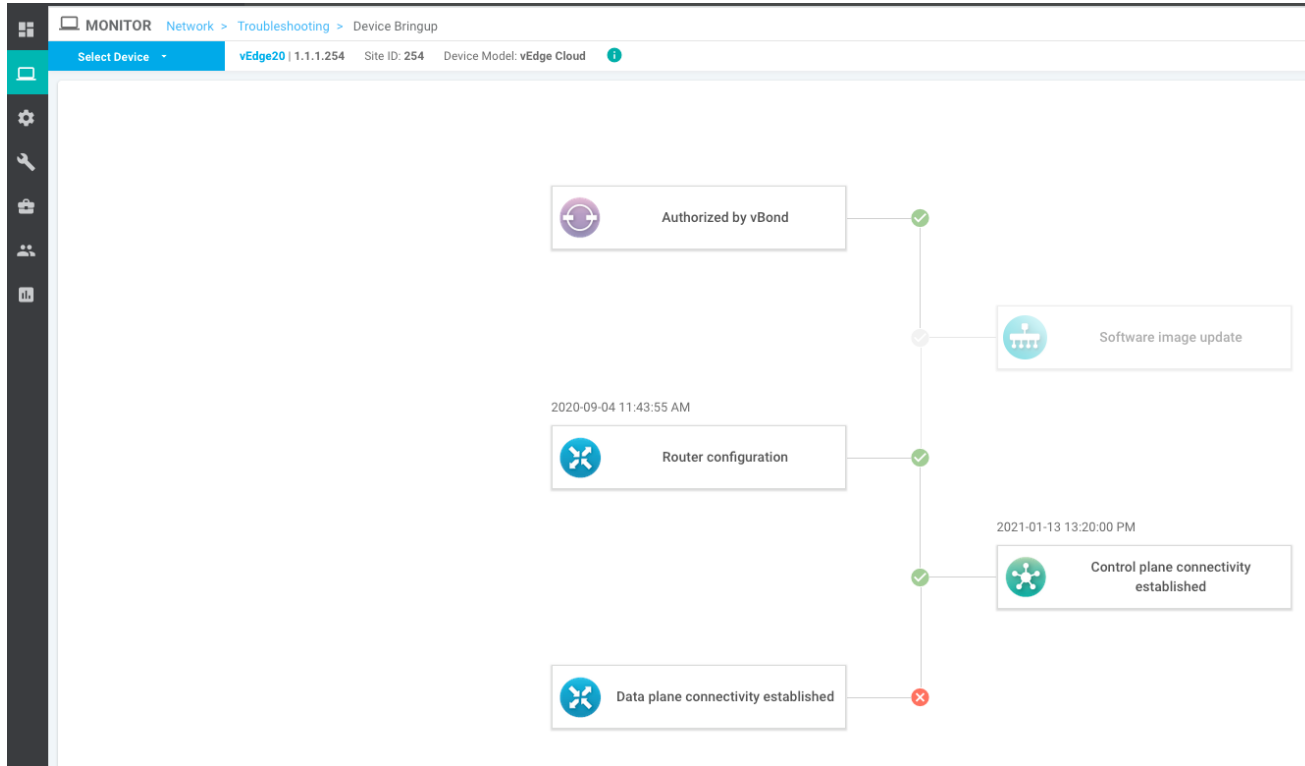
Select Device vEdge20 | 1.1.1.254 Site ID: 254 Device Model: vEdge Cloud

Device Options: omp|

- OMP Advertised Routes
- OMP Advertised TLOCs
- OMP Multicast Advertised Auto Discover
- OMP Multicast Advertised Routes
- OMP Multicast Received Auto Discover
- OMP Multicast Received Routes
- OMP Peers
- OMP Received Routes
- OMP Received TLOCs
- OMP Services
- OMP Summary
- OMP CloudExpress Routes

Host	Hostname	Type	Domain ID	Site ID	State	Legit
	smart20	vsmart	1	1	up	yes

Device Bring up



Why the control connection could fail?

Issues with the connectivity

- DTLS
- Tloc disabled

Issues with the certificate

- Certificate verification failed
- Incorrect Organization name
- Certificate was revoked or invalidated
- Serial number is not present

How to troubleshoot?

The command “show control connections-history” provide us a list of possible failures.

```
vEdge100B-01-0246AE6# show control connections-history
Legend for Errors
ACSRREJ - Challenge rejected by peer.
BDSGVERFL - Board ID Signature Verify Failure.
BIDNTPR - Board ID not Initialized.
BIDNTVRFD - Peer Board ID Cert not verified.
BIDSIG - Board ID signing failure.
CERTEXPRD - Certificate Expired
CRTREJSER - Challenge response rejected by peer.
CRTVERFL - Fail to verify Peer Certificate.
CTORGNMIS - Certificate Org name mismatch.
DCONFALL - DTLS connection failure.
DEVALC - Device memory Alloc failures.
DHSTMO - DTLS HandShake Timeout.
DISCVBD - Disconnect vBond after register reply.
DISTLOC - TLOC Disabled.
DUPCLHELO - Recd a Dup Client Hello, Reset G1 Peer.
DUPSER - Duplicate Serial Number.
DUPSYSIPDEL - Duplicate System IP.
HAFAIL - SSL Handshake failure.
IP_TOS - Socket Options failure.
LISFD - Listener Socket FD Error.
MGRTLCKD - Migration blocked. Wait for local TMO.
MEMALCFL - Memory Allocation Failure.
NOACTVB - No Active vBond found to connect.
NOERR - No Error.
NOSLPRCRT - Unable to get peer's certificate.
NEWVBNOVMNG - New vBond with no vMng connections.
NTPRMINT - Not preferred interface to vManage.
HWCERTREN - Hardware vEdge Enterprise Cert Renewed
EMBARGOFAIL - Embargo check failed
NOVMCFG - No cfg in vmanage for device.
NOZTPEN - No/Bad chassis-number entry in ZTP.
OPERDOWN - Interface went oper down.
ORPTMO - Server's peer timed out.
RMGSPR - Remove Global saved peer.
RXTRDWN - Received Teardown.
RDSIGFBD - Read Signature from Board ID failed.
SERNTPRES - Serial Number not present.
SSLNFAIL - Failure to create new SSL context.
STNMODETD - Teardown extra vBond in STUN server mode.
SYSIPCHNG - System-IP changed.
SYSPRCH - System property changed
TMRALC - Timer Object Memory Failure.
TUNALC - Tunnel Object Memory Failure.
TXCHTOBD - Failed to send challenge to BoardID.
UNMSGBDRG - Unknown Message type or Bad Register msg.
UNAUTHEL - Recd Hello from Unauthenticated peer.
VBDEST - vDaemon process terminated.
VECRTREV - vEdge Certification revoked.
VSCRTREV - vSmart Certificate revoked.
VB_TMO - Peer vBond Timed out.
VM_TMO - Peer vManage Timed out.
VP_TMO - Peer vEdge Timed out.
VS_TMO - Peer vSmart Timed out.
XTVMTRDN - Teardown extra vManage.
XTVSTRDN - Teardown extra vSmart.
STENTRY - Delete same tloc stale entry.
HWCERTREV - Hardware vEdge Enterprise Cert Revoked.
```

DTLS Connection Failure (DCONFAL)

This could be related to some or all packets dropped/filtered.

The next Hop of the router is not reachable

The Default Gateway is not installed in RIB

DTLS port is not open in the Controllers

Tips:

Verify the next hop

show ip route vpn 0

Verify ARP entry for the Default Gatewat

show arp

Ping the default gateway increasing the packets and mtu

ping x.x.x.x count 500 size 1000

Ping a public DNS

Ping 8.8.8.8

Ping/Traceroute to the vBond

SDWAN Templates (Device/Feature)

Templates

Device Templates allow to configure a device completely defining how it will function.

There're two main type of templates:

- Feature Templates.

 - Some are mandatory, and other features are optional

- CLI Templates.

 - It will be a “running-config” pasted in a template.

 - Template Variables can be used

Templates provide high scalability and improves user experience. Make your life easier!

Feature Template

vManage Mode

Can't do any CLI modification and commit.

CLI Mode

Traditional configuration mode.

Device Rollback Timer

Default timer 5 minutes.

*OMP (Overlay Management
Protocol)*

OMP

OMP is at the heart of the SD-WAN overlay routing.

- Responsible for establishing and maintaining the control plane.
- Orchestration of overlay network communication.
- Distribution of routing and related location mappings.
- Central control and distribution of routing policy.

OMP

Advertisements

- OMP will be advertising routes and services along with TLOCs.
- It will operate in an overlay networking environment.

Performs path selection loop, avoidance and policy implementation.

It will advertise:

- OMP Routes.
- Transport Locations (TLOCs)
- Service routes.

Redistributes information with other routing protocols such as EIGRP, OSPF and BGP.

OMP's AD is 250

Polling Question

Do you know what type of policy will handle the OMP routes in SD-WAN?

- A. Yes
- B. No

OMP

Best Path Algorithm and Loop Avoidance.

- 1- Check whether the OMP route is invalid.
- 2- If it is valid and if it learnt from the same Edge router, select OMP route with lower AD.
- 3- If the ADs are equal, select the OMP route with higher Preference value.
- 4- If Preference values are equal, Select OMP route with higher TLOC Preference value.
- 5- If TLOC preference values are equal, compare origin type and select one in the following order: Connected, Static, EBGP, EIGRP, OSPF Intra-area, OSPF inter-area, OSPF external, iBGP, Unknown.
- 6- If the origin types are the same, select OMP route with the higher RID.
- 7- If RIDs are equal, select OMP route with the higher private IP address.

Graceful Restart for OMP.

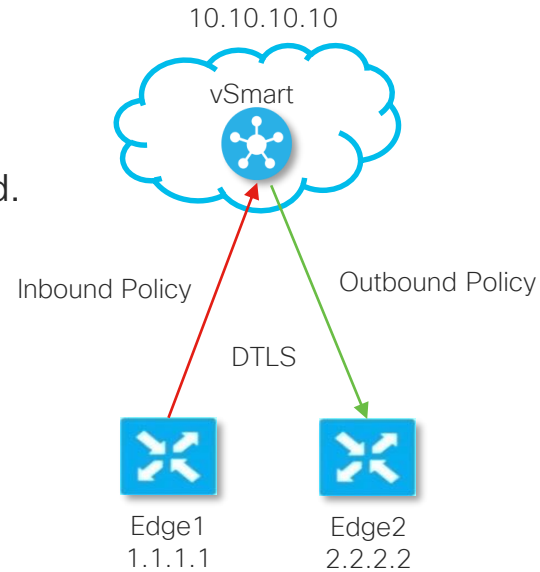
- allows the data plane in SD-WAN overlay network to continue functioning if the control plane stops functioning or becomes unavailable.

OMP

Understanding how vSmart operates.

vSmart is the Control and Data Plane authority in SD-WAN.

- Control policies can be applied inbound and outbound.
- Centralized policy is applied only on vSmart.
- vSmart behaves as a BGP route reflector.
- Control Policy will manipulate OMP routes.



Demo time!

Thanks!

Submit Your
Questions Now!



Use the Q&A panel to submit your
questions, our expert will respond

Ask Me Anything following the event



Now through Friday January 29, 2021

May the SD-WAN force be with you
With Juan Flores and Juan Rangel

Participate: <http://bit.ly/AMA-cl19thjan>



Juan Flores
Technical Consulting Engineer



Juan Rangel
Technical Consulting Engineer

Collaborate within our Social Media



Twitter

- @Cisco_Support
- <http://bit.ly/csc-twitter>

Facebook

- Cisco Community
- <http://bit.ly/csc-facebook>

Learn About Upcoming Events

We invite you to review our Social Media Channels

YouTube

- Cisco Community
- <http://bit.ly/csc-youtube>



App

- Cisco Technical Support



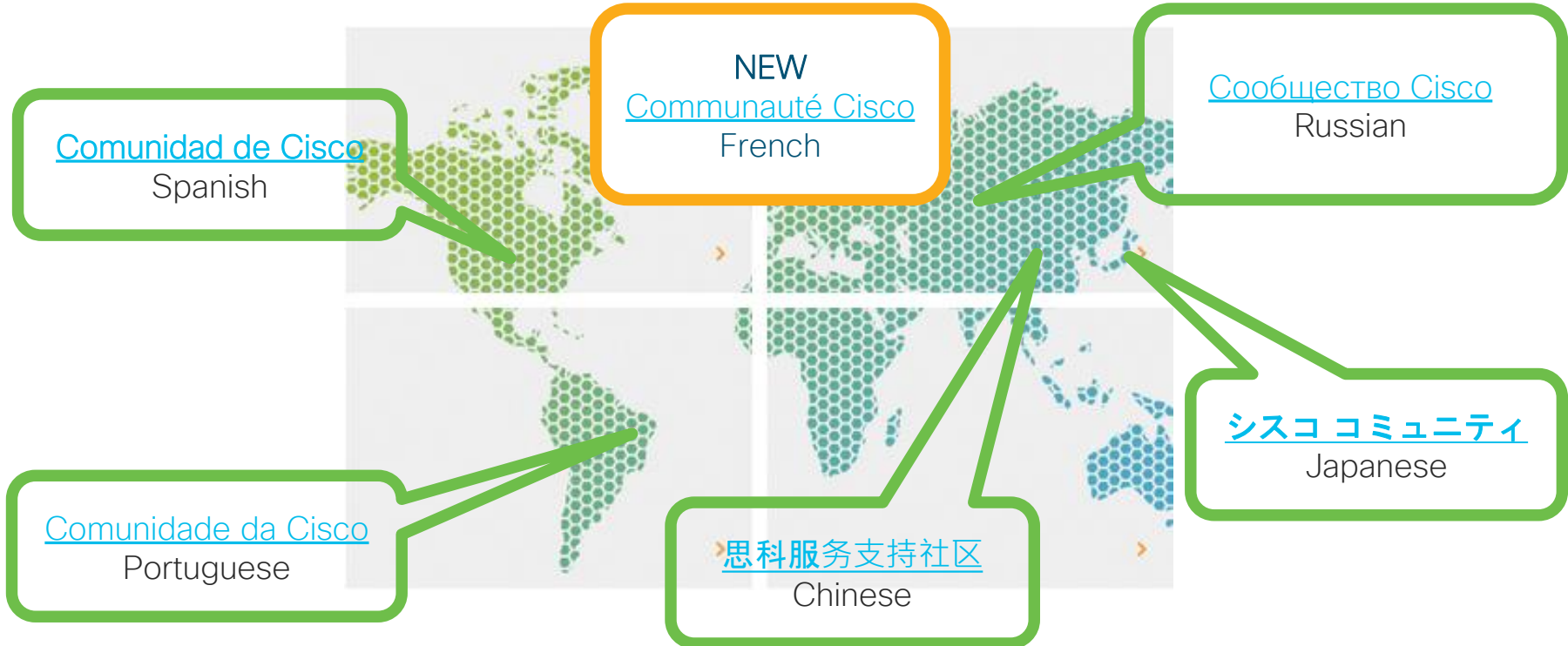
LinkedIn

- Cisco Community
- <http://bit.ly/csc-linked-in>



Cisco has support communities in other languages!

If you speak Spanish, Portuguese, Japanese, Russian or Chinese we invite you to participate & collaborate





More IT Training Videos and Technical Seminars on the Cisco Learning Network

View Upcoming Sessions Schedule
<https://cisco.com/go/techseminars>

Thank you for Your
Time!

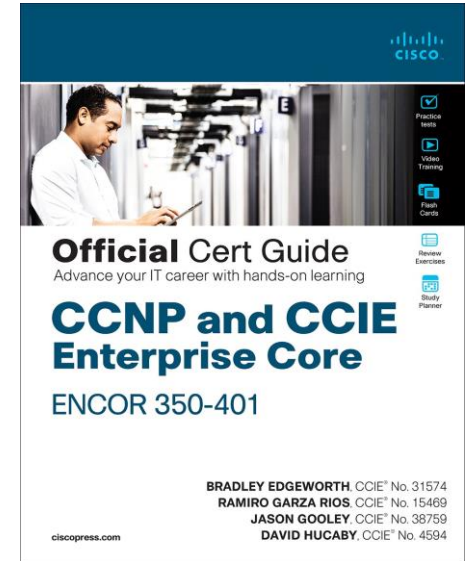
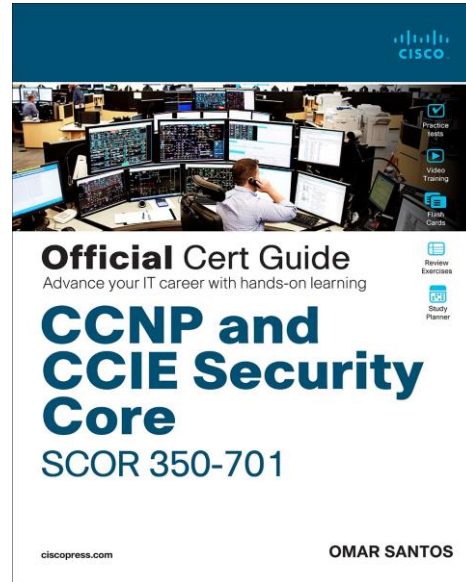
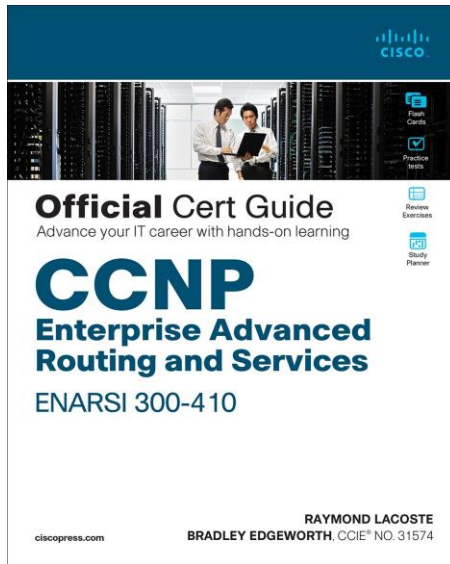
Please take a moment to complete
the survey



Thank you for participating, you earned a discount!

Redeem your 35% discount offer by entering code: CSC when checking out.

<http://bit.ly/Community-CiscoPress2020>



Thanks For Joining today!

