

Expedite your Troubleshooting with SD-WAN Manager Tools

cisco Live !

Uma Sankar Mohanty
Software Engineering Technical Leader

Session ID: BRKTRS-2595

Cisco Webex App

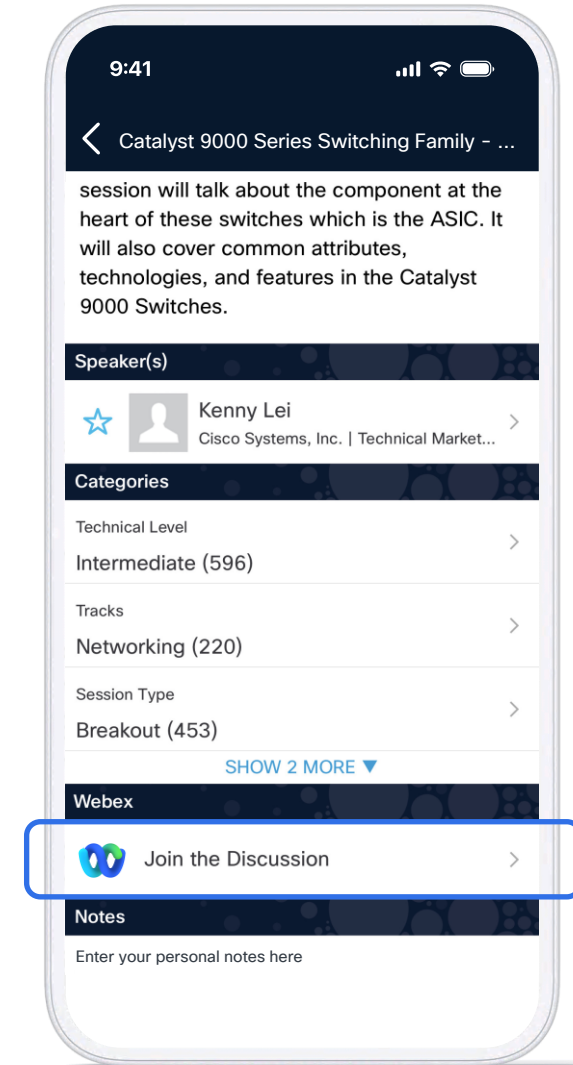
Questions?

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

How

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

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKTRS-2595>

Agenda

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



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 APIs 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.

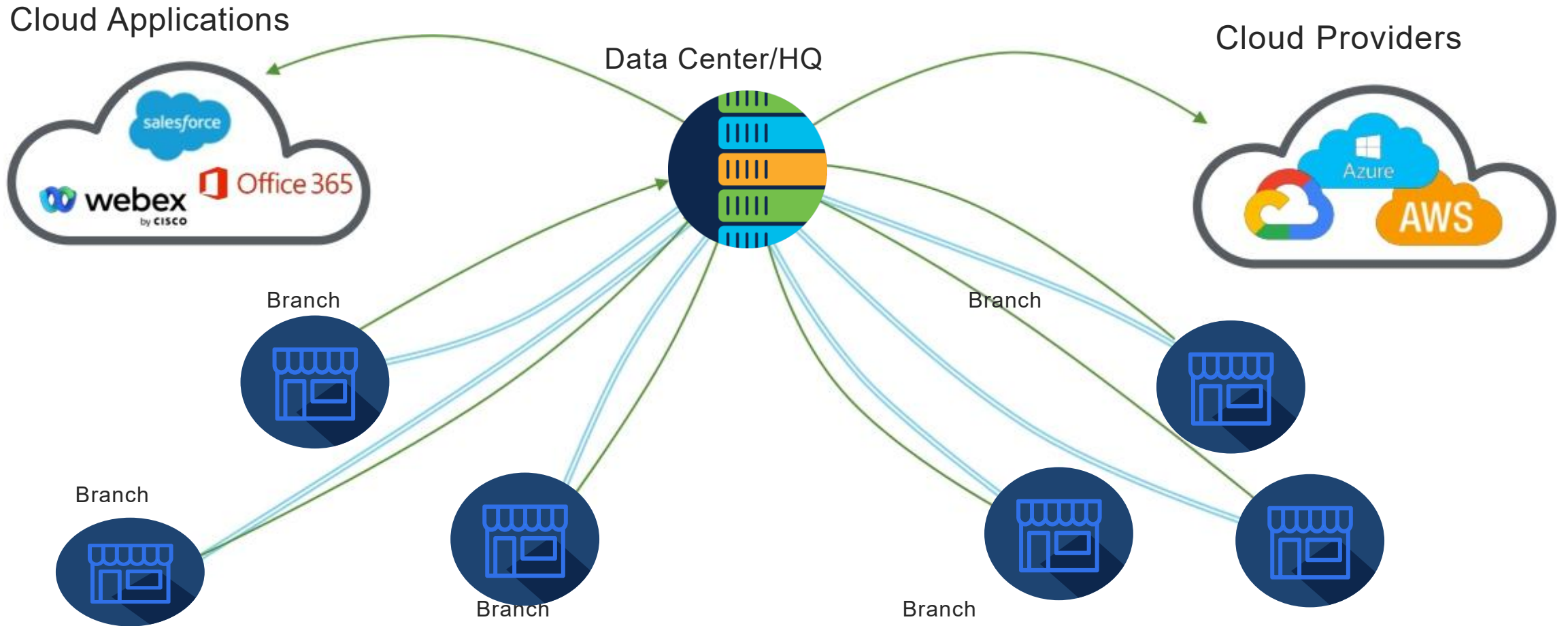
Session non-objective

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

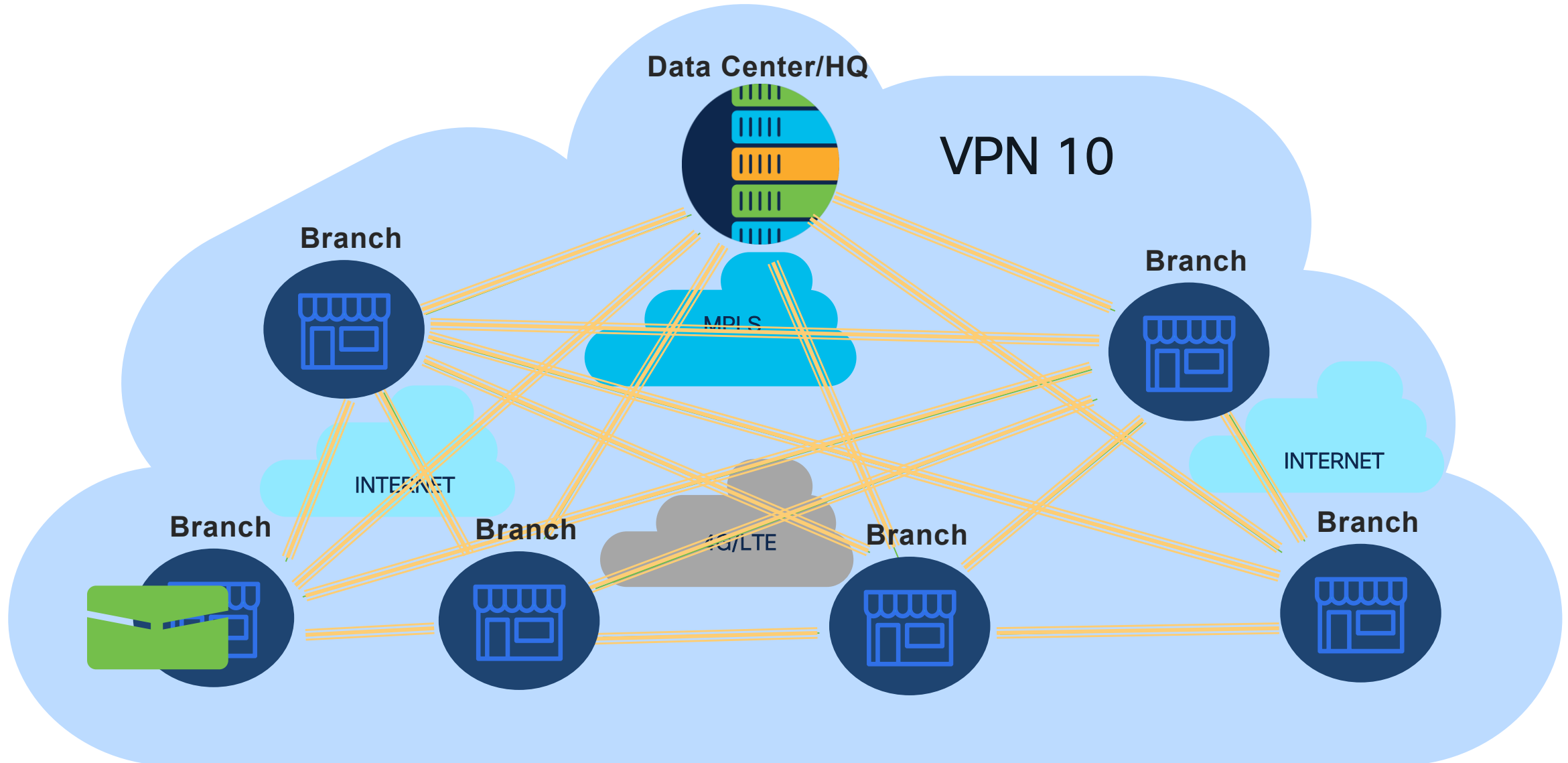
Why SD-WAN?

The hardware-based WAN of yesterday

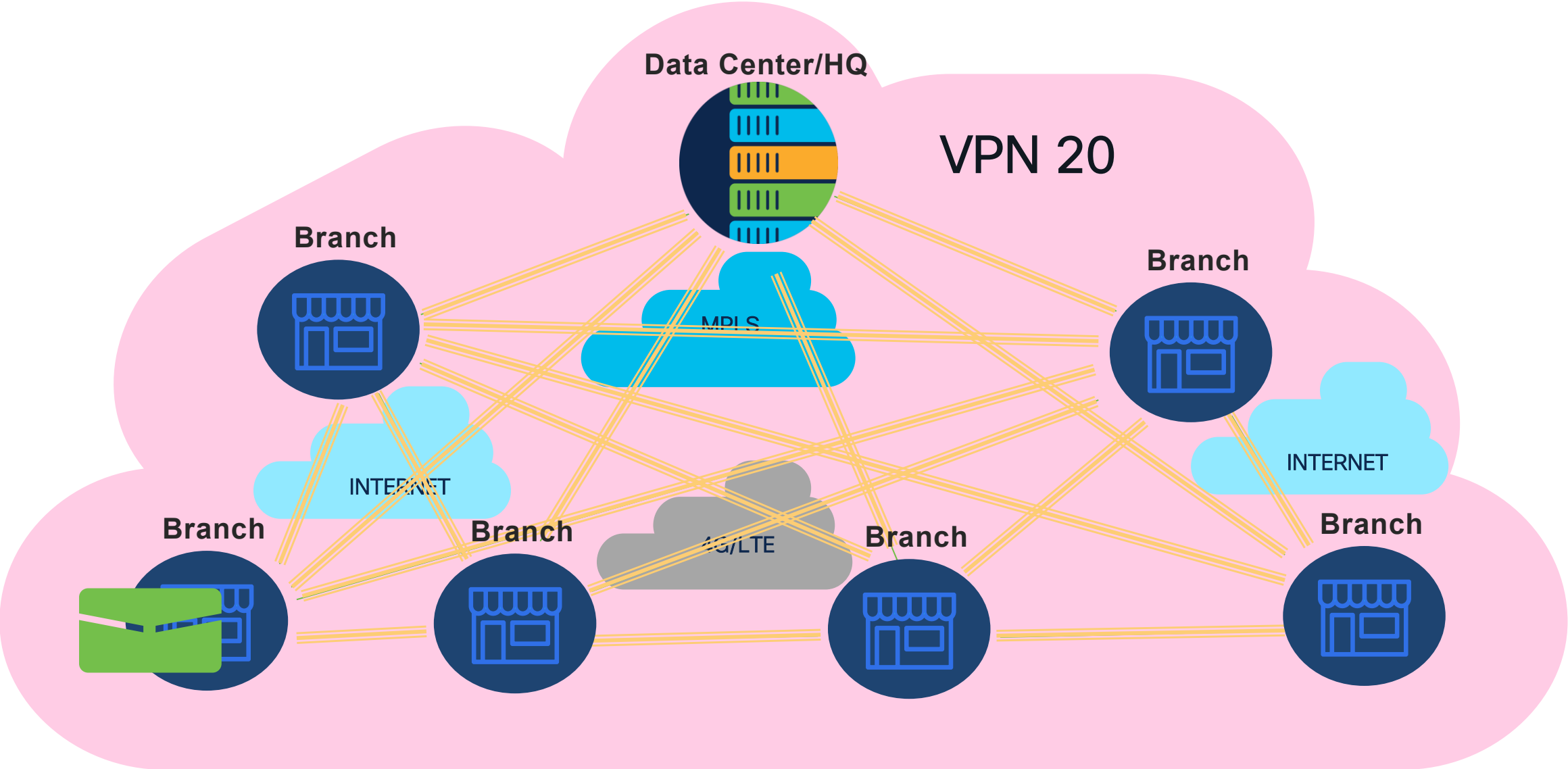
- Doesn't keep up with the needs of today



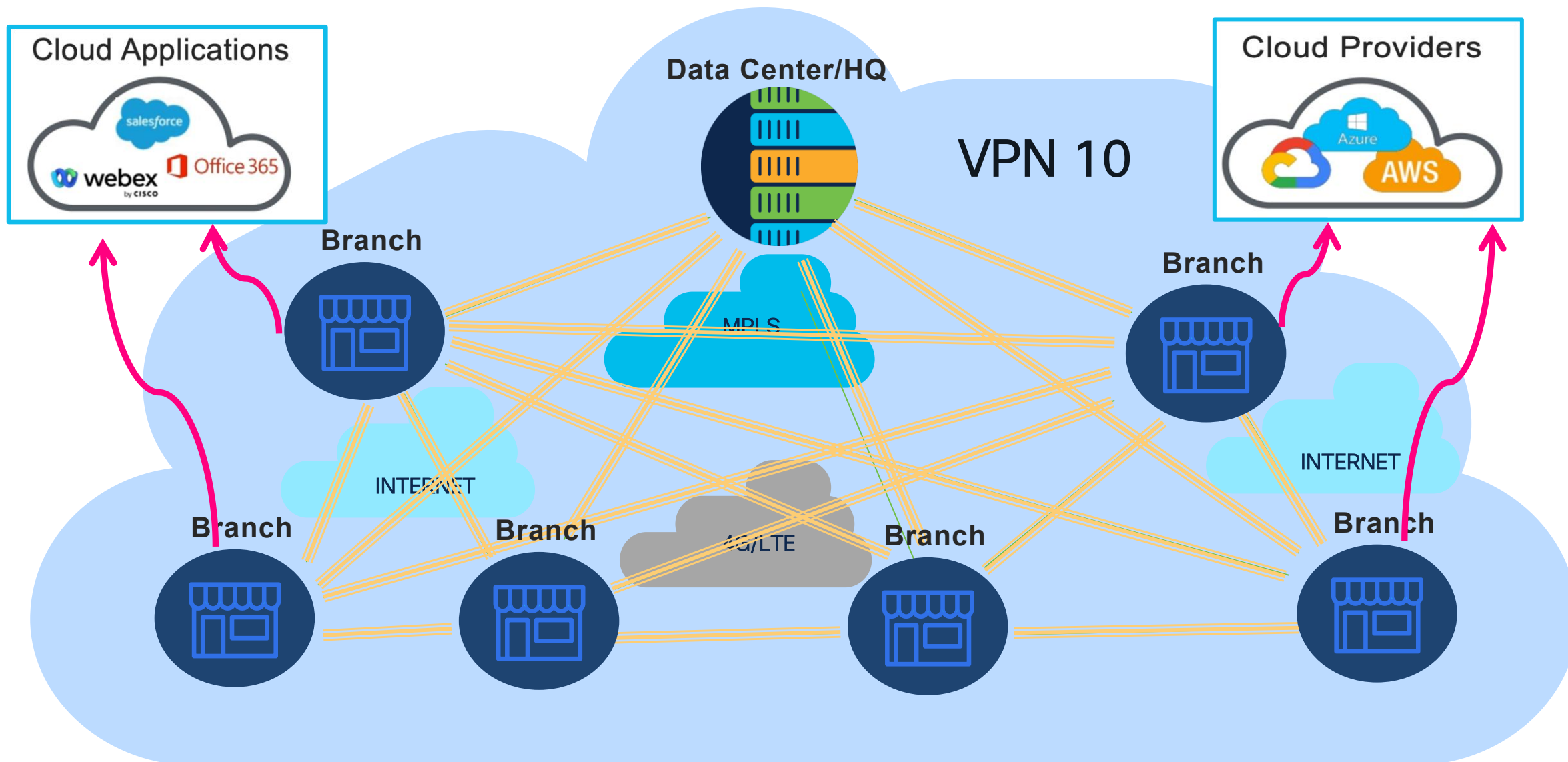
Cisco SD-WAN: software approach



Cisco SD-WAN: software approach



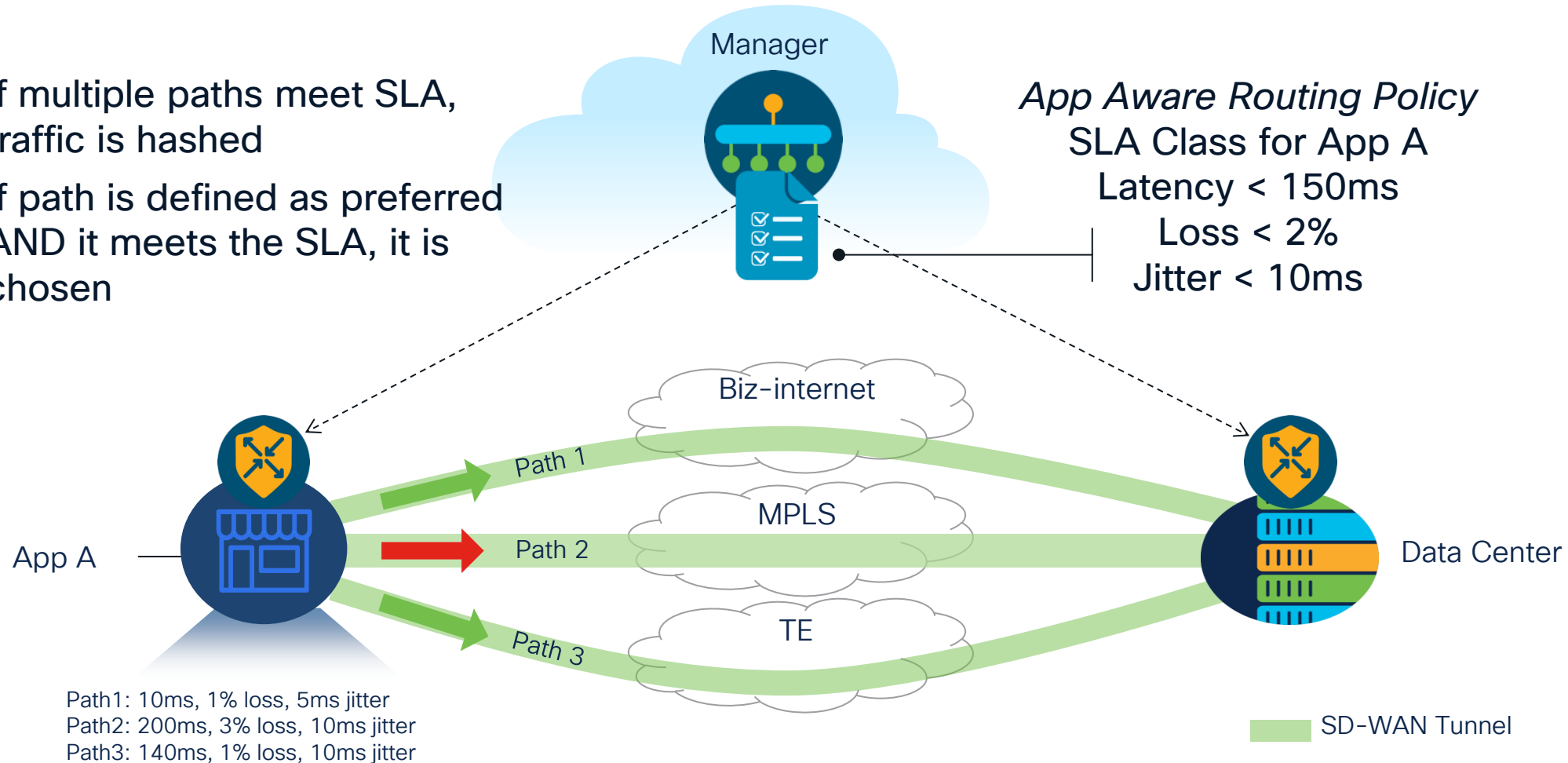
Cisco SD-WAN: software approach



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

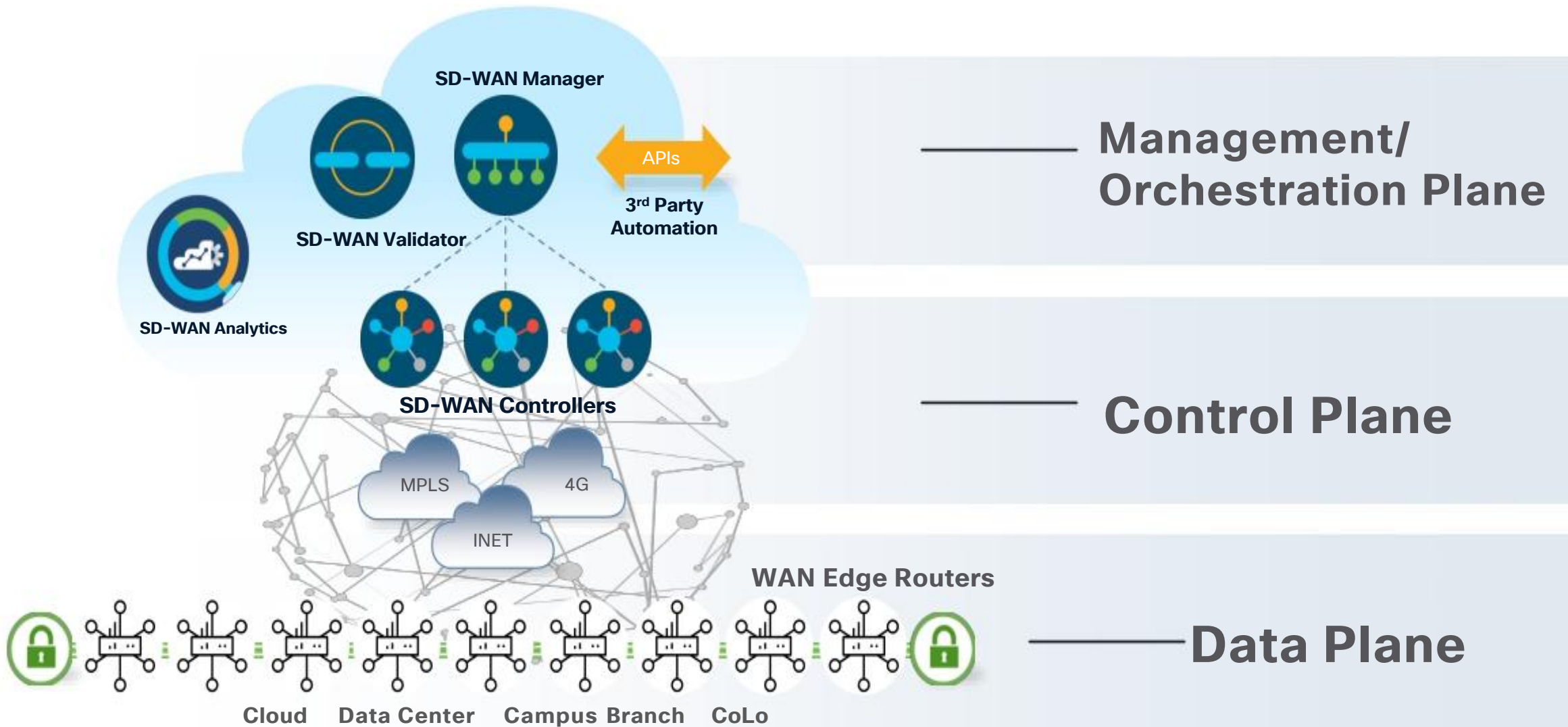




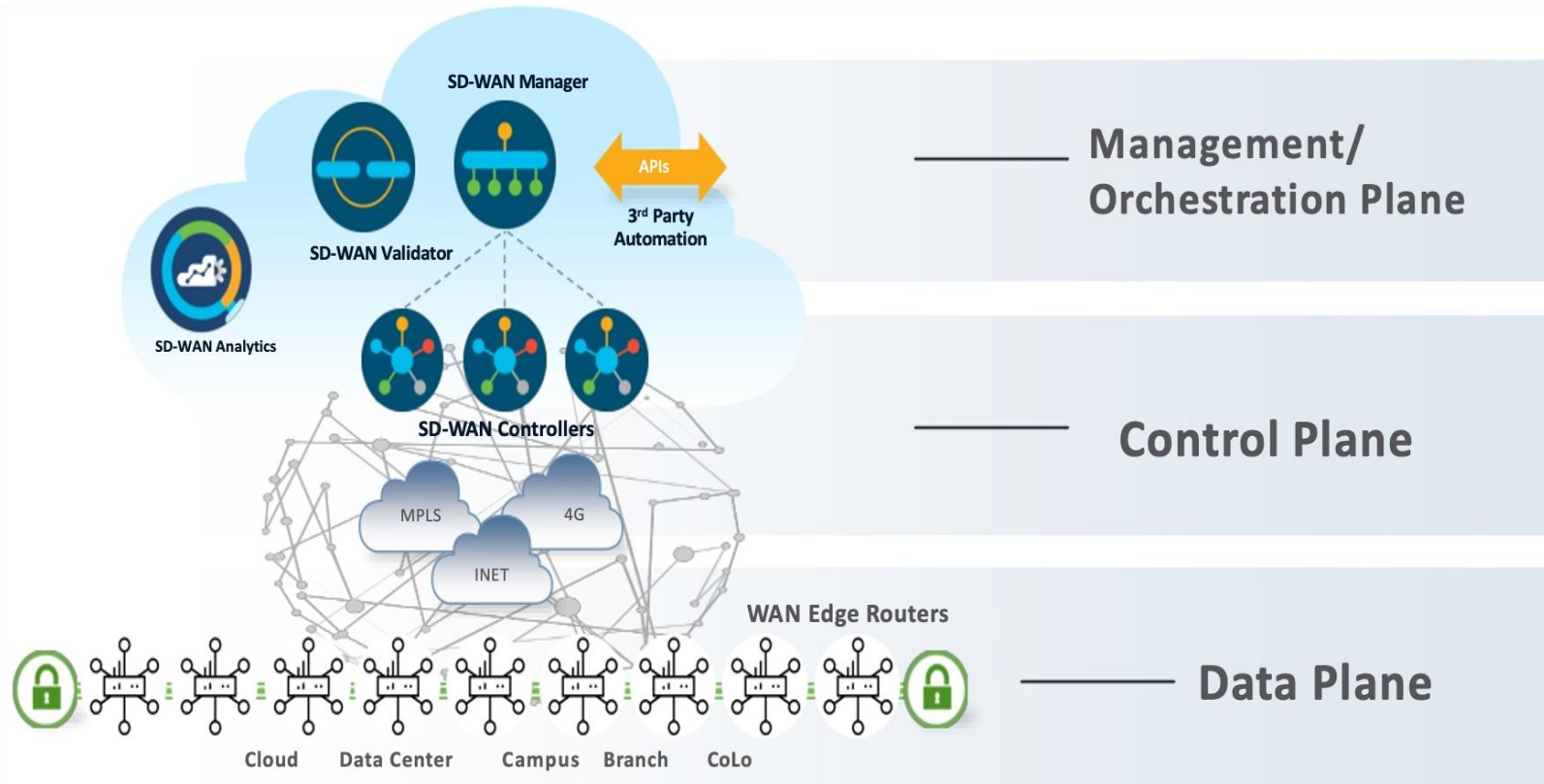
What is SD-WAN?

Solution Architecture

Cisco SD-WAN solution overview



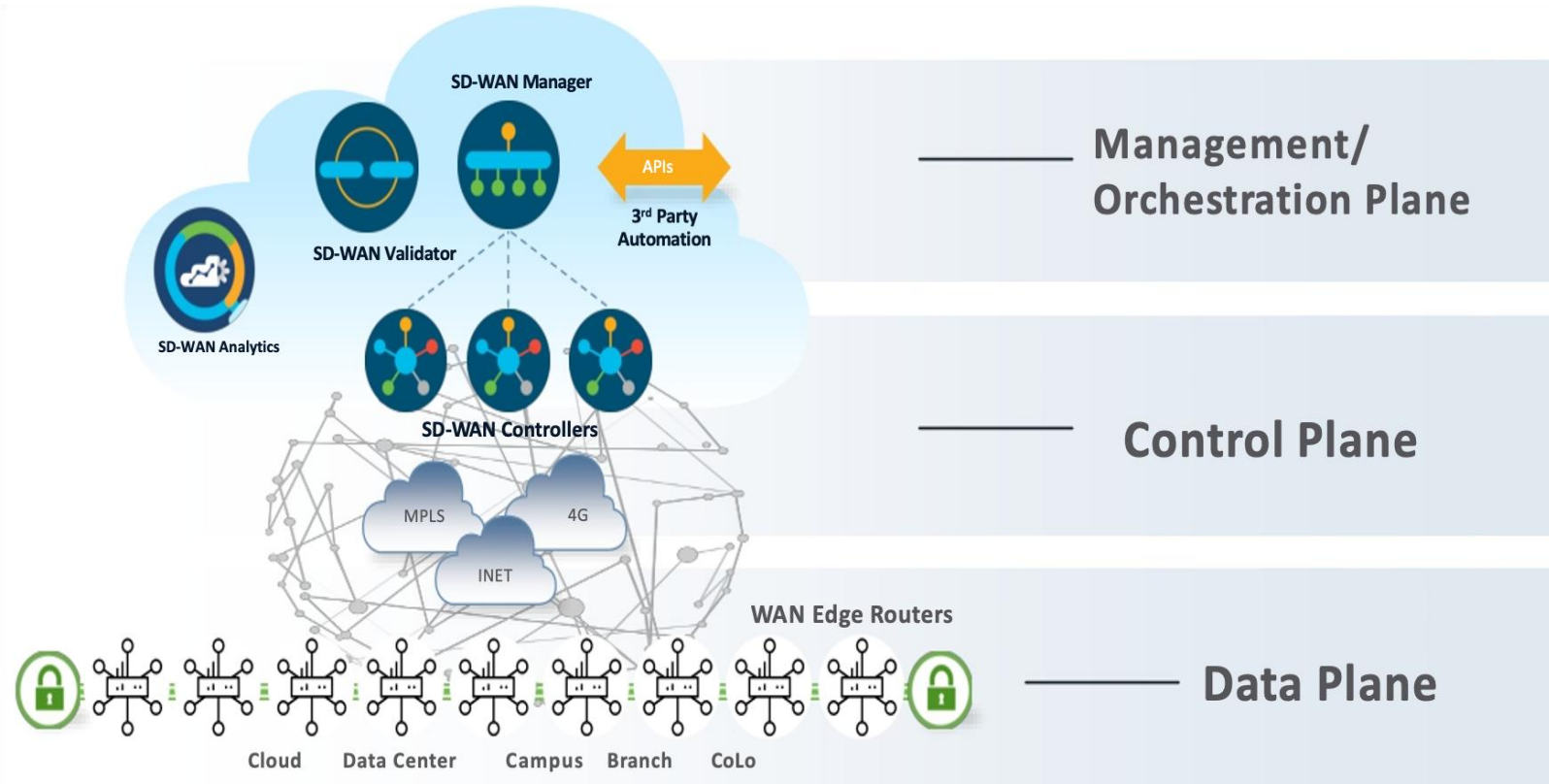
Cisco SD-WAN solution overview



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

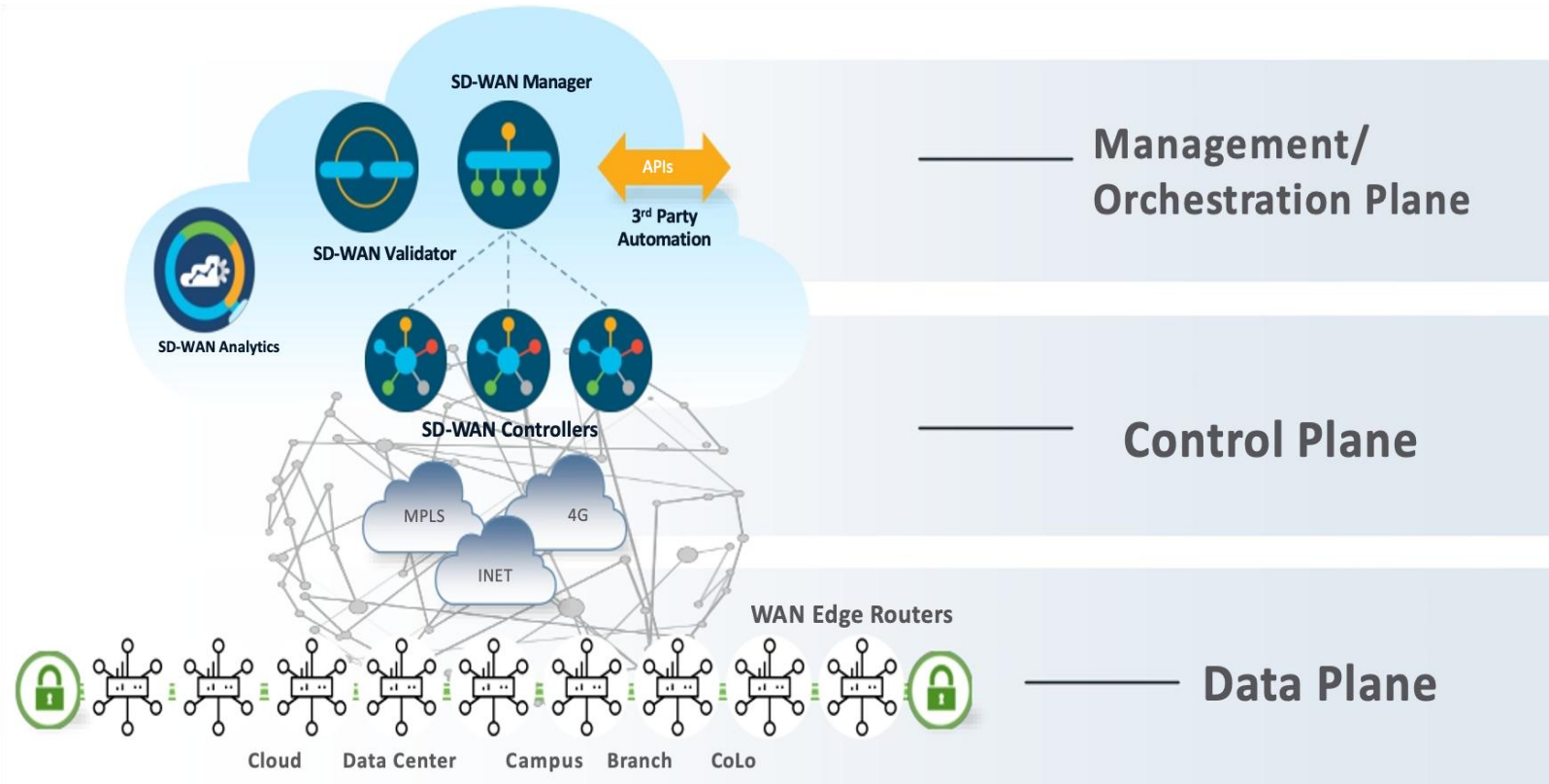
Cisco SD-WAN solution overview



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

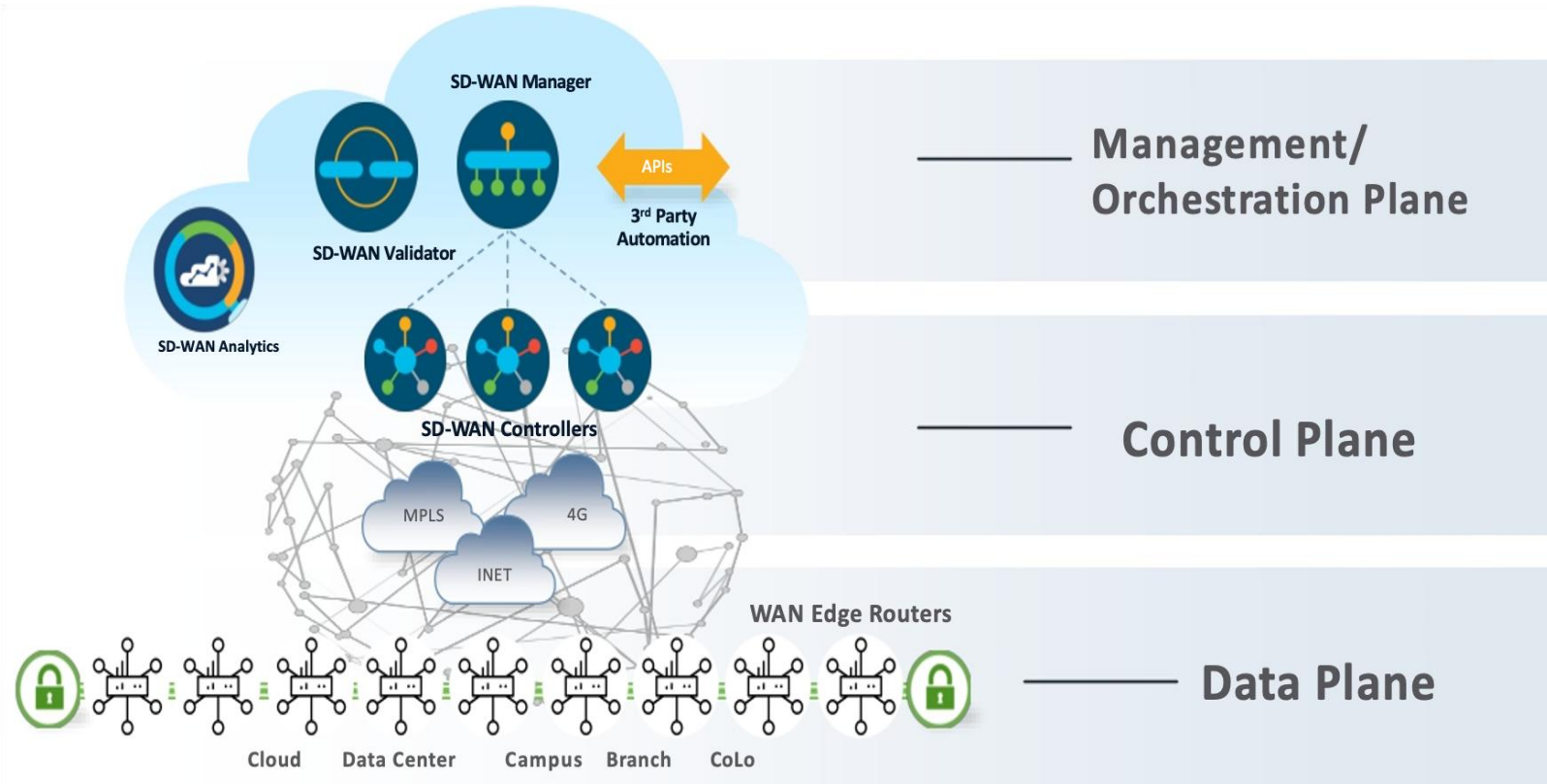
Cisco SD-WAN solution overview



Control Plane

- Facilitates fabric discovery
- Distributes 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 overview

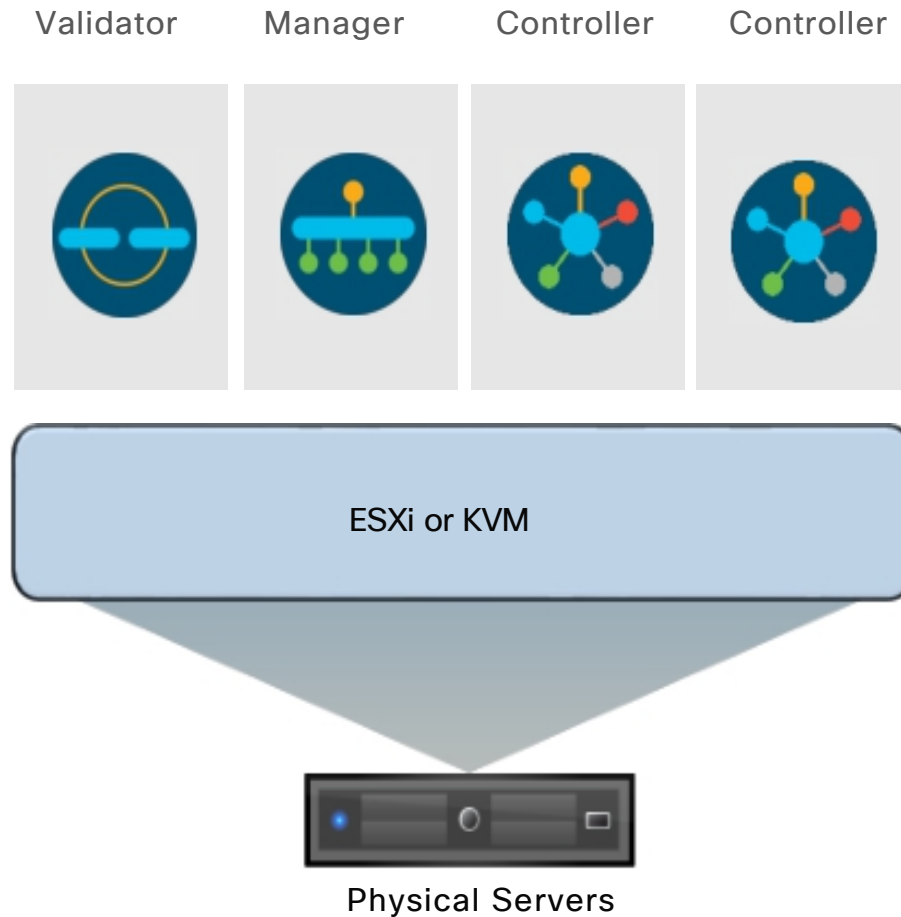


Data Plane

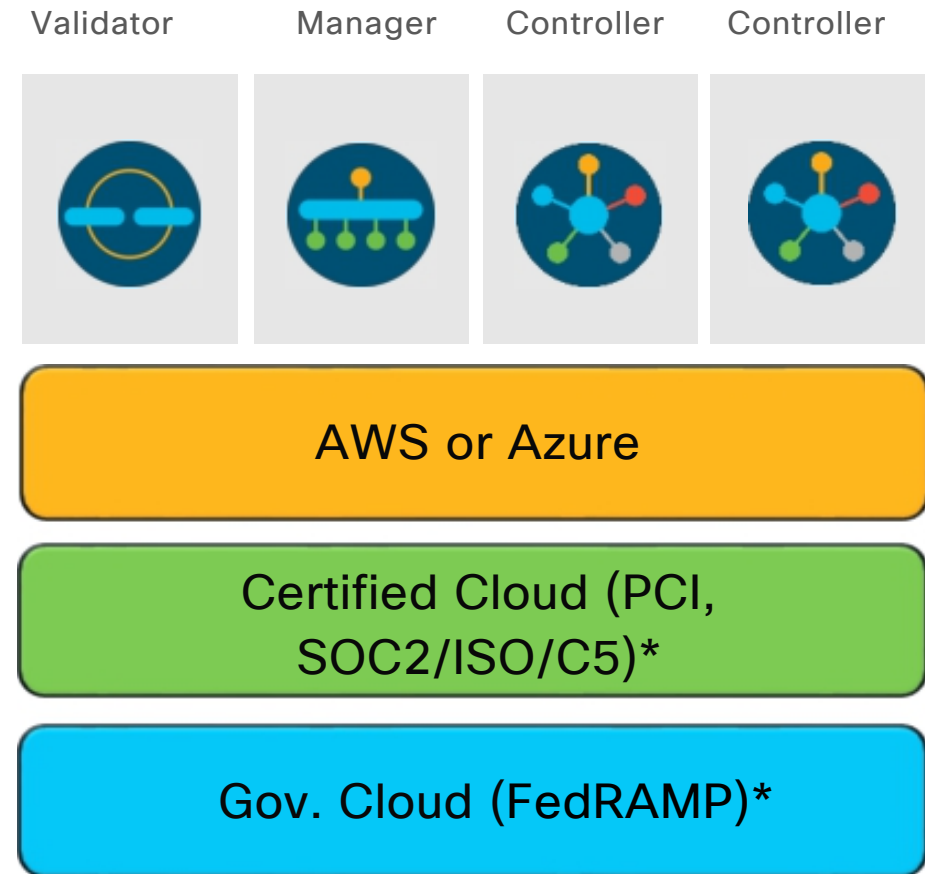
- WAN edge router
- Provides secure data plane with remote WAN Edge routers
- Establishes secure control plane with controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP, and EIGRP
- Support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

Controller deployment methodology

On-Premise



Cisco or MSP/Customer Hosted

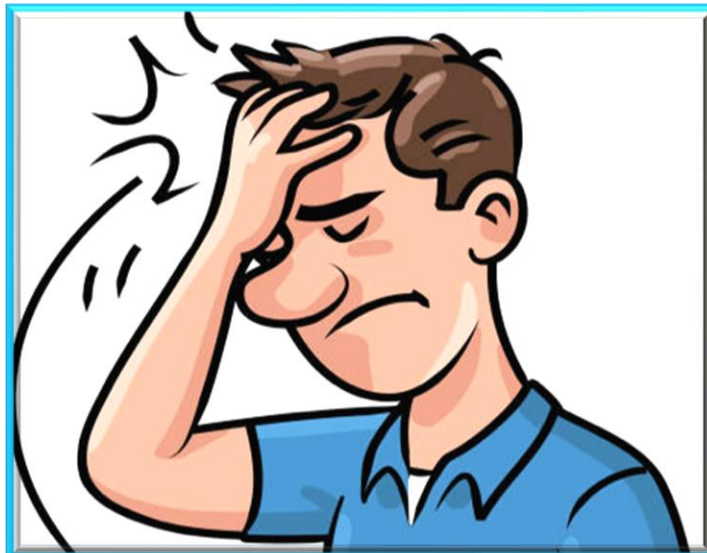


*Only Cisco hosted

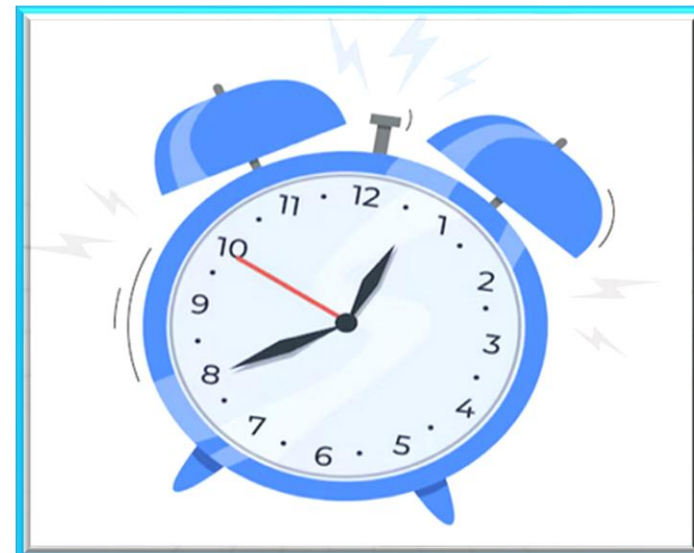
Monitoring/troubleshooting Challenges



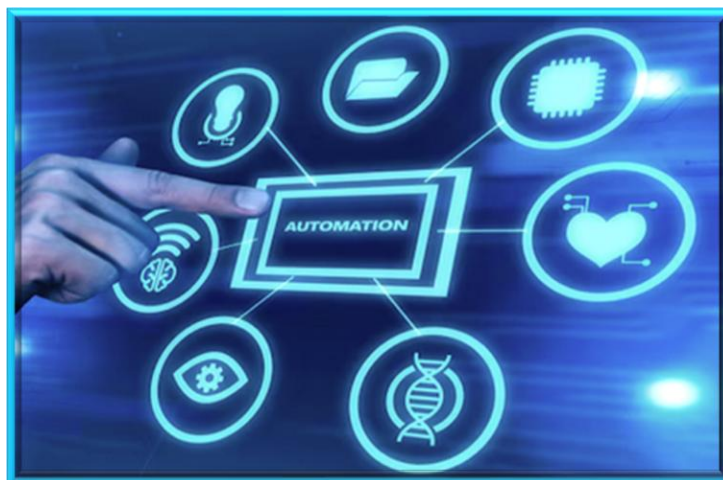
Know your Tools



What shall I look into ?



Critical/Intermittent issue –
Less time



Automation

SDWAN Manager Tools

Speed Test

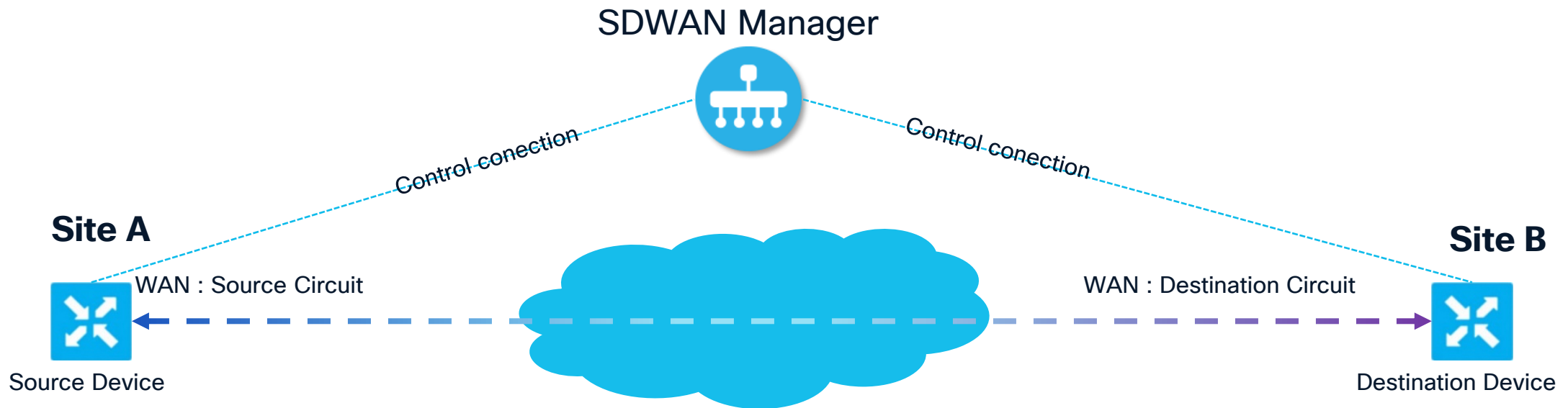
Speed test: introduction

- Used to evaluate the WAN interface's bandwidth against a remote SDWAN edge or a public/private iPerf3 server.
- Supported on Cisco devices since 17.3 & later releases.
- Two types of Speed Test
 - Site to Site Speed Test
 - Internet Speed Test



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 ⓘ

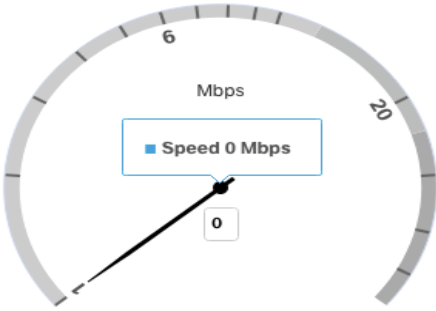
Troubleshooting ▾

Source Circuit* ⓘ
Choose ▾

Destination Device*
Choose ▾

Destination Circuit*
Choose ▾

Start Test



0 Mbps

Download Speed

0 Mbps

Upload Speed

Configured bandwidth

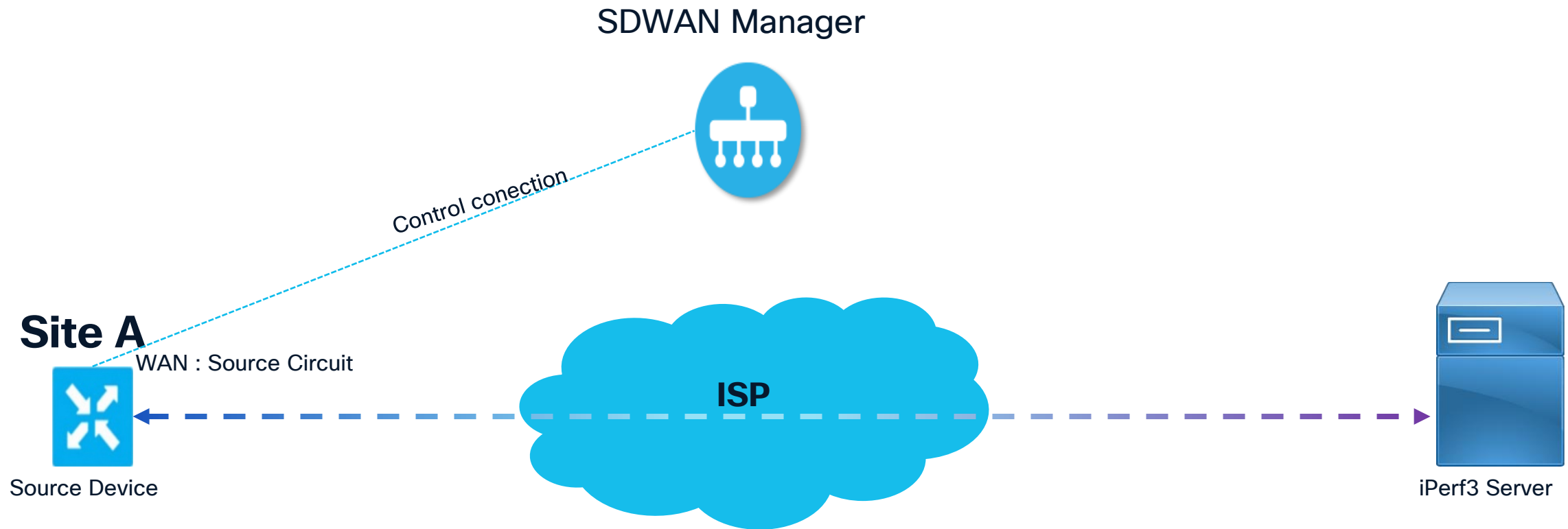
Downstream 0 Mbps

Upstream 0 Mbps

Feedback

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 ⓘ

Troubleshooting ▾

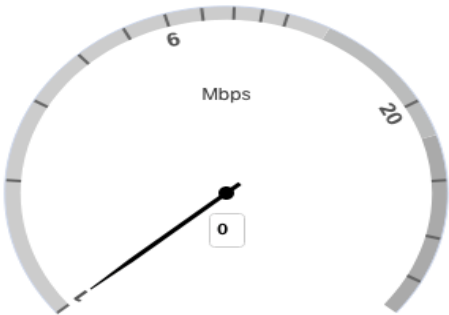
Source Circuit* ⓘ
biz-internet ▾

Destination Device*
Internet ▾

iPerf3 Server ⓘ

Server Port Range ⓘ

Start Test



0Mbps

Download Speed

0Mbps

Upload Speed

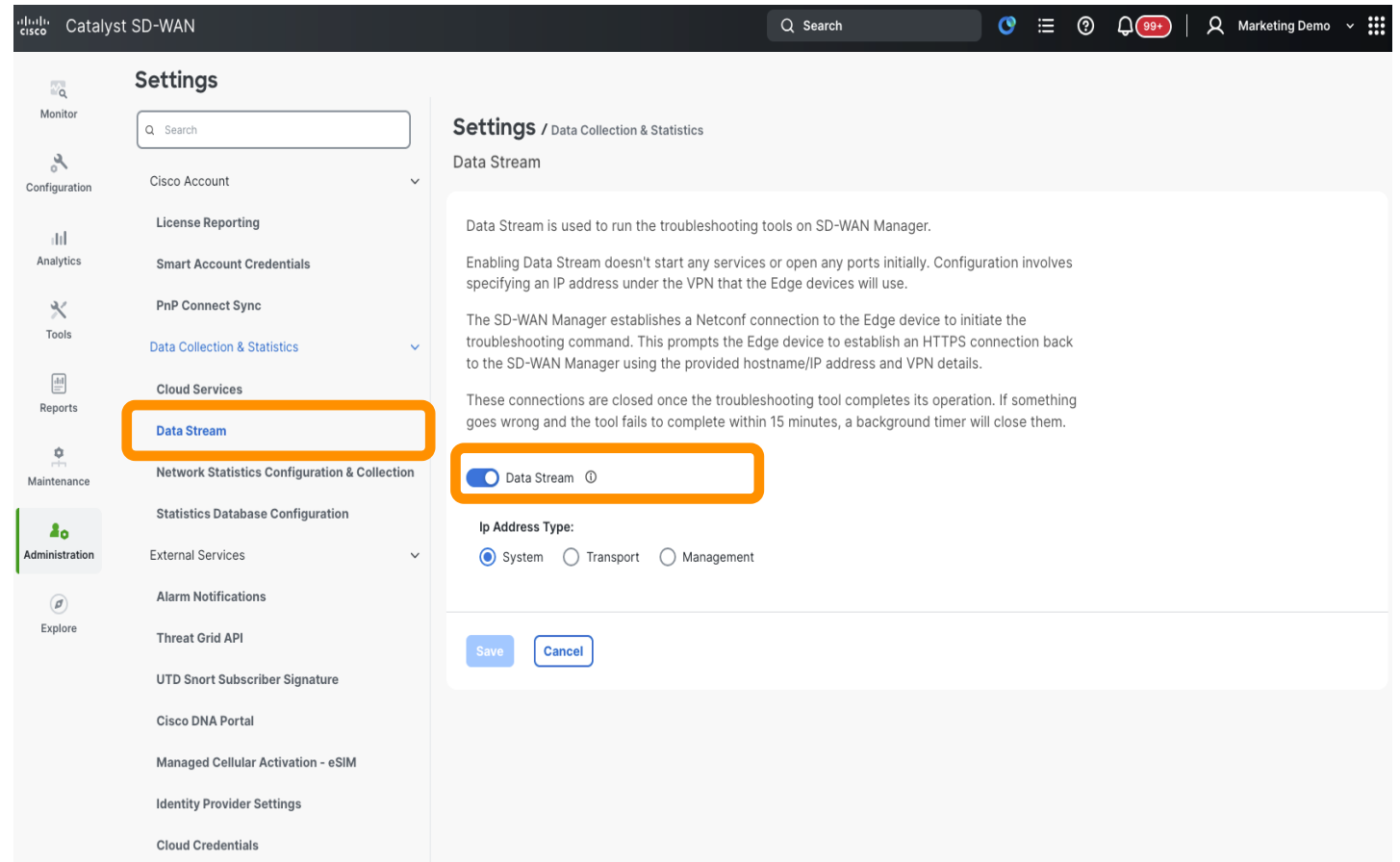
Configured bandwidth

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



Let's run a speed test

Devices > Troubleshooting > Speed Test

Select Device ▾

DC1A-SFO-C8300 | 1.2.1.210

Site Name 10020

Device Model: C8300-1N1S-4T2X ⓘ

Troubleshooting ▾

Source Circuit* ⓘ

Destination Device*

Destination Circuit*

biz-internet ▾

BR10-c8kv | 110.110.10.1 ▾

public-internet ▾

Start Test



110.78

218.8Mbps

110.78Mbps

Download Speed

Upload Speed

Configured bandwidth

Downstream 0 Mbps

Upstream 0 Mbps

Feedback ⓘ

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

Cisco SD-WAN

Select Resource Group

Monitor · Devices · Device 360

Devices > Troubleshooting

Select Device

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

APPLICATIONS

SAIE Applications

Interface

Tracker

QoS

ON-DEMAND TROUBLESHOOTING

FEC Recovery Rate

SSL Proxy

AppQoS TCP Optimization

AppQoS DRE Optimization

Connection Events

WAN Throughput

Flows

Top Talkers

WAN

TLOC

Tunnel

Connectivity



Device Bringup

Control Connections(Live View)

Ping

Trace Route

Speed Test

Traffic



Tunnel Health

App Route Visualization

Packet Capture

Simulate Flows

Logs



Debug Log

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

Traffic Filter

Interface for VPN - 10*

GigabitEthernet0/0/0.900 - ipv4 - 192.1.1.10

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 - 192.168.1.1

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 - 192.168.1.1

Traffic Filter

Source IP

Src Port

Protocol ⓘ

0-255

Destination IP

Dest Port

Bidirectional

☒

Start

Upload admin-tech and 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

Show Admin Tech List

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

Download

Delete

Refresh

Upload admin-tech file to CXD (cx.d.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

Upload

Cancel

Close

Total Rows: 15

Refresh

Settings

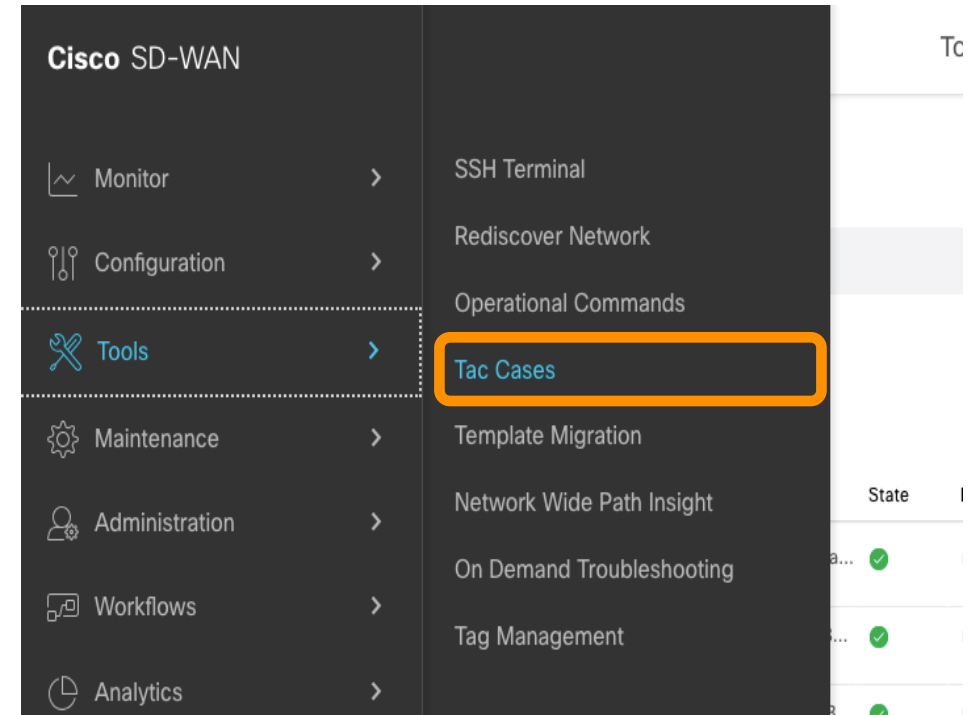
Up Since	Device Groups
14 Feb 2024 6:13:00 PM IST	No groups ...
14 Feb 2024 7:06:00 PM IST	No groups ...
14 Feb 2024 7:11:00 PM IST	No groups ...
14 Feb 2024 7:17:00 PM IST	No groups ...
14 Feb 2024 7:23:00 PM IST	No groups ...
14 Feb 2024 6:58:00 PM IST	No groups ...
14 May 2024 9:06:00 AM IST	No groups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

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKTRS-2595

TAC case

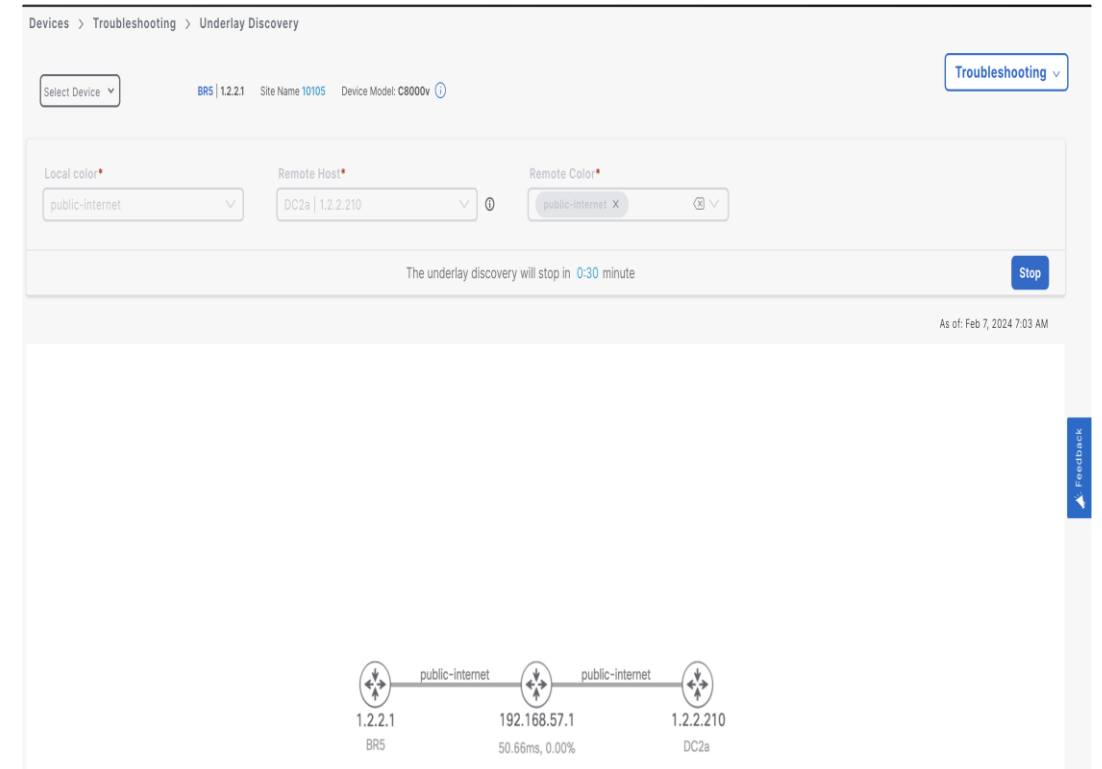
- Access SCM portal from SD-WAN Manager. Feature since 20.9.1
- Requires internet access and reachability to Support case Manager (SCM)
- Active Cisco single sign-on (SSO) login credentials to access the SCM Wizard and the cloud server.
- Open or View TAC cases from SD-WAN Manager



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.



Underlay measurement and tracing service

Path : Monitoring > Devices > Troubleshooting > Underlay Discovery

Devices > Troubleshooting > Underlay Discovery

Monitor

Configuration

Analytics

Tools

Reports

Select Device ▼

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

Troubleshooting ▼

Local color*

biz-internet ▼

Remote Host*

BR10-c8kv | 110.110.10.1 ⓘ

Remote Color*

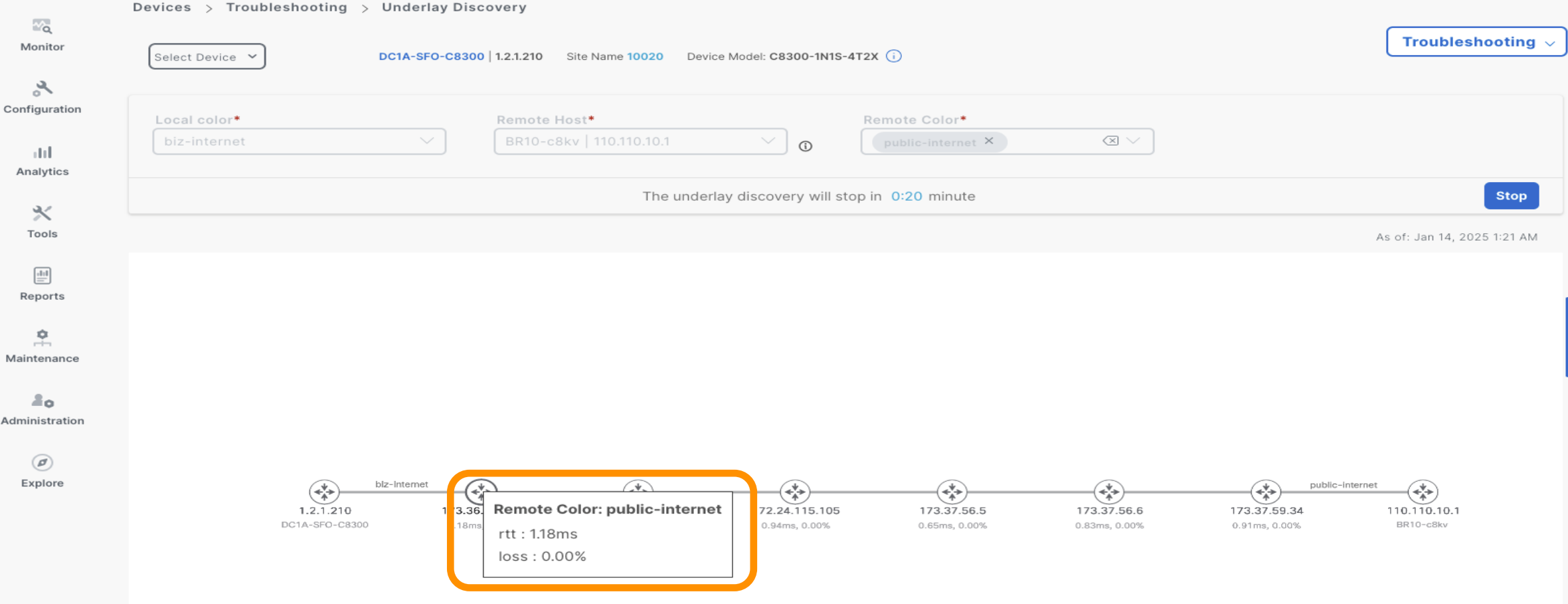
public-internet × ⌵ ⌶

Search

public-internet ✓

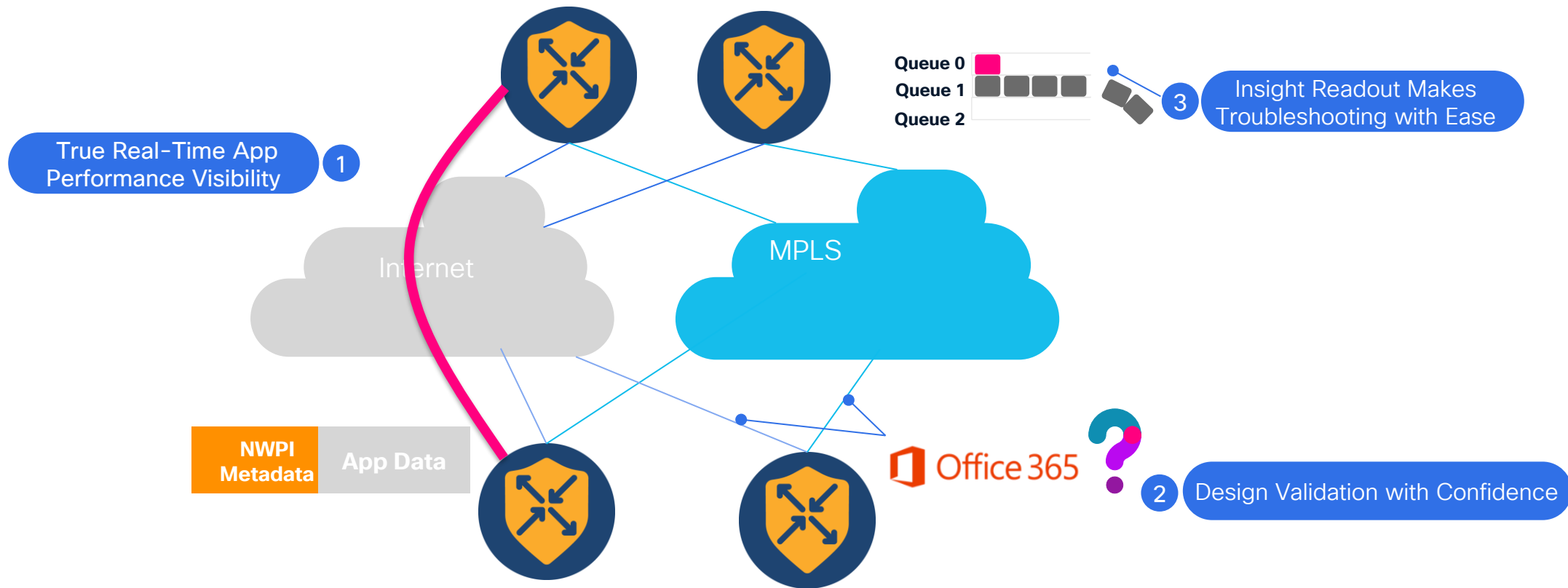
Start

Underlay measurement and tracing service



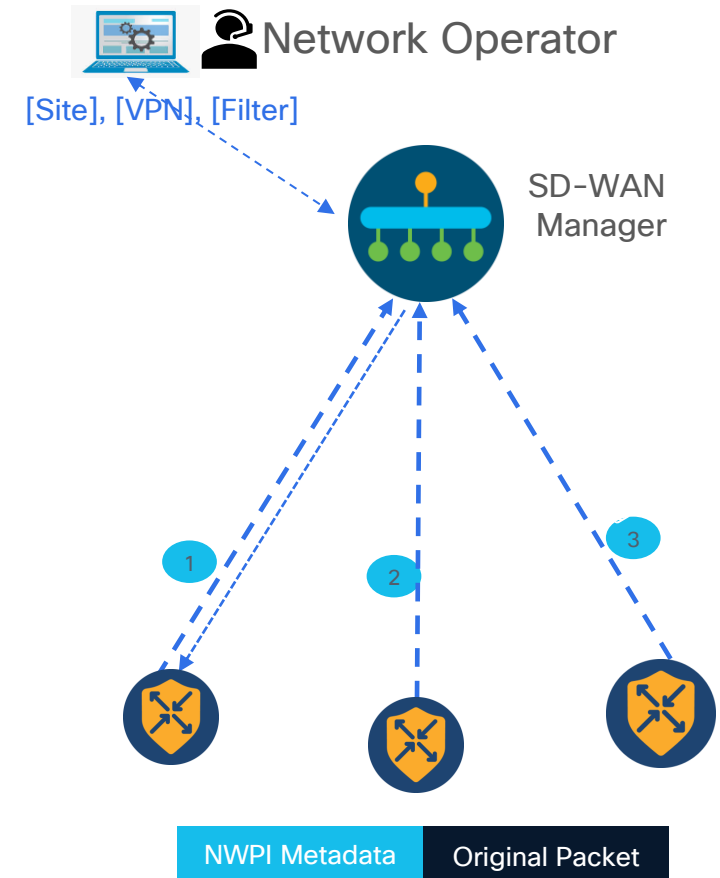
Network Wide Path Insight (NWPI)

NWPI: Trusted tool for SD-WAN operations



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



NWPI release timeline

FYI

17.9/20.9

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

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

NWPI release timeline

17.14/20.14

- NWPI and ThousandEyes Integration

17.15/20.15

- NWPI support in SD-Routing Mode

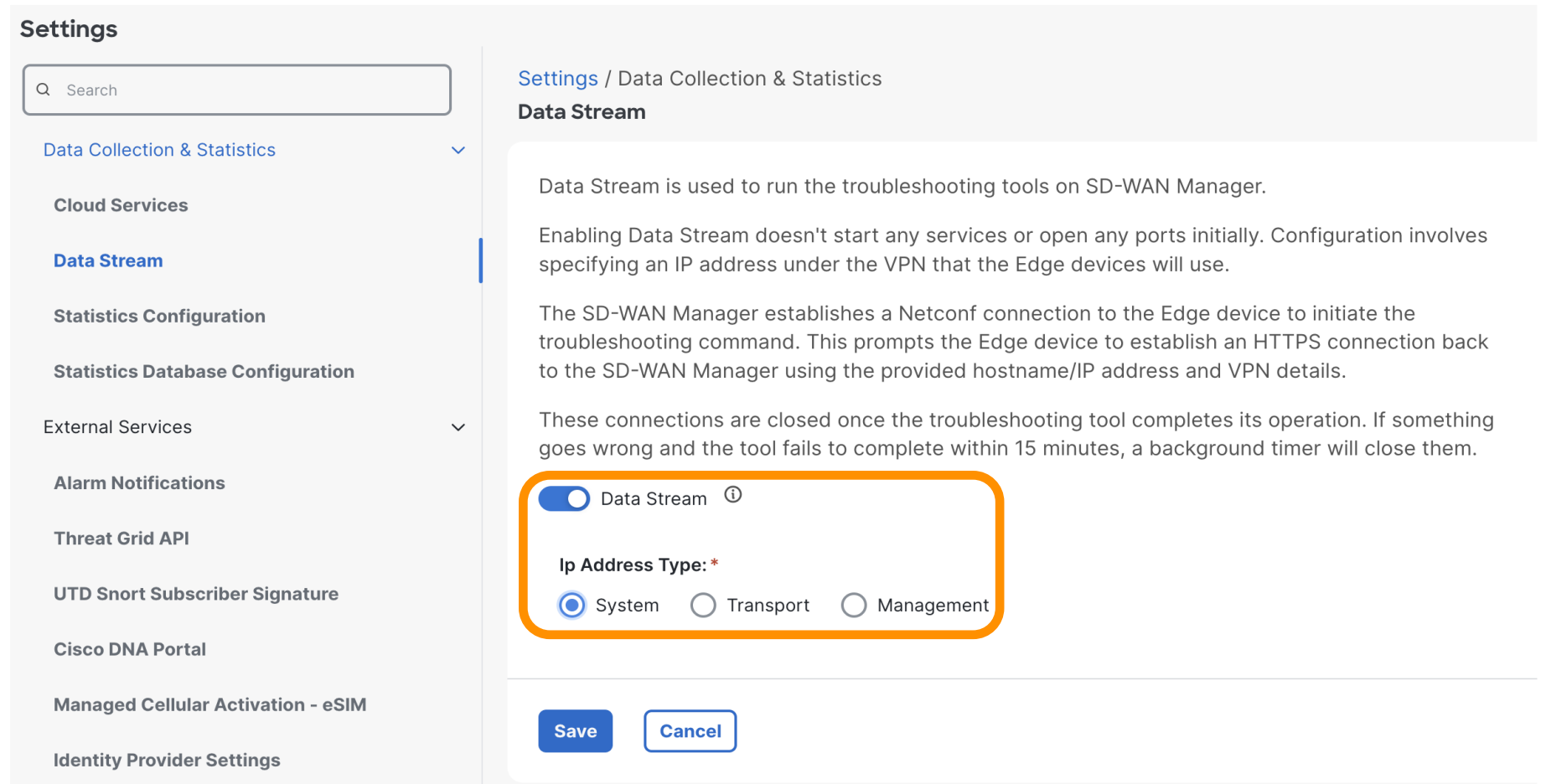
17.16/20.16

- Packet Capture Replay

Prerequisites

In SD-WAN Manager,

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



Settings

Q 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 ⓘ

Ip Address Type: *

☒ System ☐ Transport ☐ Management

Save Cancel

Start NWPI trace

Catalyst SD-WAN

99+

Sai Suchandan Reddy Marapareddy

Monitor

Configuration

Tools

Maintenance

Administration

Workflows

Reports

Analytics

Explore

TRACE

New Trace

New Auto-on Task

How to Get Started

FAQ

Administration Setting

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

Enable DNS Domain Discovery ⓘ

Trace Name

Trace Duration(minutes)

e.g trace_[site ID]

60

Filters

Select Site(branch site only) *

VPN *

Please select a site

Please select one or more vpns

Source Address/Prefix

Destination Address/Prefix

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

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

Cancel

Start

Feedback

© 2025 Cisco and/or its affiliates. All rights reserved.

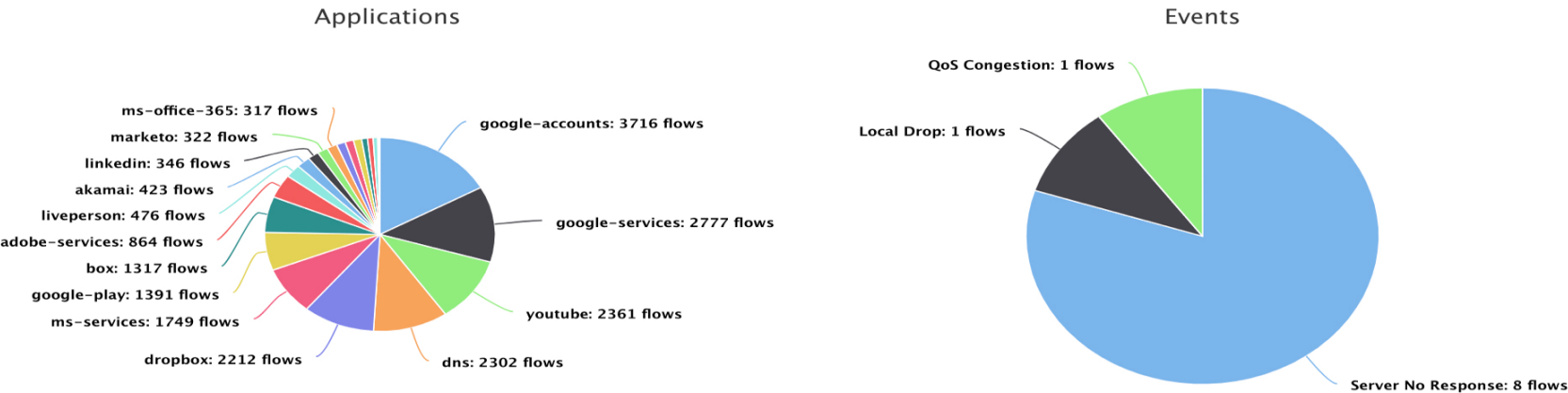
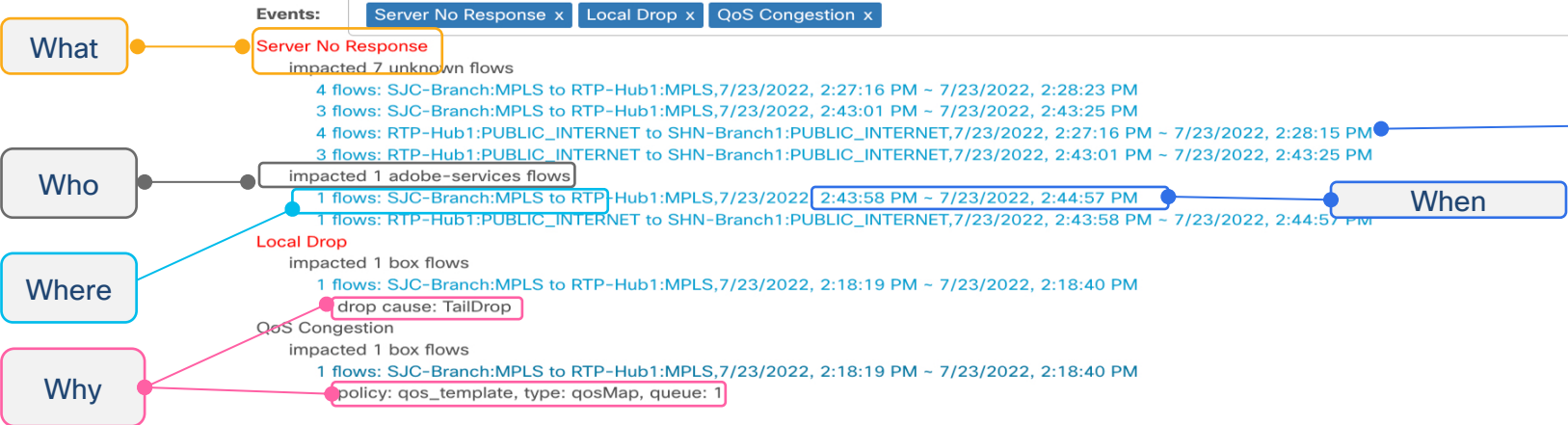
BRKTRS-2595

Insight summary - Overview

Overview App Performance Insight Event Insight QoS Insight

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

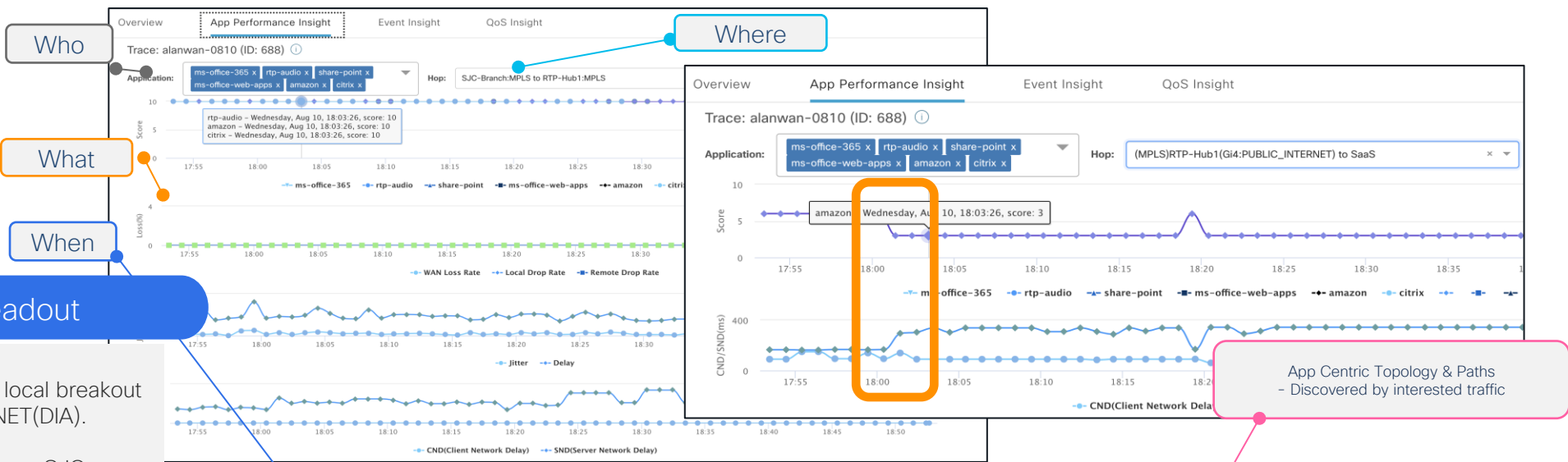
☒ Critical ☒ Warning ☐ Informational



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



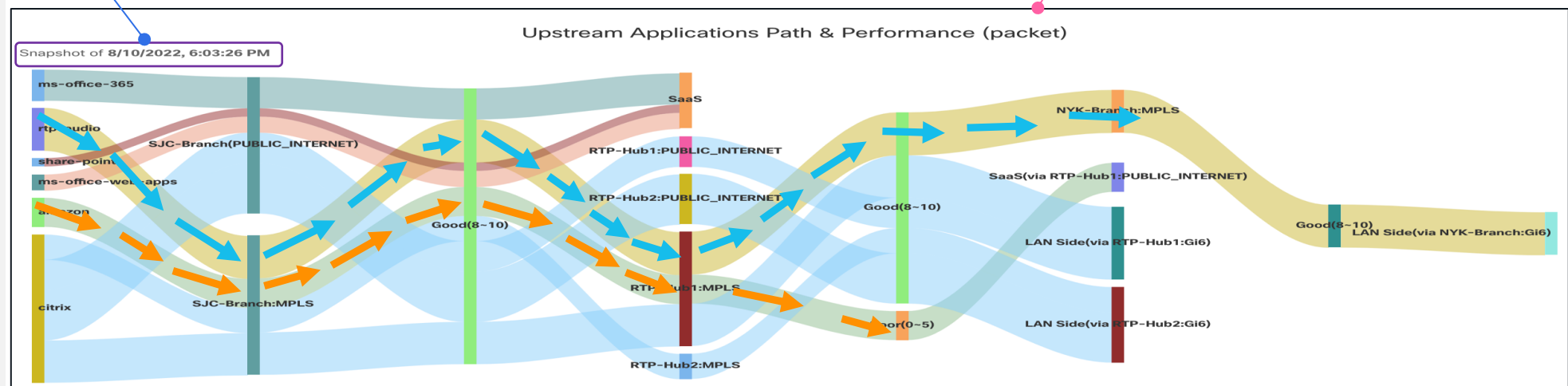
M365: SJC-Branch local breakout to SaaS Cloud via INET(DIA).

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.



Insight summary - Event Insight



Insight summary - QoS Insight

Queue	Application	Bandwidth
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

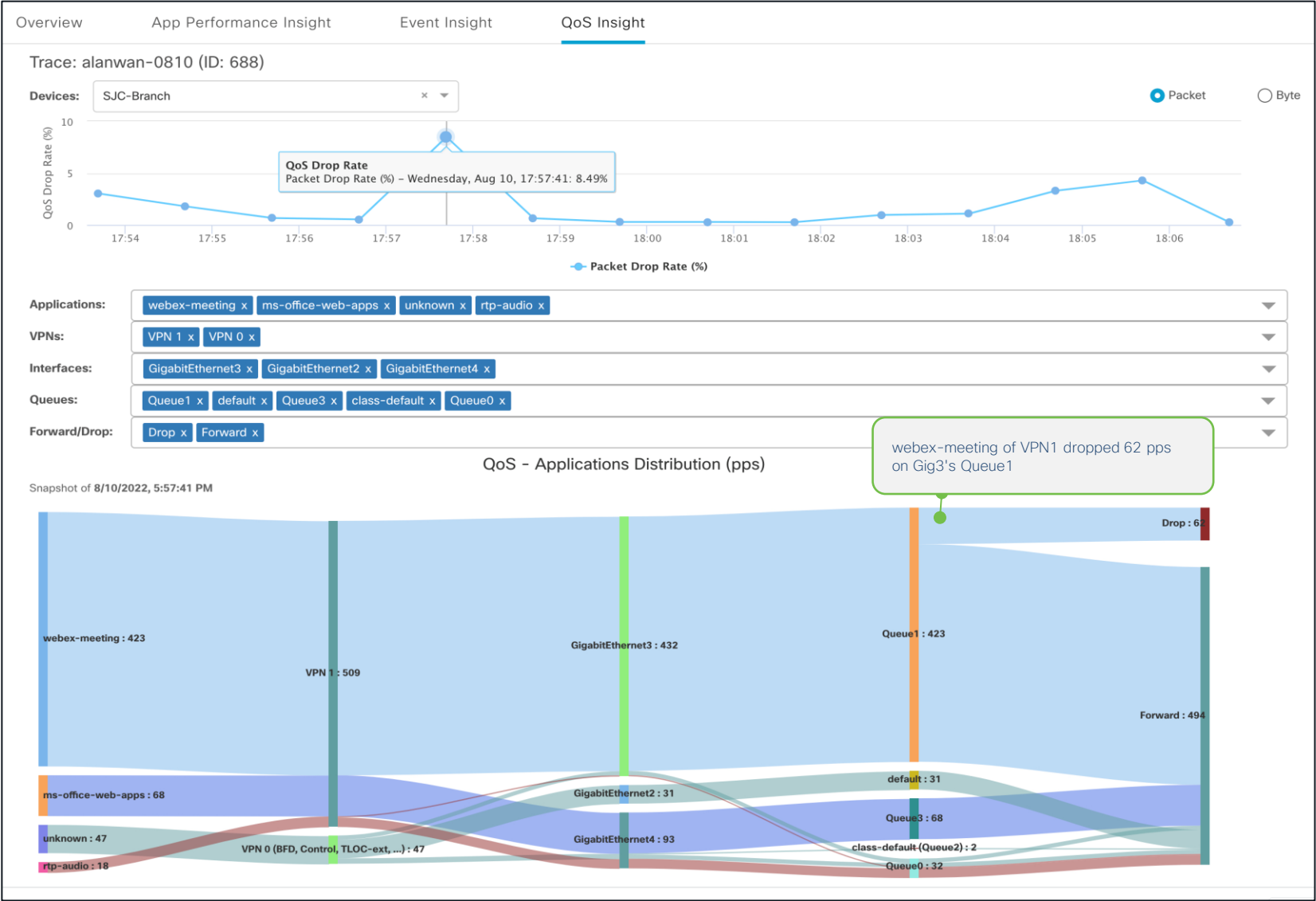
QoS Insight - Use case 1

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.



Scenario 1

Integration with NWPI and ISE

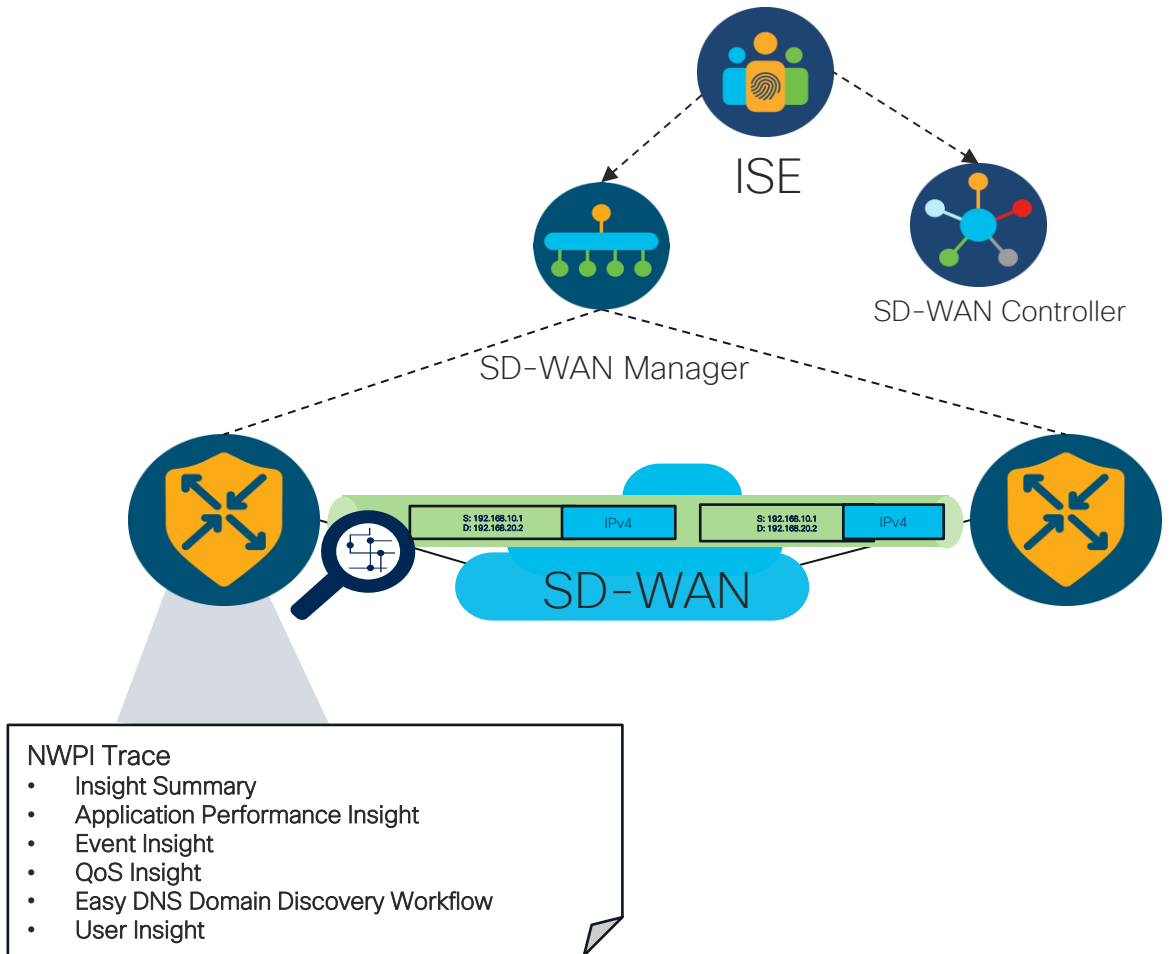
Network wide path insights (NWPI)

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.



Prerequisites

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

The screenshot shows the 'Administration Settings' page in the Cisco Catalyst SD-WAN Manager UI. The breadcrumb trail at the top right indicates the path: 'Administration · Settings'. The main heading is 'Administration Settings'. Below this, the 'Data Stream' section is highlighted, showing it is 'Enabled'. The configuration options are as follows:

- Data Stream:** ☒ Enabled ☐ Disabled (i)
- Ip Address Type:** ☒ System ☐ Transport ☐ Management
- Hostname:**
- VPN:**

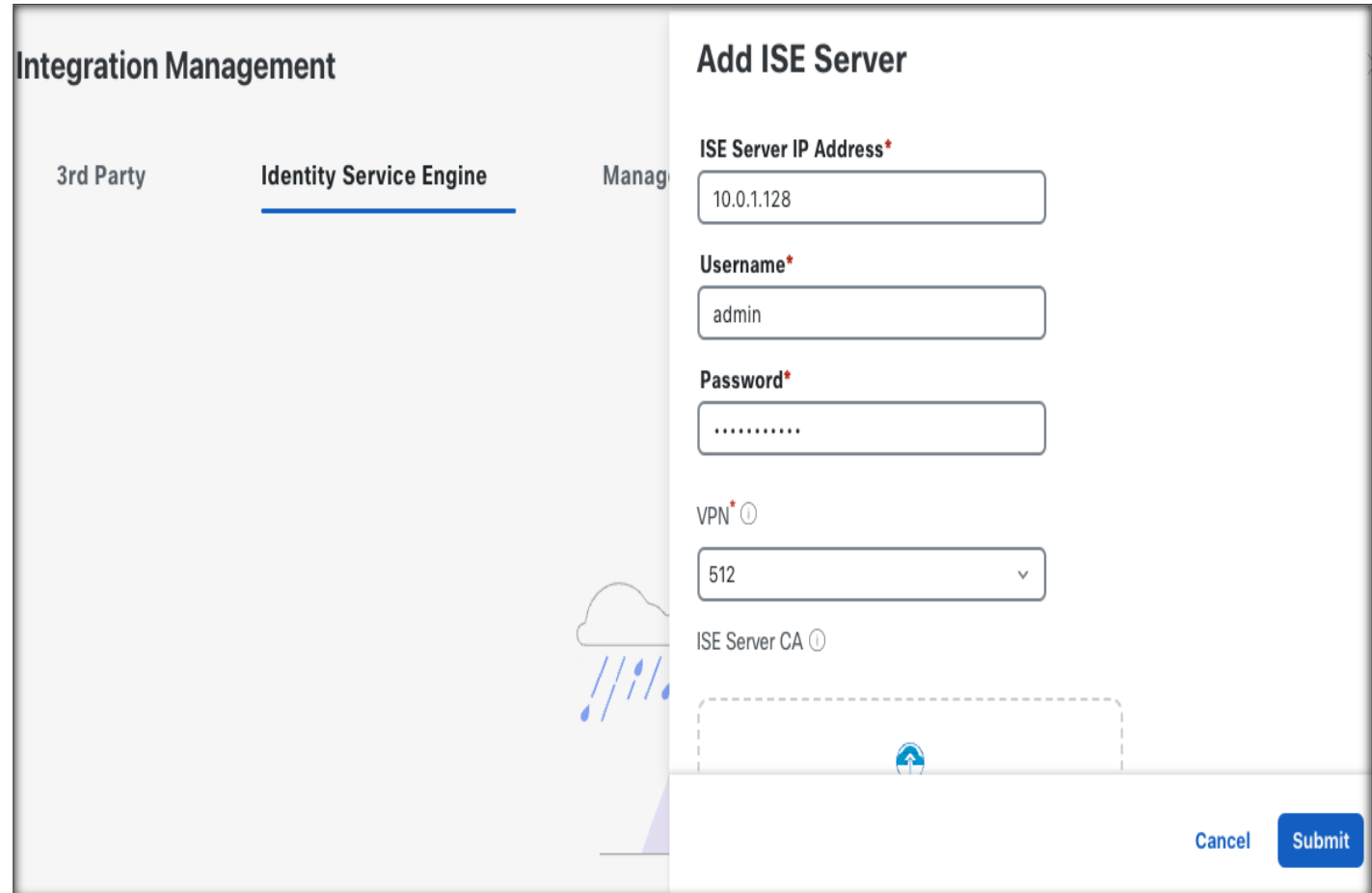
At the bottom of the configuration area, there are two buttons: a blue 'Save' button and a 'Cancel' link.

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)



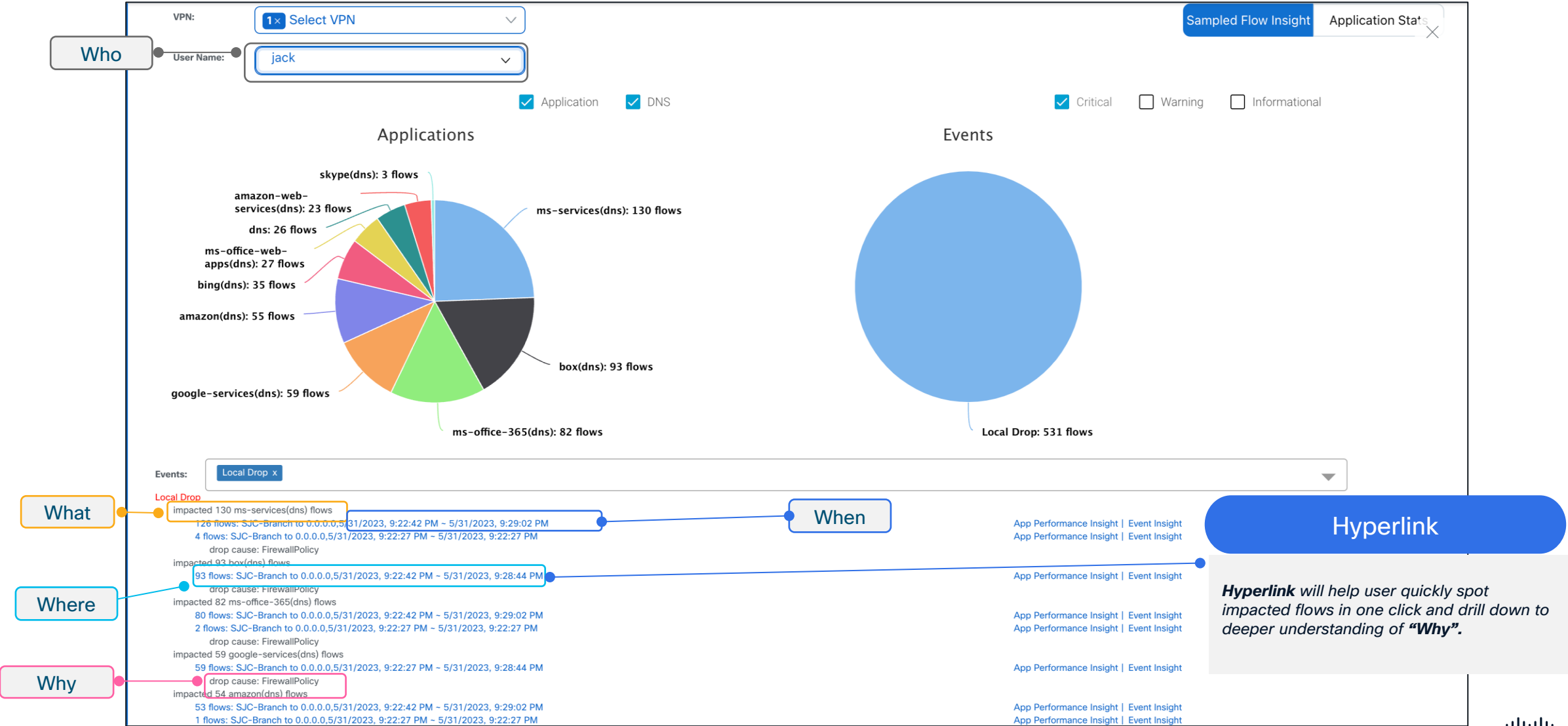
The screenshot shows the 'Add ISE Server' configuration page within the 'Integration Management' section. The 'Identity Service Engine' tab is selected. The form contains the following fields:

- ISE Server IP Address***: Text input field containing '10.0.1.128'.
- Username***: Text input field containing 'admin'.
- Password***: Password input field with masked characters '.....'.
- VPN***: Dropdown menu with a value of '512' and a help icon.
- ISE Server CA**: Field with a help icon and a dashed box containing a small icon.

At the bottom right, there are 'Cancel' and 'Submit' buttons. A decorative graphic of a cloud with rain is visible on the left side of the form area.

User unable to access application!

User Jack complains of internet access issue



User (Jack) traffic is dropped on SJC-branch

INSIGHT

Selected trace: ISE_FW_Demo (Trace Id: 21792)

ApplicationsActive FlowsCompleted Flows

Selected Flow Id: 221

Filter

May 31, 2023, 9:22:42 PMMay 31, 2023, 9:28:44 PMMay 31, 2023, 9:31:35 PM

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

Search by Domain, Application, Readout, etc.

* Readout Legend: Error, Warning, Information, Synthetic Traffic, ThousandEyes.

Search

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/A
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	
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/A



View policy and config applied for user traffic

Hostname: SJC-Branch Event List: FIRST_PACKET/DPLONGOING Expand All Features
Version: 17.13.01.0.1247, Input: GigabitEthernet4, Output: Tunnel2

Ingress Feature	Egress Feature
<div><div>+ Ingress Report</div><div>+ CEF Forwarding</div><div>+ SDWAN ACL IN >> View Policy <<</div><div>+ NBAR</div><div>+ SDWAN App Route Policy >> View Policy <<</div><div>+ SDWAN Data Policy IN >> View Policy <<</div><div>+ SDWAN Forwarding</div></div>	<div>Early cls priority: 20 Permit apps list id: 0 Sdavn Early priority 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</div> <div><div>- ZBFW >> View Policy <<</div><div>Action : Drop Reason : Policy drop:classify result Zone-pair name : 7P_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</div><div>+ DROP_REPORT</div></div>

FW Drop

FW Class-map

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-action
pass



Scenario 2

Integration with ThousandEyes & Underlay Measurement & Tracing Service

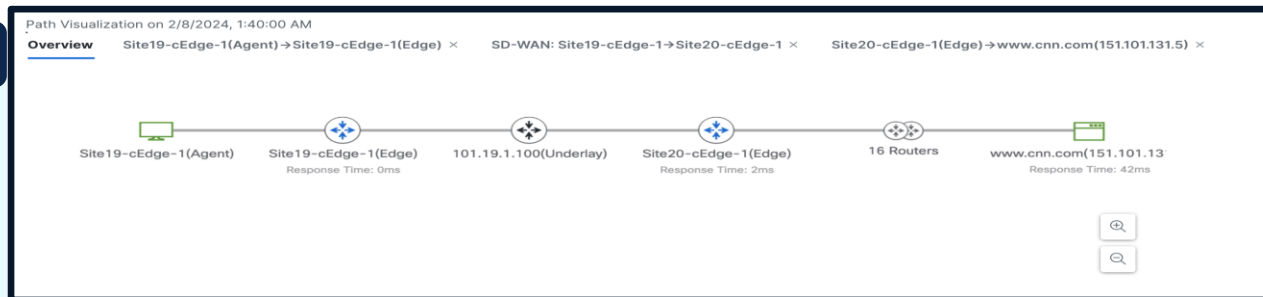
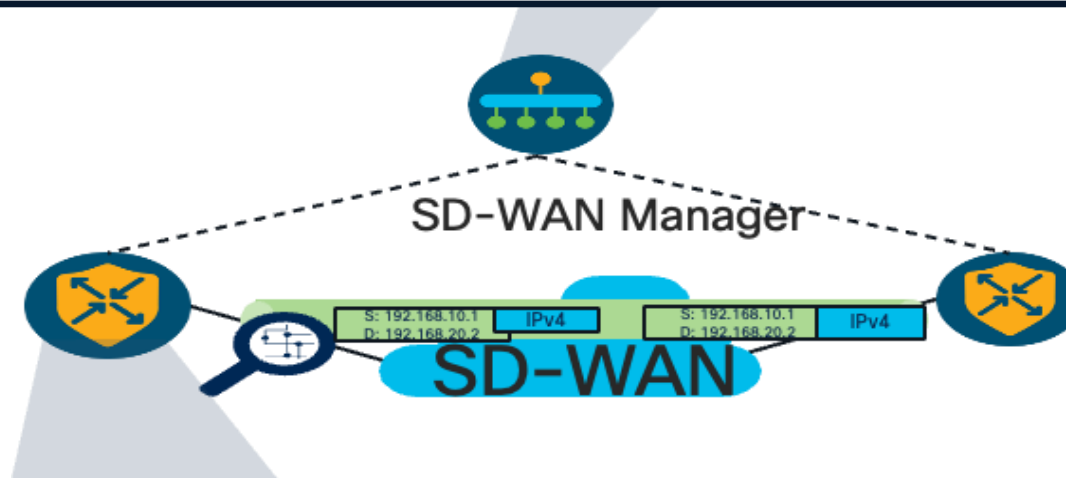
Network wide path insights

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.



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 correlated with TE Insights

NWPI Trace

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

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

The screenshot displays the ThousandEyes dashboard interface. On the left is a sidebar with navigation icons and labels: Monitor, Configuration, Tools, Maintenance, Administration, Workflows, Reports, Analytics, and Explore. The main panel is titled 'Settings' and contains a search bar with the text 'ThousandEyes User API Tokens'. Below the search bar, the path 'ThousandEyes User API Tokens' is highlighted. The right side of the panel shows the 'ThousandEyes User API Tokens' configuration page. It includes a breadcrumb 'Settings / External Services' and a title 'ThousandEyes User API Tokens'. A descriptive text states: '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.' Below this text is a button '+ Add ThousandEyes User API Tokens'. A modal form is open for adding a new token, featuring two input fields: 'Username' and 'Bearer Token'. The 'Bearer Token' field has a copy icon. An 'Ok' button is located at the bottom left of the modal.

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)

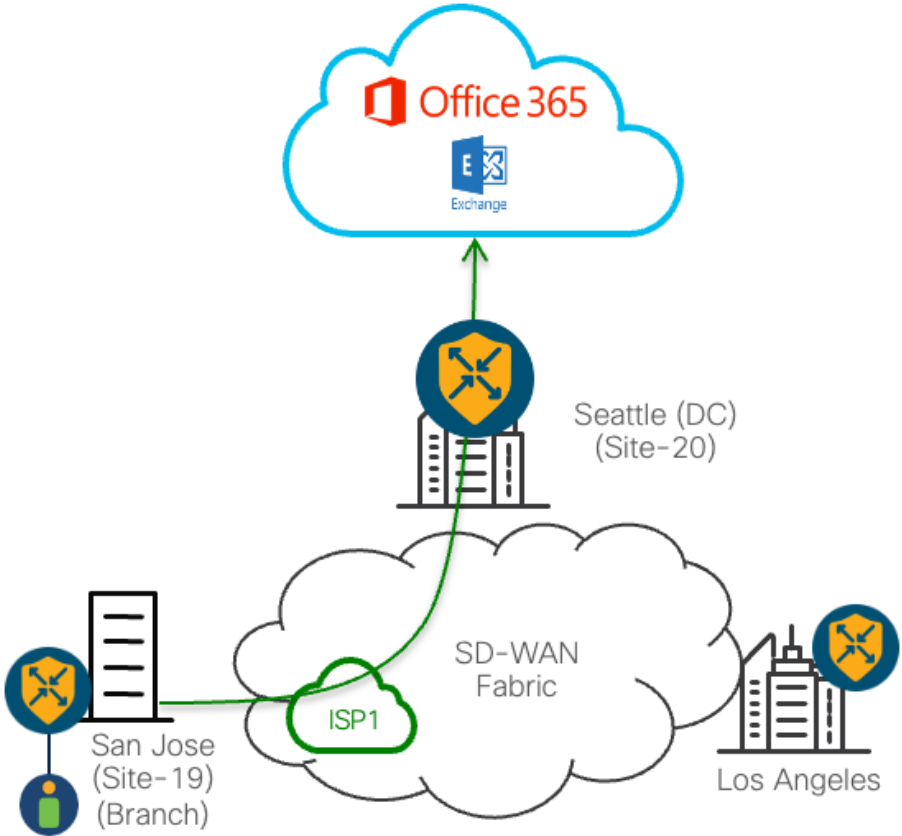
The screenshot displays the ThousandEyes configuration interface, divided into two main sections: **Advanced Filters** and **Monitor Settings**.

Advanced Filters: This section contains several dropdown menus for filtering data. The **Device** dropdown is currently empty. The **Source Interface** dropdown is also empty. The **Source Port** and **Destination Port** fields are empty. The **Protocol** dropdown is empty. The **DSCP** dropdown is empty. The **ISE Users:** checkbox is unchecked, and the dropdown below it shows "Please select one or more users". The **ThousandEyes Agent** checkbox is checked, and the dropdown below it shows "Please select ThousandEyes Agent". A search bar with the text "search .." is visible below the dropdown.

Monitor Settings: This section contains several checkboxes for enabling or disabling features. The **QoS Insight** checkbox is checked. The **ART Visibility** checkbox is checked. The **WAN Visibility** checkbox is unchecked. The **ThousandEyes Insight** checkbox is checked and highlighted with an orange circle. The **Sampling** checkbox is unchecked. The **Local Drop Rate Threshold(%)** field is set to 5.

An orange circle highlights the **ThousandEyes Agent** checkbox and the dropdown menu below it, which shows a search bar and the text "Site19-cEdge-1(Tōkyō, Japan)".

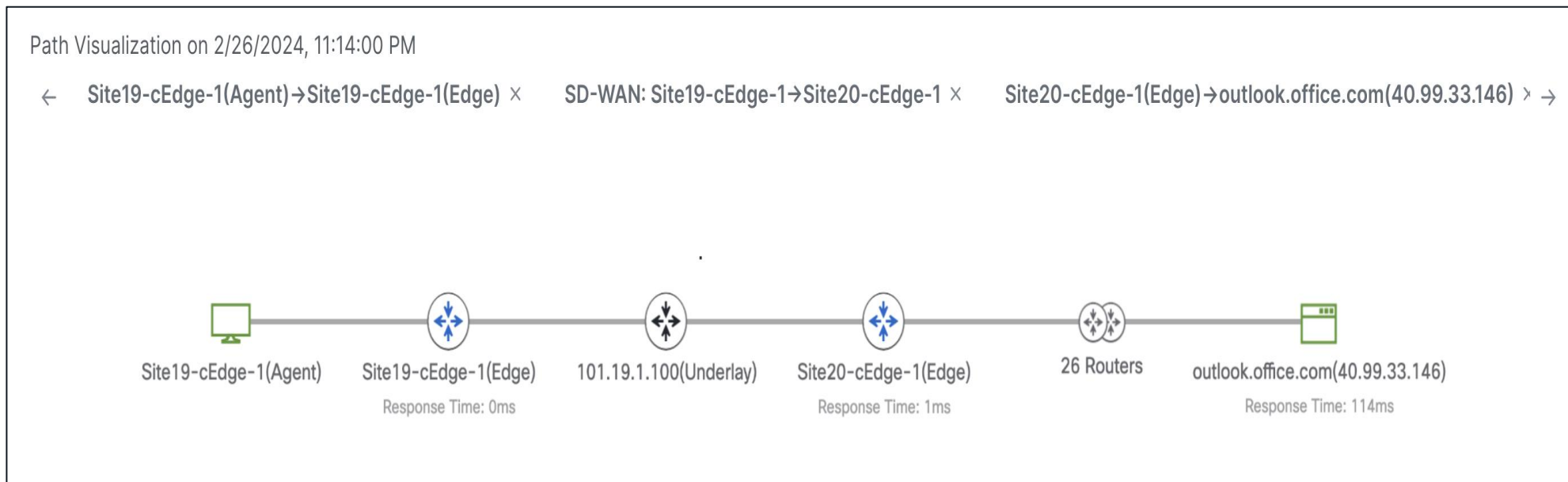
User in San Jose Branch complains that they experience slowness when accessing Outlook



End-to-end path visualization

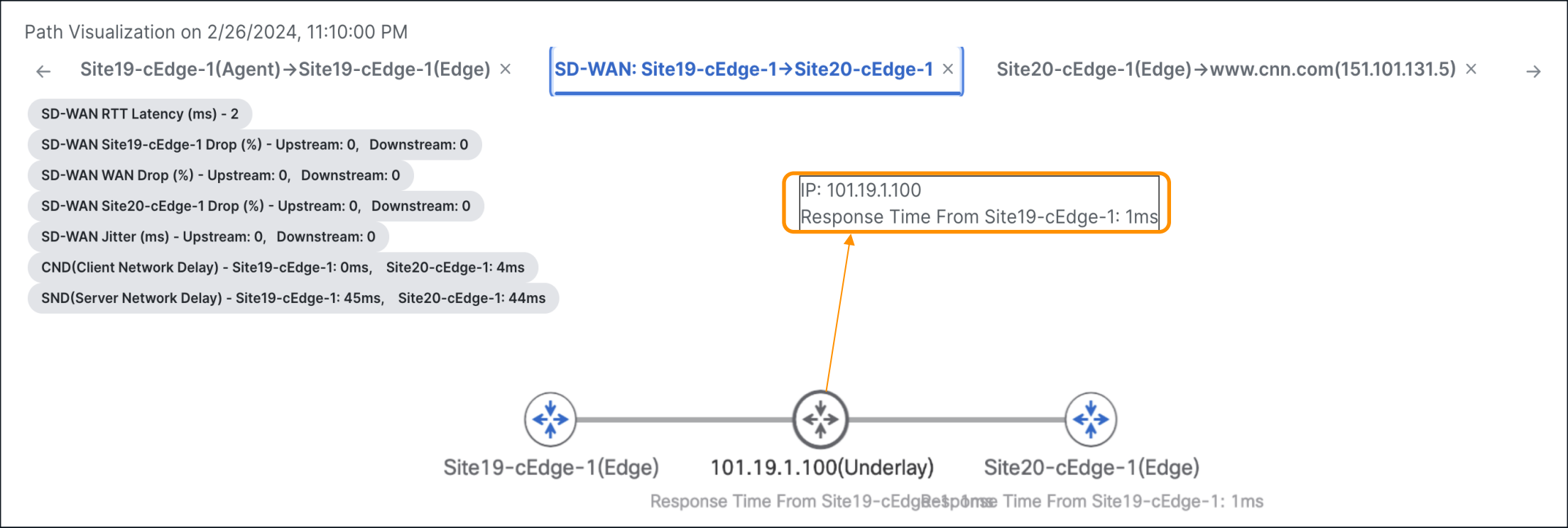
In below scenario, Path Visualization is represented for each segments such as

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

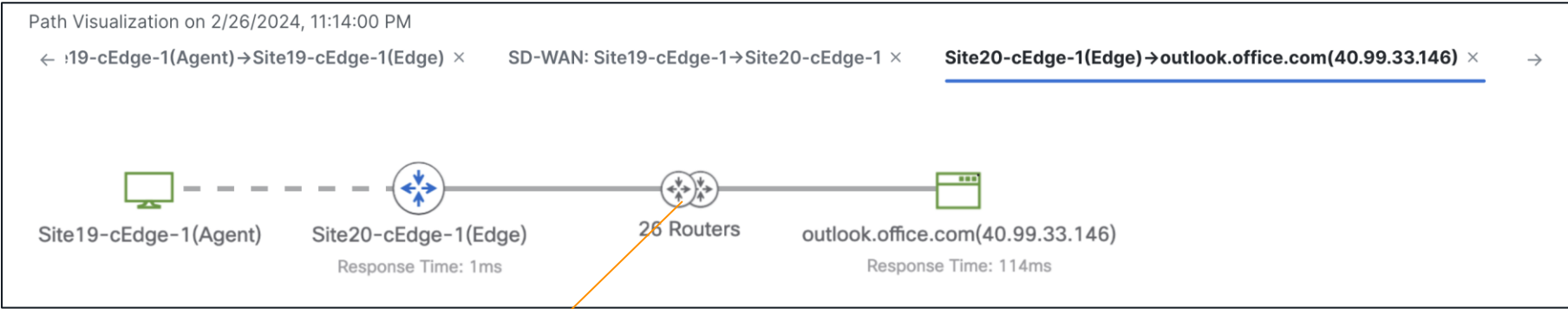
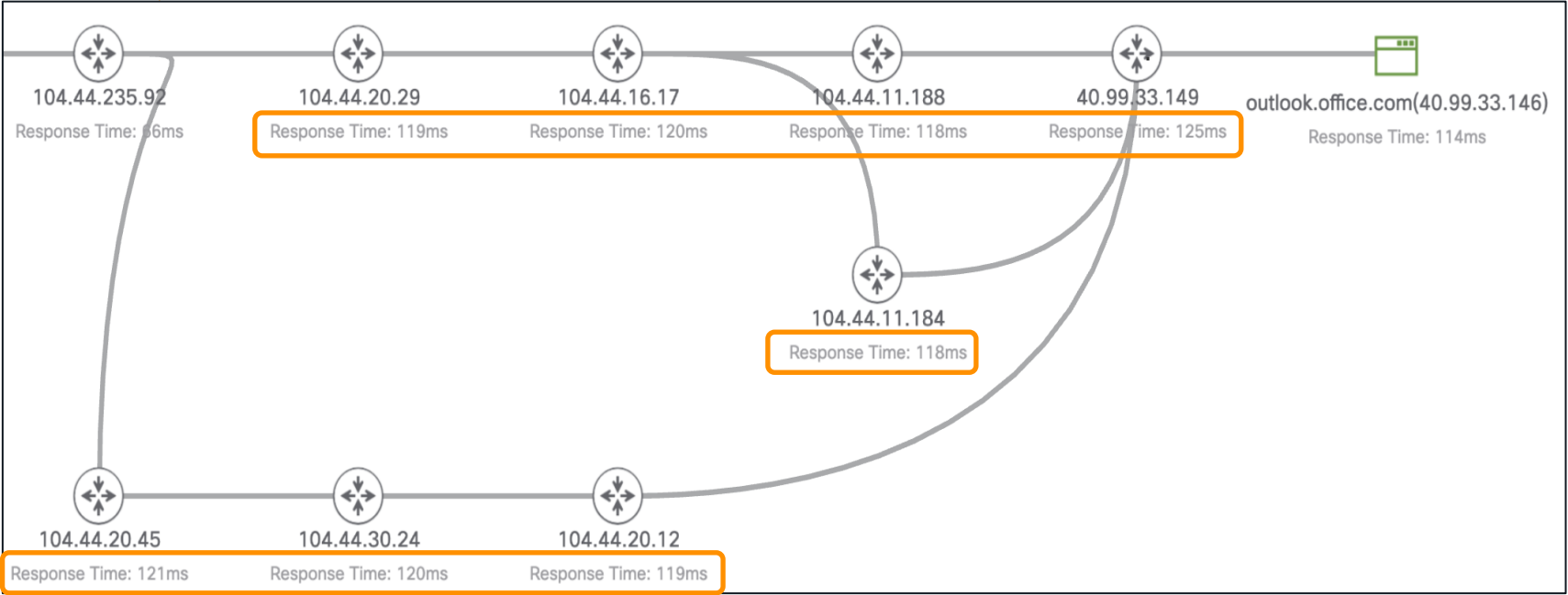


Underlay visibility for SD-WAN tunnels

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



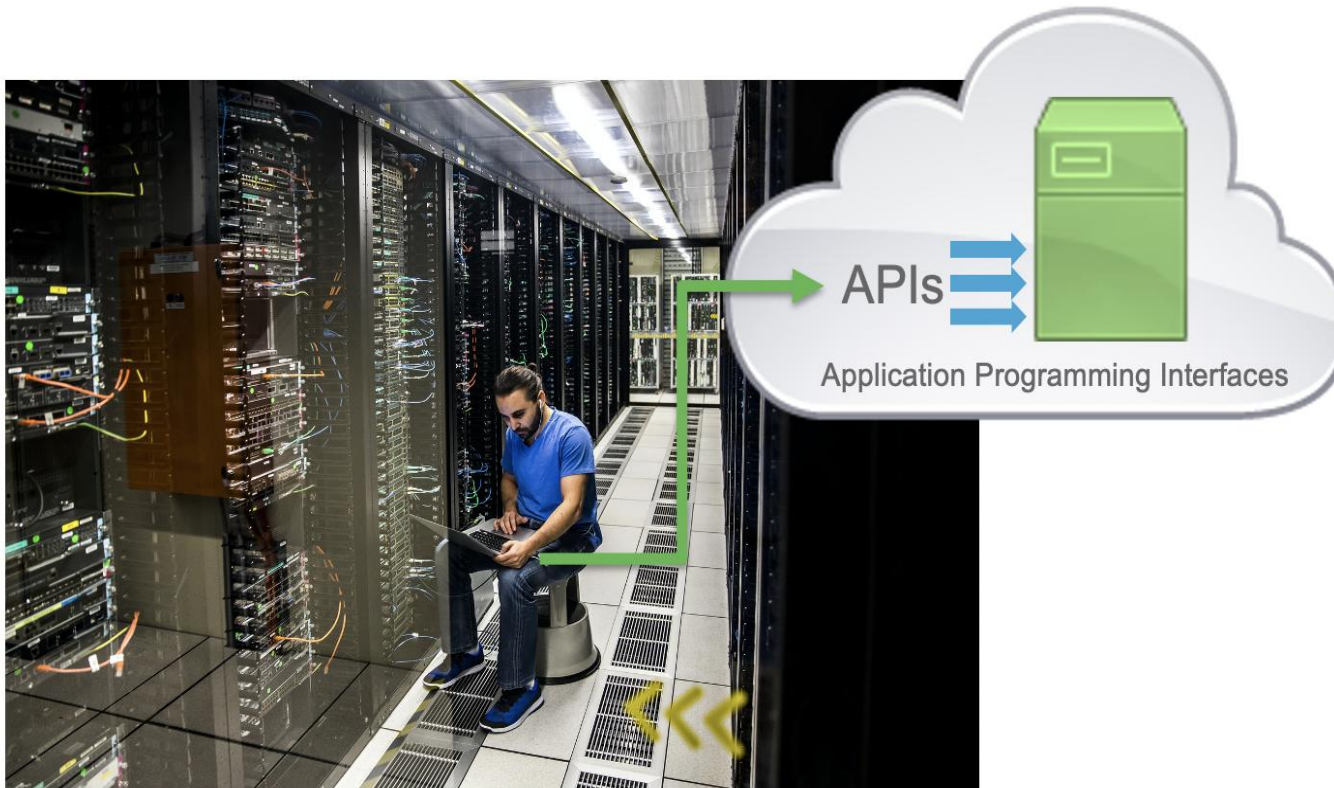
ThousandEyes path visualization for Internet hops



*Only part of Internet Path is shown in this screenshot

Build your own API-Workflow

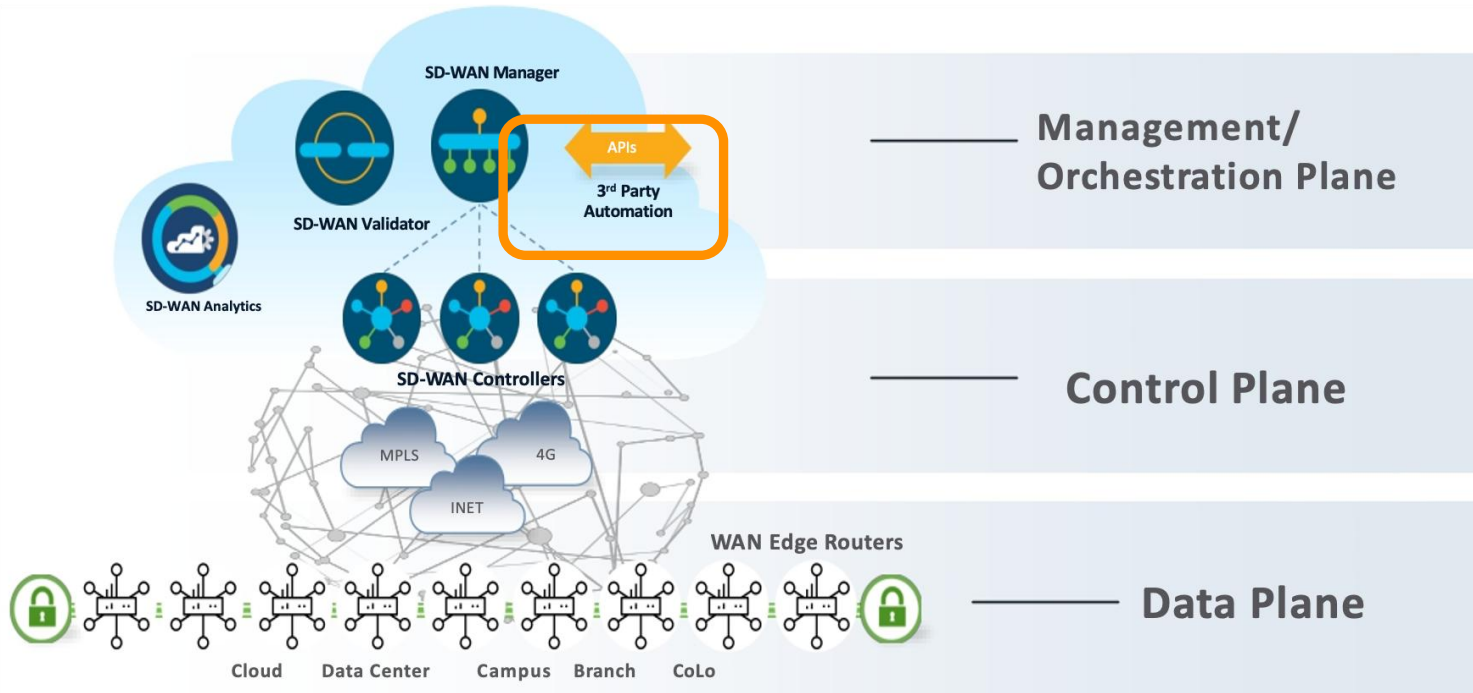
Why APIs?



Challenges

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

SD-WAN manager APIs



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 APIs

[Try it out!](#) [Hide Response](#)

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

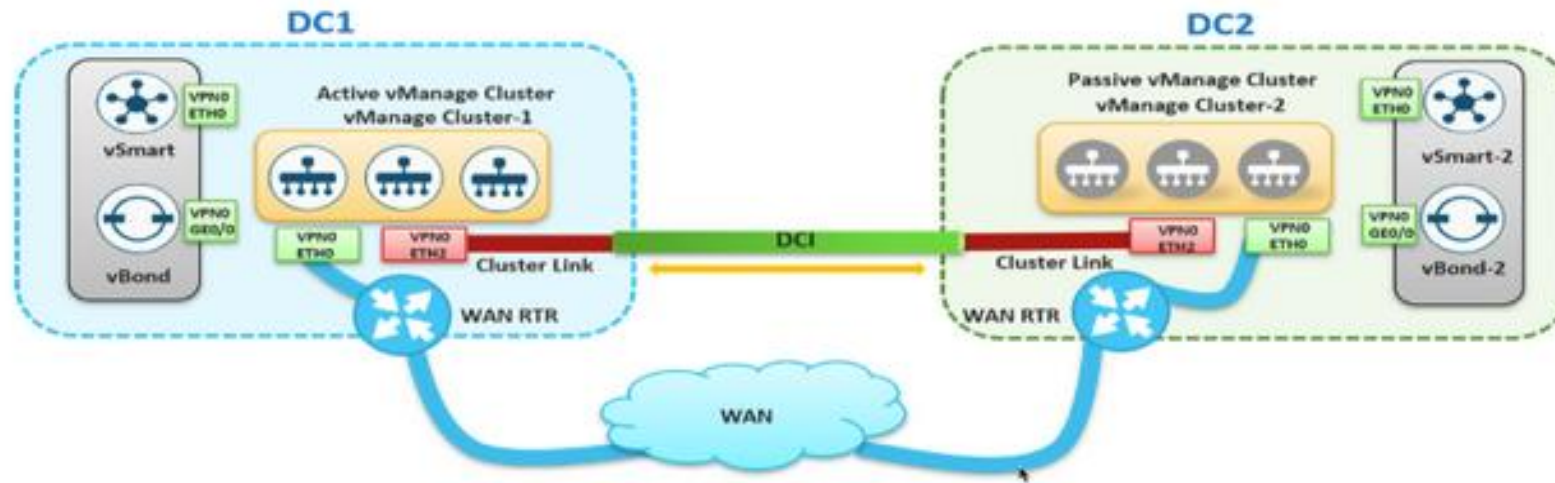
Response Headers

```
{
  "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 SD-WAN Manager 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”

Cisco SD-WAN

Select Resource Group

Administration • Disaster Recovery

☁️ ☰ ⓘ 🔔

Manage Disaster Recovery

Manage Password

⏸️ Pause Disaster Recovery

⏸️ Pause Replication

🗑️ Delete Disaster Recovery

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.

Cisco SD-WAN

Select Resource Group

Administration - Cluster Management

Service ConfigurationService Reachability

Add vManage

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

Cisco SD-WAN

Select Resource Group

Administration - Cluster Management

Service ConfigurationService Reachability

Current vManage : 1.1.1.1

Search

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 validator “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)

/dataservice/clusterManagement/reachability

```
"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

7. Send to Controllers:

`dataservice/certificate/vedge/list?action=push`

```
"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>  
]
```

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

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 scenarios
- Build your own API workflow

DR Failover prechecks



Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

