



You make **possible**



Cisco SD-WAN POC

Experiences and Best Practices

Adrien Olalainty
Technical Solution Specialist – CCIE R&S #62878

BRKRST-2096

CISCO *Live!*

Barcelona | January 27-31, 2020



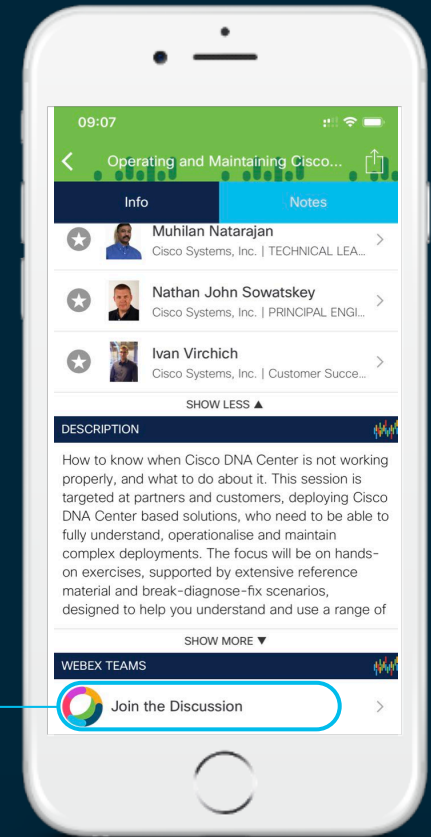
Cisco Webex Teams

Questions?

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

How

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

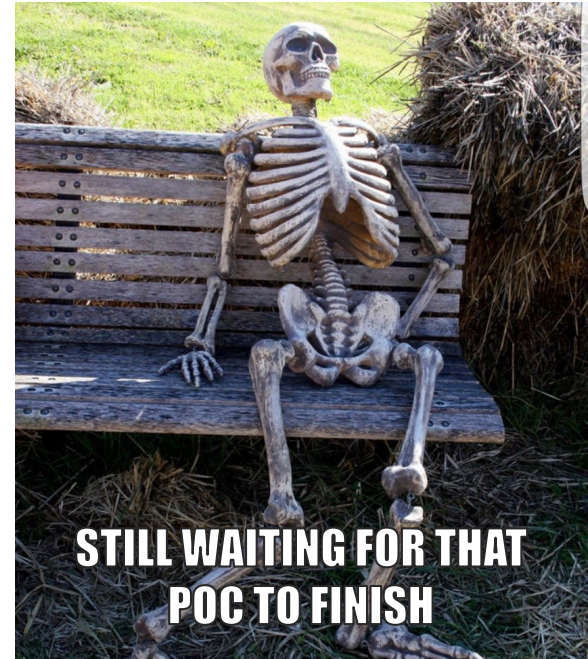
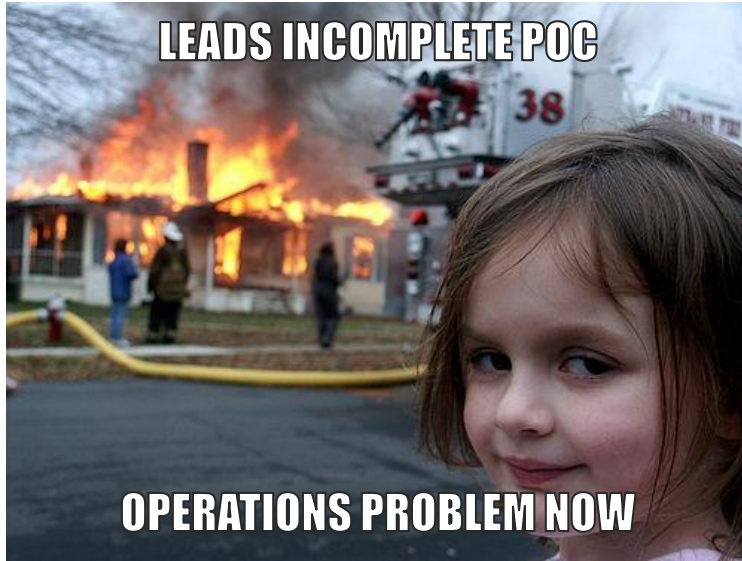


Agenda

- Introduction
- Should you do a SD-WAN POC?
- Are you ready for it? (Pre-requisites)
- Step by Step of a SD-WAN POC deployment
- Conclusion

Introduction

How POC can fail



What this session will cover...

- All the useful information around SD-WAN POC
- Best Practices from our experiences
- Tools to plan your own POC

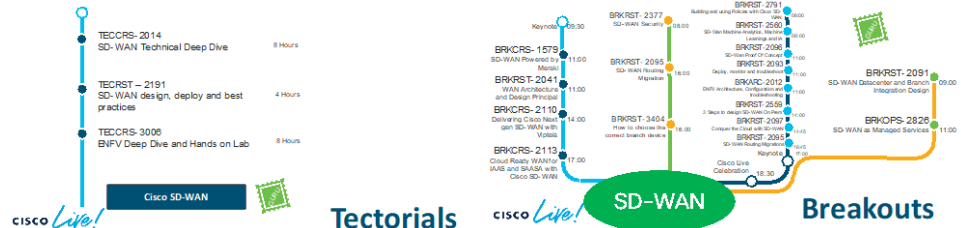
Knowledge
is
power!



cisco Live!

What it won't...

- This is not a technical deep dive
Useful sessions and documentations will be referred to
- This is not a design session
Refer to TECRST-2191 - Next-Gen SD-WAN (Viptela) Design, Deployment and Best Practices
- This is not a migration session
Refer to BRKRST-2095 - SD-WAN Routing Migrations



For your POC



- These are slides that can be useful to track your own POC
- When preparing your POC, review those slides to make sure you didn't forget any important action or pre-requisite



Main contributors

SD-WAN Architects

- Prashant Tripathi
- Jerome Durand
- Martin Schumacher
- Nadja Ilic Danailov
- Manuel Di Lenardo
- David Prall
- Jean-Louis Suzanne

SD-WAN Delivery

- Tomasz Zarski

SD-WAN Support

- Danny De Ridder
- Olivier Pelerin



Adrien Olalainty

2016 Joined Cisco

2017 Focus on SD-WAN solutions

2019 CCIE R&S #62878

- Snowboard / Basketball
- Humanitarian construction worker



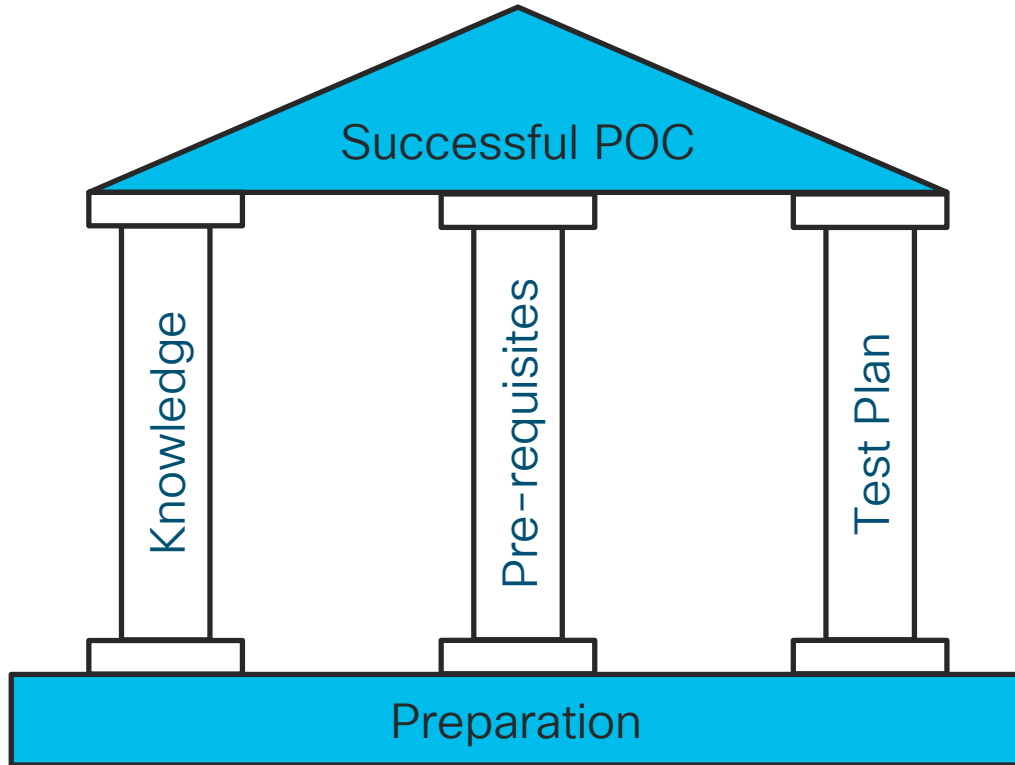
When building foundations are wrong



When building foundations are wrong



Preparation is the Foundation of your POC



Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Should you do a SD-WAN POC?

Should you?



How to reach your objective

LEARN ABOUT SD-WAN



DOCUMENTATIONS
PRESENTATIONS



Learning

Before testing, you should have good understanding of SD-WAN technology. Following documentations will help you:

- [TECCRS-2014 - Cisco SD-WAN \(Viptela\) - Technical Deep Dive](#)
- [SD-WAN on Cisco web](#)
- [Validated design SD-WAN - Design Guide](#)
- [Validated design SD-WAN - Deployment Guide](#)

Cisco SD-WAN Getting Started Guide

Your POC Bring-up Bible

Cisco SD-WAN Getting Started Guide

The screenshot shows a web interface for the Cisco SD-WAN Getting Started Guide. On the left is a 'Book Contents' sidebar with a menu icon. The main content area has a search bar at the top with the text 'Find Matches in This Book'. Below the search bar, the current chapter is 'Chapter: Cisco SD-WAN Overlay Network Bringup'. Underneath this, there is a link '> Chapter Contents'. A list of sub-topics follows, including 'Bringup Sequence of Events', 'Step 1: Download Software', 'Step 2: Deploy the vManage NMS', 'Step 3: Deploy the vBond Orchestrator', 'Step 4: Deploy the vContainer Host', 'Step 5: Deploy the vSmart Controller', 'Step 6: Deploy the vEdge Routers', 'Cluster Management', 'Certificates', and 'License Management'.

Book Contents

Find Matches in This Book

Book Title Page

System Overview

Hardware and Software Installation

Cisco SD-WAN Overlay Network Bringup

Cisco SD-WAN API Cross-Site Request Forgery Prevention

Chapter: Cisco SD-WAN Overlay Network Bringup

> Chapter Contents

- Bringup Sequence of Events
- Step 1: Download Software
- Step 2: Deploy the vManage NMS
- Step 3: Deploy the vBond Orchestrator
- Step 4: Deploy the vContainer Host
- Step 5: Deploy the vSmart Controller
- Step 6: Deploy the vEdge Routers
- Cluster Management
- Certificates
- License Management

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book.html>

How to reach your objective

LEARN ABOUT SD-WAN



DOCUMENTATIONS
PRESENTATIONS



SEE WHAT SD-WAN LOOKS LIKE



DEMO



dCloud demos

Ask your favorite partner/Cisco engineer to show you



Cisco 4D Secure SD-WAN (Viptela) Dual DC v3.3

ID: 401571 Published Date: 09-Jan-2020 19:05 Demonstration SD-WAN Enterprise Networks Routing English

Demonstrate Cisco 4D Secure SD-WAN (Viptela) capabilities including Zero Touch Provisioning, application aware routing, regional and Direct Internet Access using SD-WAN security features, policy-based topology creation, and management via vManage.

★ Favorite [Related Documents](#) [Schedule](#)

Cisco 4D Secure SD-WAN (Viptela) Single DC v3.3

ID: 399349 Published Date: 17-Dec-2019 20:59 Demonstration SD-WAN Enterprise Networks English

Demonstrate Cisco 4D Secure SD-WAN (Viptela) capabilities including Zero Touch Provisioning, application aware routing, centralized and Direct Internet Access using SD-WAN security features, policy-based topology creation, and management via vManage.

★ Favorite [Related Documents](#) [Schedule](#)

Cisco 4D Secure SD-WAN (Viptela) v3.2 - Instant Demo

ID: cisco-4d-secure-sd-wan-viptela-v3-2-instant-demo Published Date: 04-Oct-2019 23:34 Instant Demo SD-WAN

Enterprise Networks Security Enterprise Network Security Advanced Malware Protection WAN Optimization Router Security

English

Demonstrate Cisco 4D Secure SD-WAN (Viptela) capabilities including Zero Touch Provisioning (ZTP), application aware routing, regional and Direct Internet Access (DIA) using SD-WAN security features, policy-based topology creation, and management via vManage.

NOTE: Please download the user guide from the **Related Documents** link below and click **View** to access the demo.

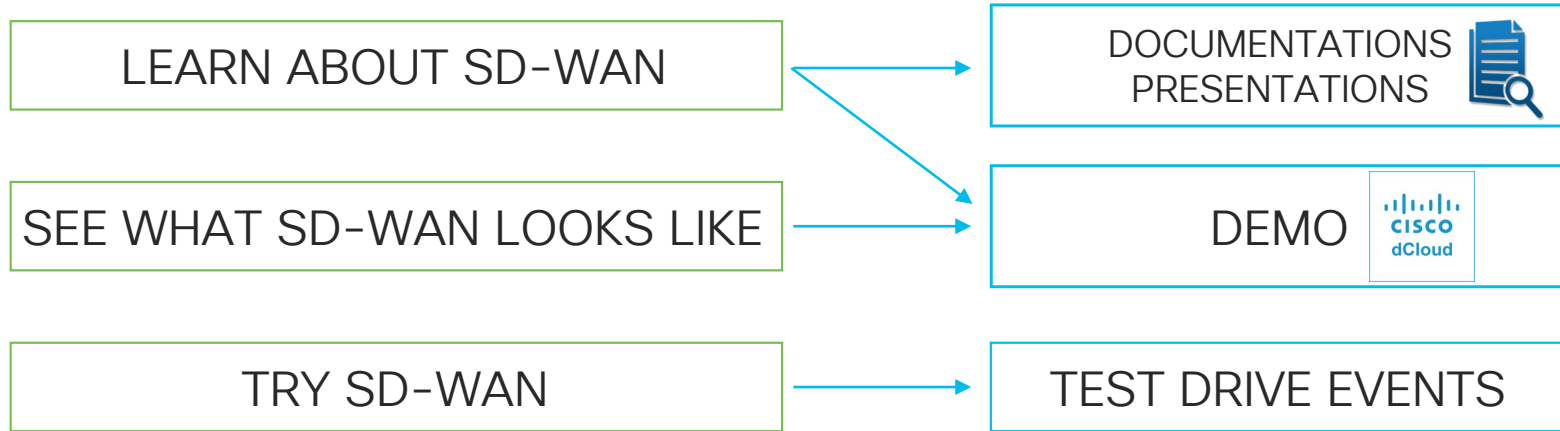
★ Favorite [Copy](#) [Related Documents](#) [View](#)

To Schedule
Sessions can be shared
Can also be used for simple POC

Always available
Read-only



How to reach your objective



Test Drive : Feel the SD-WAN

Join your local Cisco events

Cisco SD-WAN Test Drives

Cisco is hosting a series of learning events and experiences to demonstrate how Cisco SD-WAN can help you move applications to the cloud, transform your customer and employee experience in the branch, and simplify WAN infrastructure management, all without compromising security.

Register Today!

[Complete Events Calendar](#)

Select a region for the event closest to you:

[Europe](#)

[Southeast Asia](#)

[South/Central America](#)

[South Korea 대한민국](#)

[Greater China 中国](#)

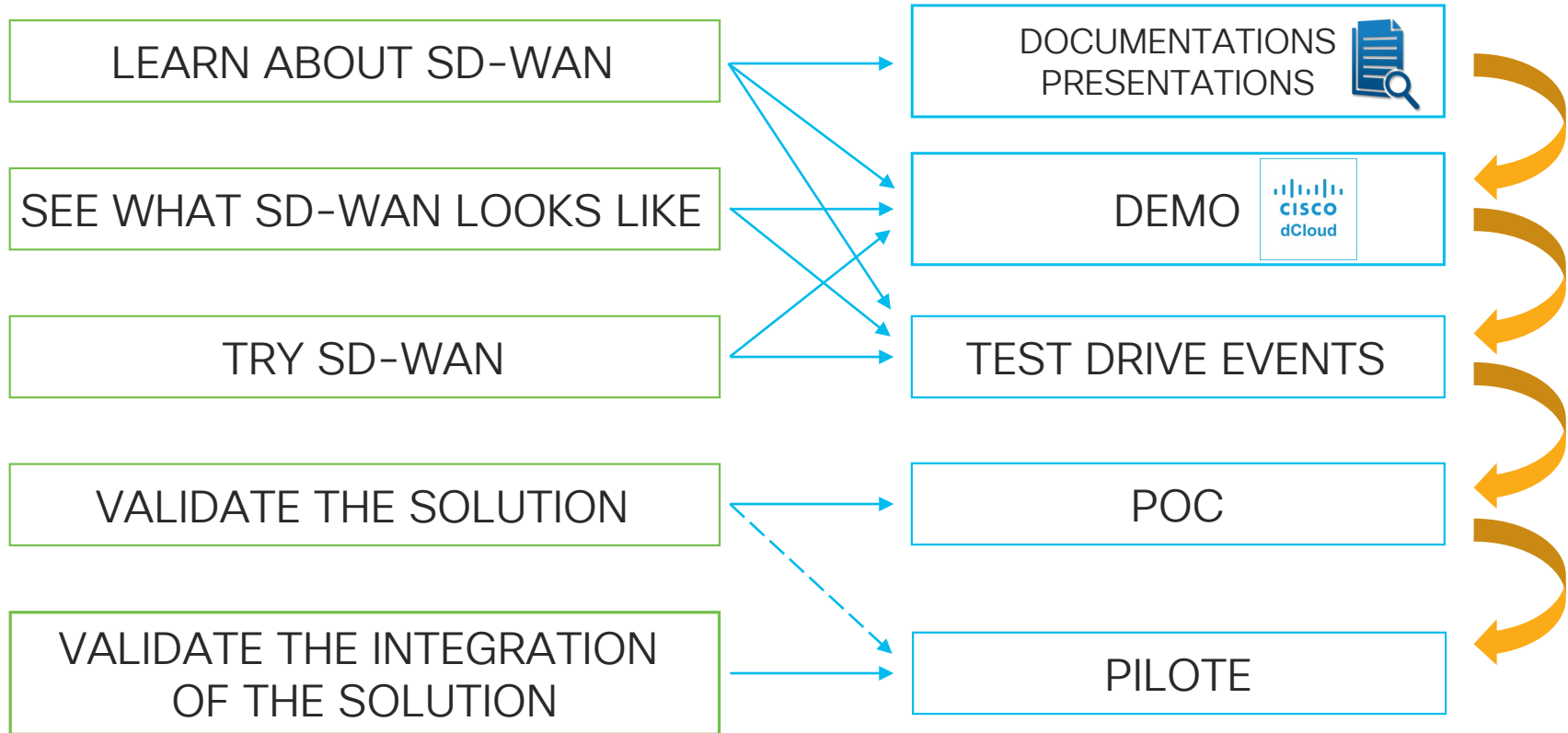
[Middle East](#)

Search...



CISCO *Live!*

How to reach your objective



Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Pre-requisites



Order to design your POC

1. Define Test Plan with test use cases and success criteria

Less is more - Focus on features of Interest

2. Plan the right devices and topology

Physical or Virtual

3. Pre-requisites preparation

IP addressing, WAN links, etc

Should you do a
SD-WAN POC?

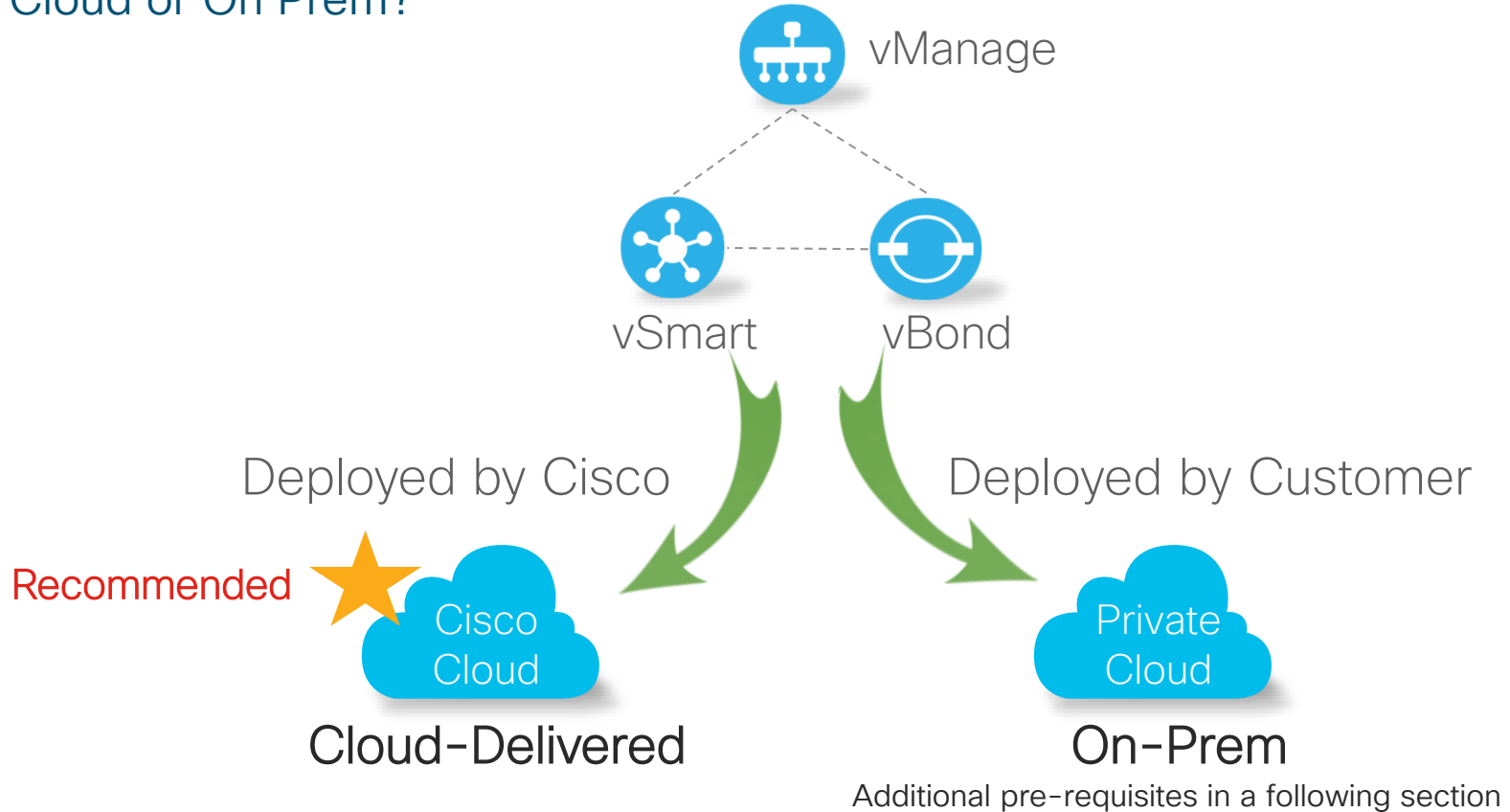
Pre-requisites

Step by Step
POC deployment

Plan the right devices and topology

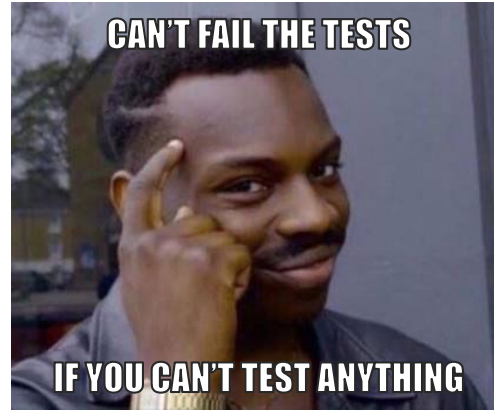
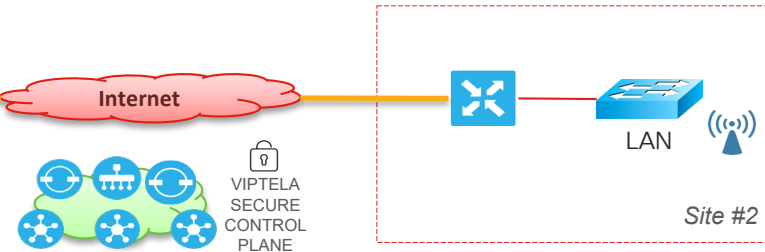
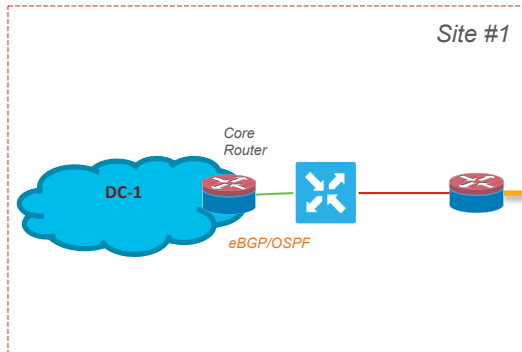
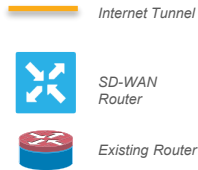
Deployment model

Cloud or On Prem?



Overall testing topology

Bad topology

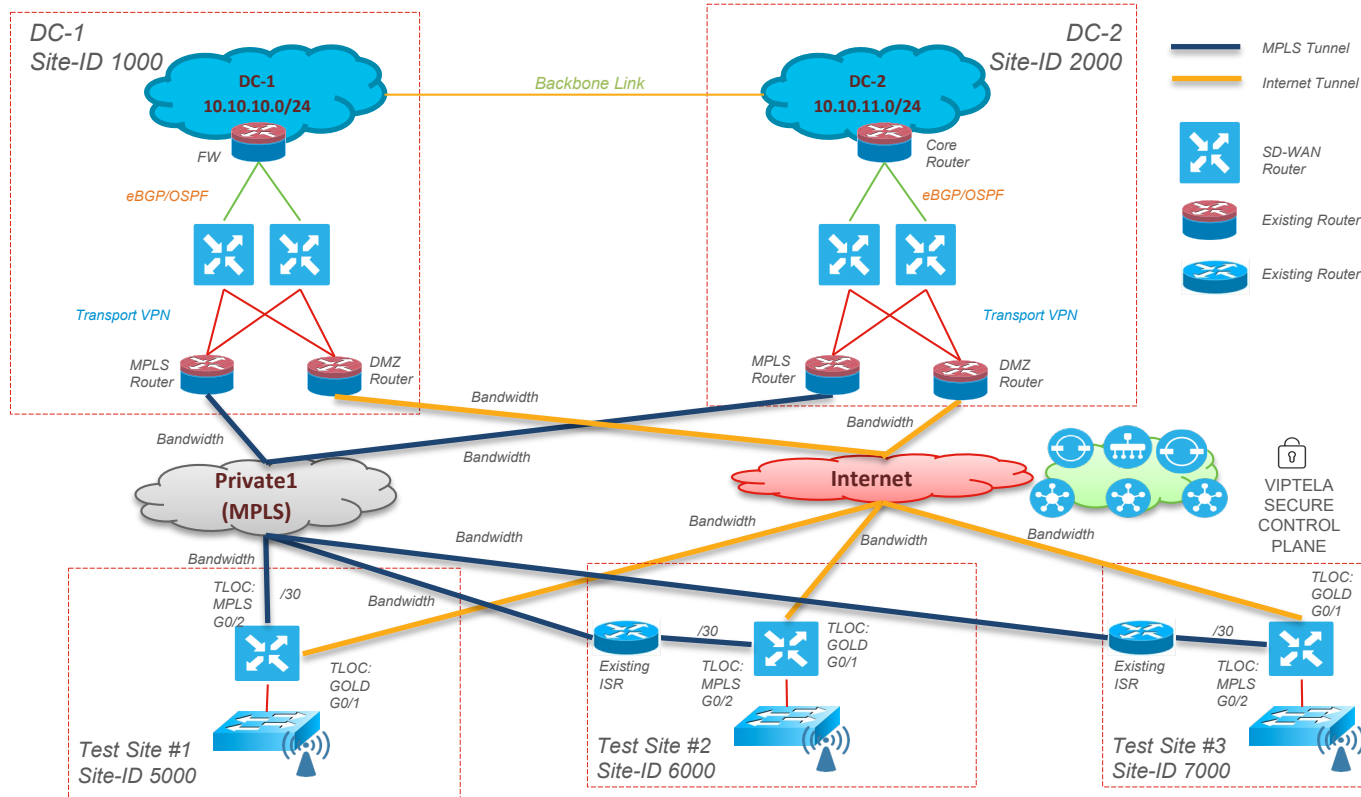


Overall testing topology

Use realistic topology – match your environment



For your POC



CISCO Live!

List of required devices



For your
POC

Product	Quantity	Rack space available?	Shipped ?	Installed ?
vEdge				
ISR				
ASR				
ENCS				
Switches ?				
SFP ?				
Cables / Fibers / Others ?				

Choose the right devices



BRKRST-3404: How to choose the correct Branch device

Pure Play SDWAN

Transport Independence,
Cloud Management & Analytics

Cloud Security

Voice Optimization

Cloud onRamp for
IaaS and SaaS

IOS-XE: ISR , ASR

Viptela OS: ISR 1100-4G, ISR 1100-6G, vEdge 2000

Integrated Services SDWAN

Interface Flexibility,
Rich Services

Cloud onRamp for
Colocation

Adv. Cloud
Security*

Multi-Domain*
(DC, Campus)

Embedded
Security

Integrated Voice*

WAN Opt *
(Caching, DRE)

Cloud Security

Voice Optimization

Cloud onRamp for
IaaS and SaaS

One User interface across Branch, Cloud and Colocation

Planning

Plan how to get the hardware, and keep time for Pre-POC Activities

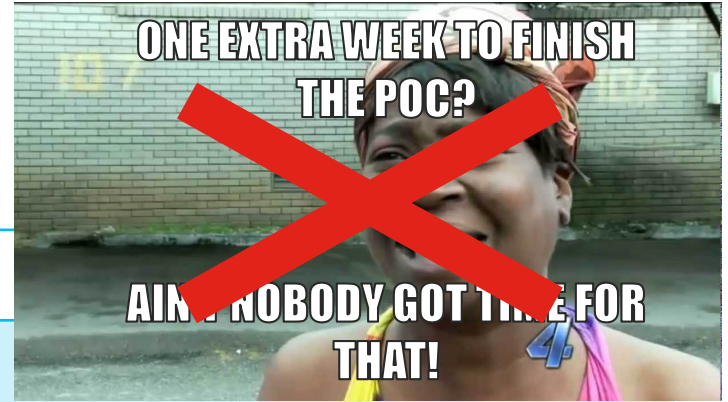


For your
POC

Item	Date
POC kick-off workshop	
POC start date (allow 6 weeks after planning meeting / check device lead time)	
POC end date (1-4 weeks after start date)	
POC Debrief meeting	

Planning

Plan how to get the hardware,
and keep time for Pre-POC Activities



Item

POC kick-off workshop

POC start date (allow 6 weeks after planning meeting / check device lead time)

POC end date (1-4 weeks after start date)

POC Debrief meeting

Leverage existing testing facilities

Save time on your POC

On-premise custom POC has strong requirements on your infrastructure
Pre-built labs exist and can be more efficient

Testing facility	Goal
dCloud – SD-WAN 4D Demo	Already deployed virtual lab
Partner's existing labs	Already deployed customizable lab
Partner's PoV lab services	Customizable fast to deploy lab
dCloud – Cisco POC Tool	Customizable fast to deploy lab

POC Tool in dCloud



Cisco 4D SD-WAN POC Tool v1.1

ID: 393443 Published Date: 25-Nov-2019 14:38

Sandbox Lab Demonstration SD-WAN Enterprise Networks Routing

WAN Optimization English

The Cisco 4D SD-WAN POC Tool enables you to create custom topologies to demo, test, and validate a whole range of use cases. You can use this tool to import and export topologies to share with other users of the tool.

★ Favorite [Related Documents](#) [Schedule](#)

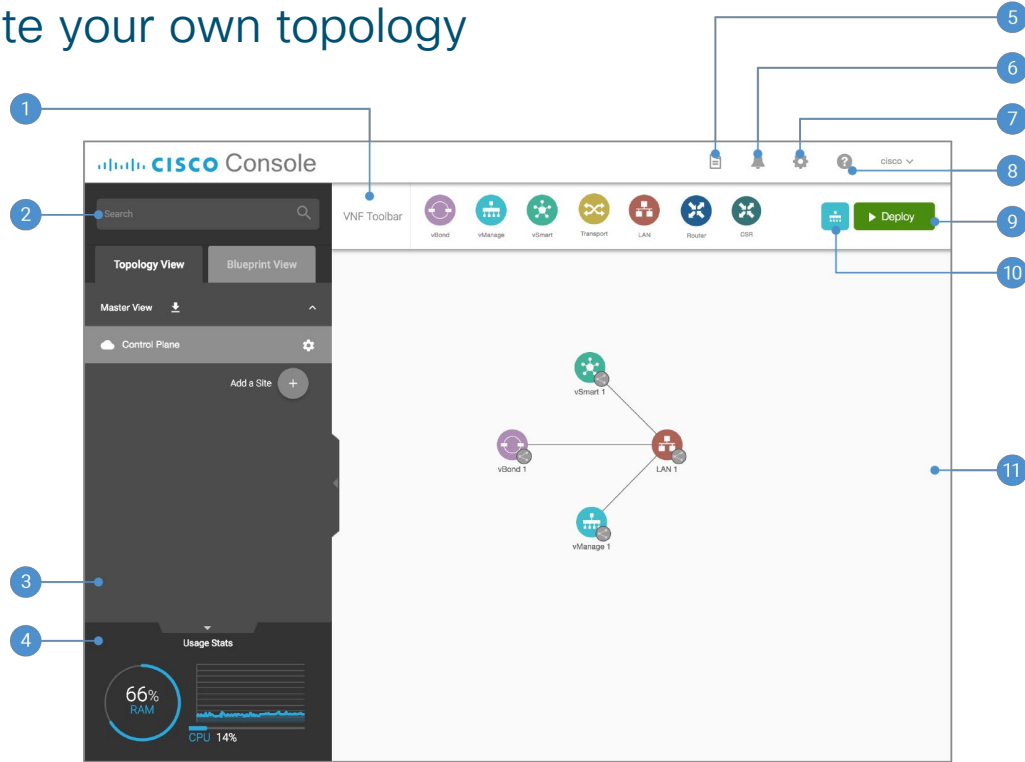
	Cisco 4D Secure SD-WAN (Viptela) v3.2 – Instant Demo	Cisco 4D Secure SD-WAN (Viptela) Single DC v3.3	Cisco 4D Secure SD-WAN (Viptela) Dual DC v3.3	Cisco 4D SD-WAN POC Tool v1.1
Type	Instant	Scheduled	Scheduled	Scheduled
Access	Read Only	Admin	Admin	Admin
Connectivity	Direct Web Browser	AnyConnect / Web RDP	AnyConnect / Web RDP	AnyConnect
Topology	2 DC, 3 Branches, 3 Transports	1 DC, 2 Branches, 2 Transports	2 DC, 3 Branches, 3 Transports	DIY
vAnalytics	Yes	No	No	DIY
Session Sharing*	No	Yes	Yes	Yes / Can export



*Only Cisco and Partners can instantiate sessions

POC Tool in dCloud

Import or create your own topology



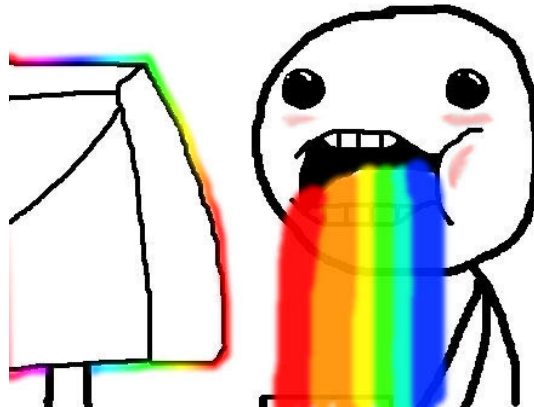
- 1. VNF Toolbar
- 2. Global Search
- 3. Navigation Sidebar
- 4. System Monitor
- 5. Logs View
- 6. Notifications
- 7. Global Settings
- 8. Help
- 9. Deploy
- 10. Access vManage
- 11. Canvas



POC Tool in summary



- Create your own topology or adapt one from the library. Export it for reuse!
- Drag and drop devices: Controllers, vEdge and CSR
- Easily add latency, traffic generators and 3rd party VNFs
- Automatically creates vManage templates to configure the devices



Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Environment pre-requisites

Define global parameters



For your
POC

Global parameters	Details
Organization-Name	
vBond FQDN or IPv4	
IPv4 address space available (Routed internally to provide reachability from outside world)	
DNS server(s)	
NTP IPv4 Servers (at least 1)	
vManage admin account/password	admin/admin

Create a secondary admin account

There is no time to be locked out

After too many failed connection attempts, the admin account will be blocked

- Ask Cisco TAC to unlock it

To prevent problems:

- Modify the default admin account password
- Create a secondary account in 'netadmin' user group



Detailed site design

Data Center - Dual Wan Edge



Site-ID:
Location:

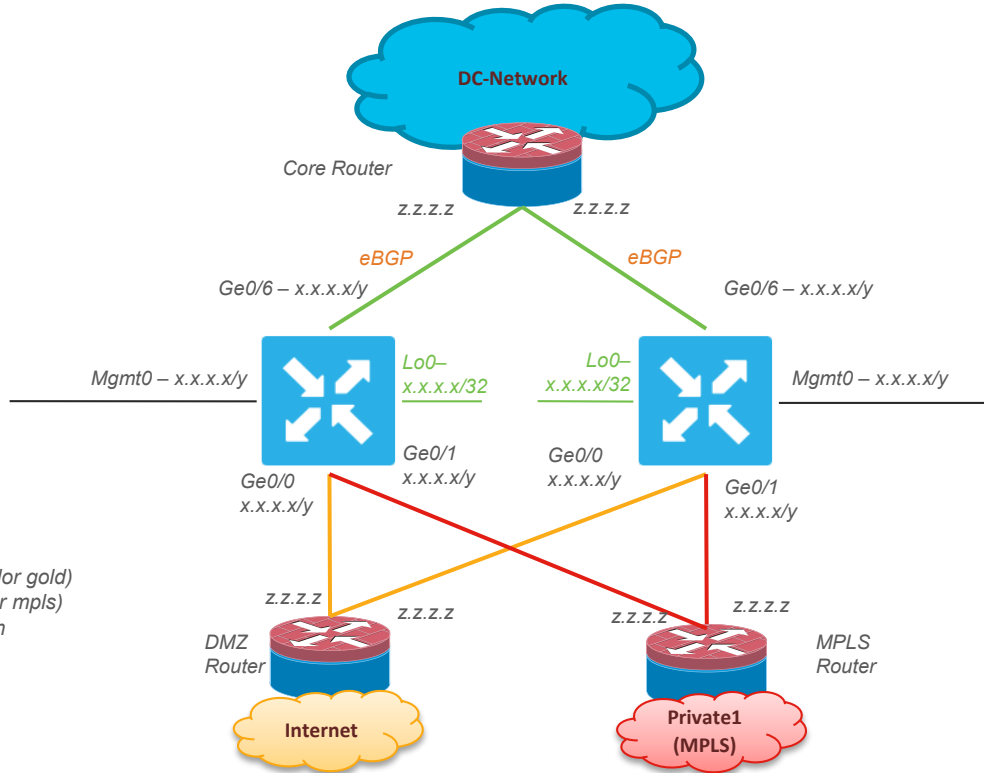
Inside VPN:

VPN Number: X
ge0/6 – BGP Interface to Core
BGP Local-AS:
BGP Neighbor IP (z.z.z.z)
BGP Remote-AS:

Hostname: wanedge-a
Serial Number:
System-IP: a.a.a.a
Mgmt gateway: z.z.z.z

Transport VPN:

Ge0/0 – Connects to Internet (color gold)
Ge0/1 – Connects to MPLS (color mpls)
Specify next-hop (z.z.z.z) for both



Inside VPN:

VPN Number: X
ge0/6 – BGP Interface to Core
BGP Local-AS:
BGP Neighbor IP (z.z.z.z)
BGP Remote-AS:

Hostname: wanedge-b
Serial Number:
System-IP: a.a.a.a
Mgmt gateway: z.z.z.z

Transport VPN:

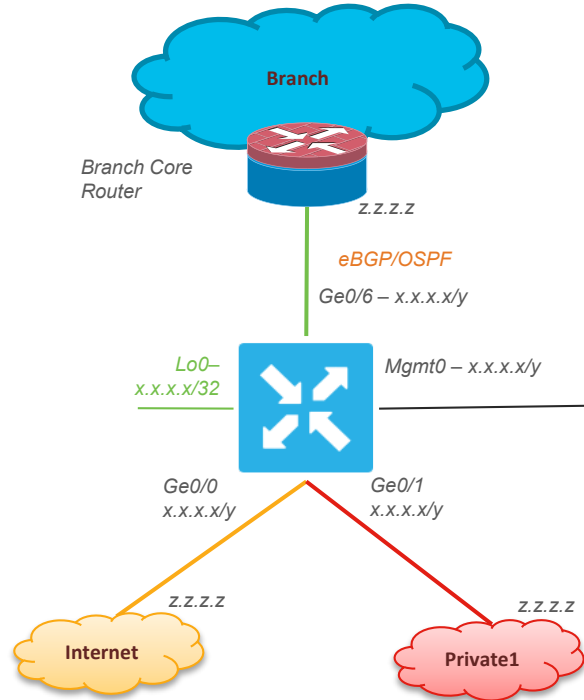
Ge0/0 – Connects to Internet (color gold)
Ge0/1 – Connects to MPLS (color mpls)
Specify next-hop (z.z.z.z) for both

Detailed site design

L3 Branch - Single WAN Edge



Site-ID:
Location:



Hostname: wanedge-a
Serial Number:
System-IP: a.a.a.a
Mgmt gateway: z.z.z.z

Inside VPN:

VPN Number: X
ge0/6 – BGP/OSPF Interface to Core
BGP Local-AS:
BGP/OSPF Neighbor IP (z.z.z.z)
BGP Remote-AS:

Transport VPN:

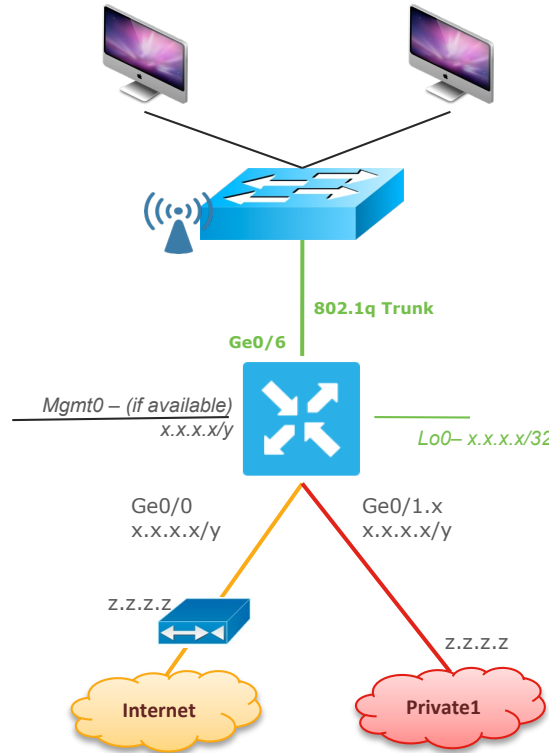
Ge0/0 – Connects to Internet (color gold)
Ge0/1 – Connects to MPLS (color mpls)
Specify next-hop (z.z.z.z) for both

Detailed site design

L2 Branch - Single WAN Edge



Site-ID:
Location:



Hostname: wanedge-a
Serial Number:
System-IP: a.a.a.a
Mgmt gateway: z.z.z.z

User-side VPN:

VPN Number: X
Gateway for VLANs:

100 - x.x.x.x/y
200 - x.x.x.x/y
300 - x.x.x.x/y
...
...

Transport VPN:

Ge0/0 - Internet Port (color gold)
Ge0/1.x - MPLS Port (color mpls)
Specify Next Hops for both if static IPs are used

Detailed site design

L2 Branch – Dual WAN Edge Configuration



For your POC

Site-ID:
Location:

User-side VPN:

VPN Number: X
Gateway for VLANs:

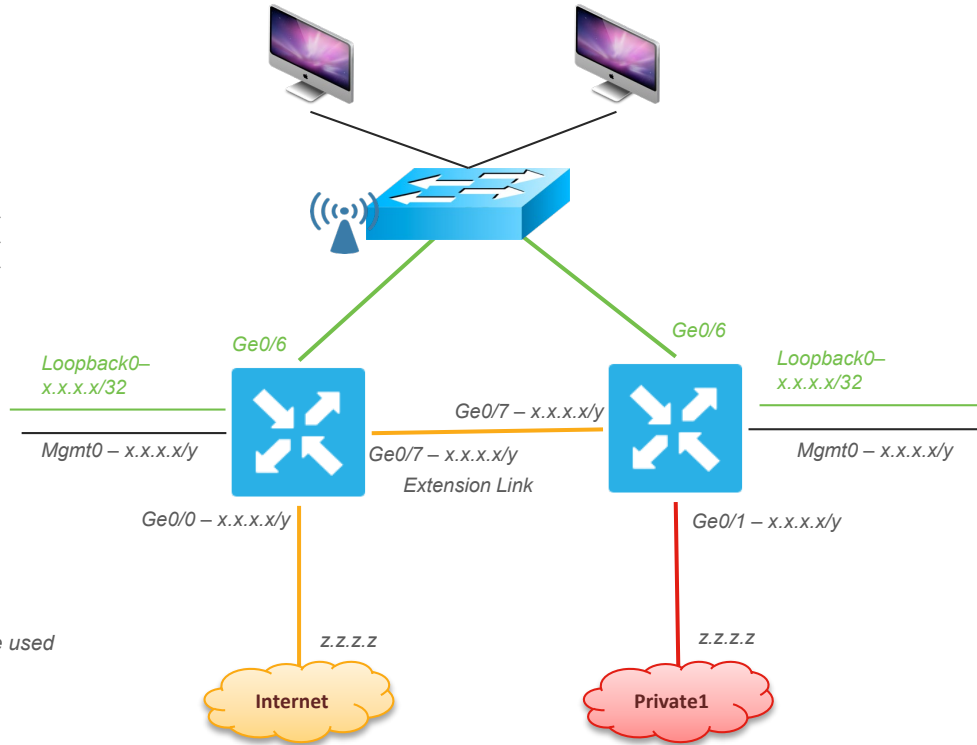
100 – x.x.x.x/y – VRRP-IP: x.x.x.x
200 – x.x.x.x/y – VRRP-IP: x.x.x.x
300 – x.x.x.x/y – VRRP-IP: x.x.x.x
...
...

Hostname: wanedge-a
Serial Number:
System-IP: a.a.a.a
Mgmt gateway: z.z.z.z

Transport VPN:

Ge0/0 – Internet Port (color gold)
Specify Next Hops if static IPs are used

Extension link used for MPLS



User-side VPN:

VPN Number: X
Gateway for VLANs:

100 – x.x.x.x/y – VRRP-IP: x.x.x.x
200 – x.x.x.x/y – VRRP-IP: x.x.x.x
300 – x.x.x.x/y – VRRP-IP: x.x.x.x
...
...

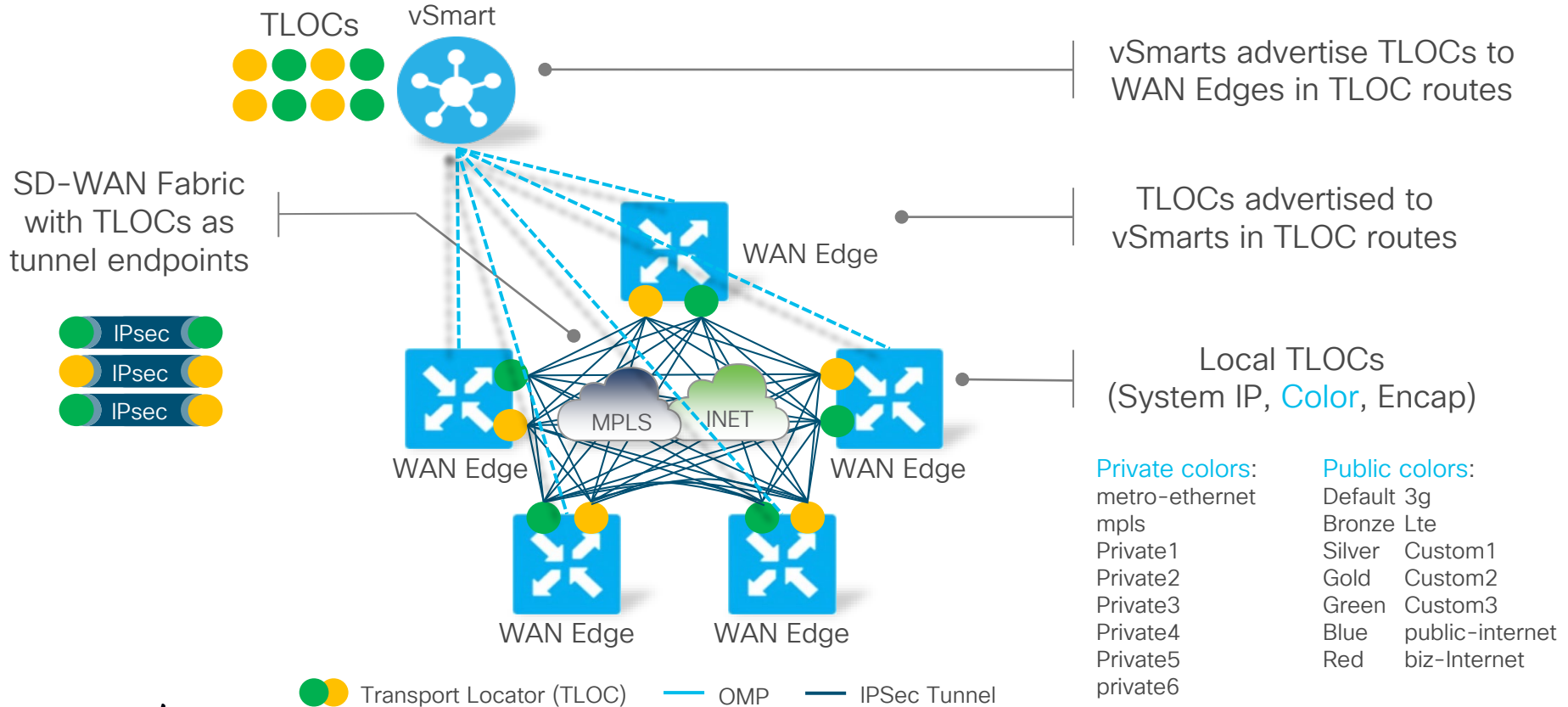
Hostname: wanedge-b
Serial Number:
System-IP: a.a.a.a
Mgmt gateway: z.z.z.z

Transport VPN:

Ge0/1 – MPLS Port (color mpls)
Specify Next Hops if static IPs are used

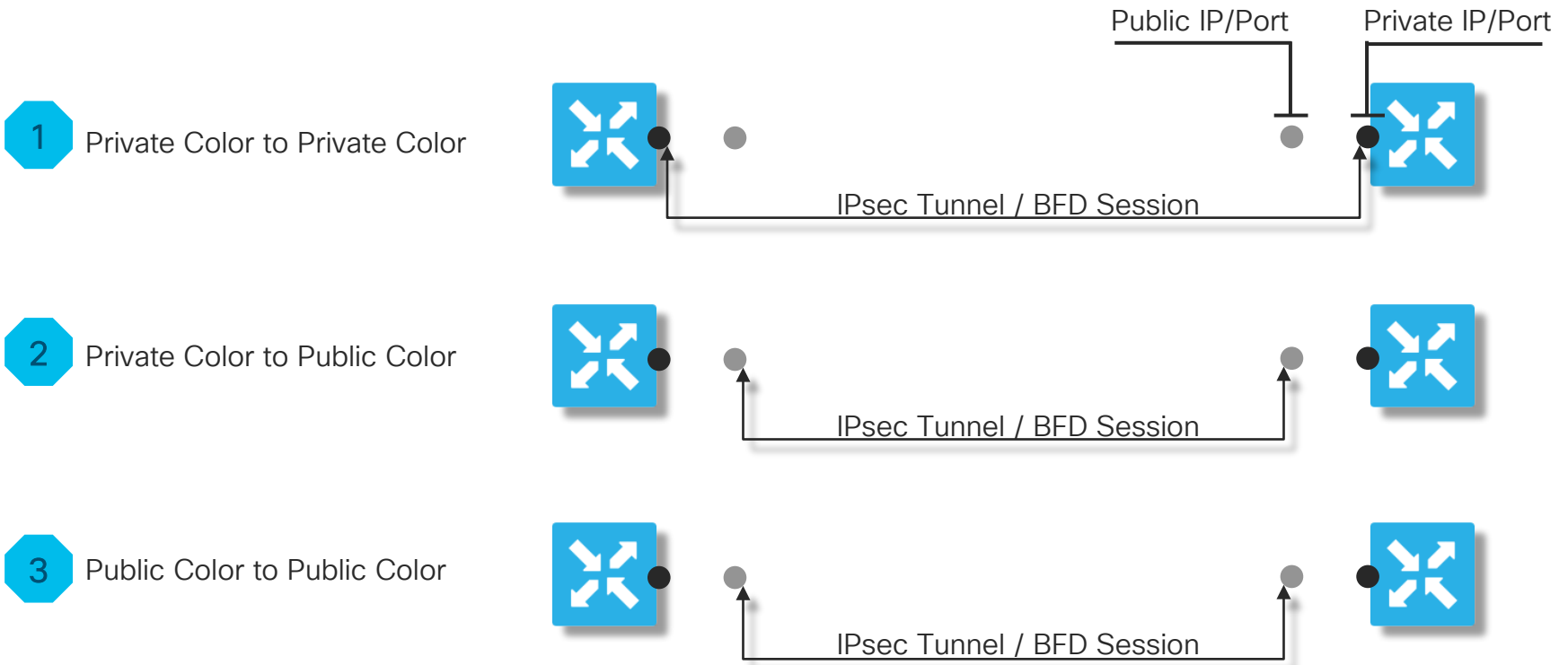
Extension link used for Internet

Transport Locators (TLOCs)



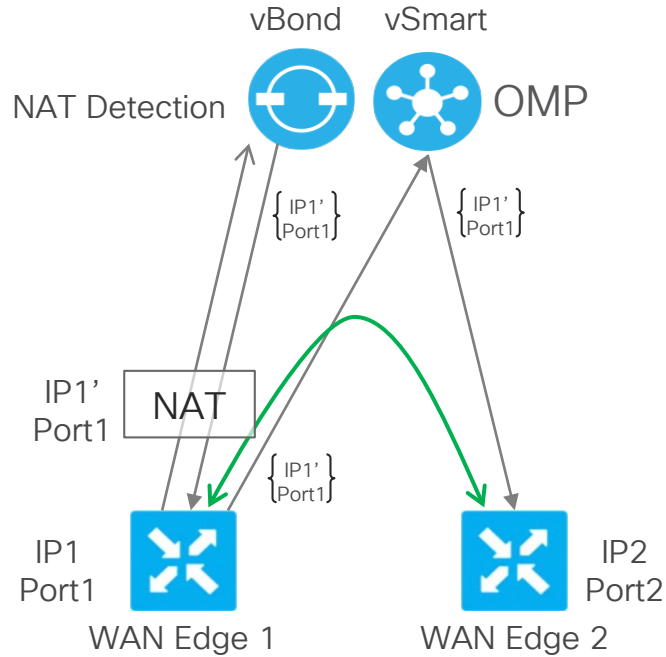
If simulating Internet, be careful with TLOC Color

Public Color will expect NAT



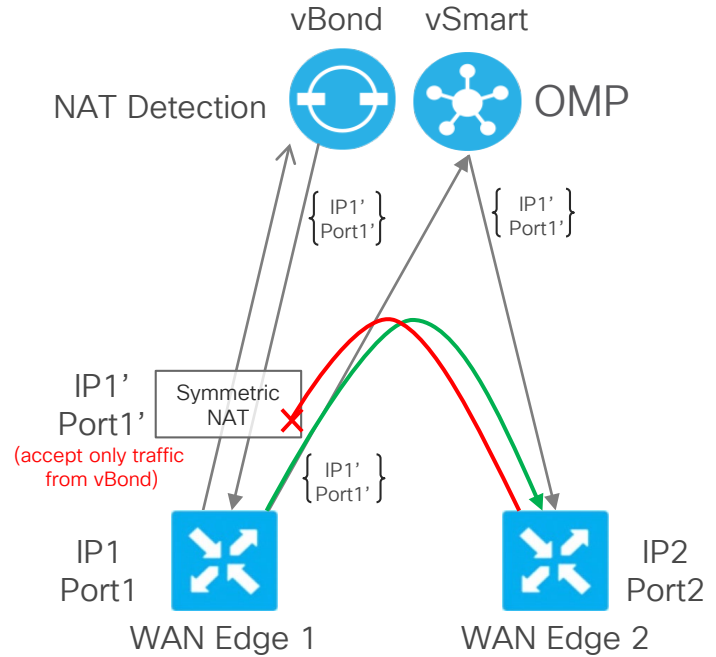
NAT Traversal

Full-Cone NAT



— Successful IPSec connection










Symmetric NAT





— Successful IPSec connection — Unsuccessful IPSec connection

NAT Traversal Combinations

vBond allows very good NAT traversal

Side A	Side B	IPSec Tunnel Status	
Public / Static	Public / Static		
Full Cone	Full Cone		
Public / Static	Full Cone		
Public / Static	Symmetric		
Full Cone	Symmetric		
Symmetric	Symmetric		

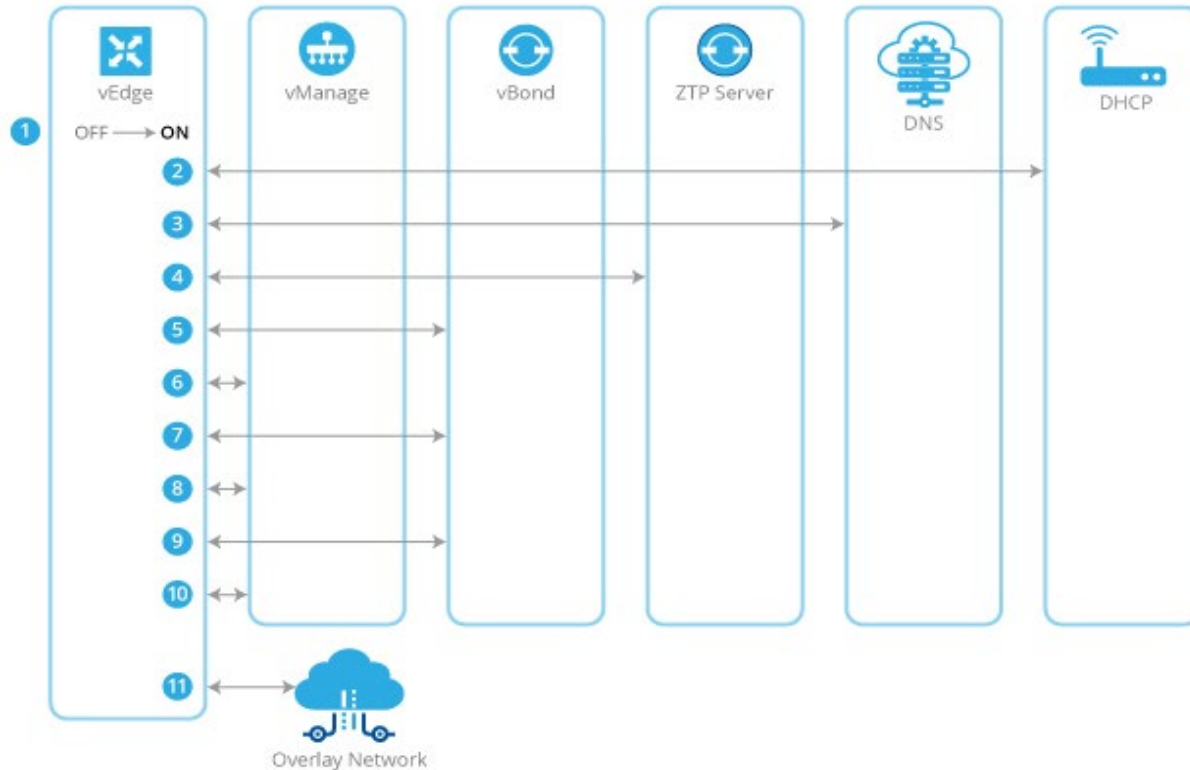
 Direct IPSec Tunnel

 No Direct IPSec Tunnel (traffic traverses hub)

 Mostly Encountered

Want to test complete Zero Touch?

Make sure **DHCP**, DNS and Internet access is available on site



Nice to Have



Network elements	IP	Information
AAA		
Syslog		
SNMP		
Netflow Collector		
Terminal server		
FTP/SCP Server		

Testing pre-requisites



For your
POC

Pre-requisites

Availability

Capability to generate loss/latency/jitter on transports
(WANem, Raspberry PI, Bufferbloat...)

Capability to generate application test traffic

Capability to measure test application experience (nice to have)

Capability to generate test traffic to measure device performance (nice to have)
(TRex, Ixia, Spirent, Ostinato...)

Note:

- ✓ In a Pilote it will be more difficult to add WAN impairment. You can however modify policy triggers above and below existing WAN performance to test both outcomes.
- ✓ WAN Edge devices are able to simulate application traffic behavior. This is a good way to test policy results.
- ✓ For Performance testing, use multiple flows with multiple IP pairs and realistic packet mixes. High CPU load is expected behavior on some devices to reduce latency, in adherence with best practice.

Pre-POC activities



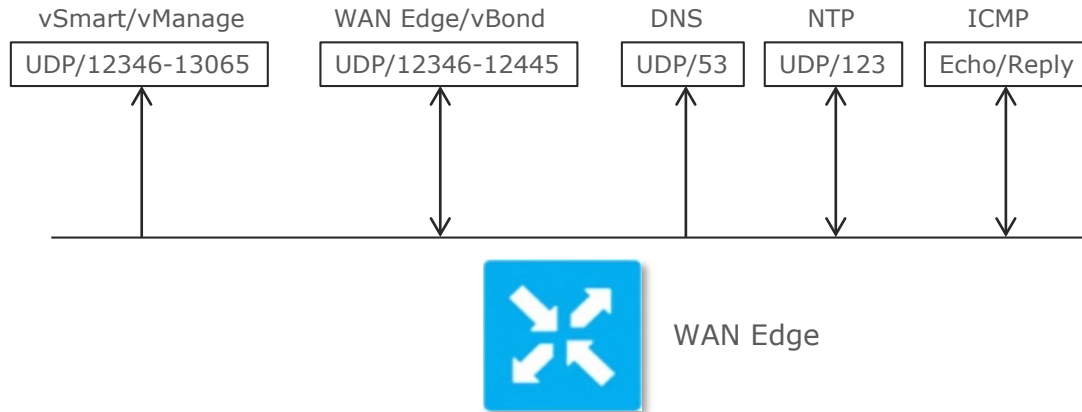
For your
POC

Pre-requisites	Person in charge	Done?
Smart Account configuration		
Controllers deployment		
WAN Edge image upgrade		
Test environment configurations		
Nat configuration		
Firewall ports opened		

Required Firewall Ports Summary

Unrestricted connection is requested

The following port ranges will allow connectivity with DTLS Control Plane (default)



More granularity on Firewall ports to open is available in the Getting Started Guide:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Firewall_Ports_for_Viptela_Deployments_8690.xml

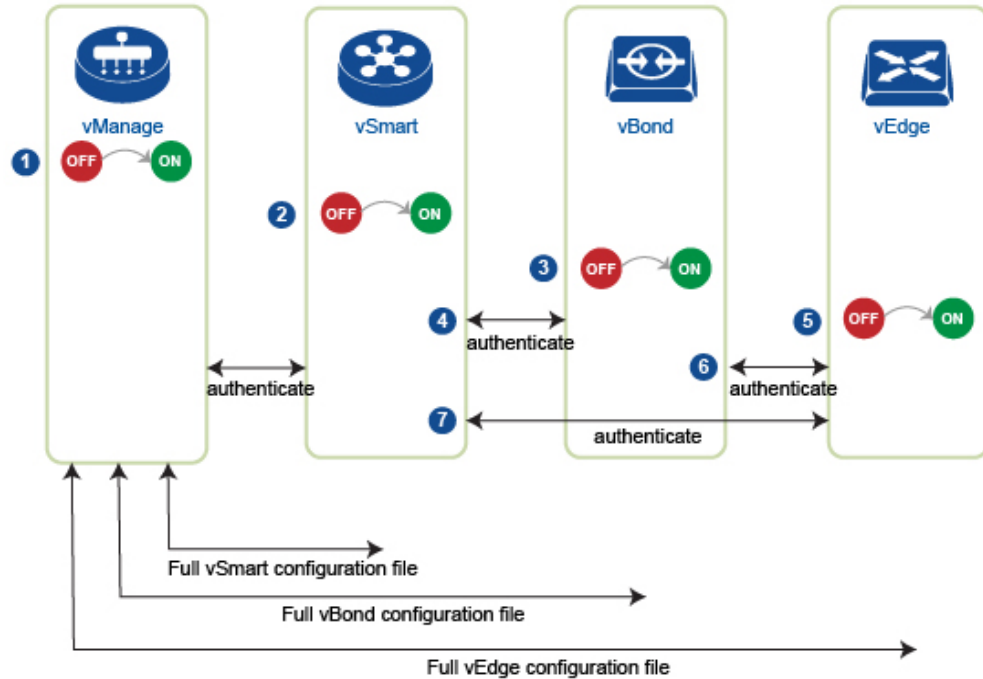
Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

On-premise controllers specific pre-requisites

Bring-up sequence of events



On-prem controllers pre-requisites



For your
POC

Pre-requisites	Availability
ESXi/KVM infrastructure available	
vManage server resources 1 mandatory	
vBond server resources 1 mandatory	
vSmart server resources 2 VM on different DC mandatory if production traffic	
Possibility to add vBond FQDN in DNS	
PKI to be used for controllers (if Cisco certificates are not used)	

Verifying vManage System Requirements

Devices	vCPUs	RAM	OS Volume	Database Volume	Bandwidth	vNICs
1-250	16	32 GB	16 GB	500 GB, 1500 IOPS	25 Mbps	2
251-1000	32	64 GB	16 GB	1 TB, 3072 IOPS	100 Mbps	2
1001 or more	32	64 GB	16 GB	1 TB, 3072 IOPS	150 Mbps	3*

* vManage Cluster requires dedicated interface for message bus

Note:

- ✓ SSD is required for normal vManage performance
- ✓ POC setup can work with less resources, but normal behavior is not guaranteed

Verifying vSmart System Requirements

Devices	vCPUs	RAM	OS Volume	Bandwidth	vNICs
1-50	2	4 GB	16 GB	2 Mbps	2
51-250	4	6 GB	16 GB	5 Mbps	2
251-1000	4	16 GB	16 GB	7 Mbps	2
1001+	8	16 GB	16 GB	10 Mbps	2

Note:

- ✓ Only SSD based volumes are officially supported (HDD possible for testing)

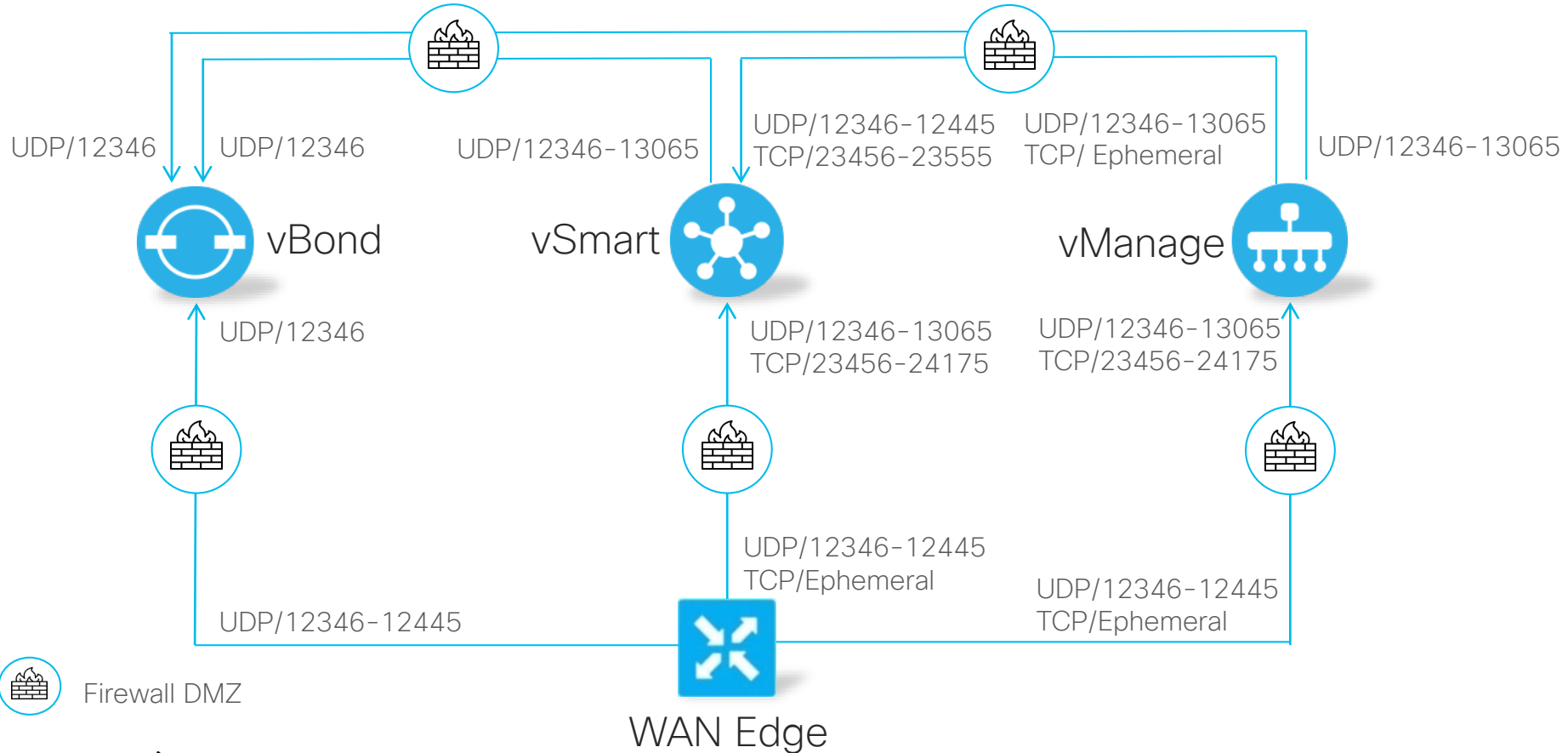
Verifying vBond System Requirements

Devices	vCPUs	RAM	OS Volume	Bandwidth	vNICs
1-50	2	4 GB	8 GB	1 Mbps	2
51-250	2	4 GB	8 GB	2 Mbps	2
251-1000	2	4 GB	8 GB	5 Mbps	2
1001+	4	8 GB	8 GB	10 Mbps	2

Note:

- ✓ Only SSD based volumes are officially supported (HDD possible for testing)
- ✓ vBond is installed using vEdgeCloud OVA
- ✓ OVA is preconfigured with four vCPUs

Firewall Rules for On-Prem Controllers



 Firewall DMZ

WAN Edge

Documentation for on-prem controllers

- Cisco Live – BRKRST-2559 – 3 Steps to Deploy Cisco SD-WAN On-Prem
<https://www.ciscolive.com/global/on-demand-library.html?search=BRKRST-2559#/>
- Cisco SD-WAN Getting Started documentation
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html - c Server Hardware Recommendations 7477.xml>
- Cisco SD-WAN Certificates Deployment Guide
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/cisco-sd-wan-certificates-deploy-2019sep.pdf>

Should you do a
SD-WAN POC?

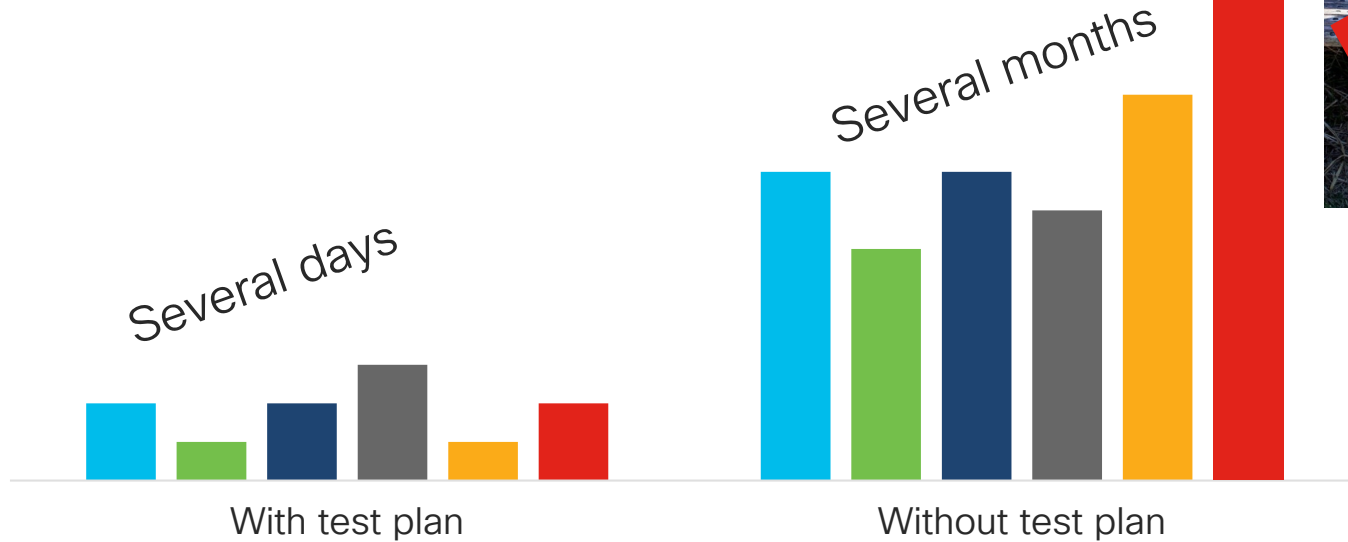
Pre-requisites

Step by Step
POC deployment

Test Plan

Time needed to do a POC

More time spent on planning means shorter POC



Having a test plan gives clear boundaries to the POC



Generic Test Plan

Create a test plan around features you need



For your
POC

Test No.	Test Description	Pass/Fail Result
1.0	System Bring-up and Baseline	Pass Fail
2.0	Zero-touch Provisioning	Pass Fail
3.0	Segmentation	Pass Fail
4.0	Service Insertion	Pass Fail
5.0	Application Aware Routing	Pass Fail
6.0	DC Routing	Pass Fail
7.0	Enhanced data plane security	Pass Fail
8.0	High-Availability	Pass Fail
8.1	Controller Failure	Pass Fail
8.2	WAN Edge Failure branch	Pass Fail
8.3	WAN Edge Failure DC	Pass Fail
8.4	Internet Failure at DC	Pass Fail
8.5	MPLS Failure at DC	Pass Fail
8.6	Internet Failure at Branch	Pass Fail
8.7	MPLS Failure at Branch	Pass Fail
9.0	QoS	Pass Fail
10.0	Direct Internet Access	Pass Fail
11.0	Software Upgrade	Pass Fail
12.0	Deep Packet Inspection	Pass Fail
13.0	Secure Cloud Gateway Integration	Pass Fail
14.0	Multicast	Pass Fail
15.0	Cloud onRamp for SaaS and IaaS	Pass Fail

*Add/Remove tests as per requirements

Some use cases



For your
POC

Test No.	Test Description	Pass/Fail Result
1	System Bring-up and Baseline	Pass Fail
1.1	SD-WAN fabric creation	Pass Fail
1.2	Routing with existing network (DC and branch)	Pass Fail
1.3	Reachability of all sites	Pass Fail
1.4	Reachability between SD-WAN branch and traditional network through gateway in DC	Pass Fail
1.5	Zero-touch Provisioning	Pass Fail
1.6	Clear isolation between overlay and underlay	Pass Fail
1.7	Segmentation (Overlapping IPs in different VPN)	Pass Fail
1.8	Monitoring capacities	Pass Fail
1.9	Troubleshooting tools	Pass Fail

*Change tests as per requirement

Topology use cases



For your
POC

Test No.	Test Description	Pass/Fail Result
2	Topology	Pass Fail
2.1	Hub and spokes	Pass Fail
2.2	Full mesh	Pass Fail
2.3	Partial mesh	Pass Fail
2.4	Per VPN topology	Pass Fail

*Change tests as per requirement

High availability use cases

A must do!



For your
POC

Test No.	Test Description	Pass/Fail Result
3	High-Availability	Pass Fail
3.1	Controller Failure	Pass Fail
3.2	WAN Edge Failure branch	Pass Fail
3.3	WAN Edge Failure DC	Pass Fail
3.4	Internet Failure at DC	Pass Fail
3.5	MPLS Failure at DC	Pass Fail
3.6	Internet Failure at Branch	Pass Fail
3.7	MPLS Failure at Branch	Pass Fail

*Change tests as per requirement

Application use cases



For your
POC

Test No.	Test Description	Pass/Fail Result
4	Application performance	Pass Fail
4.1	DPI and application dashboards	Pass Fail
4.2	Application Aware Routing (per VPN policy)	Pass Fail
4.3	DIA (per VPN policy)	Pass Fail
4.4	Cloud onRamp for SaaS (per VPN policy)	Pass Fail
4.5	Cloud onramp for IaaS	Pass Fail
4.6	QoS configuration	Pass Fail

*Change tests as per requirement

Security use cases



For your
POC

Test No.	Test Description	Pass/Fail Result
5	Content Security and others	Pass Fail
5.1	Zone based Firewall	Pass Fail
5.2	IPS*	Pass Fail
5.3	URL Filtering*	Pass Fail
5.4	Advanced Malware Protection (AMP) *	Pass Fail
5.5	Cloud Web / DNS Security	Pass Fail
5.6	Service Insertion	Pass Fail

*Requires ISR with 8 GB RAM/Flash

*Change tests as per requirement

And again use cases

Not exhaustive lists, add use cases relevant to your reality



For your
POC

Test No.	Test Description	Pass/Fail Result
6	Others	Pass Fail
6.1	Device rollback when wrong configuration is pushed	Pass Fail
6.2	Software update from vManage	Pass Fail
6.3	Service Insertion	Pass Fail
6.4	IPv6 clients	Pass Fail
6.5	Multicast	Pass Fail
6.6	Netflow	Pass Fail
6.7	vManage Northboud APIs	Pass Fail

*Change tests as per requirement

Plan each test

With description and success criteria



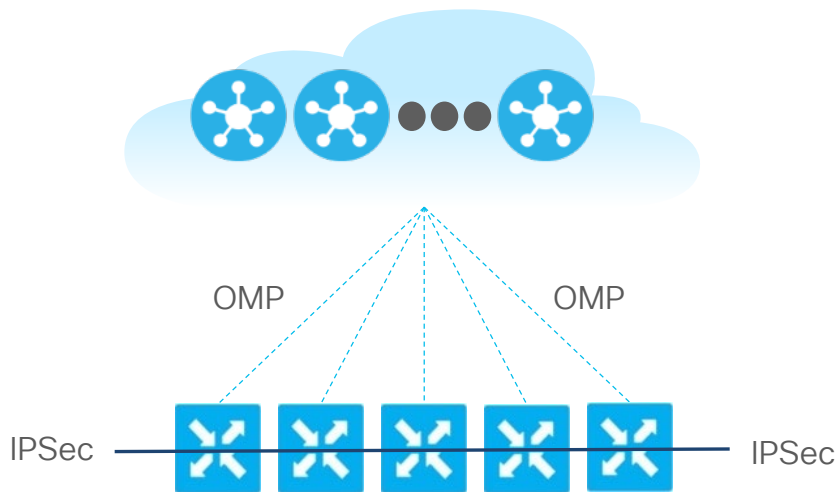
For your
POC

Test name	Test exemple
Test description	Description
Passing criteria	Criteria
Test result	Pass / Fail
Details	Details

Solution scalability

Hard to test in POC, but the solution architecture is also important

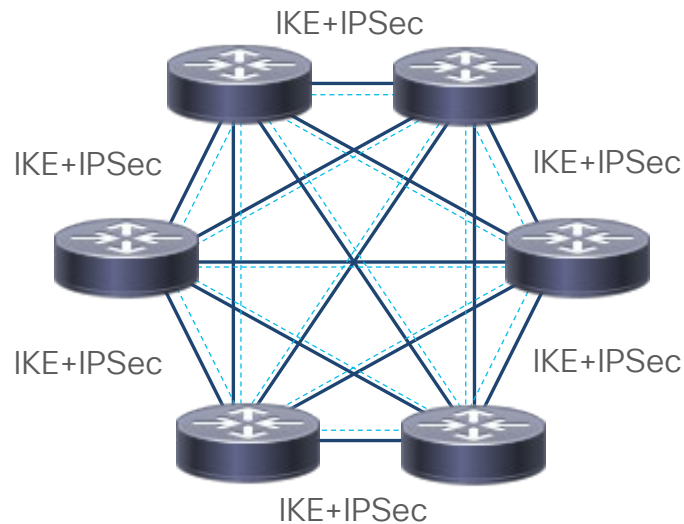
SD-WAN



Linear Control Plane Complexity
 $O(n)$

cisco *Live!*

Traditional IPsec networks



Quadratic Control Plane Complexity
 $O(n^2)$

Validating the Test Plan

- Avoid last minute changes of plan
- Follow and validate the test plan step by step
 - Make sure you understand what is happening
- Having someone prepare templates and policies in advance is ideal
- All the POC configurations can be reused in your final deployment
 - Keep the same controllers
 - Or export templates and policies using [Python scripts](#)



Device configuration via centralized Templates

The screenshot displays the Cisco vManage interface for configuring templates. The left pane shows the configuration for a 'vEdge 100 B' device model, with the 'Home-vEdge-100b' template selected. The right pane shows a table of templates with the following data:

Name	Description	Type	Device Model	Feature Templates	Devices Attached
vSmart	vSmart Productio...	CLI	vSmart	0	1
Home-vEdge-100b	Home-vEdge-100b	Feature	vEdge 100 B	16	16
home-vedge-1000	template for hom...	Feature	vEdge 1000	17	3
Home-vEdge-100	Home-vEdge-100	Feature	vEdge 100	16	1
vBond-Template	vBond Template	Feature	vEdge Cloud	12	1

The 'Basic Information' section for the selected template includes the following configuration:

- System: CorpNet-System
- Logging: CorpNet-Logging
- NTP: CorpNet-NTP
- AAA: Radius
- BFD: CorpNet-BFD
- OMP: CorpNet-vEdge-OMP
- Security: CorpNet-IPSec

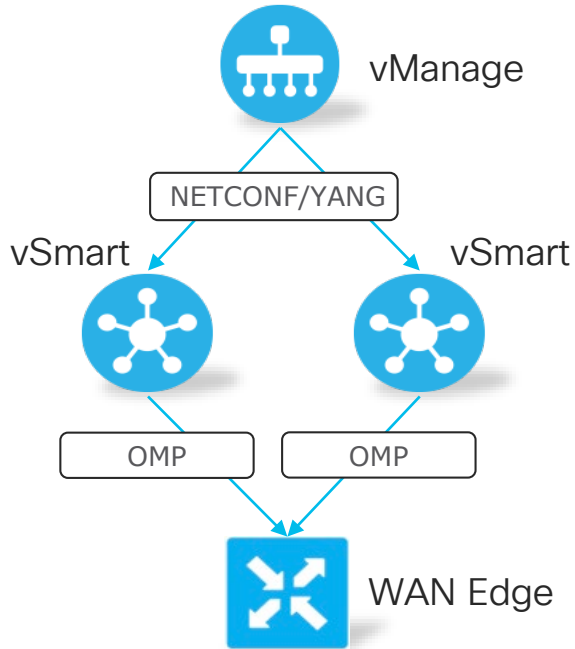
Arrows indicate the relationship between the table and the configuration pane: the 'Home-vEdge-100b' template name is linked to the configuration pane, and the '16' feature templates and '16' devices attached counts are linked to the configuration pane's 'Basic Information' section.

WAN Edge

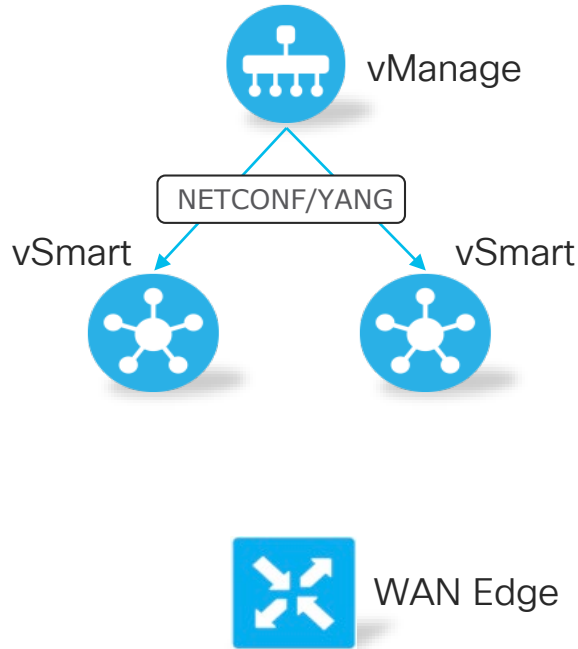
- Centralized Feature Templates
- Configuration with variables
- Self-recover on misconfiguration

Policy Framework

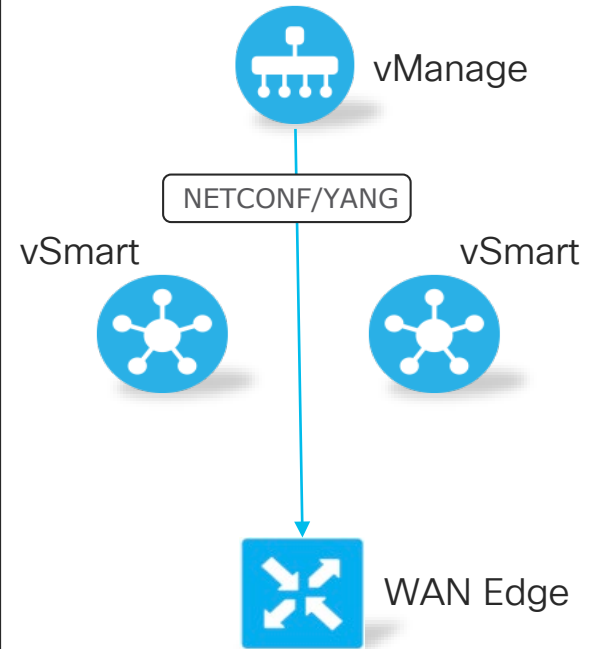
Centralized Data Policy
(Acting on VPN Traffic)
App Aware Routing Policy
(assigning SLA)



Centralized Control Policy
(acting on overlay routing, i.e. Topology)



Local Policies
(BGP, OSPF, QoS, Mirror, ACL)

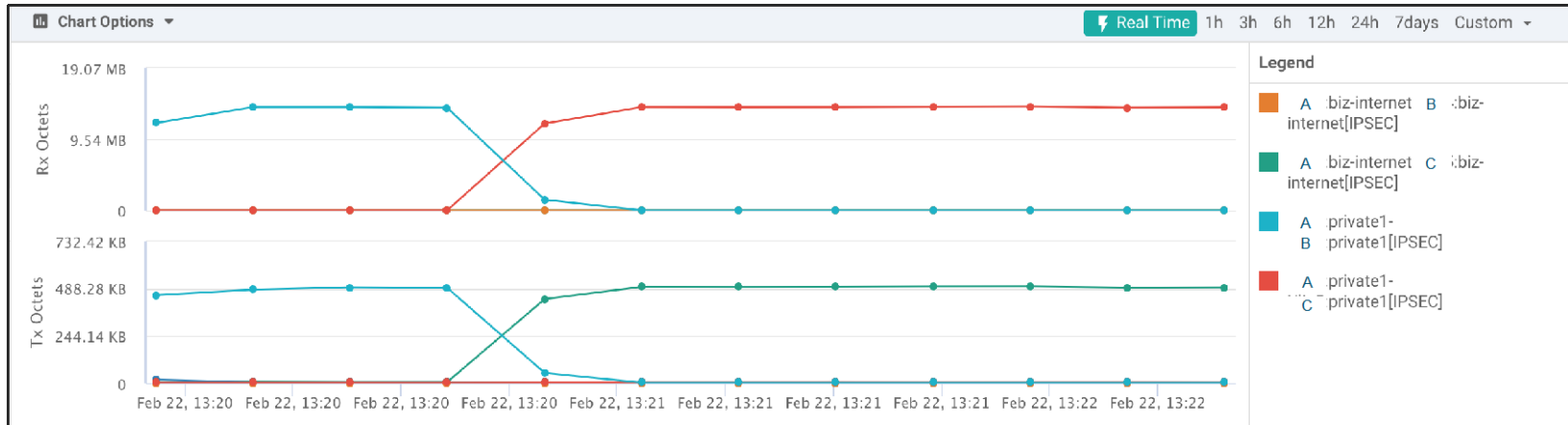


Real time monitoring

You can see the consequence of your policy in real time

To see your traffic changing path without waiting for telemetry update, use:

- 'Interface' Tab of the device in the Monitor → Network menu
- 'Kbps' setting in
- 'Real Time' time setting



Documentation for creating policies

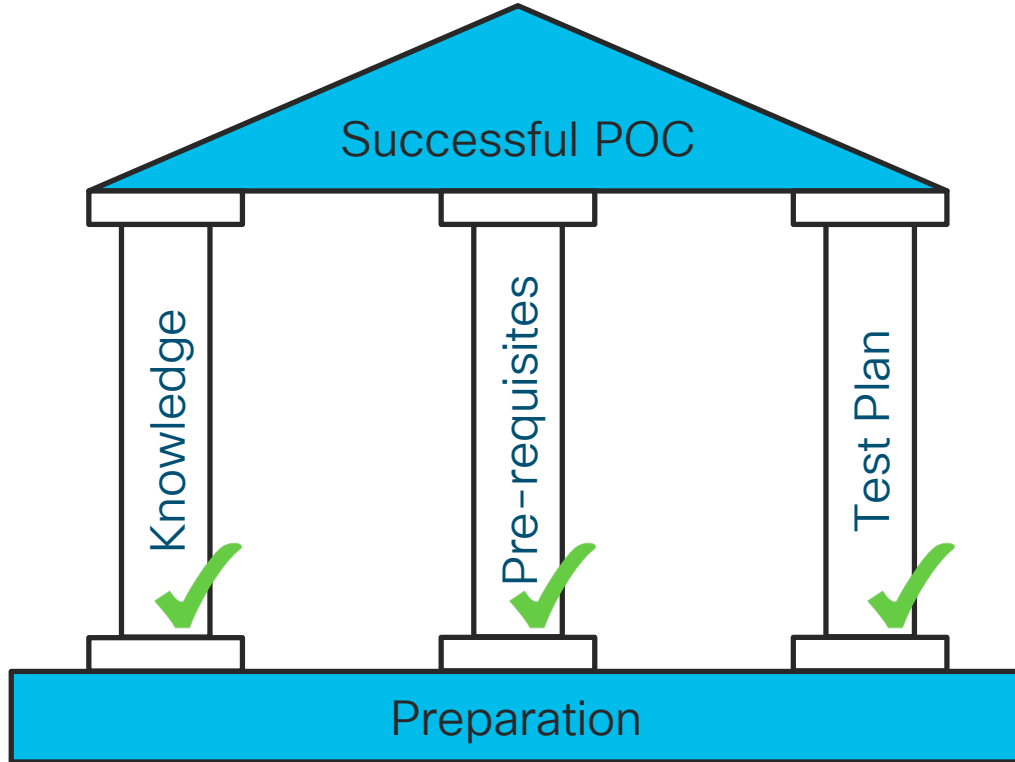
- BRKRST-2791 - Building & using Policies with Cisco SD-WAN

<https://www.ciscolive.com/global/on-demand-library.html?search=BRKRST-2791#/>

- Cisco SD-WAN Configuration Guides

<https://www.cisco.com/c/en/us/support/routers/sd-wan/products-installation-and-configuration-guides-list.html>

Preparation is the Foundation of your POC



Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

POC deployment Step by Step

POC deployment Agenda

1. Controllers deployment
2. WAN Edge Image Upgrade & Bring-up
3. Bring-up Troubleshooting
4. Tuning for POC!

Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Controllers deployment

To do before the POC

Should you do a
SD-WAN POC?

Pre-requisites

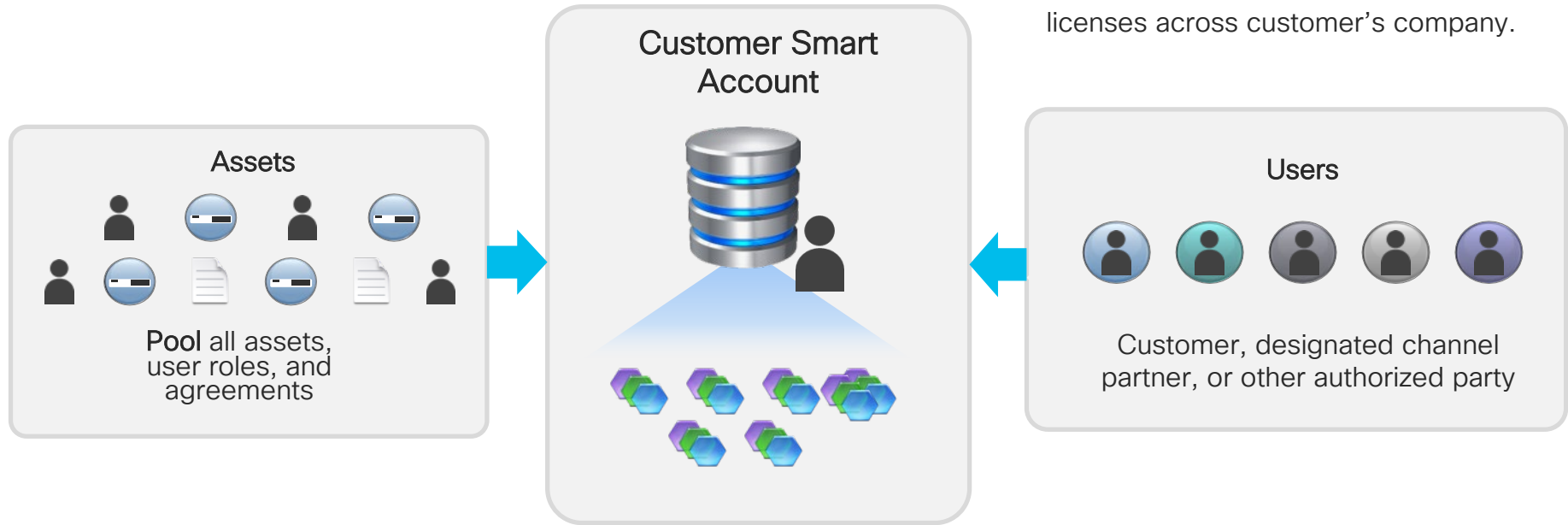
Step by Step
POC deployment

Step 1

Obtaining Smart Account and Virtual Account

Smart Accounts

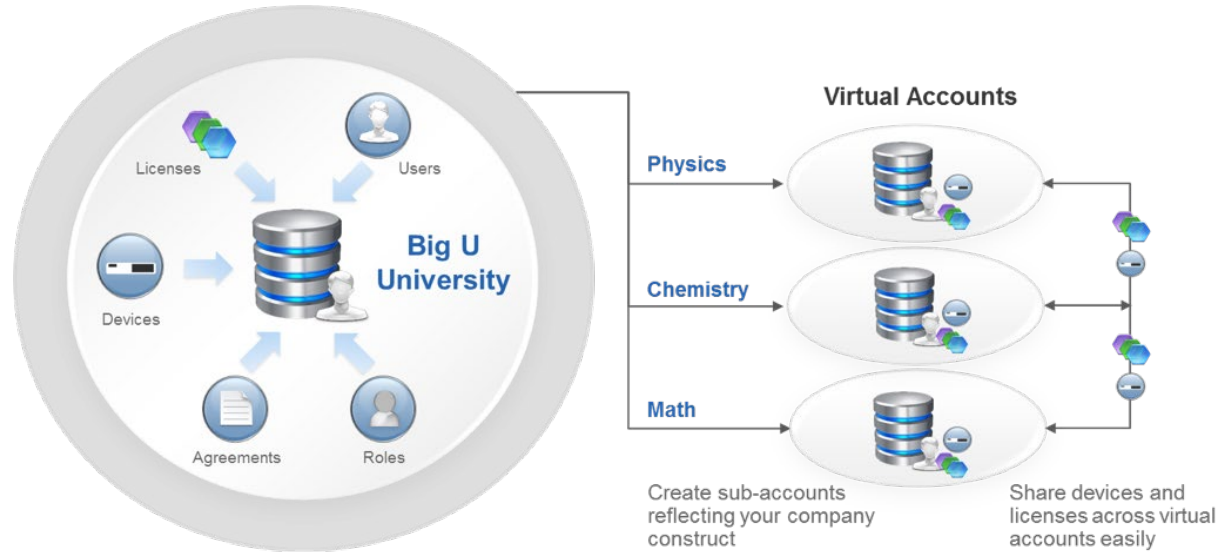
A customer or partner managed **centralized account** that provides **full visibility** and **access control** of Cisco Smart software licenses across customer's company.



Additional End State Benefits of Smart Accounts include:

- ✓ Find out what new licenses you have
- ✓ Review Service contracts
- ✓ Review logs
- ✓ Track Purchases

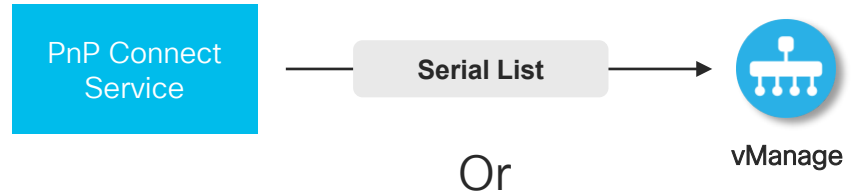
Virtual Accounts



- **Virtual Account:** A customer defined constructs to reflect company organization, geography, budgeting or other structure
- Created and maintained by the customer on the Cisco Smart Account Manager

Serial List

Devices in the Smart Account will be the device whitelist in vManage



The signed file can be provisioned into vManage in two ways:

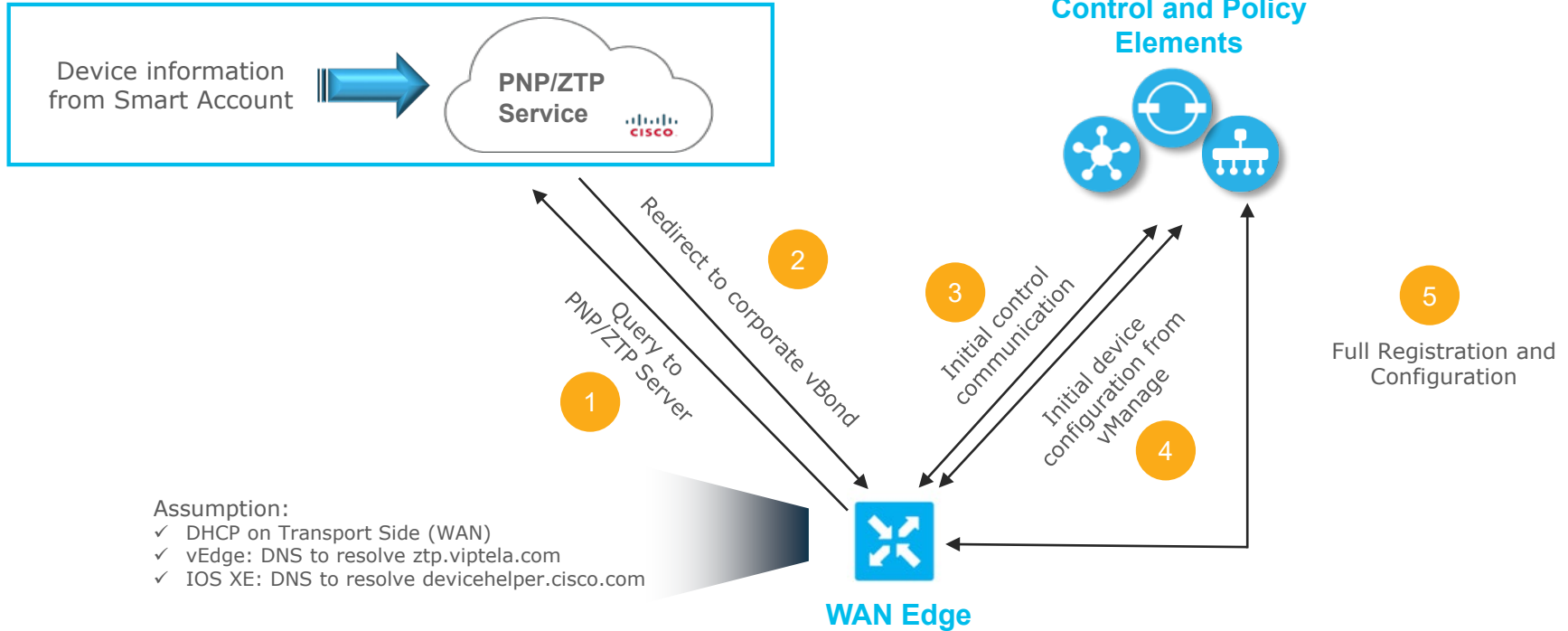
- **Automatic** – If on vManage 18.3 or later, click the ‘Sync Smart Account’ under Configuration > Devices tab
- **Manually** – If using the Sync feature is not an option, download the Serial File from the PnP Connect portal and manually upload to vManage

The screenshot shows the Cisco vManage interface. The top navigation bar includes 'Cisco vManage' and 'CONFIGURATION | DEVICES'. Below this, there are tabs for 'WAN Edge List' and 'Controllers'. A toolbar contains several buttons: 'Change Mode', 'Upload WAN Edge List', 'Export Bootstrap Configuration', and 'Sync Smart Account'. The 'Sync Smart Account' button is highlighted with a black rectangular box. Below the toolbar is a search bar and a table with the following columns: State, Device Model, Chassis Number, Serial No./Token, Hostname, and System IP.

State	Device Model	Chassis Number	Serial No./Token	Hostname	System IP
✓	vEdge Cloud	94eb2868-1776-b1c6-ad04-de55143fc7...	6fa11dcd	vedge-11	10.0.0.11
✓	vEdge Cloud	01739a52-a22e-9d1e-56f4-bda8636f20...	7846c278	vedge-12	10.0.0.12
✓	vEdge Cloud	23a802e0-6f9b-1d1e-3061-81ef9205f319	87b405f6	vedge-21	10.0.0.21
✓	vEdge Cloud	0adb013c-11cf-ebf0-bdd5-45e3e4c1a1...	8a7a1721	vedge-22	10.0.0.22
✓	vEdge Cloud	9670f486-3257-0e9a-8a42-c25f48df146f	9b39badf	vedge-31	10.0.0.31
✓	vEdge Cloud	a4646e57-32f1-b0a5-7a4c-1d2de82936...	1c3c7b7a	vedge-41	10.0.0.41
✓	vEdge Cloud	ed74d307-fee3-ed1b-377b-dd6841606...	6aea21c1	vedge-42	10.0.0.42
⚠	vEdge Cloud	6b0e358b-1538-c155-f3cc-694520bdbe...	Token - a3c6bdd2bac2...	--	--
⚠	vEdge Cloud	b03b028e-420d-e64a-d730-6f2bcafad0...	Token - 050fd60bb5cc3...	--	--

Zero Touch Provisioning

Smart Account is part of the ZTP process



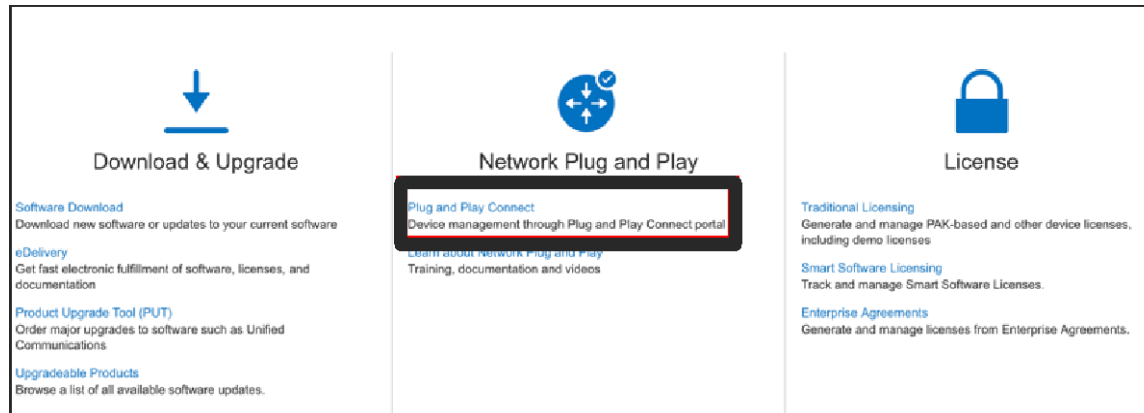
What About POCs

- For POCs where Try and Buy PIDs are ordered, the process would be automated just like it is for regular orders.
 - Virtual Account is provided during order and populated automatically
- For POCs where equipment is already available
 - **Device** information will not be auto-populated into the Virtual Account
 - **vBond** information will not be auto-populated into the Virtual Account
 - Cisco can provide Demo Smart Account / Virtual Account for POCs

Using the Virtual Account

Step1.1 – Log in Plug and Play Connect

- Login at software.cisco.com
- Click on Plug and Play Connect:

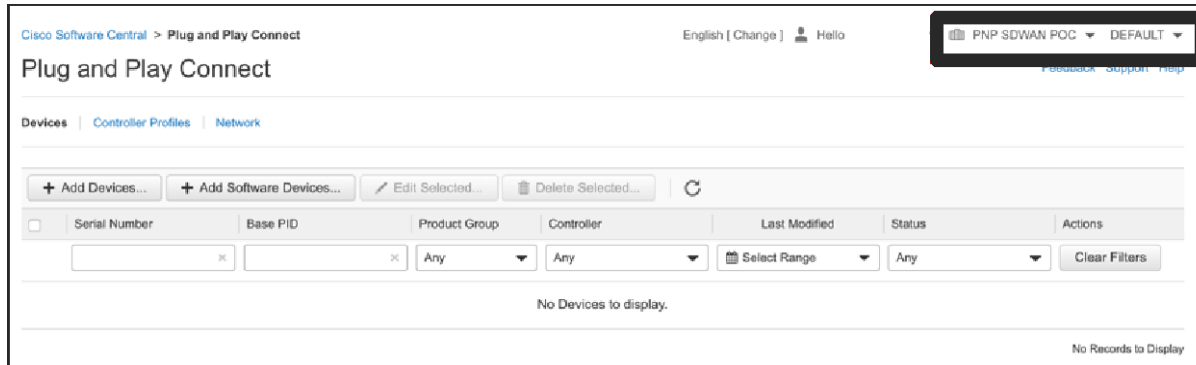


Using the Virtual Account

Step1.2 – Getting started with your Virtual Account

Ensure that your Smart Account and Virtual Account match in top right corner

- Name of the Smart Account in the left column (here PNP SDWAN POC)
- Name of the Virtual Account in the right column



The screenshot shows the Cisco Software Central interface for 'Plug and Play Connect'. In the top right corner, there is a dropdown menu for the Smart Account, currently set to 'PNP SDWAN POC', and another dropdown for the Virtual Account, currently set to 'DEFAULT'. Both dropdowns are highlighted with a black box. Below the account information, there are navigation tabs for 'Devices', 'Controller Profiles', and 'Network'. A toolbar contains buttons for '+ Add Devices...', '+ Add Software Devices...', 'Edit Selected...', and 'Delete Selected...', along with a refresh icon. Below the toolbar is a table with columns: Serial Number, Base PID, Product Group, Controller, Last Modified, Status, and Actions. The table is currently empty, displaying 'No Devices to display.' and 'No Records to Display' at the bottom.

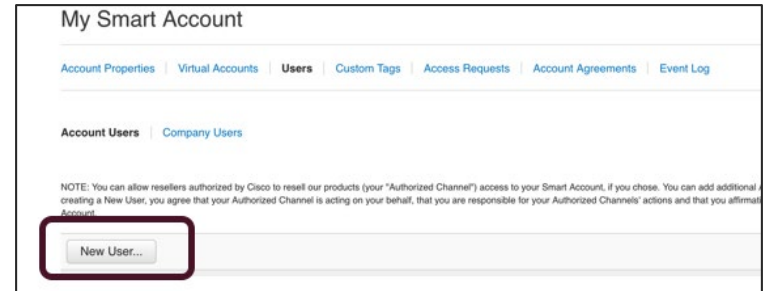
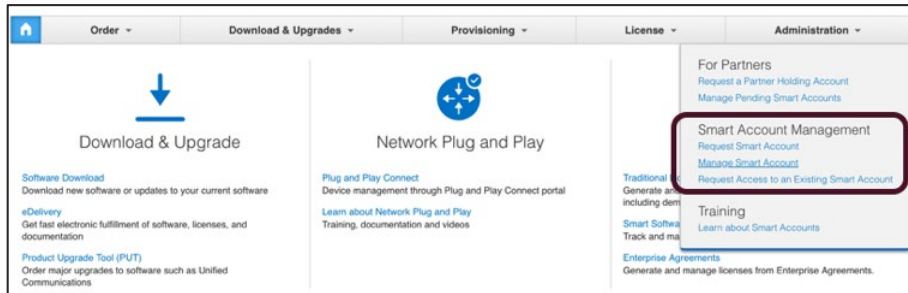
Using the Virtual Account

Step1.3 – Managing users

As an administrator, you can add other users to the account under the ‘Manage Smart Account’ option at software.cisco.com if required.

First, navigate to the account administration page:

Then select ‘New User’ in Users tab and provide the user information:



Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Step2

Instantiating the Controllers

Controllers Instantiation

2 choices:

- Hosted controllers (recommended) – Ask Cisco Sales team
 - Controllers will be deployed for up to 90 days with full features, no need for licenses
 - They will be automatically associated to the SA/VA
 - Give range of IP addresses to be whitelisted to access vManage GUI
 - vAnalytics can be included – ask for it when doing a Pilote (POC will lack data)
- On-prem controllers – Instantiate your own vManage/vSmart/vBond in your lab or datacenters.
 - Make sure IPs are reachable, through NAT and Firewall
 - Do Step3 section to associate to SA/VA

Deploying Controllers On-Prem

Installation Overview

1. Obtain [documentation](#), [software](#) and verify system requirements.
2. Import OVA.
3. Perform installation and initial configuration:
 - Connectivity (IP, GW, DNS)
 - System-IP
 - Site-ID
 - Organization-Name
 - vBond address
 - NTP
4. If using Enterprise CA server, install the enterprise root CA chain.

Documentation for on-prem controllers

- Cisco Live – BRKRST-2559 – 3 Steps to Deploy Cisco SD-WAN On-Prem
<https://www.ciscolive.com/global/on-demand-library.html?search=BRKRST-2559#/>
- Cisco SD-WAN Getting Started documentation
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html - c Server Hardware Recommendations 7477.xml>
- Cisco SD-WAN Certificates Deployment Guide
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/cisco-sd-wan-certificates-deploy-2019sep.pdf>

Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Step3

PnP Connect – Add Controller Profile

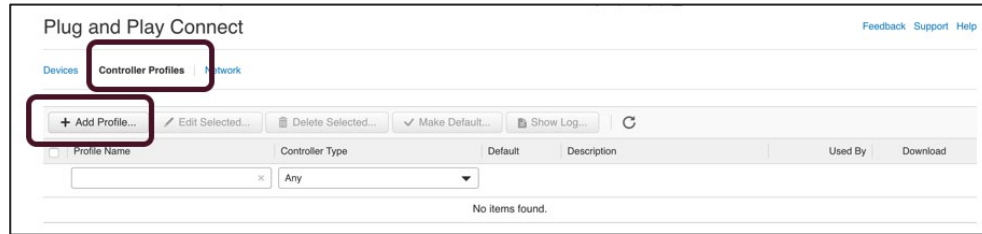
(Automatically populated for Cloud Controllers)

Add Controller Profile

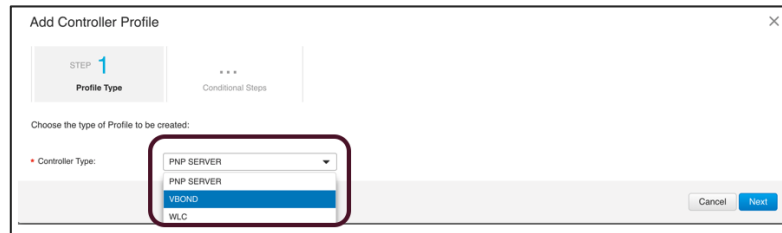
Step3.1 – Creating the Controller Profile

The Controller Profile and device information must be added in order to generate the signed serial file for vManage and provide proper PnP redirection for each device

- After connecting to the Virtual Account, click on Controller Profiles and select Add Profile:



- Select VBOND for the Controller Type:



Add Controller Profile

Step3.2 – Providing vBond information

- **Organization Name:** must match the overlay organisation-name
- **vBond address:** can be defined as a domain name (when DNS can be used) or an IP address
- Optionally, if an Enterprise CA is being used to sign certificates for the controllers, the corresponding Root CA can be provided to be downloaded to the device during the redirection process

The screenshot shows the 'Add Controller Profile' configuration window, specifically Step 2: Profile Settings. The window has a progress bar at the top with four steps: STEP 1 Profile Type (checked), STEP 2 Profile Settings (active), STEP 3 Review, and STEP 4 Confirmation. A warning message states: 'SAN in the certificate should match either the IP or hostname specified in the controller profile, SSL connectivity will fail otherwise'. The configuration fields are as follows:

- Profile Name: SDWAN-TME-LAB-PARIS
- Description: SD-WAN TME lab in Paris (ELM)
- Default Profile: Yes
- Organization Name: Cisco TME Lab Paris
- Primary Controller: IPv4, DTLS, 10.60.19.45, 12346
- Server Root CA: MIIEDCCASgIwBqUJLq5WMM9iRPMAGGCSyGS8i3DOEBwUAMGCG (Browse button)

Buttons at the bottom: Cancel, Back, Next.

Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Step4

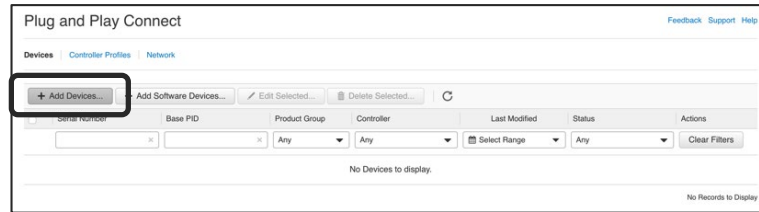
PnP Connect – Add Physical Devices

Add Physical Devices

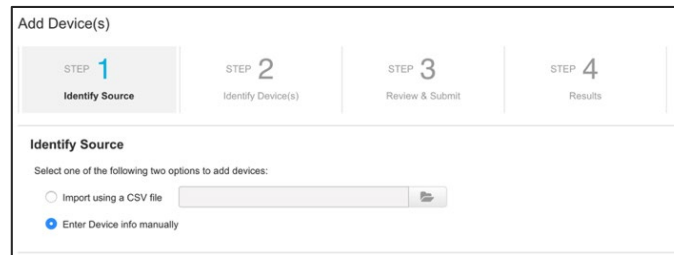
Step 4.1 – Adding the device

Once the Controller Profile is created, you can add devices into the Virtual Account and associate these to the newly-created profile.

- Under the Devices tab, click on Add Devices



- The devices can either be entered via a CSV or manually entered



Add Physical Devices

Step4.2 – Add Device Serial Number and PID

You will now be prompted for the device information:

- Serial Number
- Base PID

Identify Device

* Serial Number

* Base PID

Certificate Serial Number

Controller Profile

Description

These can be obtained via “show license udi”:

```
C4331#sh license udi
SlotID  PID                SN                UDI
-----
*       ISR4331/K9        FDO21XXXXXX      ISR4331/K9:FDO21XXXXXX
```

Add Physical Devices

Step4.3 – Certificate Serial Number (when migrating IOS XE Router)

When migrating IOS XE routers to SD-WAN, you will need to provide the SUDI Certificate Serial Number

This information can be obtained via:

- `show crypto pki certificate` if the device is still running IOS-XE* (prior to migration)
- `show sdwan certificate serial` if the device is already loaded with the SD-WAN image

This step is not necessary when the Smart Account is provided during the order

Identify Device

* Serial Number: FDO19060072

* Base PID: ISR4331/K9

Certificate Serial Number: 4021D0

Controller Profile: RTP-SDWAN-LAB

Description: Enter short optional description for this device.

```
C4331#show crypto pki certificates CISCO_IDEVID_SUDI
Certificate
  Status: Available
  Certificate Serial Number (hex): 01E92BC3
  Certificate Usage: General Purpose
[SNIP]
```

```
C4331#show sdwan certificate serial
Chassis number: ISR4331/K9-FDO213905WF   Board ID serial number: 01E92BC3
```

*Release 16.6.1 or later is needed on ASR 1000

Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

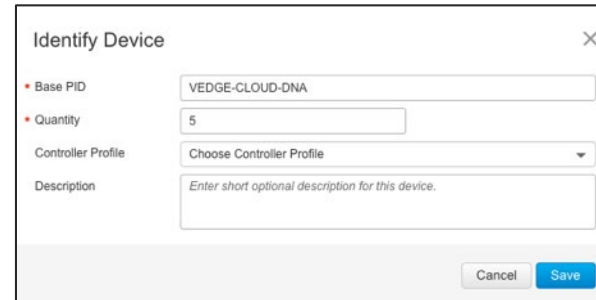
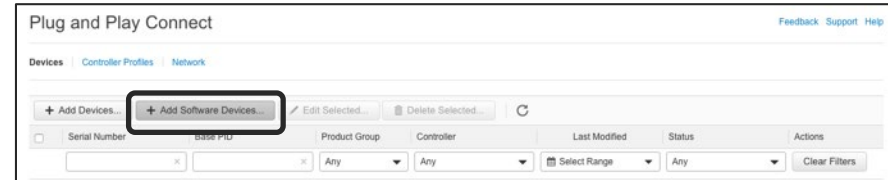
Step5

PnP Connect – Add Software Devices

Add Software Devices

Once the Controller Profile is created, you can add software devices into the Virtual Account and associate these to the newly-created profile

- Under the Devices tab, click on Add Software Devices
- Choose the Software Device you want to use with the correct PID:
 - vEdge Cloud => [VEDGE-CLOUD-DNA](#)
 - ISRv => [ISRv](#)
 - CSR1000v => [CSRv](#)

The screenshot shows the 'Identify Device' dialog box. It has a close button (X) in the top right corner. The form contains the following fields:

- 'Base PID' with a text input field containing 'VEDGE-CLOUD-DNA'.
- 'Quantity' with a text input field containing '5'.
- 'Controller Profile' with a dropdown menu showing 'Choose Controller Profile'.
- 'Description' with a text area containing the placeholder text 'Enter short optional description for this device.'.

At the bottom right, there are 'Cancel' and 'Save' buttons.

The number of devices you can add manually for the POC will be limited
After order, Cisco will populate the software devices to the Smart Account

Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Step6

Add Serial File to vManage

Add Serial File to vManage

Automatic way - Sync Smart Account

On vManage 18.3 or later:

- Click the 'Sync Smart Account' under Configuration → Devices
- Enter your Smart Account login information

The screenshot shows the Cisco vManage interface. The top navigation bar includes 'Cisco vManage' and 'CONFIGURATION | DEVICES'. The main content area is titled 'WAN Edge List' and 'Controllers'. A toolbar contains buttons for 'Change Mode', 'Upload WAN Edge List', 'Export Bootstrap Configuration', and 'Sync Smart Account'. The 'Sync Smart Account' button is highlighted with a red box. Below the toolbar is a table with columns: State, Device Model, Chassis Number, Serial No./Token, Hostname, and System IP. A dialog box titled 'Sync Smart Account' is open, showing the following fields:

- Organization Name: Cisco TME Lab Paris
- Username: [Yellow input field]
- Password: [Yellow input field with masked characters]
- Validate the uploaded vEdge List and send to controllers

At the bottom of the dialog are 'Sync' and 'Cancel' buttons.

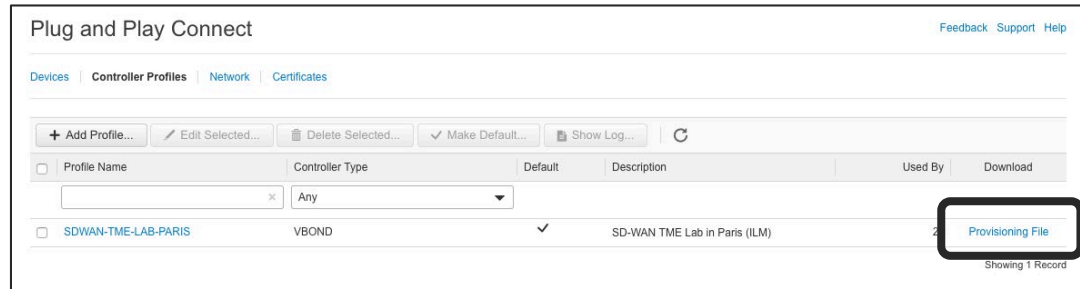
Add Serial File to vManage

Manually - Upload Serial File

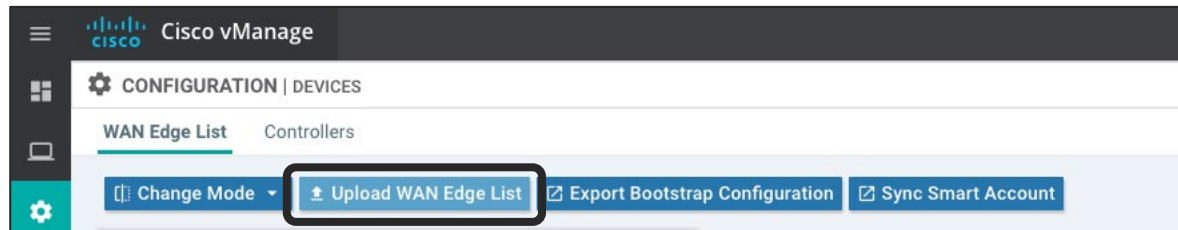
If using the Sync feature is not an option:

- Download the Serial File from the PnP Connect portal

Click on 'Provisioning File' under "Controller Profiles" - It will download the WAN Edge List



- Upload WAN Edge List under 'Configuration → Devices'



Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

To do before the POC

WAN Edge Image Upgrade

Choosing software version

- Always verify software compatibility and supported devices in release notes.
- As a best practice try to match vManage/vEdge and IOS XE software
(e.g. 19.2.097 with 16.12.1d and 19.2.099 with 16.12.1e)
- Use Suggested Release as much as possible

Compatibility Matrix

Table 8. Compatibility Matrix

Controllers	ENCS/ISR/ASR	ISRV	vEDGE
18.3.5	16.9.4	16.9.4 with NFVIS 3.9.1FC1 or NFVIS 3.9.2-FC4	17.2 or higher
18.4.0	16.10.1	16.10.1 with NFVIS 3.9.1FC1 or NFVIS 3.9.2-FC4	17.2 or higher
19.1.0	16.11.1a	16.11.1a with NFVIS 3.9.1FC1 or NFVIS 3.9.2-FC4	17.2 or higher
19.2.x	16.10.x 16.12.x	16.10.1 with NFVIS 3.9.1FC1 or NFVIS 3.9.2-FC4 16.11.1a with NFVIS 3.9.1FC1 or NFVIS 3.9.2-FC4	18.4 and 19.2

The image shows two side-by-side screenshots of a software release selection interface. Both screenshots feature a search bar at the top, followed by 'Expand All' and 'Collapse All' buttons. Below these are two expandable sections: 'Suggested Release' and 'Latest Release'. In the left screenshot, the 'Suggested Release' is '18.4.302' (marked with a star icon), and the 'Latest Release' is '19.2.097'. In the right screenshot, the 'Suggested Release' is '16.10.3a' (marked with a star icon), and the 'Latest Release' is '16.12.1d'. Below these are 'All Release' and 'Deferred Release' sections, each with a dropdown arrow.

vEdge Image Upgrade

- Download the Cisco vEdge Router Image (software.cisco.com)
- OPTION 1 - Install the new Cisco vEdge Image from CLI
- Configure the Cisco vEdge Router from ZTP / CLI / USB bootstrap
- OPTION 2 - Install the new Cisco vEdge Image from vManage

Cisco SD-WAN Getting Started documentation

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html#c_Software_Installation_and_Upgrade_for_vEdge_Routers_1369.xml

IOS XE Image Upgrade

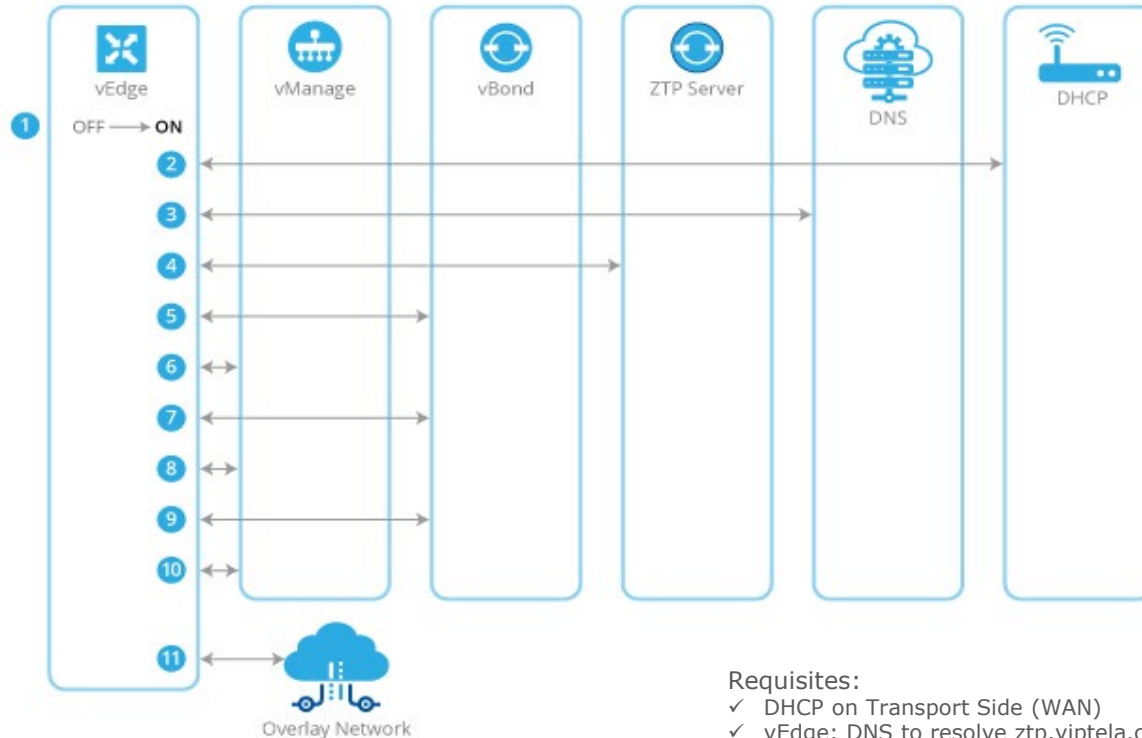
- Download the Cisco IOS XE SD-WAN Software (software.cisco.com)
- OPTION 1 - Install the Cisco IOS XE SD-WAN Software from CLI
 - In case of migration, get the certificate serial number for the SA/VA
- Configure the IOS XE Router from ZTP / CLI / USB bootstrap
- OPTION 2- Install the Cisco IOS XE SD-WAN Software from vManage
(only possible if already in IOS XE SD-WAN)

Cisco SD-WAN Getting Started documentation

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html#c_On_Site_Bootstrap_Process_for_SD_WAN_Devices_12488.xml

Configuration of WAN Edge – ZTP option

If pre-requisites are met, only step is to plug the device



Requisites:

- ✓ DHCP on Transport Side (WAN)
- ✓ vEdge: DNS to resolve ztp.viptela.com
- ✓ IOS XE: DNS to resolve devicehelper.cisco.com
- ✓ Device template created and attached to the device

Configuration of WAN Edge – USB option

- Create a device template
- Attach the template to the device
- Generate a Bootstrap in the Configuration → Devices page
- Boot the device with the bootstrap on a USB



Configuration of WAN Edge – CLI option

Minimum configuration:

- Assign Hostname / System IP / Site ID
- Configure Organisation Name
- Configure vBond address:
 - IP address or FQDN (configure DNS server)
- Configure a tunnel interface in VPN 0
- Add a default route in VPN 0
- Install root certificate chain if needed
- Commit and-quit

Cisco SD-WAN Getting Started documentation: [vEdge](#) / [IOS XE](#)

Configuration of Virtual WAN Edge

- Create a device template for virtual device and attach it to the Serial Number
- Generate a Bootstrap in the Configuration → Devices page

Bootstrap Option:

- Deploy the VM with the Bootstrap

CLI Option:

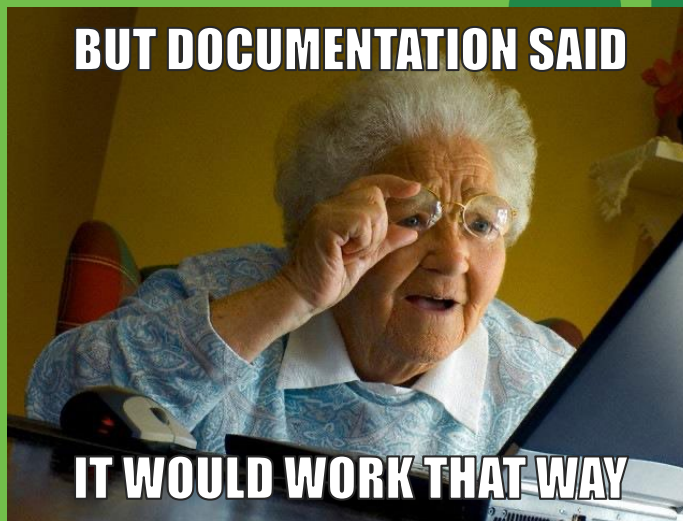
- Configure UUID and OTP on the virtual device - UUID and OTP can be found by generating cloud-init bootstrap
 - vEdge: request vedge-cloud activate chassis-number **UUID** token **OTP**
 - CSR1K: request platform software sdwan vedge_cloud activate chassis-number **UUID** token **OTP**
- Configure the virtual device from CLI - same commands as physical devices

Should you do a
SD-WAN POC?

Pre-requisites

Step by Step
POC deployment

Be ready to
troubleshoot

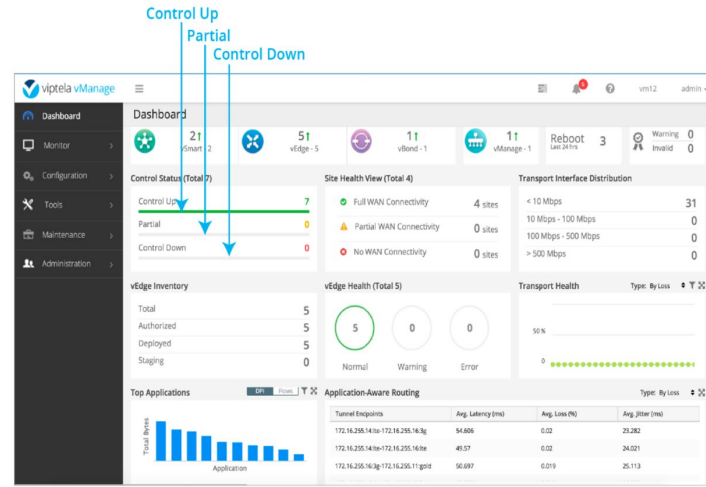


Troubleshooting Bring-up

Most common issues

Most common bring-up issues are related to:

- Incomplete WAN Edge configuration
- Firewall / NAT / Routing blocking control connections
- Wrong version in use
- Layer 1 issues (speed / duplex / vlan mismatch)



In consequence, Control Plane will show as Down or Partial:

- Down: Devices with no control plane connection to a vSmart controller
- Partial: Devices with some, but not all, operational control plane connections to vSmart controllers

Understanding Control Plane failures

2 main CLI commands to remember for Control Plane issues:

- `show control connections` → is the connection up/down/transient
- `show control connections-history` → why is it down?

Connectivity Issues

- DTLS connection failure
- TLOC disabled
- Transient conditions

Certificate Issues

- Device(s) not added
- Certificate revoked/invalidated
- Certificate Verification Failed
- Certificate verification failures

Verifying configuration

If no connection is attempted with controllers

- Verify control parameters
 - `show control local-properties`
- Verify there is a valid interface and route to controllers
 - `show interface vpn 0`
 - `show ip route vpn 0`

```
Gateway-VPC-Edge1# show control local-properties
personality vedge
sp-organization-name CLIVE-Demo
organization-name CLIVE-Demo
certificate-status Installed
root-ca-chain-status Installed
certificate-validity Valid
certificate-not-valid-before Aug 19 21:16:54 2017 GMT
certificate-not-valid-after Aug 17 21:16:54 2027 GMT
dns-name 52.5.226.23
site-id 8001
domain-id 1
protocol dtls
tls-port 0
system-ip 5.5.5.15
chassis-num/unique-id 5a5b5c5f-a91b-12c4-b2df-b7342c0b20d3
serial-num 878CAAF9
token Invalid
keygen-interval 1:00:00:00
retry-interval 0:00:00:19
no-activity-exp-interval 0:00:00:12
dns-cache-ttl 0:00:02:00
port-hopped TRUE
time-since-last-port-hop 37:01:20:07
```

DTLS connection failure

Means there was a connectivity issue

Probable causes

- NH not reachable
- Def-GW not installed in RIB
- DTLS port not open in the Controllers

Debugging steps:

- PING Def-GW
- Ping vBond if ICMP is allowed on the vBond
- Traceroute to vBond DNS Address

When you have a DTLS Connection failure, you may see the following in `'show control connections-history'`

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER		PEER			LOCAL COLOR	STATE	LOCAL ERROR	REMOTE ERROR	REPEAT COUNT	REPEAT DOWNTIME
					PRIVATE IP	PORT	PRIVATE IP	PORT	PUBLIC IP						
vbond	dtls	-	0	0	1.3.25.25	12346	1.3.25.25	12346	mpls	connect	DCONFAIL	NOERR	1	2016-09-22T10:49:04-0700	
vbond	dtls	-	0	0	1.3.25.25	12346	1.3.25.25	12346	gold	connect	DCONFAIL	NOERR	1	2016-09-22T10:49:03-0700	

Organization-name Mismatch

- For a given a overlay, the Org. Name has to match across all the controllers and vEdges so that control connections can come up.
- If not, you will see *“Certificate Org. name mismatch”* as seen below in the “show control connections” output.

PEER TYPE	PEER PROTOCOL	PEER SYSTEM	SITE ID	DOMAIN ID	PEER		PEER		LOCAL COLOR	STATE	LOCAL	REMOTE	REPEAT	DOWNTIME
					PRIVATE IP	PORT	PUBLIC IP	PORT			ERROR	ERROR	COUNT	
vbond	dtls	-	0	0	1.3.25.25	12346	1.3.25.25	12346	mpls	tear_down	CTORGNMMIS	NOERR	19	2016-10-06T00:39:37+0000
vbond	dtls	-	0	0	1.3.25.25	12346	1.3.25.25	12346	gold	tear_down	CTORGNMMIS	NOERR	28	2016-10-06T10:39:20-0000

→ Certificate Org name mismatch

When version is too old

- If vManage version is too old, it will not recognize the hardware that was supported in newer versions

Device type will show incorrect values for those Serial Numbers, which blocks from attaching a template.

- If device version is too old, it might not be able to connect to vManage
 - e.g. Controllers 19.2.x and vEdge 16.2, control connection will be established to vBond and vSmart, but not to vManage (error: VM_TMO - Peer vManage Timed out.)

- If direct upgrade is not accessible, you can copy the image from your PC to vSmart and then from vSmart to vEdge using the DTLS connection

```
vSmart:~$ scp ./<local-image-path> admin@<system-ip>:./<remote-image-path>
```

- e.g. Controllers 19.2.x and IOS XE 16.9.4, control connection may fail with CRTVERFL: Certificate Verification Failure. This is due to the root CA being different in new versions.

- If direct upgrade is not accessible, copy vBond root-cert-chain (usr/share/viptela/root-ca.crt) to the router via SCP or TCL script and install it

```
tclsh
puts [open "bootflash:root2.crt" w+] {
<paste vBond root-cert here>
}
tclquit
request platform software sdwan root-cert-chain install bootflash:root2.crt
```

If Layer 1 issue is suspected

Verify interface Drops and Errors



What if only Data Plane is down ?

Verify TLOC propagation

- `show omp tlocs`

➤ Missing TLOCs could be a topology issue

Verify device to device IPSEC connectivity

- `show ipsec inbound-connections`
- `show ipsec outbound-connections`

➤ No connectivity could be IPSEC flow being blocked

➤ No outbound connection could be a missing route to destination

```
DataCenter# show omp tlocs
```

ADDRESS						PSEUDO		PUBLIC		PRIVATE	PUBLIC	PRIVATE	PRIVATE	BFD		
FAMILY	TLOC	IP	COLOR	ENCAP	FROM	PEER	STATUS	KEY	PUBLIC	IP	PRIVATE	IPV6	IPV6	PORT	STATUS	
ipv4	1.1.1.4	biz-internet	ipsec	1.1.1.3	C,I,R	1		34.192.241.51	12346	10.0.1.32	12346	::	0	::	0	up
				1.1.1.10	C,R	1		34.192.241.51	12346	10.0.1.32	12346	::	0	::	0	up
	1.1.1.4	public-internet	ipsec	1.1.1.3	C,I,R	1		34.199.146.200	12346	10.0.3.232	12346	::	0	::	0	up
				1.1.1.10	C,R	1		34.199.146.200	12346	10.0.3.232	12346	::	0	::	0	up

Documentation for Troubleshooting

- BRKRST-2093 – Next-Gen SD-WAN (Viptela) Deployment, Monitoring, and Troubleshooting

<https://www.ciscolive.com/global/on-demand-library.html?search=BRKRST-2093#/>

- Control Plane Troubleshooting (details on error codes)

<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214509-troubleshoot-control-connections.html>

- Data Plane Troubleshooting

<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/214510-troubleshoot-bidirectional-forwarding-de.html>

Should you do a
SD-WAN POC?

Pre-requisites

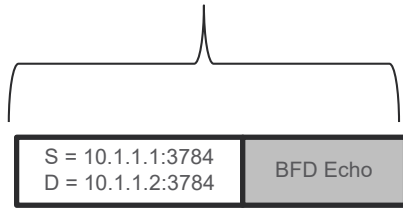
Step by Step
POC deployment

Tuning for POC!

BFD Tuning

Bi-directional Forwarding Detection (BFD)

- Utilizes UDP port 3784
- Measures Loss, Latency and Jitter
- Each BFD packet is ~100 bytes



Hello-Interval

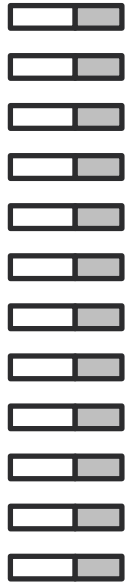
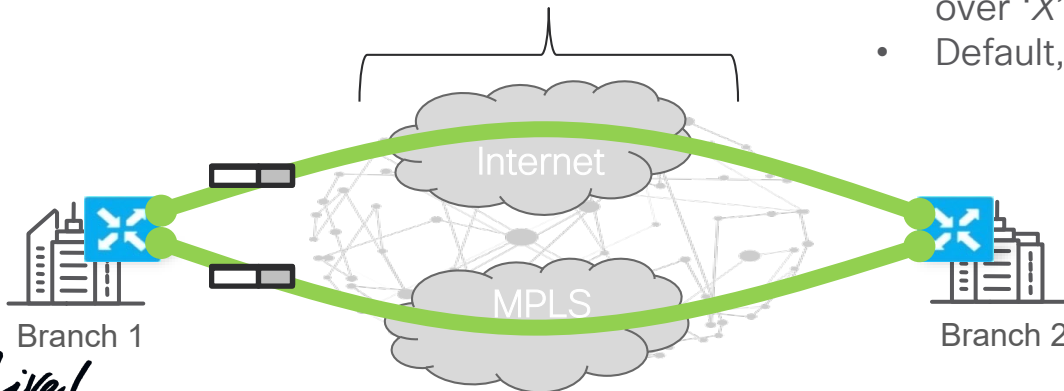
- Default, 1 BFD probe per second

Multiplier

- Average Loss, Latency and Jitter over 'X' Poll-Intervals
- Default, 6 poll-intervals

Poll-Interval

- Average Loss, Latency and Jitter over 'X' period
- Default, 600 seconds

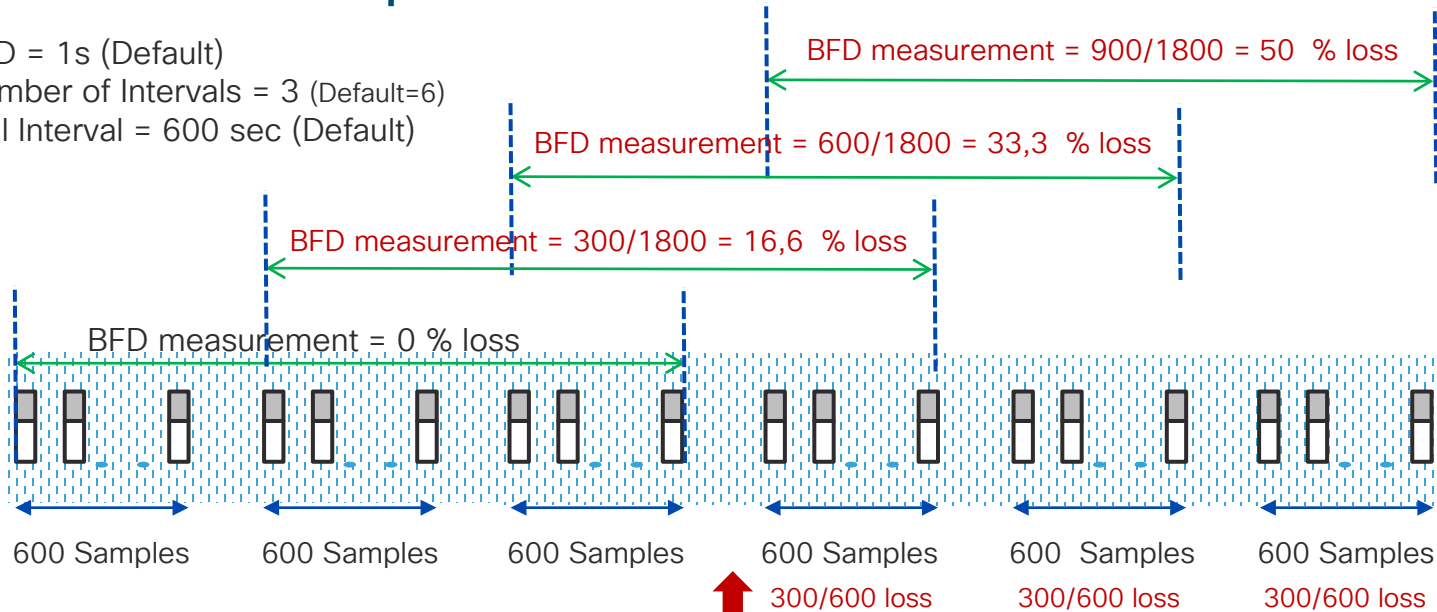


Rolling
Average

Loss: 1%
Latency: 10ms
Jitter: 5ms

BFD Example

BFD = 1s (Default)
 Number of Intervals = 3 (Default=6)
 Poll Interval = 600 sec (Default)



Convergence after
30 minutes
 (3 intervals)

AAR Policy:
 Change path if SLA is not met:
 20 % loss
 100 ms latency
 100 ms jitter



Reroute after
20 minutes
 (2 intervals)

BFD Example

Back to Default Values

BFD = 1s
Number of Intervals = 3
Poll Interval = 600 sec
Reroute after
20 minutes
(2 intervals)
Convergence after
30 minutes
(3 intervals)



BFD = 1s
Number of Intervals = 6
Poll Interval = 600 sec
Reroute after
30 minutes
(3 intervals)
Convergence after
60 minutes
(6 intervals)

AAR Policy:
Change path if SLA is not met:
20 % loss
100 ms latency
100 ms jitter
50% loss introduced

BFD Example

Back to Default Values

BFD = 1s
Number of Intervals = 6
Poll Interval = 600 sec

Reroute after
30 minutes
(3 intervals)

Convergence after
60 minutes
(6 intervals)

Do we want this ?

In Production, YES!
It avoids flapping of flows

In POC, NO!
Our time is limited

AAR Policy:
Change path if SLA is not met:
20 % loss
100 ms latency
100 ms jitter
50% loss introduced

BFD Recommendations

Aggressive (POC):

- Hello Interval: 1 second (Default)
- Multiplier: 2 intervals
- Poll Interval: 4 seconds

Max **8 seconds** brownout detection!

Moderate:

- Hello Interval: 1 second (Default)
- Multiplier: 3 intervals
- Poll Interval: 180 seconds

Max **9 minutes** brownout detection!

Conservative:

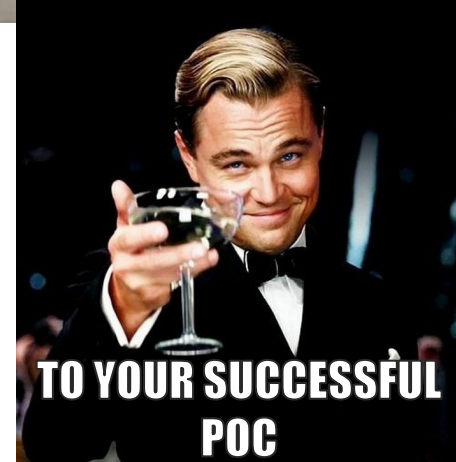
- Hello Interval: 1 second (Default)
- Multiplier: 6 intervals (Default)
- Poll Interval: 10 minutes (Default)

Max **60 minutes** brownout detection!

Note:

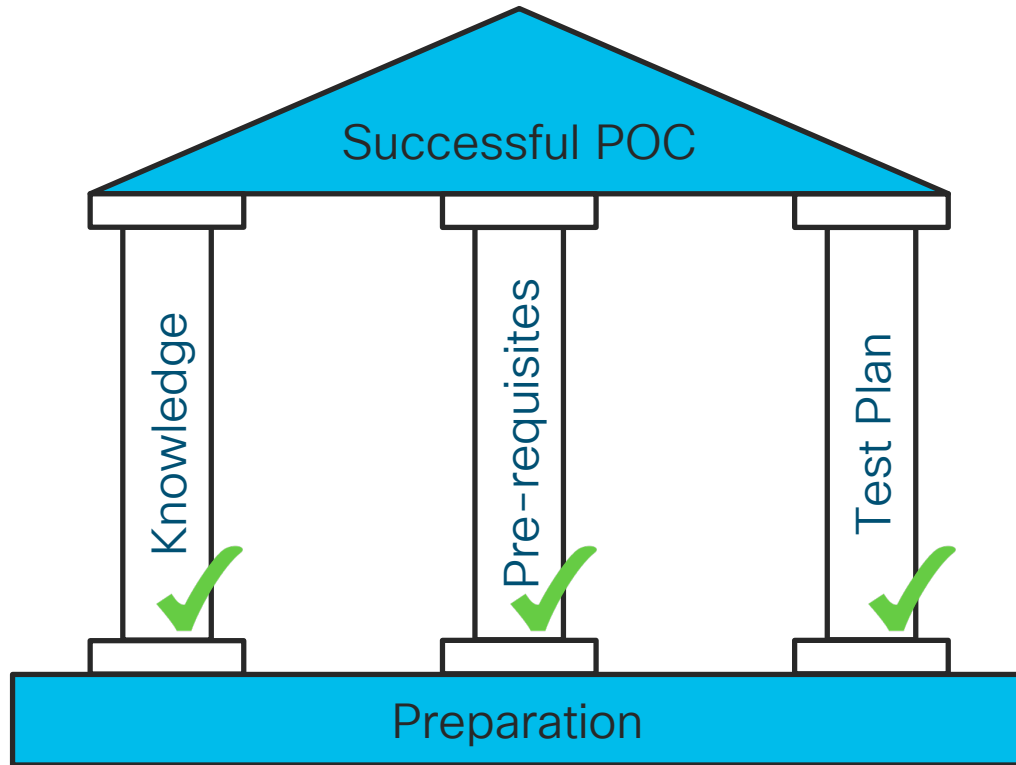
- ✓ Tuning is good for POC. For production, keep the default values unless you have specific requirements.
- ✓ You can lower the tunnel multiplier to detect tunnel down conditions (default is 7 consecutive missed BFDs).
- ✓ You can reduce Hello Interval to reach sub second failovers.
- ✓ Enable the OMP Backup Path feature for pre-calculated backup path
- ✓ WAN Edge appliances are scale tested based on default values. Tuning BFD parameters too low will increase the CPU burden on the appliance and, hence, lower scalability.

You're DONE!

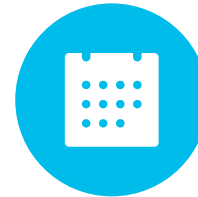


Conclusion

Take Aways



Use dcloud and virtual labs



Be Organised



Do BFD Tuning

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Thank you





You make **possible**