



Cisco Community Community Live event

Getting to know Cisco SD-WAN

David Peñaloza Seijas, Lead Network Consulting Engineer, Verizon Enterprise

Juan Flores, Technical Consulting Engineer

Juan Rangel, Technical Consulting Engineer, CCIE #62667

December 11th 2019

News & Upcoming events



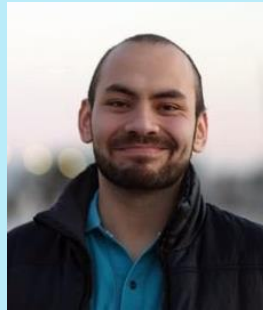
Ask Me Anything following the event

Now through Friday December 20th 2019

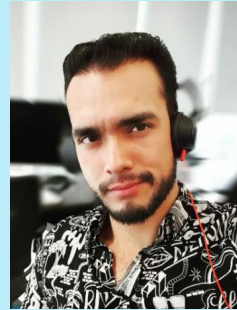


With
David Peñaloza,
Juan Flores & Juan Rangel

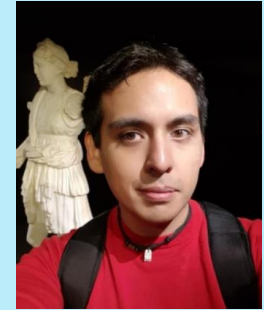
<http://bit.ly/ama-dec11>



David Peñaloza
Lead Network Consulting
Engineer



Juan Flores
Technical Consulting Engineer



Juan Rangel
Technical Consulting Engineer
CCIE #62667

Cisco Community – Ask Me Anything

Configuration, Verification & Troubleshooting of Dynamic Routing Protocols

Till Friday
December 20th 2019

With
Elvin Arias



Ask Me Anything
Elvin Arias

9 – 20 DEC

“Configuration, Verification & Troubleshooting of Dynamic Routing Protocols”

<http://bit.ly/dynamic-protocols>

Community Helping Community – Special Program

Cisco Community invites you to join Cisco in lending a hand to [Doctors Without Borders](#); an independent, global movement providing medical aid where it's needed most.

Until
January 31st, 2020

Learn more
<http://bit.ly/help-eventslides>

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

A graphic divided into two vertical panels. The left panel has a dark blue background with the text 'Community Helping Community' in white. Below the text is a circular graphic containing silhouettes of people. The right panel has a white background with the text 'Help those in need while improving the Community' in blue. Below this text is a blue button with the text 'LEARN HOW'. At the bottom of the right panel are the logos for 'MEDECINS SANS FRONTIERES DOCTORS WITHOUT BORDERS' and 'CISCO'.

Community
Helping
Community

Help those in need
while improving
the Community

LEARN HOW

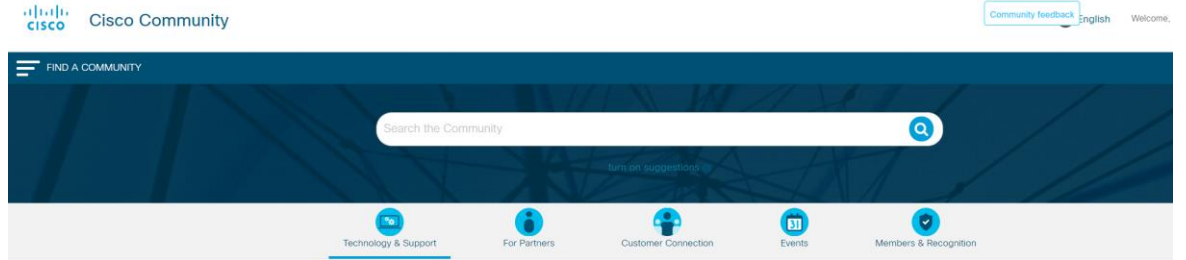
MEDECINS SANS FRONTIERES
DOCTORS WITHOUT BORDERS

CISCO

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

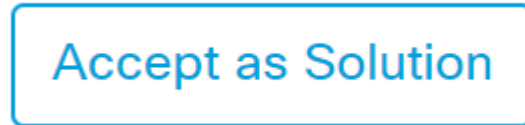
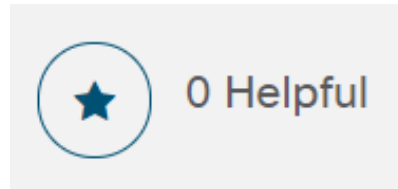


The Cisco Designated VIP program recognizes the top external individual contributors in Cisco's online communities, including the Cisco Support Community (CSC), Cisco Learning Network (CLN) and the Cisco Developers Network (CDN). Cisco Designated VIPs are recognized by their peers for their expertise 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



David Peñaloza
Lead Network Consulting Engineer



Juan Flores
Technical Consulting Engineer



Juan Rangel
Customer Success Specialist
CCIE #62667

Thank You For
Joining Us Today!



Download Today's Presentation
<http://bit.ly/slides-dec11-2019>

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 webcast



Community Live

Getting to know Cisco SD-WAN

David Penaloza Seijas

Lead Network Consulting Engineer

Juan Flores

Technical Consulting Engineer

Juan Carlos Rangel/ CCIE#62667

Technical Consulting Engineer

December 12, 2019

Description

- In this session, attendees will learn about the historical roots and drivers behind SD-WAN's adoption, its benefits, evolution and inner mechanisms that make it attractive to the businesses in the current era.
- The on-boarding activities and day 1 operations will be showcased in a live demo during the event to provide a practical overview about the solution and its capabilities

Agenda

- Evolution: Traditional WAN to SD-WAN?
- Network simplification: Why SD-WAN?
- Architecture: How does the overlay work?
- The Planes: Control, Data and Management planes
- Live Demo: Configuration and examples

Polling Question 1

Have you heard before about SD-WAN?

- A. Yes
- B. No

*Evolution: Traditional WAN to
SD-WAN?*

Evolution to SD-WAN

- Over the years, customers have worked with different types of technologies to communicate different locations through an ISP.

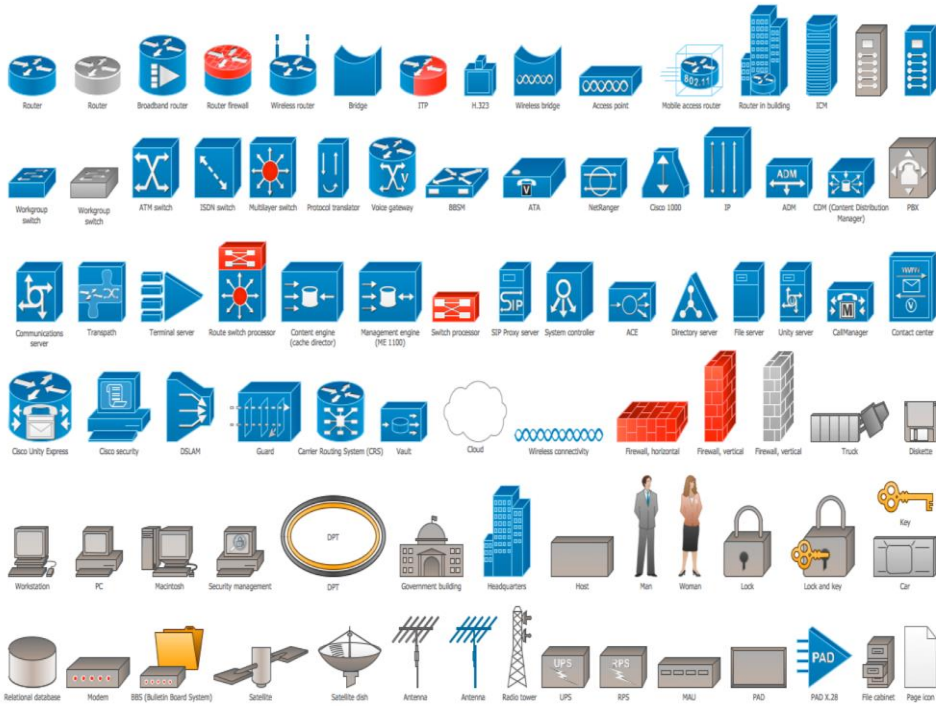


Examples of current technologies

- BGP
- MPLS Layer 3
- MPLS Layer 2
- EIGRP
- OSPF
- DMVPN
- iWAN (Pfr)



Network components

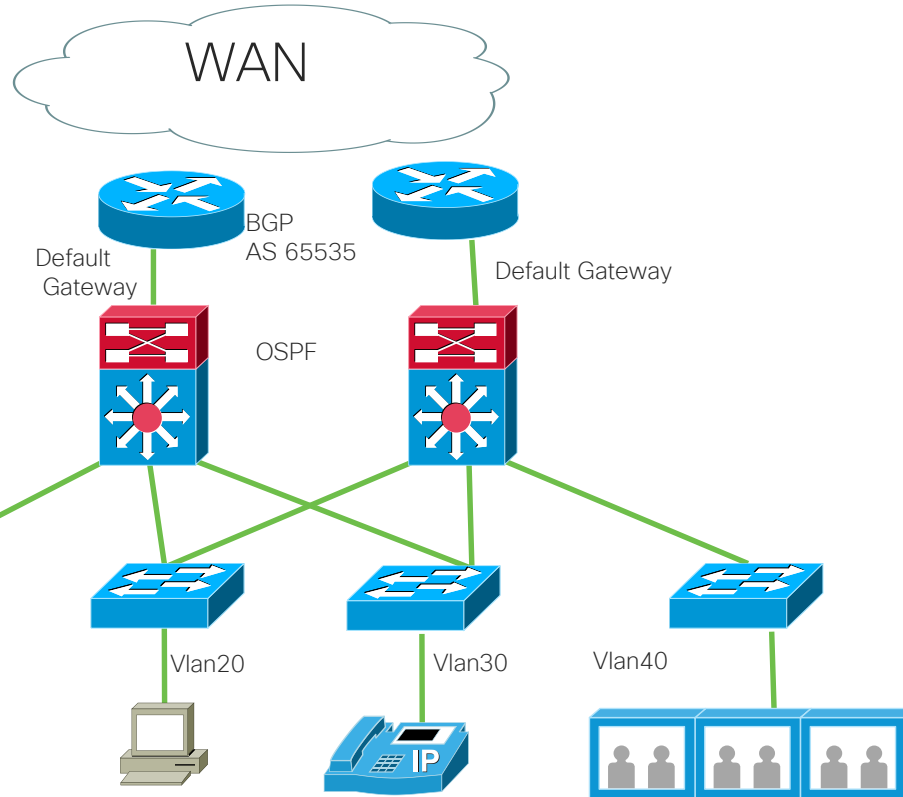


□ Networks use different components in order to share different kind of traffic such:

- Data
- Voice
- Video

□ Lets talk about LAN and WAN networks

Lan Network



We can run on LAN site protocols such

- RIP
- RIPv2
- EIGRP
- OSPF
- IS-IS

Hierarchical design

CORE

DISTRIBUTION

ACCESS



WAN Network

Autonomous system
Public 1 to 64511
Private 64512 to 65535

Routing over WAN can help to communicate different locations



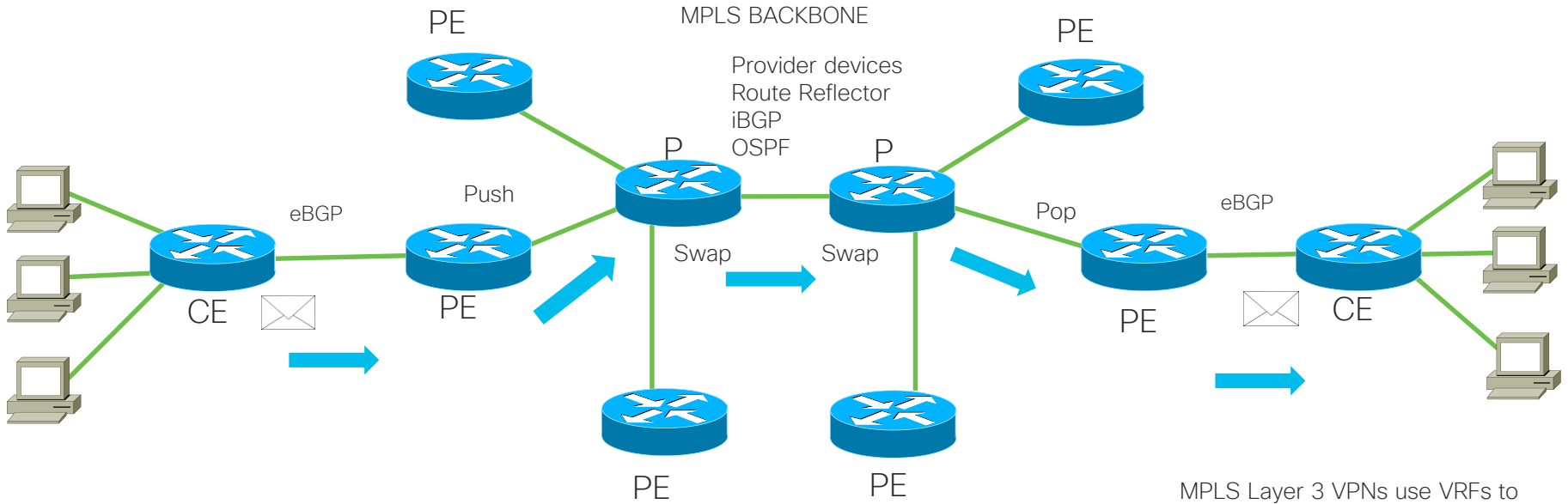
• Chicago



• Dallas

LAN site can run IGP protocol

MPLS/L3 network



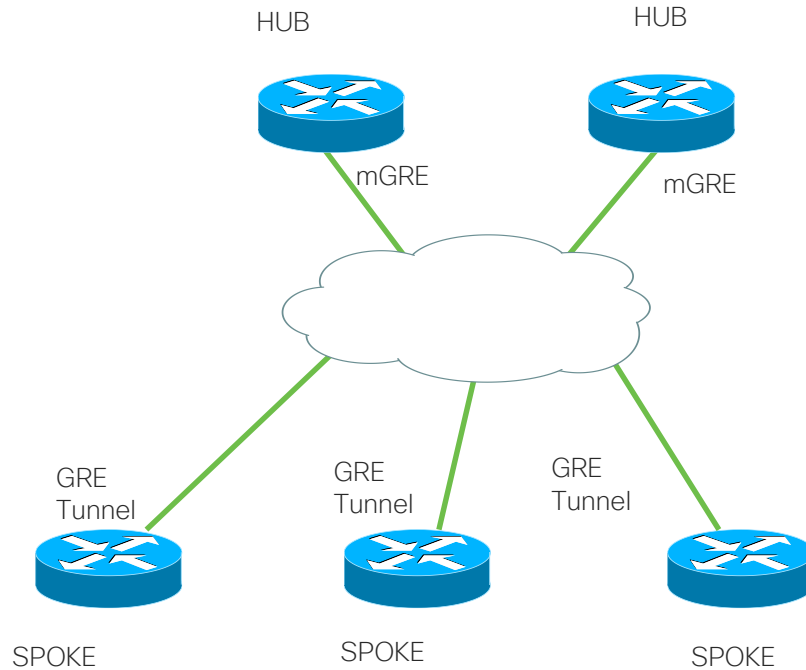
MPLS Operates using labels to switch traffic using Layer 2

Label operation
Push
Swap
Pop

MPLS Layer 3 VPNs use VRFs to have a dedicated routing table

What is a big problem with this design?

DMVPN Network

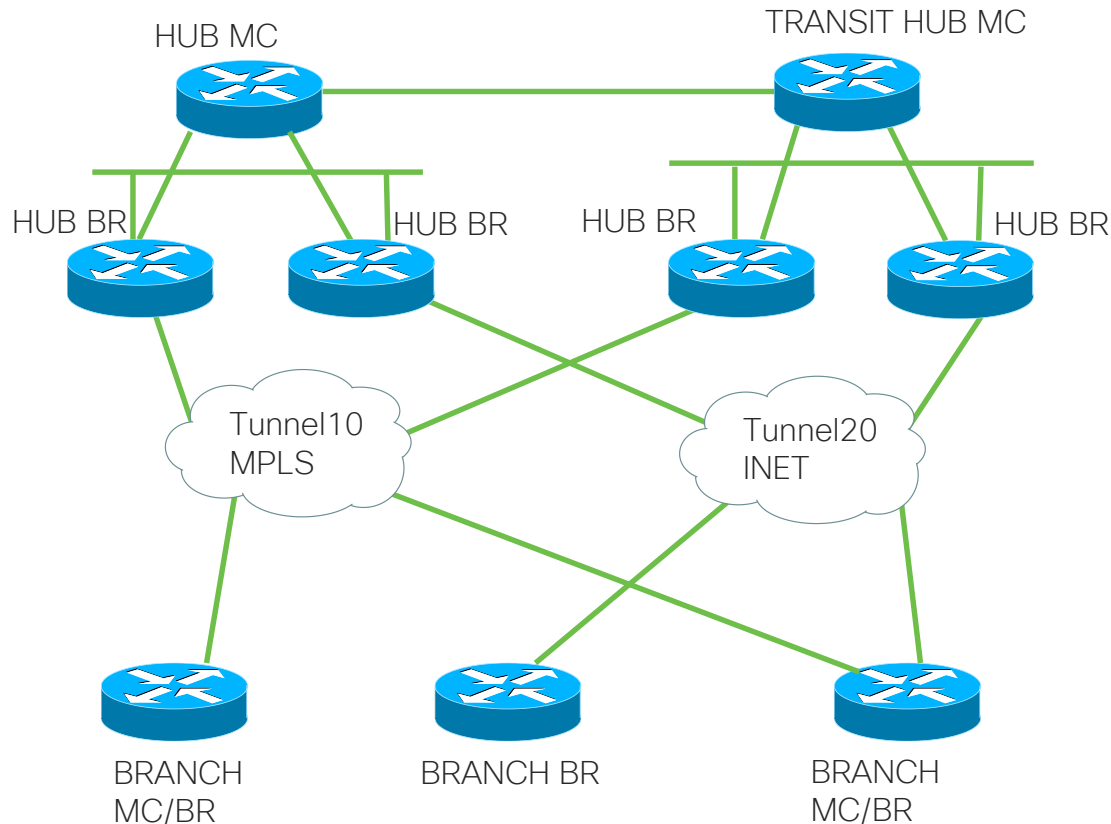


Components of DMVPN

- GRE tunnel
- Ipsec
- QoS
- Dynamic routing
- Dynamic spoke to spoke tunnels
- DMVPN Phase 1,2,3

One of the biggest advantages is to reduce costs

iWAN Pfr network



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

iWAN PFR Components

- Master controller
- Transit Hub
- Border router
- DMVPN Phase 3
- Ipsec
- IOS XE
- QoS
- Branch router

What are the advantages of iWAN over DMVPN?

Polling Question 2

Which solution do you currently use in your network?

- A. MPLS/L3
- B. MPLS/L2
- C. Frame-Relay
- D. iWAN (Pfr)

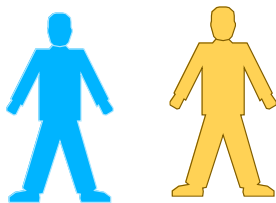
Network simplification: Why SD-WAN?

Top WAN Challenges

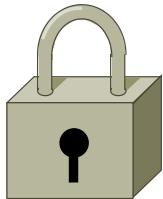
Efficiency



Experience



Security



- Complexity with multiple transport types
- Management of enterprise WAN networks
- Need better analytics and visibility into applications and network resources
- Need consistent user experience for applications independent of their location
- Security requirements to be better prepared to face changing threats
- Audit and compliance related to the network

Intent-Based Networking

Translation

Capture the business objects

Activation

Centrally define and activate policies

Assurance

Constant visibility into the network



Polling Question 3

Do we need physical hardware for SD-WAN?

- A. Yes
- B. No

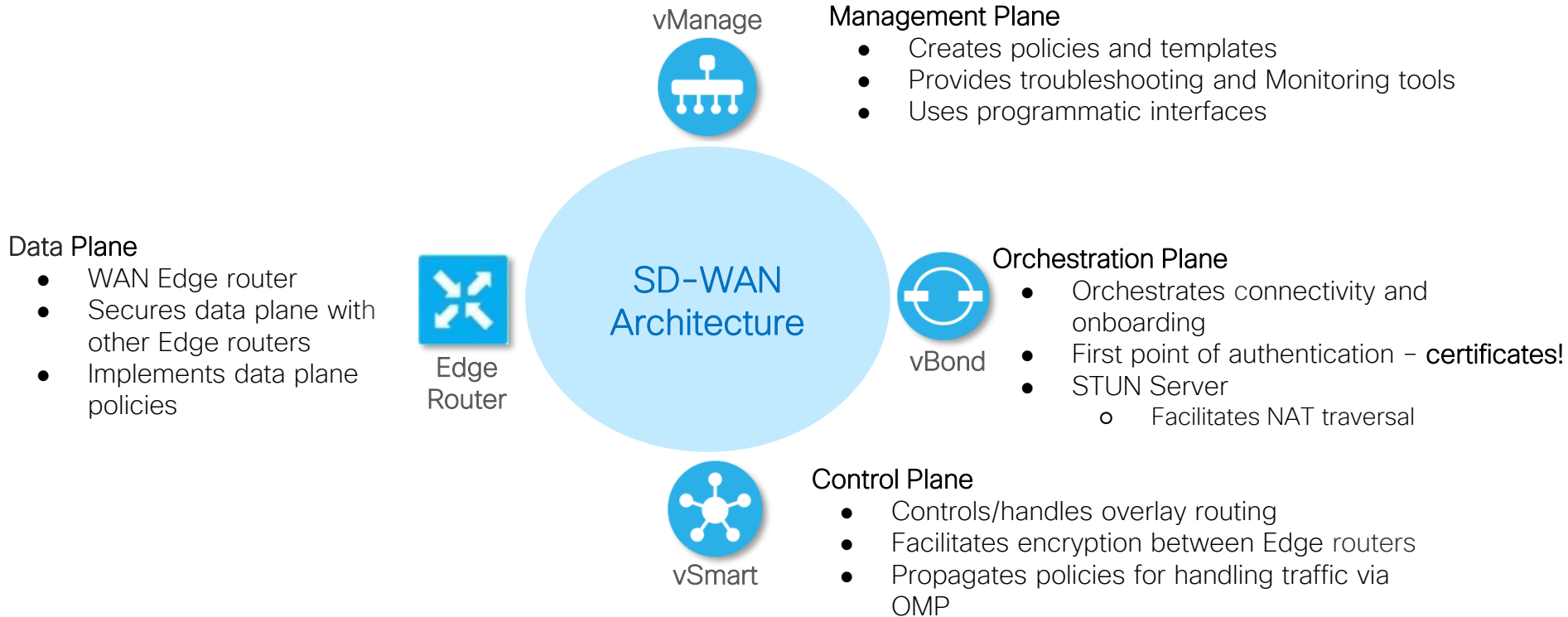
Architecture: How does the overlay work?

WAN Requirements

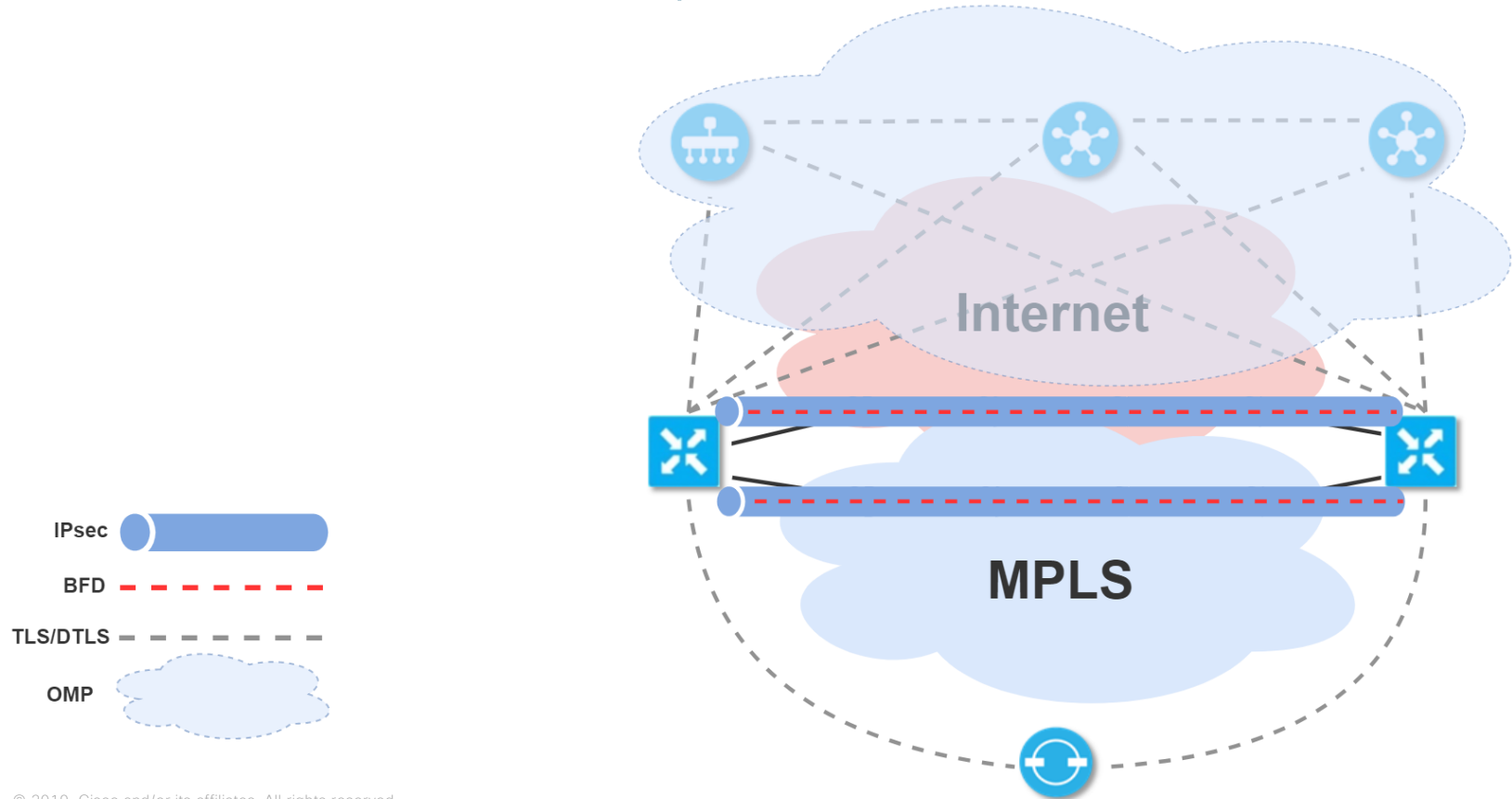
-  Visibility and analytics
-  Consistent security
-  Deterministic App Performance
-  Application bandwidth
-  Rapid Time to capability
-  Cloud-Ready Architecture



What does each one of them do?



Architecture and components



Hold on...
Isn't that chaotic?

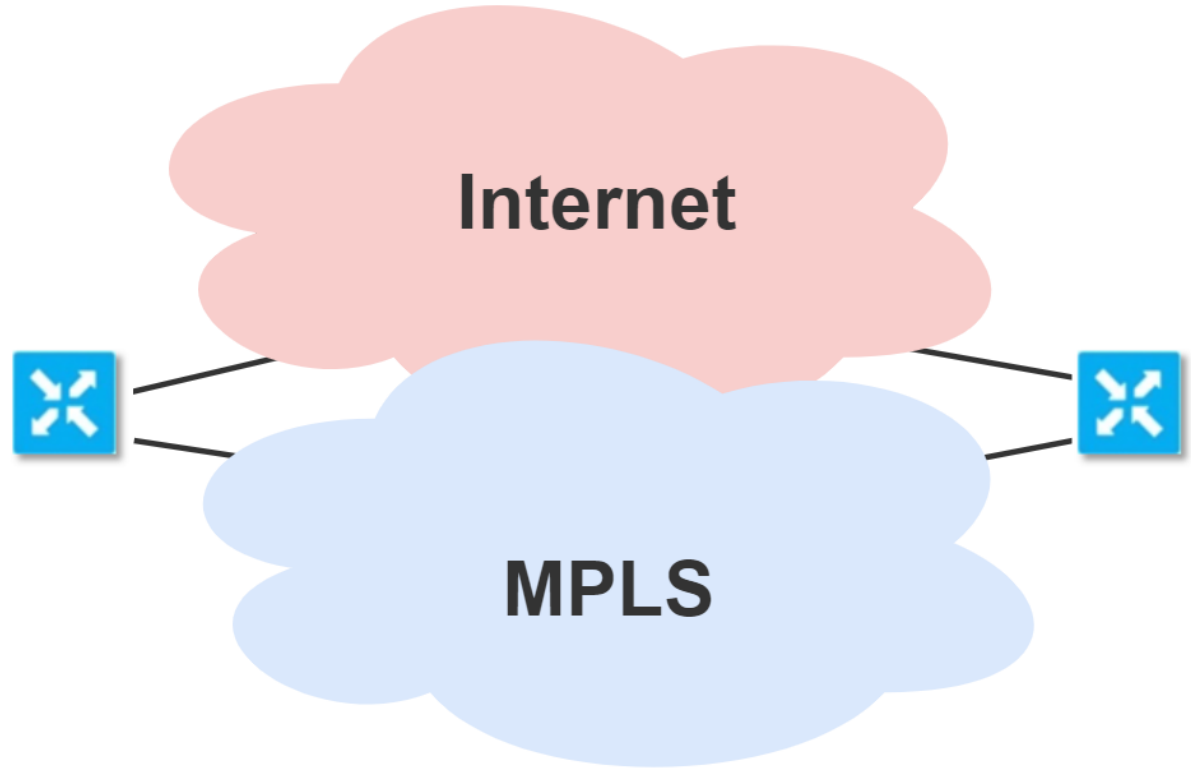
How do you eat an elephant?

Piece by piece!

Let us go step by step.

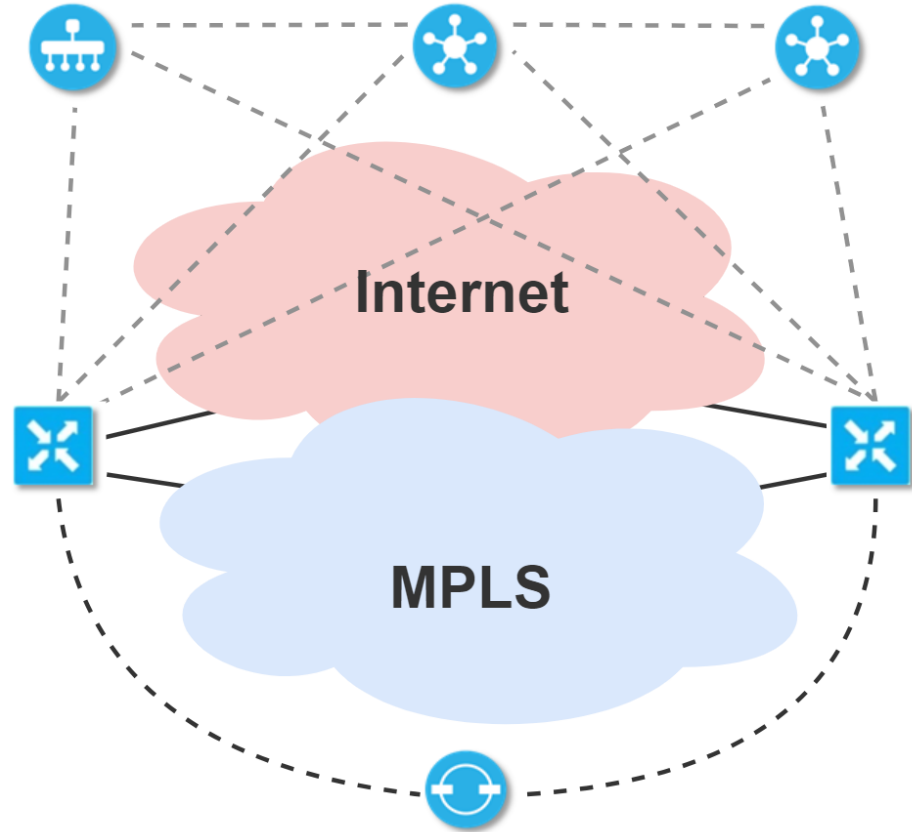
Architecture and components

- Underlay



Architecture and components

- Underlay – adding controllers



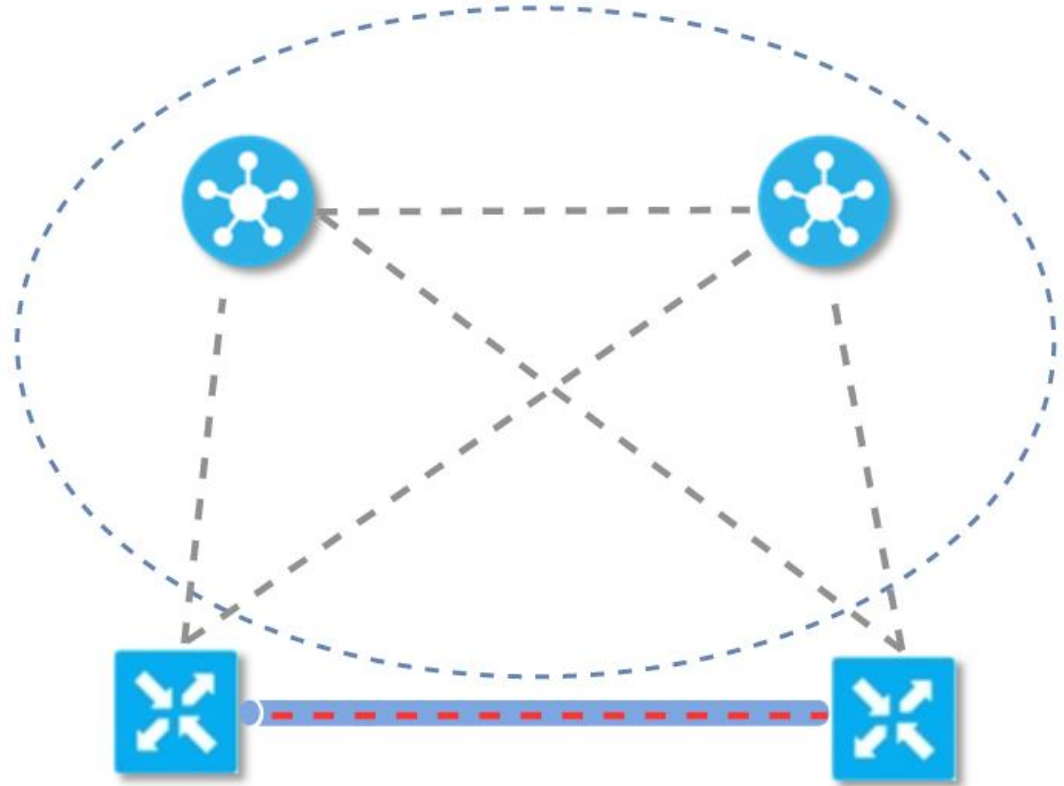
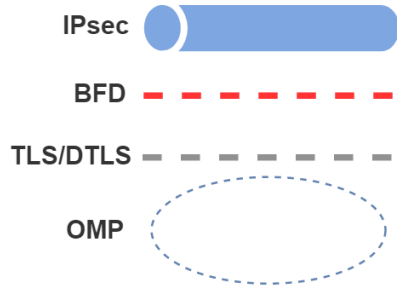
TLS/DTLS - - - - -

Architecture and components

- Overlay - abstracted view

Why DTLS and IPsec?

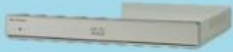
- TLS/DTLS protect control plane
- IPsec protects data plane



Deployment options

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



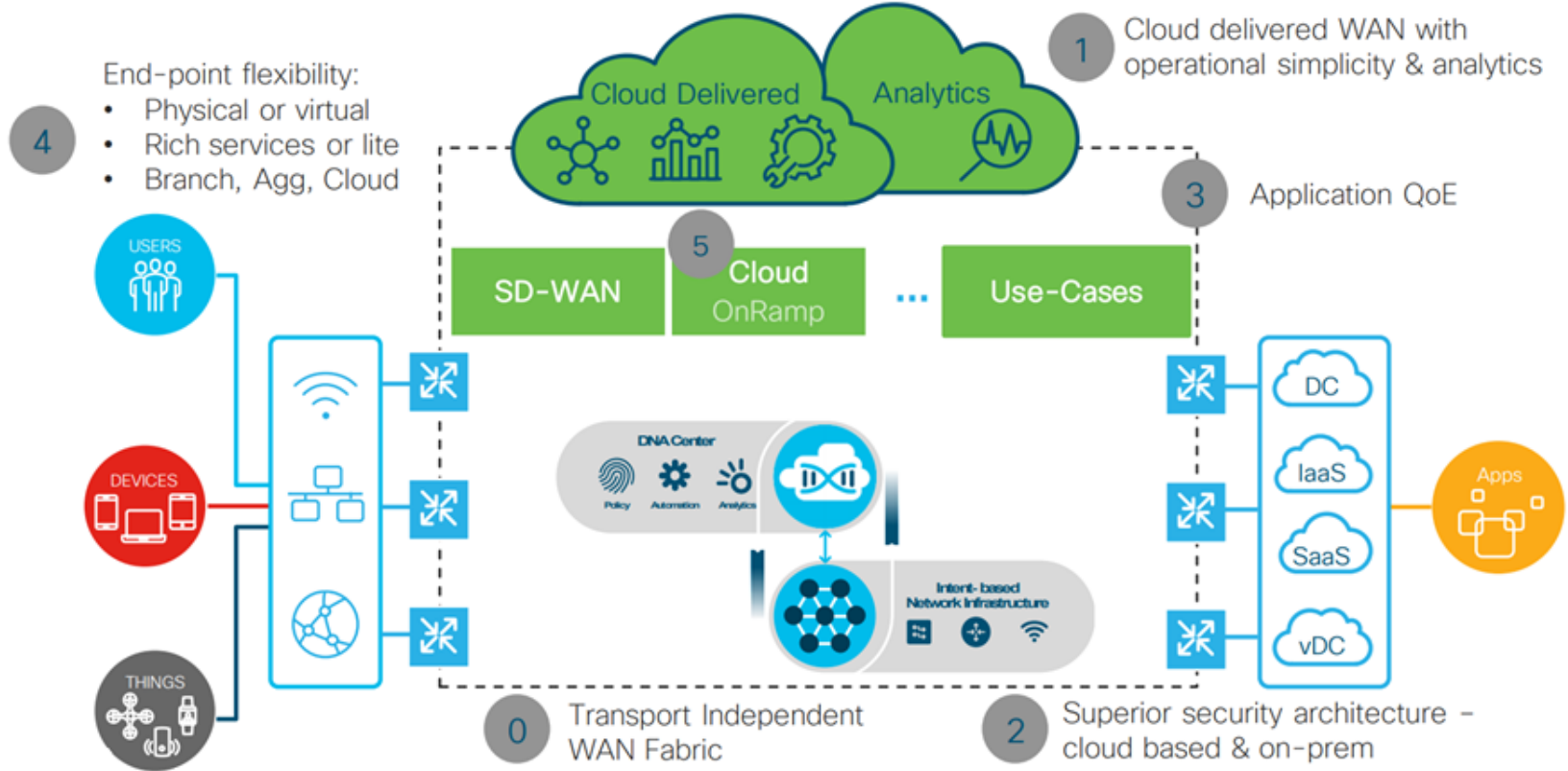
ENCS 5400



Public Cloud



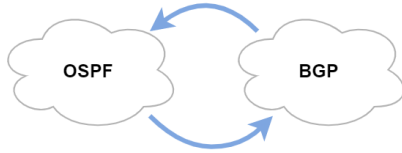
SD-WAN benefits



The Planes: Control, Data and Management planes

Fundamentals and definitions

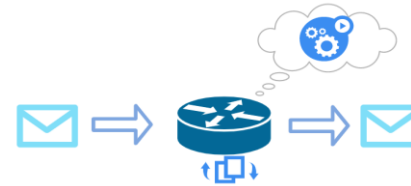
- Control plane



- Management plane



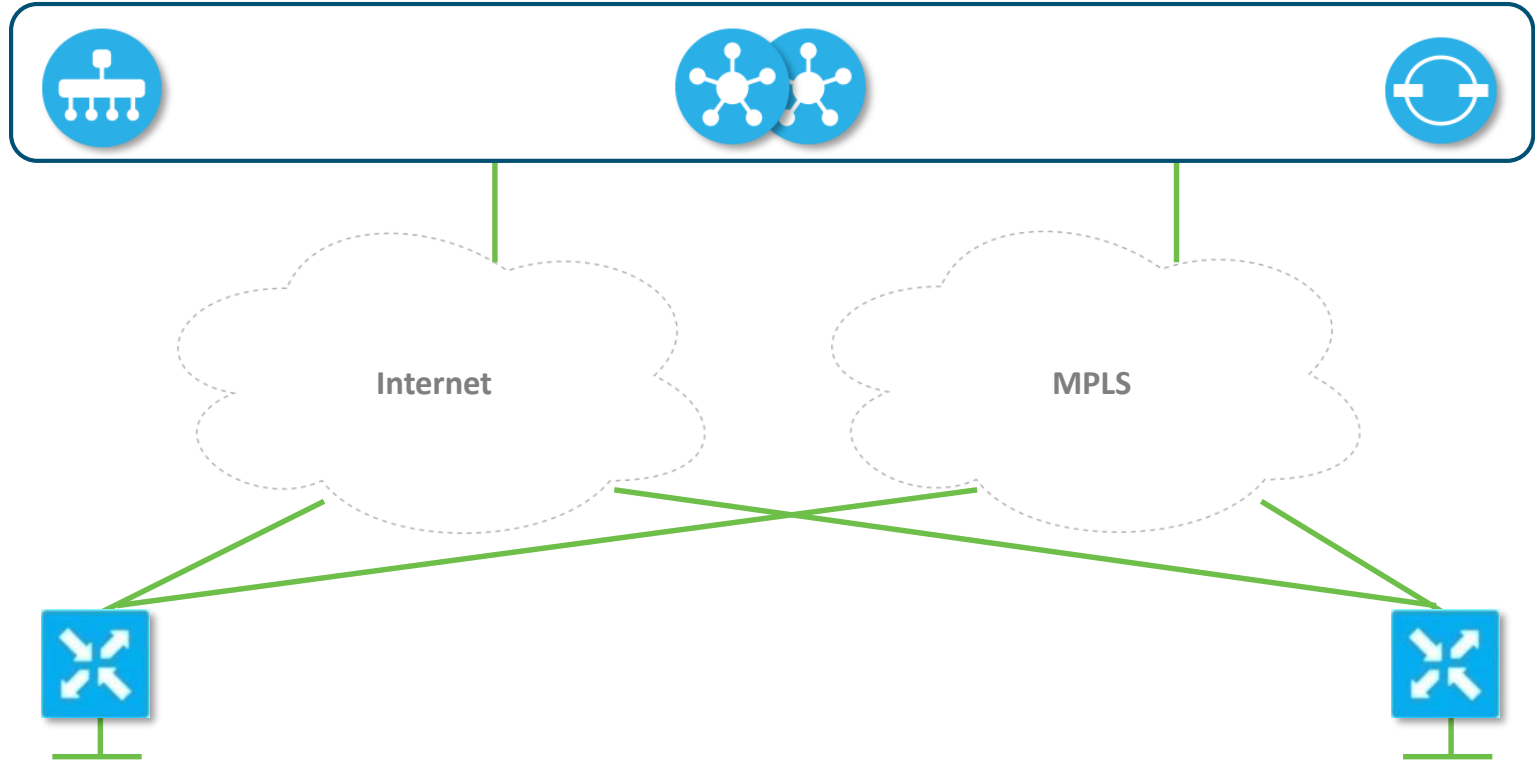
- Data plane



- Controller



Putting it all together



Learning the SD-WAN lingo

- **Overlay Management Protocol**
Control plane protocol distributing reachability, security and policies throughout the fabric
- **Transport Locator (TLOC)**
Transport attachment point and next hop route attribute
- **Color**
Control plane tag used for IPsec tunnel establishment logic
- **Site ID**
Unique per site numeric identifier used in policy application
- **System IP**
Unique per device (Edge routers and controllers) IPv4 notation identifier.
Also used as Router ID for BGP and OSPF.
- **Organization Name**
Overlay identifier common to all elements of the fabric
- **VPN**
Device level and network level segmentation

Bond under the hood – the gatekeeper

- **Whitelisting approach** – only explicitly allowed devices can join the overlay
 - List of certificates is distributed by vManage to all the controllers
 - **No authentication means no onboarding!**
- Authentication based on certificates – 2048-bit RSA keys
- What is the device's identity?
 - Hardware devices (cEdge, vEdge)
 - With or without SUDI – chipset installed during manufacturing
 - Software devices (vEdge cloud, ISRv, CSR1000v)
 - Certificate signed by vManage
- Who's the root for those certificates?
 - Digicert/Symantec – controller's identity
 - Avnet/Cisco (chipset) – Edges' identity
 - vManage – vEdge cloud's identity

AES-256 provides confidentiality
SHA-1 or SHA-2 ensure integrity

Every edge device will connect
to vBond after every reboot

vBond under the hood (Cont.)

An overlay will be limited, up to certain extent, by the policies in the underlay

- vBond is a STUN server - but... what the heck is that?
 - STUN stands for: **Session Traversal Utilities for NAT**
- How does it help in the SD-WAN overlay network? Which problem are we trying to solve?
 - The solution was built to allow a more intelligent and ubiquitous control plane
 - It supports its inner mechanisms through usage of several ports
 - PAT, restricted NAT or port filtering could potentially be detrimental
 - When devices are behind NAT, it can interfere with the sessions between them, being those:
 - BFD
 - TLS
 - DTLS
 - IPsec
 - STUN allows vBond to work as a server and all Edge routers as clients
 - vBond registers and maps public and private IP addresses with their respective ports

Which policies do we have?

- Control policy
 - Any modification affecting routing behavior - control plane
 - E.g Peerings, routing protocols, prefix filtering/tagging/announcement, VPN membership
- Data policy
 - Any modification affecting data plane forwarding
 - E.g. Packet marking, specific transport forwarding, Application Aware Routing
- Policies can be provisioned in two ways:
 - Centralized
 - Pushed from vManage to vSmart through a NETCONF transaction and then advertised to Edge devices via OMP - affect all edges matched by a list
 - Localized
 - Pushed from vManage directly to Edge devices through a NETCONF transaction - affect specific devices requiring tailored policies or settings

Templates

- Templates allow to replicate and standardize configurations
- Sets or subsets of configuration can be created and assembled into a template
- Template types available:
 - Feature Template
 - Allow to configure specific features and create subsets of config
 - E.g. OSPF, BGP, SNMP
 - Think of them as a repository of available configs blocks you can choose from
 - Device Template
 - Allows the grouping of several feature templates per device
 - Some devices might not need all the features, add only what you need!
 - Similar to building towers with LEGO
 - CLI Template
 - Analogous to the common chunks of config in any device you have seen till now
 - Old school, effective

Templates (Cont.)

Templates come with some added advantages

- Use of variables
 - Variables allows you to configure a placeholder for those values that always change in a standard site configuration
 - I.e. hostname, IP addresses, system IP, router ID, or similar information
- Templates can have many Edge routers attached and the only changes are the variables
- You can also push a change in all the devices using the same template if you modify it
 - They follow a parent-child type of logic
- Use this to your advantage, design sites as predictable as possible

If a change in the configuration prevent an Edge router from reaching vManage, it will rollback to the previously known working configuration

Demo time!

Thanks!

Submit Your
Questions Now!



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

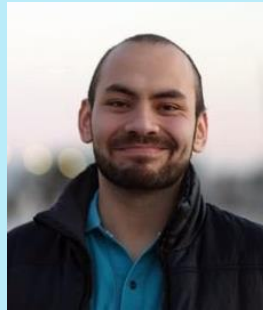
Ask Me Anything following the event

Now through Friday December 20th 2019

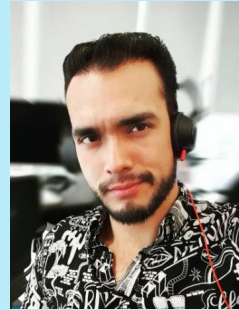


With
David Peñaloza,
Juan Flores & Juan Rangel

<http://bit.ly/ama-dec11>



David Peñaloza
Lead Network Consulting
Engineer



Juan Flores
Technical Consulting Engineer



Juan Rangel
Technical Consulting Engineer
CCIE #62667

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



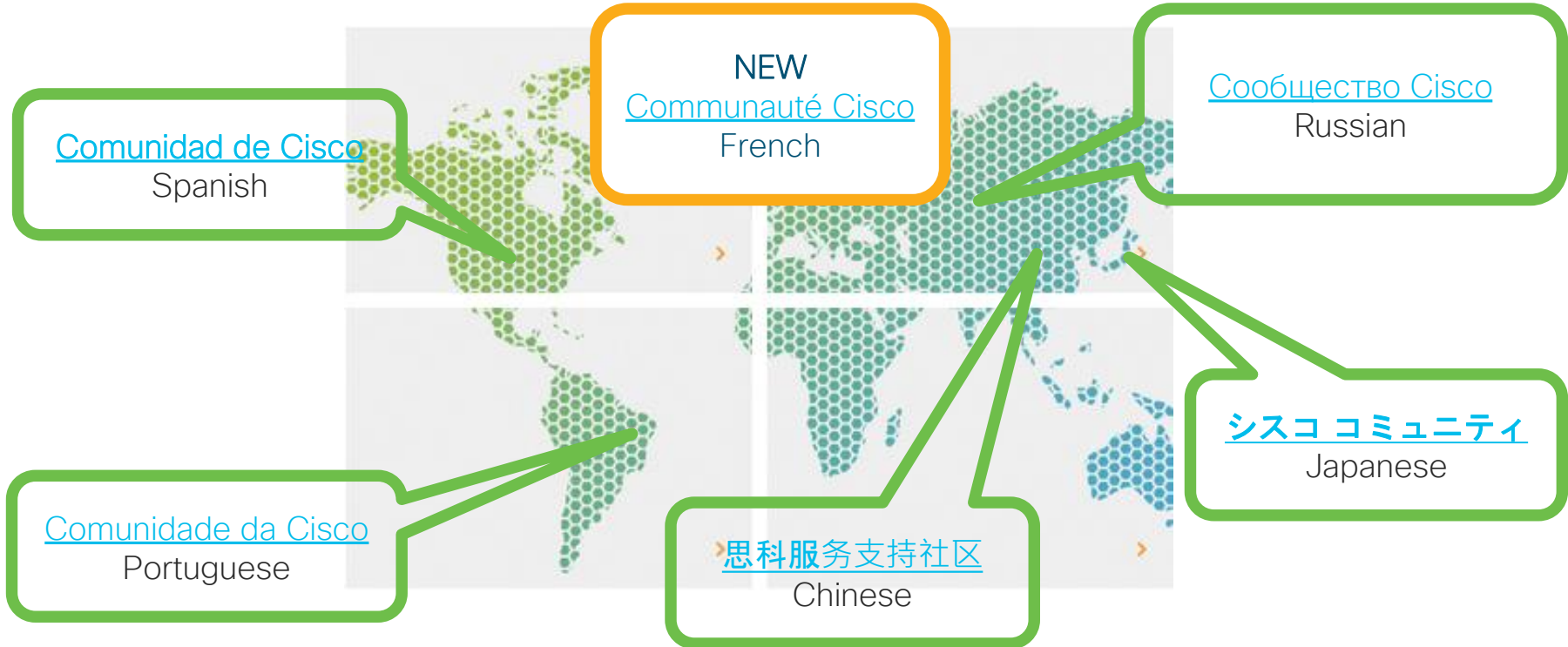
LinkedIn

- 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!

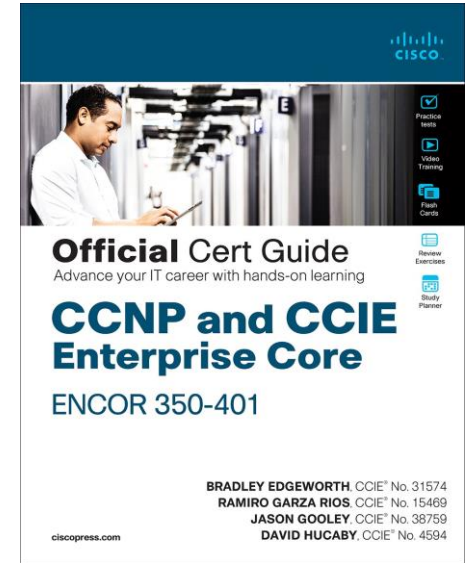
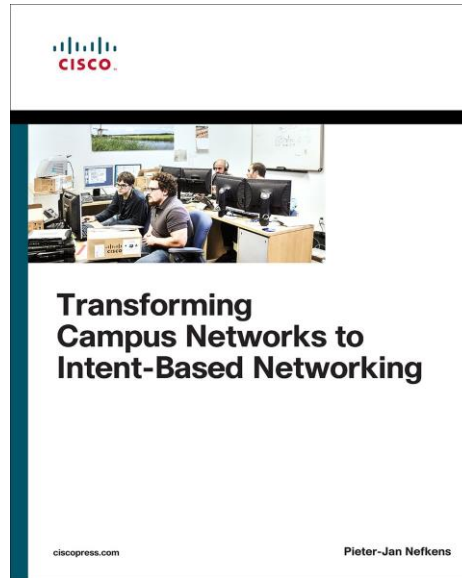
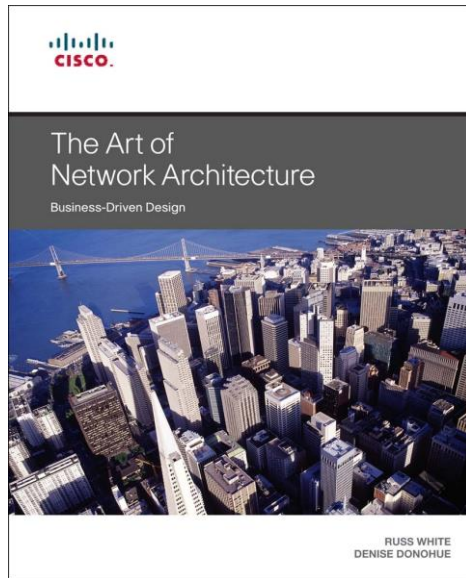
Please take a moment to complete
the survey



Thank you for participating, you earned a discount!

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

<http://bit.ly/Community-CiscoPress2019>



Thanks For Joining today!

