

LTRENS-2256

Cisco Catalyst Switching Innovations Lab

Sai Zeya – Technical Marketing Engineer

Aishwarya Sudeep – Technical Marketing Engineer

Ovua Harcourt – Technical Marketing Engineer

Table of Contents

Upon completion of this lab, you will be able to configure the following:

Topic	Time (mins)
Service Assurance with ThousandEyes	45
C9K AWS Cloud Integration (S3 & CloudWatch)	30
C9K Cloud Monitoring with Meraki	45
C9K Sustainability Features hands-on	30
xFSU	30

Disclaimer

This training document is to familiarize the student with Catalyst 9000 Innovative Technologies. Although the lab design and configuration examples could be used as a reference, this is not a real design. As a result, not all recommended features are used or enabled optimally. For design-related questions, please contact your representative at Cisco or a Cisco partner.

Introduction

Cisco Catalyst 9000 Switches are the next generation of enterprise-class switches built for security, Internet of Things (IoT), mobility, and multi-cloud taking advantage of the feature-rich Cisco IOS-XE software and field-reprogrammable UADP/Silicon One ASIC technologies which enables open programmability, analytics, and telemetry.

In this lab, the student will gain hands-on experience with some of the latest innovations of the Catalyst 9000 family switches using CLI and Cisco Catalyst Center.

All the lab scenarios are independent of one another. Based on the estimated times given in the Learning Objectives, please perform the lab exercises most important to you first.

Lab 1: Service Assurance with ThousandEyes

Learning Objectives

Upon completion of this lab, you will be able to:

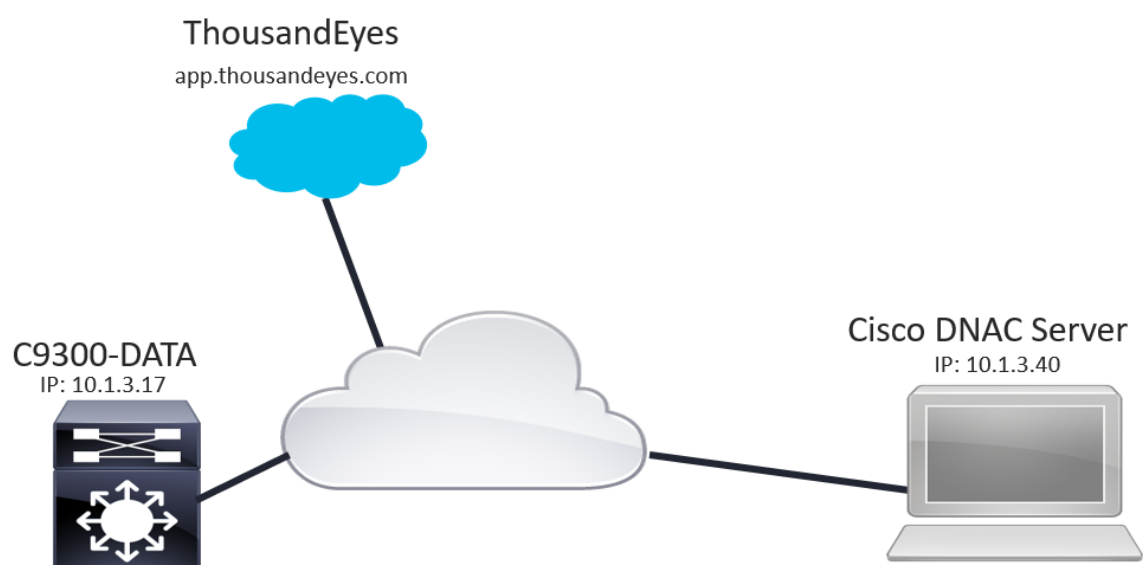
- Deploy ThousandEyes
- Use the ThousandEyes Web User Interface to complete an:
 - Agent to Server Test
 - HTTP Server Test
- Removing ThousandEyes from Switch

Scenario

ThousandEyes collects data from various vantage points deployed around the internet and inside customer networks. For the most part, these vantage points are called "agents" which can be hosted in the cloud (Cloud Agents), deployed or maintained by you or a customer (Enterprise Agents), or deployed on Windows or macOS workstations (Endpoint Agents). The ThousandEyes tests are classified based on the layers of operation such as the Network Layer. Each layer provides a means of monitoring the performance or metrics of the network of a customer or user.

In the workspace, employees are constantly utilizing SaaS applications, connecting with data centers, branch offices and interacting on the Internet. For the best user experience, network administrators need to have a constant monitoring platform to ensure that these user experiences are being done with little to no hindrance. The ThousandEyes Web UI allows different tests to be taken to understand the root cause of network issues. This enables the troubleshooting time period to be reduced drastically, allowing IT personnel to utilize their time on other resources.

Network Diagram



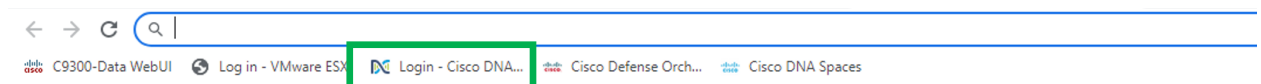
Step 1: Deploying ThousandEyes on Catalyst 9000

We will access the Cisco Catalyst Center to initiate the Day N workflow.

- Click on the **Chrome** icon pinned on the task bar



- Navigate to the bookmarked section > click **Login-Cisco Catalyst Center** (or) type **10.1.3.40** in the address bar > press Enter

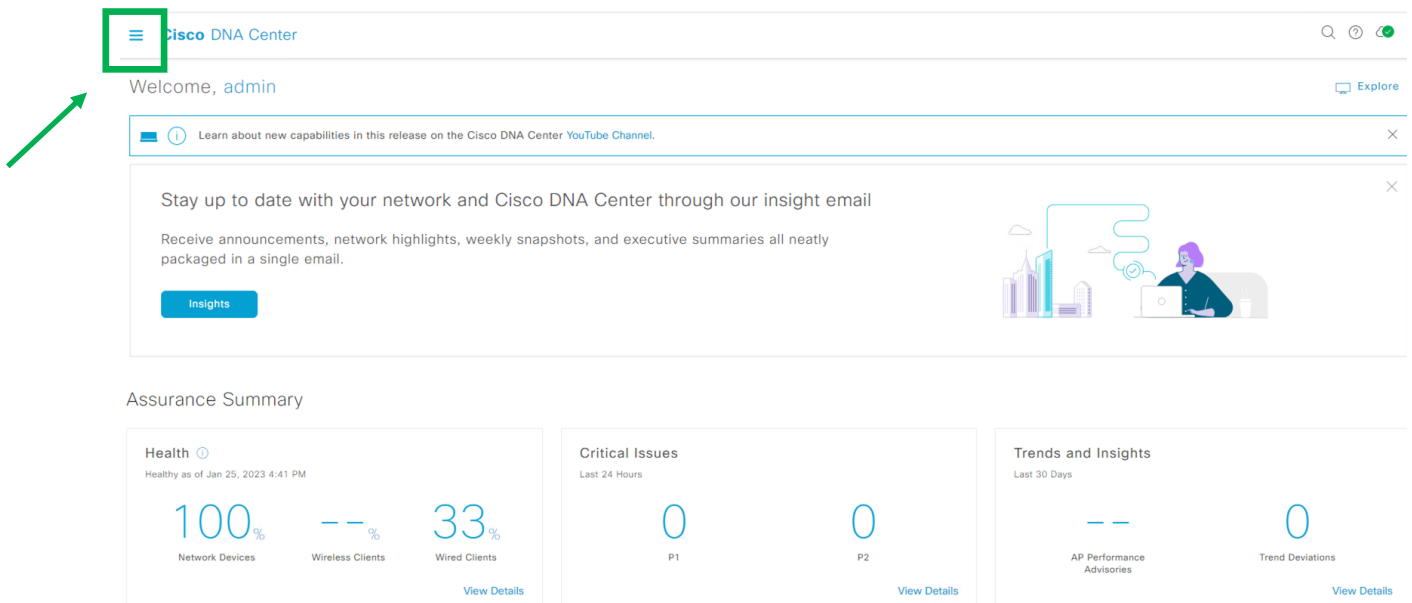


- To access **DNA Center**, enter the following credentials > click **Log in**

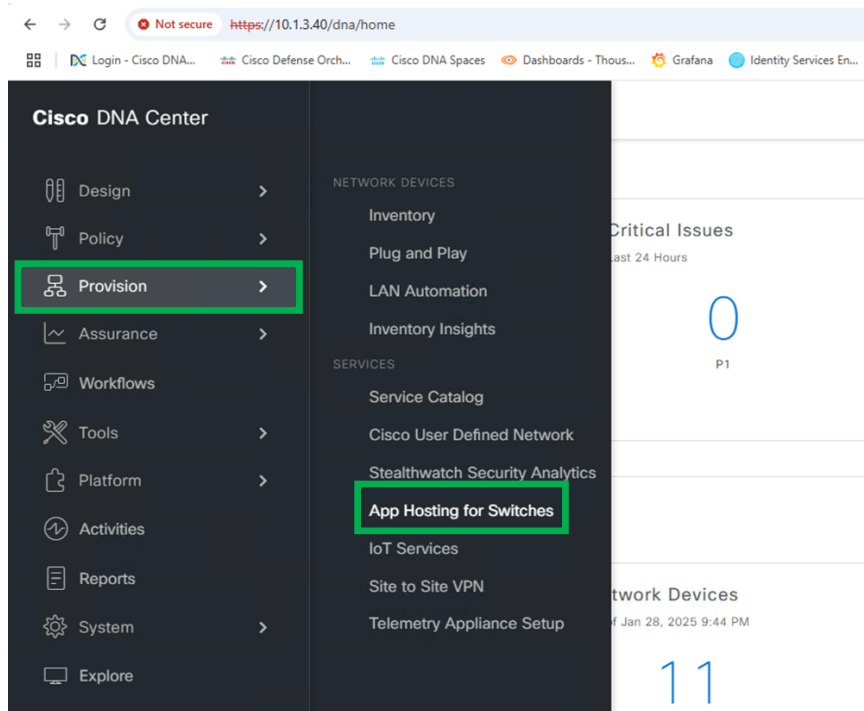
Username: admin

Password: Uabootcamp1

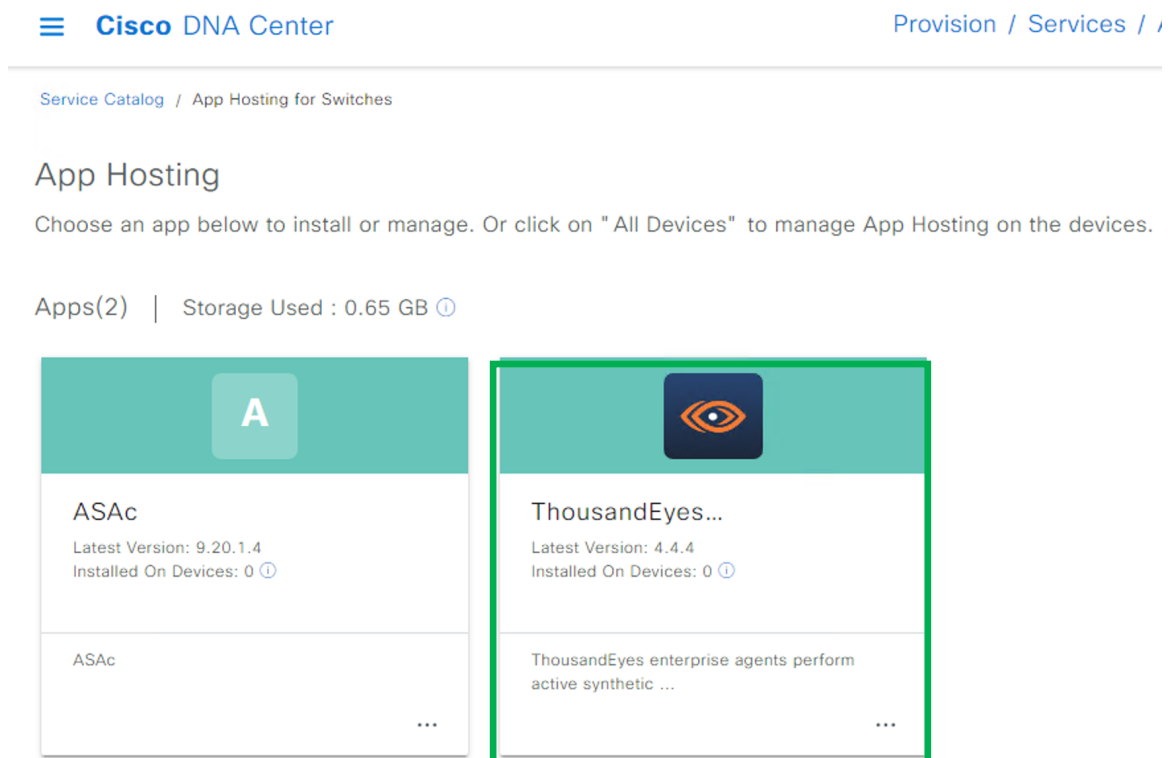
- Once logged into the DNA Center, click the **hamburger menu**



- Navigate to **Provision** > **App Hosting for Switches** to start the application deployment workflow.



- Select the **ThousandEyes App**.



- Click on **Edit** to update the Docker Runtime Options. The docker runtime option defines memory, account token key and storage volume and many others.



Edit

Author
ThousandEyes
<support@thousandeyes.com>

Last Updated On
5/14/2024, 10:41:11 AM

Update App

Delete App

ThousandEyes Enterprise Agent

Version: 4.4.4 | Installed On Devices: 0

App Description

ThousandEyes enterprise agents perform active synthetic measurements to your business-critical applications. See docs.thousandeyes.com/product-documentation/getting-started for the types of data you can collect using enterprise agents. Requires a minimum iOS-XE version of 17.3.3 on Catalyst 9300 or 17.5.1 on Catalyst 9400.

Docker Runtime Options

```
-e TEAGENT_ACCOUNT_TOKEN=token --hostname=$(SYSTEM_NAME) --mount type=tmpfs,destination=/var/tmp/te-agent,tmpfs-size=340m -e TEAGENT_PROXY_TYPE=DIRECT -e TEAGENT_PROXY_LOCATION= -e TEAGENT_PROXY_USER= -e TEAGENT_PROXY_AUTH_TYPE= -e TEAGENT_PROXY_PASS= -e TEAGENT_PROXY_BYPASS_LIST= -e TEAGENT_KDC_USER= -e TEAGENT_KDC_PASS= -e TEAGENT_KDC_REALM= -e TEAGENT_KDC_HOST= -e TEAGENT_KDC_PORT=88 -e TEAGENT_KERBEROS_WHITELIST= -e TEAGENT_KERBEROS_RDNS=1 -e PROXY_APT= -e APT_PROXY_USER= -e APT_PROXY_PASS= -e APT_PROXY_LOCATION= -e TEAGENT_AUTO_UPDATES=1 -e TEAGENT_SERVICES_ALLOW_IPV6=0
```

Edit

- Add TEAgent Account Token and Edit Hostname as below:
 -e TEAGENT_ACCOUNT_TOKEN=**jjyoh4yneku88754x96u3pfkps2brcyc**
 --hostname=**teye-pod<POD_number>**

i.e teye-pod1

Note: TEAGENT_ACCOUNT_TOKEN can get from your ThousandEyes Account.

```
-e TEAGENT_ACCOUNT_TOKEN=jjyoh4yneku88754x96u3pfkps2brcyc --hostname=teye-pod<POD_number> --mount type=tmpfs,destination=/var/log/agent,tmpfs-size=140m --mount type=tmpfs,destination=/var/lib/te-agent/data,tmpfs-size=200m -v $(APP_DATA)/data:/var/lib/te-agent -e TEAGENT_PROXY_TYPE=DIRECT -e TEAGENT_PROXY_LOCATION= -e TEAGENT_PROXY_USER= -e TEAGENT_PROXY_AUTH_TYPE= -e TEAGENT_PROXY_PASS= -e TEAGENT_PROXY_BYPASS_LIST= -e TEAGENT_KDC_USER= -e TEAGENT_KDC_PASS= -e TEAGENT_KDC_REALM= -e TEAGENT_KDC_HOST= -e TEAGENT_KDC_PORT=88 -e TEAGENT_KERBEROS_WHITELIST= -e TEAGENT_KERBEROS_RDNS=1 -e PROXY_APT= -e APT_PROXY_USER= -e APT_PROXY_PASS= -e APT_PROXY_LOCATION= -e TEAGENT_AUTO_UPDATES=1
```

- Click **“Save”** and then Click **“Install”**.

ThousandEyes Enterprise Agent

Version: 4.4.4 ✓

Installed On Devices: 0 ⓘ

App Description

ThousandEyes enterprise agents perform active synthetic measurements to your business-critical applications. See <https://docs.thousandeyes.com/product-documentation/getting-started> for the types of data you can collect using enterprise agents. Requires a minimum IOS-XE version of 17.3.3 on Catalyst 9300 or 17.5.1 on Catalyst 9400.

Docker Runtime Options

```
-e TEAGENT_ACCOUNT_TOKEN=jjyoh4yneku88754x96u3pfkps2br cyc --hostname=teye-pod2 --mount
type=tmpfs destination=/var/tmp/te-agent tmpfs-size=340m -e TEAGENT_PROXY_TYPE=DIRECT -e
TEAGENT_PROXY_LOCATION= -e TEAGENT_PROXY_USER= -e TEAGENT_PROXY_AUTH_TYPE= -e
TEAGENT_PROXY_PASS= -e TEAGENT_PROXY_BYPASS_LIST= -e TEAGENT_KDC_USER= -e
TEAGENT_KDC_PASS= -e TEAGENT_KDC_REALM= -e TEAGENT_KDC_HOST= -e TEAGENT_KDC_PORT=88 -e
TEAGENT_KERBEROS_WHITELIST= -e TEAGENT_KERBEROS_RDNS=1 -e PROXY_APT= -e APT_PROXY_USER=
-e APT_PROXY_PASS= -e APT_PROXY_LOCATION= -e TEAGENT_AUTO_UPDATES=1 -e
TEAGENT_SERVICES_ALLOW_IPV6=0
```

Cancel

Save

Manage

Install

- Type Task Name: **“ThousandEyes”** and Click **Next**

☰ Cisco DNA Center

Enable Apps on Switches

Get Started

Assign a unique name for your workflow for identification. You can exit the workflow at any stage and resume later.

ⓘ

 Ensure all prerequisites are fulfilled on the devices before proceeding with enabling app-hosting. [Click here](#) to know more.

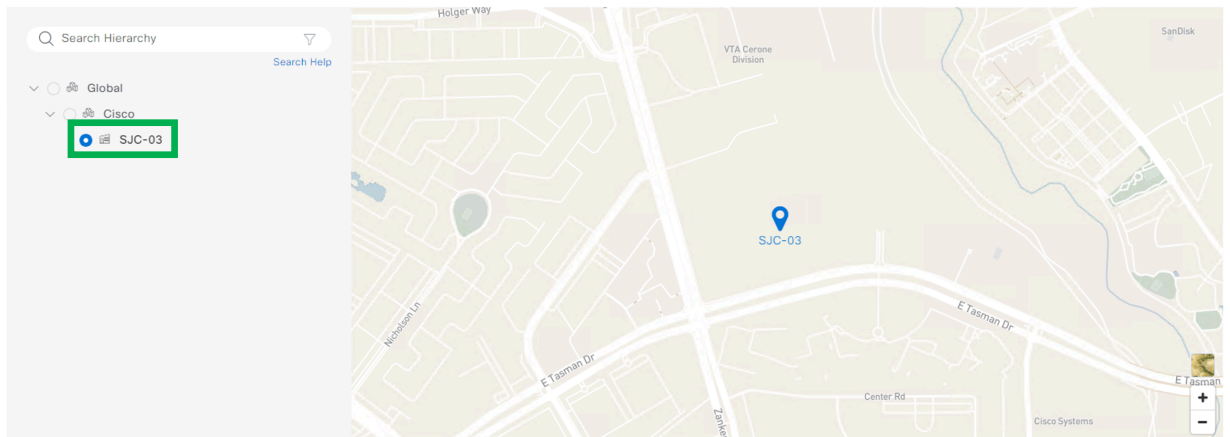
Task Name*

ThousandEyes

- Then Select Site: **SJC-03** and Click **Next**

Select Site

Select the site where you want to enable the app



- Select the **IP-BDR** switch and Click **Next**

Select Switches

Select switches where you want to enable **ThousandEyes Enterprise Agent**.

Switches (11) Import Export As of: Jan 28, 2025 10:03 PM

Filter 0 Selected

☐	Device Name	Site	IP Address	Serial Number	Image Version	Device Series	Readiness
☐	C9500-32C-1.cisco.com	.../Cisco/SJC-03	10.1.3.21	CAT2409L1UN, CAT2409L1TF	17.6.3	Cisco Catalyst 9500 Serie...	Not Ready See Details
☐	IP-BDR.cisco.com	.../Cisco/SJC-03	10.1.3.4	FCW2417D004	17.12.2prd1	Cisco Catalyst 9300 Serie...	Ready See Details
☐	S1-ACCESS-LEAF-1.cisco.com	.../Cisco/SJC-03	10.1.3.15	FXS2352Q0JS	17.13.1	Cisco Catalyst 9400 Serie...	Not Ready See Details
☐	S1-ACCESS-LEAF-2.cisco.com	.../Cisco/SJC-03	10.1.3.7	FJB2409E01P	17.13.1	Cisco Catalyst 9500 Serie...	Not Ready See Details
☐	S1-ACCESS-LEAF-3.cisco.com	.../Cisco/SJC-03	10.1.3.5	FJC2412E059	17.16.20240515:040254	Cisco Catalyst 9300 Serie...	Not Ready See Details

11 Records Show Records: 25 1 - 11

- Next, Select the VLAN for application Management
Assign VLAN 3 and Select Static as Address Type. Then Click Import to import IP address for the app.

Configure App

Configure app specific settings to bootstrap **ThousandEyes Enterprise Agent**.

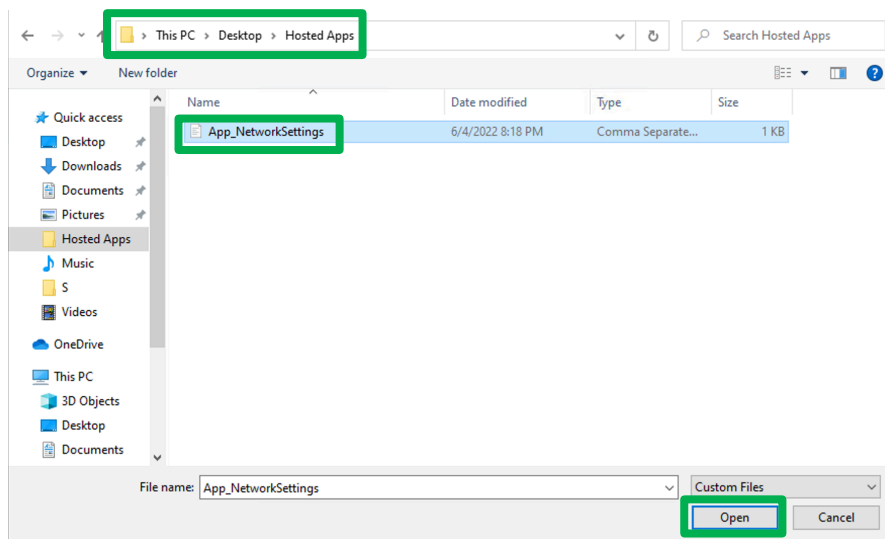
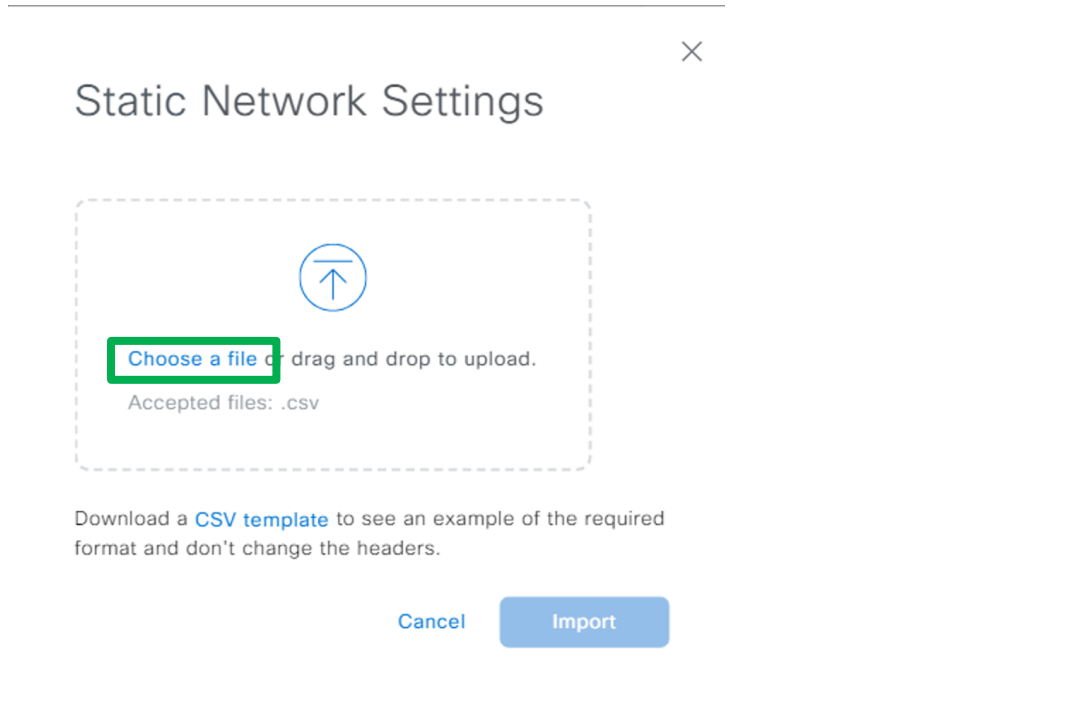
Network Settings

Interface Name: eth0

VLAN: **VLAN0003** Address Type: **Static** Import Export

Device Name	Device IP	Interface IP	Gateway IP
IP-BDR.cisco.com	10.1.3.4		

- Click **“Choose a file”** and Select **“App_NetworkSettings”** from **Desktop -> Hosted Apps folder**.



- Click **“Open”** then click **Import**.

Configure App

Configure app specific settings to bootstrap **ThousandEyes Enterprise Agent**.

Network Settings

Interface Name	VLAN	Address Type			
eth0	VLAN0003	Static	Import	Export	
Device Name	Device IP	Interface IP	Gateway IP	Prefix	DNS IP
IP-BDR.cisco.com	10.1.3.4	10.1.3.51	10.1.3.252	24	8.8.8.8

- Click **Next**.
- In Summary page, Verify the Config and Click **Provision**

Summary

Review your app deployment configurations. To make changes, click Edit. [Download Summary](#) | [Configuration Preview](#)

Site

Global/Cisco/SJC-03

Switches

Total 1 switch selected

Settings

Network Settings

Interface	eth0				
VLAN	VLAN0003				
Address Type	static				
Device Name	Device IP	Interface IP	Gateway IP	Prefix	DNS IP
IP-BDR.cisco.com	10.1.3.4	10.1.3.51	10.1.3.252	24	8.8.8.8

1 changes saved

Activate Windows

Back

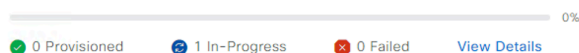
Provision

- Provisioning may take 1-2 minutes depending on number of devices you are deploying. In this lab, it should take around 1 minute.

Track Provisioning Status

Provisioning of **ThousandEyes Enterprise Agent** is in progress.

Task Progress



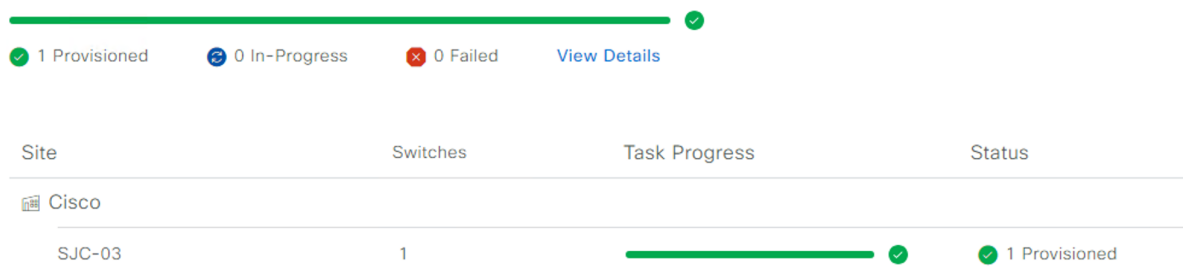
Site	Switches	Task Progress	Status
Cisco			
SJC-03	1	0%	1 In-Progress

- Once the installation is complete: Click **Next**

Track Provisioning Status

Provisioning of **ThousandEyes Enterprise Agent** is completed.

Task Progress



- Then Click **Manage App**. You will see ThousandEyes app is successfully deployed on the IP-BDR switch.



Done! Task Completed

ThousandEyes Enterprise Agent successfully enabled on 1 Switch

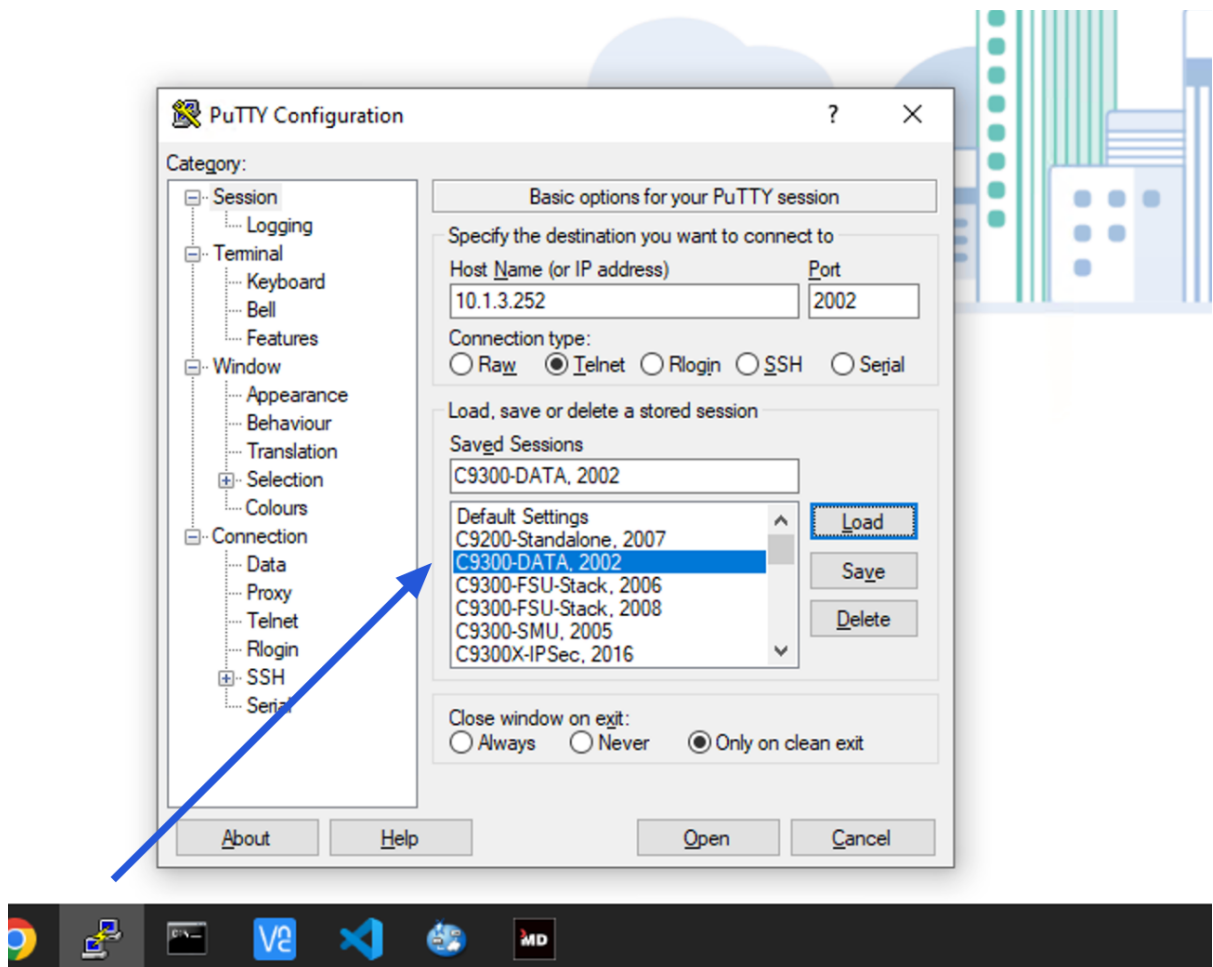
1 Switch on SJC-03 at Cisco provisioned successfully

What's Next?

[Manage App](#)

[Workflows Home](#)

- Now launch putty and telnet into the switch cli, If asked for credentials:
 Username : **tmelab**
 Password : **Uab00tcamp!**



- Run the command **show app-hosting list** to confirm the app being provisioned and configured by Cisco DNAC.

```

IP-BDR>
IP-BDR>
IP-BDR>en
IP-BDR#show app
IP-BDR#show app-hosting lis
IP-BDR#show app-hosting list
App id                                     State
-----
ThousandEyes_Enterprise_Agent             RUNNING
IP-BDR#

```

Step 2: Using the ThousandEyes Web UI

- Login to the Web UI of ThousandEyes:

<https://app.thousandeyes.com/login>

Use the following credentials access the Web UI:

Username: **teyedemo@gmail.com**

Password: **Teyedemo!**

HTTP Server Test

Almost all applications in the workplace have been moved to the cloud including Microsoft Office. This causes most organizations to rely on applications serviced by the SaaS network infrastructure over which they have no control. To ensure that the workforce has the best application experience, monitoring of the network infrastructure is critical. With SaaS, users rely on the SaaS provider's infrastructure and software performance monitoring as well as external dependencies such as DNS and ISPs. This test will provide visibility into the entire application service delivery chain for multi-layer SaaS performance management by providing deep insights into the network as well as external dependencies.

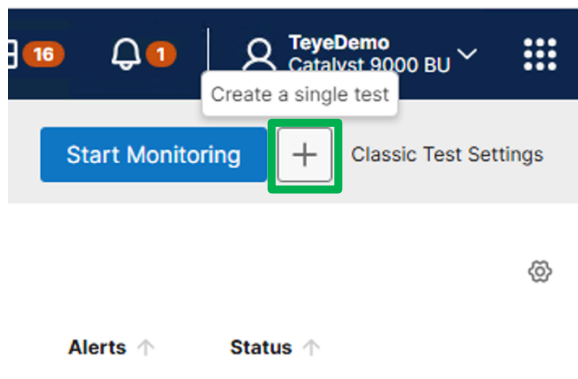
We will be accessing the performance of the network with different parameters, such as when reaching the Office365 server in the cloud with the HTTP Server Test Setting.

- Under Cloud and Enterprise Agents select Test Settings.

The screenshot displays the Cisco ThousandEyes Dashboards interface. The left sidebar contains navigation options: Cloud & Enterprise Agents (selected), Event Detection, Views, Test Settings (highlighted with a green box), Agent Settings, BGP Monitors, Endpoint Agents, Cloud Insights, Devices, and Internet Insights. The main content area shows 'OVERALL AVAILABILITY' for 'Web - HTTP Server' with a value of 99.24%. Below this are five green boxes showing availability for different services: AWS Console (100), Box (100), Facebook (95.64), GitHub (100), and Google Apps (99.98). A 'Tests' section shows a list of tests with columns for Test Name, Test Type, and Alert Status. The tests listed are Facebook, Microsoft Office 365 Login, and Google Apps / Gmail Login. The Facebook test has a red alert icon.

- To begin the HTTP server test using Office365 as an endpoint, click on the “Create a single test” button at the right corner of the screen.

- 13 -



Select the following options in the box:

- i. **Layer:** Web
- ii. **Test Type:** HTTP Server
- iii. **Test Name:** POD < your pod number >

 The screenshot shows the 'Test Settings' form. The 'New Test' section has tabs for 'Layer' (Routing, Network, DNS, Web, Voice) and 'Test Type' (HTTP Server, Page Load, Transaction, API, FTP Server). The 'Web' layer and 'HTTP Server' test type are selected and highlighted with green boxes. Below these are input fields for 'Test Name' and 'Test Description', both labeled 'Optional'. The 'Basic Configuration' section includes fields for 'URL' (e.g. http[s]://domain:port/path), 'Interval' (2 minutes), 'Agents' (Select agent(s)), and 'Alerts' (Enable, 3 of 7 alert rules selected). At the bottom are 'Cancel', 'Run Once', and 'Create New Test' buttons.

- For Basic Configuration select the following parameters
 - i. **URL:** office365.com
 - ii. **Interval :** 1 minute
 - iii. **Agents :** Select drop-down menu,

Add New Test ▾

New Test

Layer: Routing Network DNS Web Voice

Test Type: Agent to Server Agent to Agent

Test Name:

Test Description:

Basic Configuration Advanced Settings

Target:

Protocol: TCP Port:

Probing Mode: Prefer SACK Force SACK Force SYN

Path Trace Mode: ☐ In Session

Interval: 1 minute

Agents: Select agent(s)

Alerts: ☒ Enable
1 of 3 alert rules selected [Edit Alert Rules](#)

Cancel Run Once Create New Test

- iii. Under Built-In Labels on the right side of the box, select “Enterprise”.
- iv. Select the agent with your <pod name>. For example, teye-pod5.

Searching...

Show All Selected Enabled

North America
1 of 17 agents

- ☐ KLEI-SFO
- ☐ TEDemo
- ☐ teye-pod2
- ☐ teye-pod3
- ☐ teye-pod4
- ☒ teye-pod5
- ☐ teye-pod6
- ☐ teye-pod7
- ☐ teye-pod8
- ☐ teye-pod9
- ☐ teye-pod10
- ☐ teye-pod11
- ☐ teye-pod11-1420796
- ☐ teye-pod12
- ☐ teye-pod13

Built-In Labels

- ☒ Enterprise
- ☐ Enterprise Cluster
- ☐ IPv4 Compatible
- ☐ IPv6 Compatible
- ☐ Proxied
- ☐ Single Homed
- ☐ Dual Chromium

Custom Labels

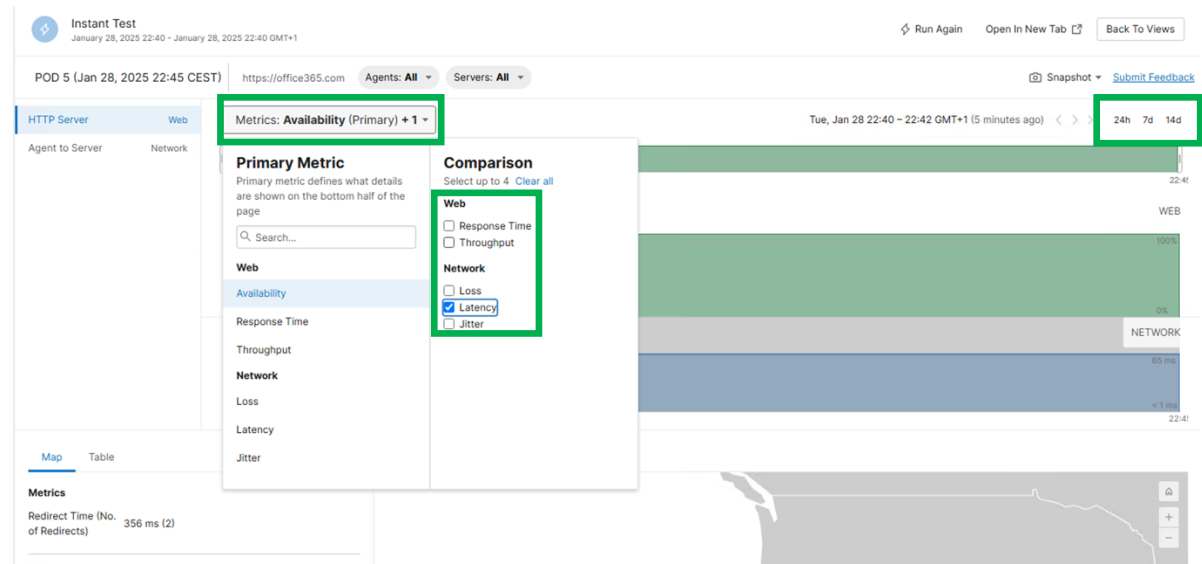
- ☐ ATX_Demo
- ☐ dacole2

- v. Select the “Create New Test” Test button at the bottom of the box to complete it.

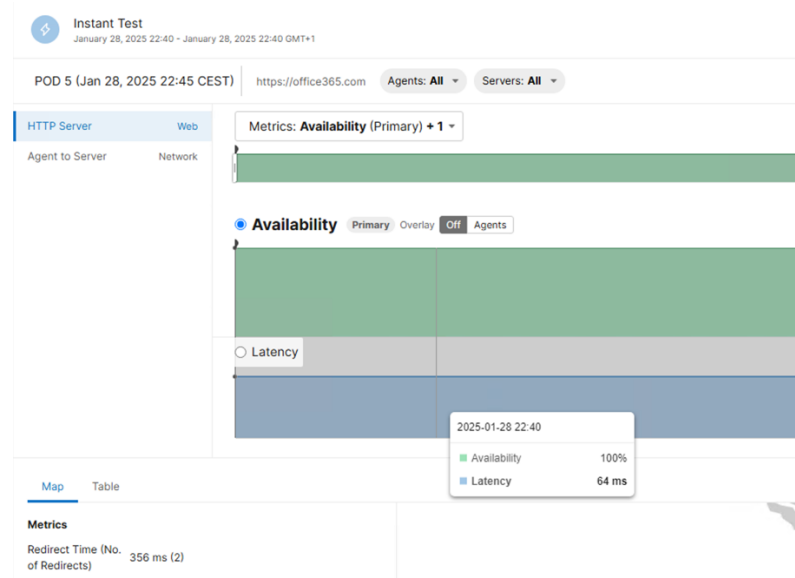
Analyze Results from Agent to Server Test

Note: Please wait about 1 minute to see the data in dashboard.

1. In the Metric drop-down box, select Latency.
2. Under Overview, the graph shows the average metric for the agent selected over a stipulated time of 24hrs, 7days or 14 days.

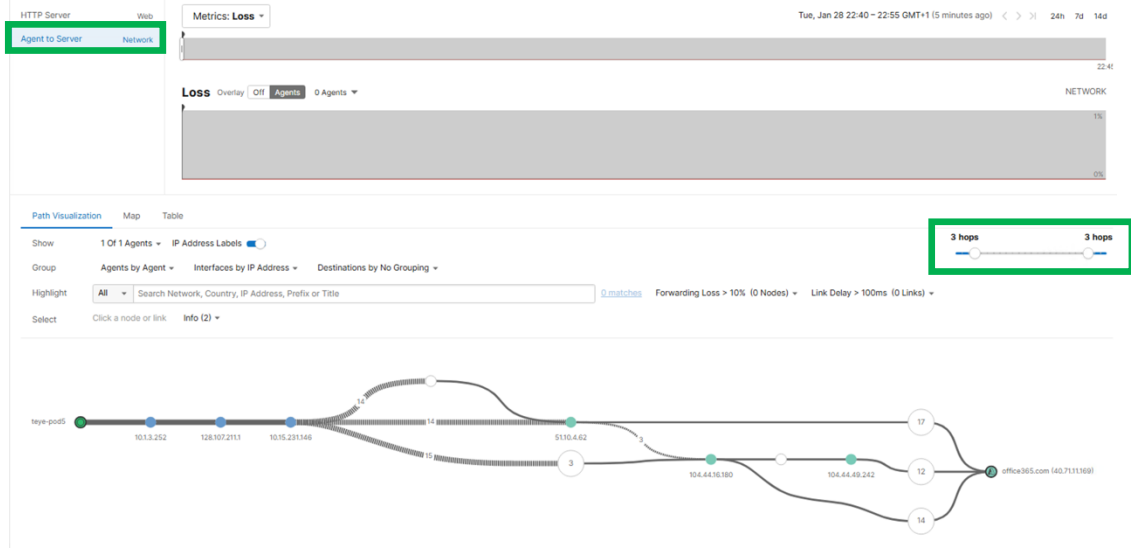


3. In the Map section of the dashboard, the “Latency” metric is displayed over the time period.



4. Select the other metrics (such as Loss and Jitter) in the “Metric” drop-down box to view.

5. In the Views section of the Dashboard, select “Agent to Server” to see full path from the C9K ThousandEyes agent to the Office365 server. Hovering the mouse over a node on the path will show more details for that node (such as location, IP and network).

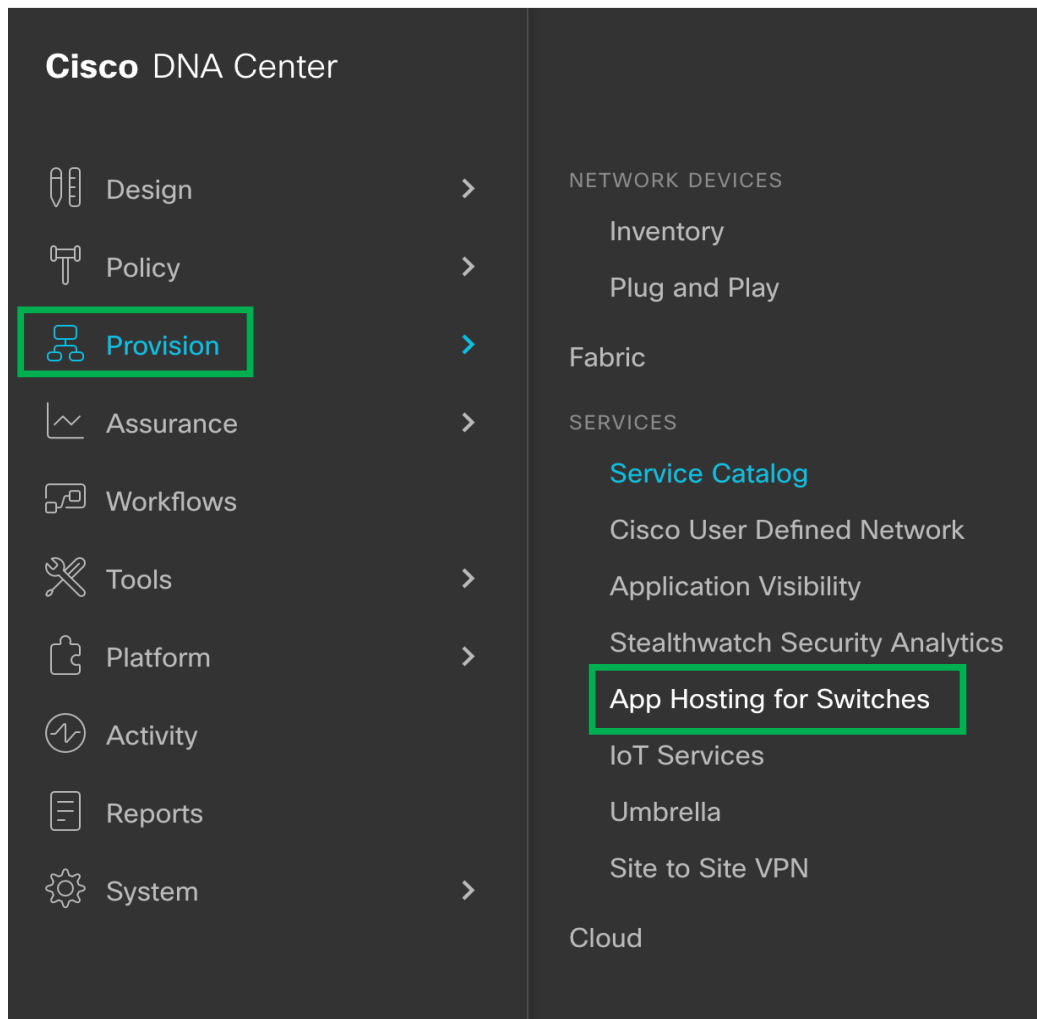


6. Hovering the mouse over each display’s information about the IP addresses of the previous and next hops, number of traces and the time taken. This provides more insight into where delays are occurring and the reason why they are occurring.

Now you have learned how to create the tests and observe the results. You can try with others test on your own before you do next task.

Step 3: Uninstalling ThousandEyes from DNA Center

- Return to the DNA Center window in Chrome.
- Select Hamburger Icon  -> **Provision** -> **App Hosting for Switches**



- Select **ThousandEyes** Enterprise Agent App
- Select **Manage**

Home / ThousandEyes Enterprise Agent



ThousandEyes Enterprise Agent

Version: 4.4.4 | Installed On Devices: 1

App Description
ThousandEyes enterprise agents perform active synthetic measurements to your business-critical applications. See docs.thousandeyes.com/product-documentation/getting-started for the types of data you can collect using enterprise agents. Requires a minimum IOS-XE version of 17.3.3 on Catalyst 9300 or 17.5.1 on Catalyst 9400.

Docker Runtime Options
~e TEAGENT_ACCOUNT_TOKEN=jjyoh4yneku88754x96u3pfks2bryc --hostname=taye-pod2 --mount type=tmpfs,destination=/var/tmp/te-agent,tmpfs-size=340m -e TEAGENT_PROXY_TYPE=DIRECT -e TEAGENT_PROXY_LOCATION= -e TEAGENT_PROXY_USER= -e TEAGENT_PROXY_AUTH_TYPE= -e TEAGENT_PROXY_PASS= -e TEAGENT_PROXY_BYPASS_LIST= -e TEAGENT_KDC_USER= -e TEAGENT_KDC_PASS= -e TEAGENT_KDC_REALM= -e TEAGENT_KDC_HOST= -e TEAGENT_KDC_PORT=68 -e TEAGENT_KERBEROS_WHITELIST= -e TEAGENT_KERBEROS_RDNS=1 -e PROXY_APT= -e APT_PROXY_USER= -e APT_PROXY_PASS= -e APT_PROXY_LOCATION= -e TEAGENT_AUTO_UPDATES=1 -e TEAGENT_SERVICES_ALLOW_IPV6=0

Author
ThousandEyes
support@thousandeyes.com

Last Updated On
5/20/2024, 10:57:12 AM

Update App
Delete App

Manage

Install

- Select **IP-BDR**
- Select **“Actions”** and from the drop down, select **“Uninstall App”**

Home / ThousandEyes Enterprise Agent / Manage

ThousandEyes Enterprise Agent

Devices (1) All Running Stopped Failed In Progress

Search Hierarchy

Search Help

Global

Unassigned Devices

Cisco

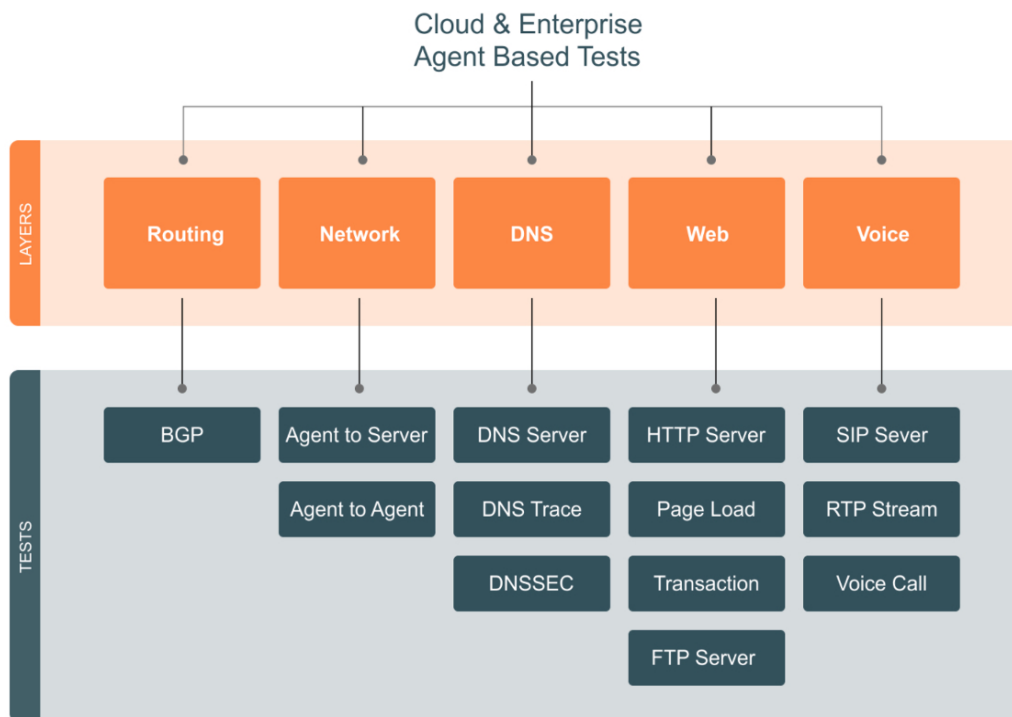
Filter 1 Selected

As we are in 'App Hosting for Switches', this page displays only

Hostname	Device IP	Actions
IP-BDR.cisco.com	10.1.3.4	Start App Stop App Upgrade App Uninstall App

Summary

Below are the different tests that can be undertaken with ThousandEyes depending on the layer of interest. This lab featured the Web and Network layers, with the tests centerer on Agent to Agent, Agent to Server and HTTP Server. ThousandEyes monitors the network infrastructure and provides analytics that aid in troubleshooting and facilitate decisions to improve the infrastructure.

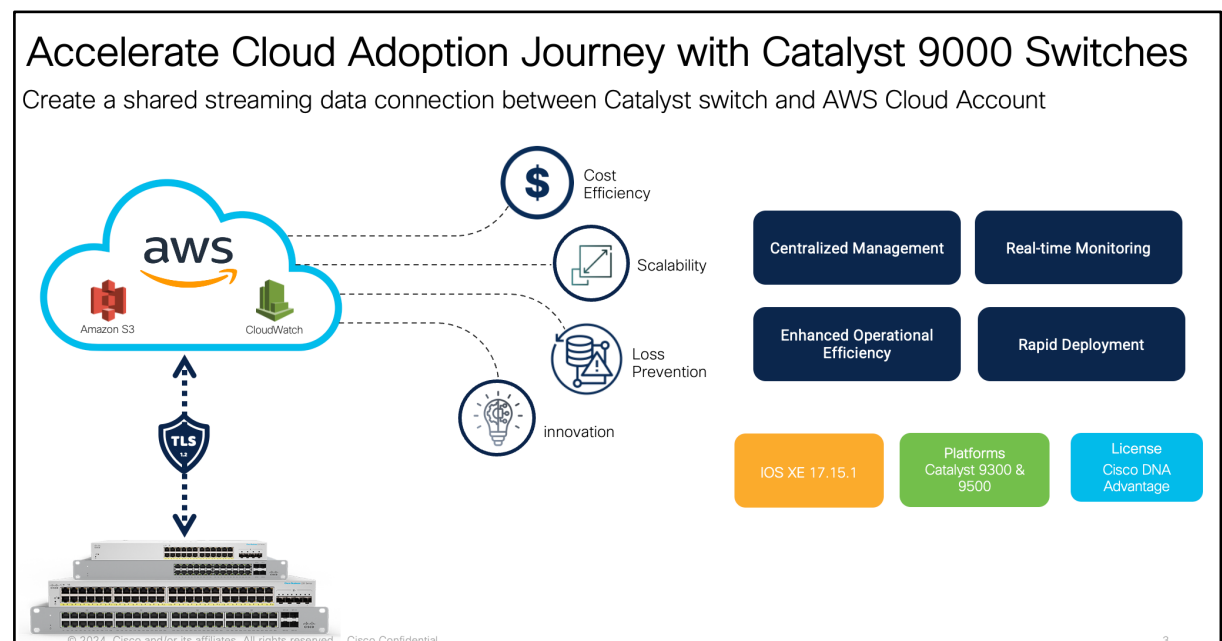


Lab 3: Cloud Integration on C9K with S3 and CloudWatch

Introduction

Cisco IOS-XE devices have built-in persistent storage. There are increasing demands on available storage in the form of increased logging rates, software images, core files etc. There are also requirements for easy distribution of software images, SMUs and various scripts to multiple devices. Reliable cloud storage such as Amazon S3 has become ubiquitous. This shared-storage option extends the available storage capabilities on Cisco IOS XE devices.

In this lab activity, you will learn how to create cloud storage instances (such as an Amazon S3 bucket and an Amazon CloudWatch log group) and make them available as part of the device file system via configuration. We will also explore use cases on moving files between our C9K switches and our cloud storage instances. A single storage instance could be mapped read-only to multiple devices for distribution of images, configuration, scripts etc. Each device could have a separate read-write storage instance mapped for storing logs, core files etc

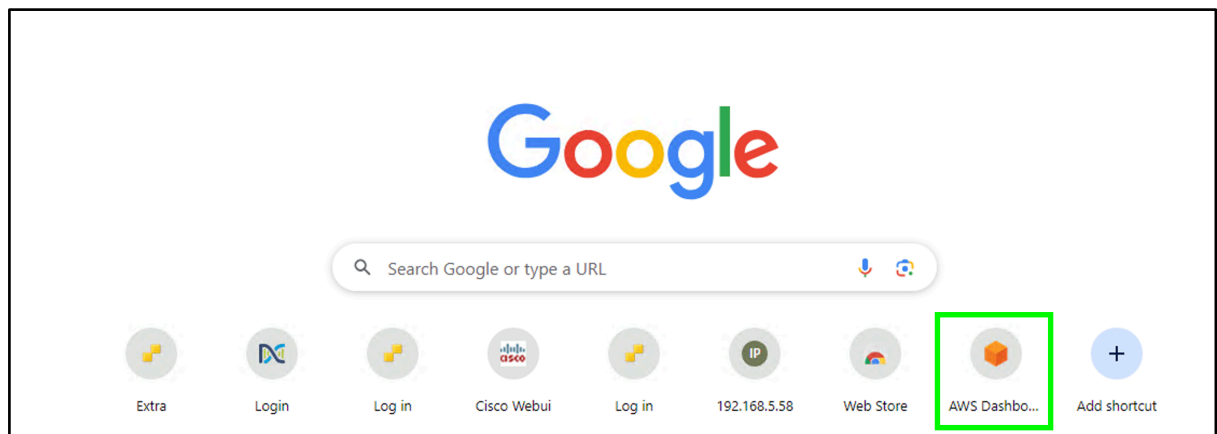


Task 1: S3 Configuration

Step 1: View S3 buckets in AWS user account

In the browser, select the AWS dashboard shortcut named: “**AWS Dashboard**” or <https://console.aws.amazon.com/> to Log into AWS user account with the below credentials.

Note: The icon for the shortcut might be different from the one shown in the image below.



Sign in using Root user email

Sign in

☒ **Root user**
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**
User within an account that performs daily tasks. [Learn more](#)

Root user email address

Next

NOTE: use email appropriate for your pod number

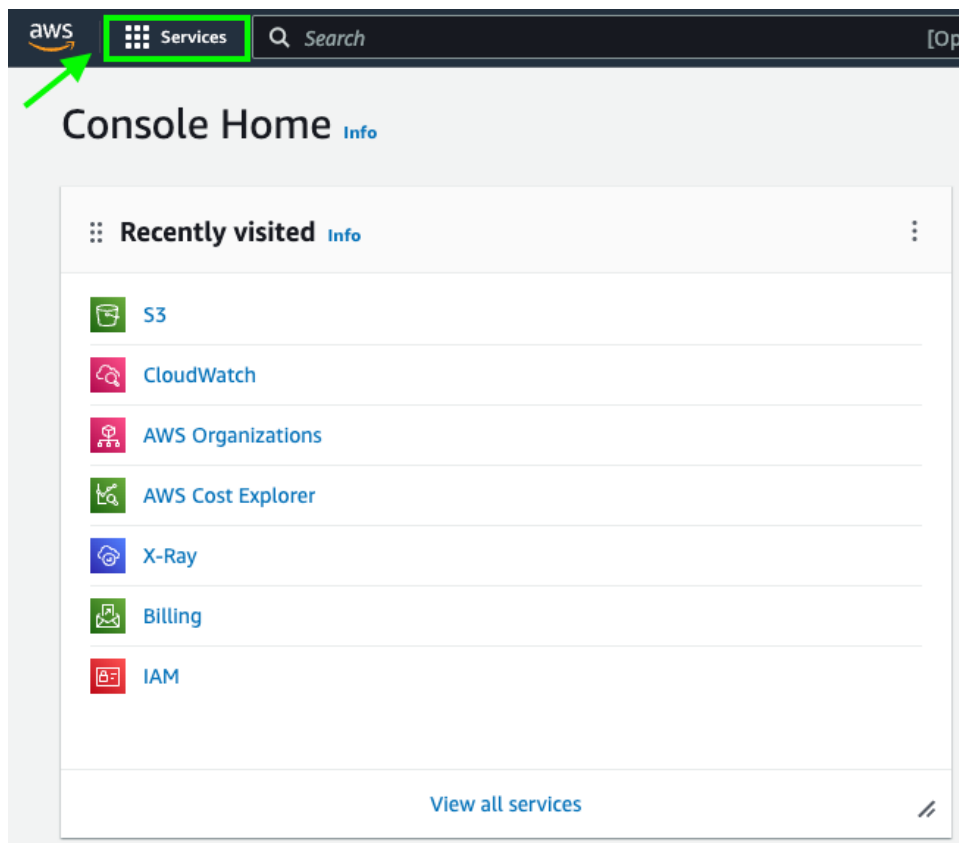
For pods 1–9 cat9k.podn@gmail.com, where n is the pod number

For pods 10–12: cat9k.podnv2@gmail.com, where n is the pod number

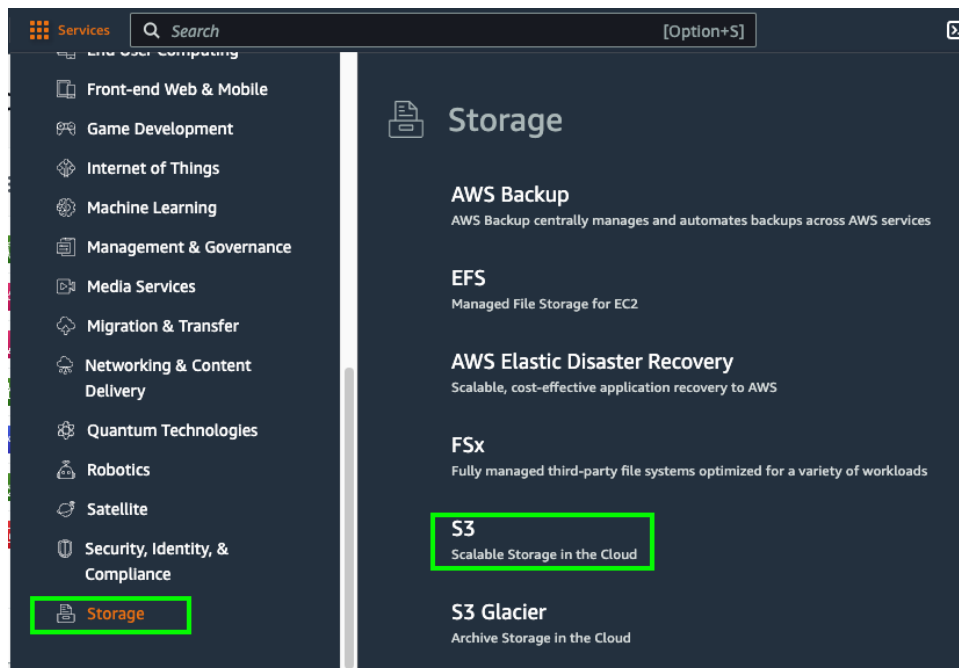
For pods 13-16: cat9k.podnv3@gmail.com, where n is the pod number
Password: C1sc0dna123

ALSO NOTE: If you are requested to provide a MFA verification code, please notify the proctor with your pod number, and you'll be provided with the code.

Once in the AWS account dashboard, select the **Services** menu on the left corner of the dashboard.



Navigate to **Storage** on the services list. Select **S3** when it pops up on the right side

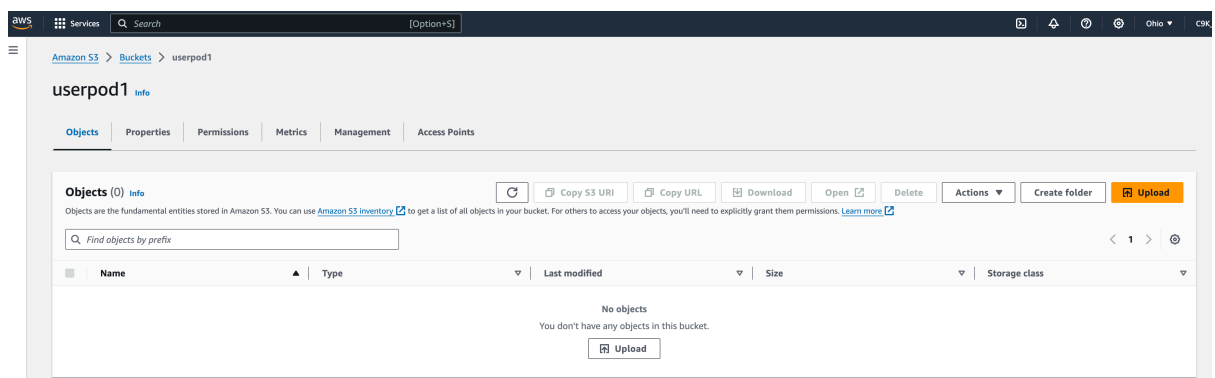


Once you are in **Amazon S3**, navigate to the **Buckets** section on the dashboard.

Here, the S3 bucket corresponds to a single pod user.

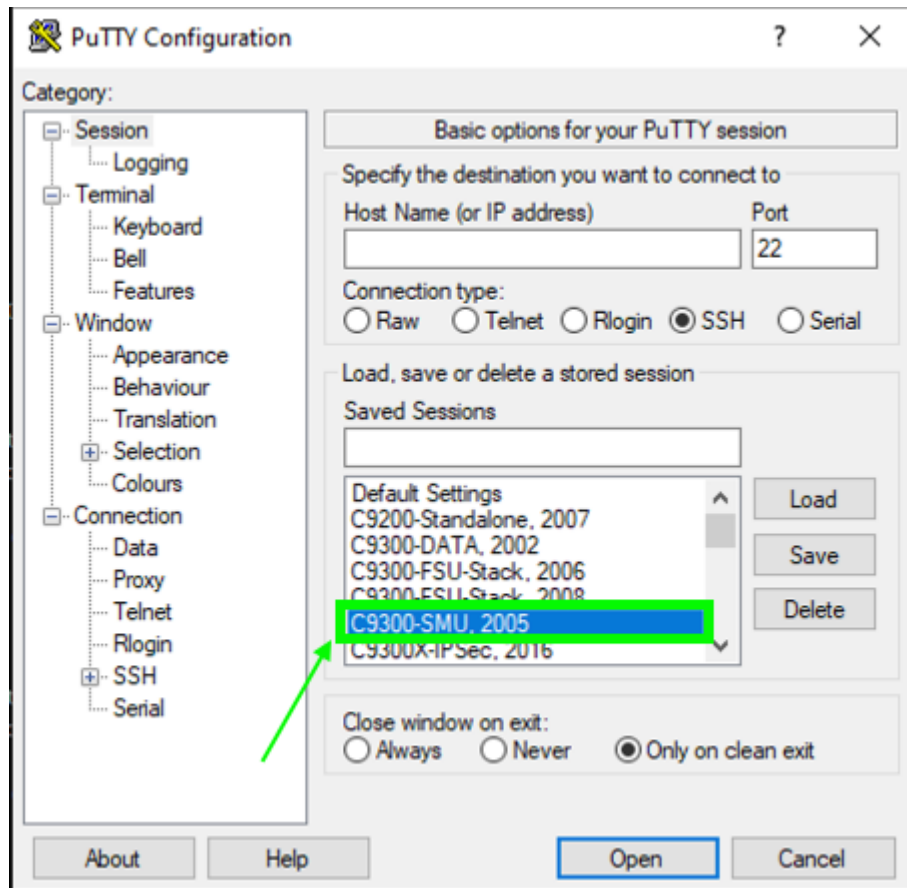
In each bucket, we can store files, images, logs and scripts that can be transferred between the switch and our AWS S3 account.

In your bucket for your pod, view the files within the bucket. You will notice there are currently no files. We will be transferring files from the switch to the AWS S3 bucket and vice versa in this lab.



Step 2: Configure S3 integration on C9300 switch.

Log into the C9300-SMU switch from Putty.



We will now configure our switch to sync with the AWS account we have. On the CLI, copy and paste the following commands to configure S3 on the switch.

Create S3 profile.

```
S1-ACCESS-LEAF-3# config terminal
S1-ACCESS-LEAF-3(config)#cloud-services aws s3 profile
s3pod<pod number>
```

Configure AWS IAM credentials. This allows to sync our catalyst switches to our AWS user accounts.

```
S1-ACCESS-LEAF-3 (config-s3-profile) #access-key key-id  
<access key> secret-key 0 <secret key>
```

Insert the access key and secret key that belongs to your pod from the table below

POD NUMBER	ACCESS KEY	SECRET KEY
POD 1	AKIA2OAJTXLNLG65PY65	Juw0amt6e8C3oZKIPImOsBx9biCUaekRFxpYwYno
POD 2	AKIA5G2VGZNPZQBPJI7M	UOYueC+1GMqmMyQCHNV1nwII1u2fFs/1epOWyx8m
POD 3	AKIA3FLD2PDOHHREV5FT	AwOUVep+xobH4+duQVjdiWkOxeWvd7i2P3cgyzDT
POD 4	AKIAXEFUNQO42UY4NHP3	UEXH07rvlctH69iyJ7MZ430YMLfx+9rvmoNLmFIW
POD 5	AKIAU5LH54DYCGQZA4P5	Az9w+DgbT5ztNckJ2KtekELiZiZ+x18YCbJPwBB
POD 6	AKIAXZ5NGMPQAZ7SWJCP	yV5A2pwxI76AVGKqGKL3w8HQGTj+qv4/354AbCxp
POD 7	AKIAT4GVR5U4TYLYH7ZN	TQTTPMIWLkHTIapeVIM7Lqktv2iEhErRzWwEJhaM
POD 8	AKIATNVEVQYZGR4SV4U3	cVQzLDJooAYGsJ6SKOwPxj860H6Tri/I3qWZCM+y
POD 9	AKIA3CMCCCTGD37FIVML	aHjUUJkF90X30bjD9BIRTy2aZ2UApUvunoqzKsBR
POD 10	AKIA2YICAP2V5GBLJB4V	WssqmOhEwRDtrPdELwazNH5+xWpbcXK5PwHp+Bpt
POD 11	AKIA3M7ACUEL7GQGNNMYD	5PO8iZ3cA/G+tJSegMmuojYbNBGKiDN9RVzDmkjl
POD 12	AKIAXYKJSTSNFU4E5TGJ	tu7Zmtw04ThqhuO7ZzGwoFJzeXfSI72Lb+qwLSh
POD 13	AKIAYXWBNVZQCXNGDEMH	v0slzCALzPKBbnGikEoikxYQhrpk50m5q5R9O+Js
POD 14	AKIAS74TMJCRVBH33KVY	QkM+4yJZKzEbqNCWB1LDZws3vJiiTIIIsELPTWs
POD 15	AKIARZ5BNC33H57VKG2Z	raKFJz7hLQVgFEkK7IJ0we1GFCACrZvlq376kAp3
POD 16	AKIAXZ5NGABOHI7ANGKE	h4dZJLrf1e4AlXI59vOYj5nSkdIs0WCNsyXnAift

Map the S3 bucket to the file system on bootflash of switch to create a shared folder between S3 and bootflash.


```
S1-ACCESS-LEAF-3(config-s3-profile)#bucket userpod<pod  
number> mount-point awsbucket
```

Example: bucket userpod7 mount-point awsbucket

Configure region and start S3 service.

```
S1-ACCESS-LEAF-3(config-s3-profile)#permissions read-  
write  
S1-ACCESS-LEAF-3(config-s3-profile)#region us-east-2  
S1-ACCESS-LEAF-3(config-s3-profile)#no shutdown  
S1-ACCESS-LEAF-3(config-s3-profile)#end
```

Step 4: Use Case 1

For the first S3 use case, we want to save the running-config on our switch for future use and shareability to other AWS users in our organization. First, we will check the directory of the mount-point to ensure there are no files in it.

```
dir bootflash:.cloudfs/awsbucket
```

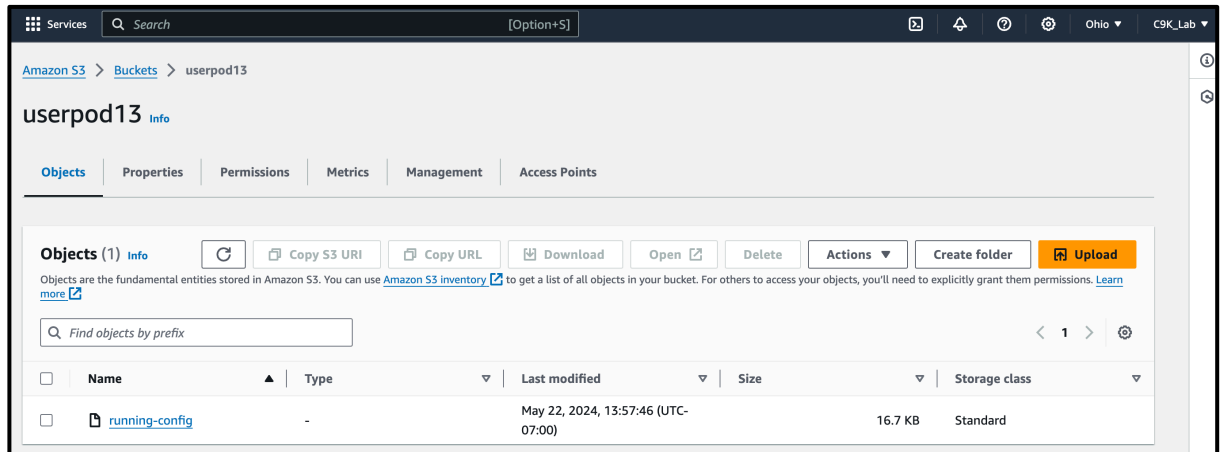
Then, we will copy the running config to the shared folder we created earlier, by copying the following command.

```
copy running-config bootflash:.cloudfs/awsbucket
```

After, we will now validate and ensure the running-config file was stored in the correct location, copy the following command.

```
dir bootflash:.cloudfs/awsbucket
```

Navigate to your pod's AWS S3 bucket to check the contents of the mounted bucket. You'll notice that the running-config file was recently added.

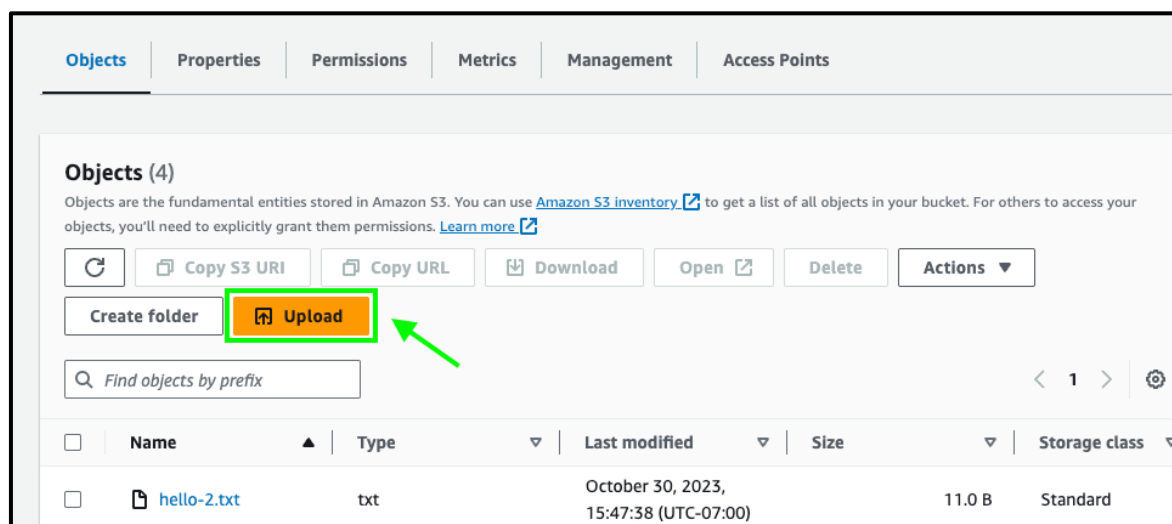


Step 5: Use Case 2

For the second S3 use case, we want to upload a file from our local machine to our S3 bucket. This provides easy image management and image distribution to switches for network admins in organizations. We will upload a file from our local machine to S3. This could be an image, script, file in whatever form. In our case, we will use a hello.txt file.

Please note that files up to 64GB can be added to the s3fs folder

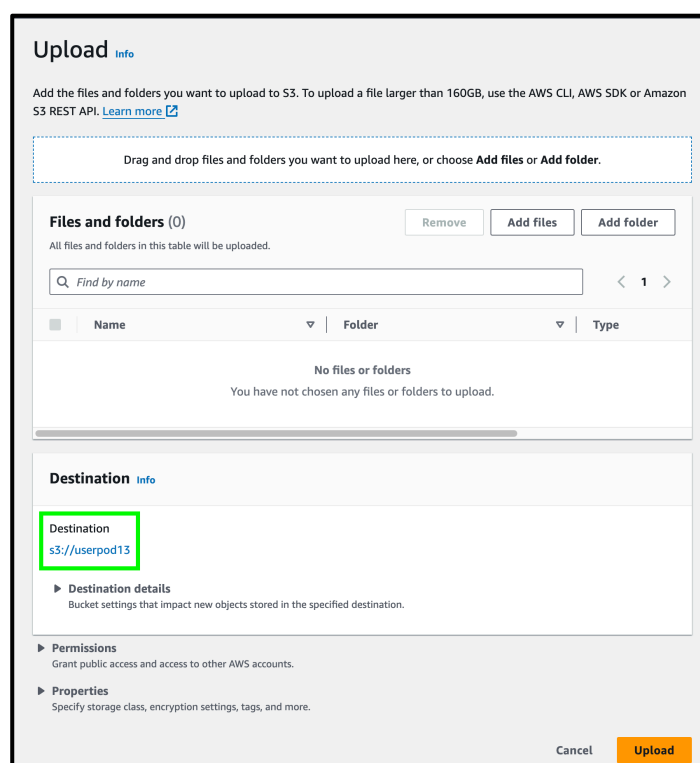
On our S3 bucket page, click the orange **“Upload”** button. Then select **Add files**.



From our local machine, select File icons and select **Downloads**.

Select the hello.txt file. When the upload is successful, you will see the file name under Files and Folders.

Under destination, it will have the s3 bucket name. Click on upload to upload the file.



Log back into the C9300-SMU switch.

We will verify that our uploaded .txt file is now uploaded to the shared folder in switch by copying the command below.

```
dir bootflash:.cloudfs/awsbucket
```

Now, we should see our uploaded file in the file system of the switch.

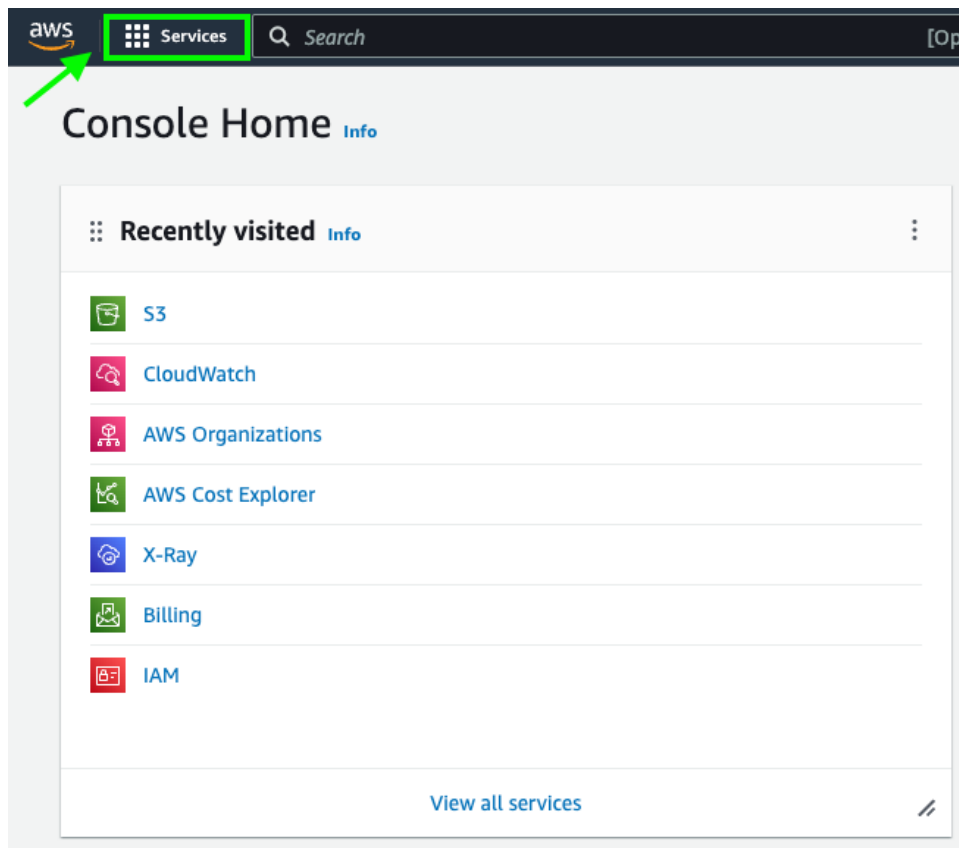
```
SI-ACCESS-LEAF-3#dir bootflash:.cloudfs/awsbucket
Directory of flash:.cloudfs/awsbucket/

4294967295  -rw-          1423  May 22 2024 21:07:26 +00:00  Hello.txt
4294967295  -rw-         17124  May 22 2024 20:57:43 +00:00  running-config

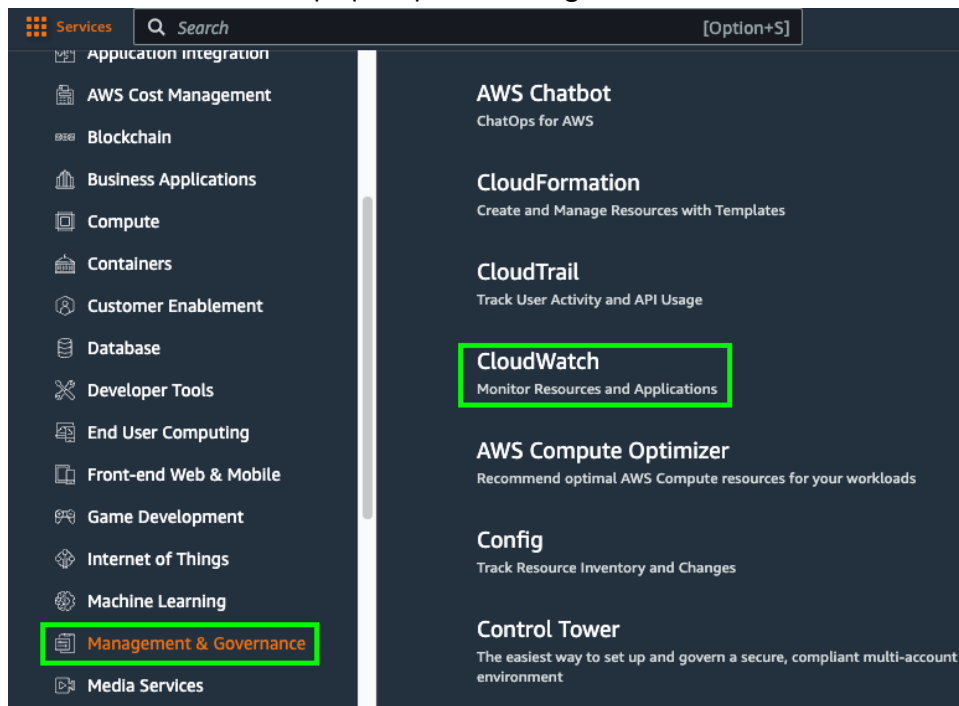
11353194496 bytes total (3164876800 bytes free)
```

Task 2: CloudWatch Configuration

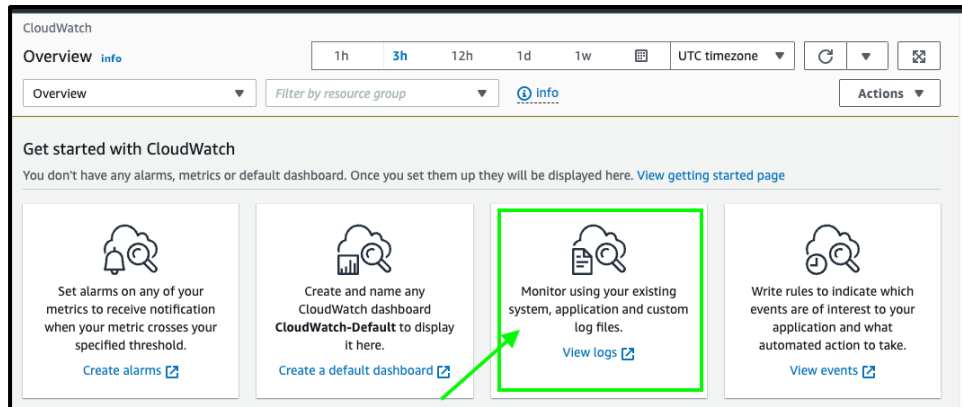
1. In the AWS account dashboard, select the **Services** menu on the left corner of the dashboard.



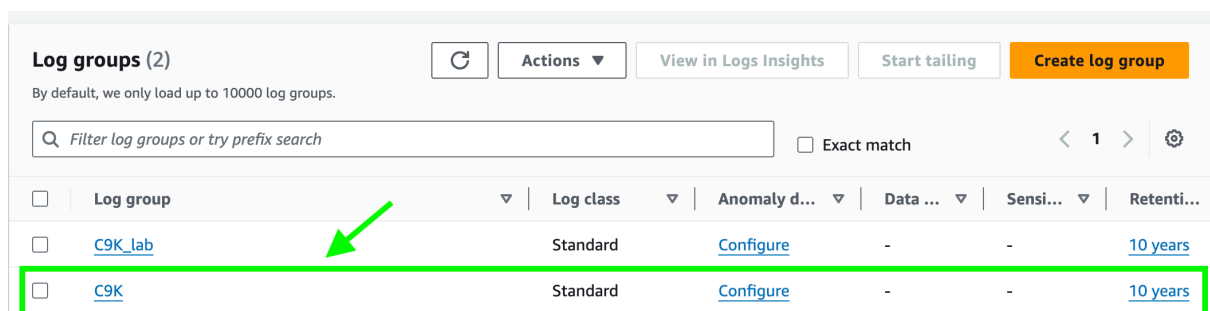
2. Navigate to **Management & Governance** on the services list. Select **Cloudwatch** when it pops up on the right.



On the CloudWatch dashboard, select **View logs** panel to view and create log groups. This allows the user to monitor their organization using existing system, application and custom log files.



We have a single log group created. For the log group C9K, there is a log streams that will be created by your pod switch.



Click on the log group and then view the contents.

There are no logstreams yet but will be populated once configured.

In this lab, we will be viewing and observing log files streams into the lab log group from our switches.

Step 2: Configure CloudWatch on C9300 Switch

Log into the C9300-SMU switch from Putty.

On the CLI, copy and paste the following commands to configure S3 on the switch.

Create the Cloudwatch profile

```
S1-ACCESS-LEAF-3(config)#conf t
S1-ACCESS-LEAF-3(config-cloudwatch-profile)#cloud-
services aws cloudwatch profile usercloudwatch<pod
number>
```

Configure AWS IAM credentials. This allows to sync our catalyst switches to our AWSer accounts.

```
S1-ACCESS-LEAF-3(config-cloudwatch-profile)# access-key
key-id <access key> secret-key 0 <secret key>
```

Use the access key and secret key corresponding to your pod from the table below.

POD NUMBER	ACCESS KEY	SECRET KEY
POD 1	AKIA2OAJTXLNLG65PY65	Juw0amt6e8C3oZKIPlmOsBx9biCUaekRFxpYwYno
POD 2	AKIA5G2VGZNPZQBPJI7M	UOYueC+1GMqmMyQCHNV1nwlI1u2fFs/1epOWyx8m
POD 3	AKIA3FLD2PDOHHREV5FT	AwOUVep+xobH4+duQVjdiWkOxeWvd7i2P3cgyzDT
POD 4	AKIAXEFUNQO42UY4NHP3	UEXH07rvlctH69iyJ7MZ430YMLfx+9rvmoNLmFIW
POD 5	AKIAU5LH54DYCGQZA4P5	Az9w+DgbT5ztNckJ2KTekEILiZiZ+x18YCbjPwBB
POD 6	AKIAXZ5NGMPQAZ7SWJCP	yV5A2pwxI76AVGKqGKL3w8HQGTj+qv4/354AbCxp
POD 7	AKIAT4GVR5U4TYLYH7ZN	TQTTPMIWLkHTlapeVIM7Lqktv2iEhErRzWvEJhaM
POD 8	AKIATNVEVQYZGR4SV4U3	cVQzLDjooAYGsJ6SKOwPxj860H6Tri/I3qWZCM+y
POD 9	AKIA3CMCCCTGD37FIVML	aHjUUJkF90X30bjD9BIRTy2aZ2UApUvunoqzKsBR
POD 10	AKIA2YICAP2V5GBLJB4V	WssqmOhEwRDtrPdELwazNH5+xWpbcXK5PwHp+Bpt
POD 11	AKIA3M7ACUEL7GQGNNMYD	5PO8iZ3cA/G+tJSegMmuojYbNBGKiDN9RVzDmkjl

POD 12	AKIAXYKJSTSNFU4E5TGJ	tu7Zmtw04ThqhuO7ZzGwoFJzeXFsSI72Lb+qwLSh
POD 13	AKIAYXWBNVZQCXNGDEMH	v0slzCALzPKBbnGlkEoikxYQhrpk50m5q5R9O+Js
POD 14	AKIAS74TMJCRVBH33KVY	QkM+4yJZKzEbqNCWB1LDZws3vJiiTIIIsELPTWs
POD 15	AKIARZ5BNC33H57VKG2Z	raKFJz7hLQVgFEkK7IJ0we1GFCAcrZvlq376kAp3
POD 16	AKIAXZ5NGABOHI7ANGKE	h4dZJLrf1e4AIXI59vOYj5nSkdIs0WCNsyXnAift

Configure Log group name and Log stream name and File path

```
S1-ACCESS-LEAF-3(config-cloudwatch-profile)# log group-  
name C9K stream-name pod<pod number>logs file-path  
/bootflash/cloudwatch/*
```

Configure Region and start service to stream logs

```
S1-ACCESS-LEAF-3(config-cloudwatch-profile)#region us-  
east-2  
S1-ACCESS-LEAF-3(config-cloudwatch-profile)#no shutdown  
S1-ACCESS-LEAF-3(config-cloudwatch-profile)#end
```

```
S1-ACCESS-LEAF-3#sh run | s cloudwatch  
cloud-services aws cloudwatch profile usercloudwatchN  
access-key key-id AKIA3FLD2PDOHREVSFT secret-key 0 AwOUVep+xobH4+duQVjdiWkOxeWvd7i2P3cgyzDT  
log group-name C9K stream-name podn_logs file-path /bootflash/cloudwatch/*  
region us-east-2  
no shutdown
```

Step 3: Log Monitoring Use Case

For this use case, we will show how network admins can easily store large amounts of log files and share them with other AWS users in their organization who may not have access to switches. These syslogs can then be shared with others for debugging/troubleshooting without the need to download log files directly from the switch.

Enter the following commands to trigger syslogs on your switch.

```
S1-ACCESS-LEAF-3#Conf t
```



```
S1-ACCESS-LEAF-3(config)#logging persistent url
bootflash:cloudwatch immediate
```

We will now view the shared folder to view the syslog files created and stored there. Copy the command below. You'll notice there are many log files that are continuously created (~every 30 mins) because we have logging enabled

```
dir bootflash:cloudwatch
```

```
S1-ACCESS-LEAF-3(config)#end
S1-ACCESS-LEAF-3#
*Jan 29 04:15:35.695: %SYS-5-CONFIG_I: Configured from console by console
S1-ACCESS-LEAF-3#dir bootflash:cloudwatch
Directory of flash:/cloudwatch/

49155   -rw-                930   Jan 29 2025 04:15:36 +00:00   log_20250129-041506

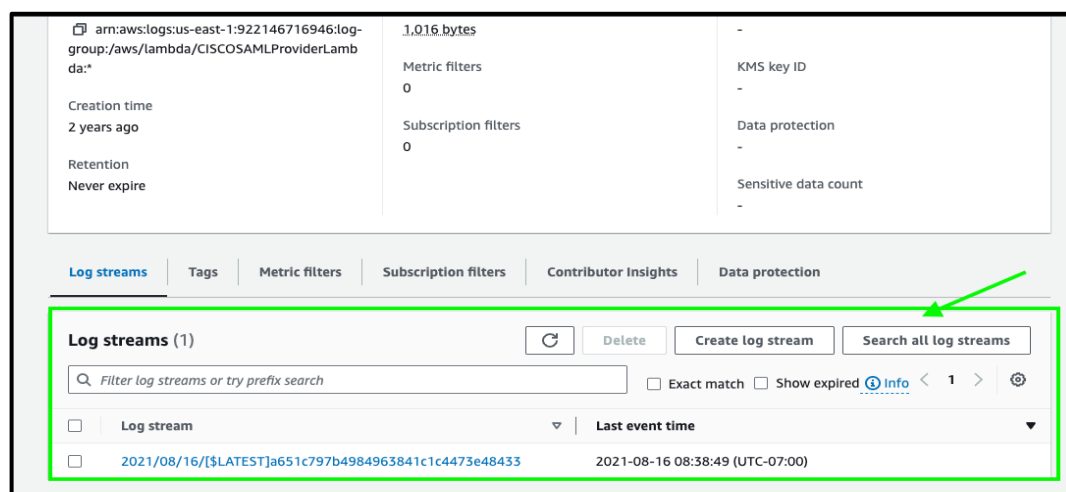
11353194496 bytes total (2386489344 bytes free)
S1-ACCESS-LEAF-3#
```

Now, to view these logs from our switch, we will navigate to the cloudwatch log group.

Note: Please make sure your region is “us-east-2”

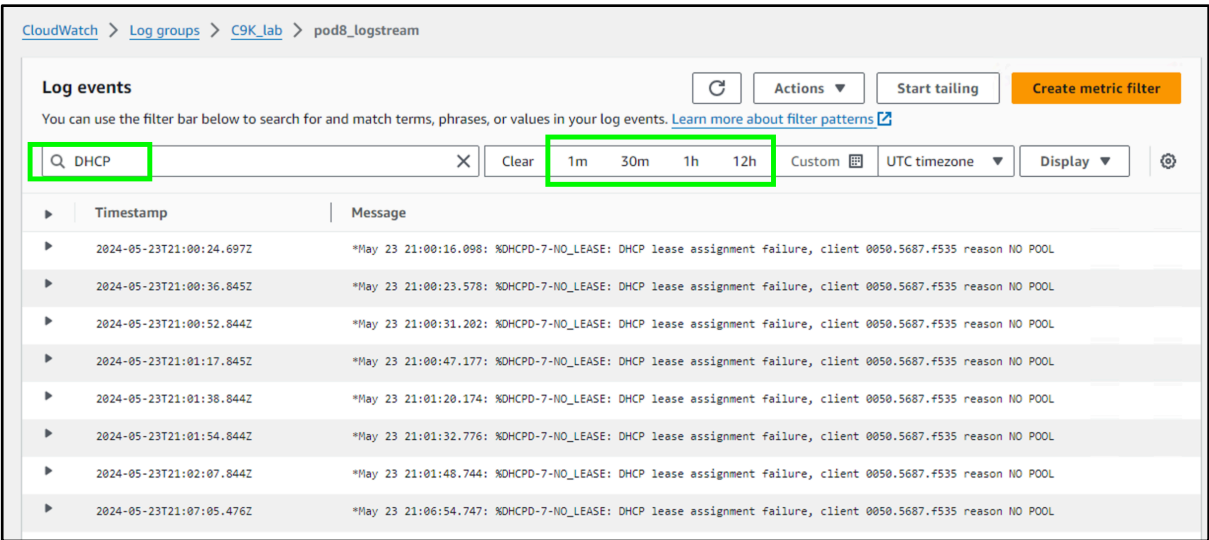
Within the log group, scroll to the log stream for your pod, podn_logs, and view the logs for the pod.

In the log stream, view the logs being sent to the AWS account from your switch.



Once the logs are coming in, you can add filters and customize the view and important alert logs in the Log Insights or other custom dashboards

First, we can search through the logs for keywords and also filter based on the time range, as shown below.



On the left side of the dashboard, select Logs insights to get more insights into the logs

We will select our log group from the drop down: C9K



There is a pre-configured code to run some queries on the log. We will click on **Run Query** to run our insights

Select log groups, and then run a query or [choose a sample query](#).

Select up to 50 log groups. ▼ Browse log groups

C9K_lab X Clear all

```
1 fields @timestamp, @message, @logStream, @log
2 | sort @timestamp desc
3 | limit 1000
```

Run query Cancel Save History

Logs Insights query can run for maximum of 60 minutes.

There are three tabs of insights “patterns, logs and visualizations”. Select the patterns and logs to view insights int provides on the logs.



Logs (321)

Patterns (24)

Visualization

Patterns (24) based on 321 of 321 records

Analyze all records

Info

Add to query

Export results

Add to dashboard

A pattern is a shared text structure that recurs in your logs. Click the magnifying glass icon to analyze a pattern.

Filter patterns by pattern string, event count, severity, event ratio or keywords

☐	Inspect	Pattern	Event count	Event ratio (%)	Severity type
☐		*May <*> <*> DHCP lease assignment failure, client <*> reason NO POOL	116	36%	NONE
☐		*May <*> <*> <*> (<*> : <*>) MKA Session successfully completed a SAK Rekey (new Latest AN/KN <*>, Old AN/KN <*>) for RxSCI <*>, AuditSessionID , CKN <*>	67	21%	NONE
☐		*May <*> <*> <*> Line protocol on Interface <*>, changed state to <*>	58	18%	NONE
☐		*May <*> <*> <*> Interface <*>, changed state to <*>	19	6%	NONE
☐		*May <*> <*> <*> Login Success [user: tmlab] [Source: <*>] [localport: <*>] at <*> UTC <*> <*> <*>	6	2%	NONE
☐		*May <*> <*> <*> Switch <*> <*> [<*>]<*>LowSetLogLevel(<*>): change debug level from [CRT] to [INF]	6	2%	DEBUG
☐		*May <*> <*> <*> <*> Session from <*> (tty = <*>) for user 'tmlab' using crypto cipher <*>, hmac <*> closed	6	2%	NONE
☐		*May <*> <*> <*> <*> User 'tmlab' authentication for <*> Session from <*> (tty = <*>) using crypto cipher <*>, hmac <*> Succeeded	6	2%	NONE
☐		*May <*> <*> <*> <*> Session request from <*> (tty = <*>) using crypto cipher			

Task 3: Removing Profiles from Switch

Delete S3 & cloudwatch profile.

```
switch# config terminal
switch# no cloud-services aws s3 profile s3pod<pod
number>
switch# no cloud-services cloudwatch profile
usercloudwatchpod<pod number>
```

Delete syslogs file from switch

```
Conf t
No logging persistent url bootflash:cloudwatch immediate
```

Lab 3: Cloud Monitoring on Catalyst 9K Switches with Meraki Dashboard

- 38 -

Scenario

Cloud monitoring for Cisco Catalyst switches provides an extensive visibility with the seamless integration of the Meraki dashboard. This provides the ability to view Catalyst switches statistics, configuration, traffic analytics and utilize some troubleshooting capabilities all on the powerful Meraki dashboard. The dashboard also provides an overview of the operational health of the network. As a monitoring tool, most operations are read-only. All live troubleshooting capabilities will also not result in persistent changes to configuration.

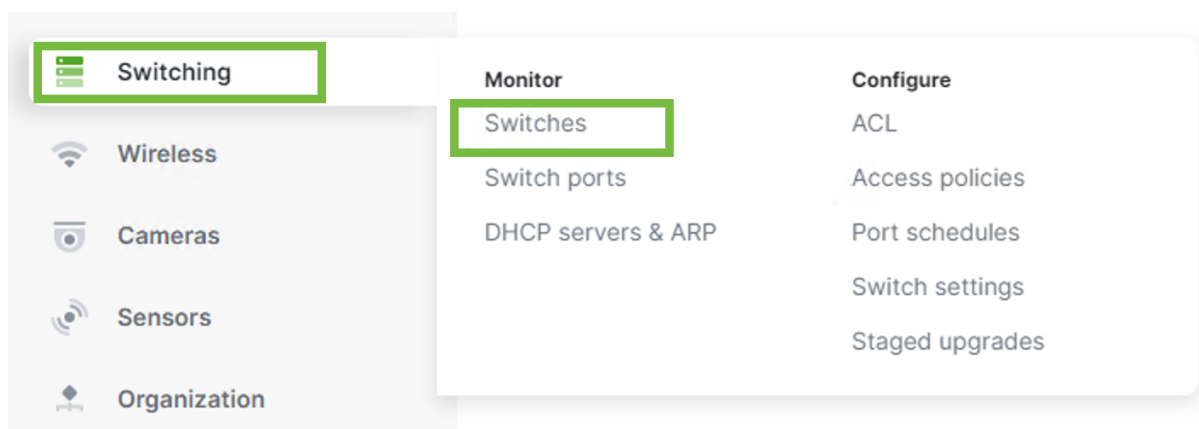
Prerequisite Steps:

All pre-onboarding checks for this lab have been already completed. Please move onto the next section to continue with the lab after reading through the prerequisites for successful implementation.

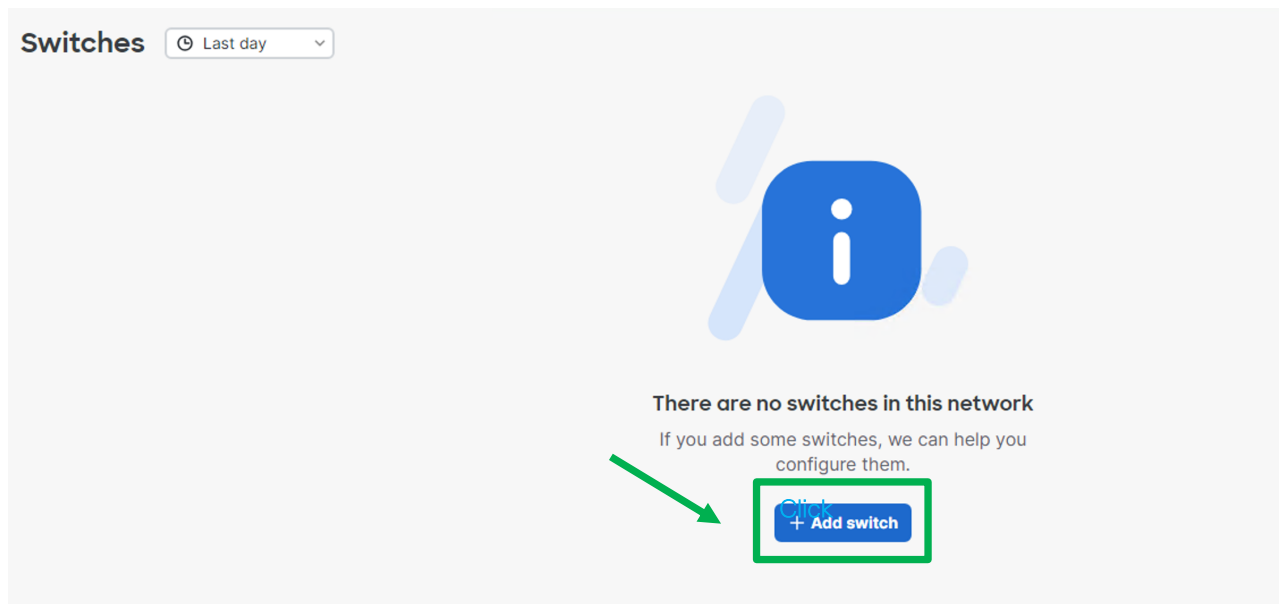
- Confirm that the switch(es) designated for onboarding are one of the supported switch models listed.
 - Catalyst 9200 series switches (including 9200L and 9200CX models)
 - Catalyst 9300 series switches (including 9300L and 9300X models)
 - Catalyst 9500 series switches
- Ensure that the switches are also running the supported software version of Cisco IOS-XE 17.3.1+
- The computer from which the onboarding application is run must be able to reach on **TCP port 443**.
- Ensure any firewall rules in place allow communication with the gateway corresponding with the dashboard region on TCP port 443.
- Telnet is required for connectivity pre-check because the onboarding application will test connectivity to the regional gateway on TCP 443 using a Telnet connection from the switch CLI.
- Ensure rules are in place to allow direct HTTPS connections since HTTPS proxies to access the API endpoint and the TLS gateway are not currently supported.
- Connectivity must be via a front-panel port (not the management interface).
- SSH access to the switch CLI must be enabled and accessible via the computer.

Step 1: Onboarding Catalyst Switch

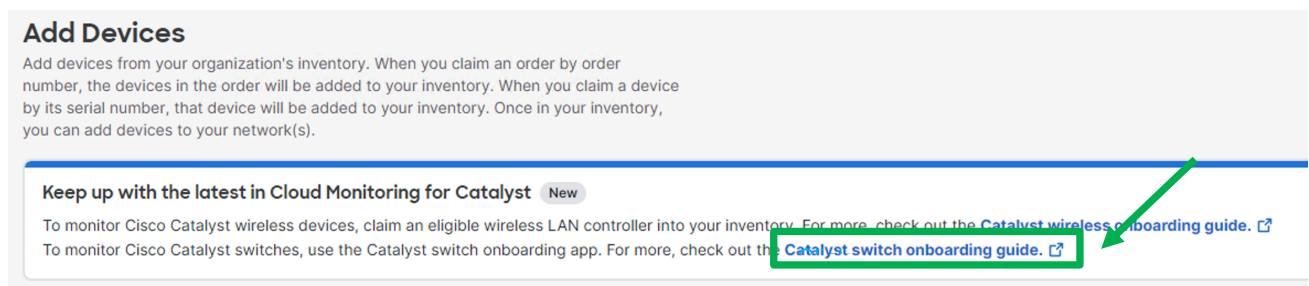
- To enable cloud monitoring for Catalyst, it must first be onboarded to the Meraki dashboard. This process connects the Catalyst device to the Meraki cloud using a TLS tunnel, which is used to communicate status and telemetry to the Meraki dashboard.
- Login to the Meraki dashboard with the following credentials
<https://dashboard.meraki.com>
 Username: cat9k.podX@gmail.com; where x is your pod number
 Password: C1sc0dna!
NOTE: If you use any of the following pods, use the below email and password instead: POD 12, POD 13, POD 14
 Username: cat9k.podXv2@gmail.com; where x is your pod number
 Password: C1sc0dna!
ALSO NOTE: If you are requested to provide a verification code, please log into the email account with the above username/password credentials and retrieve the code for the Meraki dashboard.
It's important to use the RDP session and not your local browser to access the Gmail Account
- A switching network “CiscoLive” has already been created. On the dashboard, select **Switching > Switches**.



- We currently have no switches in our network. To add our Catalyst switches, click on the “**Add Switch**” button.



- To add our Catalyst switches to the dashboard, click on the “**Catalyst switch onboarding guide.**” Hyperlink which will lead you to a new tab.



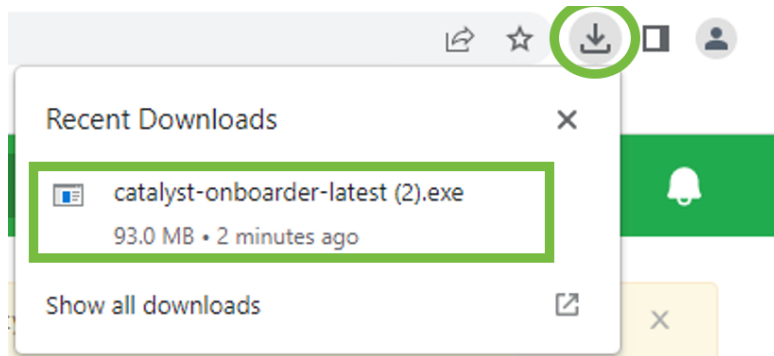
- Scroll throw the “**Cloud Monitoring for Catalyst Onboarding**” guide until you reach the “**Downloading the Onboarding Application**” section > Click on Download for Windows.

Downloading the Onboarding Application

The onboarding application can be downloaded from the following links:

- [Click Download for Windows](#)
- [Download for macOS](#)
- [Download for Linux](#)

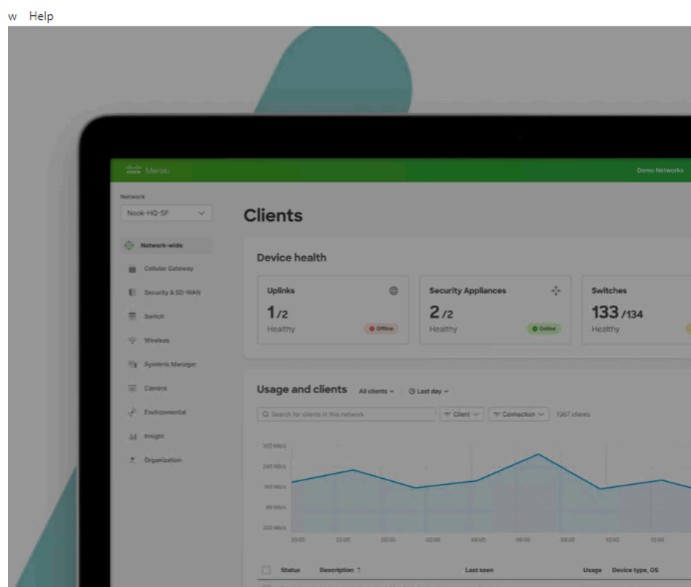
- On your browser page, at the top right, you will see a down arrow sign. Click on the sign to see the Meraki app onboarded file.



- Click on the file to install the Meraki app on

the computer.

- Open the onboarder application in your downloads, to install the application.
- Once the app is installed and opened, you will be presented with a screen. **Select Agree and Continue**
- You will also be required to provide an API key after. This key was already retrieved from the dashboard previously. This is generated by the network admins to sync the dashboard with apps.



CISCO Meraki

Cloud Monitoring for Catalyst

Make sure you have checked out our [onboarding checklist](#).

Meraki Dashboard API key ⓘ

Start

- Enter the key below for each assigned pod and click **Start**:

POD NUMBER	MERAKI DASHBOARD API KEY
1	ee2b48d778842dd48a02bec242a5745de0947f12
2	47c504e47c44663eb017e5e514ced0315d0a9660
3	bd96d1612a07b1b0574f33755c53795aba3b8811
4	47075f506e21420a354c249a0c4195f60cb47b55
5	b6e685479e73aed58512291ff2074a1bace8938d
6	8258be56a291453e6a799d6403a080c518346a0e
7	e12d6365e6a0aae6256a7a46848a6ffa42d1e469
8	e5b06ca657e68101707bb0e11265a37ddf82854f
9	9f43349f5c7821d302527a7cda65a5b0fd18605f
10	2568c6e1bdc3e67eda88782d01f4e068c5b3e5a5
11	4689888f63ca4c0d1e317f15da920f5fe6712d38
12	4ef230aab25b9c117a99c09625e1b8dfb9d50446
13	66de2aadf13f0c481bc17744941874dd085ac1db
14	f5001401b57ab9edde9ef1b2d3170ea08ee1857d
15	2559d2ef9944da87aad33f2627215b4e55c61d10
16	eebc903384e8d037e37d4aa203ea0e81a98e52e6

- To add your Catalyst switch to the Meraki dashboard, there are a couple of steps to go through for the onboarding process.
- First, select the Organization you would like to onboard the switch. In our case, select **Cisco**. Click **Next**.

Select organization

Select the organization you want to onboard to. If your organization does not appear in the list, please make sure 'Dashboard API access' is enabled.

Organization name	Region	Dashboard link
☒ Cisco	North America	Link

- Next, enter the SSH IPv4: port address for the devices you want to onboard into the Meraki Dashboard (up to 10 at a time). When running the local onboarding application, configurations are pushed to the device to allow the device establish communication with the cloud. To perform

these actions the onboarding application will connect to the device(es) over SSH.

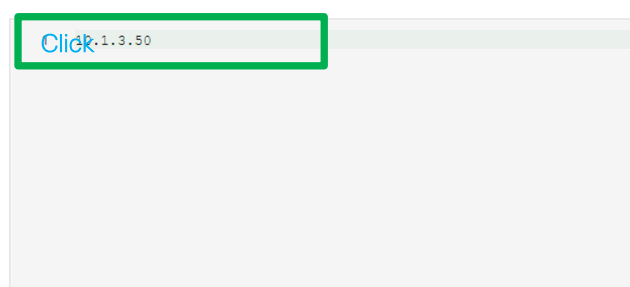
Note: We have already configured SSH on our switches.

- Enter the Catalyst 9K Switch IP: 10.1.3.50
- Next, enter the following device credentials:
Username: tmelab
Password: Uab00tcamp!
Enable password: cisco

Enter Device Information

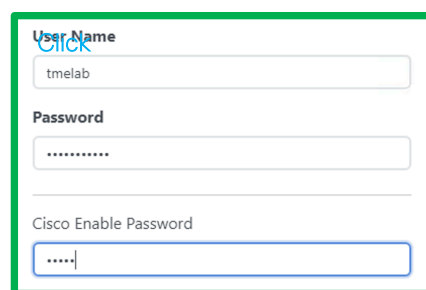
1. Enter switch device IPs.

Enter the IPv4 address and port that can be used to SSH into the device(s) you want to onboard into the Meraki Dashboard. For example: 192.168.1.1:2222. If no port is specified, we will default to port 22.



2. Enter switch device credentials.

Please provide the level 15 configuration access credentials needed to onboard your devices. You may also need to provide your Cisco enable password in some cases



- Now we will set up the SSH connection between the switch and Meraki cloud. Select **Start SSH authentication** to start. After successful connection, select **Next**

Establish SSH connection



IP address	SSH status
> 10.1.3.50	0% Not started

- Now in the next step, we will run through pre-check configurations on our switch to review configurations and make sure it is ready for onboarding. Select **Start Pre-check**. Select **Next**.

Pre-check configurations

1 Device ready to start pre-check [Start pre-check](#)

Requirements

- IOS-XE version 17.3.1+
- IOS-XE image with payload encryption
- IP domain lookup enabled
- TCP 443 connection
- AAA configuration supported
- IP routing enabled
- Loopback interface available
- VTY slots available
- ACL configuration supported

IP address	Model	Serial number	Pre-check status
> 10.1.3.50			0% Not started

- After successful onboarding, you should see the **Ready for onboarding** sign show up.

Pre-check configurations

1 Device completed pre-check

Requirements

IP address	Model	Serial number	Pre-check status
10.1.3.50	C9300-24U	FCW2123L00R	Ready for onboarding

5/25/2024, 8:55:53 PM Authenticating...

5/25/2024, 8:55:53 PM Connecting to switch via SSH and authenticating using credentials.

5/25/2024, 8:55:53 PM Confirming privilege-15 access

5/25/2024, 8:55:53 PM Device authenticated

5/25/2024, 8:57:35 PM Checking device eligibility...

5/25/2024, 8:57:39 PM Checking IOS-XE version 17.3.1+

5/25/2024, 8:57:39 PM Checking IOS-XE image with payload encryption

5/25/2024, 8:57:39 PM Checking TCP 443 connection

5/25/2024, 8:57:41 PM Checking AAA configuration supported

5/25/2024, 8:57:41 PM Checking IP domain lookup enabled

5/25/2024, 8:57:41 PM Checking IP routing enabled

5/25/2024, 8:57:42 PM Device is eligible

5/25/2024, 8:57:42 PM Checking device configuration...

5/25/2024, 8:57:42 PM Checking loopback interface availability

5/25/2024, 8:57:43 PM Checking ACL configuration supported

5/25/2024, 8:57:43 PM Checking VTY slots availability

- We will now assign our Catalyst switch into the Network of choice within the Meraki Dashboard. We have already created a network by name “Cisco Live” as previously shown. Type in **Cisco Live** and click **Next**.

Assign to networks

Select the dashboard network that monitoring-only Catalyst device should be assigned to. Note, these networks will be re-configured using the [unique client identifier](#) method for client tracking.

IP address	Model	Serial number	Assigned network
10.1.3.50	C9300-24U	FCW2123L00R	Click Cisco Live

- Now, select the checkbox with all the switch details.
- Click on **show details**. This allows to review and confirm the configurations that will be removed from the switch, and the configuration

changes that will be applied to the switch by the Meraki cloud to allow for the monitoring of the switch/network. These configurations include enabling NETCONF, LLDP, SSH, configurations for secure cloud access of traffic during transmission, SNMP logging, NetFlow on all interfaces and many more.

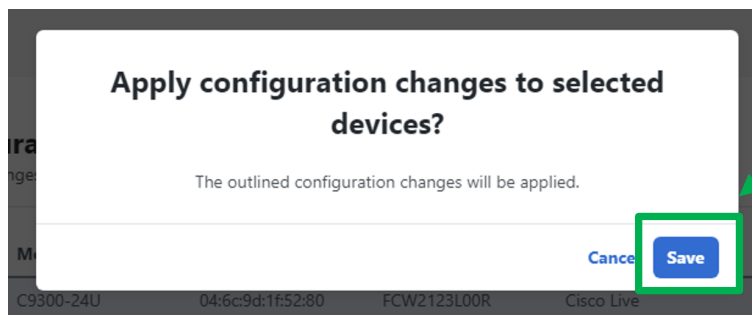
Confirm configuration changes

Review the configuration changes below and select the devices to apply changes

☒	IP address	Model	MAC address	Serial number	Assigned Network	Actions
☒	10.1.3.50	C9300-24U	04:6c9d:1f52:80	FCW2123L00R	Cisco Live	Show details

< 1 >

- Select **Close** after reviewing.
- Select **Next**. On the pop-up that comes up, select **Save** to save configurations.



- Select **Next** to finish the onboarding process. In this step, the committed configurations will be added onto the switch. You can click on the arrow down to view the stages of the applied configurations.

Confirm configuration changes

Your configuration changes are being applied. Details are shown below.

	IP address	Model	Progress	Status
⌵	10.1.3.50	C9300-24U		Waiting for device to be available...
5/25/2024, 8:55:53 PM Authenticating... 5/25/2024, 8:55:53 PM Connecting to switch via SSH and authenticating using credentials. 5/25/2024, 8:55:53 PM Confirming privilege-15 access 5/25/2024, 8:55:53 PM Device authenticated 5/25/2024, 8:57:35 PM Checking device eligibility... 5/25/2024, 8:57:39 PM Checking IOS-XE version 17.3.1+ 5/25/2024, 8:57:39 PM Checking IOS-XE image with payload encryption 5/25/2024, 8:57:39 PM Checking TCP 443 connection 5/25/2024, 8:57:41 PM Checking AAA configuration supported 5/25/2024, 8:57:41 PM Checking IP domain lookup enabled 5/25/2024, 8:57:41 PM Checking IP routing enabled 5/25/2024, 8:57:42 PM Device is eligible 5/25/2024, 8:57:42 PM Checking device configuration... 5/25/2024, 8:57:42 PM Checking loopback interface availability 5/25/2024, 8:57:43 PM Checking ACL configuration supported 5/25/2024, 8:57:43 PM Checking VTY slots availability 5/25/2024, 9:05:47 PM Backing up current config... 5/25/2024, 9:05:48 PM Starting config mode... 5/25/2024, 9:05:48 PM Shutdown the previous tunnel before cleaning up. 5/25/2024, 9:05:48 PM Ensure old tunnel config is removed. 5/25/2024, 9:05:48 PM Ensure old CA certificates are removed. 5/25/2024, 9:05:48 PM Ensure that the ssh config is removed.				

Confirm configuration changes

Your configuration changes are being applied. Details are shown below.

	IP address	Model	Progress	Status
⌵	10.1.3.50	C9300-24U		✔ Device is connected successfully. • View

- Select **Next** to completely and finish onboarding the device. After device is successfully onboarded, we can now view the switch within the Meraki dashboard.

Onboard

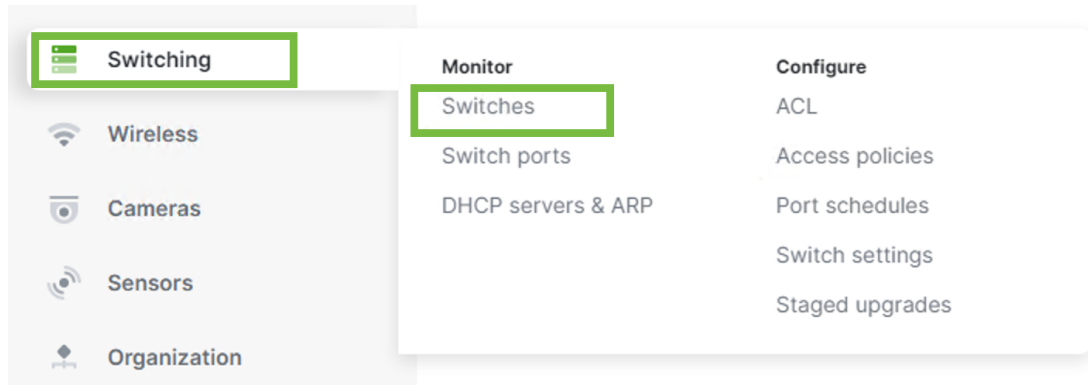
IP address	Model	MAC address	Serial number	Assigned Network	Status
10.1.3.50	C9300-24U	04:6c:9d:1f:52:80	FCW2123L00R	Cisco Live	✔ Device is connected successfully. • View

Step 2: Switch Monitoring

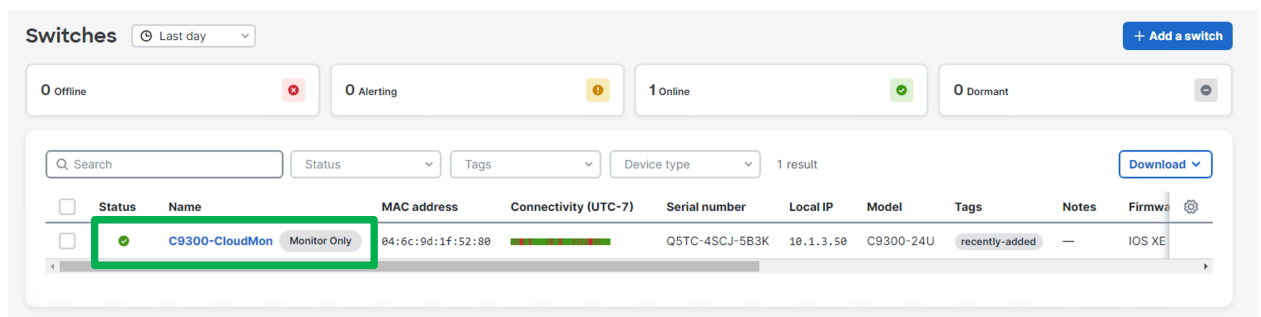
- Log back into the Meraki dashboard on your browser.



- From the menu, select **Switching > Switches**.

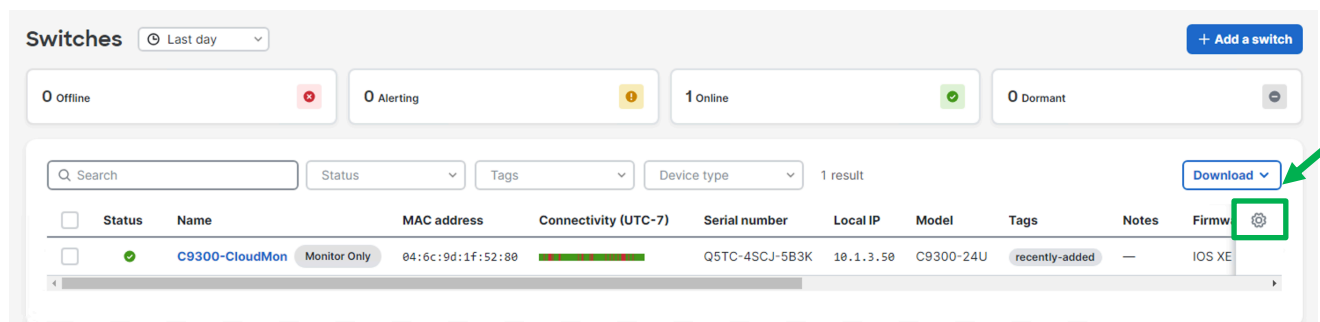


- You will see that the Catalyst 9300 switch has been added. The Meraki Dashboard will be monitoring this switch with multiple connected clients.



Note: Please wait for ~5 minutes for the switch to completely sync to the Meraki dashboard

- These cloud monitoring switches will be automatically tagged with “**Monitor Only**” in the dashboard to distinguish from fully managed Meraki switches. We can see the MAC address details, connectivity status at different times, the switch serial numbers and the local IPs of all the switches onboarded.
- You can customize the parameters that describe the switch. Select the gear icon on the right.



- You are then provided with a list of tags to select that will be displayed with the switches onboarded. Select the tags that you wish to display on the page. After selecting the tags, select **Apply**.

Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend [enabling it](#) at your earliest convenience.

Account recovery action needed
You are the only administrator for this organization. If you lose access, you will need to contact support to recover access to this organization.
[Add another administrator to ensure you can recover access.](#)

Switches

Last day

0 Offline 0 Alerting 1 Online

Q Search Status Tags Device type 1 result

Status	Name	MAC address	Connectivity (UTC-7)	Serial number	Local IP	Model
☐	C9300-CloudMon	04:6c:9d:1f:52:80		Q5TC-4SCJ-5B3K	10.1.3.50	C9300-24U

Last login: 19 days ago from your current IP address

Select columns

Check to add, drag columns to reorder.

Device

☒ Name

☐ VLAN Profile

☒ MAC address

☒ Serial number

☒ Model

☒ Tags

☒ Notes

☒ Firmware version

☒ Stack

☒ # ports

☒ # active ports

☐ Profile

Status

☐ Alerts

☒ Status

☐ Contacted at

☒ Connectivity (UTC-7)

☐ Configuration status

☐ Upgrade status

Cancel Apply

- You can now view the onboarded switches and their assigned tags that you selected.

Switches Last day

0 Offline 0 Alerting 1 Online 0 Dormant

Q Search Status Tags Device type 1 result Download

Status	Name	MAC address	Connectivity (UTC-8)	Serial number	Local IP	Tags	Model	Firmware version	# ports	# active ports
☐	C9300-CloudMon	bc:5a:56:a6:12:80		Q5TC-BVLJ-PEXN	10.1.3.50	recently-added	C9300-24U	IOS XE 17.3.4	28	6 / 28

- Select the switch by clicking on the switch name **C9300-CloudMon** which will lead you to the switch dashboard for more details.

Switches Last day

0 Offline 0 Alerting 1 Online 0 Dormant

Q Search Filters 1 result Download

Status	Name	MAC address	Connectivity (UTC-8)	Serial number	Local IP	Model	Firmware version
☐	C9300-CloudMon	bc:5a:56:a6:12:80		Q5TC-BVLJ-PEXN	10.1.3.50	C9300-24U	IOS XE 17.3.4

- There are two sections we can take note of here.
- The first section details the IP addresses, DNS, gateway information, serial number and running Cisco IOS-XE version of the switch. This is shown on the left side of the dashboard under the switch name and address.

Network
Cisco Live ▾

Network-wide

Switching

Organization

C9300-CloudMon
C9300-24U 04:6c:9d:1f:52:80
Monitor Only

ADDRESS
560 McCarthy Blvd

LAN IP
10.1.3.50 (statically assigned)

PUBLIC IP
128.107.211.28

GATEWAY
10.1.3.252

DNS
128.107.212.175
171.70.168.183

LAN IPV6
Not configured

TERMINAL
Launch Terminal

SERIAL NUMBER
FCW2123L00R (Catalyst)
Q5TC-4SCJ-5B3K (Meraki)

TAGS
recently-added

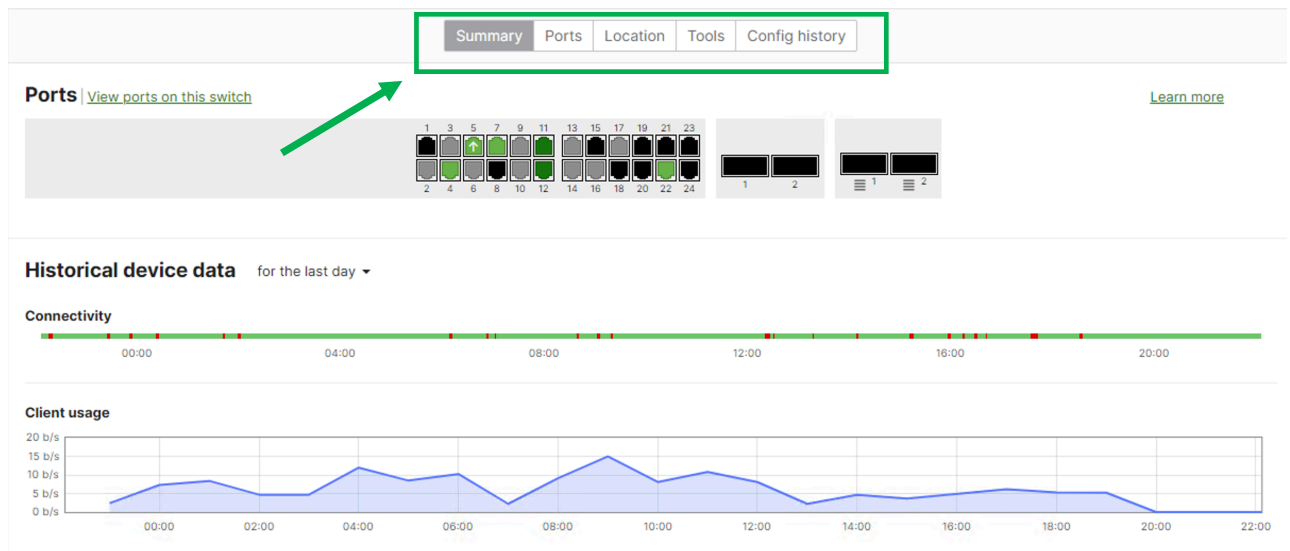
NOTES

FIRMWARE
Current version: IOS XE 17.3.4

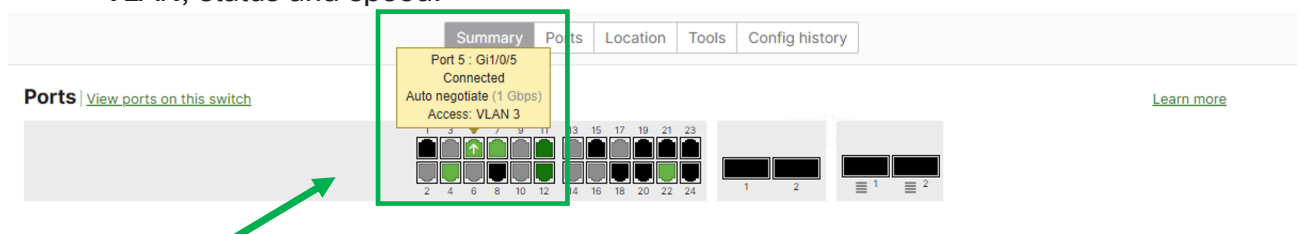
VLAN PROFILE
Default Profile

TOPOLOGY
[Show](#)

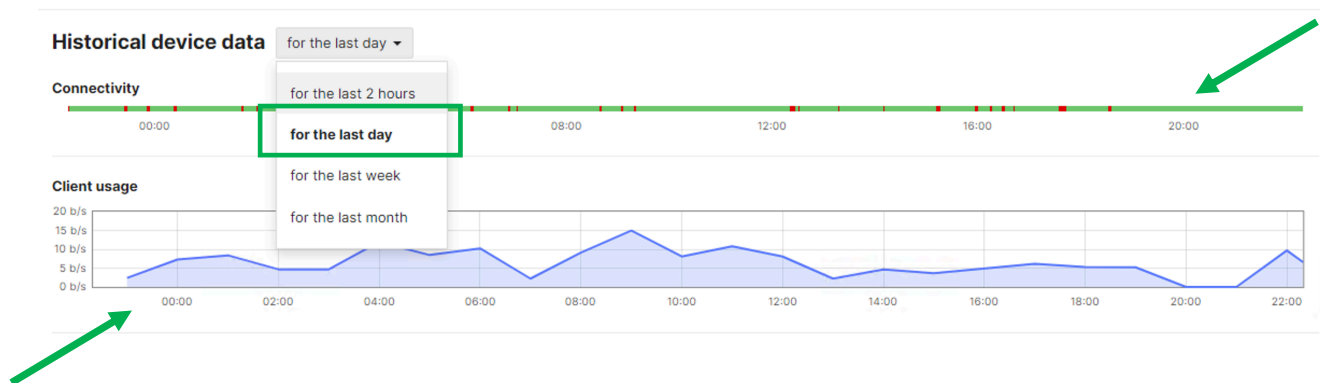
- In the second section, on the upper right side, there are five tabs to use to navigate monitoring the switch. There is the **summary**, **ports**, **location**, **tools** and **Config history** tabs.



- Under **Summary**, we can see the port view with each port showing the VLAN, status and speed.



- There is also a visual graph of both the device connectivity and the client usage shown on the dashboard to give users an idea of the connectivity and usage trend within the switch. This device data can be viewed based on a specified period. E.g. The last 12 hours, by selecting the drop-down arrow.



Note: The connected clients are not transmitting enough data so they may not show up in the client usage graph. However, in the next step of the lab, we show more details on the ports and how much traffic they are transmitting (sent and received) for monitoring.

- Next, click on the **Ports** tab.
- We now see a more detailed monitoring report of each of the ports including the port type, VLAN, port traffic, POE usage, total bytes transmitted on port, stack ports and uplink ports.
- Clicking on a specific interface or port, give an even more detailed monitoring analytics such as a breakdown of the traffic being transmitted, the PoE usage and power being drawn.

Summary **Ports** Location Tools Config history

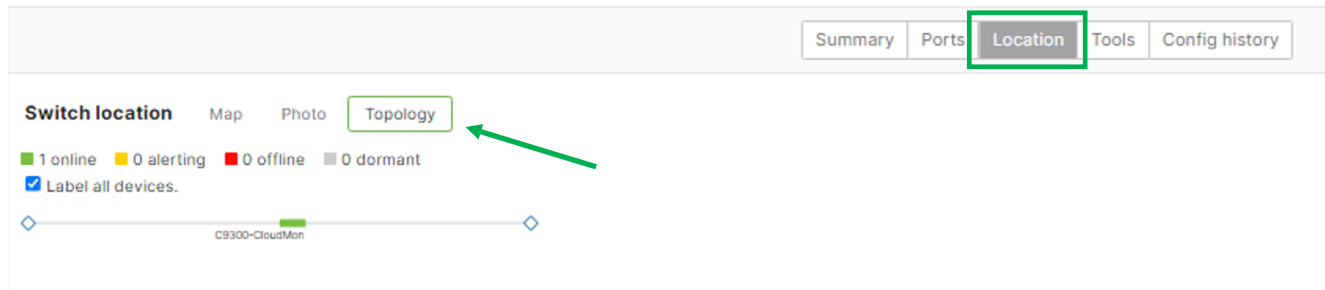
Ports [View ports on this switch](#) [Learn more](#)

Port#	Module	Name	Aggregation Group	Type	VLAN	Current traffic Sent ↓, Received ↑	Total bytes	RSTP	PoE usage	CDP/LLDP	Link	Status
1		Gi1/0/1	2	trunk	native 1	-	-	Enabled	-		Auto negotiate	
2		Gi1/0/2		access	1	-	-	Enabled	-		Auto negotiate	
3		Gi1/0/3		access	1	-	-	Enabled	-		Auto negotiate	
4		Gi1/0/4	1	access	1	495 bps (351 bps ↓, 144 bps ↑)	4.3 MB	Enabled	-	C9300-DATA.cisco.com	Auto negotiate (1 Gbps)	
5		Gi1/0/5		access	3	152.1 Kbps (121.5 Kbps ↓, 30.6 Kbps ↑)	160.3 MB	Enabled	-	SW-POD2	Auto negotiate (1 Gbps)	
6		Gi1/0/6 - underlay-connection-to-C9400-2-Gi1-0-24		trunk	native 192	-	-	Enabled	-		Auto negotiate	
7		Gi1/0/7		access	1	668 bps (547 bps ↓, 120 bps ↑)	6.3 MB	Enabled	-	C9300-DATA.cisco.com	Auto negotiate (1 Gbps)	
8		Gi1/0/8		access	1	-	-	Enabled	-		Auto negotiate	
9		Gi1/0/9		access	1	-	-	Enabled	-		Auto negotiate	
10		Gi1/0/10		access	1	-	-	Enabled	-		Auto negotiate	

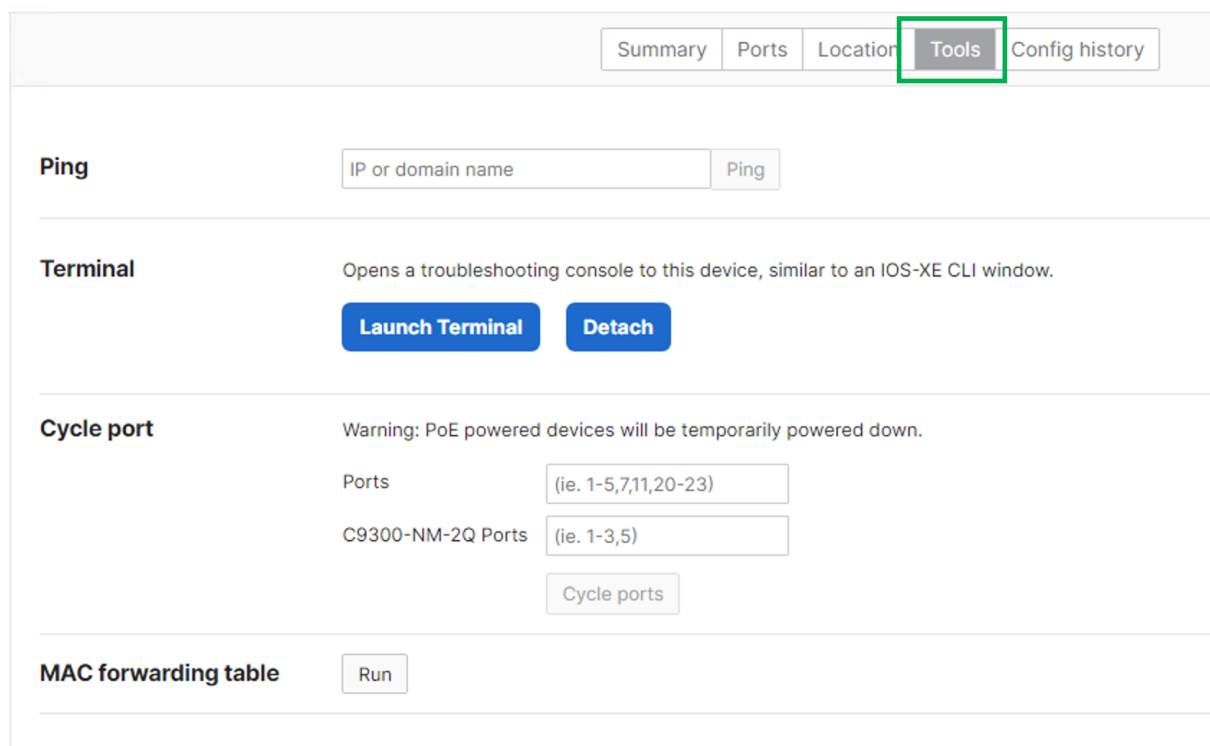
Note that the configuration shown is a subset of settings on the port. There may be additional configuration settings on the Catalyst switch itself that are not shown here.

- Select the **Location** tab.

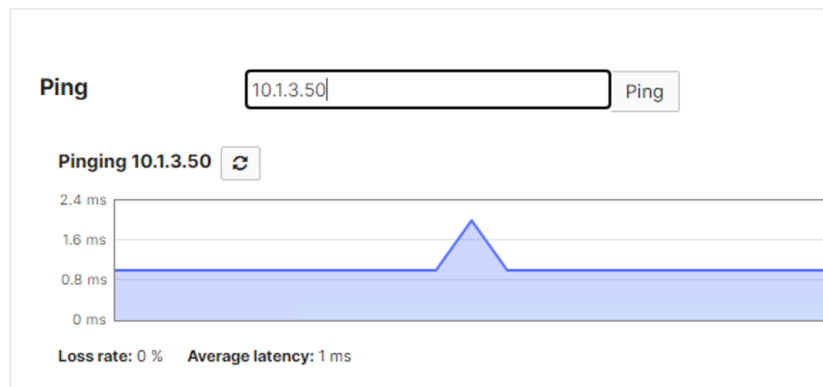
We can view the switch in three different ways, with map of where the switch is located, a photo of the switch or the switch topology. Catalyst switches are integrated into the Meraki dashboard topology for the network. Layer 2 topology is currently supported.



- Select the **Tools** tab. Here, live troubleshooting tools are available.



- **Ping** Initiates a ping from the switch and displays the results visually to see latency over time. Try pinging to an IP address and the dashboard will display a visualized loss rate and average latency.



- **Terminal** is a console providing read-only access to "show" commands through a console emulator to assist with troubleshooting operations. Note: Write commands and configuration are not permitted.
 - Navigate to Terminal and click on **Launch terminal** to open the troubleshooting console/CLI.

Terminal

Opens a troubleshooting console to this device, similar to an IOS-XE CLI window.

Launch Terminal

Detach

Note: The "Detach" button will open the console in a new tab.

Terminal

Opens a troubleshooting console to this device, similar to an IOS-XE CLI window.

Close Terminal

Detach

i This terminal allows limited access to read-only IOS-XE commands, such as **show**.

Welcome to Meraki Troubleshooting Console..

Note: You can enter "show ?" anytime to get the list of currently supported commands and shortcuts

C9300-CloudMon#

- Navigate to the CLI and enter **show version** to check the SW version running on the switch and click enter.

C9300-CloudMon#show version

Cisco IOS XE Software, Version 17.03.04

Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.4, RELEASE SOFTWARE (fc3)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2021 by Cisco Systems, Inc.

Compiled Sat 03-Jul-21 01:55 by mcpre

- **Cycle port** is a potentially disruptive operation and is equivalent to the “shutdown” and “no shutdown” commands applied in sequence on a Catalyst switch port. This can be useful diagnostically, but please be aware that this may cause traffic disruption on the port, including but not limited to spanning tree reconvergence, depending on the design and topology of the network.
- **MAC forwarding table** displays the MAC addresses of clients learned via Layer 2 interfaces, including the associated VLAN and physical port number. Select Run to see the displayed tables.

MAC forwarding table Run

MAC forwarding table 🔄

Filter by:

11 MAC addresses

MAC	Port	VLAN
00:17:e0:c9:72:20	5	3
00:1b:0c:dd:5f:d6	5	3
00:50:56:87:55:ce	5	3
00:a3:d1:45:01:00	5	3
28:ff:3c:9e:5f:c9	12	3
52:54:dd:a5:f0:f6	5	3
00:50:56:87:e2:93	7	21
52:54:dd:71:fc:01	7	21
a0:f8:49:16:19:17	7	21
04:6c:9d:1f:54:81	AGGR/2	41

10 results per page

Note: With cloud monitoring, you can still make configuration changes outside of dashboard. If needed, you can re-onboard devices at any time using the Onboarding application.

Early Access – Config History Feature

- Navigate back to the above listed tabs > Click on **Config history**. This feature allows you to view the current and previous versions of the IOS-XE running configuration of each monitored switch.

Summary Ports Location Tools **Config history**

Configuration Compare changes

Catalyst switches are currently in Monitor Only mode. That means you can see all traffic coming through this switch via Meraki dashboard, but you are not able to change any of the configuration options. However, if you are curious to see the actual configuration of this switch, we have provided it for you here. [Learn more about monitor only mode.](#)

Modified on 5/26/2024, 11:14:20 AM

[Copy this configuration](#) [Download this configuration](#)

```

1 !
2 ! Last configuration change at 18:14:20 UTC Sun May 26 2024
3 !
4 version 17.3
5 service timestamps debug datetime msec

```

- The running configuration of **C9300-CloudMon** is shown below. The configuration is automatically updated in Dashboard when changes are detected. A previous version can be selected using the dropdown list.

Note: Times are displayed in the time zone of the computer/user accessing Dashboard.

Summary

Ports

Location

Tools

Config history

Configuration

Catalyst switches are currently in Monitor Only mode. That means you can see all traffic coming through this switch via Meraki dashboard, but you are not able to change any of the configuration options. However, if you are curious to see the actual configuration of this switch, we have provided it for you here. [Learn more about monitor only mode.](#)

Modified on 5/26/2024, 11:14:20 AM ^

Copy this configuration

5/26/2024, 11:14:20 AM

5/26/2024, 7:49:39 AM

5/26/2024, 5:57:12 AM

5/26/2024, 5:20:39 AM

5/26/2024, 2:00:21 AM

5/25/2024, 9:06:57 PM

1 !

2 ! La

3 !

4 ver

5 ser

6 ser

7 ser

8 ser

9 ser

10 no platform punt-keepalive disable-kernel-core

11 !

12 hostname C9300-CloudMon

13 !

14 !

15 vrf definition Mgmt-vrf

16 !

- To compare two different versions of the configuration, toggle the **Compare changes** switch.

Configuration

Compare changes

Catalyst switches are currently in Monitor Only mode. That means you can see all traffic coming through this switch via Meraki dashboard, but you are not able to change any of the configuration options. However, if you are curious to see the actual configuration of this switch, we have provided it for you here. [Learn more about monitor only mode.](#)

Modified on 5/26/2024, 11:14:20 AM

Modified on 5/26/2024, 7:49:39 AM

Copy this configuration Download this configuration

Copy this configuration Download this configuration

- Select the time stamp that you want to compare with to view any config diffs.

Summary Ports Location Tools **Config history**

Configuration

Compare changes ☒

Catalyst switches are currently in Monitor Only mode. That means you can see all traffic coming through this switch via Meraki dashboard, but you are not able to change any of the configuration options. However, if you are curious to see the actual configuration of this switch, we have provided it for you here. [Learn more about monitor only mode.](#)

Modified on 5/26/2024, 11:14:20 AM

[Copy this configuration](#) [Download this configuration](#)

```

487 overlay interface Loopback1000
488 local-interface Vlan3 priority 1
489 pki trustpoint CISCO_IDEVID_SUDI sign
490 pki trustpoint MERAKI_TLSGW_CA verify
491 !
492 !
493 !
494 !
495 !
496 !
497 !
498 !
499 !
500 interface Loopback6
501 ip address 6.6.6.6 255.255.255.0
502 !
503 interface Loopback1000
504 description Meraki TLS Connection
505 ip address 20.0.98.203 255.255.255.255
506 !
507 interface Port-channel1
508 no switchport
509 !

```

Modified on 5/26/2024, 5:57:12 AM

[Copy this configuration](#) [Download this configuration](#)

```

487 overlay
488 local-interface Vlan3 priority 1
489 pki trustpoint CISCO_IDEVID_SUDI sign
490 pki trustpoint MERAKI_TLSGW_CA verify
491 !
492 !
493 !
494 !
495 !
496 !
497 !
498 !
499 !
500 interface Loopback6
501 ip address 6.6.6.6 255.255.255.0
502 !
503 interface Loopback1000
504 description Meraki TLS Connection
505 ip address 20.0.74.78 255.255.255.255
506 !
507 interface Port-channel1
508 no switchport
509 !

```

Note: Configurations are checked for changes every 15 minutes. Updates may take up to 15 minutes to appear in the Dashboard. Multiple changes within a 15-minute window will be recorded as a single modified timestamp, including all changes made during that period.

Early Access - Packet Capture Feature

- Navigate back to the above listed tabs > Click on **Summary** > Click on **Port 5** on the visual representation of the switch.

Summary Ports Location Tools Config history

Ports [View ports on this switch](#)

- This eventually takes you back to the Port/Config details for Gi1/0/5 (**the port suggested to take the packet capture**).

Summary **Ports** Location Tools Config history

Port 5: Gi1/0/5 | [Return to port list](#) [Learn more](#)



Historical data for the last day ▾

Port traffic



Configuration

Port status Enabled

- Scroll down to **Troubleshooting** section > Click on the **hyperlink Run a packet capture on this port**.

Troubleshooting

Packet capture

[Run a packet capture on this port](#)

Cycle port



Disable and re-enable this port

Warning: PoE powered devices will be temporarily powered down.

- Takes you the Packet capture page with all switch/port details entered.

Network
Cisco Live ▾

Network-wide

Switching

Organization

Two-factor Authentication is not currently enabled on your Meraki

Account recovery action needed
You are the only administrator for this organization. If you lose access, you will not be able to recover access. [Add another administrator to ensure you can recover access.](#)

Packet capture for switches ▾

Switch: C9300-CloudMon ▾

Switch ports: 1 ⊗

Output: Download .pcap file (for Wireshark) ▾

Duration (secs): 60

Filter expression:

File name: Cisco Live - switch-C9300-CloudMon_IF-Gi1_

Start capture

Note: This page can also be accessed if you navigate to Network-wide > Monitor > Packet Capture, where you choose the device type, the device, port.

- Click **start capture** and wait until it states complete, will take ~1 min.

Packet capture for switches

Switch:

Switch ports:

Output:

Duration (secs):

Filter expression:

File name:

Completed Start capture

Sample filter expressions

ipv4 protocol udp 198.51.100.0/24 eq 20001 any
set various explicit filters

mac 0030.9629.9f84 0000.0000.0000 any
set a filter for MAC addresses

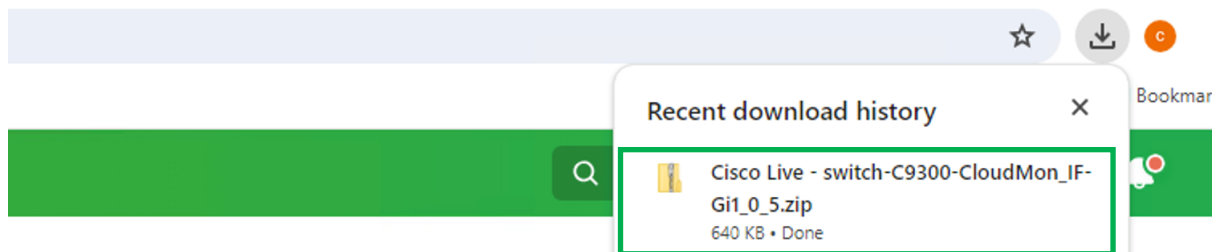
ipv4 198.51.100.0/24 host 198.51.100.1
set a filter for IPv4 traffic

See more [examples](#).

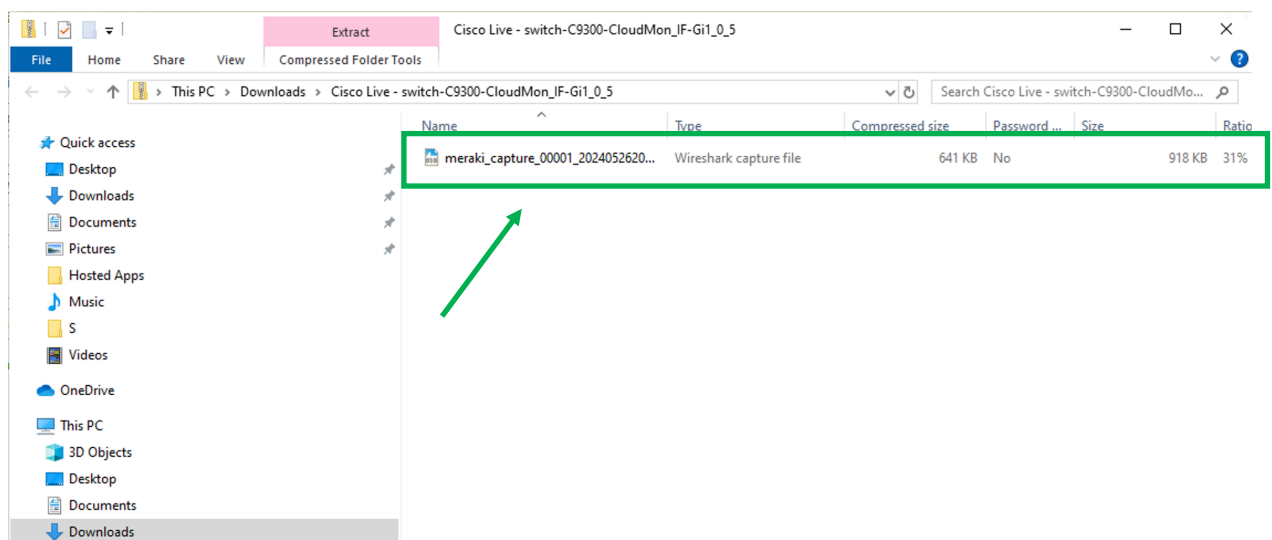
This capture will stop after 60 seconds, or when 100,000 packets are running.

[Packet capture logs](#)

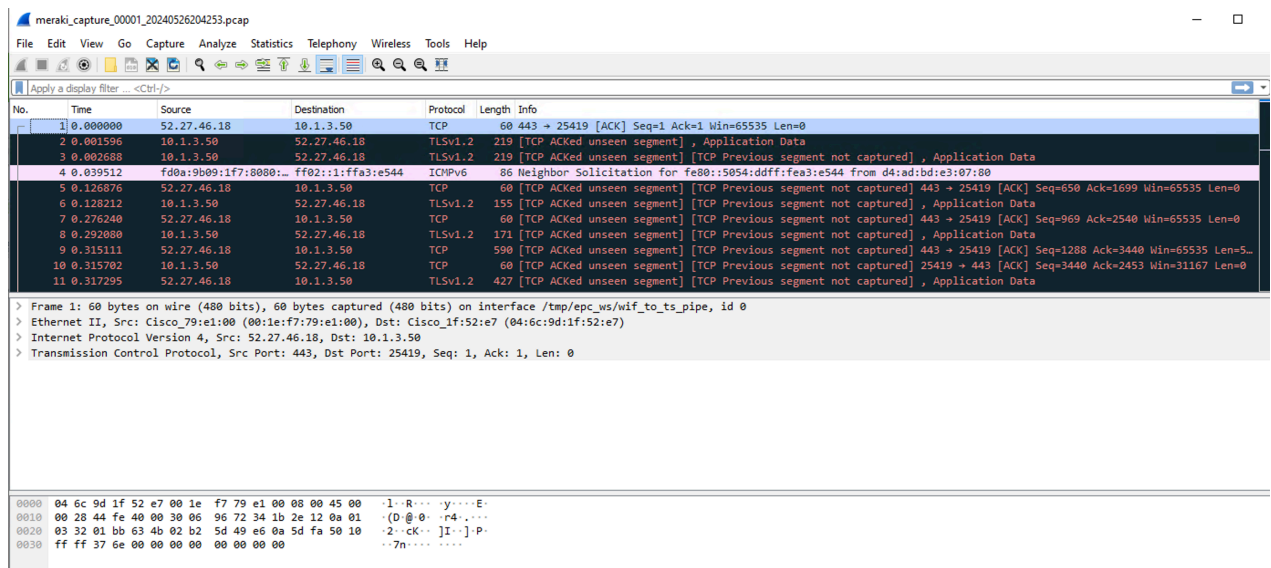
- Click on download icon on the browser to access the .zip file which contains the .pcap file > Double Click on the .zip file.



- Double click on the Wireshark capture file in the downloads folder to view the captures on the local Desktop.

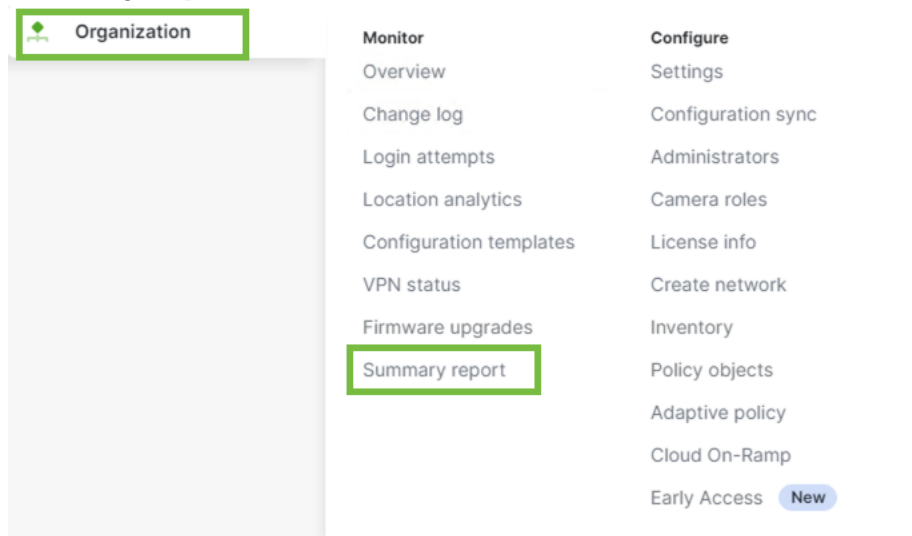


- View Packet captures taken on Port Gi1/0/5 via Wireshark.

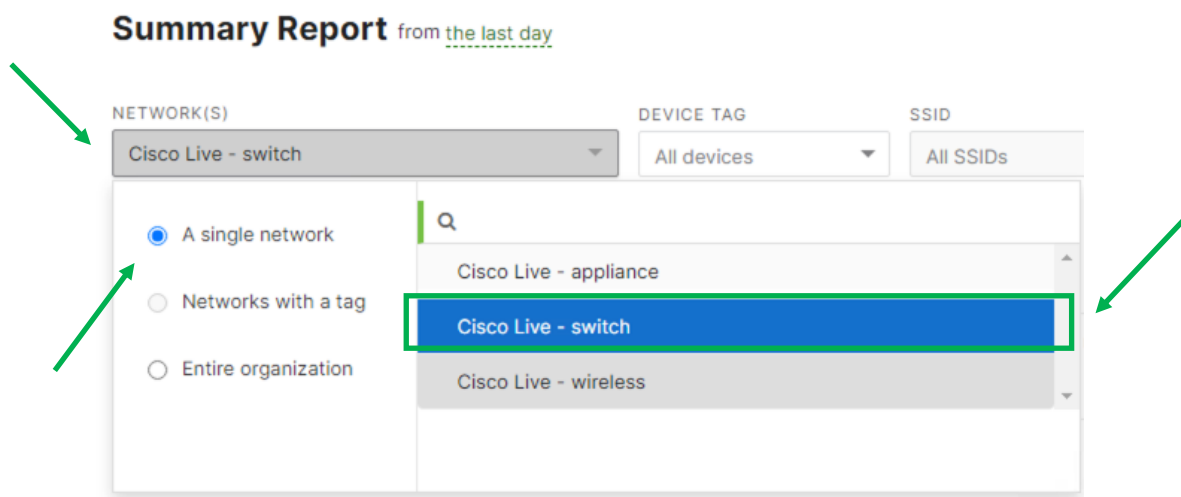


Close Wireshark once done.

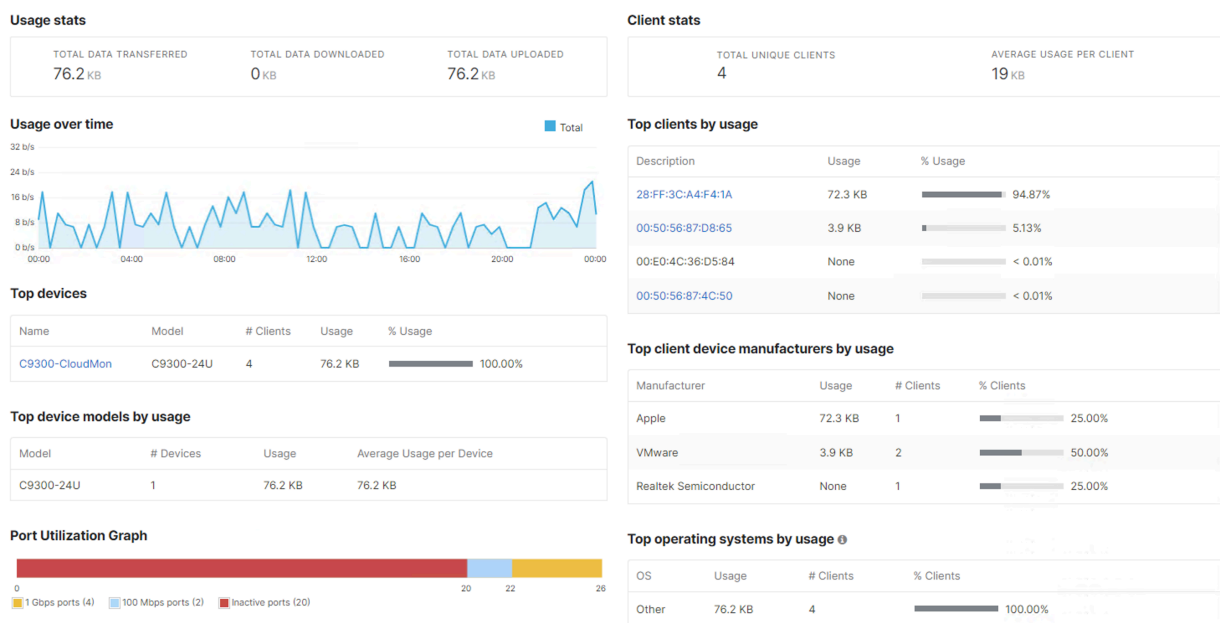
- To view the summary report of the network, we can utilize the summary report feature.
- On the dashboard menu on the left, select **Organization**. Under **Monitor**, select **Summary Report**.



- At the top of the page, you have the option to select viewing the report per a single network or for the entire organization. In our case, we will Select **Organization** since there is just one network we have currently.



- This report provides a comprehensive report of the data usage stats, Top Devices, Top Clients, Clients Stats, Port Utilization and many more statistics that can be used to view the network holistically on the Meraki Dashboard.



- There is also the option to customize the report to select parameters that are more useful to your organization.

SSID: All SSIDs | SHOW TOP RESULTS: 10 | Export to Excel | Customize report

Client stats

TOTAL DATA UPLOADED: 76.2 KB

TOTAL UNIC: 4

Top clients by usage

Description
28:FF:3C:A4:F4:1A
00:50:56:87:D8:65
00:E0:4C:36:D5:84
00:50:56:87:4C:50

Customize report options:

- Ethernet Power**
 - ☒ Power rate over time
 - ☒ Top switches by power usage
- Applications**
 - ☒ Top application categories
 - ☒ Top applications by usage
 - ☐ Top Blocked Sites by URL
 - ☐ Top Blocked Sites by Category
 - ☐ Top Security Threats by Signature
- Port Utilization**
 - ☒ Port Utilization Graph
- Clients**
 - ☒ Client stats
 - ☒ Top clients by usage
 - ☒ Top client device manufacturers by usage
 - ☒ Top operating systems by usage
- Usage**
 - ☒ Usage stats
 - ☒ Usage over time
 - ☒ Top devices
 - ☒ Top device models by usage

- This report can be exported via excel to be used externally as well.

Step 3: Removing Switch from Dashboard

- Select **Switching > Switches**
- **Select the checkbox** next to the switch (C9300-CloudMon).
- On the right, select **Remove**. This will remove the switches from the Meraki dashboard.

Q Search | Filters: 1 result | Download

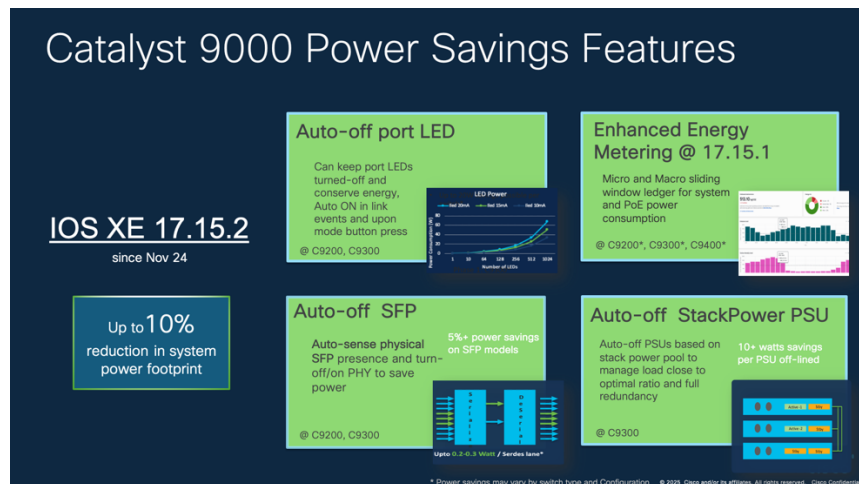
1 Item selected | Clear all | Cancel | Tag | Move | Remove | Clone

Status	Name	MAC address	Connectivity (UTC-8)	Serial number	Local IP	Model	Firmware version
☒	C9300-CloudMon	Monitor Only	bc:5a:56:a6:12:80	Q5TC-BVLJ-PEXN	10.1.3.50	C9300-24U	IOS XE 17.3.4

- In the pop-up message, select **Remove** to confirm removing the switch.

Lab 4: C9K Sustainability Features hands-on

The Catalyst 9200 and 9300 series switches with IOS XE 17.15.2 offers a powerful and intelligent approach to switch power management. By leveraging these auto-off features, we can considerably reduce system power footprint and improve power savings, operational efficiency thus contributing towards sustainable methods.



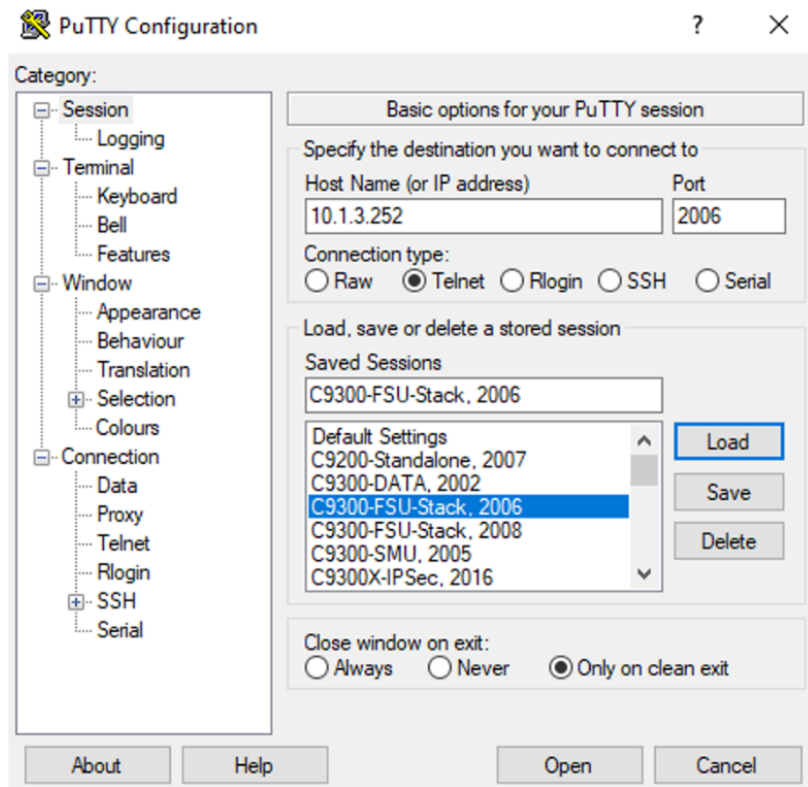
We have introduced 3 different power saving features and 1 power telemetry feature with energy metering feature in IOS-XE 17.15.2 release,

1. Auto-off Port LEDs
2. Auto-off SFP port SerDes
3. Auto-off Power-stack power supplies
4. Enhanced Energy Metering

In this lab we will implement all these 3 auto-off features using switch CLI, this lab is being performed on a C9300 mixed switch stack that is built with C9300-24U and C9300-24UX.

The switch stack has both data-stacking and StackPower enabled, to confirm the stack current operating status, ssh into the switch CLI using putty on the desktop and run the command

Ssh to switch IP 10.1.3.252 port 2006



Confirm the switch stack status using the command

“show switch detail”

```
C9300-xFSU#show switch detail
Switch/Stack Mac Address : 046c.9d1f.3100 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	046c.9d1f.3100	14	V01	Ready
2	Standby	d4ad.7136.8100	1	V02	Ready

Switch#	Stack Port Status		Neighbors	
	Port 1	Port 2	Port 1	Port 2
1	OK	OK	2	2
2	OK	OK	1	1

Once we confirm that the data stack is operational.

Switchport LED Auto-off

With this feature, we can keep the port LEDs turned off while the switch and port links are functional and forward traffic. This feature is introduced to eliminate power wastage with the always on LEDs of frontpanel port LEDs indicating link status. With auto-off enabled, the switch tends to keep the LEDs shutdown and conserve energy while the ports operate normally. In the case of port LEDs needed, admins can turn on LEDs by disabling auto-off feature on the running config or anyone local to the switch can press the mode button on the front panel to wake up the port LEDs from auto-off state and this keeps port lights turned on for 10 minutes until auto-off turn them off.

Run the command “show hardware led” to confirm whether the LEDs are operational and there is no auto-off currently enabled.

```
C9300-xFSU#show hardware led

Current Mode: STATUS
LED Auto off: Disabled

SWITCH: 1
SYSTEM: GREEN
MASTER: GREEN
STATUS: (40) Gil/0/1:ACT_GREEN Gil/0/2:BLACK Gil/0/3:ACT_GREEN Gil/0/4:ACT_GREEN Gil/0/5:ACT_GREEN Gil/0/6:BLACK Gil/0/7:ACT_GREEN Gil/0/8:BLACK Gil/0/9:BLACK Gil/0/10:BLACK Gil/0/11:ACT_GREEN Gil/0/12:BLACK Gil/0/13:BLACK Gil/0/14:BLACK Gil/0/15:BLACK Gil/0/16:BLACK Gil/0/17:BLACK Gil/0/18:BLACK Gil/0/19:BLACK Gil/0/20:BLACK Gil/0/21:BLACK Gil/0/22:ACT_GREEN Gil/0/23:BLACK Gil/0/24:BLACK Gil/1/1:BLACK Gil/1/2:BLACK Gil/1/3:BLACK Gil/1/4:BLACK Tel/1/1:BLACK Tel/1/2:BLACK Tel/1/3:BLACK Tel/1/4:BLACK Tel/1/5:BLACK Tel/1/6:BLACK Tel/1/7:BLACK Tel/1/8:BLACK Fol/1/1:BLACK Fol/1/2:BLACK Twel/1/1:BLACK Twel/1/2:BLACK
DUPLEX: (40) Gil/0/1:GREEN Gil/0/2:BLACK Gil/0/3:GREEN Gil/0/4:GREEN Gil/0/5:GREEN Gil/0/6:BLACK Gil/0/7:GREEN Gil/0/8:BLACK Gil/0/9:BLACK Gil/0/10:BLACK Gil/0/11:GREEN Gil/0/12:BLACK Gil/0/13:BLACK Gil/0/14:BLACK Gil/0/15:BLACK Gil/0/16:BLACK Gil/0/17:BLACK Gil/0/18:BLACK Gil/0/19:BLACK Gil/0/20:BLACK Gil/0/21:BLACK Gil/0/22:GREEN Gil/0/23:BLACK Gil/0/24:BLACK Gil/1/1:BLACK Gil/1/2:BLACK Gil/1/3:BLACK Gil/1/4:BLACK Tel/1/1:BLACK Tel/1/2:BLACK Tel/1/3:BLACK Tel/1/4:BLACK Tel/1/5:BLACK Tel/1/6:BLACK Tel/1/7:BLACK Tel/1/8:BLACK Fol/1/1:BLACK Fol/1/2:BLACK Twel/1/1:BLACK Twel/1/2:BLACK
SPEED: (40) Gil/0/1:BLINK GREEN Gil/0/2:BLACK Gil/0/3:GREEN Gil/0/4:BLINK GREEN Gil/0/5:BLINK GREEN Gil/0/6:BLACK Gil/0/7:BLINK GREEN Gil/0/8:BLACK Gil/0/9:BLACK Gil/0/10:BLACK Gil/0/11:GREEN Gil/0/12:BLACK Gil/0/13:BLACK Gil/0/14:BLACK Gil/0/15:BLACK Gil/0/16:BLACK Gil/0/17:BLACK Gil/0/18:BLACK Gil/0/19:BLACK Gil/0/20:BLACK Gil/0/21:BLACK Gil/0/22:BLINK GREEN Gil/0/23:BLACK Gil/0/24:BLACK Gil/1/1:BLACK Gil/1/2:BLACK Gil/1/3:BLACK Gil/1/4:BLACK Tel/1/1:BLACK Tel/1/2:BLACK Tel/1/3:BLACK Tel/1/4:BLACK Tel/1/5:BLACK Tel/1/6:BLACK Tel/1/7:BLACK Tel/1/8:BLACK Fol/1/1:BLACK Fol/1/2:BLACK Twel/1/1:BLACK Twel/1/2:BLACK
STACK: (40) Gil/0/1:FLASH_GREEN Gil/0/2:BLACK Gil/0/3:BLACK Gil/0/4:BLACK Gil/0/5:BLACK Gil/0/6:BLACK Gil/0/7:BLACK Gil/0/8:BLACK Gil/0/9:BLACK Gil/0/10:BLACK Gil/0/11:BLACK Gil/0/12:BLACK Gil/0/13:BLACK Gil/0/14:BLACK Gil/0/15:BLACK Gil/0/16:BLACK Gil/0/17:BLACK Gil/0/18:BLACK Gil/0/19:BLACK Gil/0/20:BLACK Gil/0/21:BLACK Gil/0/22:BLACK Gil/0/23:BLACK Gil/0/24:BLACK Gil/1/1:BLACK Gil/1/2:BLACK Gil/1/3:BLACK Gil/1/4:BLACK Tel/1/1:BLACK Tel/1/2:BLACK Tel/1/3:BLACK Tel/1/4:BLACK Tel/1/5:BLACK Tel/1/6:BLACK Tel/1/7:BLACK Tel/1/8:BLACK Fol/1/1:BLACK Fol/1/2:BLACK Twel/1/1:BLACK Twel/1/2:BLACK
POE: (40) Gil/0/1:BLACK Gil/0/2:AMBER Gil/0/3:GREEN Gil/0/4:BLACK Gil/0/5:BLACK Gil/0/6:AMBER Gil/0/7:BLACK Gil/0/8:BLACK Gil/0/9:AMBER Gil/0/10:AMBER Gil/0/11:BLACK Gil/0/12:BLACK Gil/0/13:AMBER Gil/0/14:AMBER Gil/0/15:BLACK Gil/0/16:AMBER Gil/0/17:AMBER Gil/0/18:BLACK Gil/0/19:BLACK Gil/0/20:BLACK Gil/0/21:BLACK Gil/0/22:BLACK Gil/0/23:BLACK Gil/0/24:BLACK Gil/1/1:BLACK Gil/1/2:BLACK Gil/1/3:BLACK Gil/1/4:BLACK Tel/1/1:BLACK Tel/1/2:BLACK Tel/1/3:BLACK Tel/1/4:BLACK Tel/1/5:BLACK Tel/1/6:BLACK Tel/1/7:BLACK Tel/1/8:BLACK Fol/1/1:BLACK Fol/1/2:BLACK Twel/1/1:BLACK Twel/1/2:BLACK
STACK POWER: BLACK
XPS: BLACK

RJ45 CONSOLE: GREEN
USB CONSOLE: BLACK
BEACON: BLACK
```

Now that we know the LEDs are enabled and the active links have LEDs turned on, we can quickly see what the power consumption on the switch is by running the command ‘show power detail’

This command gives us the instantaneous power consumption data for the switch.

```
C9300-xFSU#show power detail
SW  PID          Serial#      Status      Sys Pwr  PoE Pwr  Watts
--  -
1A  FWR-C1-715WAC-P  DCC2445C0VL OK          Good    Good    715
1B  FWR-C1-1100WAC   LIT21212W2R OK          Good    Good   1100
2A  FWR-C1-1100WAC-P  DCC2215D1KD OK          Good    Good   1100
2B  FWR-C1-715WAC    DCA2232G1XR OK          Good    Good    715

PS Configuration Mode : StackPower
PS Operating state    : StackPower

Power supplies currently active : 4
Power supplies currently available : 4

Automatic Module Shutdown : Enabled
shutdown Power
Mod Model No      Priority State    Budget Instantaneous Peak Out of In
-----
1   C9300-24U      4      accepted 235      84      84   235   50
2   C9300-24UX    4      accepted 505      118     118  505   50
-----
Total                                740      202

Power Summary
(in Watts)  Allocated Consumed Maximum
-----
System Power 740      202 880
POE Power    15       3   2750
-----
Total        755      205 3630

Meter start time 2025-01-27 20:27:58 UTC
Energy Data For Last 180 Minute

Mod Model No      System Energy (MilliWattSec) System Meter Update
-----
1   C9300-24U      867128571      2025-01-30 07:11:06 UTC
2   C9300-24UX    1249069750     2025-01-30 07:11:06 UTC
-----
```

Note : Your output may vary

since the power-savings by enabling auto-off on LEDs is milliwatts to max of 2 watts on a 2 switch stick, we may not see the power consumption dropping heavily.

Running the below configuration to put port LEDs in auto-off state

```
“”
conf t
hw-module switch 1 auto-off led
hw-module switch 2 auto-off led
“”
```

Now run “show hardware led” to confirm the auto-off being enabled for both switches

```

C9300-xFSU#show hardware led

Current Mode: STATUS
LED Auto off: Enabled

SWITCH: 1
SYSTEM: GREEN
MASTER: GREEN
STATUS: (40) Gi1/0/1:BLACK Gi1/0/2:BLACK Gi1/0/3:BLACK Gi1/0/4:BLACK Gi1/0/5:BLACK Gi1/0/6:BLACK
Gi1/0/11:BLACK Gi1/0/12:BLACK Gi1/0/13:BLACK Gi1/0/14:BLACK Gi1/0/15:BLACK Gi1/0/16:BLACK Gi1/0/17:BLACK
Gi1/0/18:BLACK Gi1/0/19:BLACK Gi1/0/20:BLACK Gi1/0/21:BLACK Gi1/0/22:BLACK Gi1/0/23:BLACK Gi1/0/24:BLACK Gi1/1/1:BLACK Gi1/1/2:BLACK Gi1/1/3:BLACK
Gi1/1/4:BLACK Tel1/1/5:BLACK Tel1/1/6:BLACK Tel1/1/7:BLACK Tel1/1/8:BLACK Tel1/1/9:BLACK Tel1/1/10:BLACK Tel1/1/11:BLACK Tel1/1/12:BLACK
Tel1/1/13:BLACK Tel1/1/14:BLACK Tel1/1/15:BLACK Tel1/1/16:BLACK Tel1/1/17:BLACK Tel1/1/18:BLACK Tel1/1/19:BLACK Tel1/1/20:BLACK Tel1/1/21:BLACK
Tel1/1/22:BLACK Tel1/1/23:BLACK Tel1/1/24:BLACK Tel1/1/25:BLACK Tel1/1/26:BLACK Tel1/1/27:BLACK Tel1/1/28:BLACK Tel1/1/29:BLACK Tel1/1/30:BLACK
Tel1/1/31:BLACK Tel1/1/32:BLACK Tel1/1/33:BLACK Tel1/1/34:BLACK Tel1/1/35:BLACK Tel1/1/36:BLACK Tel1/1/37:BLACK Tel1/1/38:BLACK Tel1/1/39:BLACK
Tel1/1/40:BLACK
DUPLX: (40) Gi1/0/1:BLACK Gi1/0/2:BLACK Gi1/0/3:BLACK Gi1/0/4:BLACK Gi1/0/5:BLACK Gi1/0/6:BLACK
Gi1/0/11:BLACK Gi1/0/12:BLACK Gi1/0/13:BLACK Gi1/0/14:BLACK Gi1/0/15:BLACK Gi1/0/16:BLACK Gi1/0/17:BLACK
Gi1/0/18:BLACK Gi1/0/19:BLACK Gi1/0/20:BLACK Gi1/0/21:BLACK Gi1/0/22:BLACK Gi1/0/23:BLACK Gi1/0/24:BLACK Gi1/1/1:BLACK Gi1/1/2:BLACK Gi1/1/3:BLACK
Gi1/1/4:BLACK Tel1/1/5:BLACK Tel1/1/6:BLACK Tel1/1/7:BLACK Tel1/1/8:BLACK Tel1/1/9:BLACK Tel1/1/10:BLACK Tel1/1/11:BLACK Tel1/1/12:BLACK
Tel1/1/13:BLACK Tel1/1/14:BLACK Tel1/1/15:BLACK Tel1/1/16:BLACK Tel1/1/17:BLACK Tel1/1/18:BLACK Tel1/1/19:BLACK Tel1/1/20:BLACK Tel1/1/21:BLACK
Tel1/1/22:BLACK Tel1/1/23:BLACK Tel1/1/24:BLACK Tel1/1/25:BLACK Tel1/1/26:BLACK Tel1/1/27:BLACK Tel1/1/28:BLACK Tel1/1/29:BLACK Tel1/1/30:BLACK
Tel1/1/31:BLACK Tel1/1/32:BLACK Tel1/1/33:BLACK Tel1/1/34:BLACK Tel1/1/35:BLACK Tel1/1/36:BLACK Tel1/1/37:BLACK Tel1/1/38:BLACK Tel1/1/39:BLACK
Tel1/1/40:BLACK
SPEED: (40) Gi1/0/1:BLACK Gi1/0/2:BLACK Gi1/0/3:BLACK Gi1/0/4:BLACK Gi1/0/5:BLACK Gi1/0/6:BLACK
Gi1/0/11:BLACK Gi1/0/12:BLACK Gi1/0/13:BLACK Gi1/0/14:BLACK Gi1/0/15:BLACK Gi1/0/16:BLACK Gi1/0/17:BLACK
Gi1/0/18:BLACK Gi1/0/19:BLACK Gi1/0/20:BLACK Gi1/0/21:BLACK Gi1/0/22:BLACK Gi1/0/23:BLACK Gi1/0/24:BLACK Gi1/1/1:BLACK Gi1/1/2:BLACK Gi1/1/3:BLACK
Gi1/1/4:BLACK Tel1/1/5:BLACK Tel1/1/6:BLACK Tel1/1/7:BLACK Tel1/1/8:BLACK Tel1/1/9:BLACK Tel1/1/10:BLACK Tel1/1/11:BLACK Tel1/1/12:BLACK
Tel1/1/13:BLACK Tel1/1/14:BLACK Tel1/1/15:BLACK Tel1/1/16:BLACK Tel1/1/17:BLACK Tel1/1/18:BLACK Tel1/1/19:BLACK Tel1/1/20:BLACK Tel1/1/21:BLACK
Tel1/1/22:BLACK Tel1/1/23:BLACK Tel1/1/24:BLACK Tel1/1/25:BLACK Tel1/1/26:BLACK Tel1/1/27:BLACK Tel1/1/28:BLACK Tel1/1/29:BLACK Tel1/1/30:BLACK
Tel1/1/31:BLACK Tel1/1/32:BLACK Tel1/1/33:BLACK Tel1/1/34:BLACK Tel1/1/35:BLACK Tel1/1/36:BLACK Tel1/1/37:BLACK Tel1/1/38:BLACK Tel1/1/39:BLACK
Tel1/1/40:BLACK

```

Run “show power detail” command to see if power consumption has any change.
(your power consumption numbers would be varying)

Power Summary (in Watts)	Allocated	Consumed	Maximum Available
System Power	740	196	880
POE Power	15	3	2750
Total	755	199	3630

When auto-off is enabled for port LEDs, one can press the mode button and turn on the port LEDs for port status for 10 minutes.

Auto-off Optics

Auto-off optics is designed to turn-off SerDes on the SFP port/port-group on the switch ‘when there is no physical module inserted into the SFP ports.

since speed/bandwidth of the ports is proportionate to number of dedicated SerDes lanes to that port/port-group. This translates to, the higher the bandwidth of the ports are, the higher the possible power savings.

Run the below configuration to do enable auto-off for optics.

“”

Conf t

hw-module switch 1 auto-off optics

hw-module switch 2 auto-off optics

“”

After this we can run “show power detail” however the power savings varies based on the port type. These savings would not be applied to a copper port.

```
Power Summary
(in Watts)   Allocated Consumed Maximum Available
-----
System Power 740      195      880
POE Power    15        3       2750
-----
Total       755      198      3630

Meter start time 2025-01-27 20:27:58 UTC
Energy Data For Last 180 Minute

Mod Model No          System Energy (MilliWattSec) System Meter Update Time
-----
1   C9300-24U          837467131      2025-01-30 07:35:06 UTC
2   C9300-24UX         1206461625     2025-01-30 07:35:06 UTC
-----

C9300-xFSU(config)#
C9300-xFSU(config)#
C9300-xFSU(config)#hw-module switch 1 auto-off optics
C9300-xFSU(config)#hw-module switch 2 auto-off optics
C9300-xFSU(config)#
C9300-xFSU(config)#do shw pow det
C9300-xFSU(config)#do shw pow detail

SW  PID              Serial#      Status      Sys Pwr  PoE Pwr  Watts
---  ---
1A  PWR-C1-715WAC-P    DCC2445C0VL OK          Good     Good     715
1B  PWR-C1-1100WAC     LIT21212W2R OK          Good     Good     1100
2A  PWR-C1-1100WAC-P    DCC2215D1KD OK          Good     Good     1100
2B  PWR-C1-715WAC      DCA2232G1XR OK          Good     Good     715

PS Configuration Mode : StackPower
PS Operating state    : StackPower

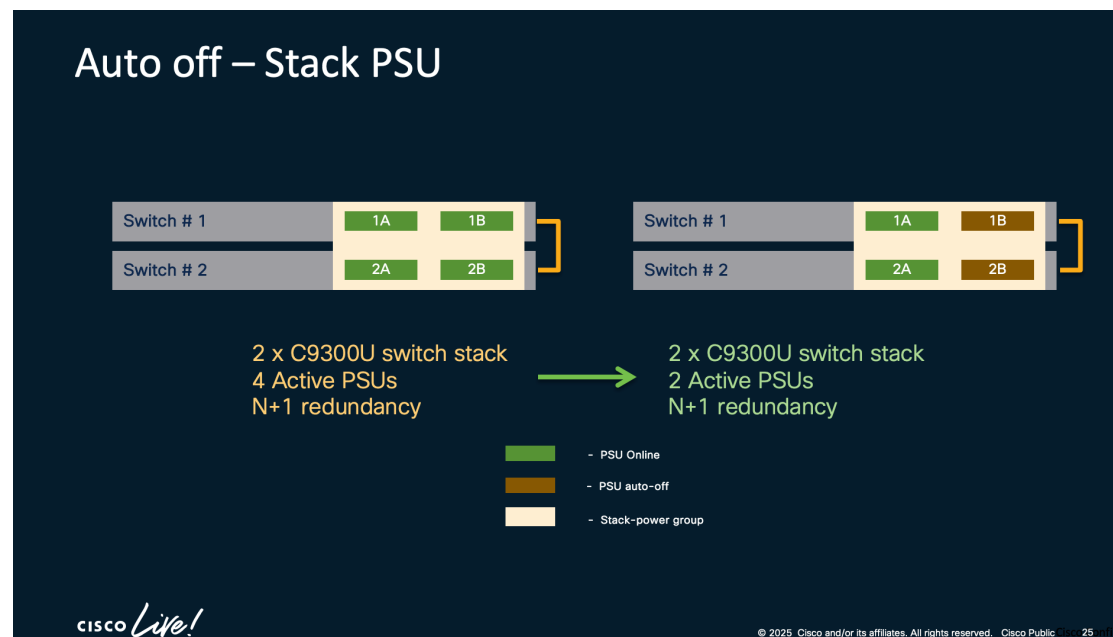
Power supplies currently active : 4
Power supplies currently available : 4

Automatic Module Shutdown : Enabled
shutdown Power
Mod Model No          Priority State Budget Instantaneous Peak Out of In
-----
1   C9300-24U          4     accepted 235    80      80    235  50
2   C9300-24UX         4     accepted 505    119     119   505  50
-----
Total                    740    198

before auto-off optics enabled

after auto-off optics enabled
```





Cisco StackPower technology enables power aggregation on a catalyst 9300 switch stack configuration to pool the power in shared mode. This feature is designed to increase redundancy, high power availability across stack members and enables efficient design methods. With this new 'auto-off' feature on stack-power the system will now auto shutdown power supplies that are more than needed beyond 50% load and n+1 redundancy. For example, in the below CLI output picture of a switch stack. We can observe 4 different points in this output,

1. Wattage available by each Power supply individually
2. Current operating mode of these power supplies
3. How many power supplies are currently active
4. What is the aggregate power pool wattage with all power supplies if in stackpower combined.

Run the command “show power detail” to understand the overall operational power status of the switch.

```

C9300-xFSU#show power detail
SW  PID                Serial#      Status      Sys Pwr  PoE Pwr  Watts
-----
1A  PWR-C1-715WAC-P      DCC2445C0VL OK          Good    Good    715
1B  PWR-C1-1100WAC       LIT21212W2R OK          Good    Good    1100
2A  PWR-C1-1100WAC-P     DCC2215D1KD OK          Good    Good    1100
2B  PWR-C1-715WAC        DCA2232G1XR OK          Good    Good    715

PS Configuration Mode : StackPower
PS Operating state    : StackPower

Power supplies currently active : 4
Power supplies currently available : 4

Automatic Module Shutdown : Enabled
shutdown
Power
Mod  Model No      Priority  State      Budget  Instantaneous  Peak  Out of  In
-----
1    C9300-24U      4        accepted  235     81             81    235    50
2    C9300-24UX     4        accepted  505     116            117   505    50
Total
740    197

Power Summary
(in Watts)  Allocated  Consumed  Maximum
-----
System Power 740      197      880
POE Power    15        3        2750
Total        755      200      3630

Meter start time 2025-01-30 08:05:31 UTC
Energy Data For Last 180 Minute

Mod  Model No      System Energy  System Meter Update
-----
1    C9300-24U      799125300     2025-01-30 19:15:36 UTC
2    C9300-24UX    1144900500    2025-01-30 19:15:36 UTC

```

Run the command “show environment all” to see the input and output power for each power supply.

```

C9300-xFSU#show environment all
Sensor List: Environmental Monitoring
Sensor      Location  State      Reading      Range (min-max)
PS1 Vout    1        GOOD      55918 mV     na
PS1 Vin     1        GOOD      208500 mV    90 - 264
PS1 CURin   1        GOOD      273 mA       na
PS1 Curout  1        GOOD      422 mA       na
PS1 POWin   1        GOOD      27250 mW     na
PS1 POWout  1        GOOD      23500 mW     na
PS1 FAN     1        GOOD      2960 rpm     na
PS2 Vout    1        GOOD      56000 mV     na
PS2 Vin     1        GOOD      208000 mV    90 - 264
PS2 CURin   1        GOOD      500 mA       na
PS2 CURout  1        GOOD      1375 mA      na
PS2 POWin   1        GOOD      92000 mW     na
PS2 POWout  1        GOOD      80000 mW     na
PS2 FAN     1        GOOD      4192 rpm     na
SYSTEM INLET 1        GREEN     31 Celsius   0 - 56
SYSTEM OUTLET 1        GREEN     42 Celsius   0 - 125
SYSTEM HOTSPOT 1        GREEN     54 Celsius   0 - 125

Switch  FAN      Speed  State  Airflow direction

```

We can now filter the same command output to only monitor what is the power draw by all the power supplies on this stack by running the command. Do run

this command on your switch and understand what the actual total power is drawn across all power supplies.

“Show environment all | I POW”

For example, in the following output we can see that stack is currently drawing about 1572 watts.

```
C9300-xFSU#show environment all | i POW
PS1 POWin      1  ← switch 1 PS#1      27250 mW      na
PS1 POWout     1      GOOD      24000 mW      na
PS2 POWin      1  ← switch 2 PS#2      92000 mW      na
PS2 POWout     1      GOOD      80000 mW      na
PS1 POWin      2  ← switch 1 PS#1      63250 mW      na
PS1 POWout     2      GOOD      55625 mW      na
PS2 POWin      2  ← switch 2 PS#2      57500 mW      na
PS2 POWout     2      GOOD      44750 mW      na
C9300-xFSU#
```

Now run “show power detail” to understand the load, in the below screenshot we can see the switch is have an active load of 205 watts and active power draw is 239.75 watts. The system power allocation is 740 watts while the aggregate power available on the pool is 3265 watts.

To maintain N+1 redundancy the switch can now scale down to 3 power supplies based on the installed power supply capacity.

```
C9300-xFSU#show power detail
SW  PID          Serial#      Status      Sys Pwr  PoE Pwr  Watts
---  -
1A  PWR-C1-350WAC-P  DCC2316B26P OK          Good     Good     350
1B  PWR-C1-1100WAC   LIT21212PCW OK          Good     Good    1100
2A  PWR-C1-1100WAC-P  DCC2215D1YH OK          Good     Good    1100
2B  PWR-C1-715WAC    DCA2232G1XW OK          Good     Good     715

PS Configuration Mode   : StackPower
PS Operating state      : StackPower

Power supplies currently active   : 4
Power supplies currently available : 4

Automatic Module Shutdown : Enabled
shutdown Power
Mod  Model No      Priority  State   Budget  Instantaneous  Peak  Out of  In
-----
1    C9300-24U       3        accepted 235     85           85   235    50
2    C9300-24UX     4        accepted 505     120          120  505    50
Total
740    205

Power Summary
(in Watts)  Allocated  Consumed  Maximum
-----
System Power 740      205      770
POE Power    0        0        2495
Total        740      205      3265
```

Run ‘show stack-power detail’ to identify the stack-power domain name and tack-power neighbors along the status of auto-off configuration on the stack

```
C9300-xFSU#sho stack-power detail
```

Power Stack Num	Stack Name	Stack Mode	Stack Topolgy	Total Pwr (W)	Rsvd Pwr (W)	Alloc Pwr (W)	Sw_Avail Pwr (W)
4	Powerstack-1	SP-PS	Ring	3265	30	740	2495

```

Power stack name: Powerstack-1
Stack mode: Power sharing
Stack topology: Ring
Stack total input power: 3265
Power Supply auto-off: Disable
Switch 1:
  Power budget: 1500
  Power allocated: 235
  Low port priority value: 21
  High port priority value: 12
  Switch priority value: 3

```

```
xFSU-C9300-stack#sho stack-power detail
```

Power Stack Name	Stack Mode	Stack Topolgy	Total Pwr (W)	Rsvd Pwr (W)	Alloc Pwr (W)	Sw_Avail Pwr (W)	Num SW	Num PS
Powerstack-2	SP-PS	Ring	4400	30	740	3630	2	4

```

Power stack name: Powerstack-2
Stack mode: Power sharing
Stack topology: Ring
Stack total input power: 4400
Power Supply auto-off: Disable
Switch 2:
  Power budget: 1945
  Power allocated: 505
  Low port priority value: 22
  High port priority value: 13
  Switch priority value: 4
  Port 1 status: Connected
  Port 2 status: Connected
  Neighbor on port 1: Switch 1 - 046c.9dlf.1a80
  Neighbor on port 2: Switch 1 - 046c.9dlf.1a80

Switch 1:
  Power budget: 1675
  Power allocated: 235
  Low port priority value: 21
  High port priority value: 12
  Switch priority value: 3
  Port 1 status: Connected
  Port 2 status: Connected
  Neighbor on port 1: Switch 2 - 7018.a723.3880
  Neighbor on port 2: Switch 2 - 7018.a723.3880

```

Now configure auto-off on the stackpower

“”

Conf t

stack-power stack <Power Stack name> i.e Powerstack-1 or 2
auto-off

“”


```

C9300-xFSU#
C9300-xFSU#conf
000314: *Jan 30 21:54:31.037: %SYS-5-CONFIG_I: Configured from console by console t
Enter configuration commands, one per line. End with CNTL/Z.
C9300-xFSU(config)#stack-power stack Powerstack-1
C9300-xFSU(config-stackpower)#auto-off
Auto off is already enabled
C9300-xFSU(config-stackpower)#
C9300-xFSU(config-stackpower)#

```

This feature not only makes the stack runs with leaner number of PSUs but also efficient. This is because industry grade platinum rated, and titanium rated power supplies are peak efficient at 30-54% operational load. This is achieved by reducing the total number of active power supplies and tuning the load to supply ratio on the power supplies.

Level	White	Bronze	Silver	Gold	Platinum	Titanium
						
10%	X	X	X	X	X	90%
20%	80%	82%	85%	87%	90%	92%
50%	80%	85%	88%	90%	92%	94%
100%	80%	82%	85%	87%	89%	90%

Now run “show stack-power detail” to confirm the auto-off status

Power stack name: Powerstack-1
Stack mode: Power sharing
Stack topology: Standalone
Stack total input power: 1815
Power Supply auto-off: Enable

Once enabled, this will trigger the auto-off process and the switch will now gauge the running load to supply ratio and detect the possibility of soft-shutting power supplies. In the screenshot below we can see a power supply being off-lined aka softshut.


```

Power stack name: Powerstack-1
  Stack mode: Power sharing
  Stack topology: Standalone
  Stack total input power: 1815
  Power Supply auto-off: Enable
Switch 1:
  Power budget: 1675
  Power allocated: 250
  Low port priority value: 22
  High port priority value: 13
  Switch priority value: 4
  Port 1 status: Not connected
  Port 2 status: Not connected
  Neighbor on port 1: 0000.0000.0000
  Neighbor on port 2: 0000.0000.0000

C9300-xFSU#
000316: *Jan 30 21:57:38.306: %PLATFORM_FEP-6-FRU_PS_OIR: Switch 1: FRU power supply A powered off
000317: *Jan 30 21:57:46.314: %ILPOWER-6-SET_AVAILABLE_ILPOWER: Available POE budget for switch 1 is
C9300-xFSU#
C9300-xFSU#
C9300-xFSU#

```

By running “show power detail” we can now see how many power supplies are active

```

C9300-xFSU#sho power detail
SW  PID          Serial#      Status      Sys Pwr  PoE Pwr  Watts
--  -
1A  PWR-C1-350WAC-P DCC2316B26P Disabled    Bad     Bad     350
1B  PWR-C1-1100WAC  LIT21212PCW OK          Good    Good    1100
2A  PWR-C1-1100WAC-P DCC2215D1YH OK          Good    Good    1100
2B  PWR-C1-715WAC   DCA2232G1XW Disabled    Bad     Bad     715

PS Configuration Mode : StackPower
PS Operating state    : StackPower

Power supplies currently active : 2
Power supplies currently available : 4

Automatic Module Shutdown : Enabled
shutdown Power
Mod  Model No      Priority  State    Budget  Instantaneous  Peak  Out of  In
-----
1    C9300-24U      3        accepted 235      87         87   235    50
2    C9300-24UX     4        accepted 505      124        124  505    50
Total
-----
Total          740      211

Power Summary
(in Watts)    Allocated  Consumed  Maximum
-----
System Power  740        211      770
POE Power     0          0        1430
Total         740        211      2200

```

After auto-off enabled and after few iterations, there are now 2 active power supplies out of 4, run the below command to count total power drawn at the power supplies.

Show environment all | I POWin

```

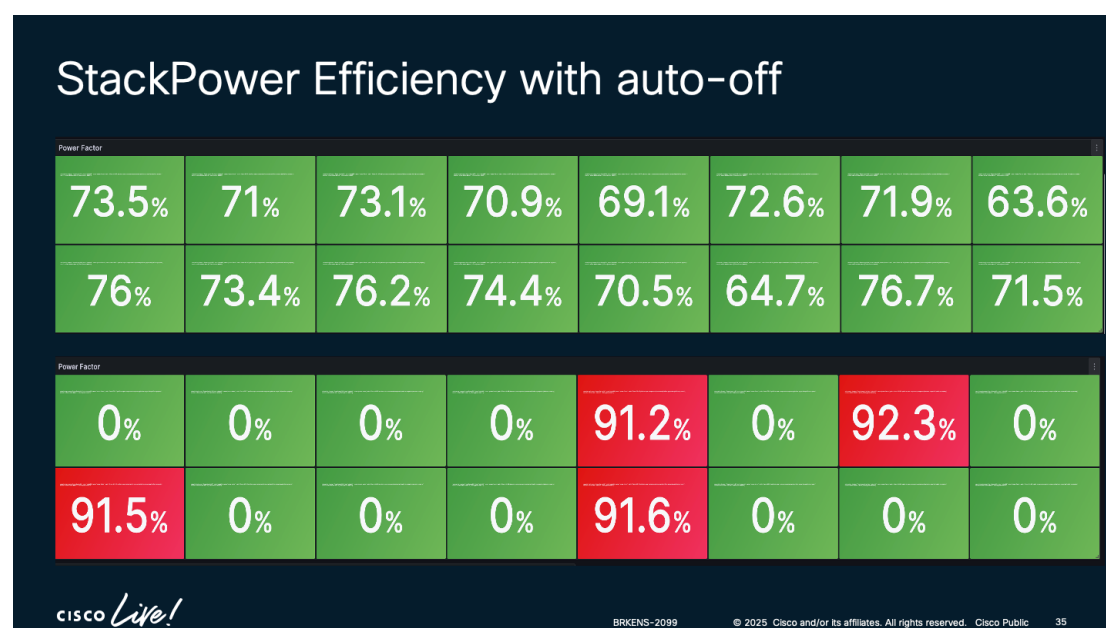
C9300-xFSU#Show environment all | I POWin
PS1 POWin      1      PRESENT      0 mW      na
PS2 POWin      1      GOOD        128000 mW  na
PS1 POWin      2      GOOD        104750 mW  na
PS2 POWin      2      PRESENT      0 mW      na
C9300-xFSU#

```

Now the system is currently drawing a total of 228.75 watts from the AC power supply to operate the entire stack with n+1 redundancy. That is a active+standby power footprint reduction from.

That is a 12+ watts of idle power reduction with 2 PSU's offlined while the stack still have N+1 redundancy. The savings gets bigger as this auto-off scales over higher number of switches in a stack.

An example of power efficiency improvements at a bigger stack, in the following picture we can see how the power factor reflecting the power efficiency of an operational PSU with auto-off enabled on a 8-switch stack can be seen.



Optional : disable auto-off on stackpower and this will bring all PSUs online

Conf t

stack-power stack < Power Stack name> i.e Power stack-1 or 2
no auto-off

This completes the C9K sustainability features hands-on lab.

Lab 5: Extended Fast Software Upgrade for Catalyst 9300 Series Switches

Learning Objectives

The goal of this lab is to leverage the xFSU (Extended Fast Software Upgrade) capability on the 9300 series switch to successfully upgrade a 2-member stack from one Extended Maintenance release (EMR) to another and experience a traffic downtime of less than 5 sec measured via Spirent.

Upon completion of this lab, you will be able to:

- Check if your switch is eligible for an xFSU upgrade/ Fast Reload
- Successfully execute xFSU upgrade

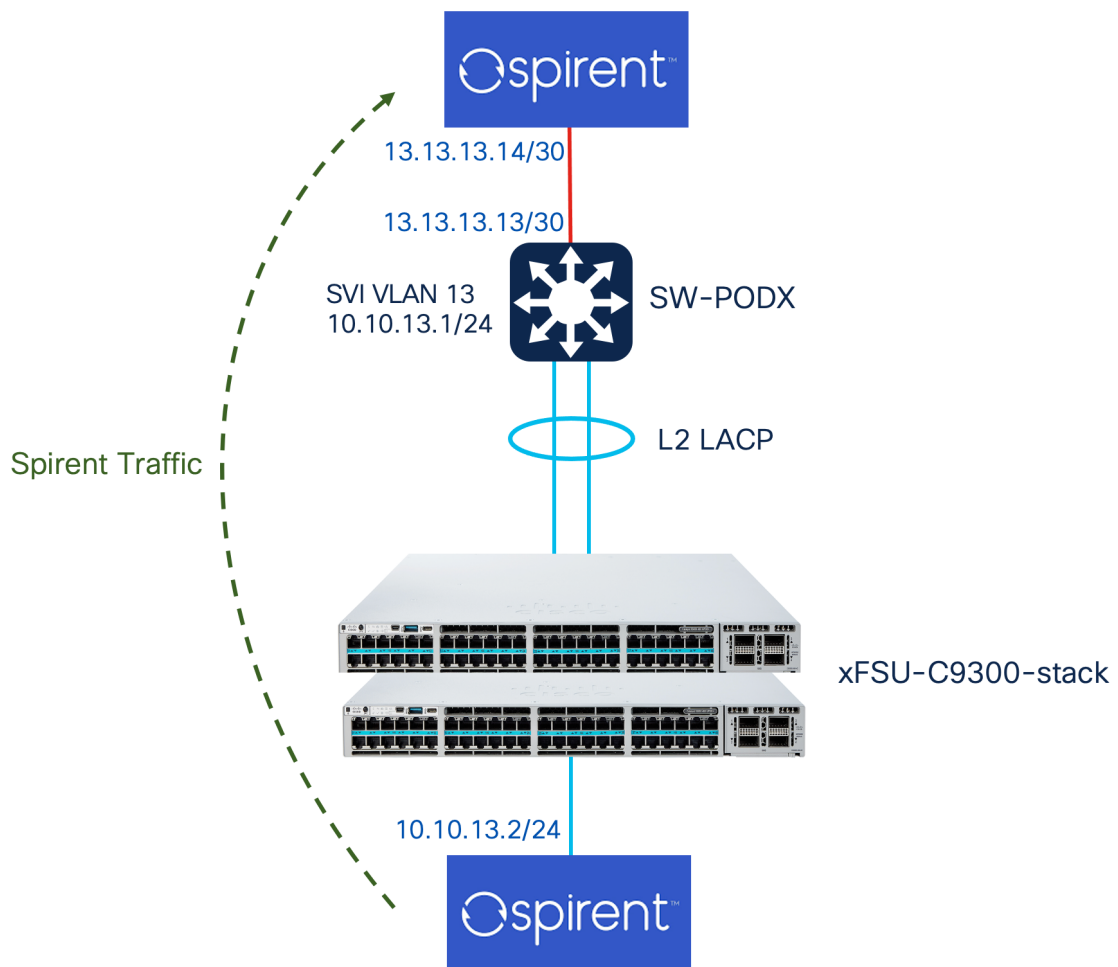
Scenario

In traditional upgrades, network downtime can exceed 10 minutes, which is unacceptable in mission-critical environments such as hospitals, airports etc. The total disruption includes not just the reload/upgrade duration but also the time required for network recovery. xFSU addresses this challenge by significantly reducing downtime to less than 5 sec from IOS XE 17.15.2, making it ideal for access layer deployments where endpoints often rely on aggressive failover timers.

Designed for Catalyst 9300 series switches, whether deployed in standalone or stacked mode. It minimizes traffic downtime to less than 5 seconds during software upgrades and reloads, with no topology changes, regardless of whether the switch operates as a Layer 2 access node or a Layer 3 routed access node, while also, ensuring hitless Perpetual PoE for uninterrupted power to connected devices.

Network Diagram

This lab consists of a 2-member 9300 stack (xFSU-C9300-stack) as a L2 access node connected to a L3 switch (SW-PODX, where X is your POD number) using a L2 LACP port channel.



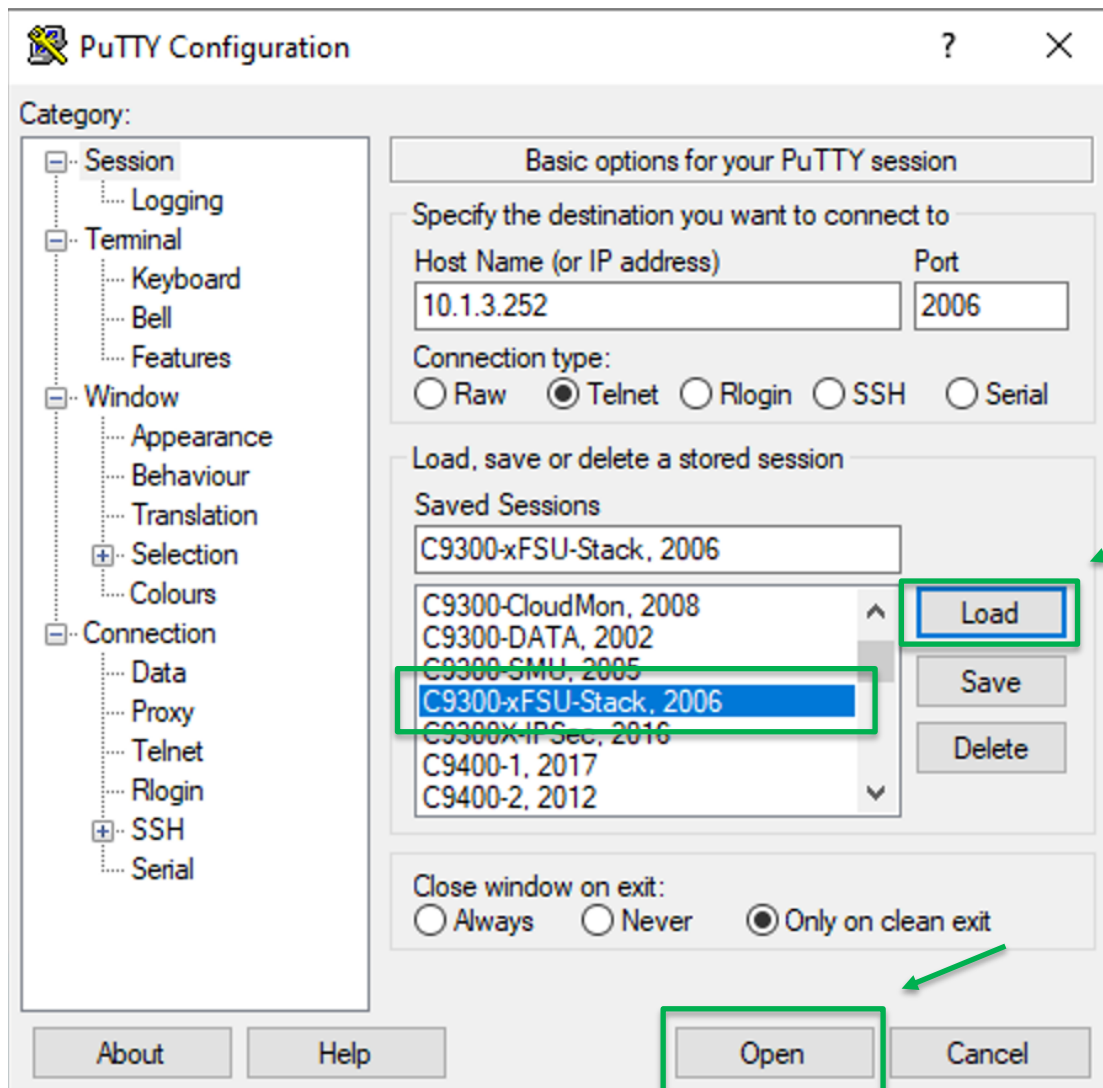
Unidirectional south-to-north traffic will be transmitted using a Spirent traffic generator while executing the xFSU upgrade on the switch stack.

Task 1: Verify the xFSU requirement

- Launch the putty session by clicking on the **Putty icon** pinned on the task bar.



- Click **C9300-FSU-Stack** under saved sessions > **Load** > **Open** to successfully open a session to the xFSU-C9300-stack switch.



If asked, enable password: **cisco**

- Enter the command **show version / beg SW Version** to display the software version and boot mode for the two switches in the stack.

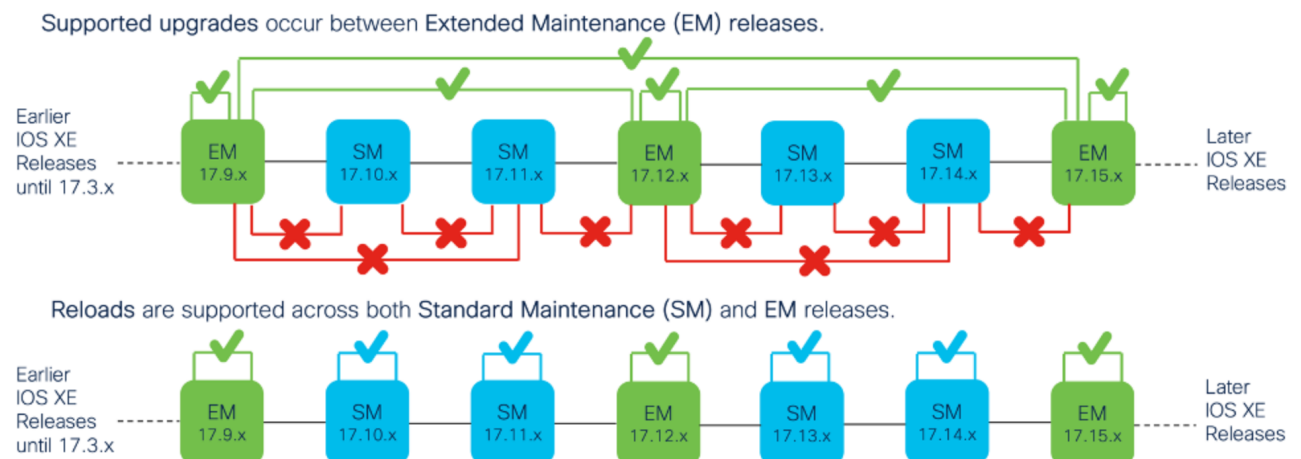
xFSU-C9300-stack# **show version / begin SW Version**

Switch	Ports	Model	SW Version	SW Image	Mode
* 1	41	C9300-24U	17.15.02	CAT9K_IOSXE	INSTALL
2	41	C9300-24UX	17.15.02	CAT9K_IOSXE	INSTALL

Note: This feature is supported only in **Install Mode** and Cisco IOS® XE 17.3.2a release and later onwards.

IOS XE Release	17.3.2a	→ 17.7.1	→ 17.15.2
Supported 9300 Platforms	Catalyst 9300/L	All	All
Downtime	< 30 seconds	< 30 seconds	< 5 seconds

Note: xFSU supports software upgrades and reloads for specific IOS XE releases, including upgrades within EM releases, upgrades between EM releases, and reloads across both SM and EM releases.



- Enter the command ***show license summary*** to check the switch's license status

```
xFSU-C9300-stack# show license summary
```

```
Account Information:
```

```
Smart Account: <none>
```

```
Virtual Account: <none>
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage	(C9300-24 Network Advan...)	2	IN USE
dna-advantage	(C9300-24 DNA Advantage)	2	IN USE

Note: Minimum licensing requires **Network Essentials** for standalone switches and **Network Advantage** for stacked switches.

As this is a 2-member stack, it requires **Network Advantage License** as displayed.

- Enter the command **show spanning-tree summary** to check if the following STP conditions are met for this switch:

1. Spanning Tree Mode

The device must be configured with either Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP)

2. Root Bridge Information

The device must not be a ROOT BRIDGE

3. Port State for the VLAN connected to the STP peer, in this labs case VLAN13. xFSU is supported only if the number of ports in the forwarding state connected to an STP peer is less than or equal to 1

```
xFSU-C9300-stack# show spanning-tree summary

Switch is in rapid-pvst mode
Root bridge for: none

Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
BPDU sender conflict is enabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is long

Name Blocking Listening Learning Forwarding STP Active
-----
VLAN0013 0 0 0 2 2
-----
1 vlan 0 0 0 2 2
```

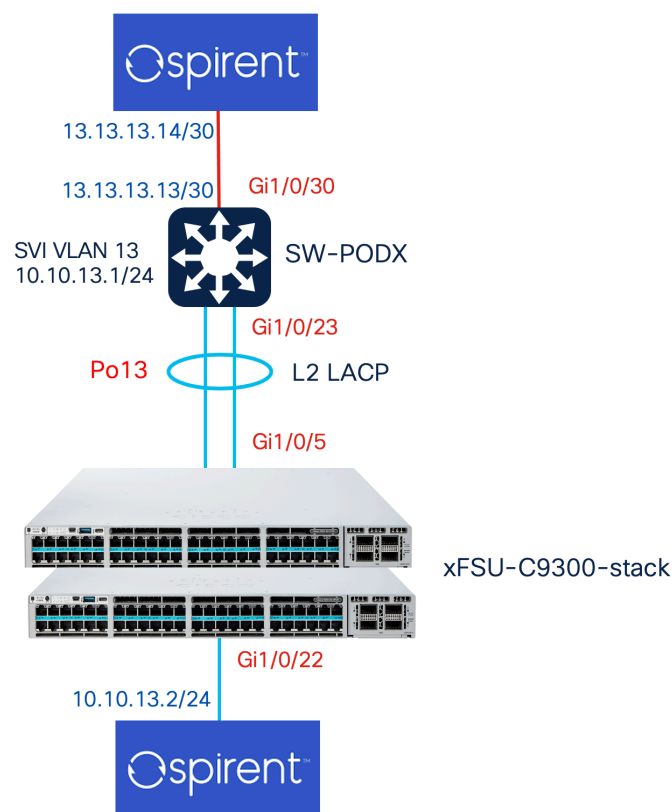
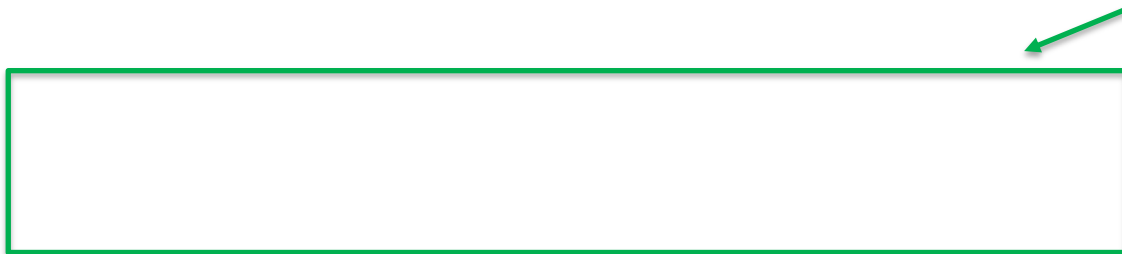
Spanning Tree details to determine if this holds true for xFSU eligibility.

- Enter the command **show spanning-tree vlan 13** to check VLAN 13's STP details, including port roles, forwarding status etc. essential for xFSU eligibility verification.

```
xFSU-C9300-stack# show spanning-tree vlan 13

VLAN0013
Spanning tree enabled protocol rstp
Root ID Priority 24589
Address 885a.925c.c100
Cost 20000
Port 3061 (Port-channel13)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32781 (priority 32768 sys-id-ext 13)
Address 046c.9d1f.1a80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```



In this setup, Spirent is an edge device as it does not participate in Spanning Tree or send BPDUs. **PortFast** is enabled on its connected interface to ensure immediate forwarding.

```
xFSU-C9300-stack# show run interface Gi1/0/22
```

```
interface GigabitEthernet1/0/22
description Spirent connection for xFSU
switchport access vlan 13
switchport mode access
spanning-tree portfast trunk
end
```


Since Gi1/0/22 is an edge port (P2P Edge), it does not count as an STP peer, thereby meeting the xFSU condition.

NOTE: xFSU will function only if the specified STP criteria are met as seen above. When deployed in the access layer, STP-related issues are unlikely. However, in distribution or core layer deployments, you may need to make necessary adjustments to ensure compliance with the STP requirements.

- Enter the command **show redundancy status** to verify that SSO is configured on the device to meet xFSU eligibility criteria.

```
xFSU-C9300-stack# show redundancy states
```

```
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit = Primary
Unit ID = 1
```

```
Redundancy Mode (Operational) = sso
```

```
Redundancy Mode (Configured) = sso
```

```
Redundancy State = sso
```

```
Maintenance Mode = Disabled
```

```
Manual Swact = enabled
```

```
Communications = Up
```

```
client count = 122
```

```
client_notification_TMR = 30000 milliseconds
```

```
RF debug mask = 0x0
```

•

```
xFSU-C9300-stack# show xfsu eligibility
```

```
Reload fast supported: Yes
```

```
Warnings based on the configuration.
```

```
If upgrade is done to an image with incompatible FPGA or ROMON, XFSU will fail
```

```
xFSU PLATFORM Status: Not started yet
```

```
Stack Configuration: Yes
```

Eligibility Check	Status
=====	=====

Autoboot Enabled	Yes
------------------	-----

Install Mode	Yes
--------------	-----

Network Advantage License	Yes
---------------------------	-----

Full ring stack	Yes
-----------------	-----

Check macsec eligibility	Eligible
--------------------------	----------

Note: All the status should be Yes or eligible to continue xFSU

Spanning Tree	Eligible
---------------	----------

Note: For STP status should be eligible to continue xFSU

SSO Mode	Yes
----------	-----

All these criteria need to be met!
> Since this is a 2-member stack, it needs to be operating in full ring.
> Macsec cannot be configured.

This command summarizes all the requirements for xFSU. If any criteria are not met, it will be marked as ineligible.

Now that all xFSU criteria are met, we can proceed with Reload Fast (reload) or Extended Fast Software Upgrade (upgrade).

KEY DESIGN CONSIDERATIONS:

Since this is an **L2 Access Node**, no Graceful Restart (GR) configuration is needed. However, for an L3 Routed Access Node running BGP, IS-IS, or OSPF, ensure the appropriate GR configuration is applied.

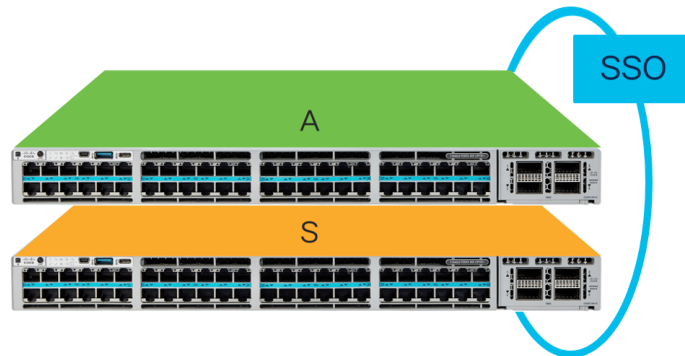
Task 2: Upgrading the Switch using xFSU and calculating the Convergence time

During a **Fast Reload** or **Extended Fast Software Upgrade (xFSU)**, it separates the control plane and data plane, leveraging NSF and Graceful Restart for control plane continuity while maintaining data plane traffic. Additionally, it uses cache and flush architecture for the data plane, ensuring minimal traffic disruption during the upgrade process.



xFSU isn't just limited to standalone setups – it also supports stack configurations. For protocols requiring control plane intervention, the stack xFSU reload/upgrade process works seamlessly.

- intact, Standby switch goes for a reload and comes back online to form SSO with current Active Switch
- Active Switch goes for a reload triggering auto-switchover causing the standby switch to become the new active
- Active Switch comes back online to become the new standby and forms SSO with new Active Switch



AIM: Upgrading the 2-member stack (xFSU-C9300-stack) from IOS® XE 17.15.2 to IOS® XE 17.15.3 using xFSU.

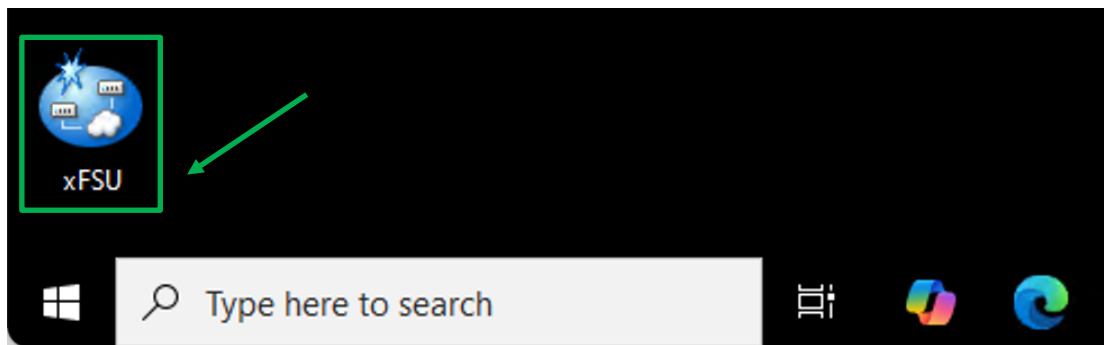
- The switch is running IOS® XE 17.15.2 > Enter the command **show flash: / include .bin** to find IOS® XE 17.15.03 .bin image available on the flash to upgrade to.

```
xFSU-C9300-stack# show flash: / include .bin
```

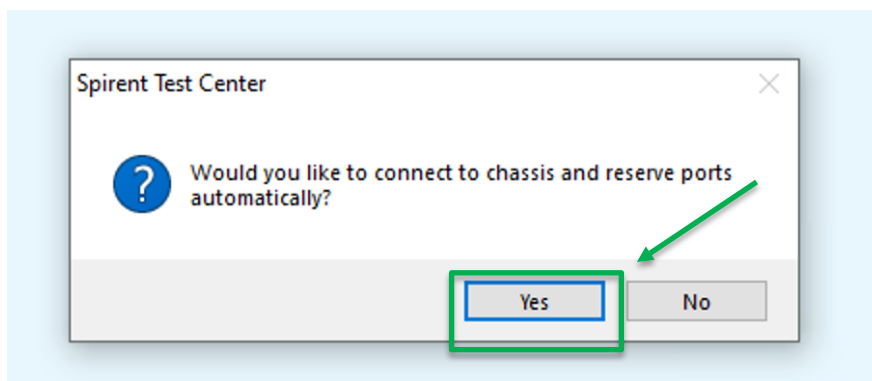
```
130 1281247872 Jan 31 2025 20:20:00 +00:00 cat9k_iosxe.17.15.02.SPA.bin
301 1281360707 Jan 31 2025 00:27:03 +00:00 cat9k_iosxe.17.15.03prd2.SPA.bin
```

NOTE: IOS® XE 17.15.3 will be officially out in March 2025, this is an engineering production image.

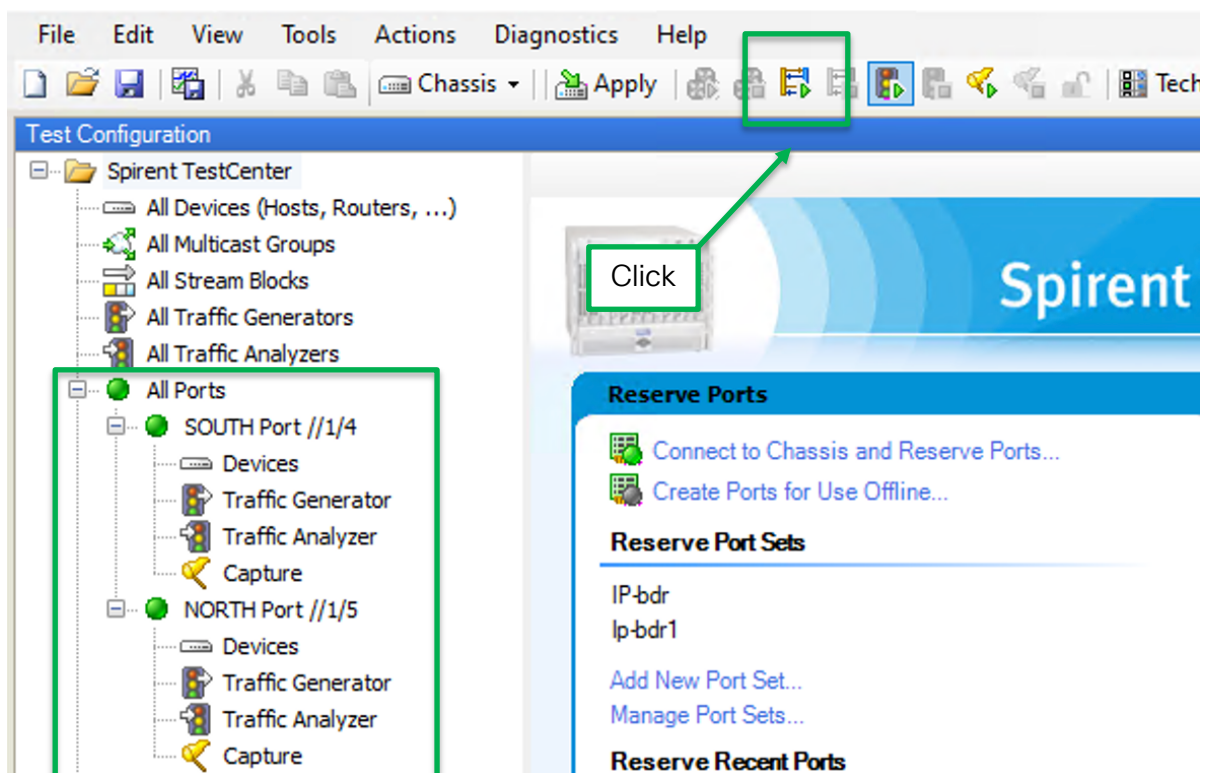
- To start traffic, log into Spirent by clicking the **xFSU** saved file on the RDP desktop.



- Click **Yes**



- Cross check if the two assigned Spirent ports are **online** (green), if yes > Click on the button indicated below to start ARP



Make sure parameters get populated in the **Stream Block Result**

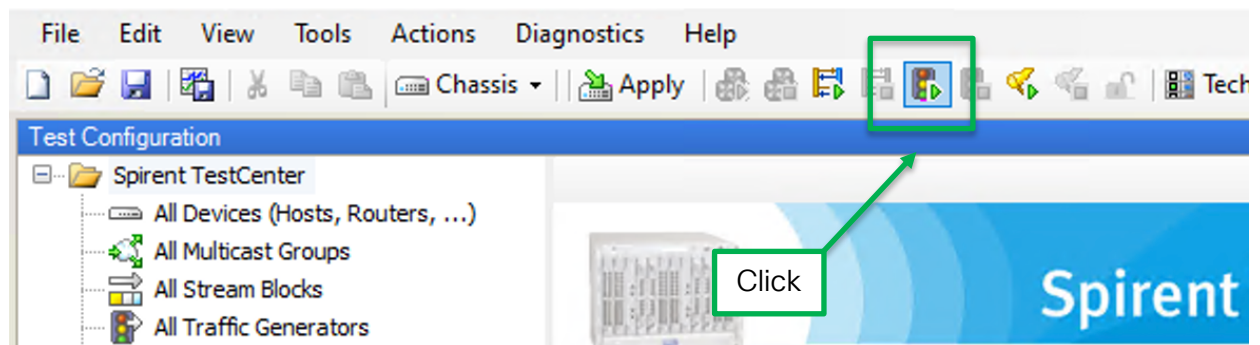
Streams > Stream Block Results | Change Result View | 1 of 1 | Show:

All Ports | Change Counter Mode: Basic Mode

Basic Counters | Errors | Basic Sequencing | Advanced Sequencing | Histograms

	Tx Port Name	Rx Port Names	Stream Block	Tx Count (Frames)	Rx Count (Frames)	Tx Rate (fps)	Rx Rate (fps)
▶	SOUTH Port /...	NORTH Port /...	xFSU-2	0	0	0	0

- Next click on the button indicated below to start traffic on all ports



- Right Click on **Dropped Frame Duration (us)** > **Change Units**

xFSU:Results 1

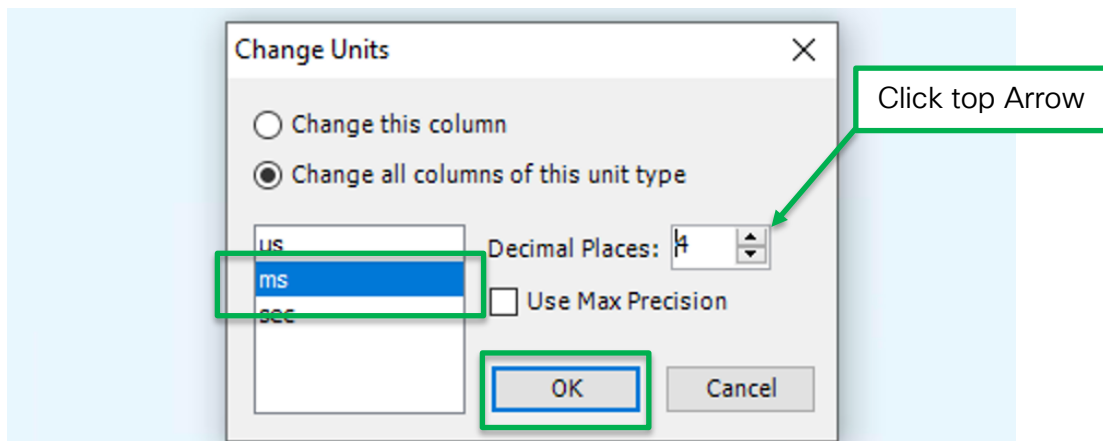
xFSU_Convergence | Change Result View |

StreamBlock Name	Dropped Frame Duration (us)	Port Name	Actual Rx Port Name	Tx Count (Frames)	Rx Count (Frames)

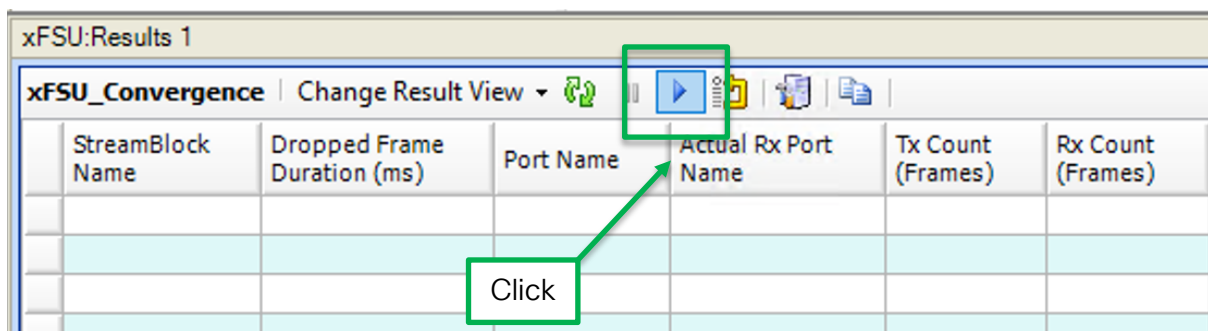
Right Click

Change Units...
 Reset Units
 Reset Layout

- Select **ms (milliseconds)** > Increase decimal place to **4** > Click **OK**



- Next, click on the **play button** to get real time updates on the customized traffic Analyser (xFSU) created for this lab



Make sure frames start transmitting as shown below:

xFSU_Convergence Change Result View						Result Count: 1
StreamBlock Name	Dropped Frame Duration (ms)	Port Name	Actual Rx Port Name	Tx Count (Frames)	Rx Count (Frames)	
xFSU-2	0	SOUTH Port...	NORTH Port //1/5	345,260	345,595	

- Log back into the switch xFSU-C9300-stack
- Enter the below **Extended Fast Software Upgrade** command:
install add file flash:cat9k_iosxe.17.15.03prd2.SPA.bin activate xfsu commit prompt-level none to upgrade the switch to IOS® XE 17.15.3 using the engineering production image stored in the flash.

NOTE: Adding ***prompt-level none*** at the end of the command lets the system automatically proceed through all steps without any manual confirmation after pre-check.

This overall upgrade (Control and Data plane) will take approx.10 mins, do not interrupt the CLI.

```
xFSU-C9300-stack# install add file flash:cat9k_iosxe.17.15.03prd2.SPA.bin activate xfsu commit prompt-level none
```

```
install_add_activate_commit: START Tue Feb 4 02:33:56 UTC 2025
STACK_GR: Inside xFSU check if switch stack
Checking STP eligibility: Eligible
```

```
[1 2]: Performing xFSU-pre-check
300+0 records in
```

xFSU
Precheck:
PASS

[2] Add package(s) on switch 2
[2] Finished Add on switch 2
Checking status of Add on [1 2]
Add: Passed on [1 2]
Finished Add

Extract the Image

Image added. Version: 17.15.03.0.5109
install_add_activate_commit: Activating PACKAGE

Following packages shall be activated:
/flash/cat9k-wlc.17.15.03prd2.SPA.pkg
/flash/cat9k-webui.17.15.03prd2.SPA.pkg
/flash/cat9k-srdriver.17.15.03prd2.SPA.pkg
/flash/cat9k-rpboot.17.15.03prd2.SPA.pkg
/flash/cat9k-rpbase.17.15.03prd2.SPA.pkg
/flash/cat9k-lni.17.15.03prd2.SPA.pkg
/flash/cat9k-guestshell.17.15.03prd2.SPA.pkg
/flash/cat9k-cc_srdriver.17.15.03prd2.SPA.pkg

--- Verifying Platform specific xFSU admission criteria ---
SUCCESS: xFSU image pre-check

--- Starting Activate ---
Performing Activate on all members

Image Precheck: **PASS**

--- Starting list of software package changes ---
Old files list:
Modified cat9k-cc_srdriver.17.15.02.SPA.pkg
Modified cat9k-guestshell.17.15.02.SPA.pkg
Modified cat9k-lni.17.15.02.SPA.pkg
Modified cat9k-rpbase.17.15.02.SPA.pkg
Modified cat9k-rpboot.17.15.02.SPA.pkg
Modified cat9k-srdriver.17.15.02.SPA.pkg
Modified cat9k-webui.17.15.02.SPA.pkg
Modified cat9k-wlc.17.15.02.SPA.pkg


```
--- Starting list of software package changes ---
Old files list:
Modified cat9k-cc_srdriver.17.15.02.SPA.pkg
Modified cat9k-guestshell.17.15.02.SPA.pkg
Modified cat9k-lni.17.15.02.SPA.pkg
Modified cat9k-rpbase.17.15.02.SPA.pkg

Modified cat9k-srdriver.17.15.02.SPA.pkg
Modified cat9k-webui.17.15.02.SPA.pkg
Modified cat9k-wlc.17.15.02.SPA.pkg
New files list:
Added cat9k-cc_srdriver.17.15.03prd2.SPA.pkg
Added cat9k-guestshell.17.15.03prd2.SPA.pkg
Added cat9k-lni.17.15.03prd2.SPA.pkg
Added cat9k-rpbase.17.15.03prd2.SPA.pkg
Added cat9k-rpboot.17.15.03prd2.SPA.pkg
Added cat9k-srdriver.17.15.03prd2.SPA.pkg
Added cat9k-webui.17.15.03prd2.SPA.pkg
Added cat9k-wlc.17.15.03prd2.SPA.pkg
Finished list of software package changes
[2] Finished Activate on switch 2
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate
```

IOS XE 17.15.03 Image is
Activated and **Committed**

```
--- Starting Commit ---
Performing Commit on all members
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
[2] Commit package(s) on switch 2
[2] Finished Commit on switch 2
Checking status of Commit on [1 2]
Commit: Passed on [1 2]
Finished Commit
```


Packages
files contents
verified

[1 2]: Performing Upgrade_Service

```
300+0 records in
300+0 records out
307200 bytes (307 kB, 300 KiB) copied, 0.195626 s, 1.6 MB/s
PID TTY      TIME CMD
SUCCESS: Upgrade_Service finished
STACK_GR: doing the check before writing to chasfs for Starting Stack GR:STACK_GR:
Starting Stack GR:=====
Stage 1/2: Fast reloading Standby/Members
=====
(-2) --- Starting wait for Standby to reach terminal redundancy state ---
PID TTY      TIME CMD
```

```
>
>
>
```

Performing Upgrade Service on Standby Switch

```
>
>
```

```
=====
Stage 2/2: Fast reloading Active(Switchover)
=====
```

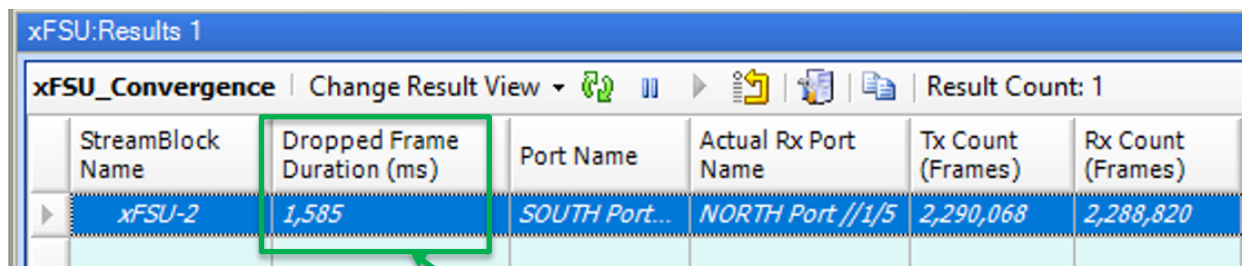
```
Check xFSU support and verification on switch
[1]: xFSU-Verify-Package package(s) on switch 1
Finished preverifying before xFSU
SUCCESS to verify packages
SUCCESS to verify before xFSU
[1]: Finished xFSU-Verify-Package successful on switch 1
(-2) SUCCESS: Finished xFSU-Verify-Package: Success on [1]
```

```
>
>
>
>
>
```

Performing Upgrade Service on Active Switch

Keep an eye on Spirent, to check the traffic convergence during the upgrade!

- Go back to Spirent > Under **Dropped frame duration (ms)** > Take note of the loss



StreamBlock Name	Dropped Frame Duration (ms)	Port Name	Actual Rx Port Name	Tx Count (Frames)	Rx Count (Frames)
xFSU-2	1,585	SOUTH Port...	NORTH Port //1/5	2,290,068	2,288,820

NOTE: From IOS XE 17.15.2 onwards we expect a packet drop duration of less than 5 sec.

- Enter the command **show version / beg SW Version** to display the software version

```
xFSU-C9300-stack# show version / begin SW Version
```

Switch	Ports	Model	SW Version	SW Image	Mode
* 1	41	C9300-24U	17.15.03	CAT9K_IOSXE	INSTALL
2	41	C9300-24UX	17.15.03	CAT9K_IOSXE	INSTALL

- Use the command **show xfsu status** to check the status of the upgrade

```
xFSU-C9300-stack# show xfsu status
```

xFSU PLATFORM Status: **Stack reloaded, all nodes connected**

CONCLUSION: We have successfully upgraded a 9300-stack using xFSU to upgrade from IOS XE 17.15.2 to 17.15.3 , achieving a traffic convergence of under 5 sec.

Additionally, ***Fast Reload*** uses the same mechanism to reload a Catalyst 9300 switch in less than 5 sec of traffic downtime from IOS XE 17.15.2 onwards.

Thank You