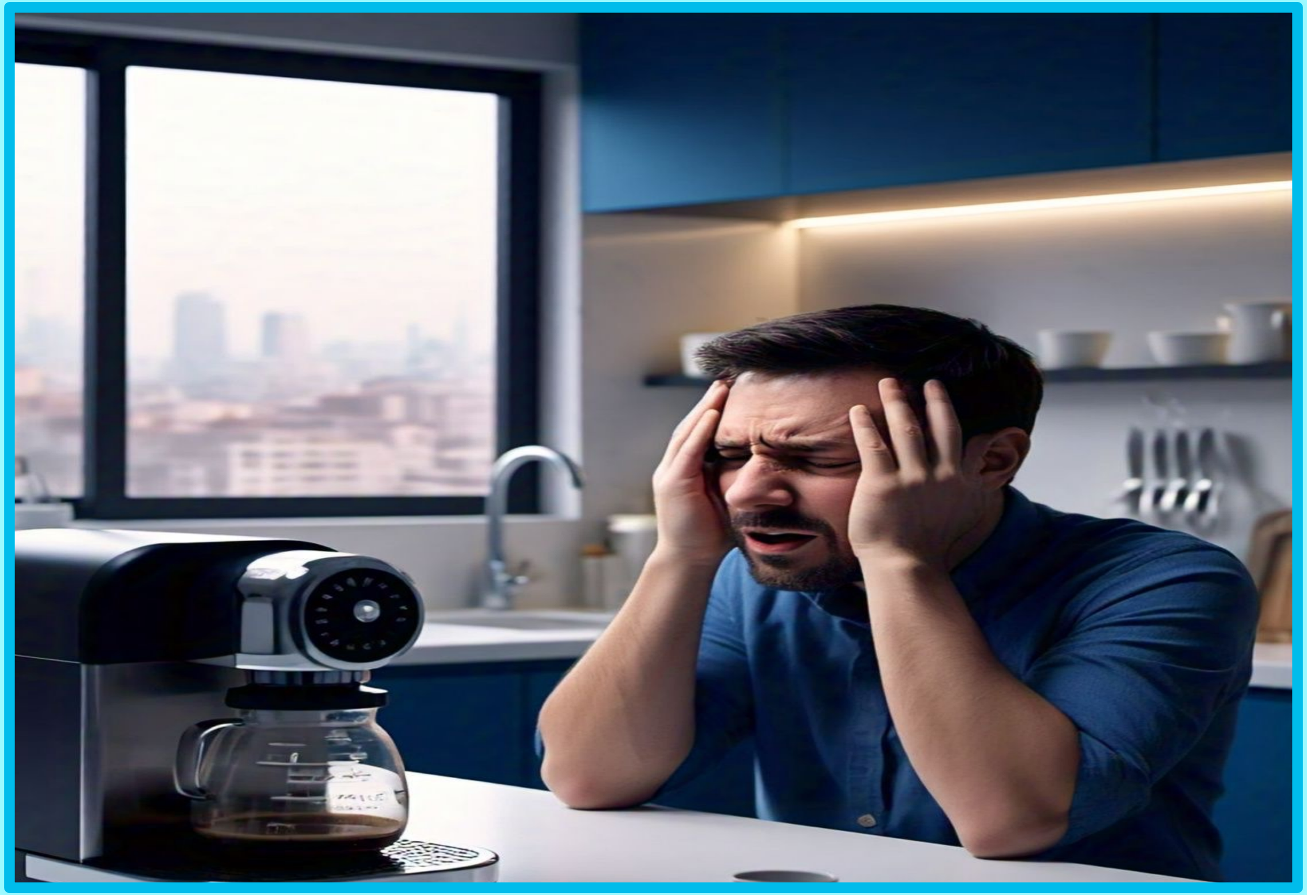
Expedite your Troubleshooting with SD-WAN Manager Tools

Uma Sankar Mohanty
Software Engineering Technical Leader

BRKTRS-2595

Agenda

- The WW(What & Why) of SD-WAN
- Monitoring/Troubleshooting Challenges
- SD-WAN Manager Tools
  - Speed Test
  - Packet Capture
  - Upload admin-tech & TAC case
  - Underlay Measurement and Tracing Service
  - Network Wide Path Insight(NWPI)
- Build your own API Workflow
- Key-Takeaways



Courtesy : Google Images

The WW(What & Why) of SD-WAN

Session Objective :

This Session Focuses on :

- Brief Overview of Cisco SDWAN.
- The session covers a whole package of tools that comes with the SD-WAN Manager which can help to expedite our troubleshooting approach.
- We will also touch upon how effectively we can use the rich set of SD-WAN Manager API's and design workflows to cater to our needs.

By the end, I hope everyone in this room gets a better understanding of these tools and utilize them in your troubleshooting approach to resolve issues much faster than the traditional methods.

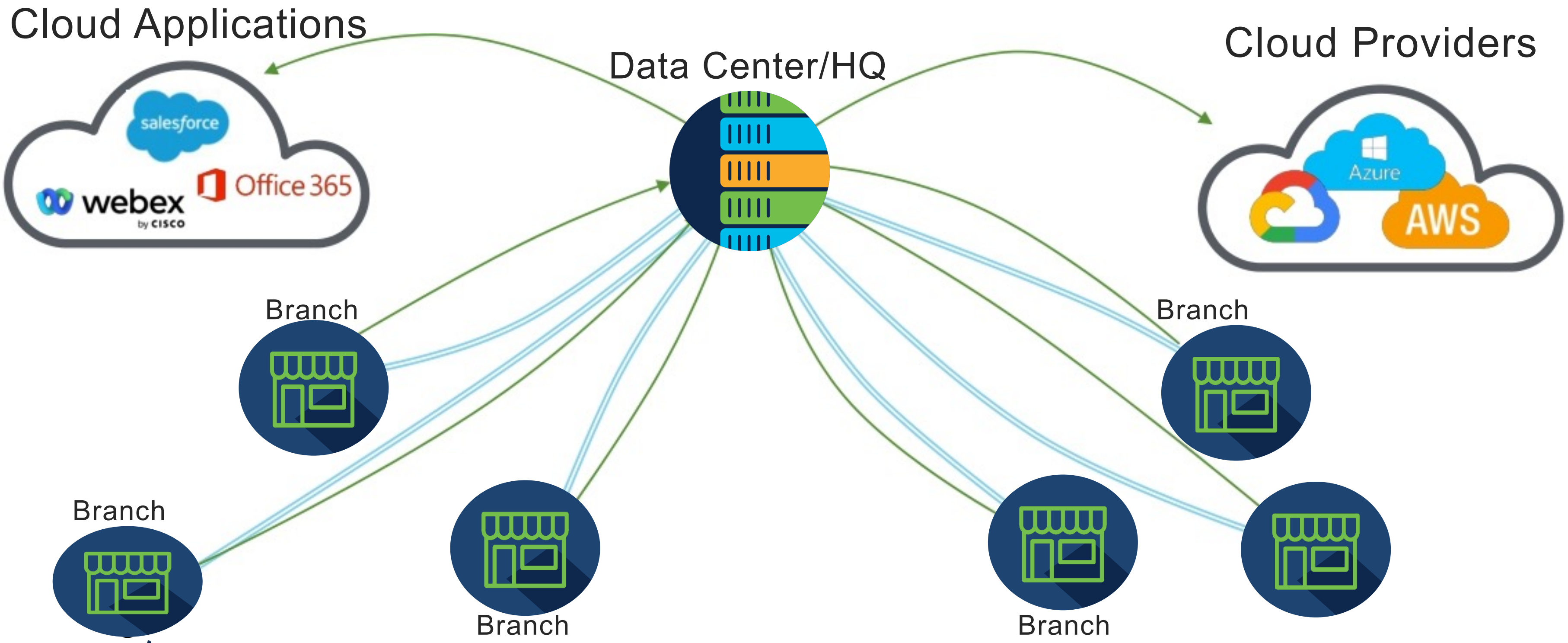
Session Non-Objective :

- We will not cover any of the installation aspects of these components.
- We will not focus on SD-WAN Analytics.

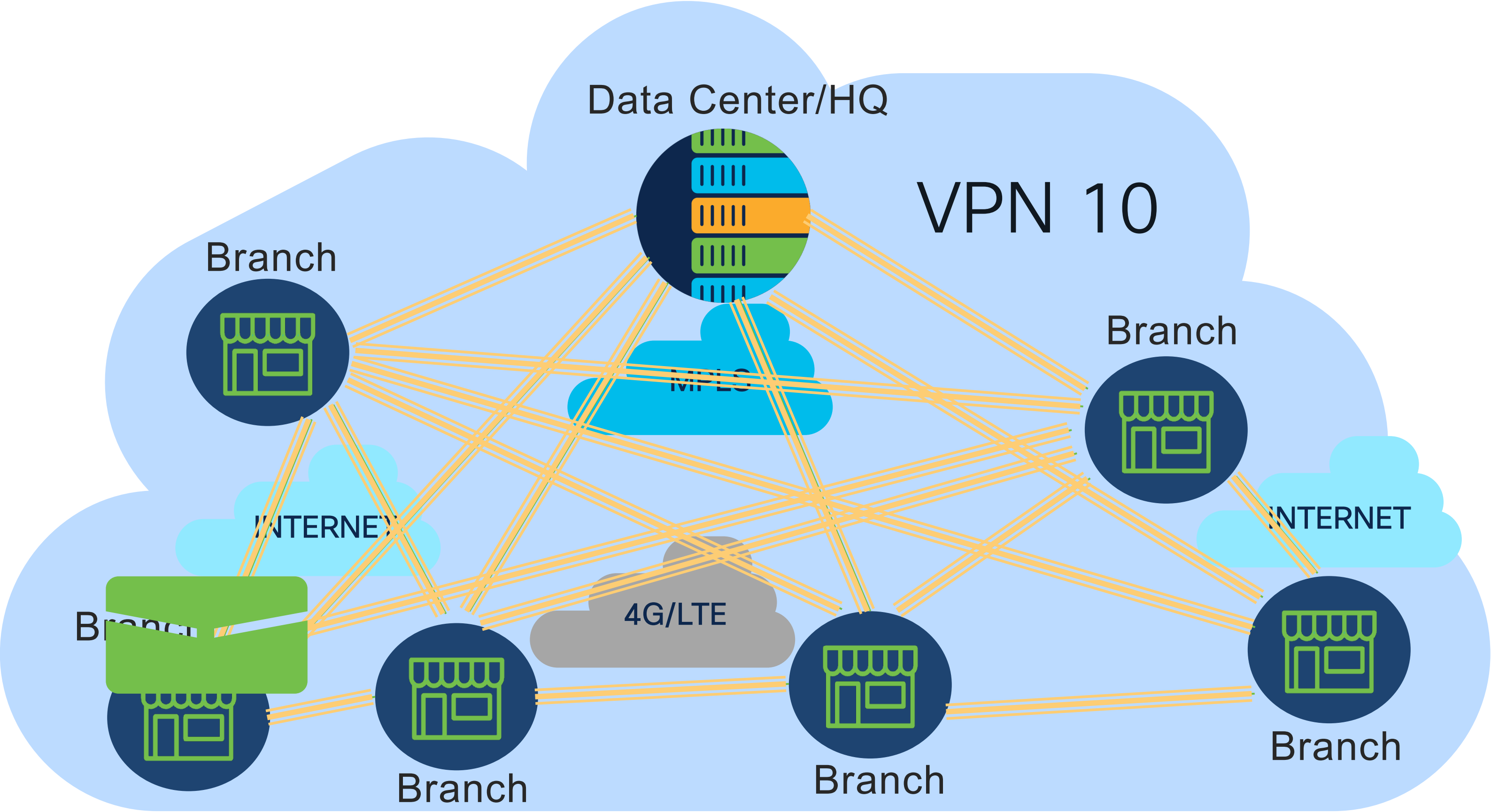
Why SD-WAN?

The Hardware Based WAN of Yesterday

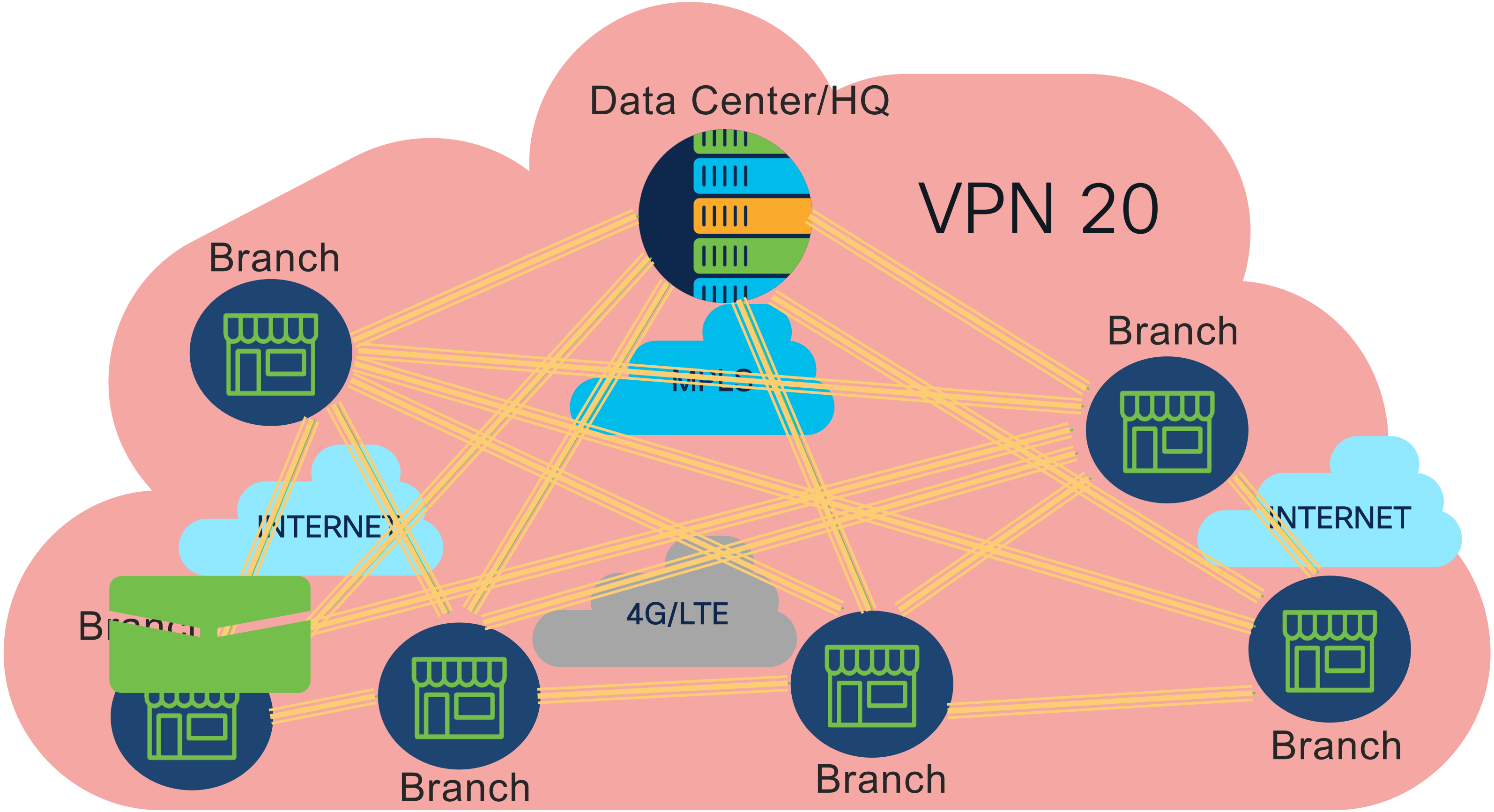
Doesn’t Keep up with the Needs of Today



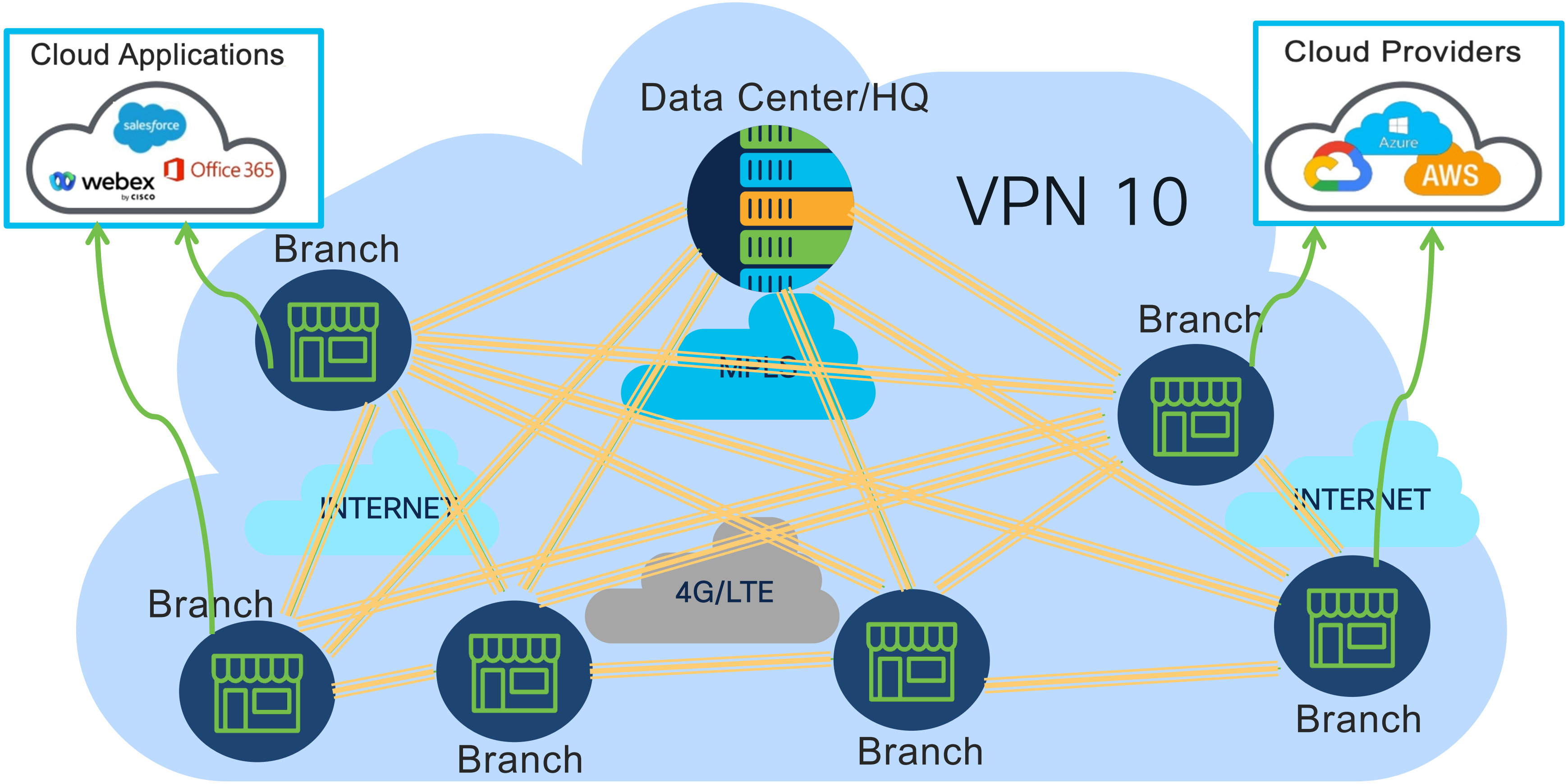
Cisco SD-WAN: Software Approach



Cisco SD-WAN: Software Approach



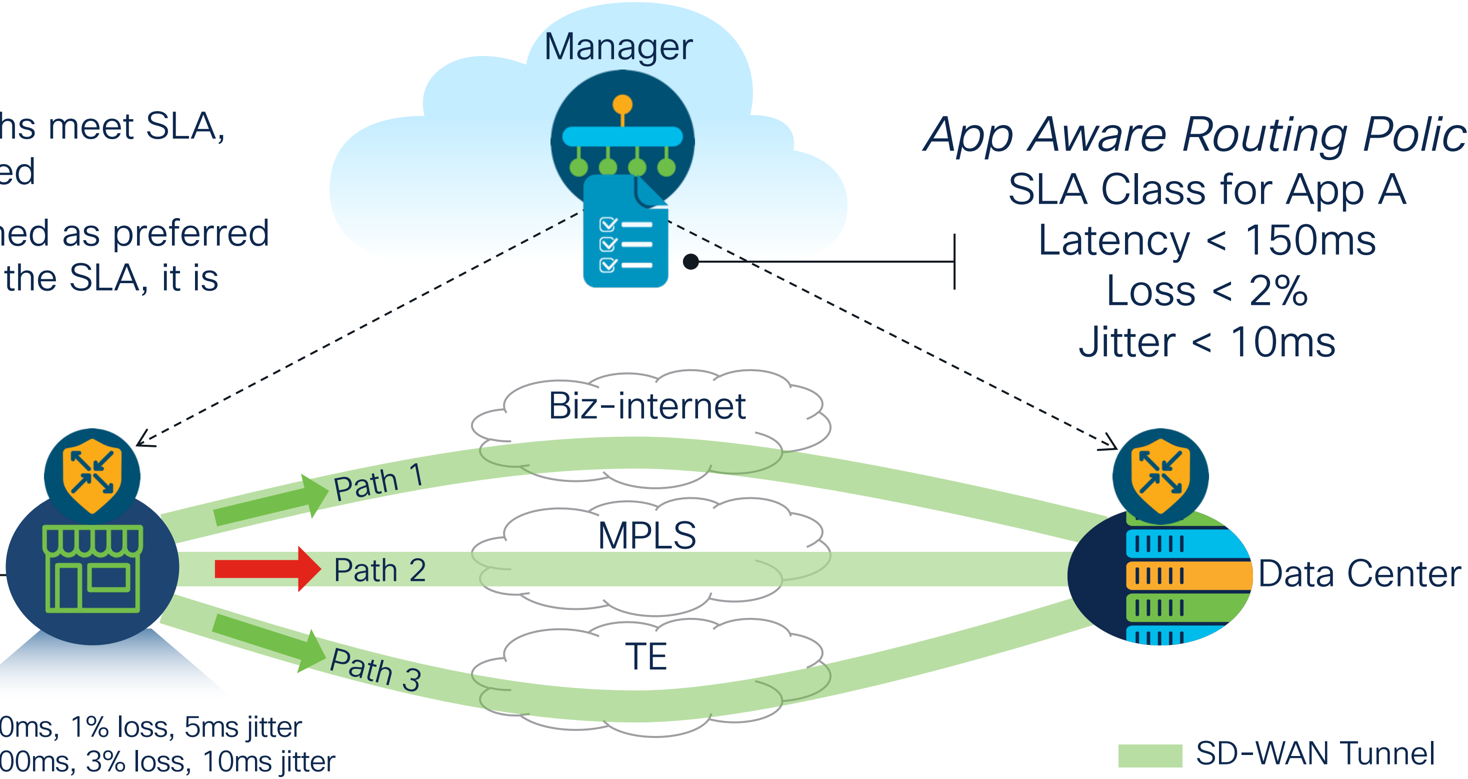
Cisco SD-WAN: Software Approach



Cisco SD-WAN: Software Approach

Application Aware Routing

- If multiple paths meet SLA, traffic is hashed
- If path is defined as preferred AND it meets the SLA, it is chosen



App Aware Routing Policy

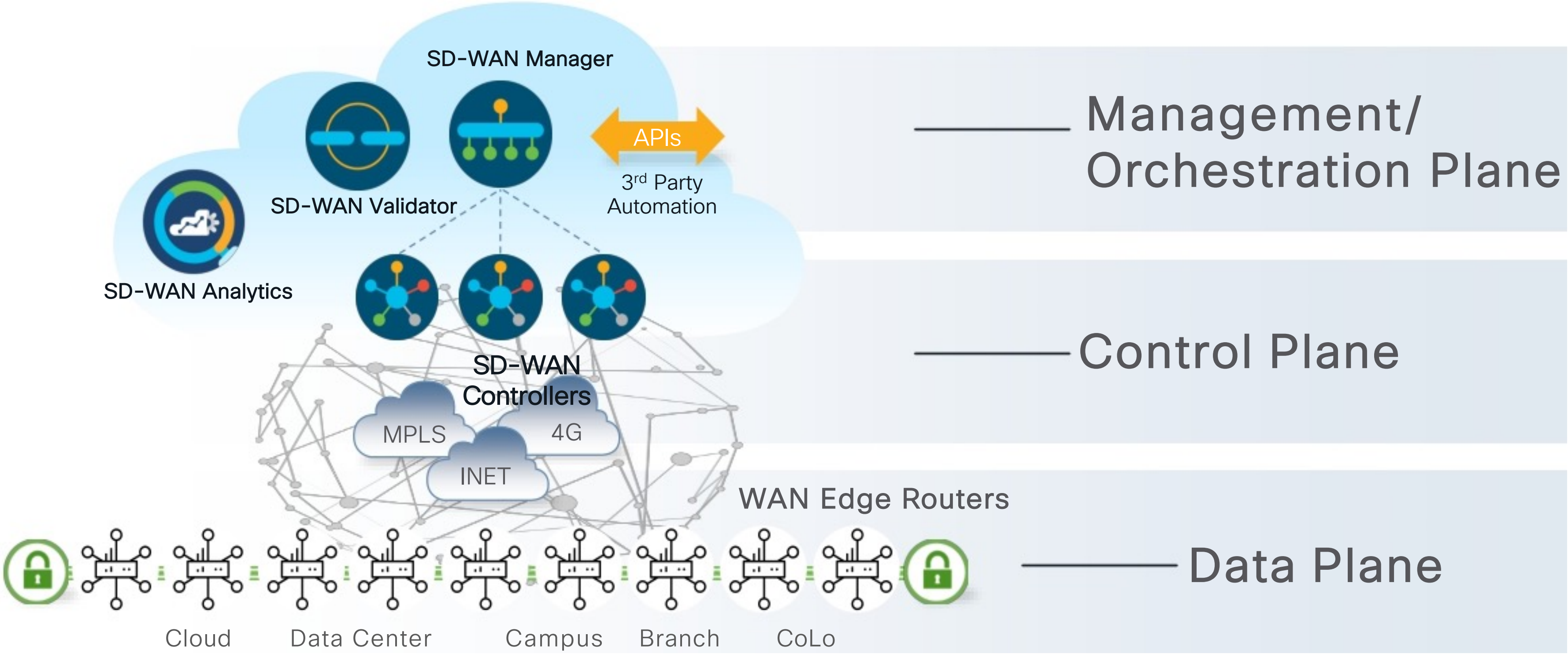
SLA Class for App A
Latency < 150ms
Loss < 2%
Jitter < 10ms

Path1: 10ms, 1% loss, 5ms jitter
Path2: 200ms, 3% loss, 10ms jitter
Path3: 140ms, 1% loss, 10ms jitter

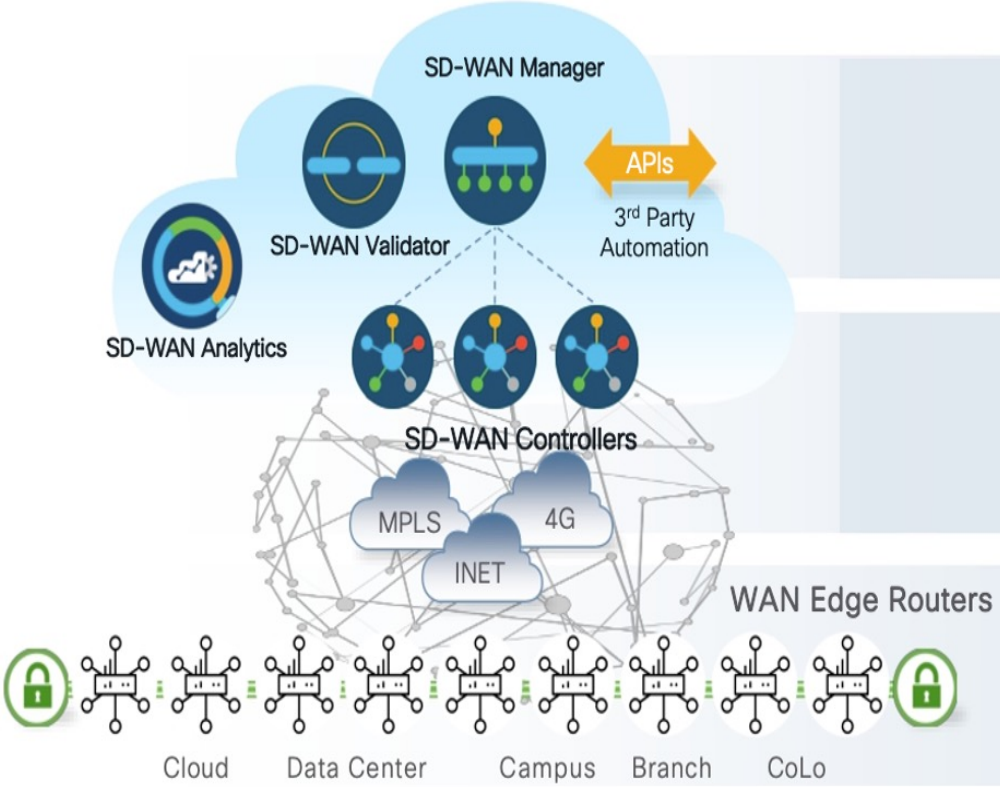
What is SD-WAN?

Solution Architecture

Cisco SD-WAN Solution Overview



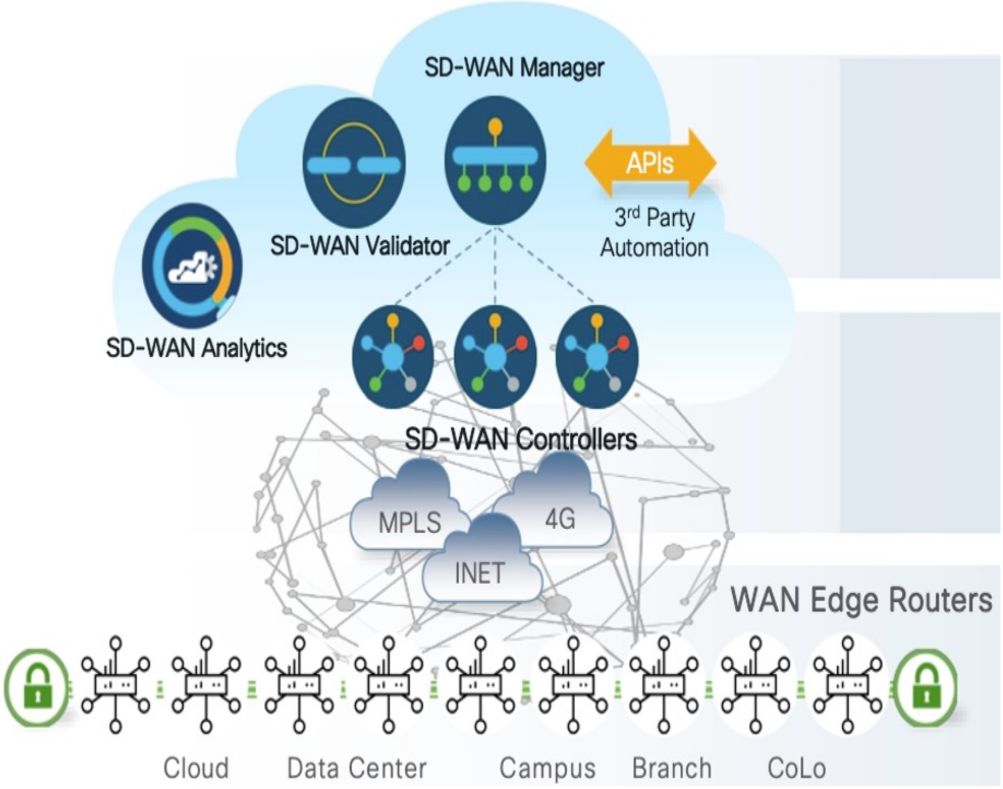
Cisco SD-WAN Solution Elements



Management Plane

- Single pane of glass for Day0, Day1 and Day2 operations
- Multitenant with web scale
- Centralized provisioning
- Policies and Templates
- **Troubleshooting and Monitoring**
- Software upgrades
- GUI with RBAC
- **Programmatic interfaces (REST, NETCONF)**
- Highly resilient

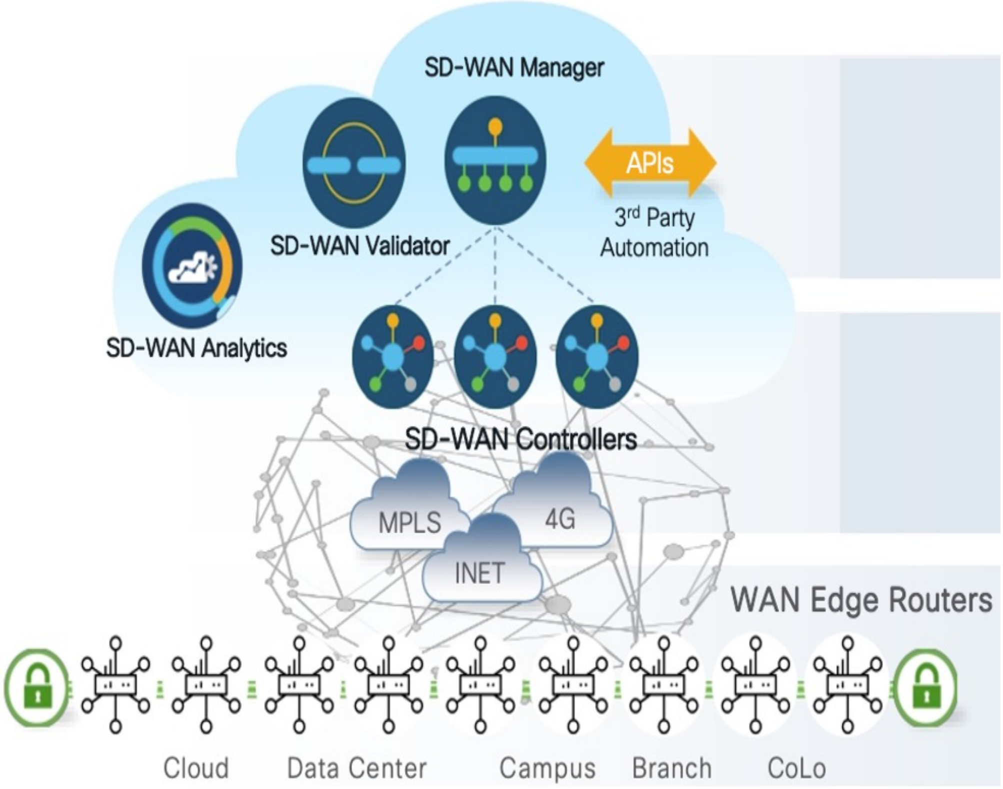
Cisco SD-WAN Solution Elements



Orchestration Plane

- First point of authentication (white-list model)
- Distributes list of Controllers/ Manager to all WAN Edge routers
- Facilitates NAT traversal
- Requires public IP Address. [could sit behind 1:1 NAT]
- Highly resilient

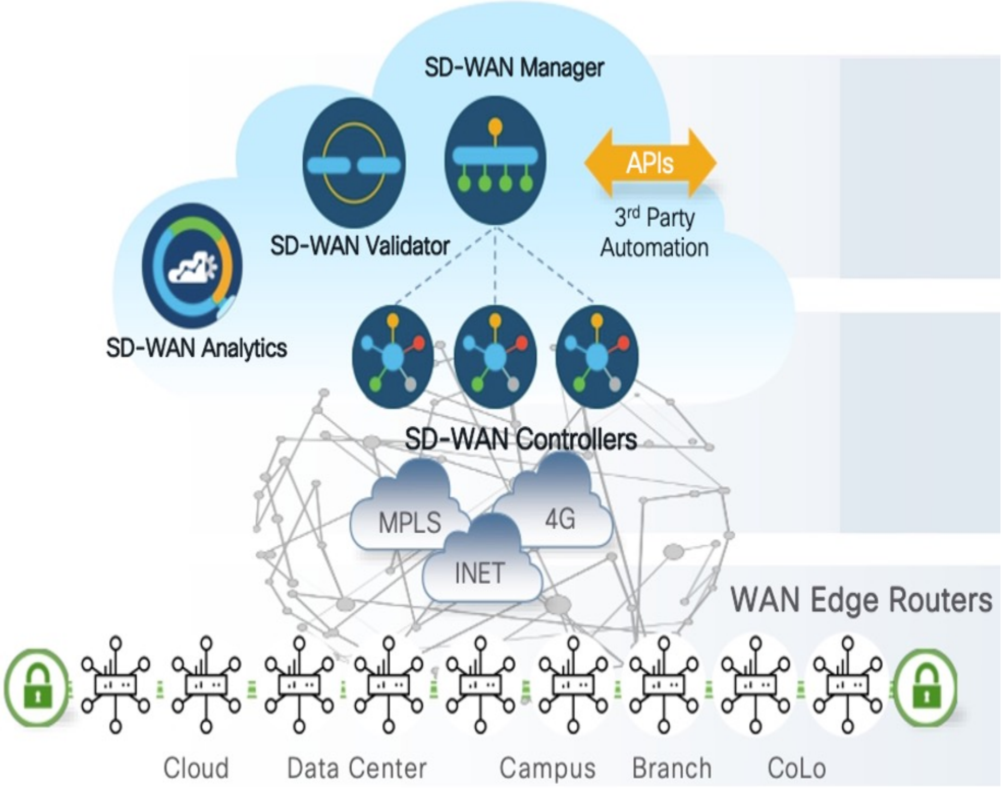
Cisco SD-WAN Solution Elements



Control Plane

- Facilitates fabric discovery
- Dissimilates control plane information between WAN Edge Routers
- Distributes data plane and app-aware routing policies to the WAN Edge routers
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity & highly resilient

Cisco SD-WAN Solution Elements

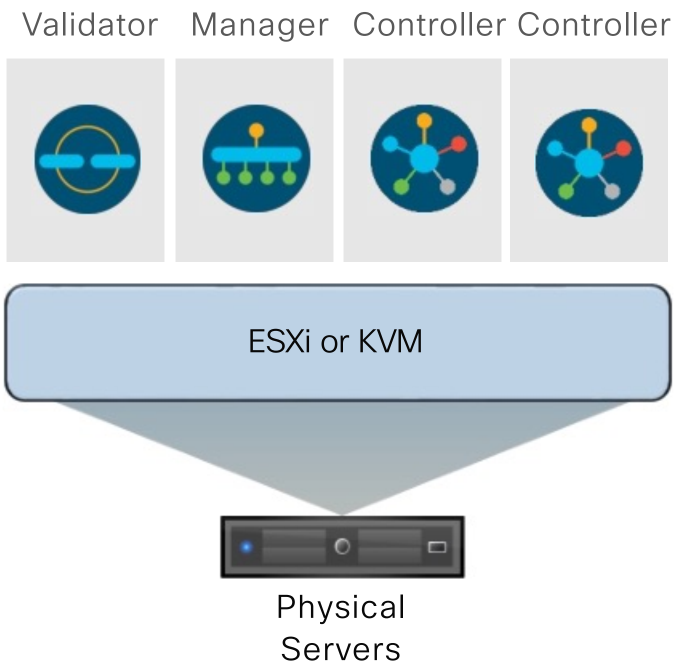


Data Plane

- WAN edge router
- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routingprotocols like OSPF, BGP, and EIGRP
- Support Zero Touch Deployment
- Physical or Virtual form factor(100Mb, 1Gb, 10Gb,40Gb, 100Gb)

Controller Deployment Methodology

On-Premise

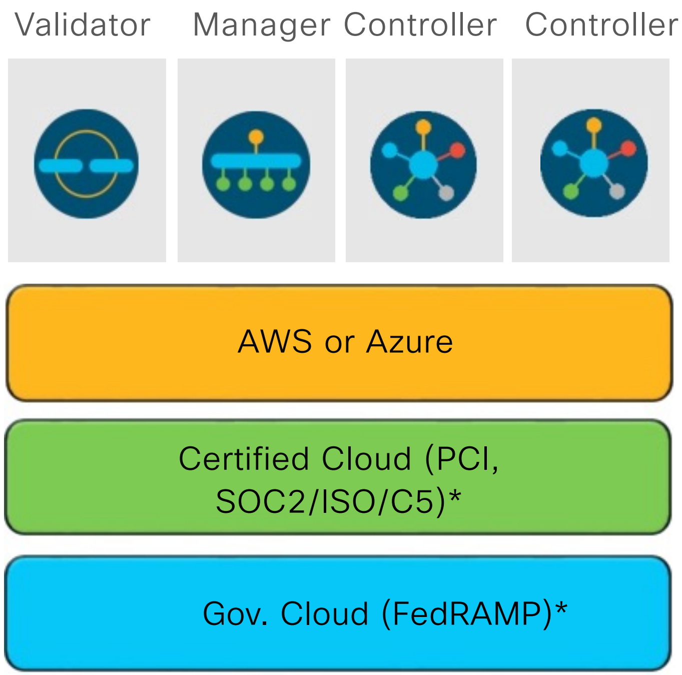


Validator Manager Controller Controller

ESXi or KVM

Physical Servers

Cisco or MSP/Customer Hosted



Validator Manager Controller Controller

AWS or Azure

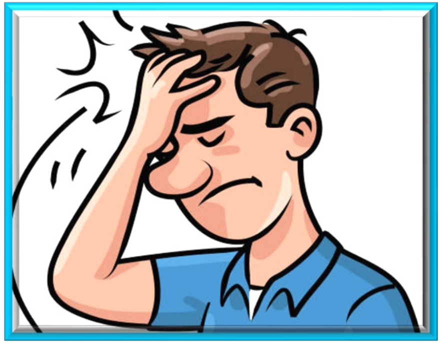
Certified Cloud (PCI, SOC2/ISO/C5)*

Gov. Cloud (FedRAMP)*

*Only Cisco hosted

Monitoring/Troubleshooting Challenges

Know your Tools



What shall I look into ?

Critical/Intermittent issue – Less time

Automation

SDWAN Manager Tools

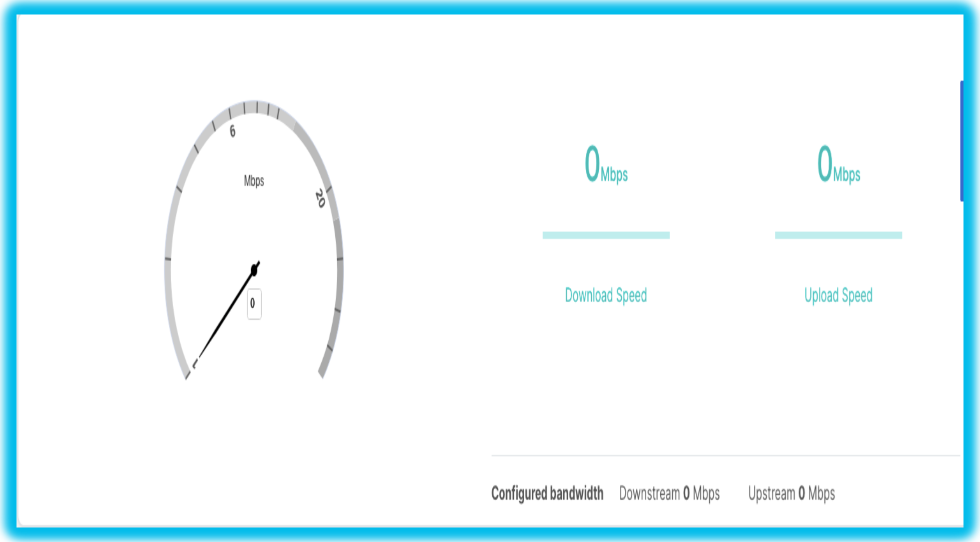
Speed Test

Speed Test : Introduction

- Used to evaluate the WAN interface’s bandwidth against a remote SDWAN edge or an iPerf3 server.

- Supported on cEdge since 17.3 & later releases.

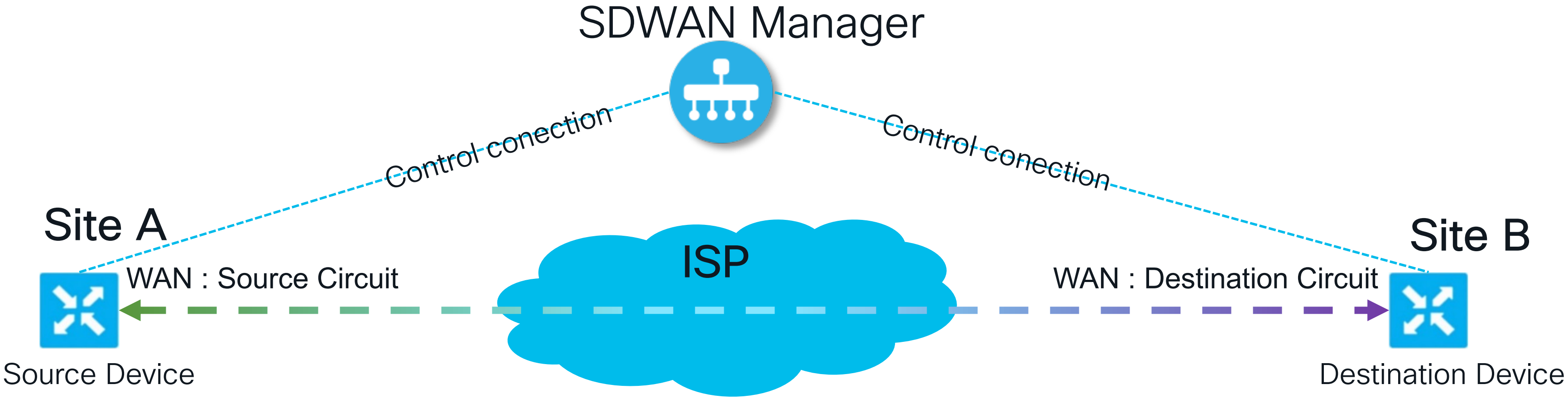
- Two types of Speed Test
  - Site to Site Speed Test
  - Internet Speed Test



Configured bandwidth Downstream **0** Mbps Upstream **0** Mbps

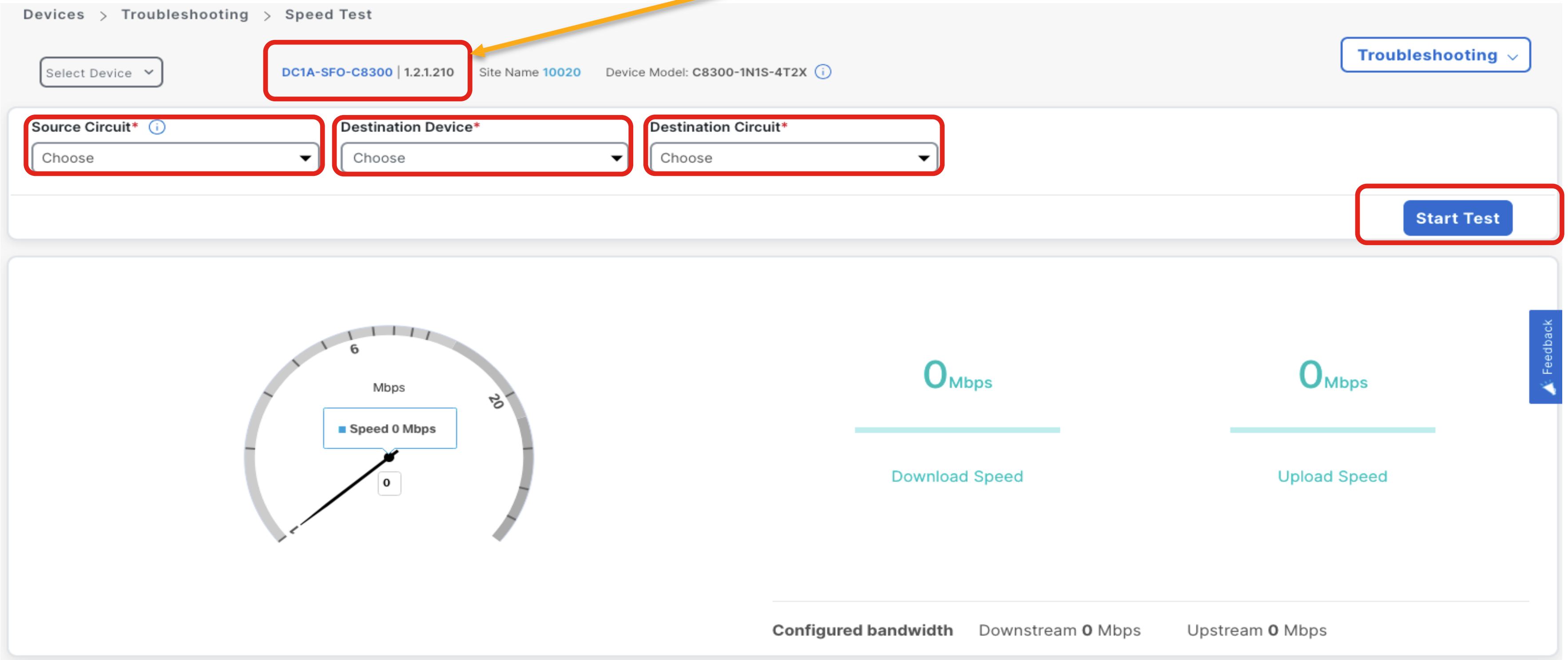
Site to Site Speed Test

Used for testing speed from the specified WAN interfaces to a remote SDWAN site's specified WAN interface.



Site to Site Speed Test

Device on which Speed Test needs to be performed



Devices > Troubleshooting > Speed Test

Select Device

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Source Circuit*: Choose

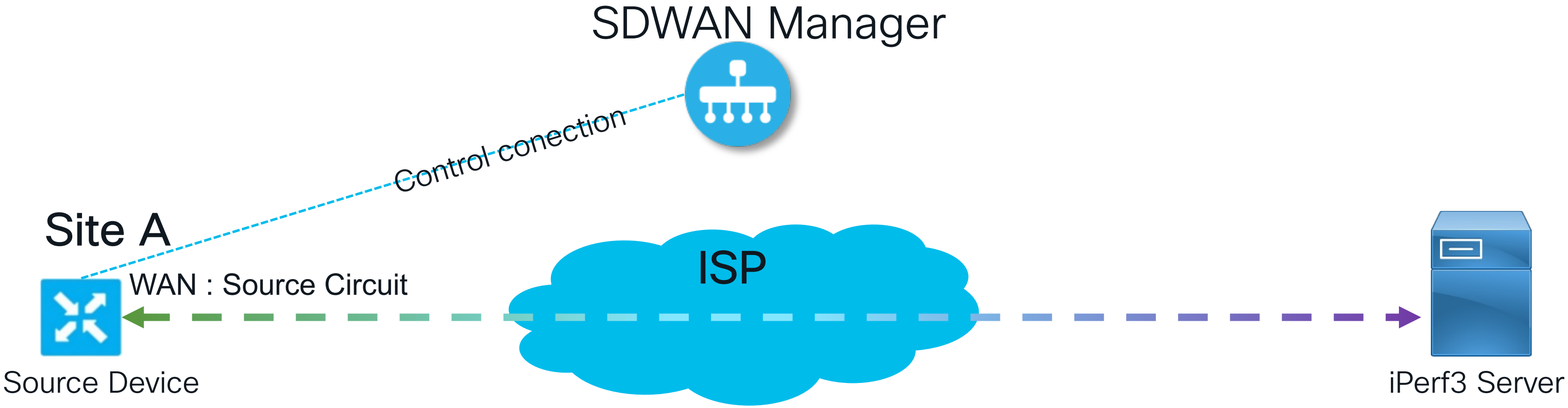
Destination Device*: Choose

Destination Circuit*: Choose

Configured bandwidth Downstream 0 Mbps Upstream 0 Mbps

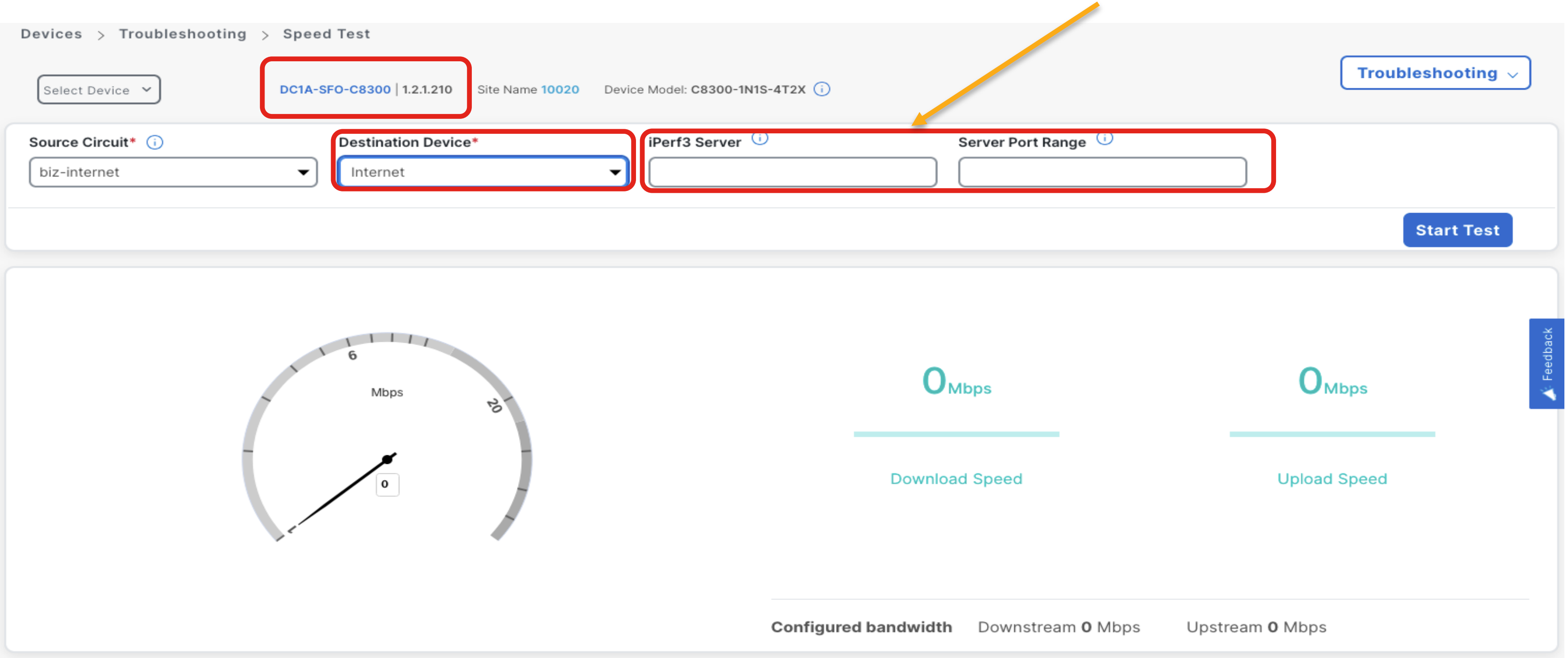
Internet Speed Test

Used for testing speed from the specified WAN interfaces against a public iPerf3 server.



Internet Speed Test

- iPerf3 server and Port fields provided beyond 20.10/17.10 release.
- Will use hardcoded iPerf3 server list if left blank



Devices > Troubleshooting > Speed Test

Select Device

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Source Circuit*: biz-internet

Destination Device*: Internet

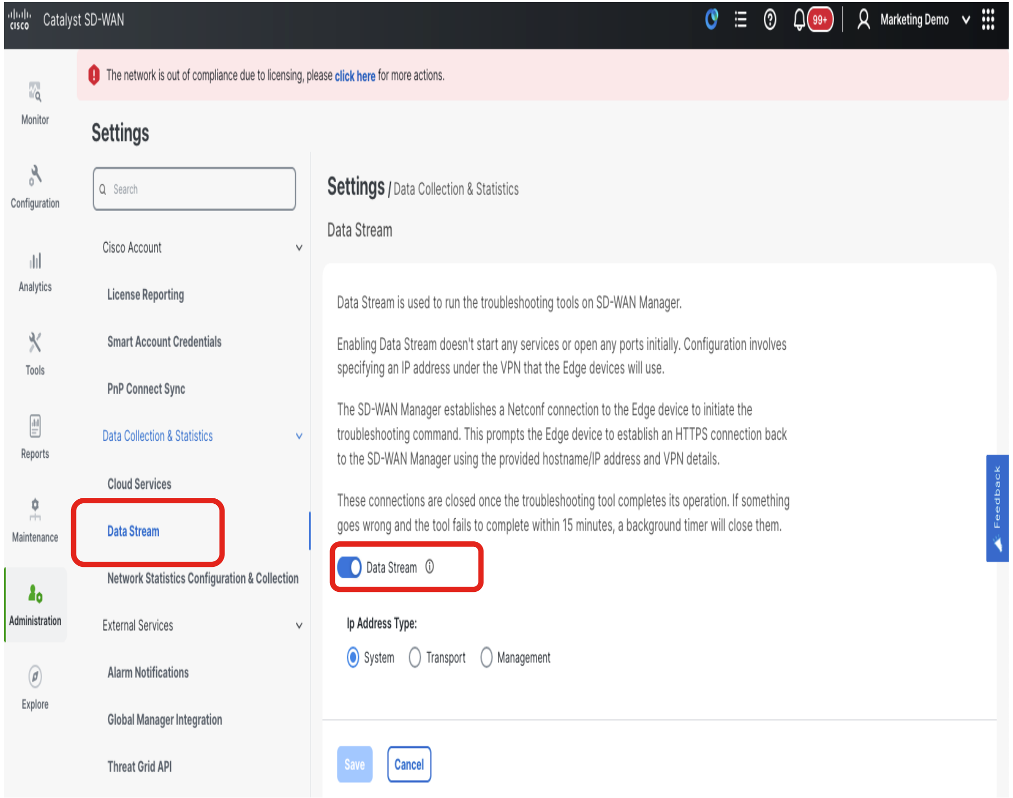
iPerf3 Server:

Server Port Range:

Configured bandwidth Downstream 0 Mbps Upstream 0 Mbps

Prerequisites

- Speed test can only be run from the SDWAN Manager.
- No specific configurations to be done on the device.
- Ensure Data Stream is enabled Administration > Settings > Data stream



The network is out of compliance due to licensing, please click here for more actions.

Settings

Settings / Data Collection & Statistics

Data Stream

Data Stream is used to run the troubleshooting tools on SD-WAN Manager.

Enabling Data Stream doesn't start any services or open any ports initially. Configuration involves specifying an IP address under the VPN that the Edge devices will use.

The SD-WAN Manager establishes a Netconf connection to the Edge device to initiate the troubleshooting command. This prompts the Edge device to establish an HTTPS connection back to the SD-WAN Manager using the provided hostname/IP address and VPN details.

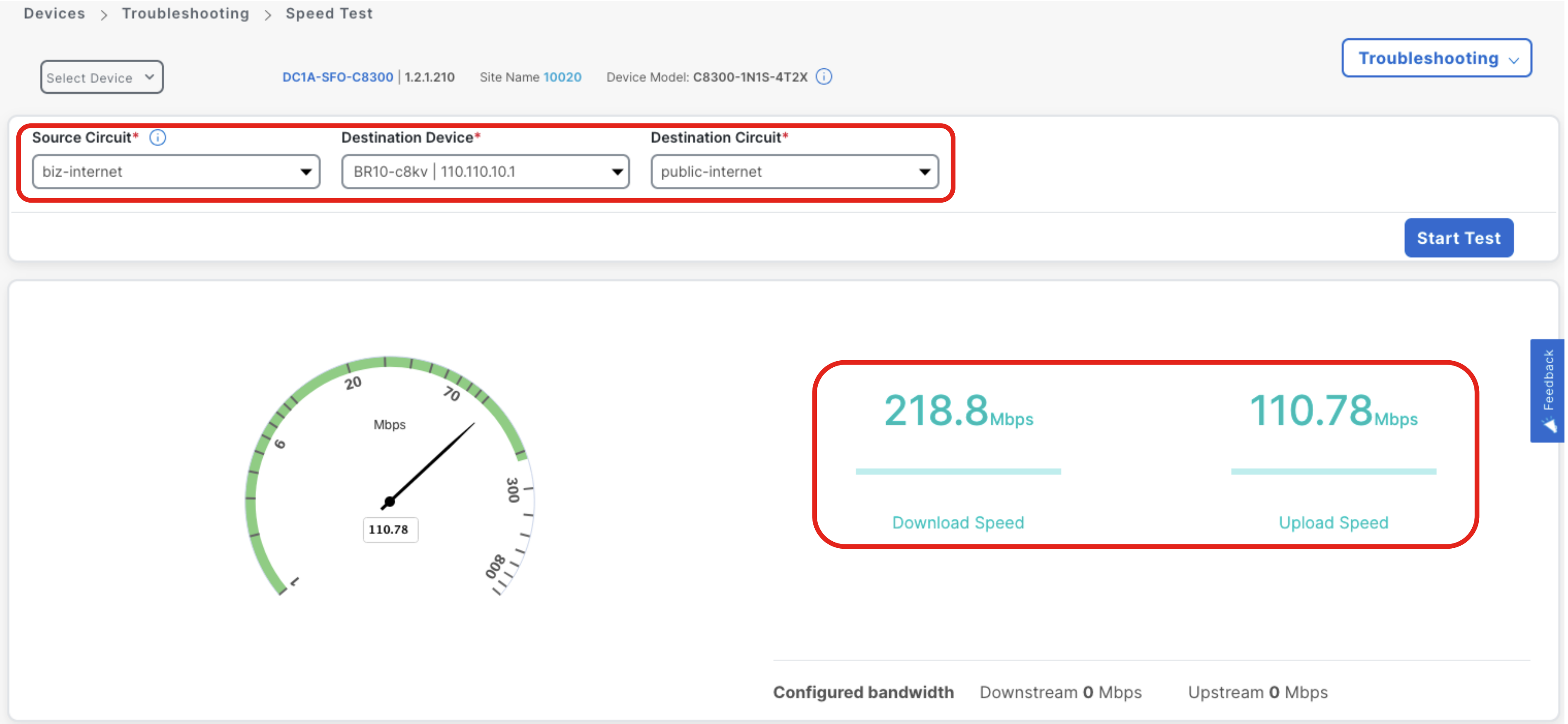
These connections are closed once the troubleshooting tool completes its operation. If something goes wrong and the tool fails to complete within 15 minutes, a background timer will close them.

Data Stream ⓘ

Ip Address Type:

● System ○ Transport ○ Management

Let’s run a Speed Test



Devices > Troubleshooting > Speed Test

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Source Circuit*: biz-internet

Destination Device*: BR10-c8kv | 110.110.10.1

Destination Circuit*: public-internet

218.8Mbps Download Speed

110.78Mbps Upload Speed

Configured bandwidth Downstream 0 Mbps Upstream 0 Mbps

SDWAN Manager Tools

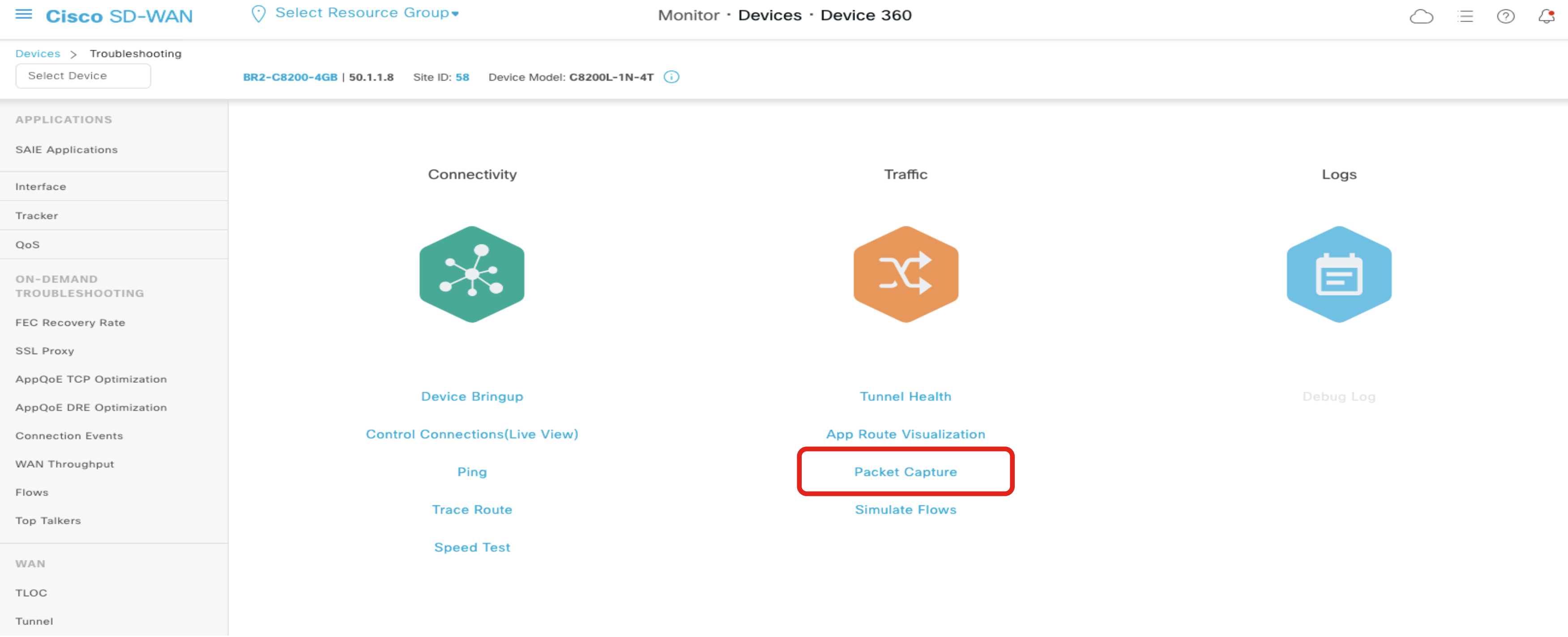
Packet Capture

Packet Capture made easy...

- Capture packets at the click of a button with no additional configs.
- Traffic can be captured with or without filters.
- 5 min or 5-MB file can be captured.
- 3-Step easy process to capture, prepare and download.

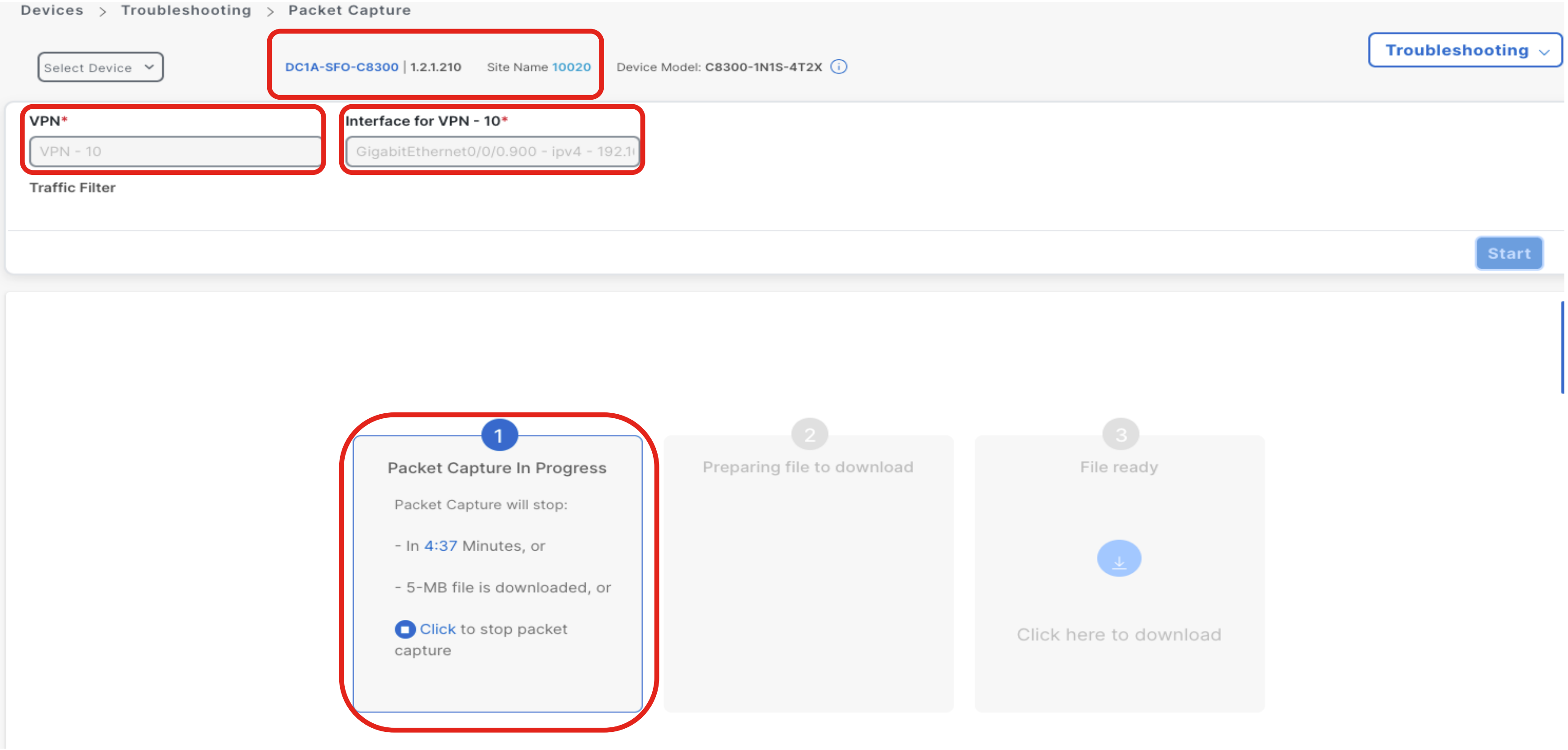
Packet Capture made easy...

Devices > Troubleshooting



BR2-C8200-4GB | 50.1.1.8 Site ID: 58 Device Model: C8200L-1N-4T

Let’s take some captures



Devices > Troubleshooting > Packet Capture

Select Device

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Troubleshooting

VPN*: VPN - 10

Interface for VPN - 10*: GigabitEthernet0/0/0.900 - ipv4 - 192.1

Traffic Filter

Start

1 Packet Capture In Progress

Packet Capture will stop:

- In 4:37 Minutes, or

- 5-MB file is downloaded, or

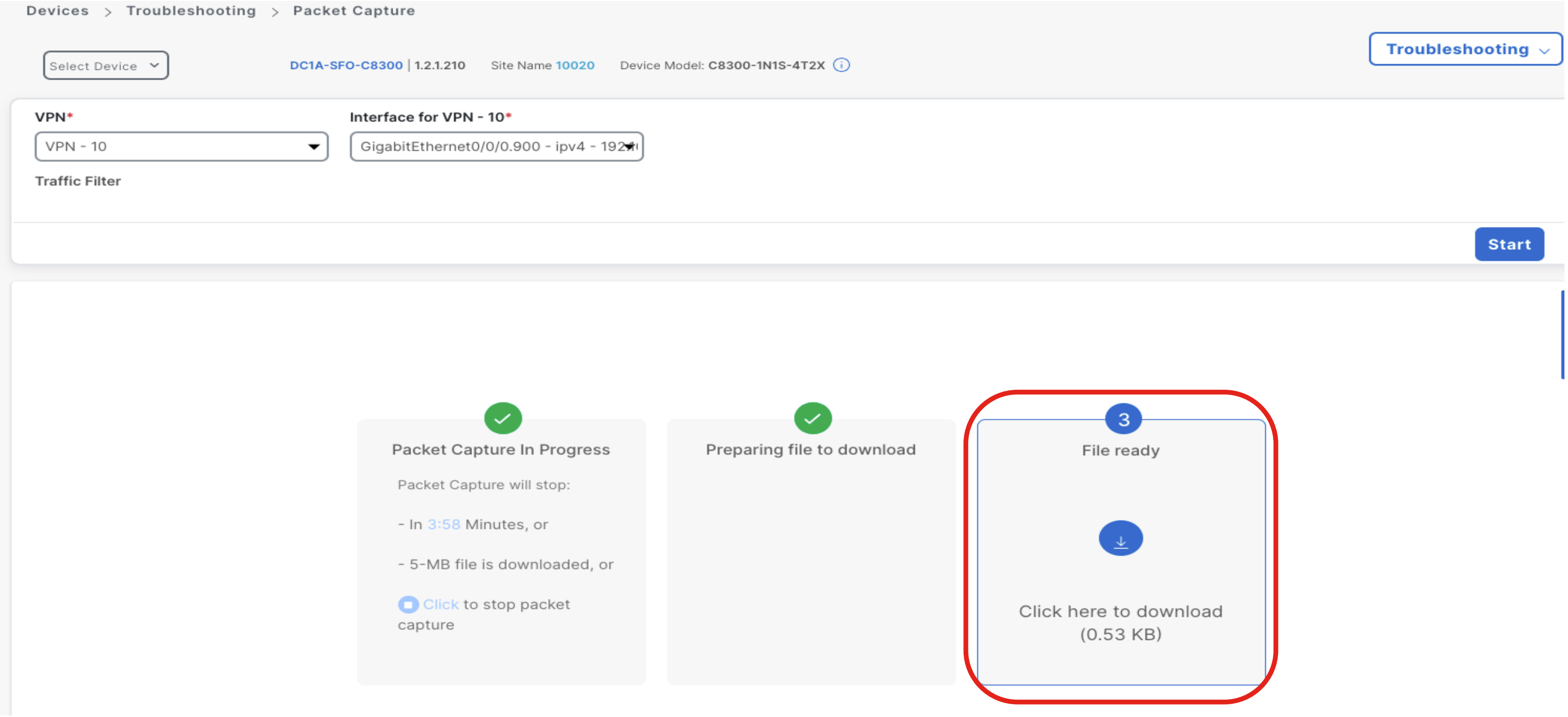
Click to stop packet capture

2 Preparing file to download

3 File ready

Click here to download

Let’s take some captures



Devices > Troubleshooting > Packet Capture

Select Device

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Troubleshooting

VPN*: VPN - 10

Interface for VPN - 10*: GigabitEthernet0/0/0.900 - ipv4 - 192

Traffic Filter

Start

Packet Capture In Progress

Packet Capture will stop:

- In 3:58 Minutes, or

- 5-MB file is downloaded, or

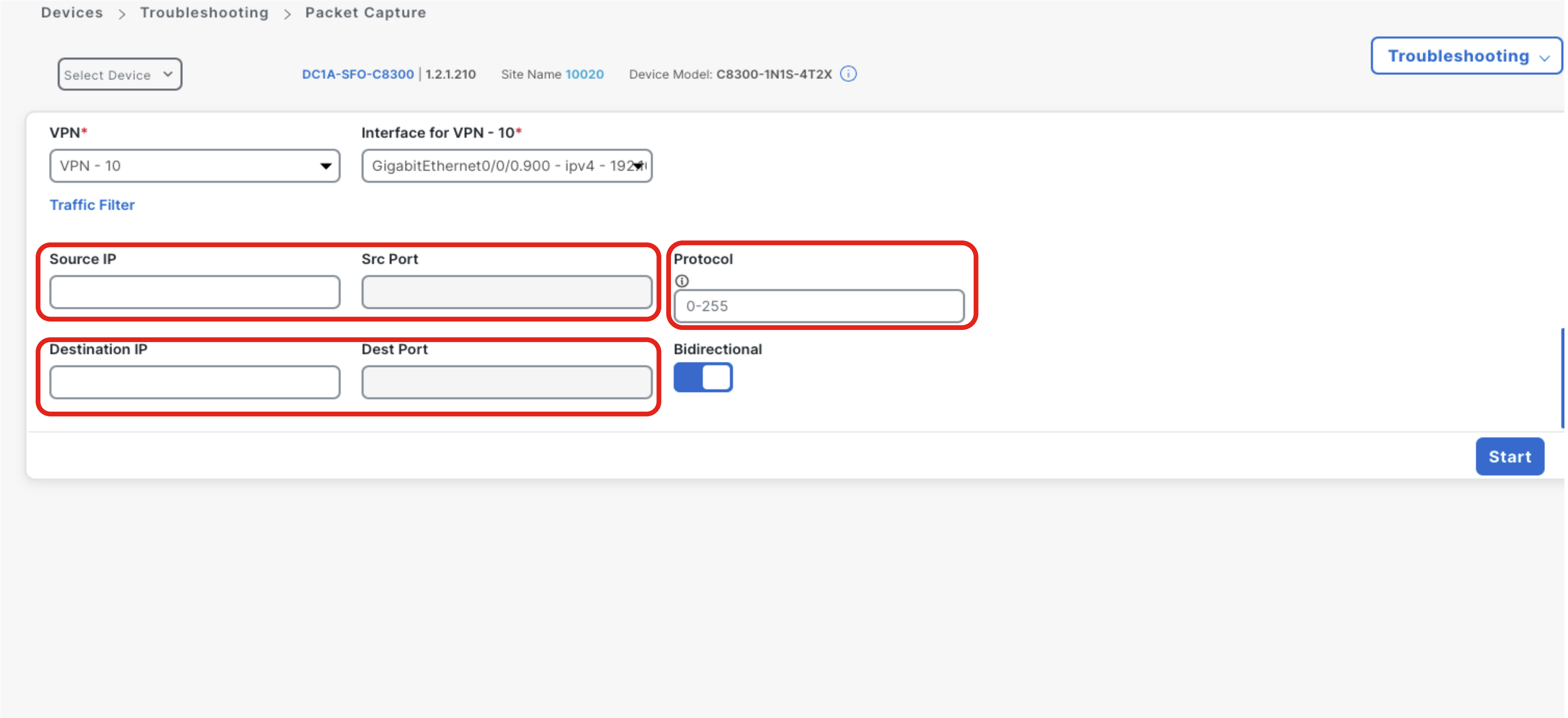
Click to stop packet capture

Preparing file to download

3 File ready

Click here to download (0.53 KB)

Using filters



Devices > Troubleshooting > Packet Capture

Select Device

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Troubleshooting

VPN*: VPN - 10

Interface for VPN - 10*: GigabitEthernet0/0/0.900 - ipv4 - 192.

Traffic Filter

Source IP:

Src Port:

Protocol: 0-255

Destination IP:

Dest Port:

Bidirectional

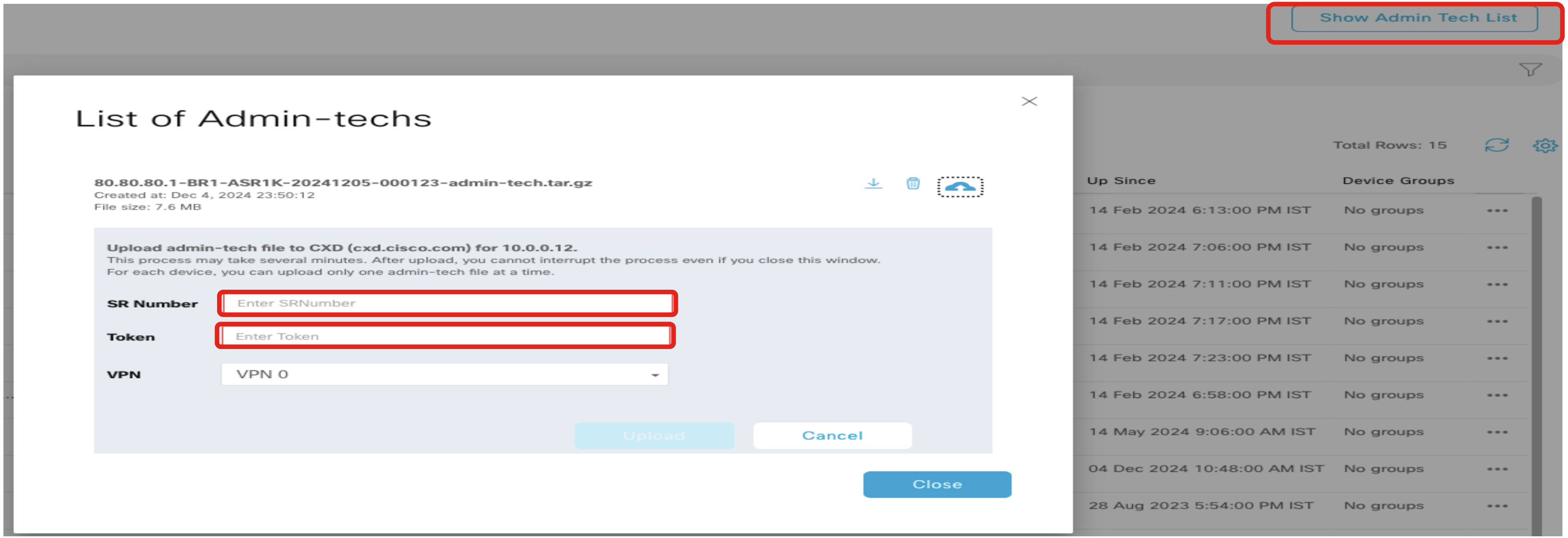
Start

Upload admin-tech & TAC case

Upload Admin-tech :

- Upload admin-tech directly to TAC case from SD-WAN Manager. Feature since 20.7.1/17.7.1a
- Requires internet access to cxd.cisco.com & upload token from TAC SR.
- Generate admin-tech from the vManage.

Upload Admin-tech :



List of Admin-techs

80.80.80.1-BR1-ASR1K-20241205-000123-admin-tech.tar.gz
Created at: Dec 4, 2024 23:50:12
File size: 7.6 MB

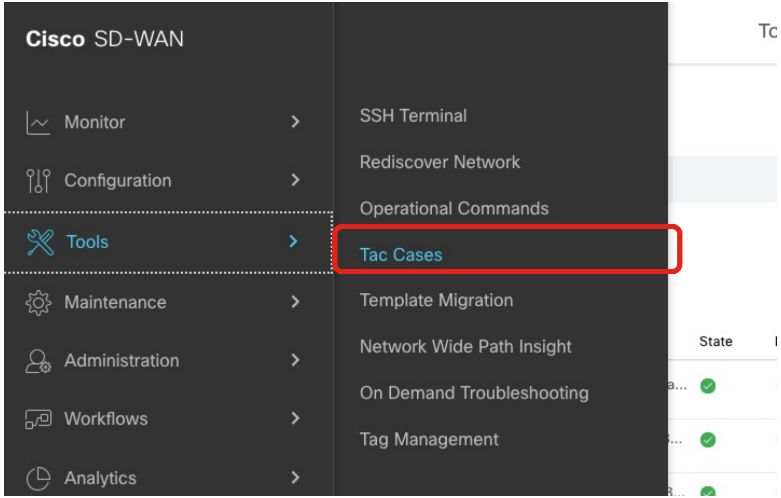
Upload admin-tech file to CXD (cxd.cisco.com) for 10.0.0.12.
This process may take several minutes. After upload, you cannot interrupt the process even if you close this window.
For each device, you can upload only one admin-tech file at a time.

SR Number	Enter SRNumber
Token	Enter Token
VPN	VPN 0

Up Since	Device Groups
14 Feb 2024 6:13:00 PM IST	No groups
14 Feb 2024 7:06:00 PM IST	No groups
14 Feb 2024 7:11:00 PM IST	No groups
14 Feb 2024 7:17:00 PM IST	No groups
14 Feb 2024 7:23:00 PM IST	No groups
14 Feb 2024 6:58:00 PM IST	No groups
14 May 2024 9:06:00 AM IST	No groups
04 Dec 2024 10:48:00 AM IST	No groups
28 Aug 2023 5:54:00 PM IST	No groups

TAC Case :

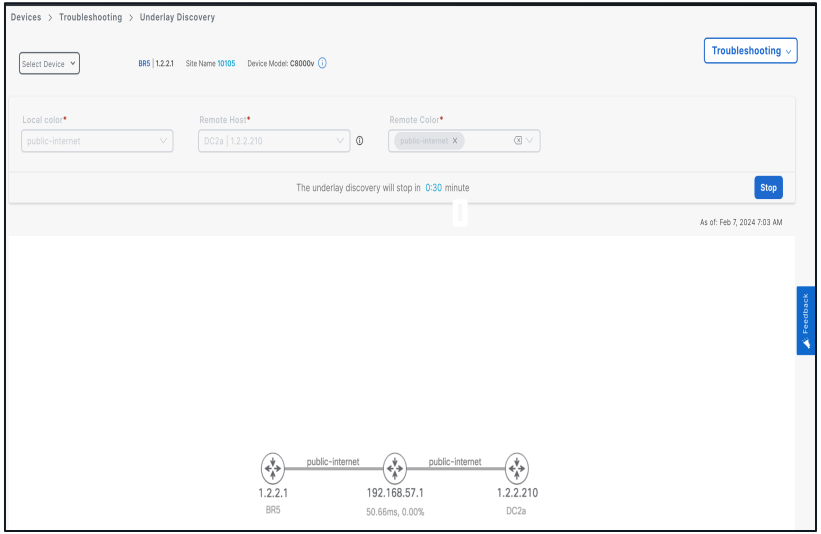
- Access SCM portal from SD-WAN Manager. Feature since 20.9.1
- Requires internet access and reachability to Support case Manager (SCM)
- Active Cisco single sign-on (SSO) login credentials to access the SCM Wizard and the cloud server.
- Open or View TAC cases from SD-WAN Manager



Underlay Measurement and Tracing Service

Underlay Measurement and Tracing Service

- From 17.10/20.10 release, XE-SDWAN routers can perform discovery (Tracing + Measurement) of underlay path.
- Determine exact node/provider is/are responsible for latency in underlay network.
- Displays the exact path which is being used by SD-WAN overlay tunnel.



BR5 | 1.2.2.1 Site Name 10105 Device Model: C8000v

Local color*: public-internet

Remote Host*: DC2a | 1.2.2.210

Remote Color*: public-internet

The underlay discovery will stop in 0:30 minute

As of: Feb 7, 2024 7:03 AM

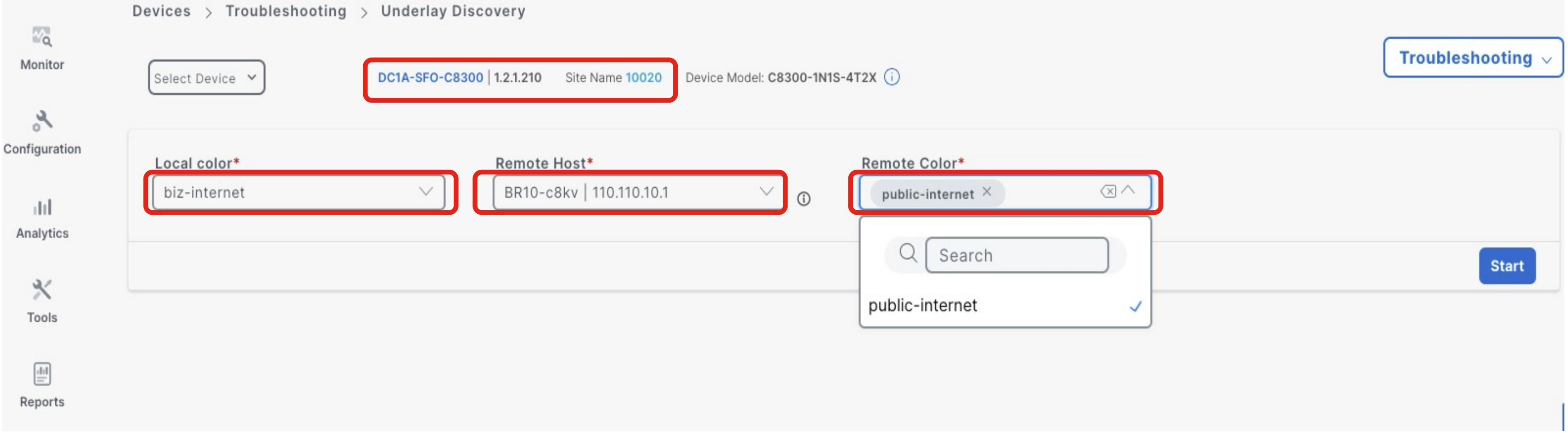
1.2.2.1 BR5

192.168.57.1 50.66ms, 0.00%

1.2.2.210 DC2a

Underlay Measurement and Tracing Service

Path : Monitoring > Devices > Troubleshooting > Underlay Discovery



Devices > Troubleshooting > Underlay Discovery

Select Device

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

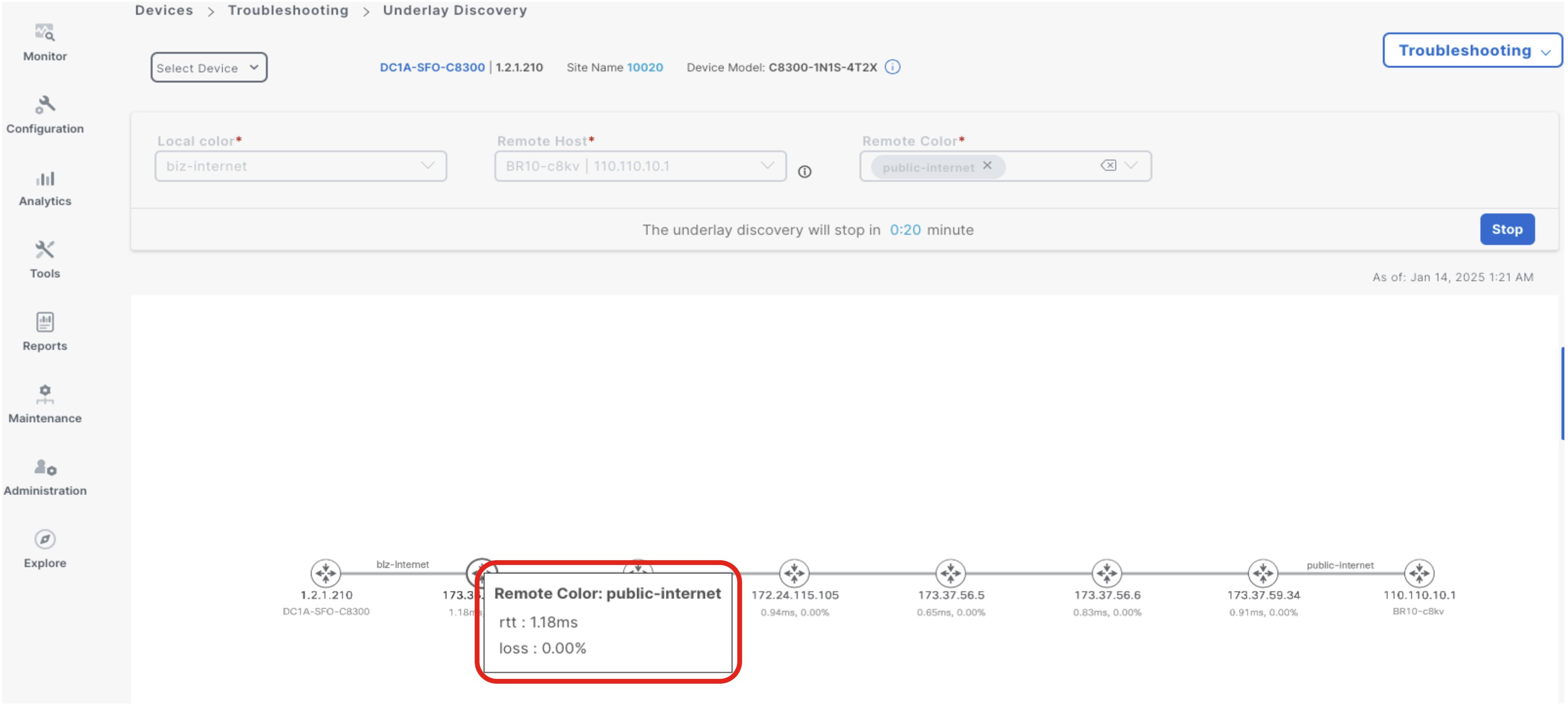
Local color*: biz-internet

Remote Host*: BR10-c8kv | 110.110.10.1

Remote Color*: public-internet

public-internet ✓

Underlay Measurement and Tracing Service



Devices > Troubleshooting > Underlay Discovery

DC1A-SFO-C8300 | 1.2.1.210 Site Name 10020 Device Model: C8300-1N1S-4T2X

Local color*: biz-internet

Remote Host*: BR10-c8kv | 110.110.10.1

Remote Color*: public-internet

The underlay discovery will stop in 0:20 minute

As of: Jan 14, 2025 1:21 AM

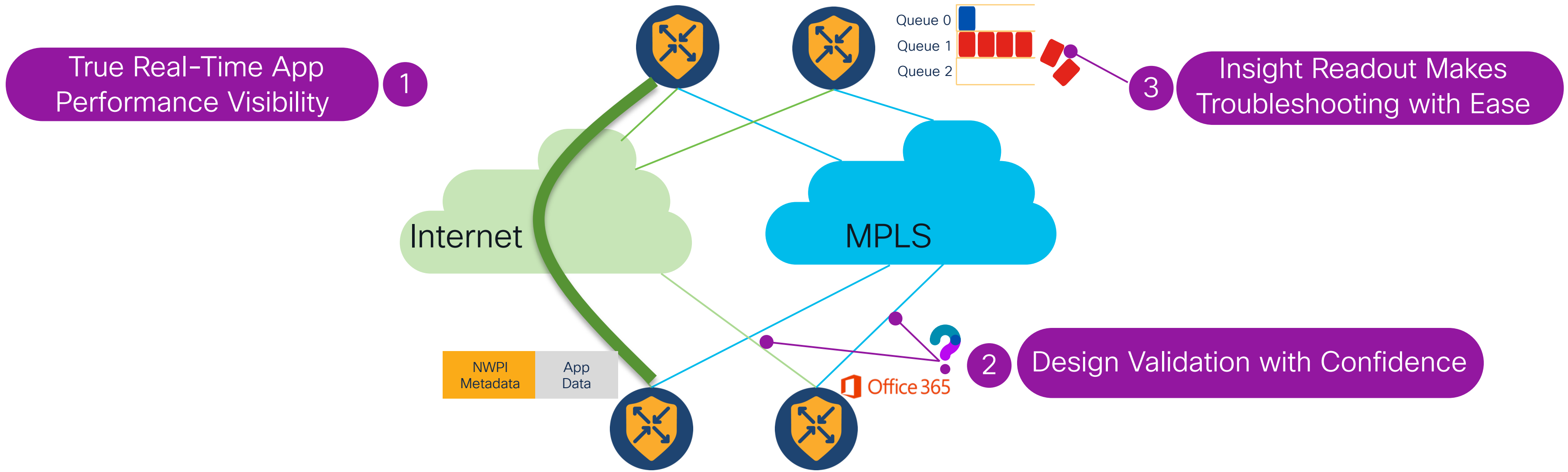
Remote Color: public-internet

rtt : 1.18ms

loss : 0.00%

Network Wide Path Insight (NWPI)

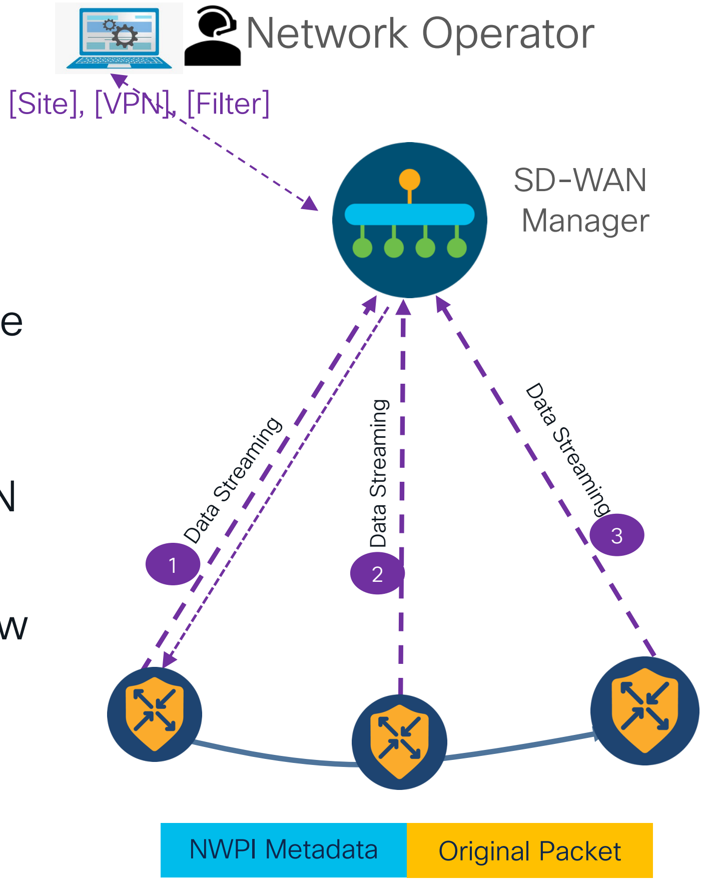
NWPI: Confidant for SD-WAN Operations:



True Real-Time App Performance Visibility
1
Queue 0
Queue 1
Queue 2
3
Insight Readout Makes Troubleshooting with Ease
Internet
MPLS
NWPI Metadata
App Data
Office 365
2
Design Validation with Confidence

How NWPI works?

- Network operator creates trace
- SD-WAN Manager instructs first router to write NWPI metadata into SD-WAN header
- Subsequent routers in path use NWPI metadata to send flow information to SD-WAN Manager
- SD-WAN Manager correlates into a single view



FYI

NWPI Release Timeline

17.4/20.4

- NWPI Metadata Streaming integration with SD-WAN Manager
- On-demand Trace with basic filters
- Flow-level Insight
  - Flow path, DSCP, Loss, Delay and Jitter
  - Flow journey inside SD-WAN edge, e.g., data policy, queueing etc.

17.6/20.6

- DNS Domain Discovery
- More advanced filters and options (e.g., ART and app visibility)
- App Domain Insight
- Flow-level Insight- Advanced View
  - App Trend, Flow Trend
  - Intelligent Readout for Critical Use Cases

17.9/20.9

- Insight Summary
  - Overview
  - App Performance Insight
  - Event Insight
  - QoS Insight
- Flow-level Path Insight

FYI

NWPI Release Timeline

17.12/20.12

- Synthetic Traffic for Design Validation
- Multiple VPNs Trace Supported
- UX 2.0 Global Topology and NWPI Integration
- Auto On NWPI Tasks for SLA Violation and QoS Congestion events

17.13/20.13

- NWPI and ISE Integration.
- User ID Grouping field

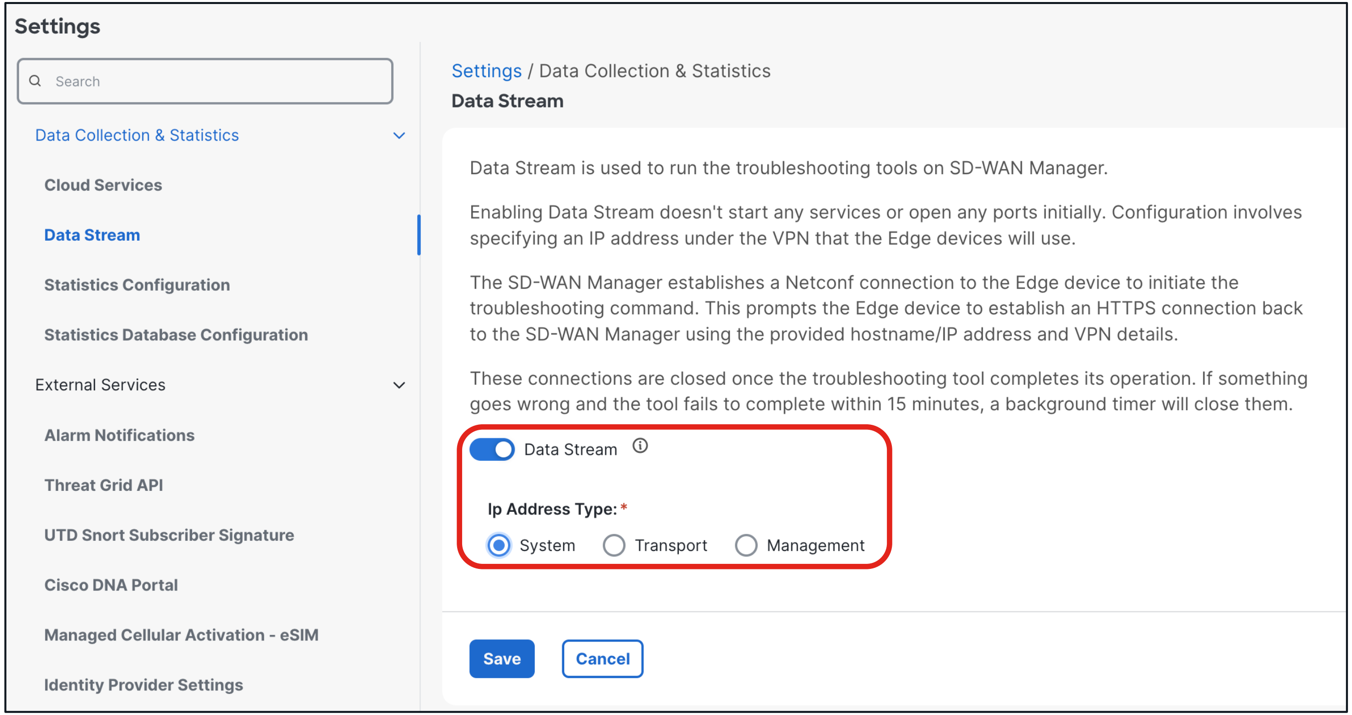
17.14/20.14

- NWPI and ThousandEyes Integration

Prerequisites

In SD-WAN Manager,

Administration->
Settings->
Data Stream ->
Select
System



Settings
Search
Data Collection & Statistics
Cloud Services
Data Stream
Statistics Configuration
Statistics Database Configuration
External Services
Alarm Notifications
Threat Grid API
UTD Snort Subscriber Signature
Cisco DNA Portal
Managed Cellular Activation - eSIM
Identity Provider Settings

Settings / Data Collection & Statistics

Data Stream

Data Stream is used to run the troubleshooting tools on SD-WAN Manager.

Enabling Data Stream doesn't start any services or open any ports initially. Configuration involves specifying an IP address under the VPN that the Edge devices will use.

The SD-WAN Manager establishes a Netconf connection to the Edge device to initiate the troubleshooting command. This prompts the Edge device to establish an HTTPS connection back to the SD-WAN Manager using the provided hostname/IP address and VPN details.

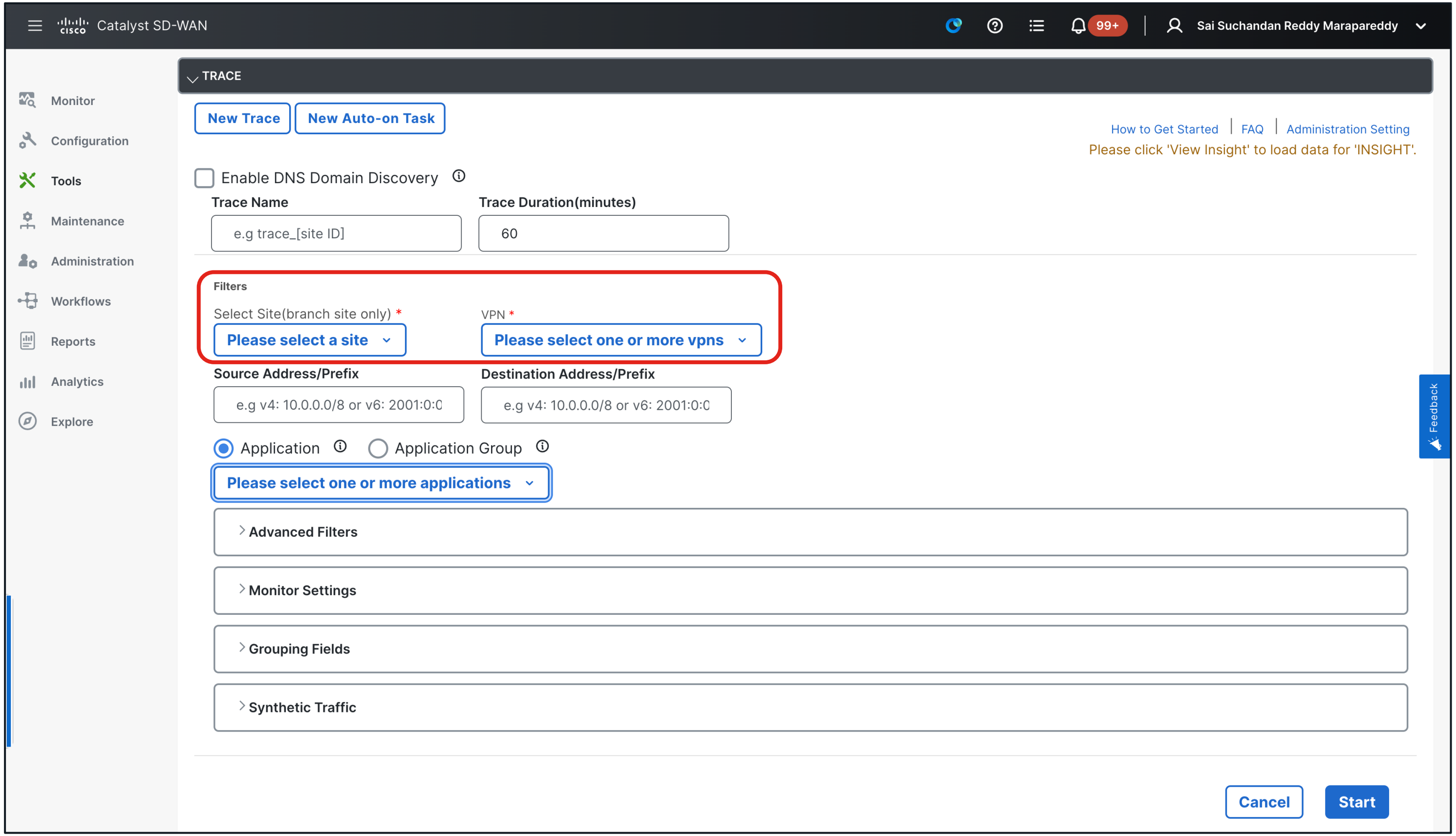
These connections are closed once the troubleshooting tool completes its operation. If something goes wrong and the tool fails to complete within 15 minutes, a background timer will close them.

Data Stream: on

Ip Address Type: *

● System ○ Transport ○ Management

Start NWPI Trace



Please click 'View Insight' to load data for 'INSIGHT'.

□ Enable DNS Domain Discovery ⓘ

Trace Name: e.g trace_[site ID]

Trace Duration(minutes): 60

Filters

Select Site(branch site only) *: Please select a site

VPN *: Please select one or more vpns

Source Address/Prefix: e.g v4: 10.0.0.0/8 or v6: 2001:0:0

Destination Address/Prefix: e.g v4: 10.0.0.0/8 or v6: 2001:0:0

● Application ⓘ ○ Application Group ⓘ

Please select one or more applications

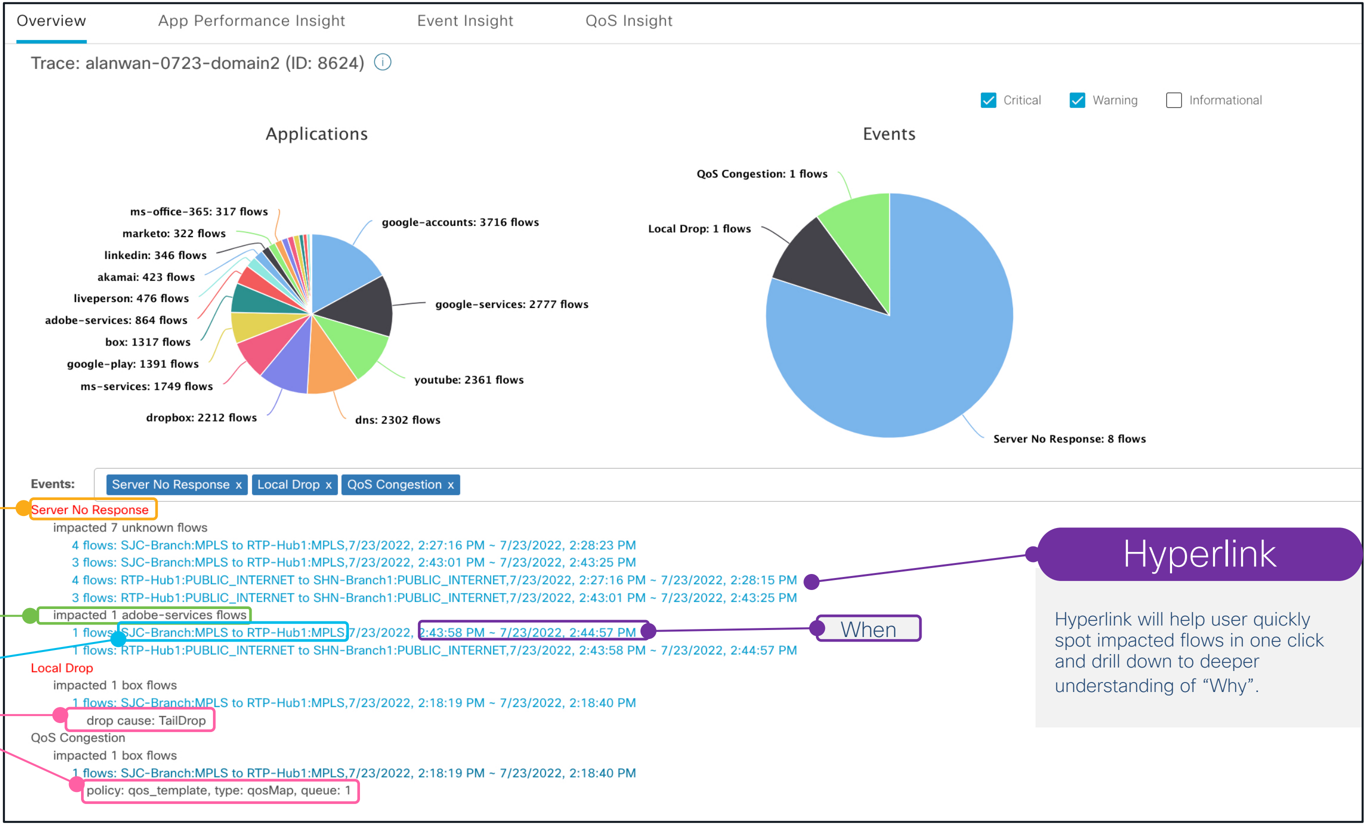
› Advanced Filters

› Monitor Settings

› Grouping Fields

› Synthetic Traffic

Insight Summary – Overview



Trace: alanwan-0723-domain2 (ID: 8624) ⓘ

☑ Critical ☑ Warning □ Informational

Events: Server No Response x Local Drop x QoS Congestion x

Server No Response
impacted 7 unknown flows
4 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:27:16 PM ~ 7/23/2022, 2:28:23 PM
3 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:43:01 PM ~ 7/23/2022, 2:43:25 PM
4 flows: RTP-Hub1:PUBLIC_INTERNET to SHN-Branch1:PUBLIC_INTERNET,7/23/2022, 2:27:16 PM ~ 7/23/2022, 2:28:15 PM
3 flows: RTP-Hub1:PUBLIC_INTERNET to SHN-Branch1:PUBLIC_INTERNET,7/23/2022, 2:43:01 PM ~ 7/23/2022, 2:43:25 PM
impacted 1 adobe-services flows
1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:43:58 PM ~ 7/23/2022, 2:44:57 PM
1 flows: RTP-Hub1:PUBLIC_INTERNET to SHN-Branch1:PUBLIC_INTERNET,7/23/2022, 2:43:58 PM ~ 7/23/2022, 2:44:57 PM
Local Drop
impacted 1 box flows
1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:18:19 PM ~ 7/23/2022, 2:18:40 PM
drop cause: TailDrop
QoS Congestion
impacted 1 box flows
1 flows: SJC-Branch:MPLS to RTP-Hub1:MPLS,7/23/2022, 2:18:19 PM ~ 7/23/2022, 2:18:40 PM
policy: qos_template, type: qosMap, queue: 1

What

Who

Where

Why

When

Hyperlink

Hyperlink will help user quickly spot impacted flows in one click and drill down to deeper understanding of “Why”.

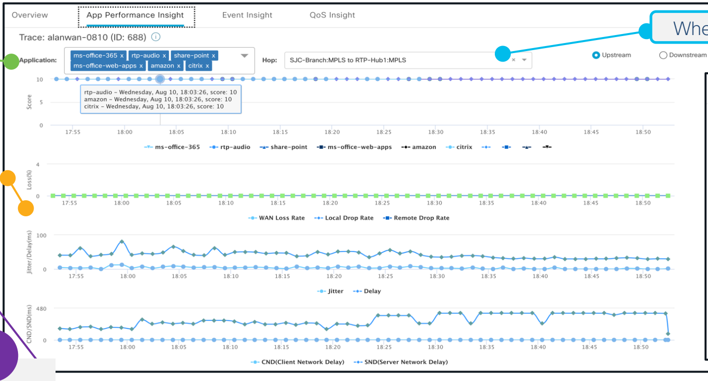
Insight Summary - App Performance Insight

Who

What

When

Where



Overview | App Performance Insight | Event Insight | QoS Insight

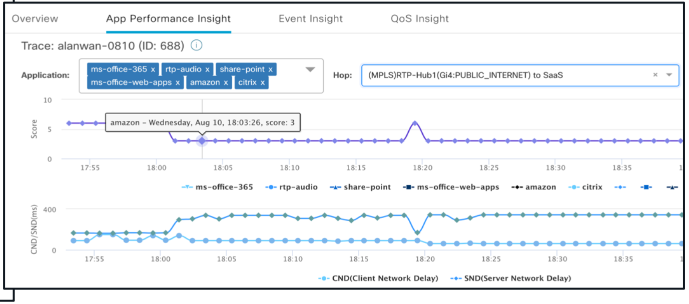
Trace: alanwan-0810 (ID: 688)

Application: ms-office-365 x, rtp-audio x, share-point x, ms-office-web-apps x, amazon x, citrix x

Hop: SJC-Branch:MPLS to RTP-Hub1:MPLS

● Upstream ○ Downstream

rtp-audio - Wednesday, Aug 10, 18:03:26, score: 10
amazon - Wednesday, Aug 10, 18:03:26, score: 10
citrix - Wednesday, Aug 10, 18:03:26, score: 10



Overview | App Performance Insight | Event Insight | QoS Insight

Trace: alanwan-0810 (ID: 688)

Application: ms-office-365 x, rtp-audio x, share-point x, ms-office-web-apps x, amazon x, citrix x

Hop: (MPLS)RTP-Hub1(Gi4:PUBLIC_INTERNET) to SaaS

amazon - Wednesday, Aug 10, 18:03:26, score: 3

Readout

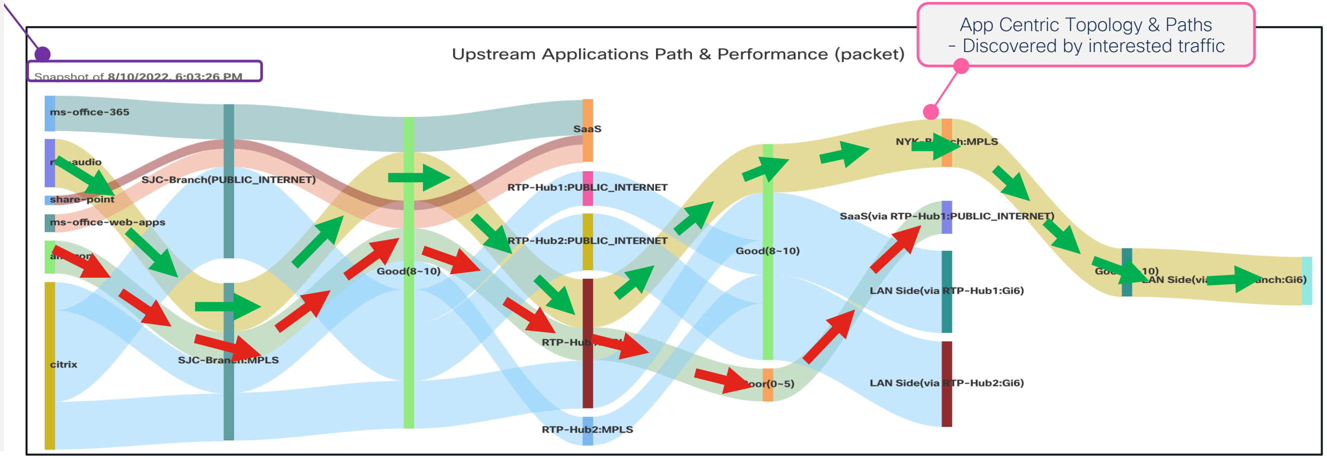
M365: SJC-Branch local breakout to SaaS Cloud via INET(DIA).

Amazon: Backhaul from SJC-branch to RTP-Hub1 via MPLS, then breakout to SaaS Cloud via INET(DIA).
Poor performance on the hop:
RTP-Hub1 to SaaS (via INET)
high server network delay, score 3

rtp-audio: SJC-Branch to NYK-Branch via RTP-Hub1 (MPLS)

Citrix: Load balance from SJC-branch to RTP-Hub1/Hub2 via MPLS/INET, then toward Campus/DC via LAN.

App Centric Topology & Paths
– Discovered by interested traffic



Upstream Applications Path & Performance (packet)

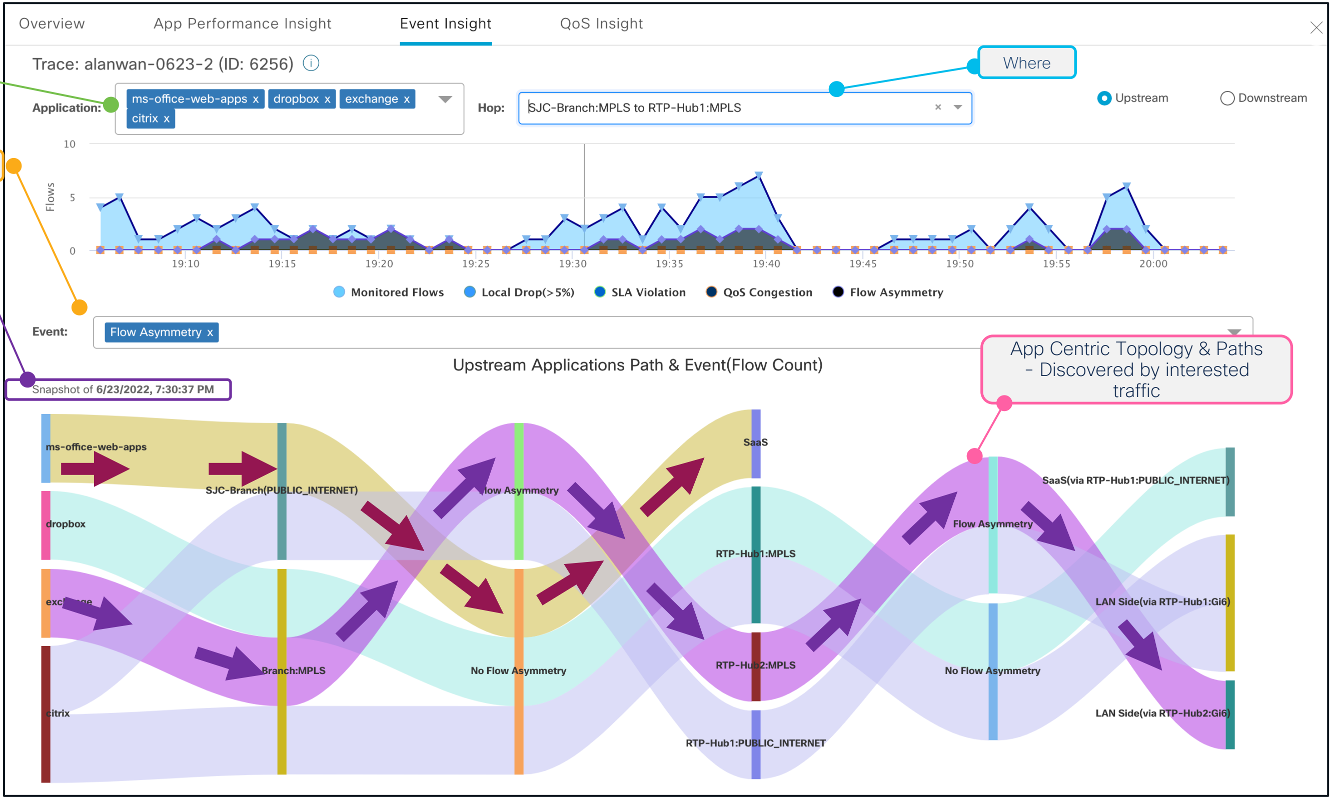
Snapshot of 8/10/2022, 6:03:26 PM

Insight Summary - Event Insight

Who

What

When



Trace: alanwan-0623-2 (ID: 6256)

Application: ms-office-web-apps x dropbox x exchange x citrix x

Hop: SJC-Branch:MPLS to RTP-Hub1:MPLS

● Upstream ○ Downstream

Event: Flow Asymmetry x

Upstream Applications Path & Event(Flow Count)

Snapshot of 6/23/2022, 7:30:37 PM

Where

App Centric Topology & Paths - Discovered by interested traffic

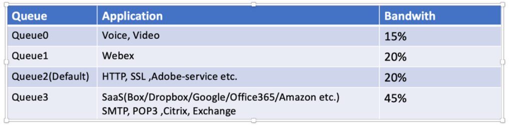
Readout

Office: SJC-Branch local breakout to SaaS Cloud via INET(DIA).

Dropbox: Backhaul from SJC-branch to RTP-Hub1 via MPLS, then breakout to SaaS Cloud via INET(DIA).

Exchange/Citrix: Backhaul from SJC-branch to RTP-Hub1/Hub2 via MPLS/INET, then toward Campus/DC via LAN. Both apps have some flows run into asymmetry on some hops.

Insight Summary - QoS Insight



Queue	Application	Bandwith
Queue0	Voice, Video	15%
Queue1	Webex	20%
Queue2(Default)	HTTP, SSL ,Adobe-service etc.	20%
Queue3	SaaS(Box/Dropbox/Google/Office365/Amazon etc.) SMTP, POP3 ,Citrix, Exchange	45%

Tips

QoS Insight – Use case 1

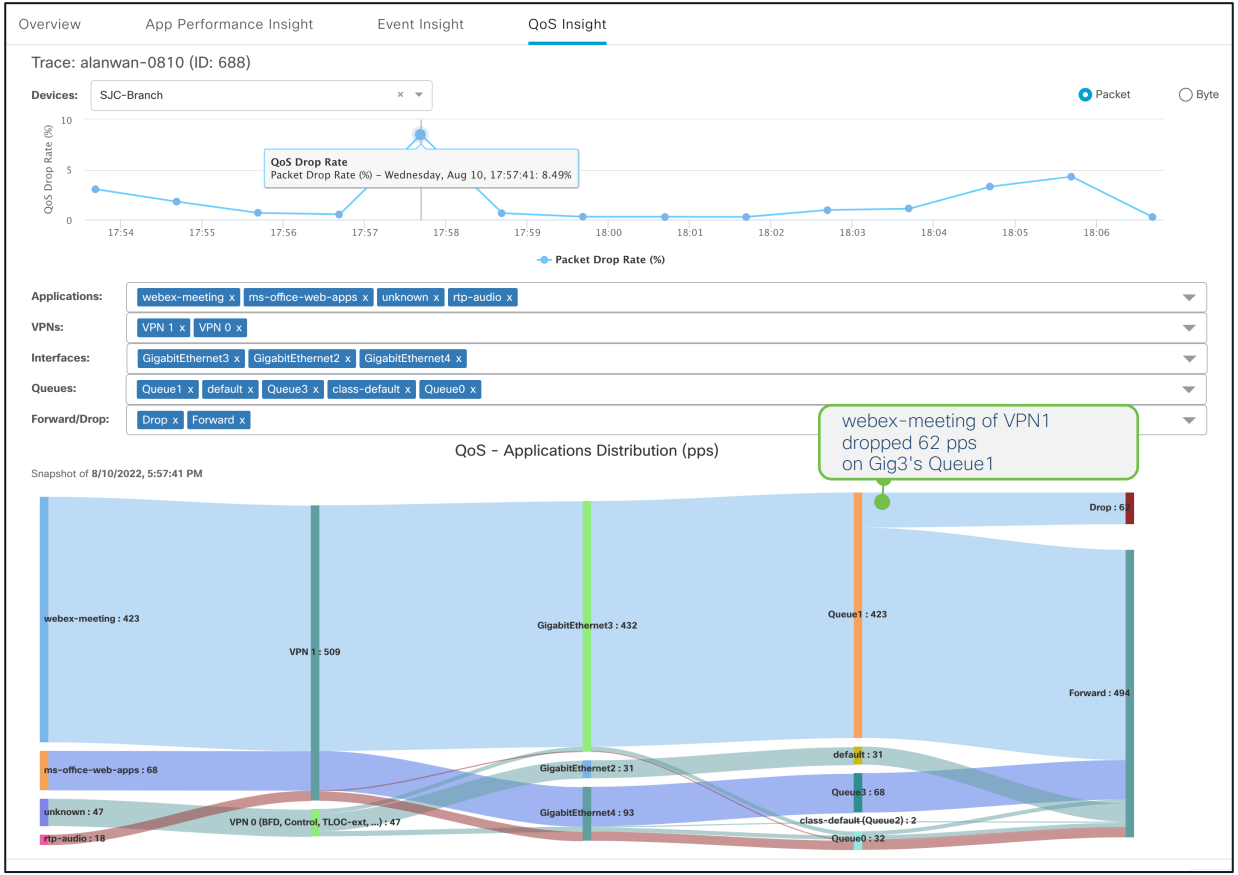
CIO's Webex meeting run into bad quality. Finally, root cause was:

More attendees joined the Webex meeting from same site and run out of planned bandwidth.

" QoS insight" , for QoS congestion debug or bandwidth capacity planning.

Remediation Actions:

1. Allocate more bandwidth for Webex/Queue1
2. Buy more bandwidth for circuit Gig3.
3. Allocate other apps to different queue if competing bandwidth is in same queue
4. Revisit traffic steering policy, for example not to prefer MPLS, load-balance to other WAN circuits.



Trace: alanwan-0810 (ID: 688)

Devices: SJC-Branch

● Packet ○ Byte

QoS Drop Rate
Packet Drop Rate (%) – Wednesday, Aug 10, 17:57:41: 8.49%

Applications: webex-meeting x ms-office-web-apps x unknown x rtp-audio x

VPNs: VPN 1 x VPN 0 x

Interfaces: GigabitEthernet3 x GigabitEthernet2 x GigabitEthernet4 x

Queues: Queue1 x default x Queue3 x class-default x Queue0 x

Forward/Drop: Drop x Forward x

QoS - Applications Distribution (pps)

Snapshot of 8/10/2022, 5:57:41 PM

webex-meeting of VPN1 dropped 62 pps on Gig3's Queue1

Scenario 1

Integration with NWPI and ISE

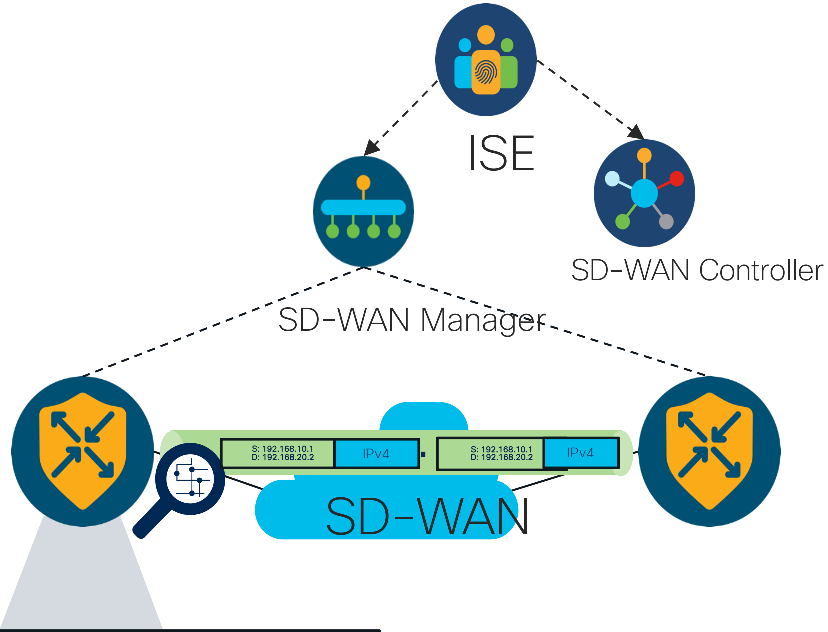
Network Wide Path Insights (NWPI)

NWPI provides network wide insights such as

- Path insight overview,
- Application Performance Insight,
- Event Insight,
- QoS Insight,
- Flow Level Path Insights,
- DNS domain discovery,
- Path performance metrics.

NWPI helps to validate policy design and insights for various application performance issues.

In 20.13/17.13, in NWPI trace settings we can trigger trace for specific user and group Insight summary based on user filter.

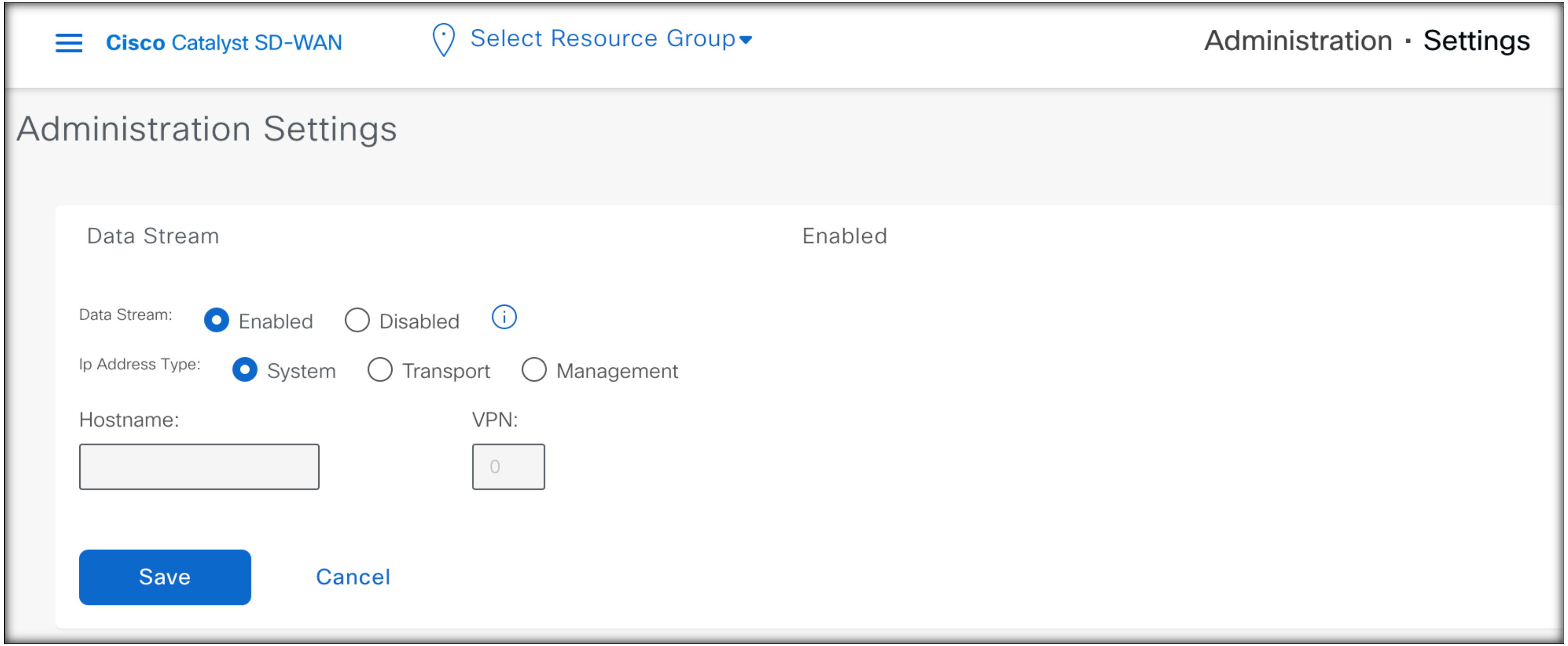


NWPI Trace

- Insight Summary
- Application Performance Insight
- Event Insight
- QoS Insight
- Easy DNS Domain Discovery Workflow
- User Insight

Prerequisites

In SD-WAN Manager UI, go to Administration-> Settings-> Data Stream to enable Data Stream configuration.



Administration Settings

Data Stream Enabled

Data Stream: ● Enabled ○ Disabled

Ip Address Type: ● System ○ Transport ○ Management

Hostname:

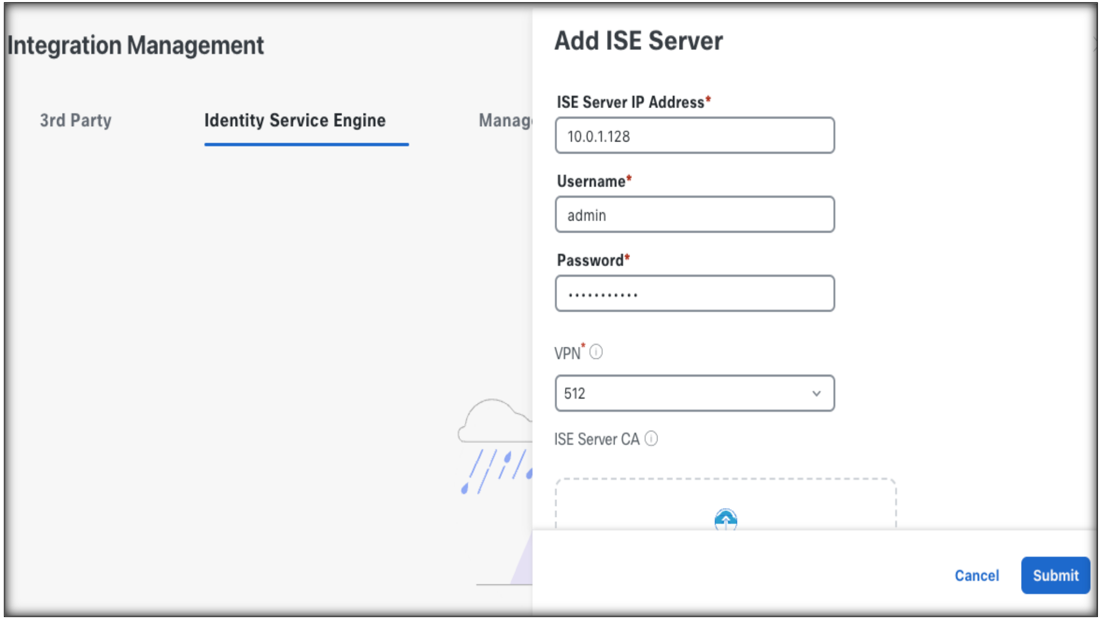
VPN: 0

Add ISE Server

Before Adding ISE Server, make sure SD-WAN controller (vSmart) is in SD-WAN Manager (vManage) mode

Add the ISE connection details

- Server IP
- Admin username, password
- VPN to connect to ISE from SD-WAN Manager (0 or 512)



Add ISE Server

ISE Server IP Address*: 10.0.1.128

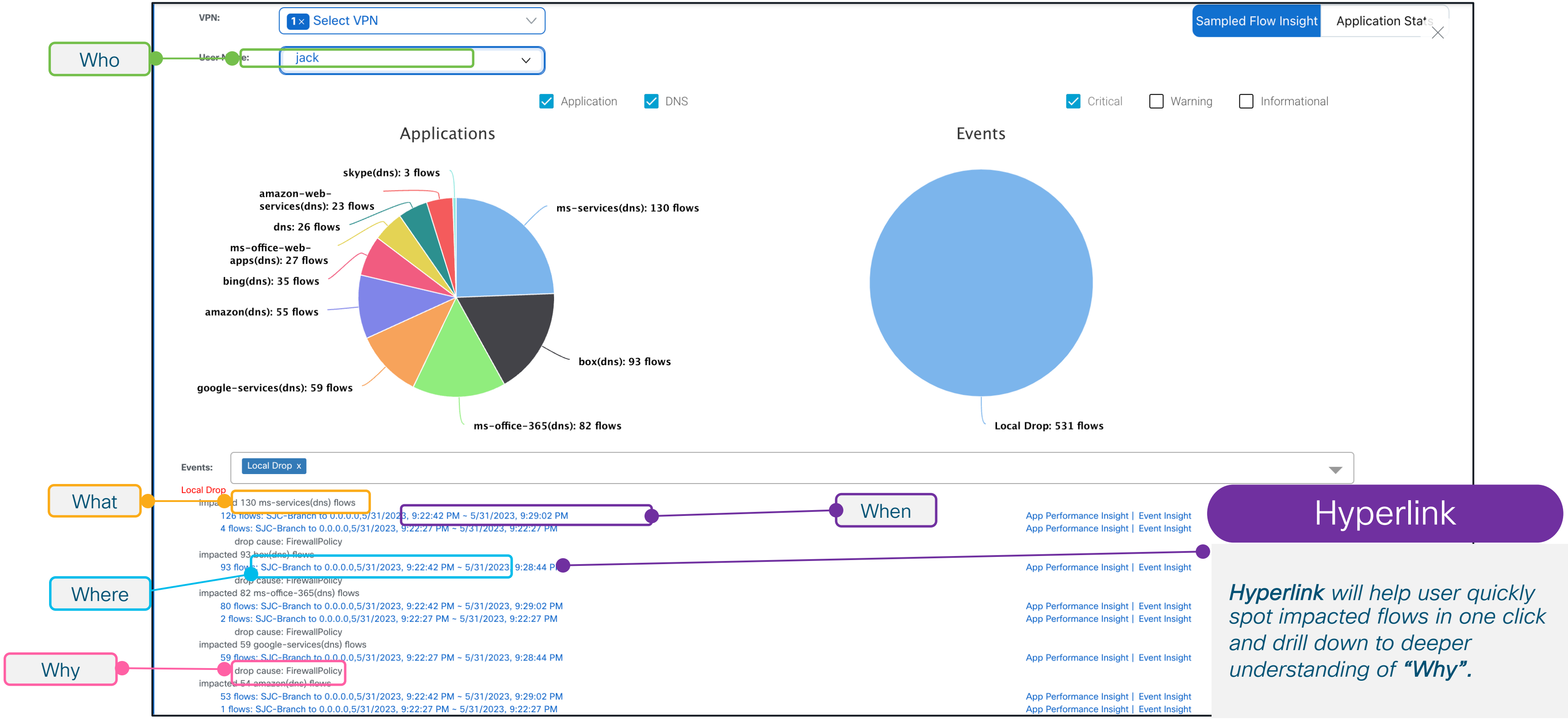
Username*: admin

Password*: ••••••••••••

VPN*: 512

User Unable To Access Application!!

User Jack complains internet access issue



VPN: 1× Select VPN

User Name: jack

☑ Application ☑ DNS

☑ Critical ☐ Warning ☐ Informational

Events: Local Drop x

Local Drop

impacted 130 ms-services(dns) flows
- 126 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:42 PM ~ 5/31/2023, 9:29:02 PM — App Performance Insight | Event Insight
- 4 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:27 PM ~ 5/31/2023, 9:22:27 PM — App Performance Insight | Event Insight

drop cause: FirewallPolicy

impacted 93 box(dns) flows
- 93 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:42 PM ~ 5/31/2023, 9:28:44 PM — App Performance Insight | Event Insight

drop cause: FirewallPolicy

impacted 82 ms-office-365(dns) flows
- 80 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:42 PM ~ 5/31/2023, 9:29:02 PM — App Performance Insight | Event Insight
- 2 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:27 PM ~ 5/31/2023, 9:22:27 PM — App Performance Insight | Event Insight

drop cause: FirewallPolicy

impacted 59 google-services(dns) flows
- 59 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:27 PM ~ 5/31/2023, 9:28:44 PM — App Performance Insight | Event Insight

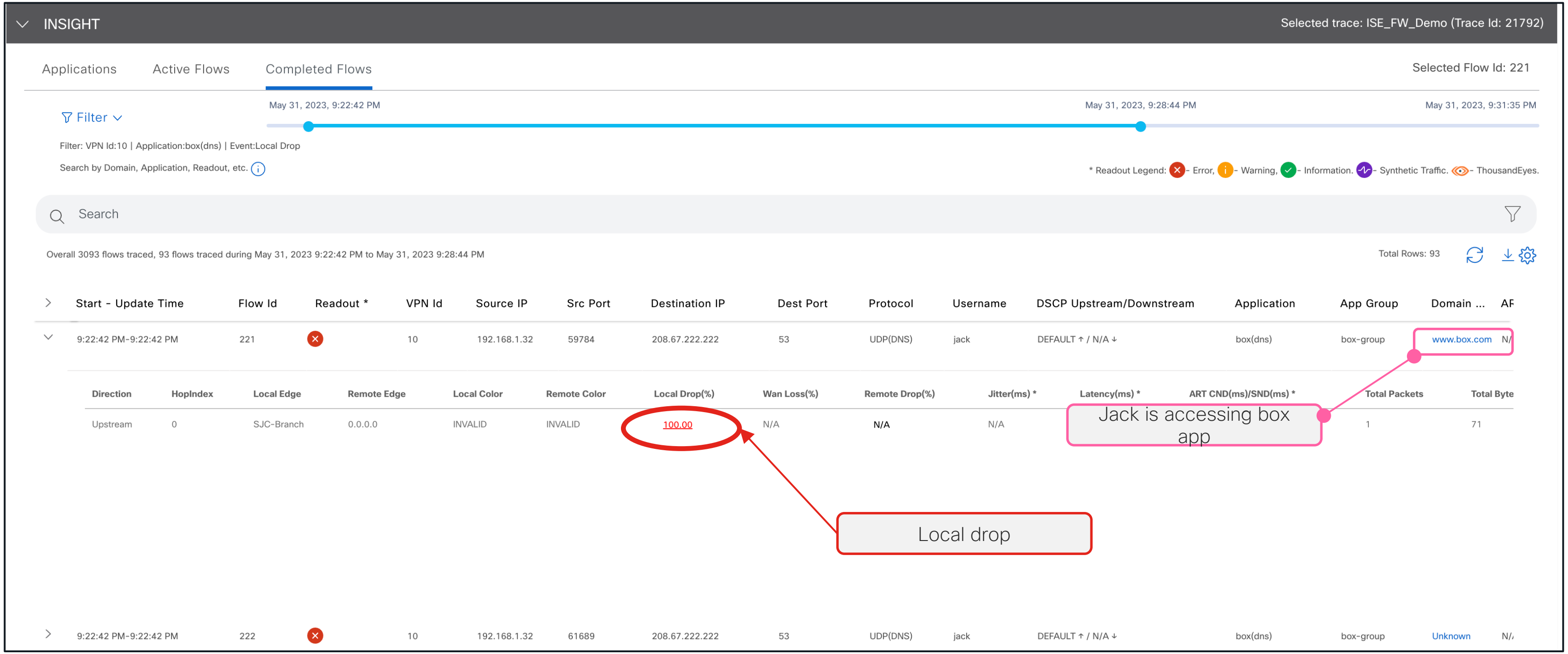
drop cause: FirewallPolicy

impacted 54 amazon(dns) flows
- 53 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:42 PM ~ 5/31/2023, 9:29:02 PM — App Performance Insight | Event Insight
- 1 flows: SJC-Branch to 0.0.0.0,5/31/2023, 9:22:27 PM ~ 5/31/2023, 9:22:27 PM — App Performance Insight | Event Insight

Hyperlink

__Hyperlink__ will help user quickly spot impacted flows in one click and drill down to deeper understanding of __“Why”__.

User(Jack) traffic is dropped on SJC-Branch



INSIGHT

Selected trace: ISE_FW_Demo (Trace Id: 21792)

Applications | Active Flows | Completed Flows

Selected Flow Id: 221

Filter: VPN Id:10 | Application:box(dns) | Event:Local Drop

Search by Domain, Application, Readout, etc.

* Readout Legend: ✕ - Error, ! - Warning, ✓ - Information, - Synthetic Traffic, - ThousandEyes.

Overall 3093 flows traced, 93 flows traced during May 31, 2023 9:22:42 PM to May 31, 2023 9:28:44 PM

Total Rows: 93

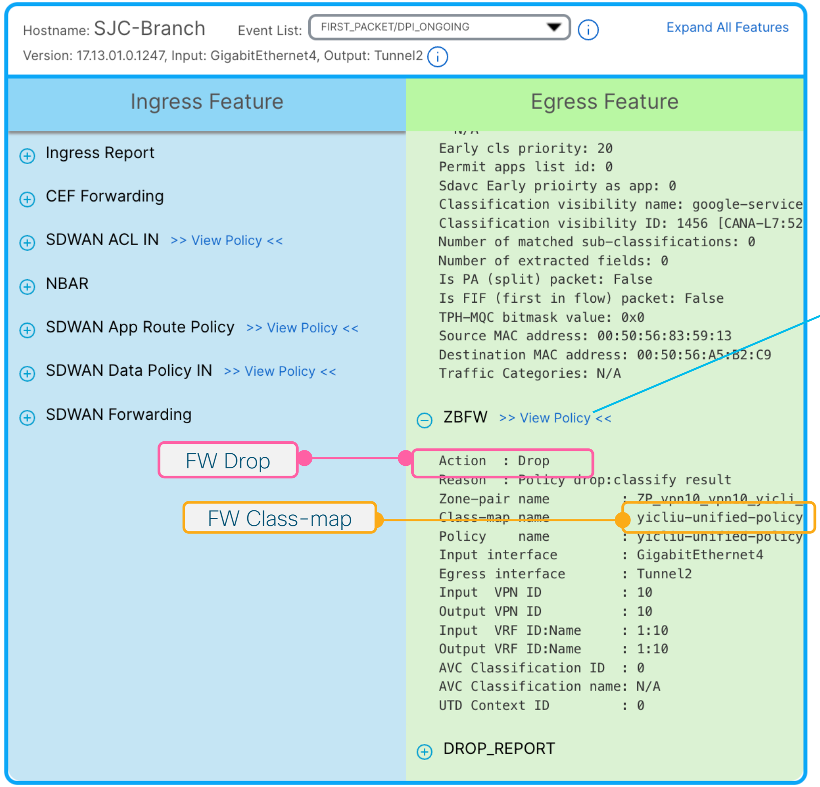
Start - Update Time	Flow Id	Readout *	VPN Id	Source IP	Src Port	Destination IP	Dest Port	Protocol	Username	DSCP Upstream/Downstream	Application	App Group	Domain ...	AF
9:22:42 PM-9:22:42 PM	221	✕	10	192.168.1.32	59784	208.67.222.222	53	UDP(DNS)	jack	DEFAULT ↑ / N/A ↓	box(dns)	box-group	www.box.com	N/
9:22:42 PM-9:22:42 PM	222	✕	10	192.168.1.32	61689	208.67.222.222	53	UDP(DNS)	jack	DEFAULT ↑ / N/A ↓	box(dns)	box-group	Unknown	N/

Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms) *	Latency(ms) *	ART CND(ms)/SND(ms) *	Total Packets	Total Byte
Upstream	0	SJC-Branch	0.0.0.0	INVALID	INVALID	100.00	N/A	N/A	N/A			1	71

Jack is accessing box app

Local drop

View Policy & Config applied for user traffic



Hostname: SJC-Branch   Event List: FIRST_PACKET/DPI_ONGOING ▾ ⓘ   Expand All Features

Version: 17.13.01.0.1247, Input: GigabitEthernet4, Output: Tunnel2 ⓘ

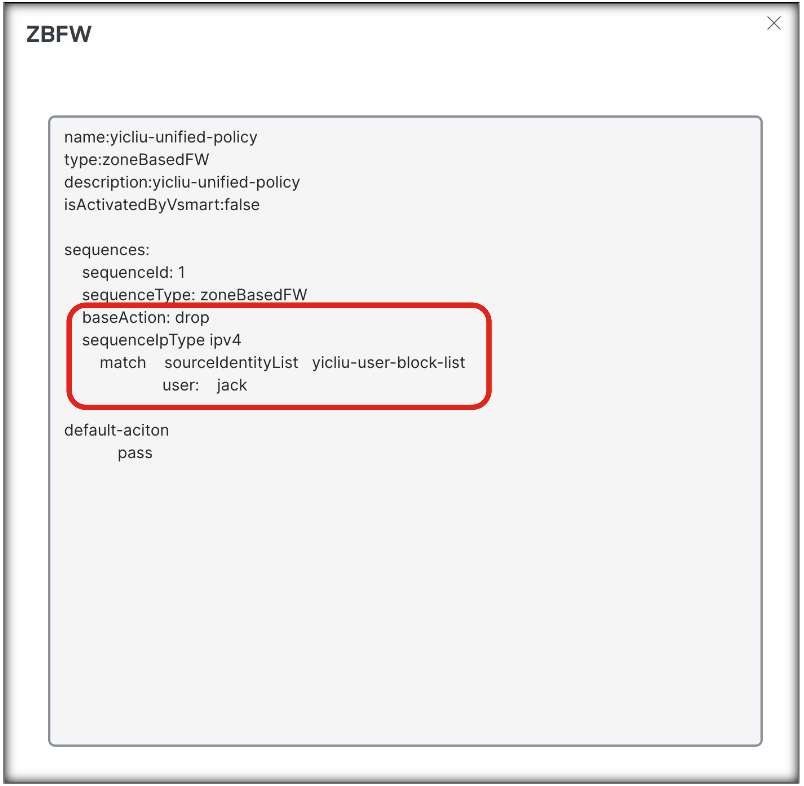
Ingress Feature
⊕ Ingress Report
⊕ CEF Forwarding
⊕ SDWAN ACL IN >> View Policy <<
⊕ NBAR
⊕ SDWAN App Route Policy >> View Policy <<
⊕ SDWAN Data Policy IN >> View Policy <<
⊕ SDWAN Forwarding
FW Drop
FW Class-map
Egress Feature

```
    N/A
Early cls priority: 20
Permit apps list id: 0
Sdavc Early prioirty as app: 0
Classification visibility name: google-service
Classification visibility ID: 1456 [CANA-L7:52
Number of matched sub-classifications: 0
Number of extracted fields: 0
Is PA (split) packet: False
Is FIF (first in flow) packet: False
TPH-MQC bitmask value: 0x0
Source MAC address: 00:50:56:83:59:13
Destination MAC address: 00:50:56:A5:B2:C9
Traffic Categories: N/A
```

⊖ ZBFW >> View Policy <<

```
Action  : Drop
Reason  : Policy drop:classify result
Zone-pair name          : ZP_vpn10_vpn10_yicli_
Class-map name            yicliu-unified-policy
Policy    name          : yicliu-unified-policy
Input interface         : GigabitEthernet4
Egress interface        : Tunnel2
Input  VPN ID           : 10
Output VPN ID           : 10
Input  VRF ID:Name      : 1:10
Output VRF ID:Name      : 1:10
AVC Classification ID   : 0
AVC Classification name: N/A
UTD Context ID          : 0
```

⊕ DROP_REPORT



ZBFW

```
name:yicliu-unified-policy
type:zoneBasedFW
description:yicliu-unified-policy
isActivatedByVsmart:false

sequences:
  sequenceId: 1
  sequenceType: zoneBasedFW
  baseAction: drop
  sequenceIpType ipv4
    match   sourceIdentityList  yicliu-user-block-list
            user:   jack

default-aciton
      pass
```

Scenario 2

Integration with ThousandEyes & Underlay Measurement & Tracing Service

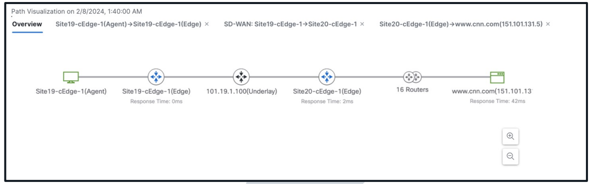
Network Wide Path Insights

Problem

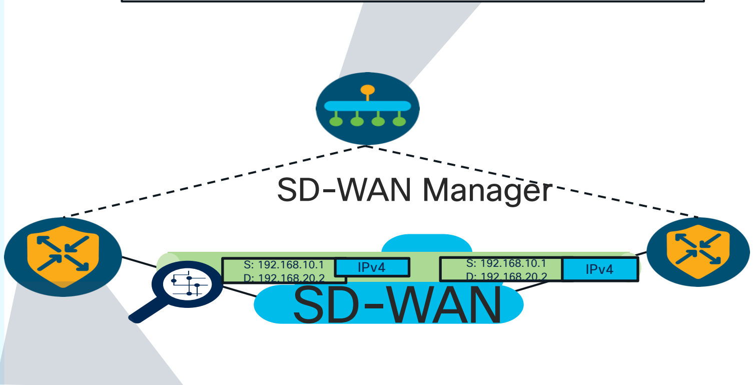
NWPI provides Network Wide Insights such as

- Path Insight overview,
- Application Performance Insight
- Event Insight, QoS Insight etc.

However, it doesn't provide insights in to Underlay Path and Performance metrics at each hop.



Path Visualization on 2/8/2024, 1:40:00 AM



NWPI Trace

- Insight Summary
- Application Performance Insight
- Event & QoS Insight
- User Insight
- ThousandEyes Insight

Solution

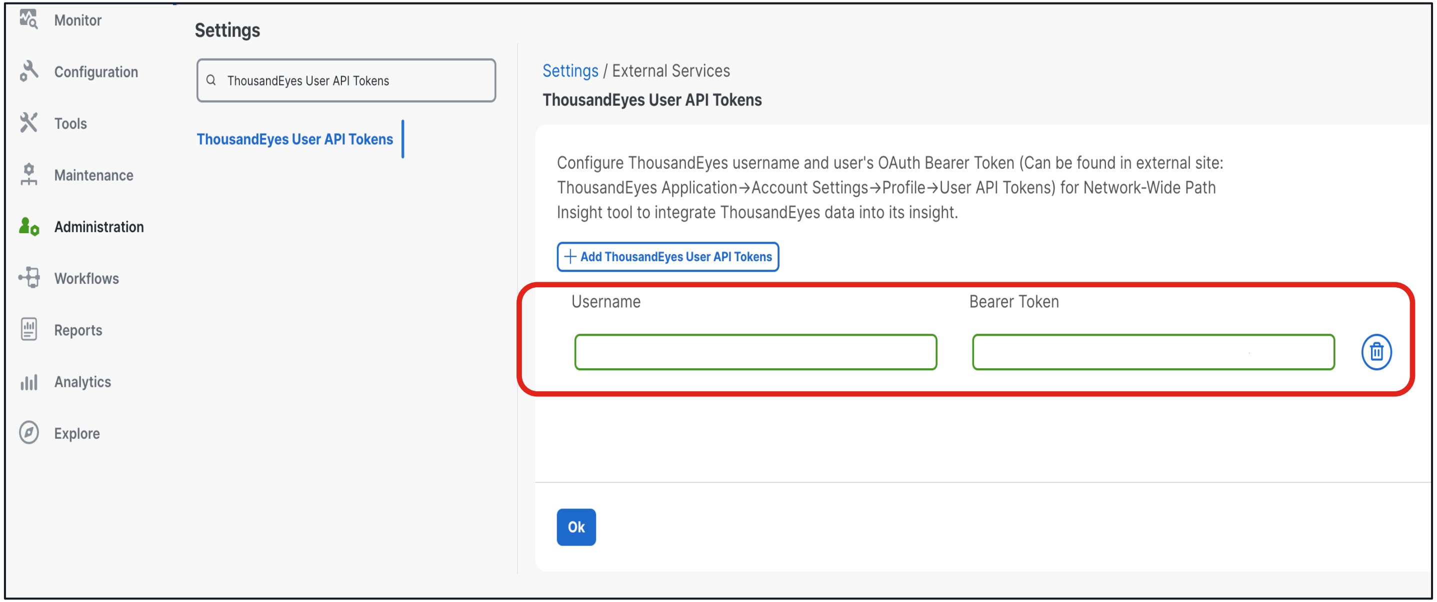
With ThousandEyes Integration, NWPI Trace data and TE probe tests results are auto co-related.

ThousandEyes Path Visualization provides visibility into Internet hops used when accessing the Public/SaaS apps.

NWPI is integrated with Underlay Measurement and Tracing Service (UMTS) to provide underlay insights corelated with TE Insights

Configure ThousandEyes API Token

- For ThousandEyes Insights, configure ThousandEyes Username and OAuth Bearer Token.
- API Token can be fetched from ThousandEyes Dashboard in below path.
  - ThousandEyes Application → Account Settings → Profile → User API Tokens



Settings / External Services

ThousandEyes User API Tokens

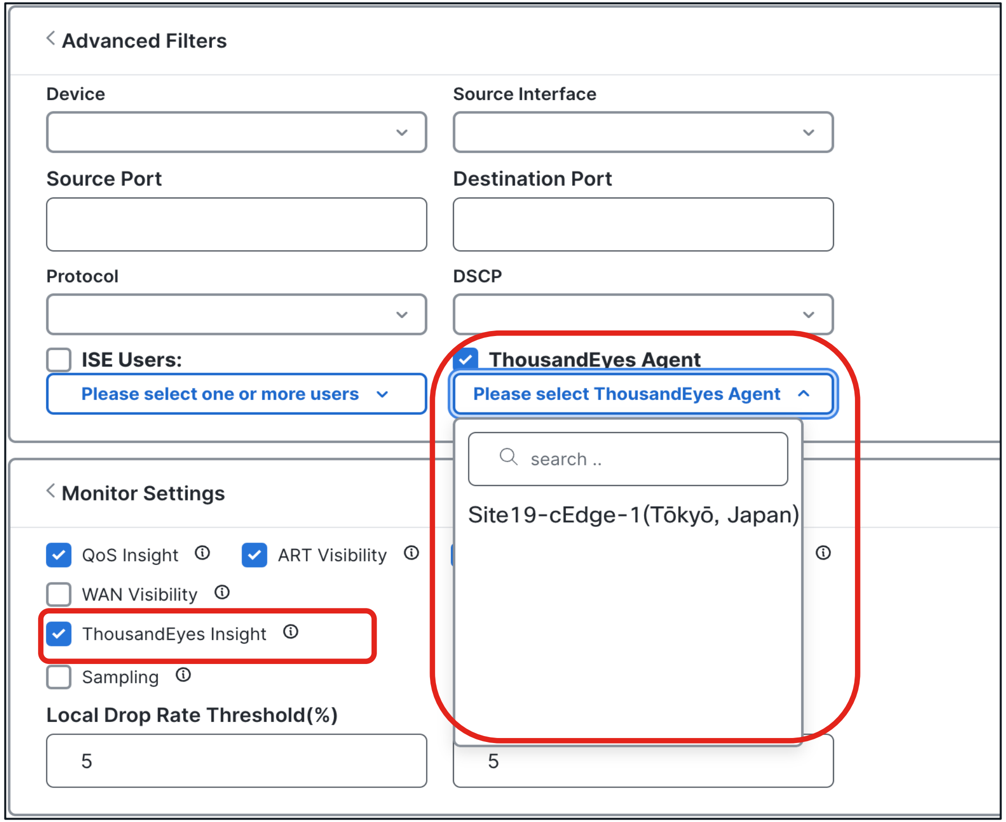
Configure ThousandEyes username and user's OAuth Bearer Token (Can be found in external site: ThousandEyes Application→Account Settings→Profile→User API Tokens) for Network-Wide Path Insight tool to integrate ThousandEyes data into its insight.

Start NWPI Trace

- Select ThousandEyes Agent from Advanced Filters

- TE Agent can be running on the XE SDWAN router or TE Agent can be located behind the router on Service Side.

- Enable ThousandEyes Insights Flag in Monitor Settings. (It is optional, With TE account configured in SD-WAN Manager Admin Settings, this flag is enabled by default)



Advanced Filters

Device

Source Interface

Source Port

Destination Port

Protocol

DSCP

□ ISE Users: Please select one or more users

☑ ThousandEyes Agent: Please select ThousandEyes Agent

search ..

Site19-cEdge-1(Tōkyō, Japan)

Monitor Settings

☑ QoS Insight ☑ ART Visibility

□ WAN Visibility

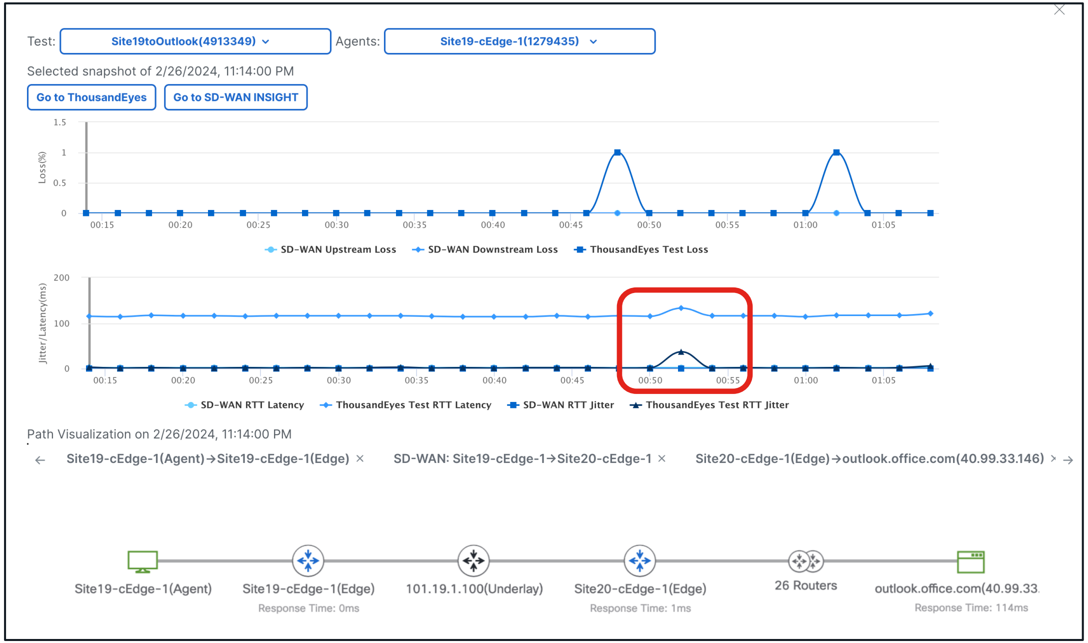
☑ ThousandEyes Insight

□ Sampling

Local Drop Rate Threshold(%): 5

5

User in San Jose Branch complains that they experience slowness when accessing Outlook



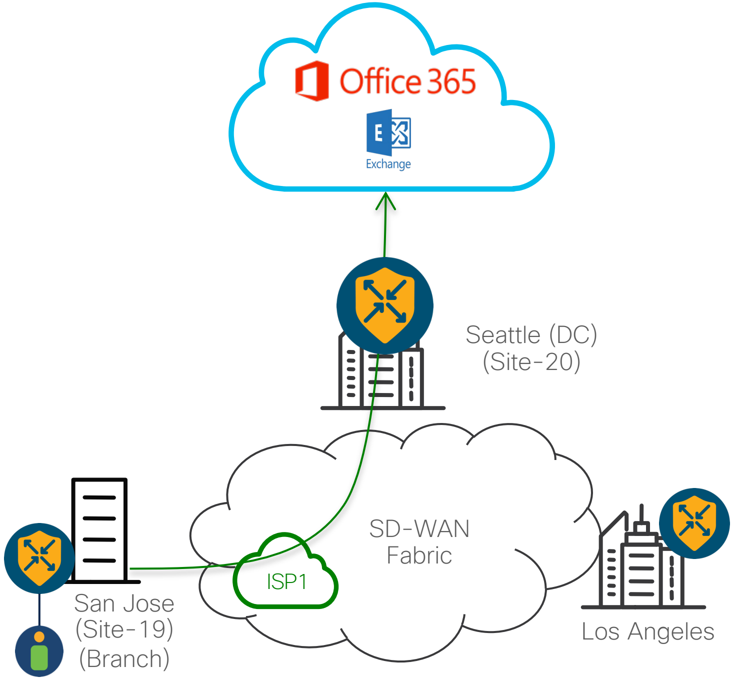
Test: Site19toOutlook(4913349) ⌄ Agents: Site19-cEdge-1(1279435) ⌄

Selected snapshot of 2/26/2024, 11:14:00 PM

Go to ThousandEyes | Go to SD-WAN INSIGHT

Path Visualization on 2/26/2024, 11:14:00 PM

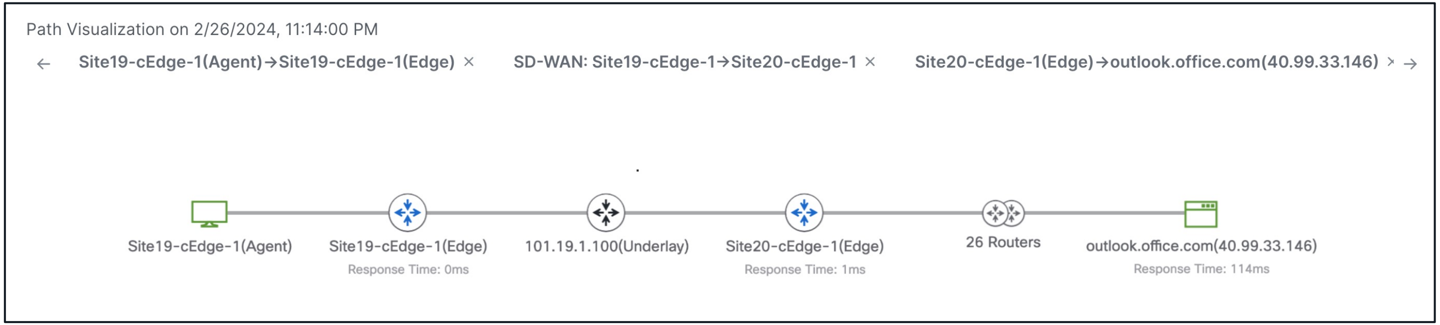
← Site19-cEdge-1(Agent)→Site19-cEdge-1(Edge) × SD-WAN: Site19-cEdge-1→Site20-cEdge-1 × Site20-cEdge-1(Edge)→outlook.office.com(40.99.33.146) × →



End-to-End Path Visualization

In below scenario, Path Visualization is represented for each segments such as

- SD-WAN Branch -> SD-WAN DC
- SD-WAN DC -> SaaS Endpoint

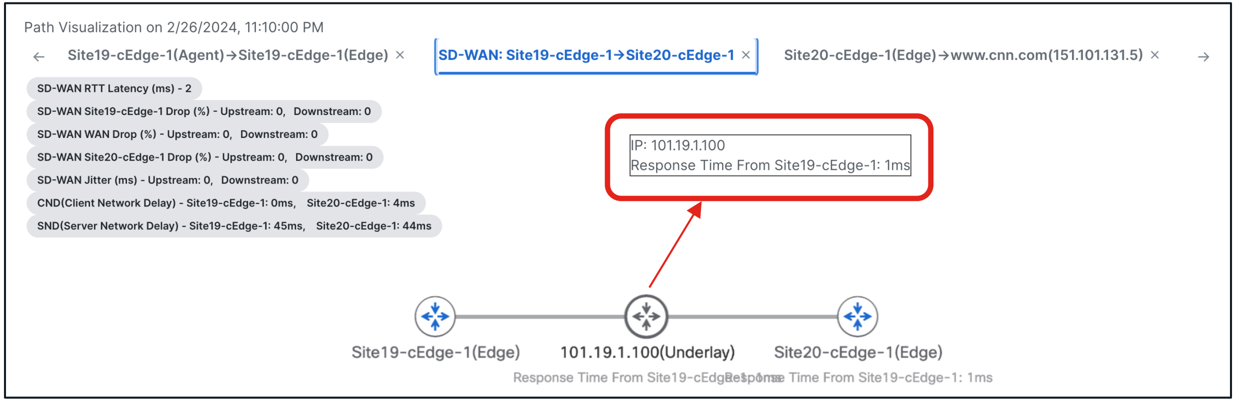


Path Visualization on 2/26/2024, 11:14:00 PM

←
Site19-cEdge-1(Agent)→Site19-cEdge-1(Edge) ×
SD-WAN: Site19-cEdge-1→Site20-cEdge-1 ×
Site20-cEdge-1(Edge)→outlook.office.com(40.99.33.146) ×
→
Site19-cEdge-1(Agent)
Site19-cEdge-1(Edge)
Response Time: 0ms
101.19.1.100(Underlay)
Site20-cEdge-1(Edge)
Response Time: 1ms
26 Routers
outlook.office.com(40.99.33.146)
Response Time: 114ms

Underlay Visibility for SD-WAN Tunnels

- Latency in Underlay Hops corresponding to SD-WAN Tunnel between Branch and DC



Path Visualization on 2/26/2024, 11:10:00 PM

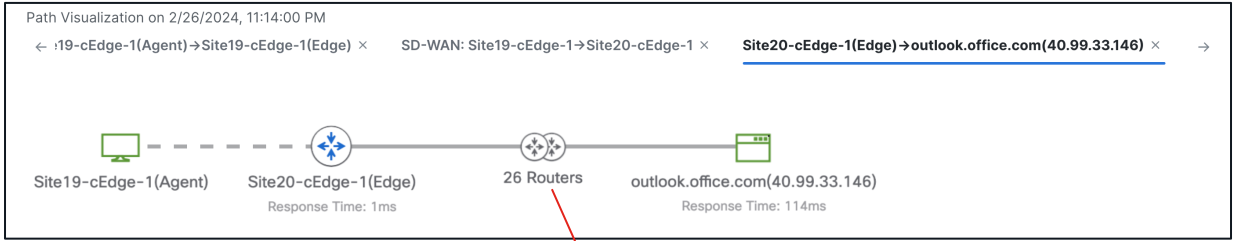
← Site19-cEdge-1(Agent)→Site19-cEdge-1(Edge) × | SD-WAN: Site19-cEdge-1→Site20-cEdge-1 × | Site20-cEdge-1(Edge)→www.cnn.com(151.101.131.5) × →

- SD-WAN RTT Latency (ms) - 2
- SD-WAN Site19-cEdge-1 Drop (%) - Upstream: 0, Downstream: 0
- SD-WAN WAN Drop (%) - Upstream: 0, Downstream: 0
- SD-WAN Site20-cEdge-1 Drop (%) - Upstream: 0, Downstream: 0
- SD-WAN Jitter (ms) - Upstream: 0, Downstream: 0
- CND(Client Network Delay) - Site19-cEdge-1: 0ms, Site20-cEdge-1: 4ms
- SND(Server Network Delay) - Site19-cEdge-1: 45ms, Site20-cEdge-1: 44ms

IP: 101.19.1.100
Response Time From Site19-cEdge-1: 1ms

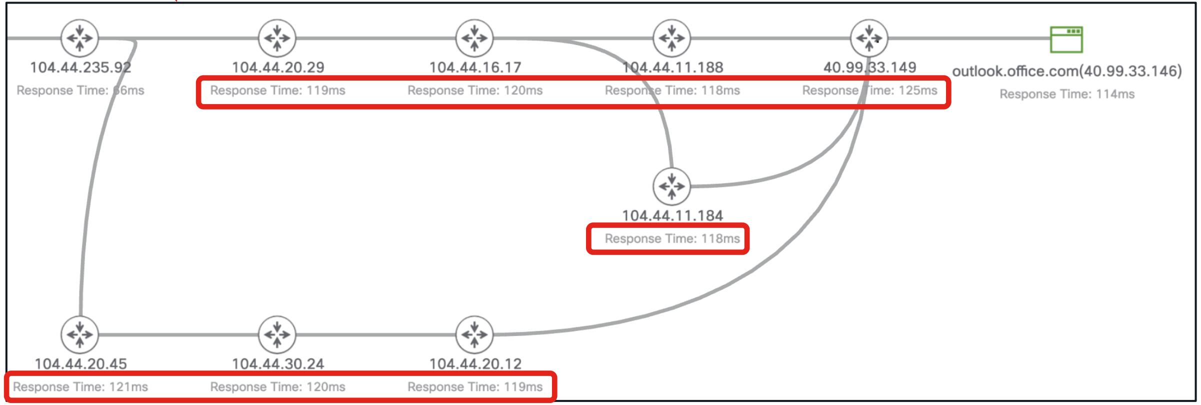
Site19-cEdge-1(Edge)
101.19.1.100(Underlay)
Response Time From Site19-cEdge-1: 1ms
Site20-cEdge-1(Edge)
Response Time From Site19-cEdge-1: 1ms

ThousandEyes Path Visualization for Internet Hops



Path Visualization on 2/26/2024, 11:14:00 PM

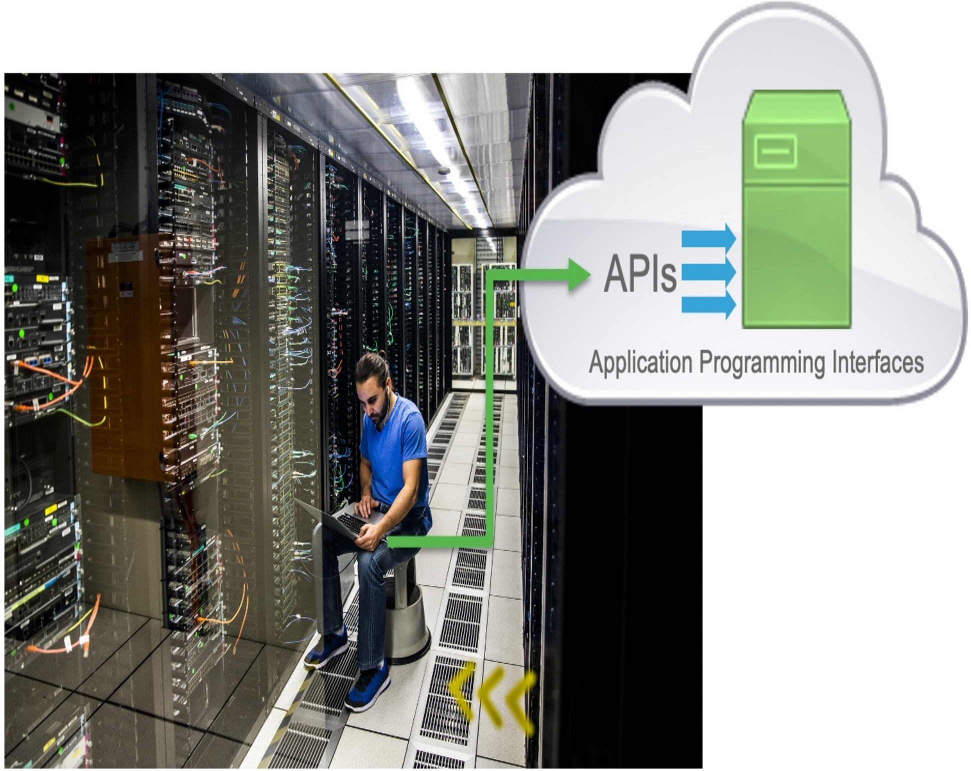
←
19-cEdge-1(Agent)→Site19-cEdge-1(Edge) ×
SD-WAN: Site19-cEdge-1→Site20-cEdge-1 ×
Site20-cEdge-1(Edge)→outlook.office.com(40.99.33.146) ×
→
Site19-cEdge-1(Agent)
Site20-cEdge-1(Edge)
Response Time: 1ms
26 Routers
outlook.office.com(40.99.33.146)
Response Time: 114ms



*Only part of Internet Path is shown in this screenshot

Build your own API-Workflow

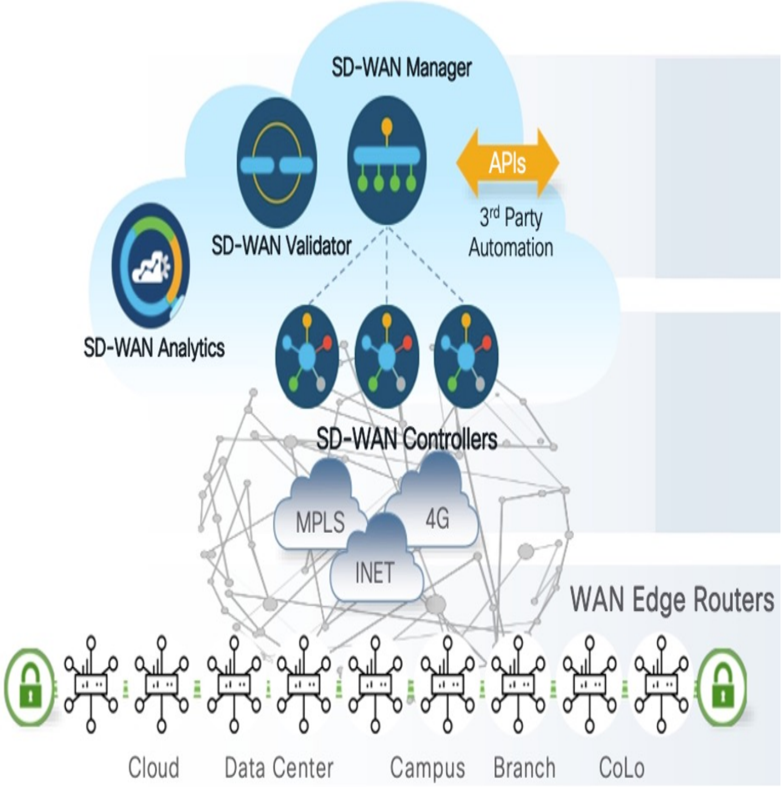
Why API's ?



Challenges

- Manually Performing the Tasks
- Repetition of Tasks
- Prone to Human Errors
- Time consuming
- Need dedicated Human resource

SD-WAN Manager API's

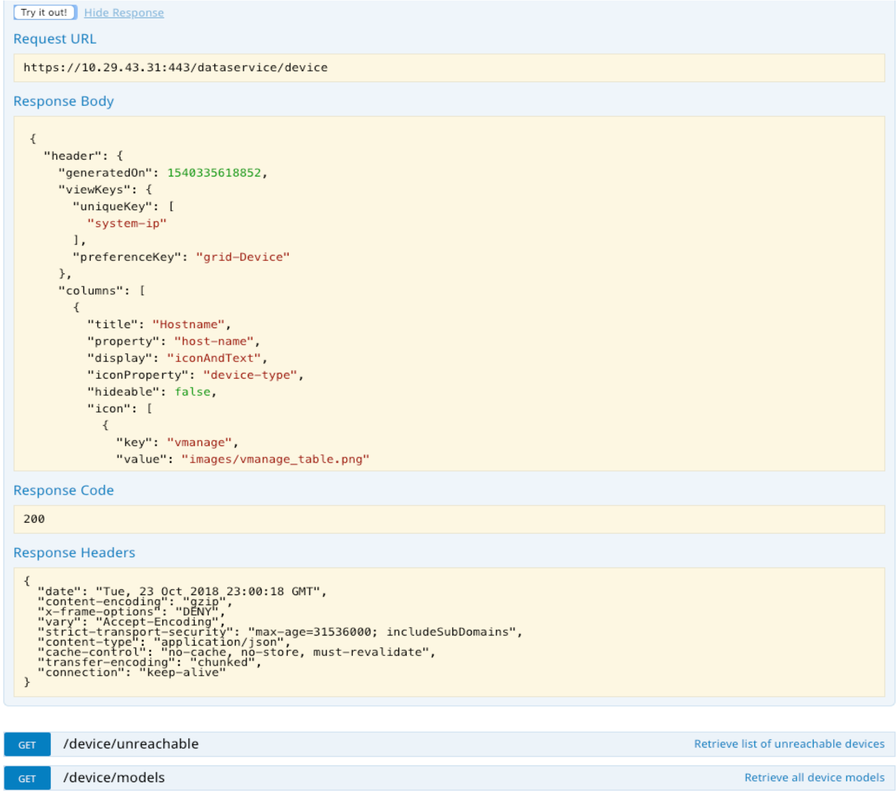


Cisco SD-WAN vManage API is a REST API interface for controlling, configuring, and monitoring the Cisco devices in an overlay network.

- Monitoring device status
- Configuring a device, such as attaching a template to device
- Querying and aggregating device statistics

Base URI: https://<vmanage-server>/dataservice

SD-WAN Manager API’s



Request URL

```
https://10.29.43.31:443/dataservice/device
```

Response Body

```
{
  "header": {
    "generatedOn": 1540335618852,
    "viewKeys": {
      "uniqueKey": [
        "system-ip"
      ],
      "preferenceKey": "grid-Device"
    },
    "columns": [
      {
        "title": "Hostname",
        "property": "host-name",
        "display": "iconAndText",
        "iconProperty": "device-type",
        "hideable": false,
        "icon": [
          {
            "key": "vmanage",
            "value": "images/vmanage_table.png"
```

Response Code

```
200
```

Response Headers

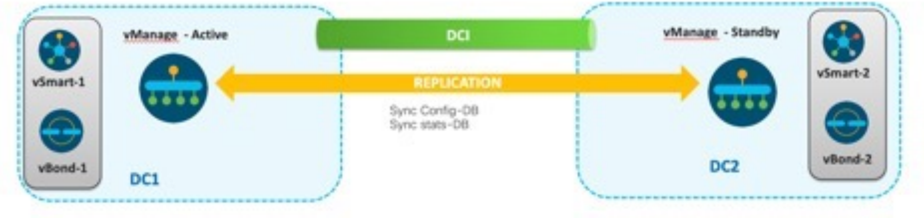
```
{
  "date": "Tue, 23 Oct 2018 23:00:18 GMT",
  "content-encoding": "gzip",
  "x-frame-options": "DENY",
  "vary": "Accept-Encoding",
  "strict-transport-security": "max-age=31536000; includeSubDomains",
  "content-type": "application/json",
  "cache-control": "no-cache, no-store, must-revalidate",
  "transfer-encoding": "chunked",
  "connection": "keep-alive"
}
```

GET /device/unreachable Retrieve list of unreachable devices

GET /device/models Retrieve all device models

- Swagger-based documentation is accessible through your vManage instance at https://IP-ADDRESS:port/apidocs.

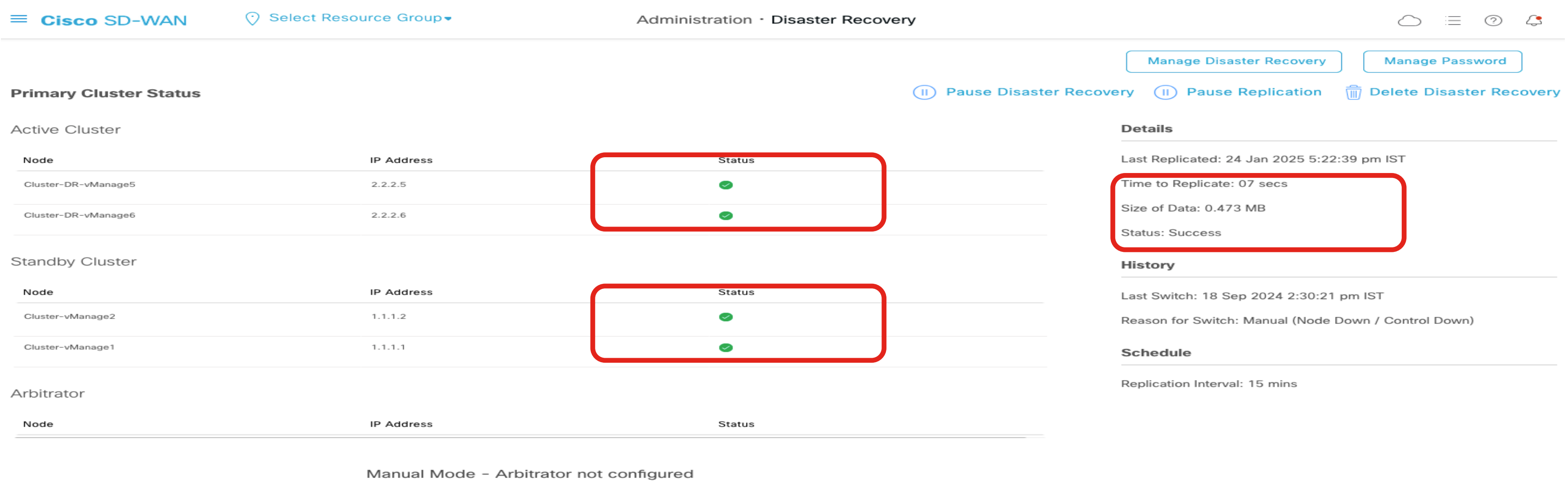
Need of Workflow



Courtesy : Google Images

Precheck MOP(Method of Procedure)

1. Perform a status check by choosing Administration > Disaster Recovery. (On both Active & Standby)
    - Status is seen as green
    - Details section should be showing “Success”



Primary Cluster Status

Active Cluster

Node	IP Address	Status
Cluster-DR-vManage5	2.2.2.5	✓
Cluster-DR-vManage6	2.2.2.6	✓

Standby Cluster

Node	IP Address	Status
Cluster-vManage2	1.1.1.2	✓
Cluster-vManage1	1.1.1.1	✓

Arbitrator

Node	IP Address	Status

Manual Mode - Arbitrator not configured

Details

Last Replicated: 24 Jan 2025 5:22:39 pm IST

Time to Replicate: 07 secs

Size of Data: 0.473 MB

Status: Success

History

Last Switch: 18 Sep 2024 2:30:21 pm IST

Reason for Switch: Manual (Node Down / Control Down)

Schedule

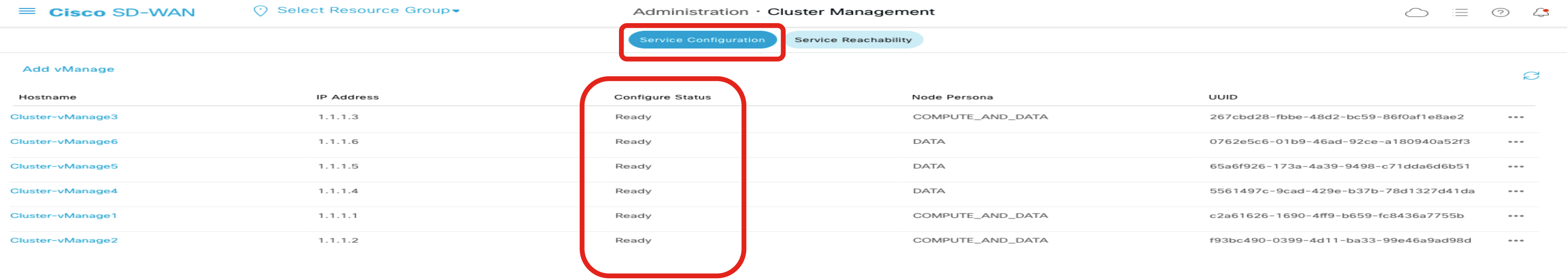
Replication Interval: 15 mins

Precheck MOP(Method of Procedure)

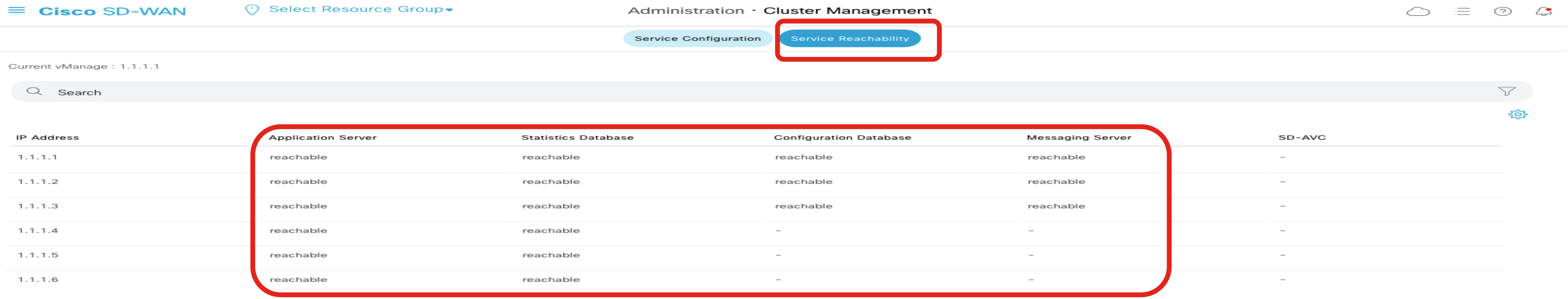
2. Perform a check on the services by choosing Administration > Cluster Management

- **Service Configuration** should show status of the Nodes as “Ready”

- **Service Reachability** should show all the services as reachable.



Hostname	IP Address	Configure Status	Node Persona	UUID
Cluster-vManage3	1.1.1.3	Ready	COMPUTE_AND_DATA	267cbd28-fbbe-48d2-bc59-86f0af1e8ae2
Cluster-vManage6	1.1.1.6	Ready	DATA	0762e5c6-01b9-46ad-92ce-a180940a52f3
Cluster-vManage5	1.1.1.5	Ready	DATA	65a6f926-173a-4a39-9498-c71dda6d6b51
Cluster-vManage4	1.1.1.4	Ready	DATA	5561497c-9cad-429e-b37b-78d1327d41da
Cluster-vManage1	1.1.1.1	Ready	COMPUTE_AND_DATA	c2a61626-1690-4ff9-b659-fc8436a7755b
Cluster-vManage2	1.1.1.2	Ready	COMPUTE_AND_DATA	f93bc490-0399-4d11-ba33-99e46a9ad98d



Current vManage : 1.1.1.1

IP Address	Application Server	Statistics Database	Configuration Database	Messaging Server	SD-AVC
1.1.1.1	reachable	reachable	reachable	reachable	-
1.1.1.2	reachable	reachable	reachable	reachable	-
1.1.1.3	reachable	reachable	reachable	reachable	-
1.1.1.4	reachable	reachable	-	-	-
1.1.1.5	reachable	reachable	-	-	-
1.1.1.6	reachable	reachable	-	-	-

Precheck MOP(Method of Procedure)

3. Controller full mesh verification

   - Serial list check :

   In vbond “show orchestrator valid-vsmart” should be same across all validators
   [total = no. of vmanage nodes + vsmart nodes]

4. Send to controller should pass without any issues

API Workflow

1. Check the status of the Nodes on the DR page :

/dataservice/disasterrecovery/localdc

Sample Output :

```
[
 {
   " dcName" : " DC2" ,
   " nodes" : [
     {
       " hostName" : " Cluster-vManage2" ,
       " deviceIP" : " 1.1.1.2" ,
       " state" : " UP"
     },
     {
       " hostName" : " Cluster-vManage1" ,
       " deviceIP" : " 1.1.1.1" ,
       " state" : " UP"
     },
<Snipped>
   " dcName" : " DC1 (Primary)" ,
   " nodes" : [
     {
       " hostName" : " Cluster-DR-vManage5" ,
       " deviceIP" : " 2.2.2.5" ,
       " state" : " UP"
     },
     {
       " hostName" : " Cluster-DR-vManage6" ,
       " deviceIP" : " 2.2.2.6" ,
       " state" : " UP"
     },
<Snipped>
     }
   ]
 }
]
```

API Workflow

2. Check the Status if it is Success :

/dataservice/disasterrecovery/details

Sample output :

```
{
 " replicationDetails" : [
   {
     " lastReplicated" : 1729598480308,
     " exportDuration" : " 07 secs" ,
     " exportSize" : " 0.312 MB" ,
     " replicationStatus" : ”success"                    <<< Check for Success
   }
 ]
}
```

3. Check the status of the Nodes who’s Primary and who’s Secondary :

/dataservice/disasterrecovery/drstatus

Sample Output :

```
[
 {
   " mgmtIPAddress" : " 1.1.1.1" ,
   " dcPersonality" : " secondary"
 },
 {
   " mgmtIPAddress" : " 2.2.2.1" ,
   " dcPersonality" : " primary"
 }
]
```

API Workflow

4. Check for Cluster health :
(Check if state for all nodes is Ready)

/dataservice/clusterManagement/list

Sample Output :

```
 " data" : [
  {
    " isIPConfigured" : true,
    " data" : [
     {
       " vmanageID" : " 3" ,
       " configJson" : {
         " uuid" : " 1158cc4d-b77d-4d96-8e68-5d41a13b57b9" ,
         " host-name" : " Cluster-DR-vManage4" ,
         " deviceIP" : " 2.2.2.4" ,
         " state" : " Ready" ,
         " container-manager" : false,
         " persona" : " DATA"
       }
     },
     {
       " vmanageID" : " 4" ,
       " configJson" : {
         " uuid" : " 80740a8c-170c-4a43-8b62-3a8d6174eafe" ,
         " host-name" : " Cluster-DR-vManage5" ,
         " deviceIP" : " 2.2.2.5" ,
         " state" : " Ready" ,
         " container-manager" : false,
         " persona" : " DATA"
       }
     },
<Snipped>
    ]
  }
 ]
}
```

API Workflow

5. Check for the Cluster services health : (Check if all services are True)

```
" data" : [
   {
     " deviceIP" : " 2.2.2.1"
   },
   {
     " statistics-db" : true,
     " application-server" : true,
     " messaging-server" : true,
     " configuration-db" : true,
     " deviceIP" : " 2.2.2.1"
   },
   {
     " statistics-db" : true,
     " application-server" : true,
     " messaging-server" : true,
     " configuration-db" : true,
     " deviceIP" : " 2.2.2.2"
   },
   {
<Snipped>
```

API Workflow

6. Check for Serial list (show orchestrator valid-vsmart) :

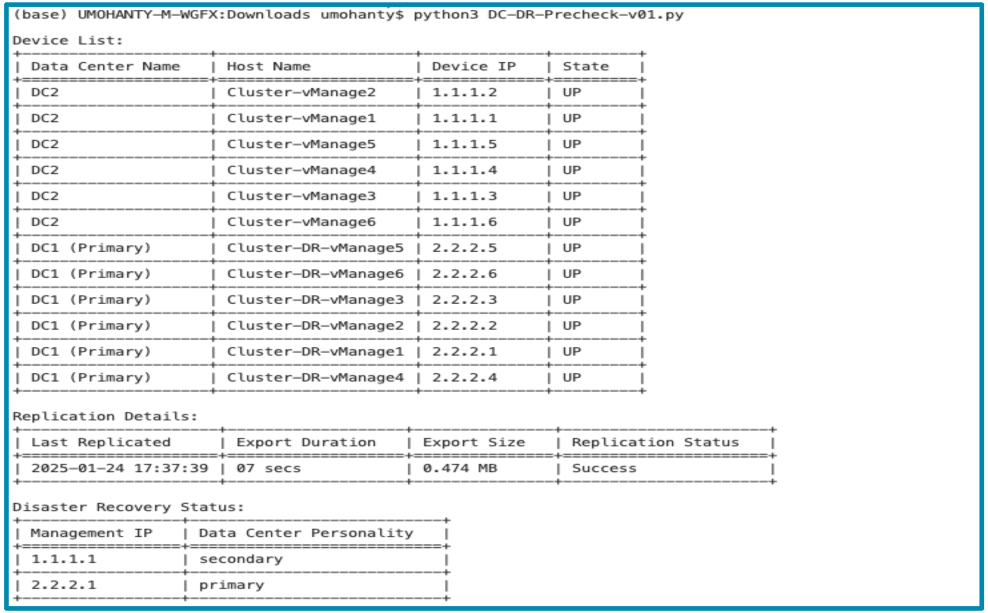
dataservice/device/orchestrator/validvsmarts?deviceId=192.168.88.21

NOTE : Need to run this for all the SD-WAN Validator system IP’s.
The Serial list should match on all the Validators

```
 " data" : [
   {
     " vdevice-dataKey" : " 192.168.88.21-
16DEA96BCF940761954EA5AEE34F25735A399180" ,
     " vdevice-name" : " 192.168.88.21" ,
     " serial-number" : " 16DEA96BCF940761954EA5AEE34F25735A399180" ,
     " lastupdated" : 1729600844665,
     " vdevice-host-name" : " Cluster-vbond1-DC"
   },
   {
     " vdevice-dataKey" : " 192.168.88.21-
1D08B5AA3D691FFF1A575472DC09A8E8327EC858" ,
     " vdevice-name" : " 192.168.88.21" ,
     " serial-number" : " 1D08B5AA3D691FFF1A575472DC09A8E8327EC858" ,
     " lastupdated" : 1729600844665,
     " vdevice-host-name" : " Cluster-vbond1-DC"
   },
<Snipped>
```

API Workflow

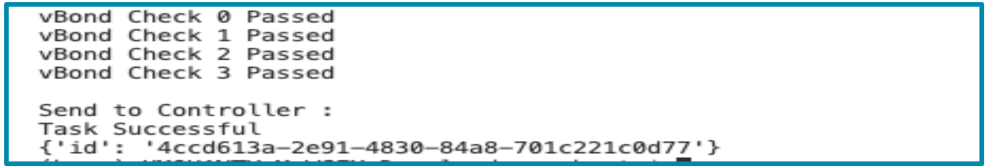
https://github.com/umohanty/DR-Precheck



```
(base) UMOHANTY-M-WGFX:Downloads umohanty$ python3 DC-DR-Precheck-v01.py
Device List:
+--------------------+---------------------+-------------+---------+
| Data Center Name   | Host Name           | Device IP   | State   |
+====================+=====================+=============+=========+
| DC2                | Cluster-vManage2    | 1.1.1.2     | UP      |
+--------------------+---------------------+-------------+---------+
| DC2                | Cluster-vManage1    | 1.1.1.1     | UP      |
+--------------------+---------------------+-------------+---------+
| DC2                | Cluster-vManage5    | 1.1.1.5     | UP      |
+--------------------+---------------------+-------------+---------+
| DC2                | Cluster-vManage4    | 1.1.1.4     | UP      |
+--------------------+---------------------+-------------+---------+
| DC2                | Cluster-vManage3    | 1.1.1.3     | UP      |
+--------------------+---------------------+-------------+---------+
| DC2                | Cluster-vManage6    | 1.1.1.6     | UP      |
+--------------------+---------------------+-------------+---------+
| DC1 (Primary)      | Cluster-DR-vManage5 | 2.2.2.5     | UP      |
+--------------------+---------------------+-------------+---------+
| DC1 (Primary)      | Cluster-DR-vManage6 | 2.2.2.6     | UP      |
+--------------------+---------------------+-------------+---------+
| DC1 (Primary)      | Cluster-DR-vManage3 | 2.2.2.3     | UP      |
+--------------------+---------------------+-------------+---------+
| DC1 (Primary)      | Cluster-DR-vManage2 | 2.2.2.2     | UP      |
+--------------------+---------------------+-------------+---------+
| DC1 (Primary)      | Cluster-DR-vManage1 | 2.2.2.1     | UP      |
+--------------------+---------------------+-------------+---------+
| DC1 (Primary)      | Cluster-DR-vManage4 | 2.2.2.4     | UP      |
+--------------------+---------------------+-------------+---------+

Replication Details:
+---------------------+-------------------+---------------+----------------------+
| Last Replicated     | Export Duration   | Export Size   | Replication Status   |
+=====================+===================+===============+======================+
| 2025-01-24 17:37:39 | 07 secs           | 0.474 MB      | Success              |
+---------------------+-------------------+---------------+----------------------+

Disaster Recovery Status:
+-----------------+---------------------------+
| Management IP   | Data Center Personality   |
+=================+===========================+
| 1.1.1.1         | secondary                 |
+-----------------+---------------------------+
| 2.2.2.1         | primary                   |
+-----------------+---------------------------+
```



```
   vBond Check 0 Passed
   vBond Check 1 Passed
   vBond Check 2 Passed
   vBond Check 3 Passed

   Send to Controller :
   Task Successful
   {'id': '4ccd613a-2e91-4830-84a8-701c221c0d77'}
```

Key Takeaways

Key Takeaways

- Overview of SD-WAN
- Monitoring & Troubleshooting Challenges
- Cisco SD-WAN Manager Tools & Use case scenario’s
- Build your own API workflow

DR Failover prechecks

Webex App

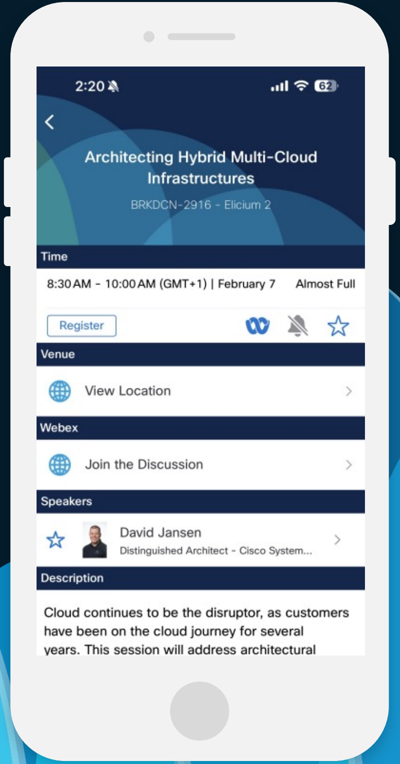
Questions?

Use the Webex app 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 the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



2:20

Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Register

Venue

View Location

Webex

Join the Discussion

Speakers

David Jansen
Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

cisco Live!

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

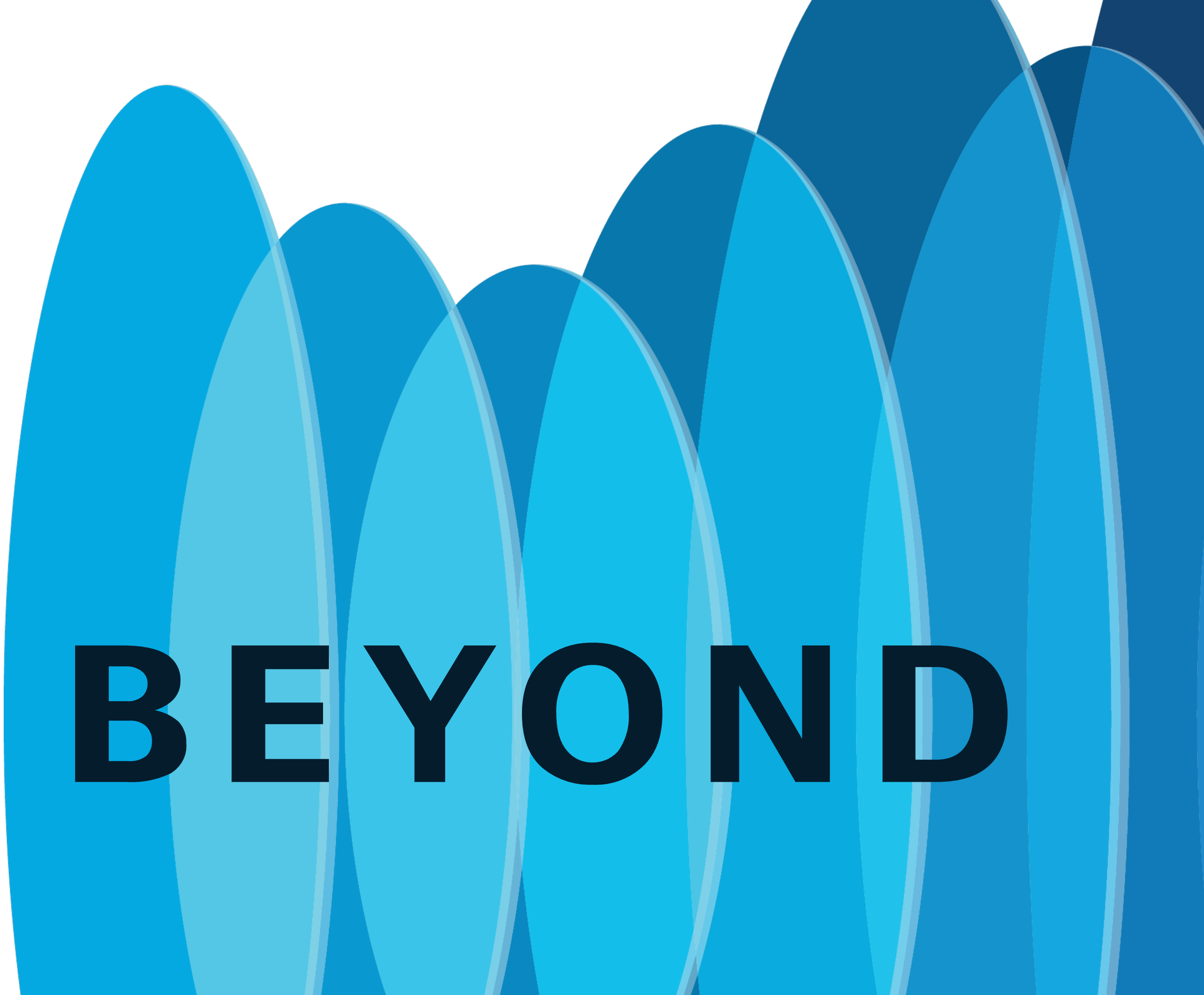
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: umohanty@cisco.com

Thank you

cisco Live!



GO BEYOND