Designing Access and Core Switching Architectures with Meraki

Enterprise Cloud managed switching

Brennan Martin
Technical Leader, Enterprise Switching Experiences

BRKENS-1402

Cisco Webex App

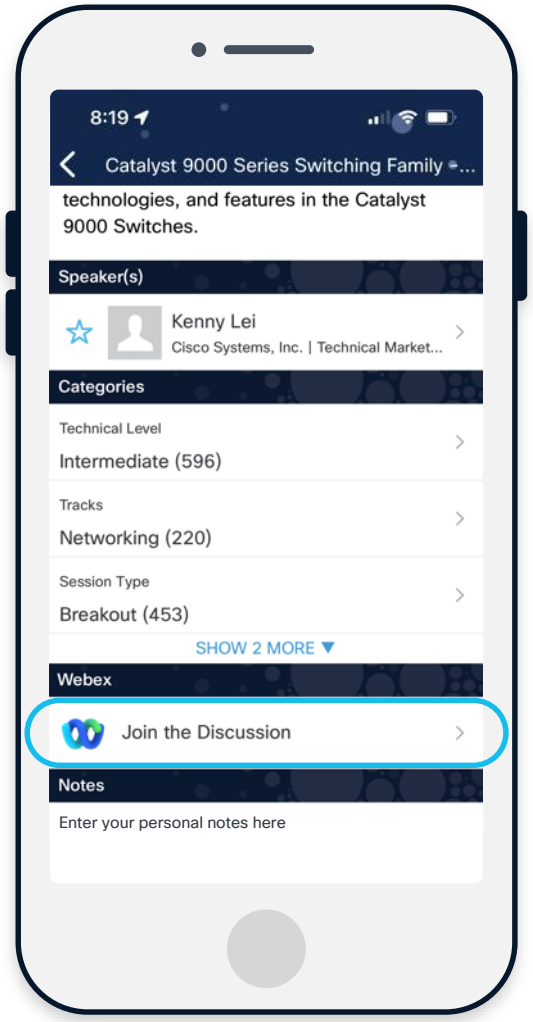
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2025.



Agenda

01 Intro

02 Cloud management with IOS XE

03 Configuration Source

04 Cloud Configuration

05 Platforms

06 Preview: IOS XE 17.18 Cloud switching

07 Enterprise Switching Architectures

I’m a Canadian that loves building networks

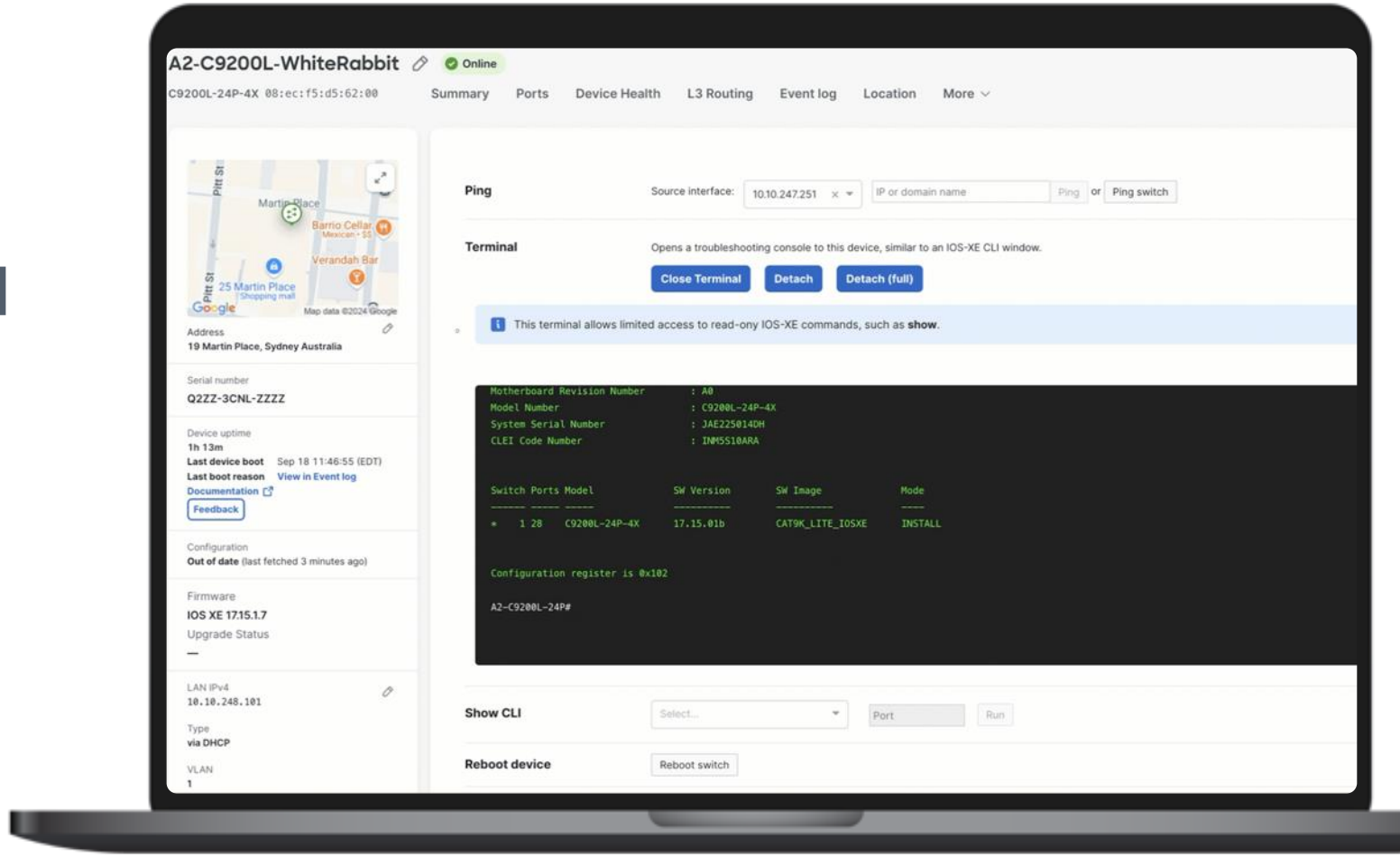
- Based in Saskatoon, Saskatchewan – Canada
- 20+ years building networks
- CCIE R/S #50782
- More time underground than in data centers
- Ask me about potash
- I know the secret to a happy life

Cloud management with IOS XE

We’ve been busy on cloud enablement

IOS XE 17.15 – *50% improvement in config apply and boot times*

- Streamlined Onboarding
- Config on device or cloud
- Cloud CLI
- Support for C9200L



Streamlined Onboarding

```
WW_CORE_9300(config)# service meraki connect

Switch 1 has been successfully registered
Meraki MAC: AABBCCDDEEFF
Cloud ID: QXXX-XXXX-YYYY

*May  7 00:16:03.519: %MERAKI-5-SWITCH_REGISTER_SUCCESS: Switch 1 has been succesfully registered.
*May  7 00:16:03.519: %MERAKI-5-MAC_ADDR: Meraki MAC: AABBCCDDEEFF
*May  7 00:16:03.519: %MERAKI-5-CLOUD_ID: Cloud ID: QXXX-XXXX-YYYY

Device Registration Status:
---------------------------
Switch                Serial                                          Migration
Num    PID            Number           Cloud ID       Mac Address     Status       Mode
-------------------------------------------------------------------------------------
1   C9300-24UX        XXYYQQCCXXC      QXXX-XXXX-YYYY  aabb.ccdd.eeff  Registered   C9K-C [Monitoring]
```

Cloud Management App-less Onboarding

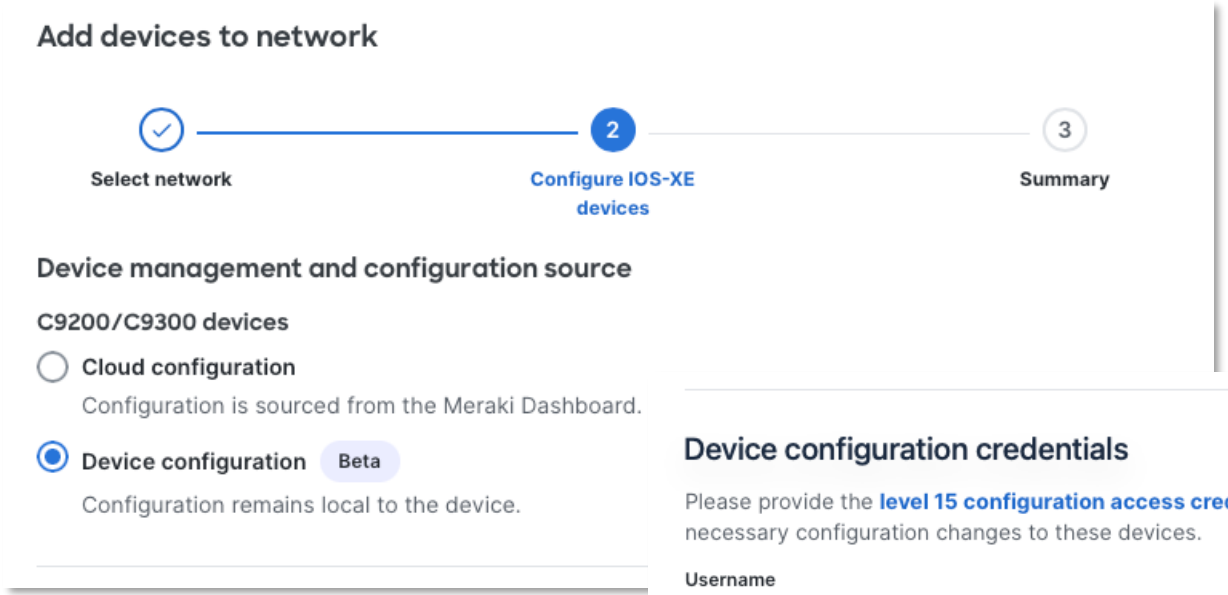
- Automated Registration and Nextunnel creation (`service meraki connect`)
- Simply claim the Cloud ID and add to a network

```
Service meraki connect: enable

Meraki Tunnel Config
---------------------------------
  Fetch State:
  Fetch Fail:
  Last Fetch(UTC):
  Next Fetch(UTC):
  Config Server:
  Primary:                  usw.nt.meraki.com
  Secondary:                use.nt.meraki.com
  Client IPv6 Addr:         FD0A:9B09:1F7:1:9A18:88FF:FE00:CC00
  Network Name:             .Corrin - switch

Meraki Tunnel State
---------------------------------
  Primary:                  Up
  Secondary:                Up
  Primary Last Change(UTC):   2024-05-29 23:34:02
  Secondary Last Change(UTC): 2024-05-29 23:34:02
  Client Last Restart(UTC):   2024-05-29 23:33:56

Meraki Tunnel Interface
---------------------------------
  Status:                   Enable
  Rx Packets:               795767
  Tx Packets:               600246
  Rx Errors:                0
  Tx Errors:                0
  Rx Drop Packets:          0
  Tx Drop Packets:          0

Meraki Device Registration
---------------------------------
  url:                      https://catalyst.meraki.com/nodes/register
```

Connection State (`show meraki connect`)

Streamlined Onboarding

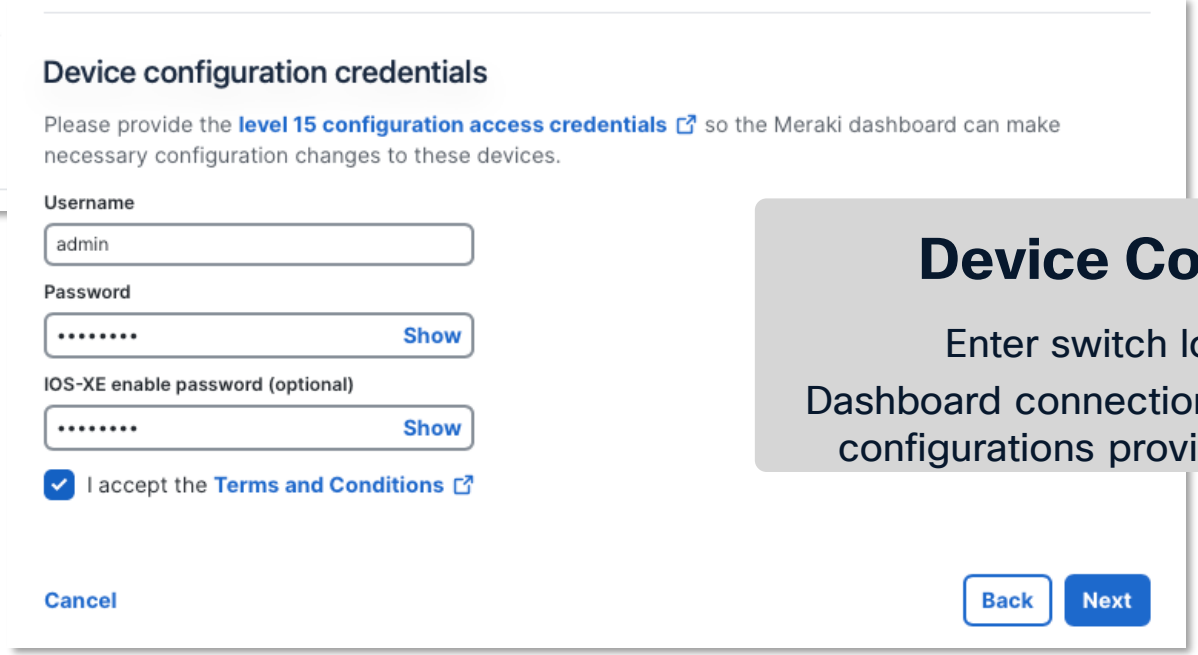
Choose Your Configuration Source When Onboarding



Cloud Configuration

Existing configuration removed

Reload with full cloud configurations synced to IOS XE



Device Configuration

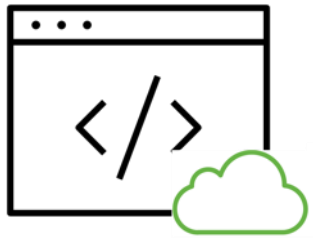
Enter switch local credentials

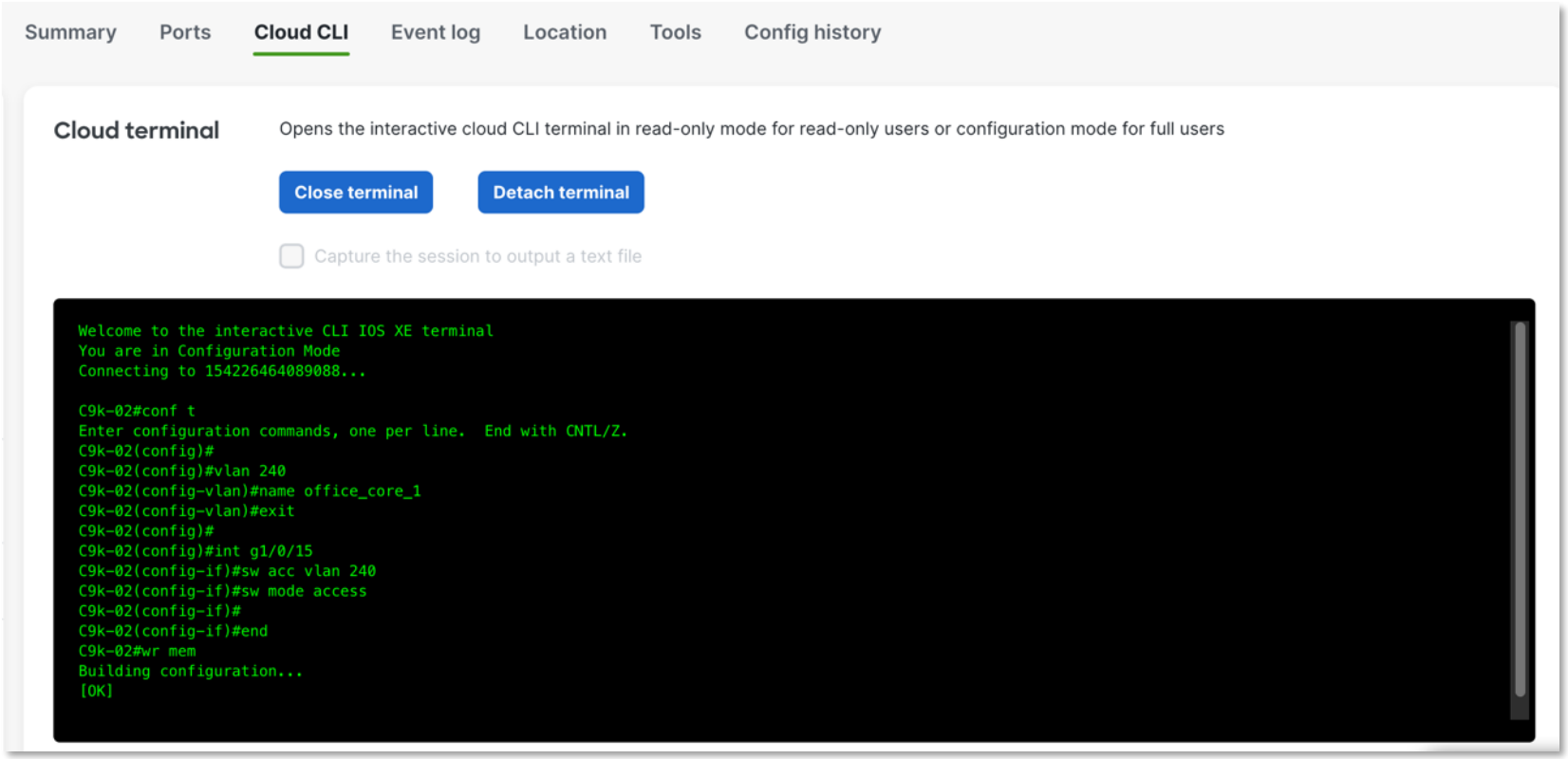
Dashboard connection and telemetry IOS XE configurations provisioned by Dashboard

Cloud CLI for Cloud Managed Catalyst

IOS XE 17.15

Interactive CLI terminal for all cloud managed IOS XE switches



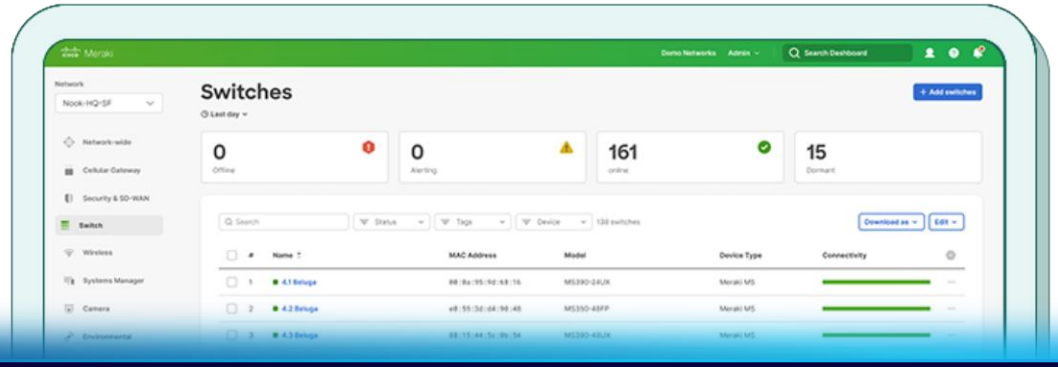


Secure direct terminal with IOS XE Meraki tunnel

CLI access from anywhere

Complete config commands with audit logging

Now supporting 9200L



IOS XE 17.15 – AVAILABLE NOW

C9300L

C9300

C9300 X

C9200L

Configuration Source

Configuration Source

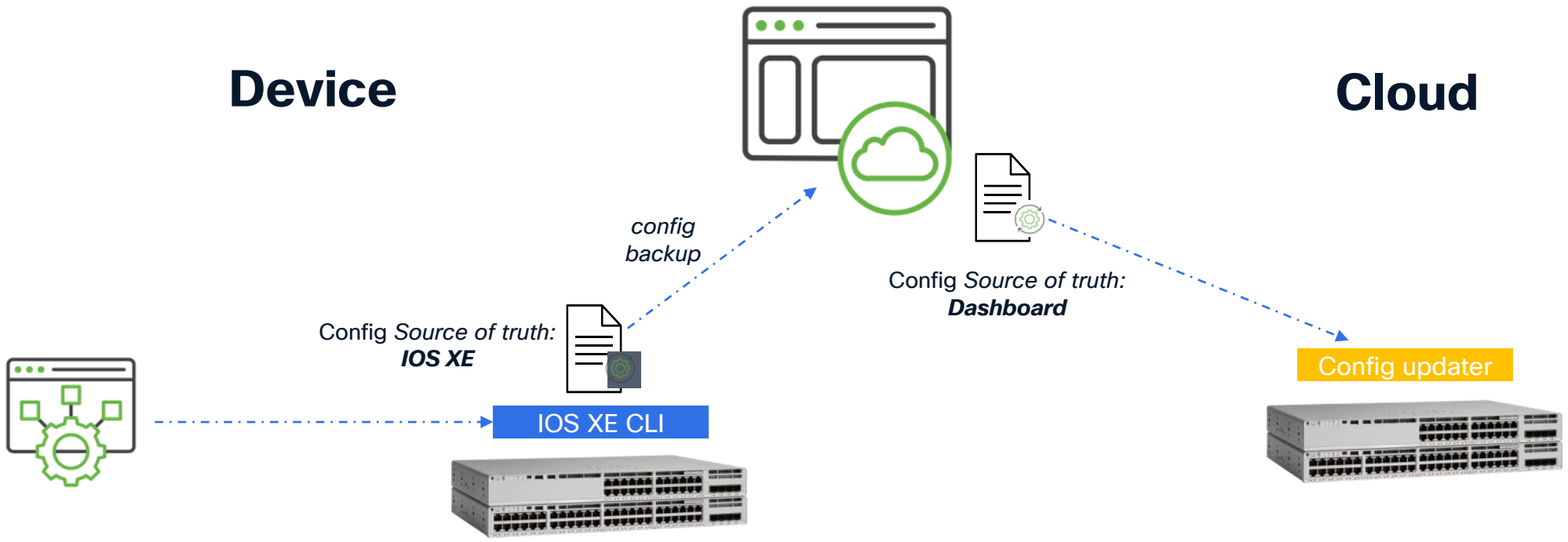
Cloud Configuration

- Exclusively managed by Dashboard
- Config stored in cloud and synced to IOS XE
- Perform configurations with Dashboard UI
- Uplink auto configuration

Device Configuration

- Management flexibility
- Config stored in IOS XE with cloud backup
- Perform configurations with Cloud CLI terminal
- Uplink discovery

Configuration Source



Adopt cloud-managed networking as you evolve your IT operations to cloud

Full cloud-managed for efficient and scalable cloud network operations

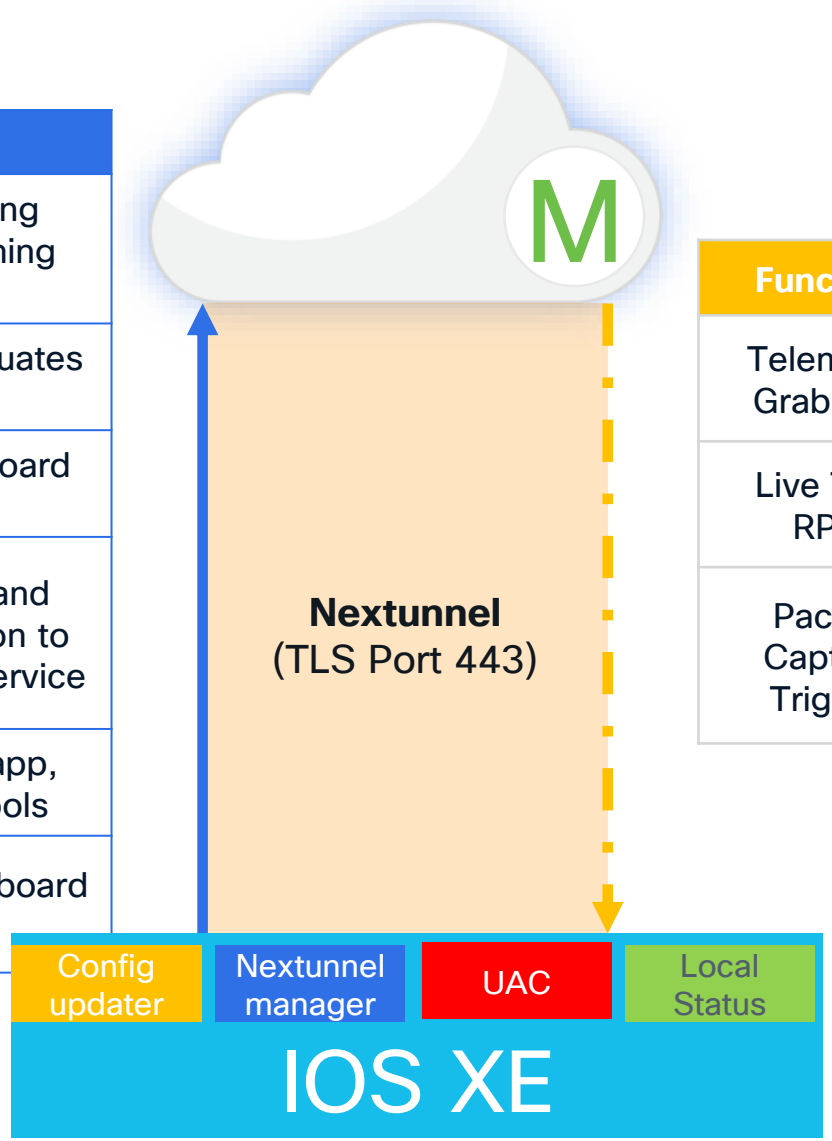
Cloud Configuration

Cloud management with IOS XE

Architecture Advancements

How did we improve the architecture?

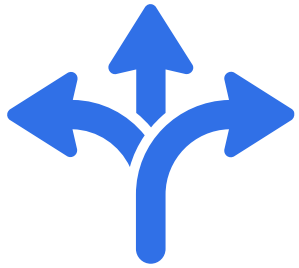
Function	Use
Uplink Auto Configuration (UAC)	Dynamic interface creation using discovery mechanisms maintaining connectivity to dashboard
Connect Service	Checks in to dashboard and evaluates state flags
Packet Capture	Stream packet capture to dashboard browser proxy
Config File DL/UL and deployment	Uploads current configuration and pulls XML formatted configuration to deploy locally against NetConf Service
Local Status Page	Hosted in IOS XE instead of in app, providing local configuration tools
Telemetry Cache	Stores telemetry on box for Dashboard grabbers to retrieve



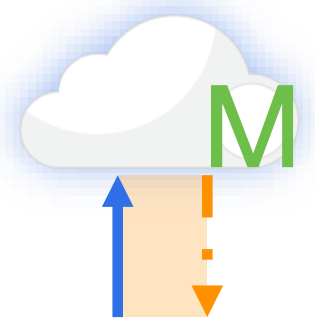
Function	Use
Telemetry Grabbers	Pulls telemetry directly from IOS XE for presentation in Dashboard
Live Tool RPC	Executes Live Tools via NetConf RPC
Packet Capture Trigger	Executes packet capture process using NetConf RPC

Resilient connectivity to the Cloud

Uplink Auto Config (UAC) *Can I reach Dashboard?*



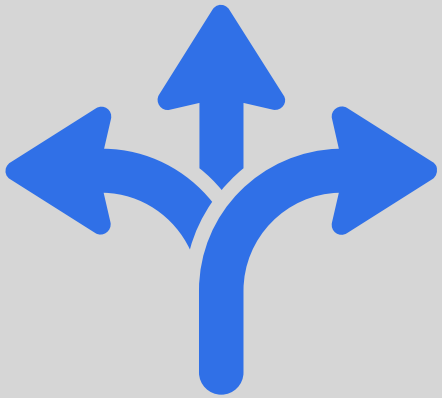
Nextunnel *Connect to Dashboard*



Config Updater Apply and Synchronize Config, Safe config rollback

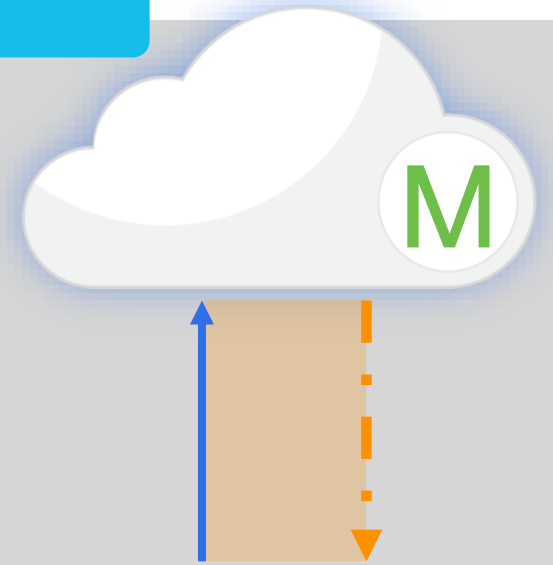
Resilient connectivity to the Cloud

IOS XE 17.15



Uplink Auto Config (UAC)

- Automated discovery for dashboard connectivity
- Automated failover / path discovery
- Tunable for primary interface
- Creates a ranked/scored interface list



Nextunnel

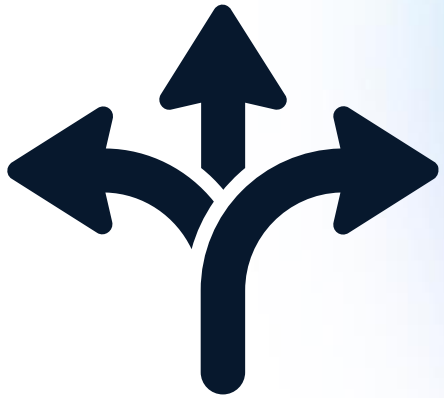
- Secure tunnel to Dashboard for configuration and telemetry

Uplink Auto Config

```
Rocky_and_Bullwinkle#show uac ?
  active-vlan  Active vlans in network
  uplink       Uplink Autoconfig Uplink info
```

show uac

- Which VLANs has UAC discovered?
- Which VLAN has the best score?
- Which SVI is being used to reach Meraki Dashboard?

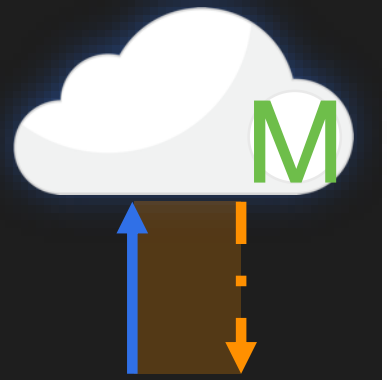


Nextunnel

show meraki connect

- Has the switch fetched tunnel config?
- Is the tunnel up?
- Are packets coming/going?

```
Rocky_and_Bullwinkle#sh meraki connect
Service meraki connect: enable

Meraki Tunnel Config
------------------------------------
  Fetch State:                 Config fetch succeeded
  Fetch Fail:
  Last Fetch(UTC):             2025-01-28 16:25:24
  Next Fetch(UTC):             2025-01-28 17:28:58
  Config Server:               cs46-2037.meraki.com
  Primary:                     usw.nt.meraki.com
  Secondary:                   use.nt.meraki.com
  Client IPv6 Addr:            FD0A:9B09:1F7:1:2E3F:BFF:FE2B:9F80
  Network Name:                Eh2 - switch

Meraki Tunnel State
------------------------------------
  Primary:                     Up
  Secondary:                   Up
  Primary Last Change(UTC):    2025-01-23 19:17:42
  Secondary Last Change(UTC):  2025-01-23 19:17:42
  Client Last Restart(UTC):    2025-01-22 19:25:10

Meraki Tunnel Interface
------------------------------------
  Status:                      Enable
  Rx Packets:                  22355237
  Tx Packets:                  35429584
  Rx Errors:                   0
  Tx Errors:                   0
  Rx Drop Packets:             0
  Tx Drop Packets:             0

Meraki Device Registration
------------------------------------
  url:                         https://catalyst.meraki.com/nodes/register
```



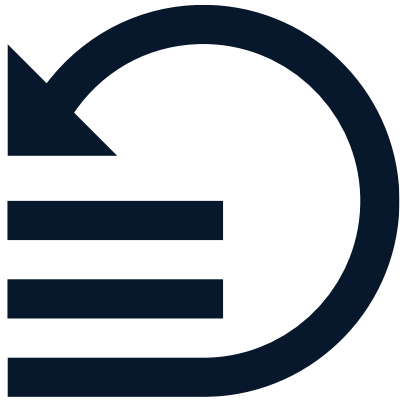
Resilient connectivity to the Cloud

IOS XE 17.15

Config Updater

- Fetch and apply config from Dashboard
- Safe configuration rollback: 30 minute recovery mechanism for configuration error

Config Updater

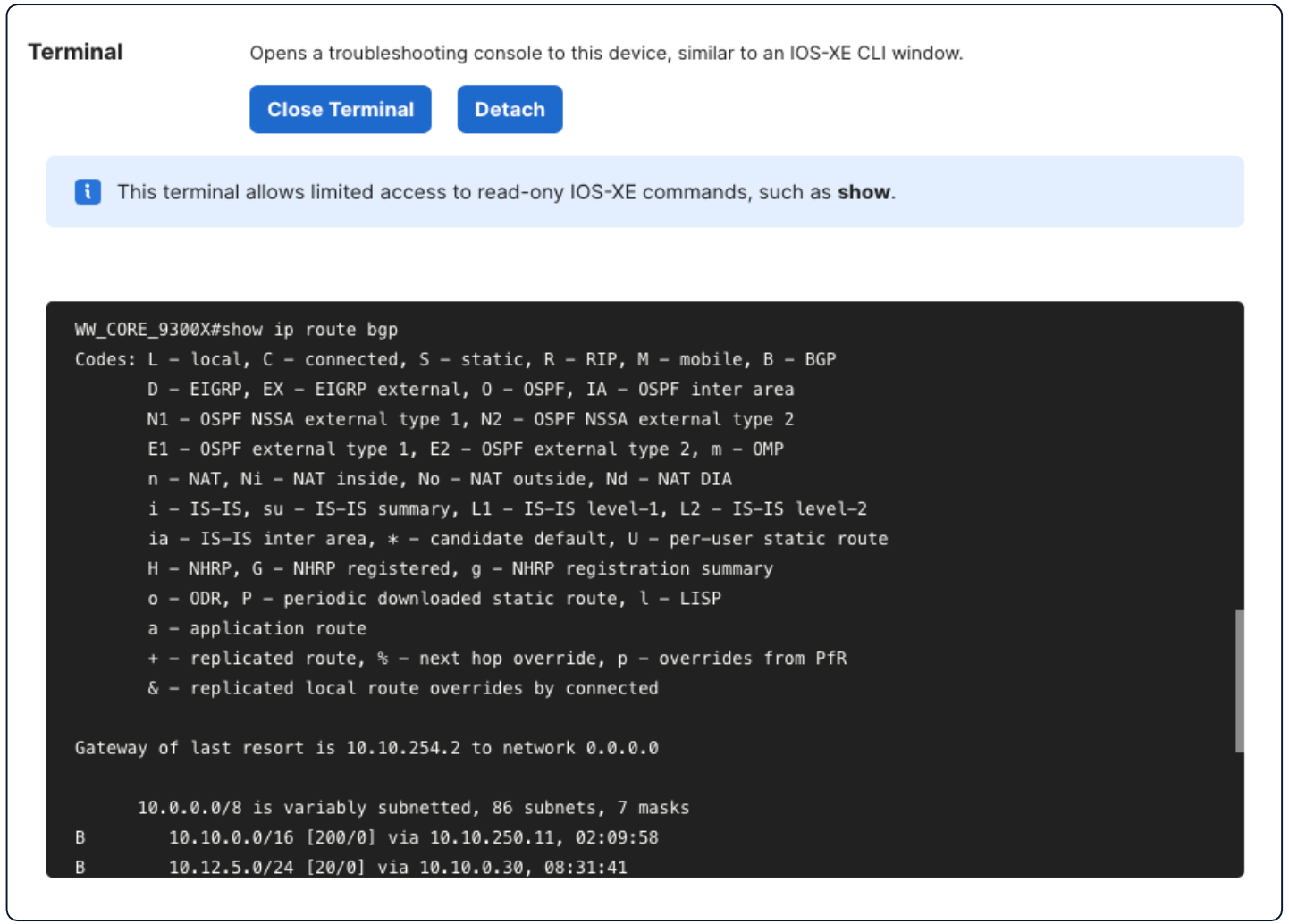


show meraki config updater

- Can the switch fetch config?
- Can the switch upload the config?
- Does the switch need to upload config?

```
Rocky_and_Bullwinkle#sh meraki config updater
Config Updater
-----------------------------------
  Current state:                Ready

Latest operation
-----------------------------------
  Upload running config

  Get running config: Pass
    start time(UTC): 2025-01-29 22:22:15
    result time(UTC): 2025-01-29 22:22:33
    Running config location: /flash/meraki/config_updater/monitor/upload.config
  Get presigned url: Not needed
    start time(UTC): 2025-01-29 22:22:33
    result time(UTC): 2025-01-29 22:22:36
    dashboard status code: 204
  Upload config: Not started
```

Demo: Cloud CLI



Optimizations

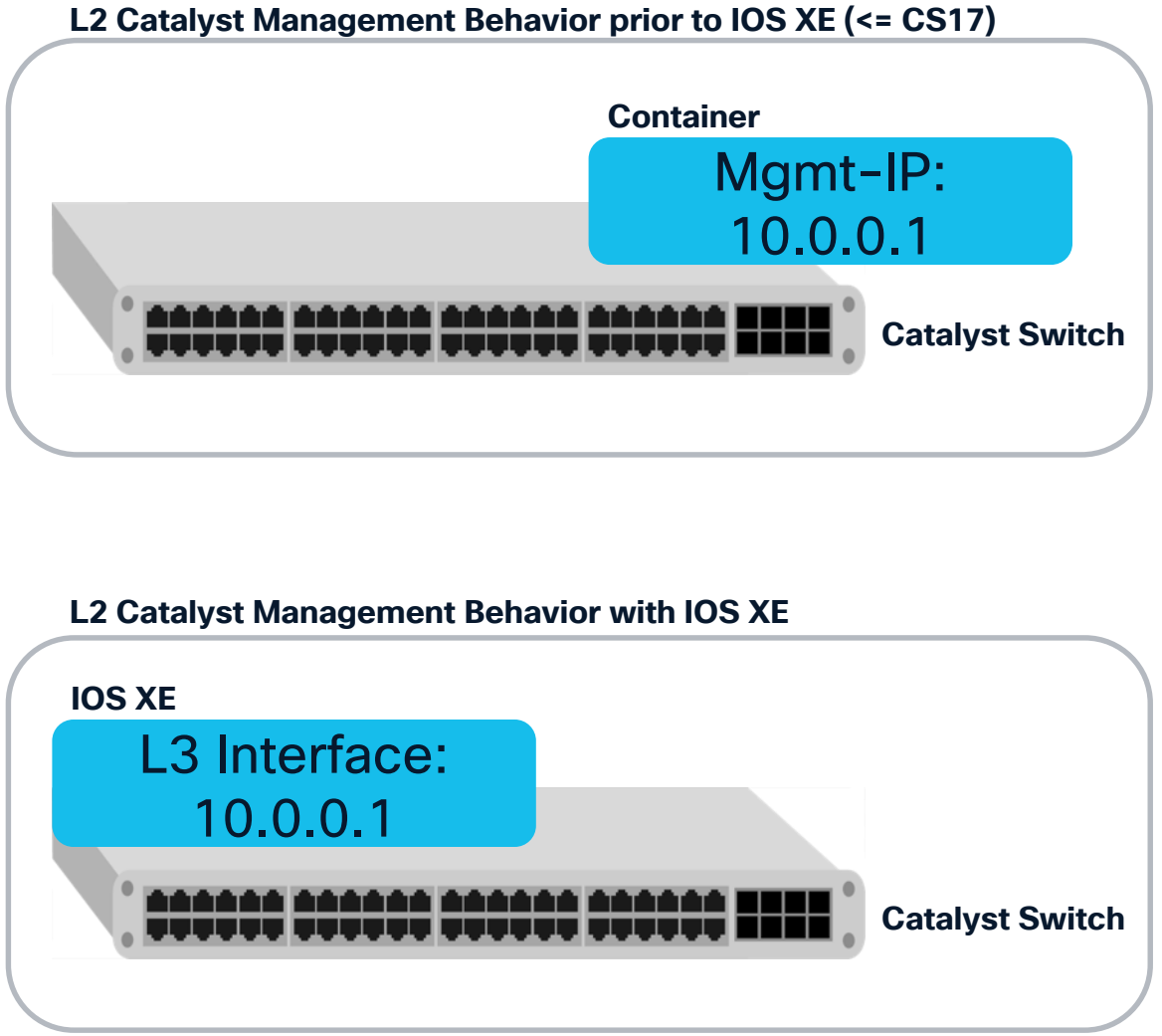
Management Interface Architecture Change

Default Network Module

Command Runner

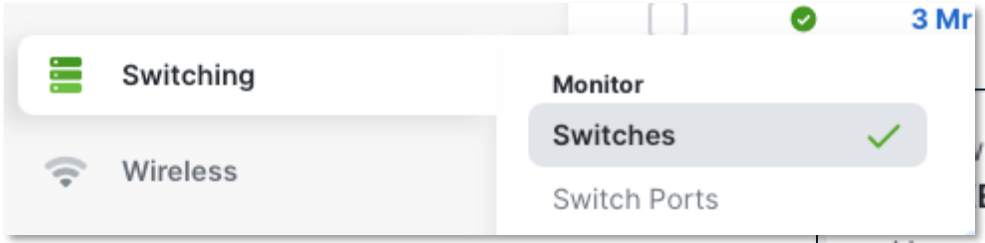
Management Interface Architecture Change

- The management interface is now an L3 Interface. Switches running CS firmware required a dedicated management IP address, now management is handled by **any L3 interface**
- All configuration for management connectivity and L3 interfaces is now available on the Routing & DHCP page.
- If a switch is L2 only, DHCP will work 👍 but enabling L3 requires first setting a static management IP

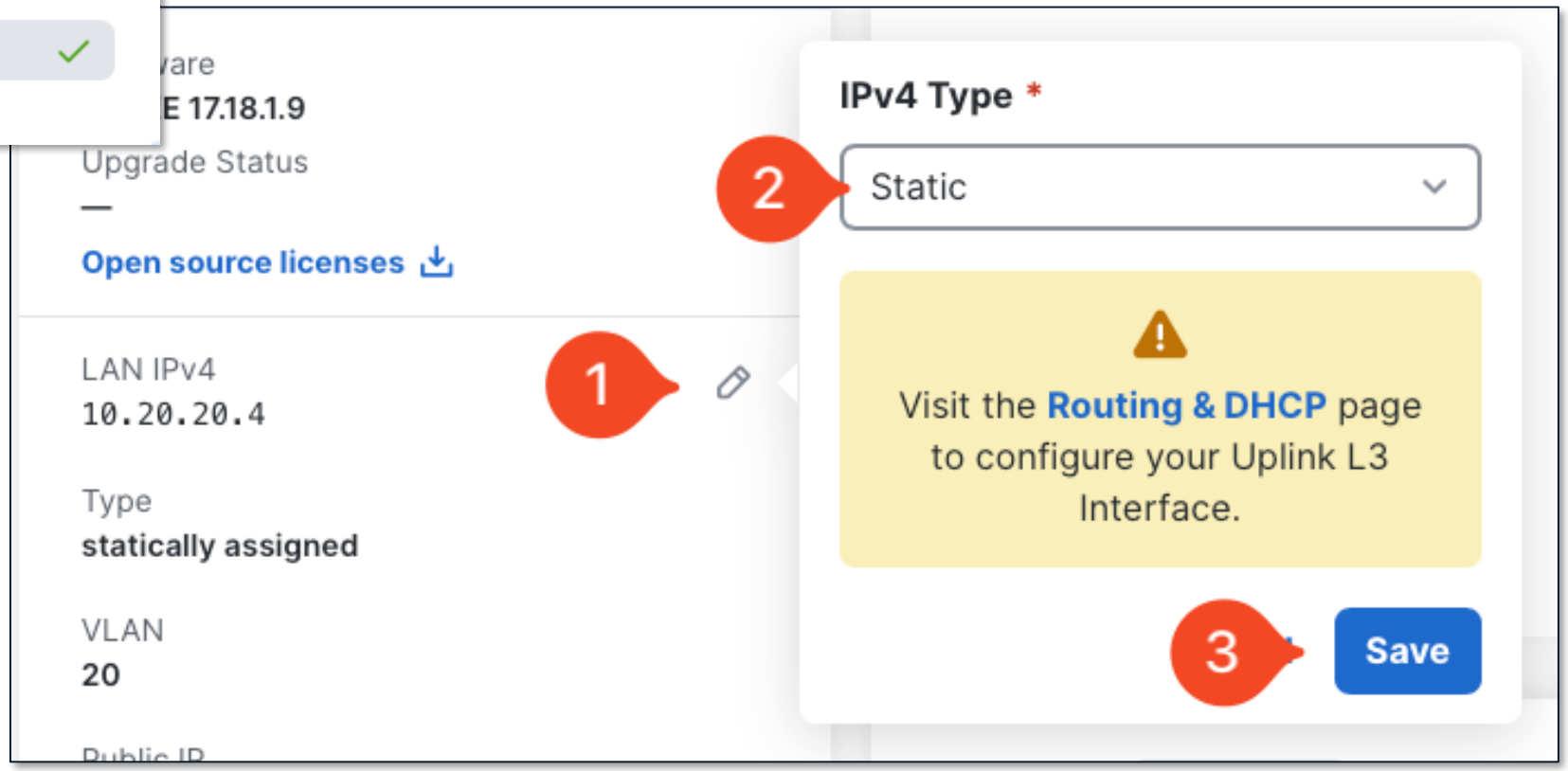


Management Interface Architecture Change

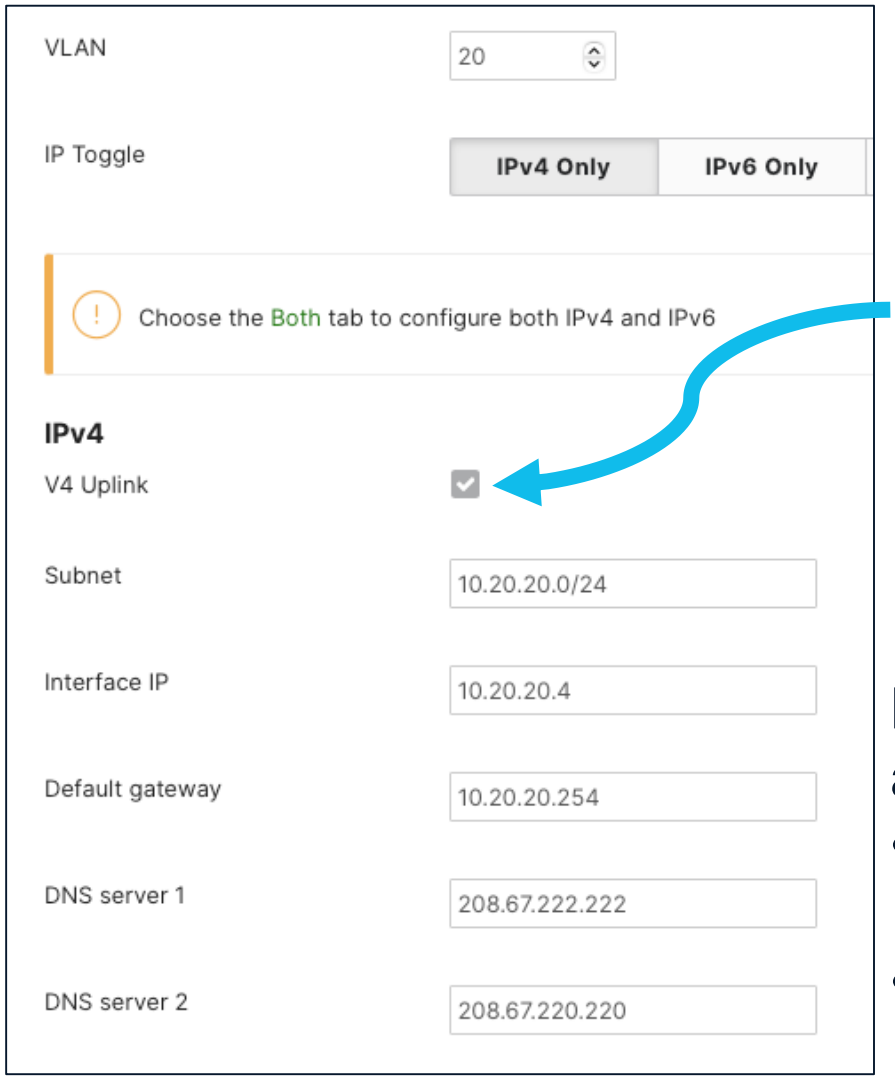
Switch Summary page>



1. Edit IP config
2. Change Type to Static
3. Redirect to Routing & DHCP page



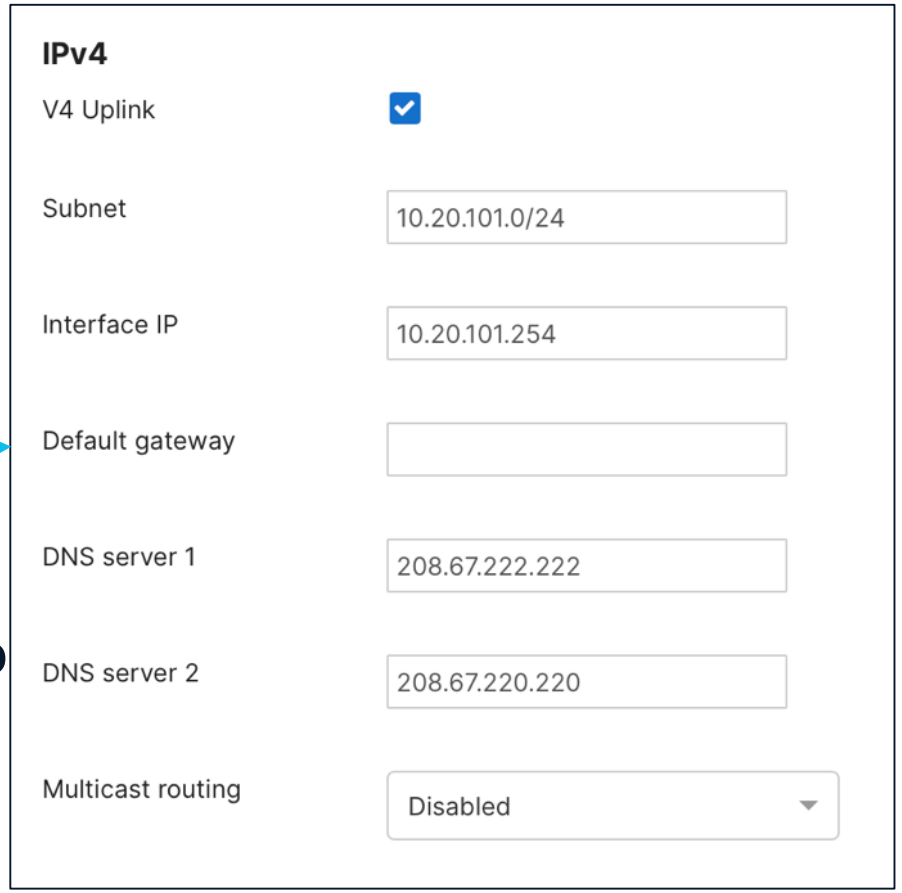
Management Interface Architecture Change



Uplink interfaces include DNS and Default Gateway settings

Easily move the uplink to a different interface

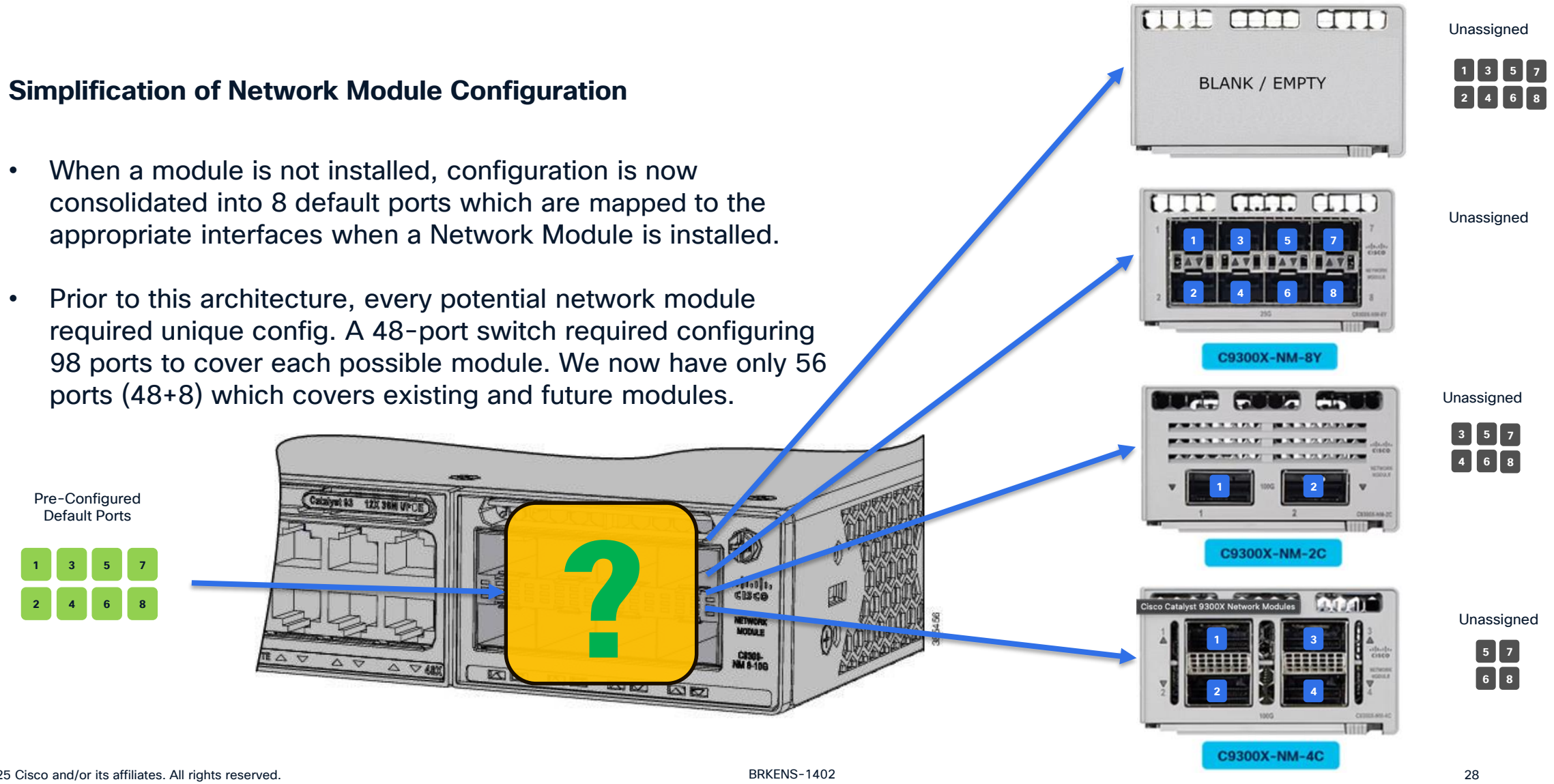
- Define the new gateway
- Confirm DNS



Default Network Module

Simplification of Network Module Configuration

- When a module is not installed, configuration is now consolidated into 8 default ports which are mapped to the appropriate interfaces when a Network Module is installed.
- Prior to this architecture, every potential network module required unique config. A 48-port switch required configuring 98 ports to cover each possible module. We now have only 56 ports (48+8) which covers existing and future modules.



Default Network Module

The CS way:

- Which module is installed?
- Is any module installed?

C9300-NM-4G

C9300X-NM-8Y

C9300X-NM-2C

- STACK-MS390-RR / 4×10G / 1 details
- STACK-MS390-RR / 4×10G / 2 details
- STACK-MS390-RR / 4×10G / 3 details
- STACK-MS390-RR / 4×10G / 4 details
- STACK-MS390-RR / 8×10G / 1 details
- STACK-MS390-RR / 8×10G / 2 details
- STACK-MS390-RR / 8×10G / 3 details
- STACK-MS390-RR / 8×10G / 4 details
- STACK-MS390-RR / 8×10G / 5 details
- STACK-MS390-RR / 8×10G / 6 details
- STACK-MS390-RR / 8×10G / 7 details
- STACK-MS390-RR / 8×10G / 8 details
- STACK-MS390-RR / 2×40G / 1 details
- STACK-MS390-RR / 2×40G / 2 details

Default Network Module

The IOS XE 17.15.2+ way:

- Bullwinkle / DEFAULT / 1 details
- Bullwinkle / DEFAULT / 2 details
- Bullwinkle / DEFAULT / 3 details
- Bullwinkle / DEFAULT / 4 details
- Bullwinkle / DEFAULT / 5 details
- Bullwinkle / DEFAULT / 6 details
- Bullwinkle / DEFAULT / 7 details
- Bullwinkle / DEFAULT / 8 details

No module installed

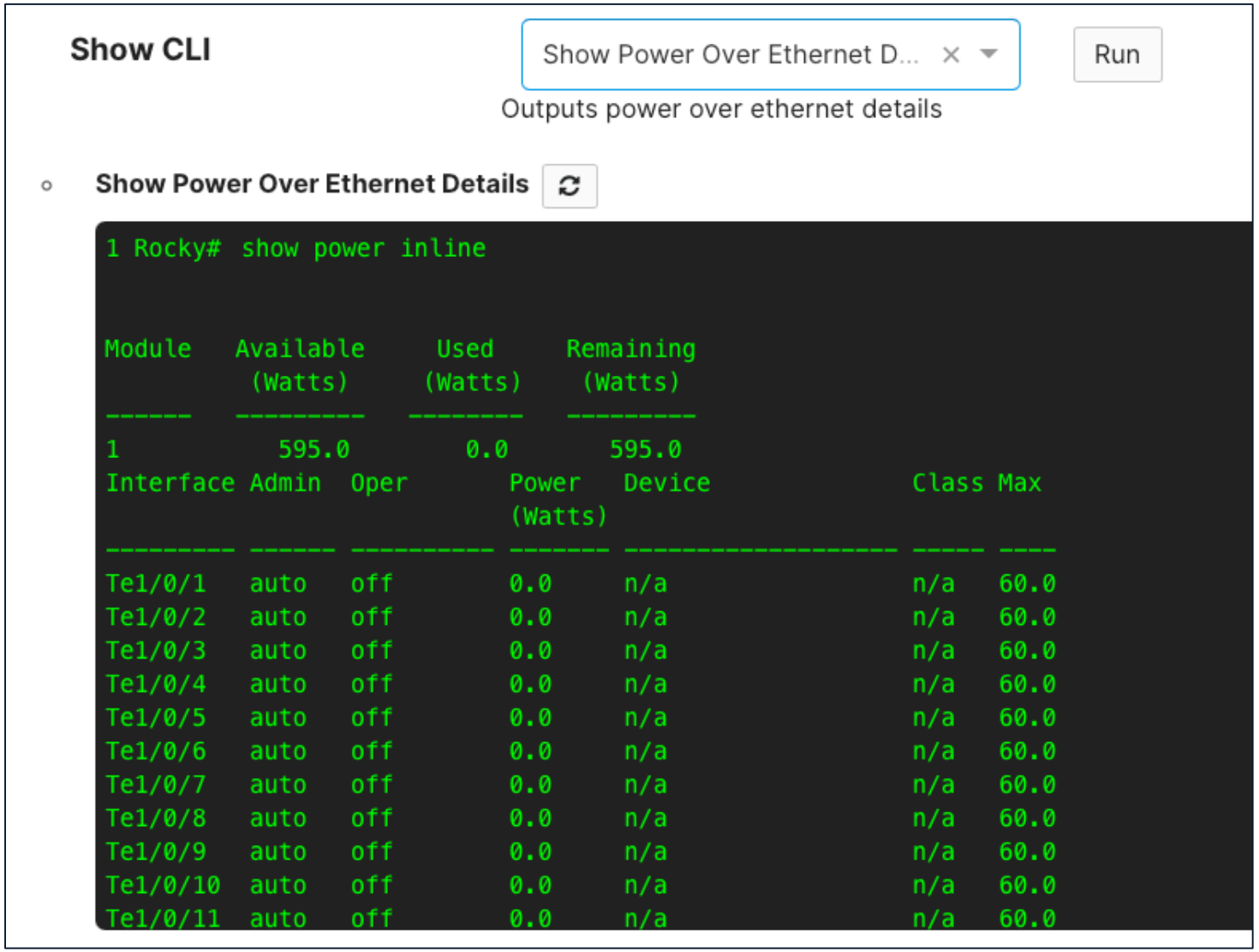
8x10G installed

- Mr Peabody / 8×10G / 1 details
- Mr Peabody / 8×10G / 2 details
- Mr Peabody / 8×10G / 3 details
- Mr Peabody / 8×10G / 4 details
- Mr Peabody / 8×10G / 5 details
- Mr Peabody / 8×10G / 6 details
- Mr Peabody / 8×10G / 7 details
- Mr Peabody / 8×10G / 8 details

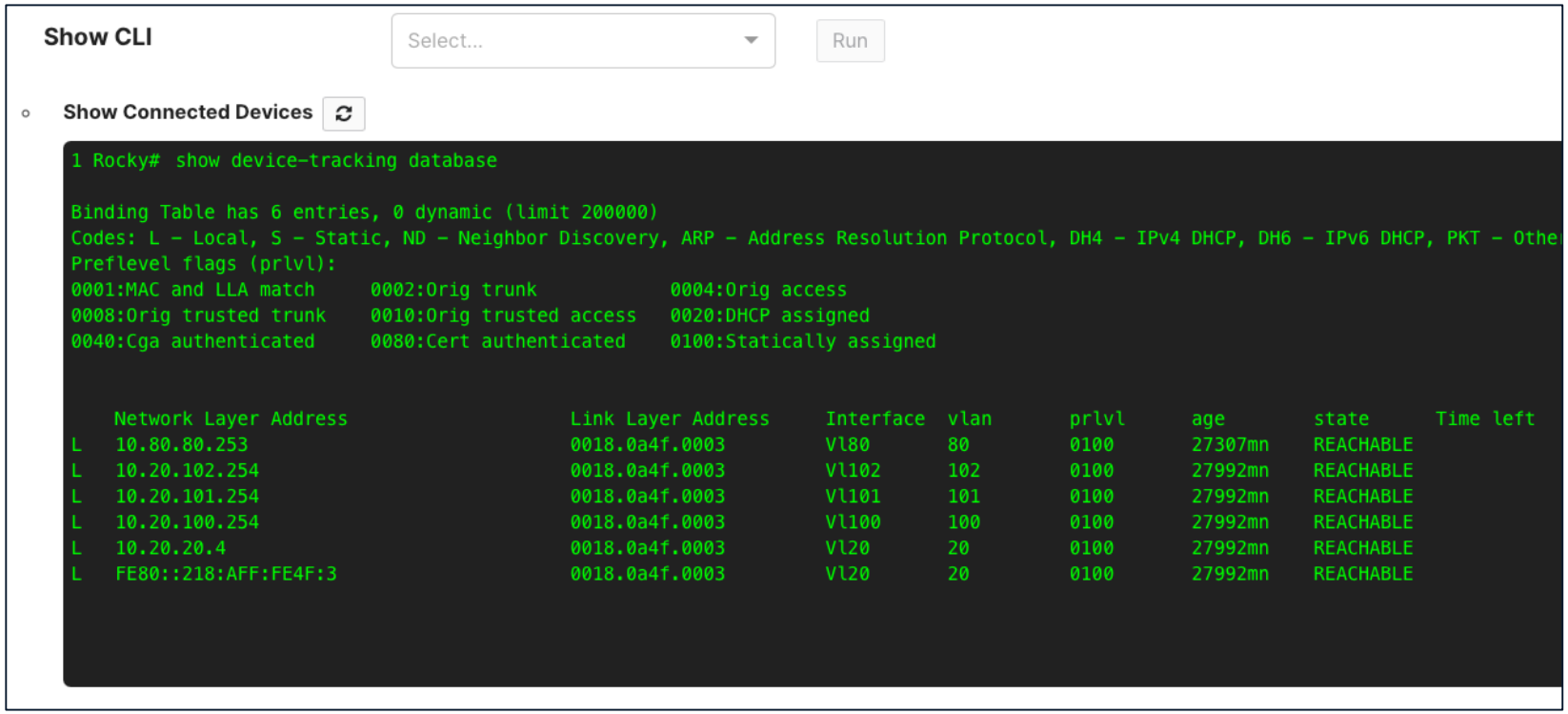
Show CLI / Command runner

Quick access to over 30 common CLI outputs

- Platform monitoring
- Device tracking
- Stacking details
- Dashboard connection status
- Etc…



Demo: Command Runner



Platforms

A next-gen model for every network need

MS17

IOS XE 17.15

Access

Enhanced PoE and Stacking

NEW

MS130/R

IP30

30W PoE+

2.5 GbE

10 GbE SFP+

MS150

80 Gbps stacking

60W PoE++ (802.3bt)

C9200L

All Models

80 Gbps stacking

30W PoE+

C9300L-M

320 Gbps stacking

60W UPOE+ (802.3bt)

C9300-M

480 Gbps stacking + StackPower 60W UPOE+ (802.3bt)

C9300X-M

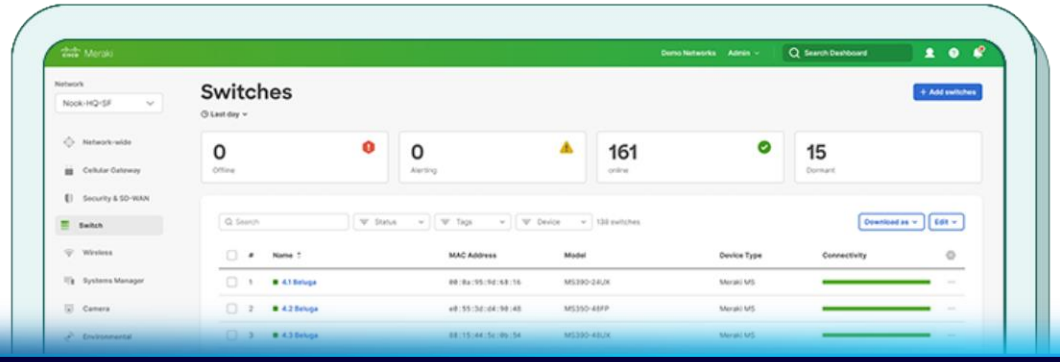
1Tbps stacking + StackPower 90W UPOE+ (802.3bt)

C9300/X-M

480 Gbps /1Tbps stacking + StackPower

Common policy | Scalable segmentation | End-to-end network management | Zero-touch provisioning

Unlocking the full C9000 Portfolio



Preview: Extend secure connectivity to rugged outdoor networks
Targeting Spring 2026

IE3500*

IOS XE 17.15 – AVAILABLE NOW

C9300L

C9300

C9300X

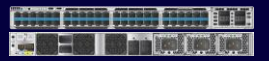
C9200L

IOS XE 17.18

C9500

C9200/CX

C9300LM



C9350

Every C9200 and C9300 model

Preview: IOS XE 17.18 Cloud switching

beta summer 2025

Cloud Managed Enterprise Switching on IOS XE 17.18

Enterprise Feature Development

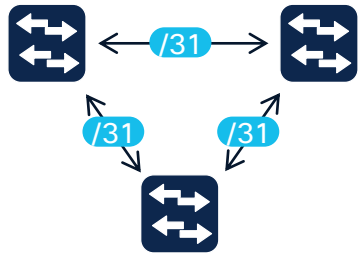
Advanced Routing

Routed Ports	Loop-free Routed Access
VRF Lite	Scalable Macro Segmentation
BGP	Flexible, Open Dynamic Routing

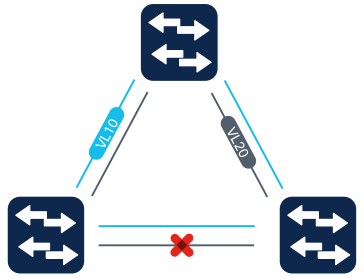
High-Availability

Rapid PVST+	Enhanced L2 Loop Prevention
StackWise Virtual (SVL) ISSU	Sub-second downtime firmware upgrades

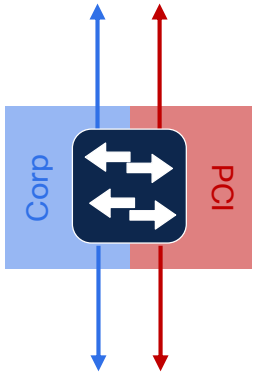
Routed Ports



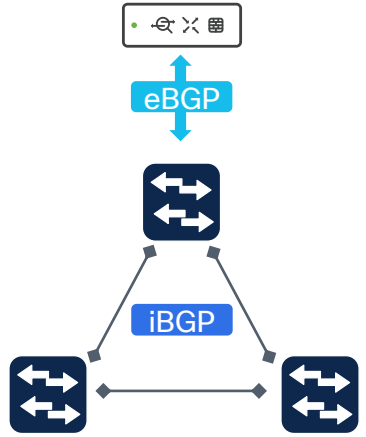
RPVST+



VRF Lite



BGP



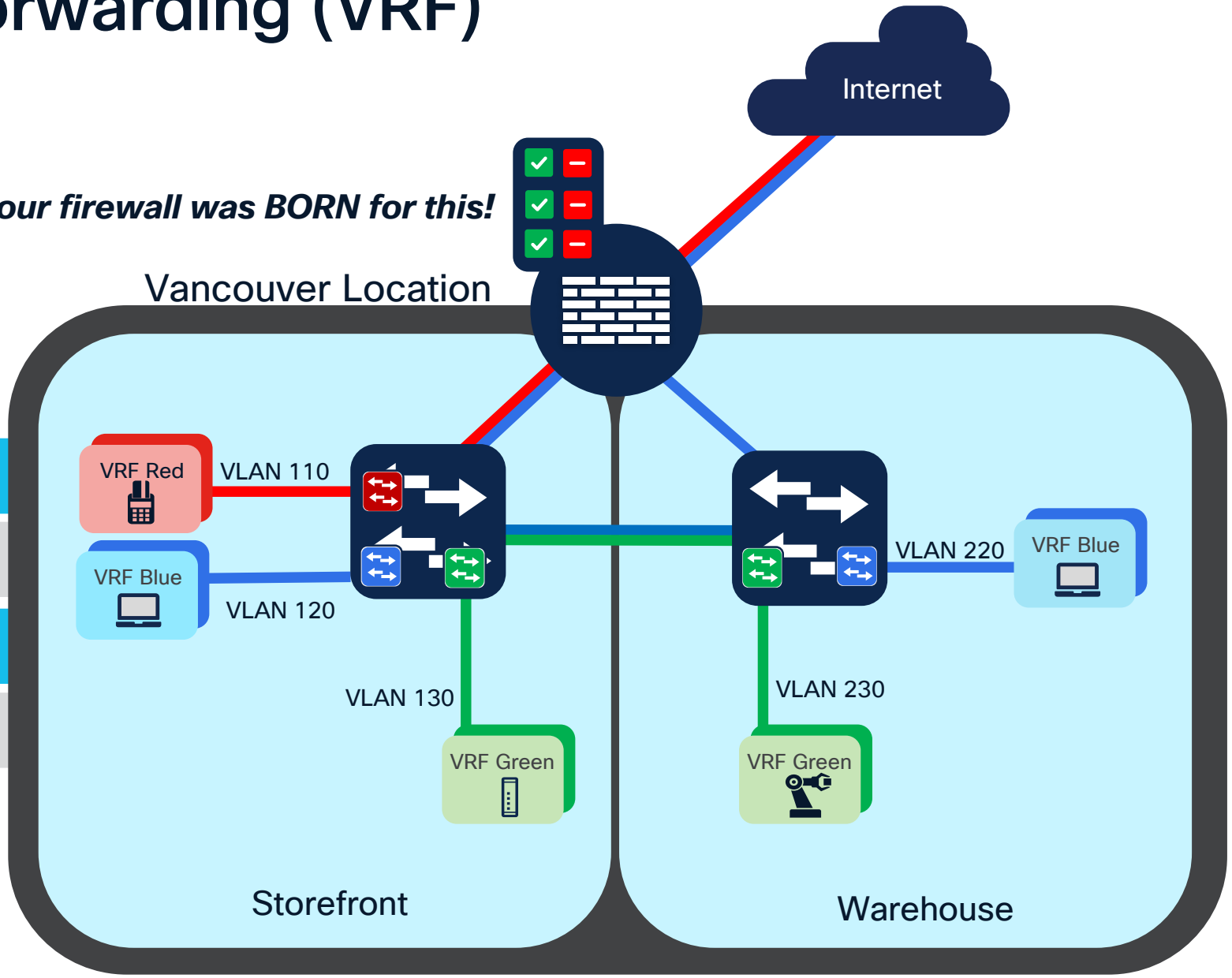
Virtual Routing and Forwarding (VRF)

Macro-segmentation that scales

Centralized ACLs

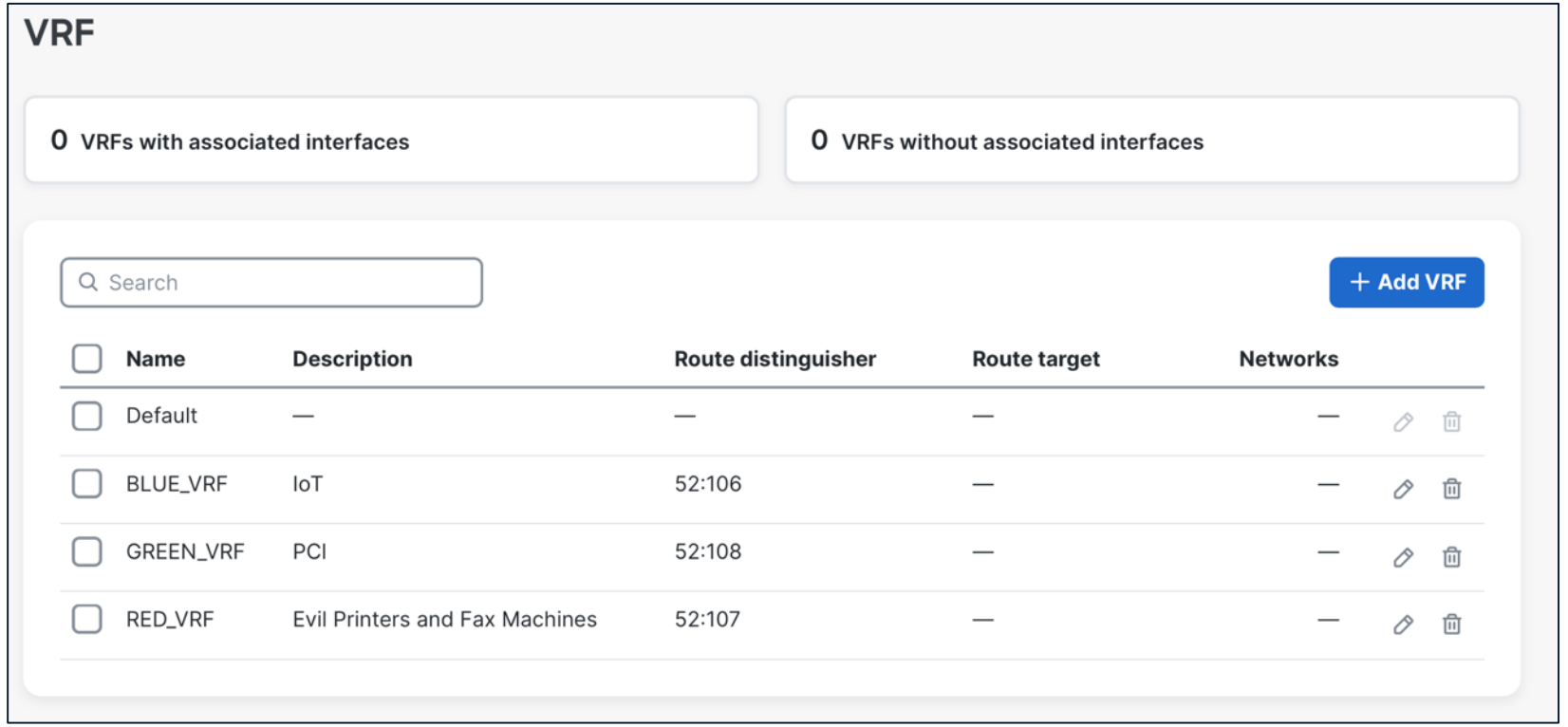
Efficient route handling and forwarding

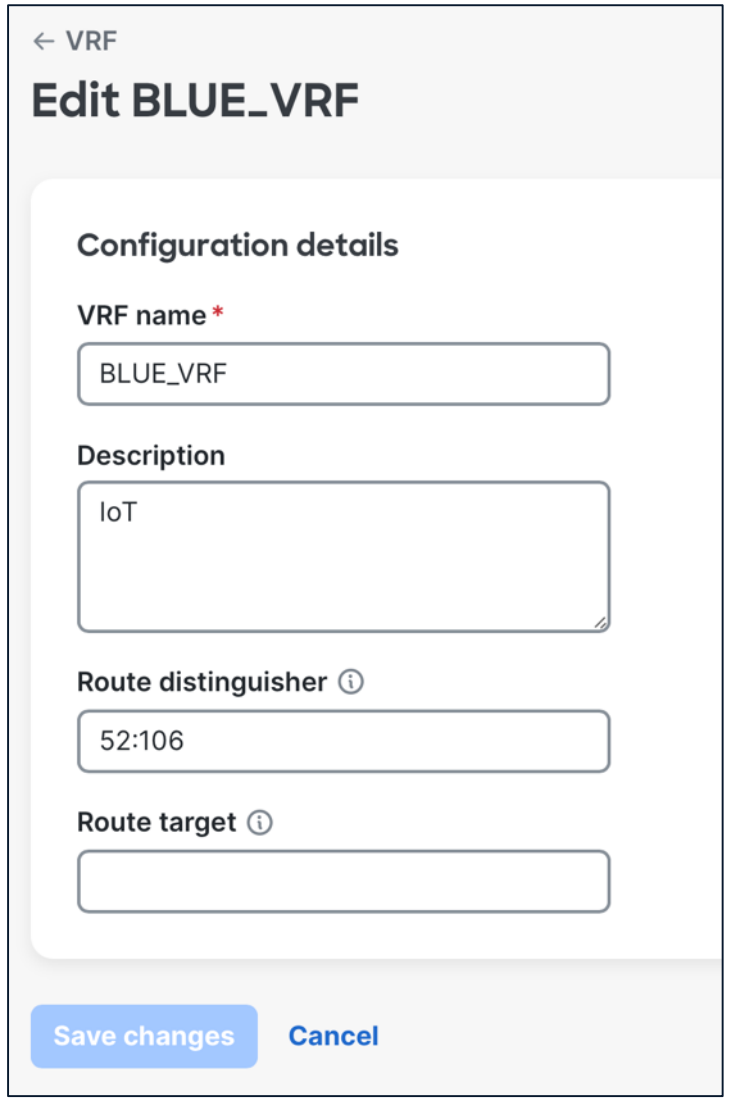
A separate lane for management traffic



VRF Config

Organization > VRFs



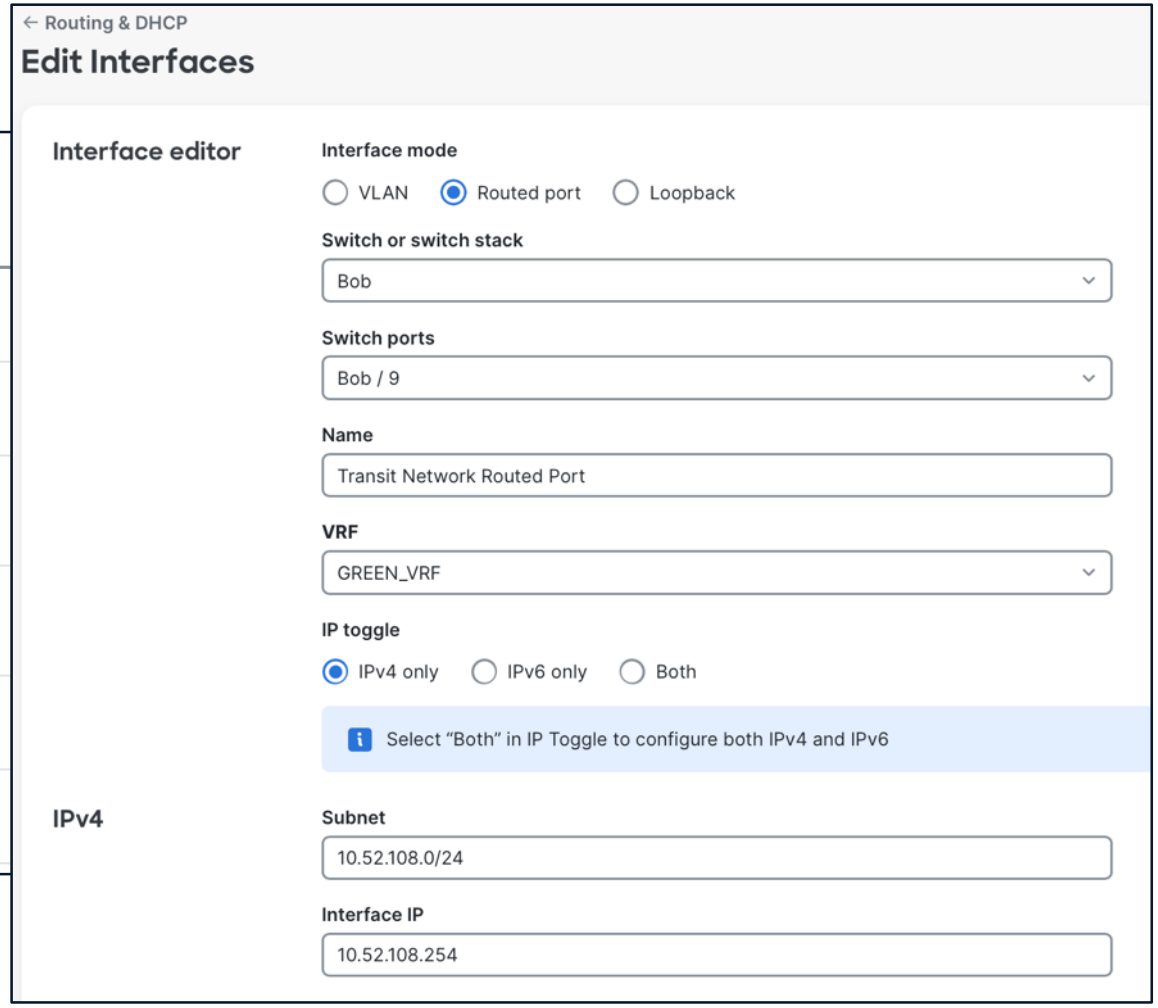


- Create VRFs at an organization-level
- Assign a name, and Route Distinguisher

VRF Config

Switching > Routing & DHCP

Switch or switch stack	Interface	Name	VRF	Subnet
Doug	80 VLAN	eighty	BLUE_VRF	10.80.80.0/24
Rocky_and_Bullwinkle	80 VLAN	BLUE VLAN 80	BLUE_VRF	10.80.80.0/24
Bob	Bob / 13 Routed	Bobs routed port	BLUE_VRF	10.88.88.0/24
Bob	Bob / 14 Routed	Bobs 2nd routed port	BLUE_VRF	10.89.89.0/24
Doug	0 Loop	0	BLUE_VRF	10.252.252.252/32
Doug	20 VLAN	Uplink Vlan 20	Default	10.20.20.0/24



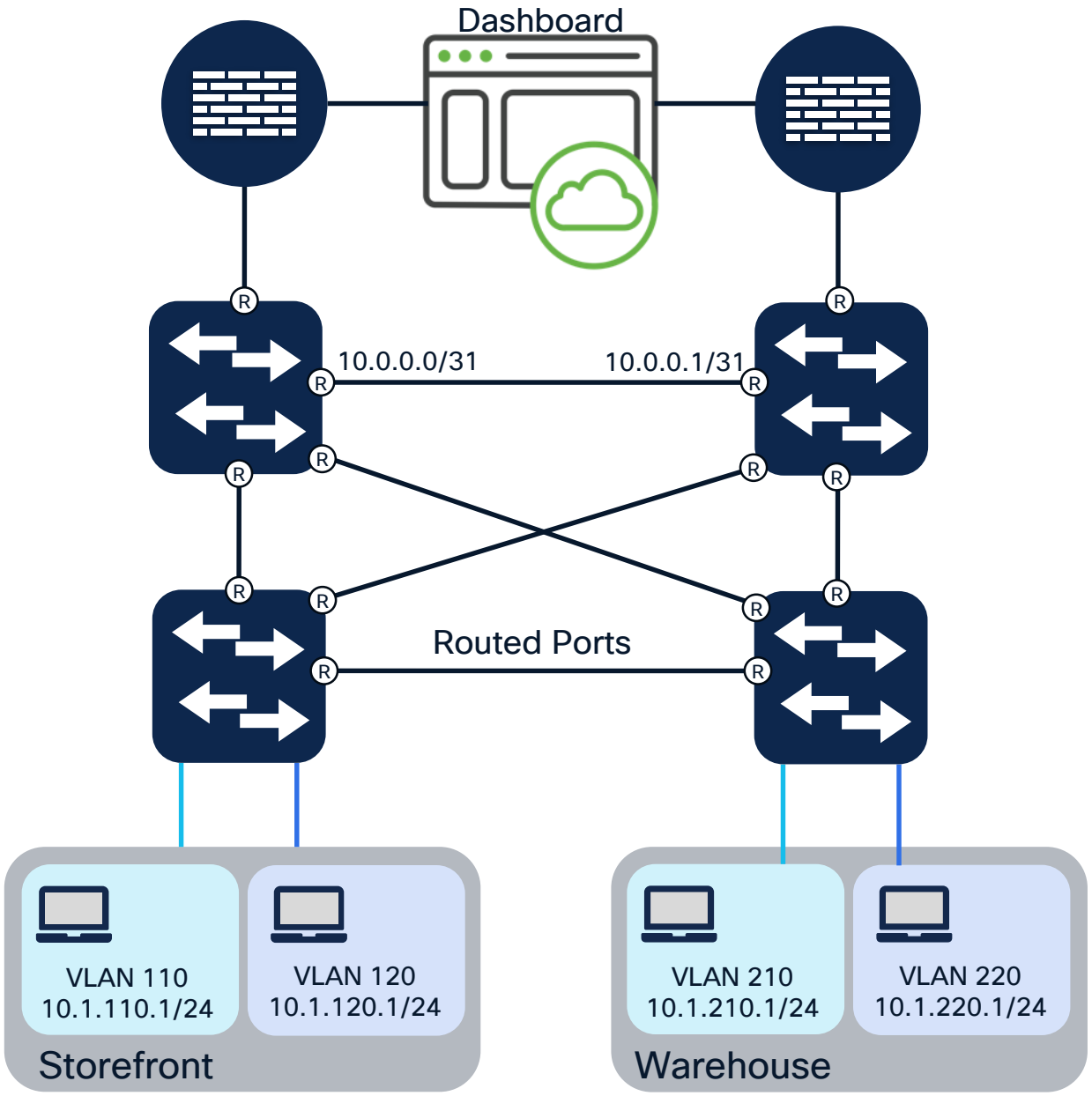
- Assign interfaces to a VRFs

Routed Ports

Routed peer to peer links

East/West and North/South

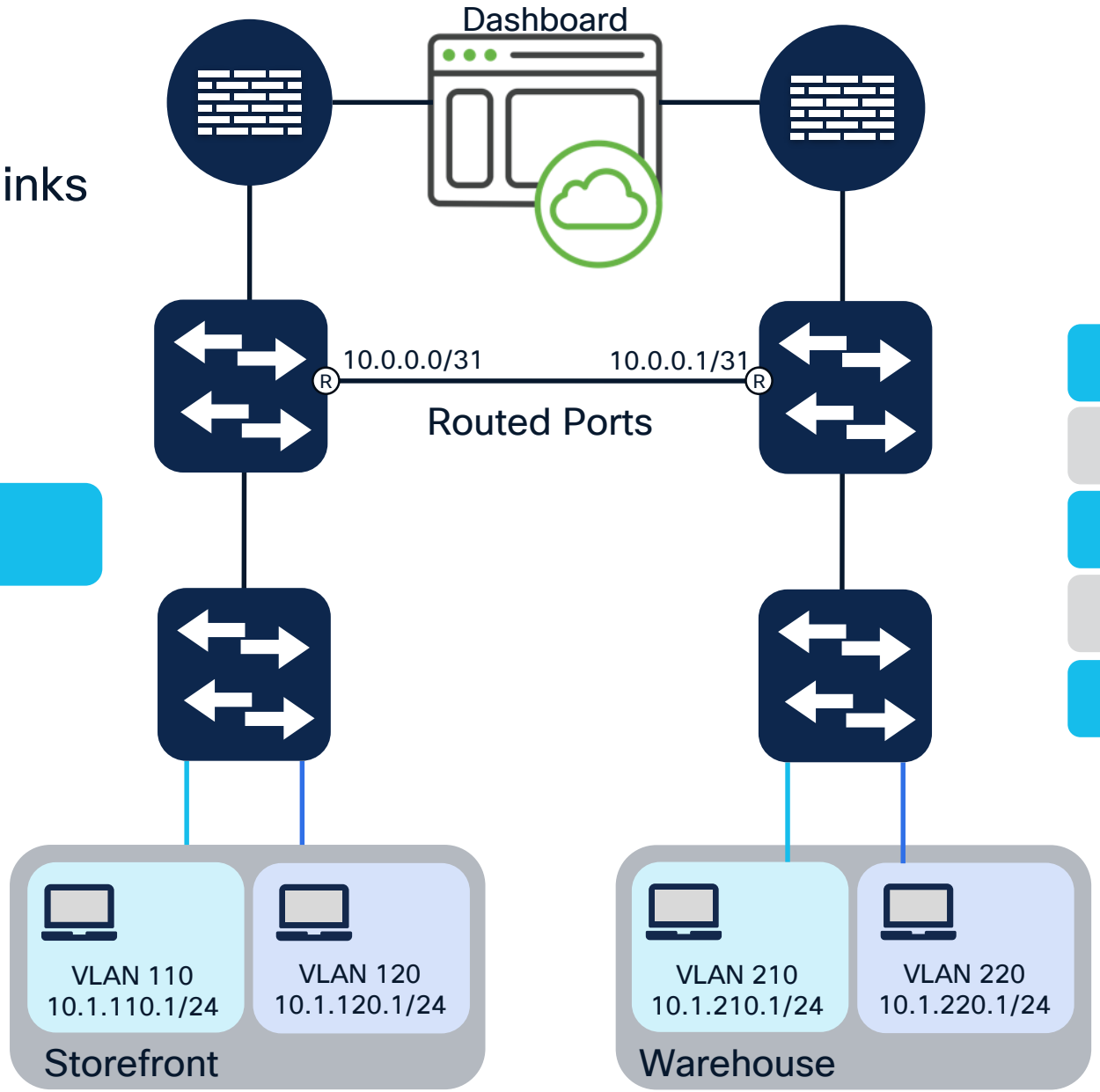
- /31 Addressing
- Reduced VLAN ID consumption
- Faster Convergence
- STP boundaries
- Equal cost load balancing



Routed Ports

East/West peer to peer links
(no Dashboard uplink)

Join separate networks



/31 Addressing

Reduced VLAN ID consumption

Faster Convergence

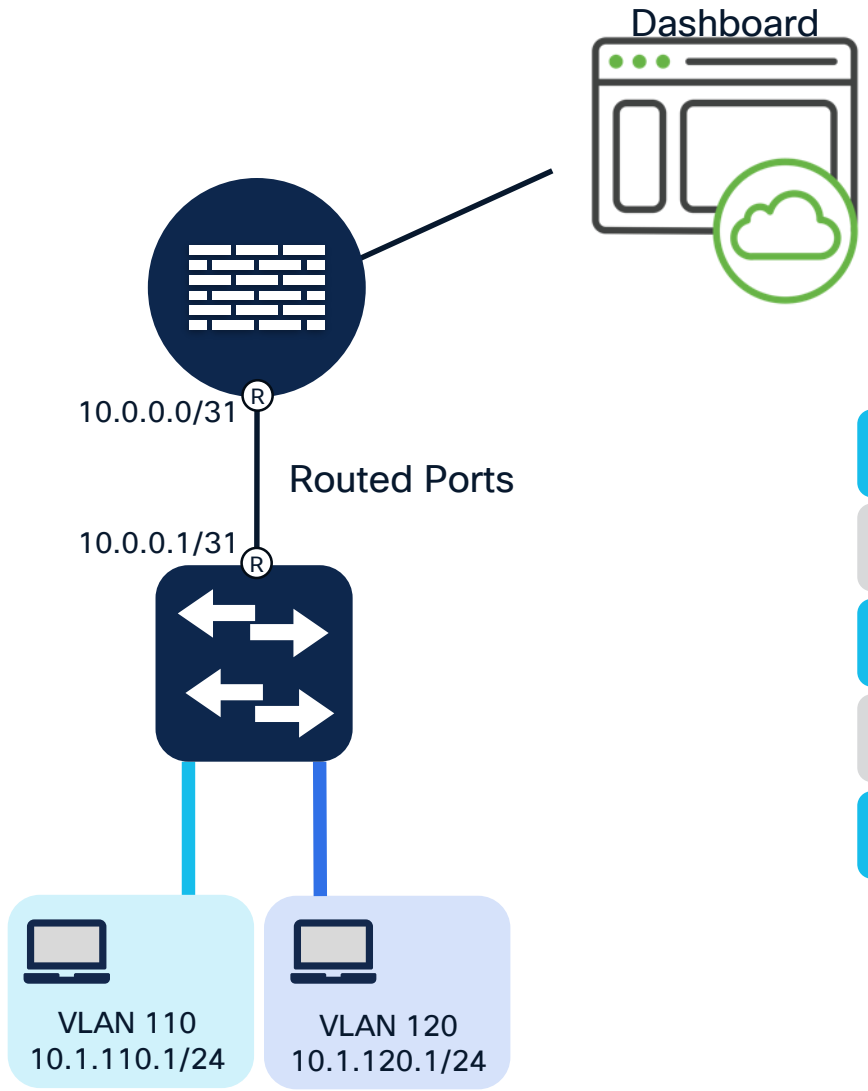
STP boundaries

Equal cost load balancing

Routed Ports

Northbound peer to peer links with Dashboard uplink

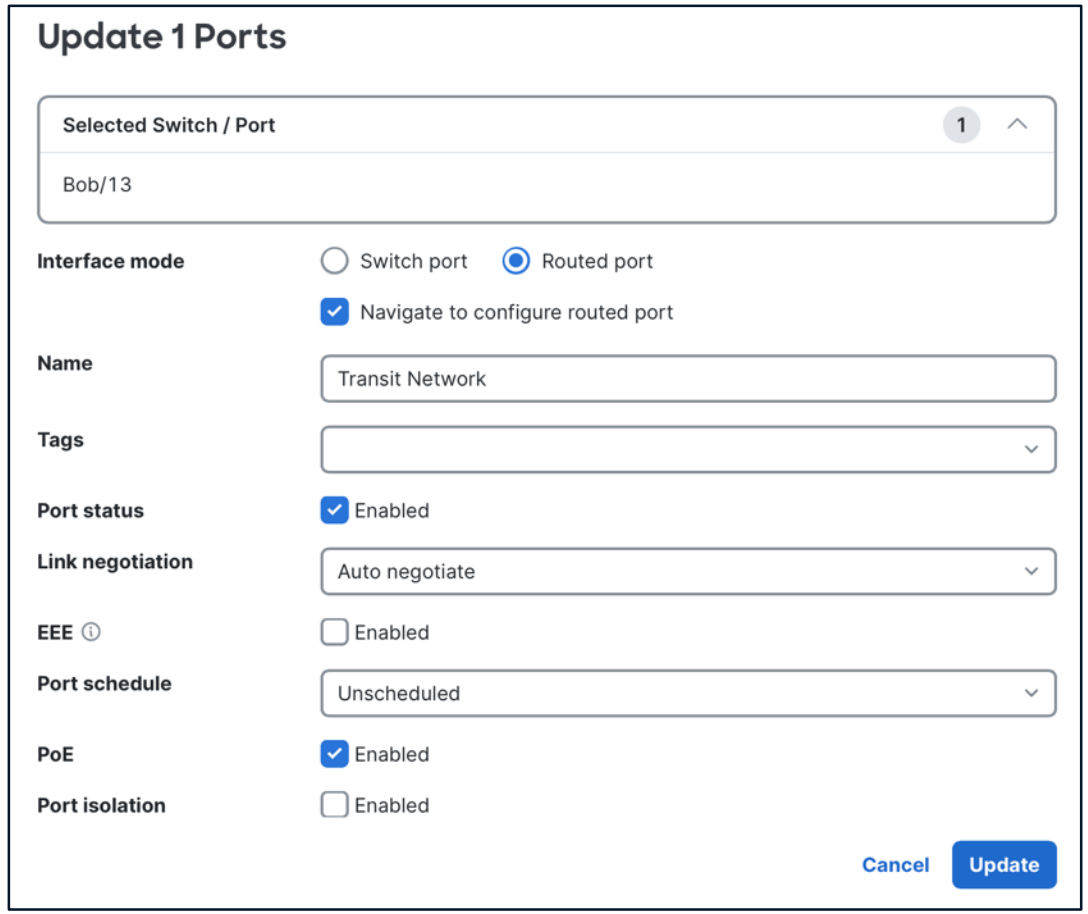
Routed uplink to Dashboard



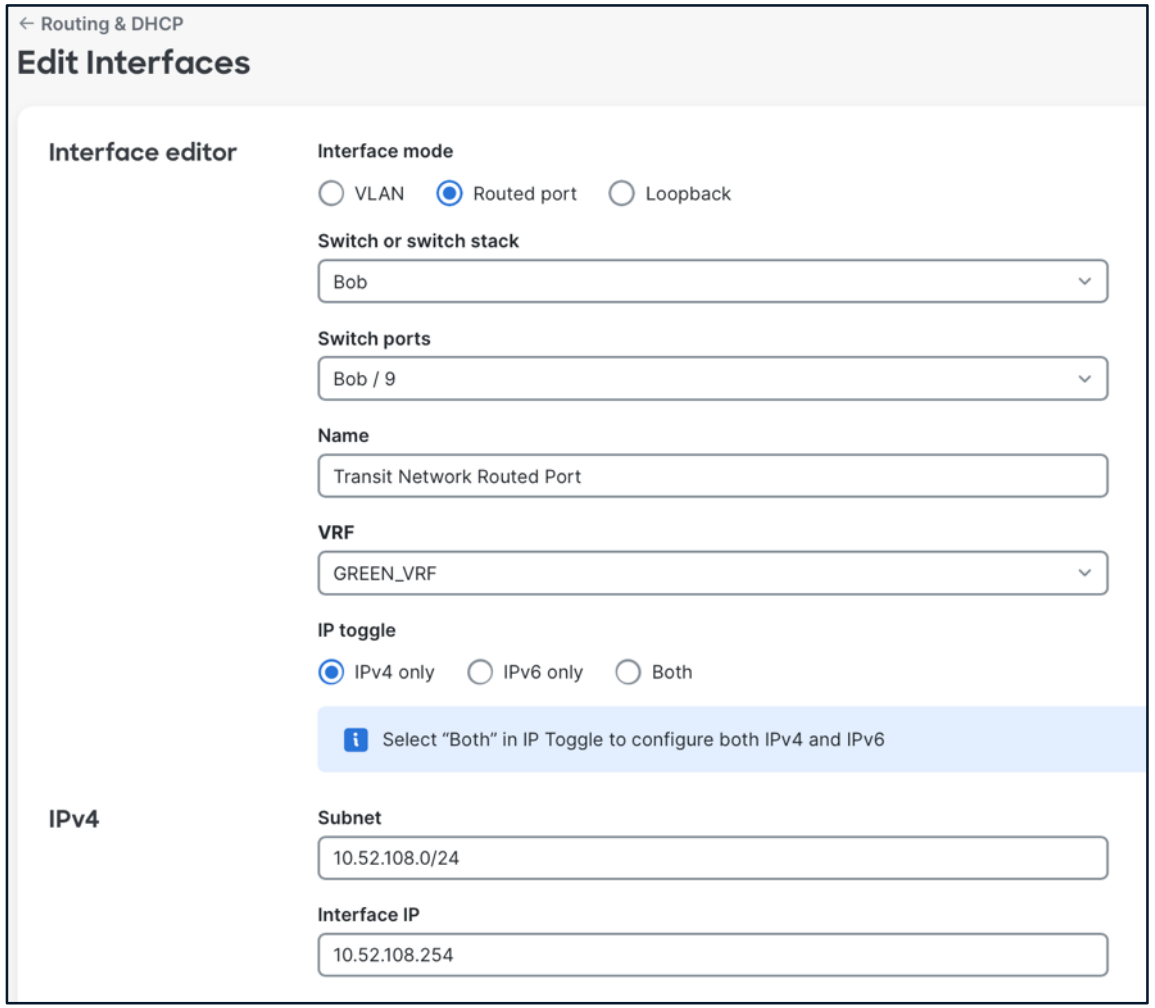
- /31 Addressing
- Reduced VLAN ID consumption
- Faster Convergence
- STP boundaries
- Equal cost load balancing

Routed Port Config

Switching > Switches > Switch Summary

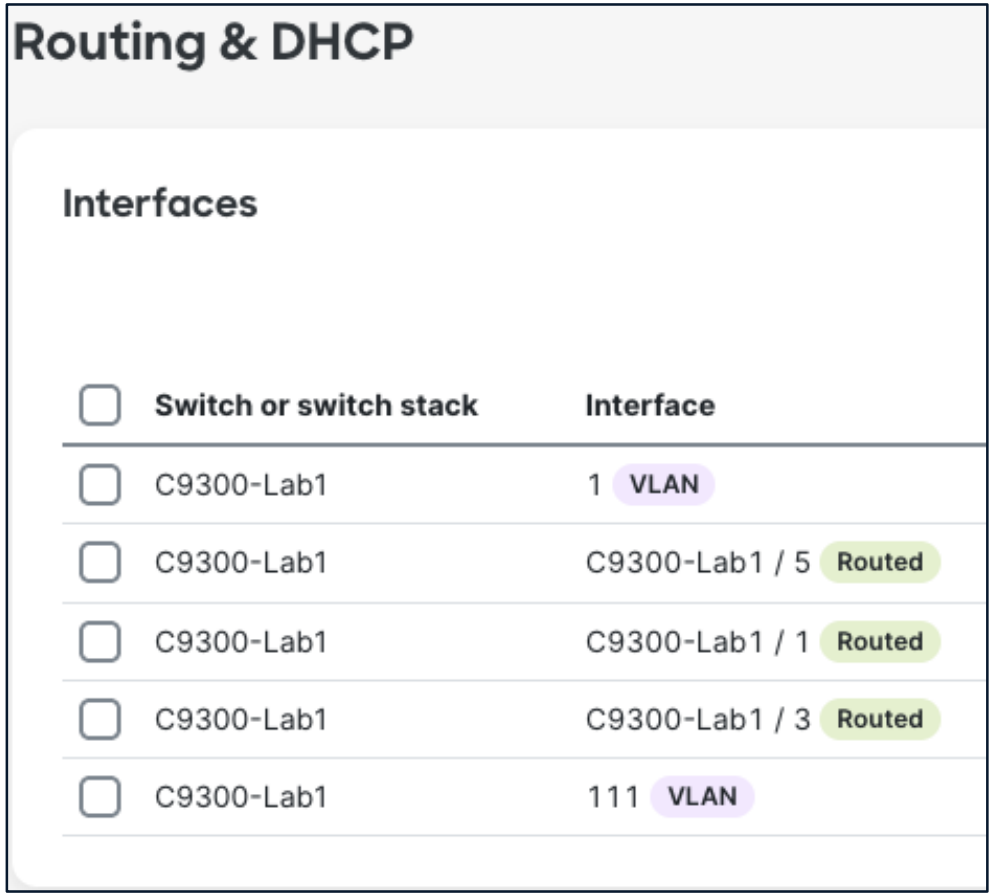


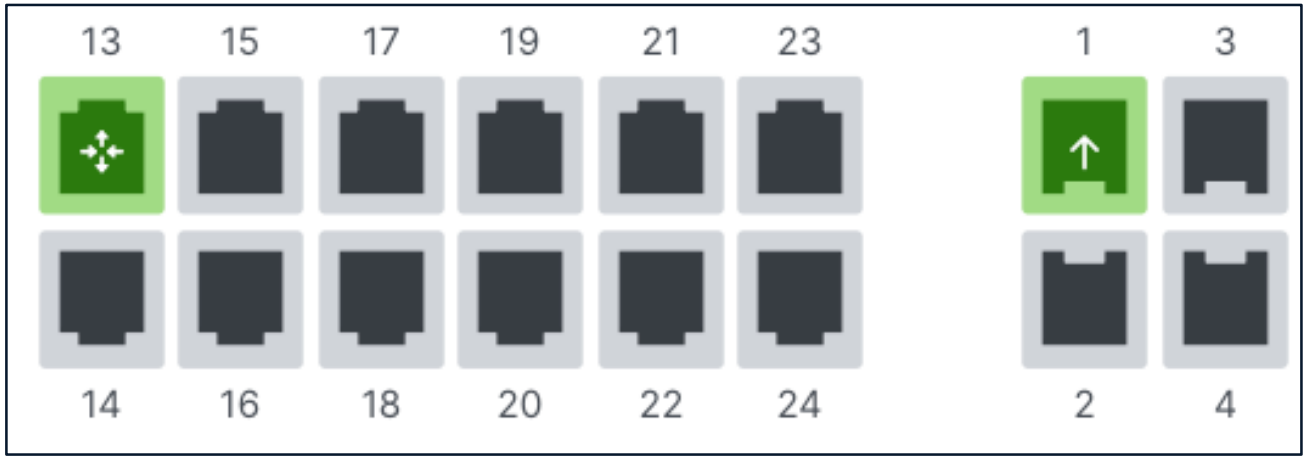
Switching > Routing & DHCP



Routed Port Config

Switching > Routing & DHCP





Adorable new routed port icon ♥

New tags for routed ports and VLAN Interfaces(SVIs)

BGP

Simple eBGP/iBGP

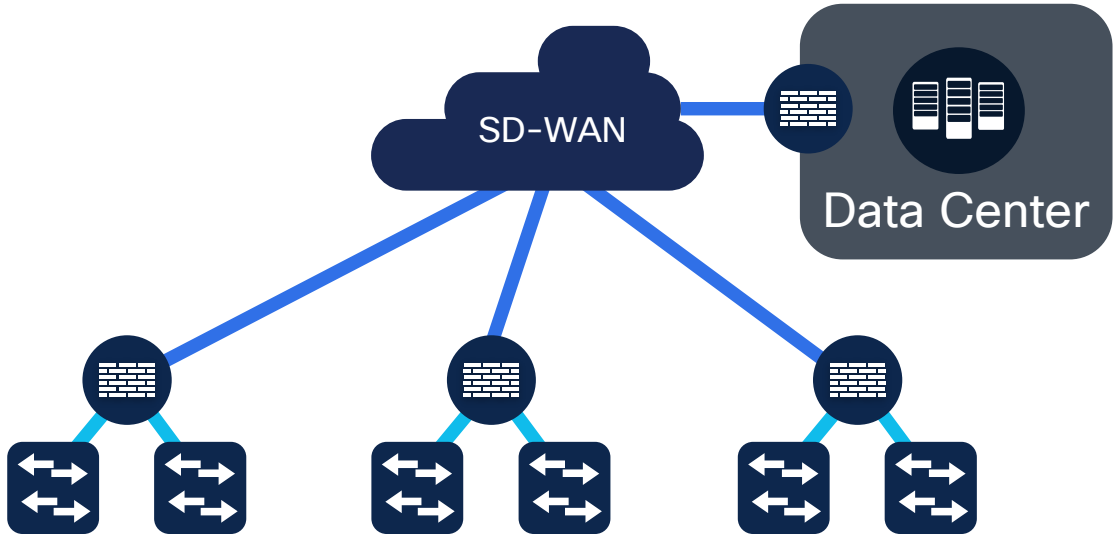
- Full stack meraki (MX + Catalyst)
- Vendor neutral peering

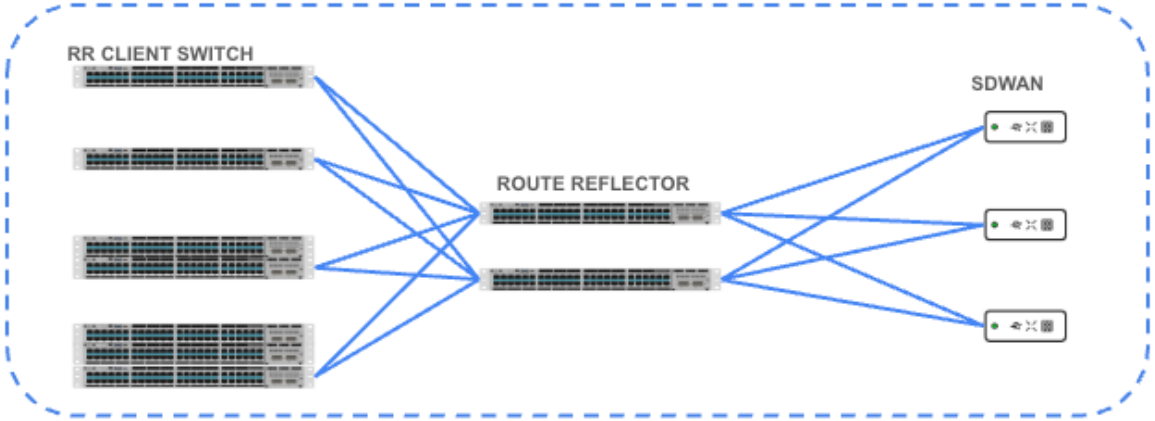
Large Campus Route-Reflector

- iBGP peer route-reflector
- Loopback support
- Route filtering and AS-path control
- Traffic ECMP

Spin your own

- Per-switch configuration
- Peer-group templates
- Common policy objects





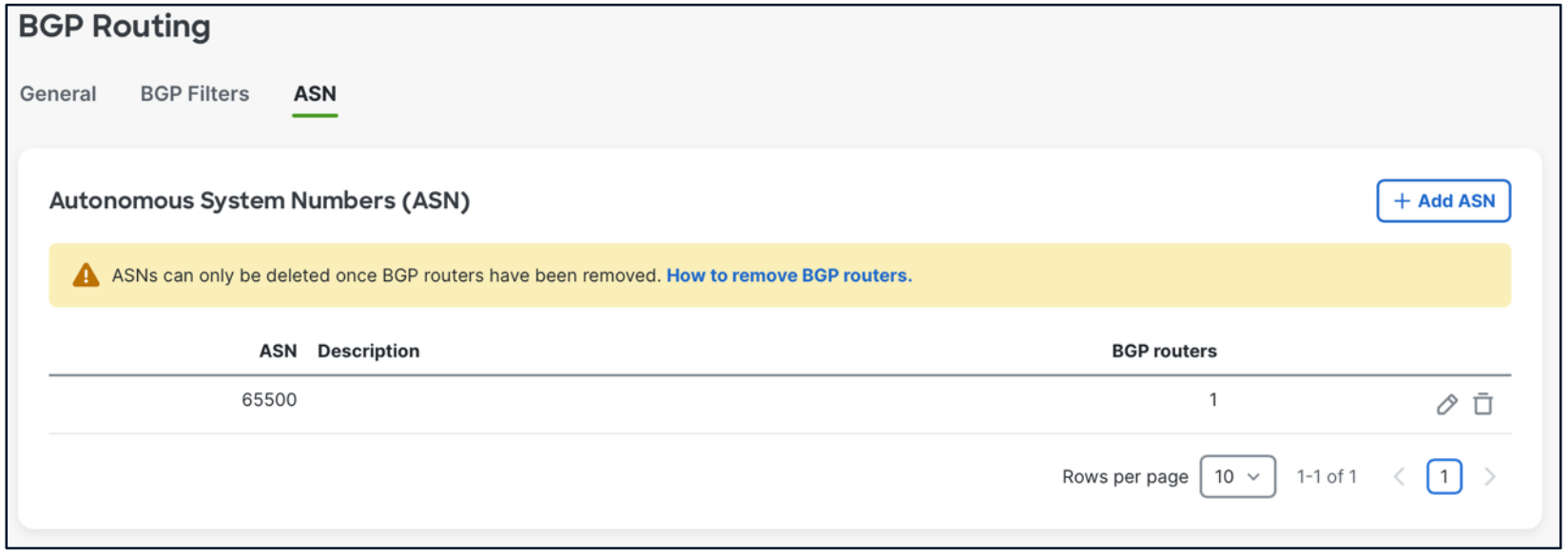
Requirements

- Firmware: IOS XE 17.18+
- HW: C9500, C9300X, C9300, C9300L, C9300LM

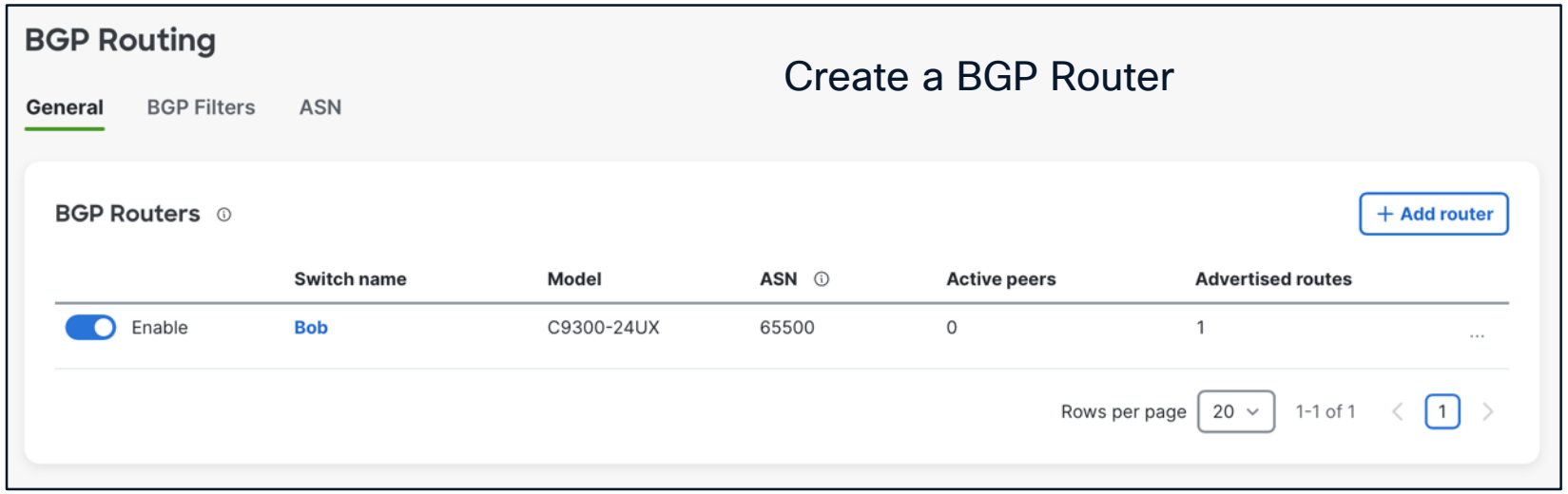
BGP Config

Switching > BGP Routing

Create an ASN



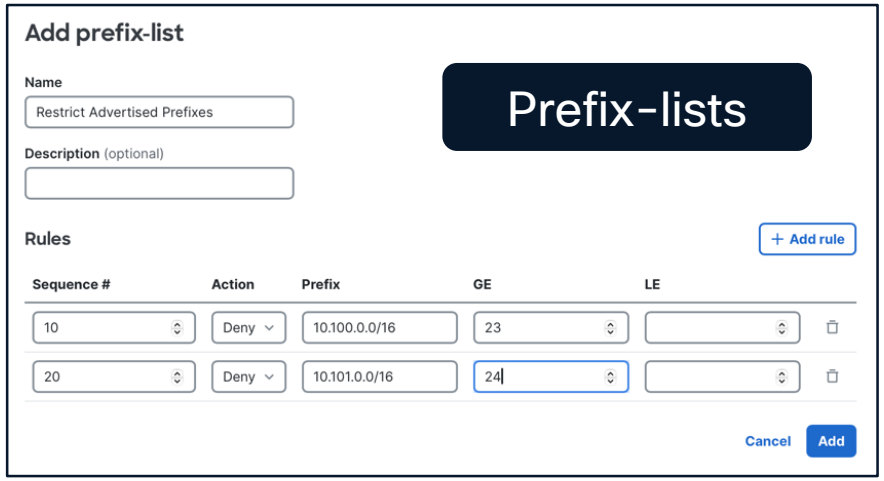
Create a BGP Router



Enable BGP per switch

BGP Config

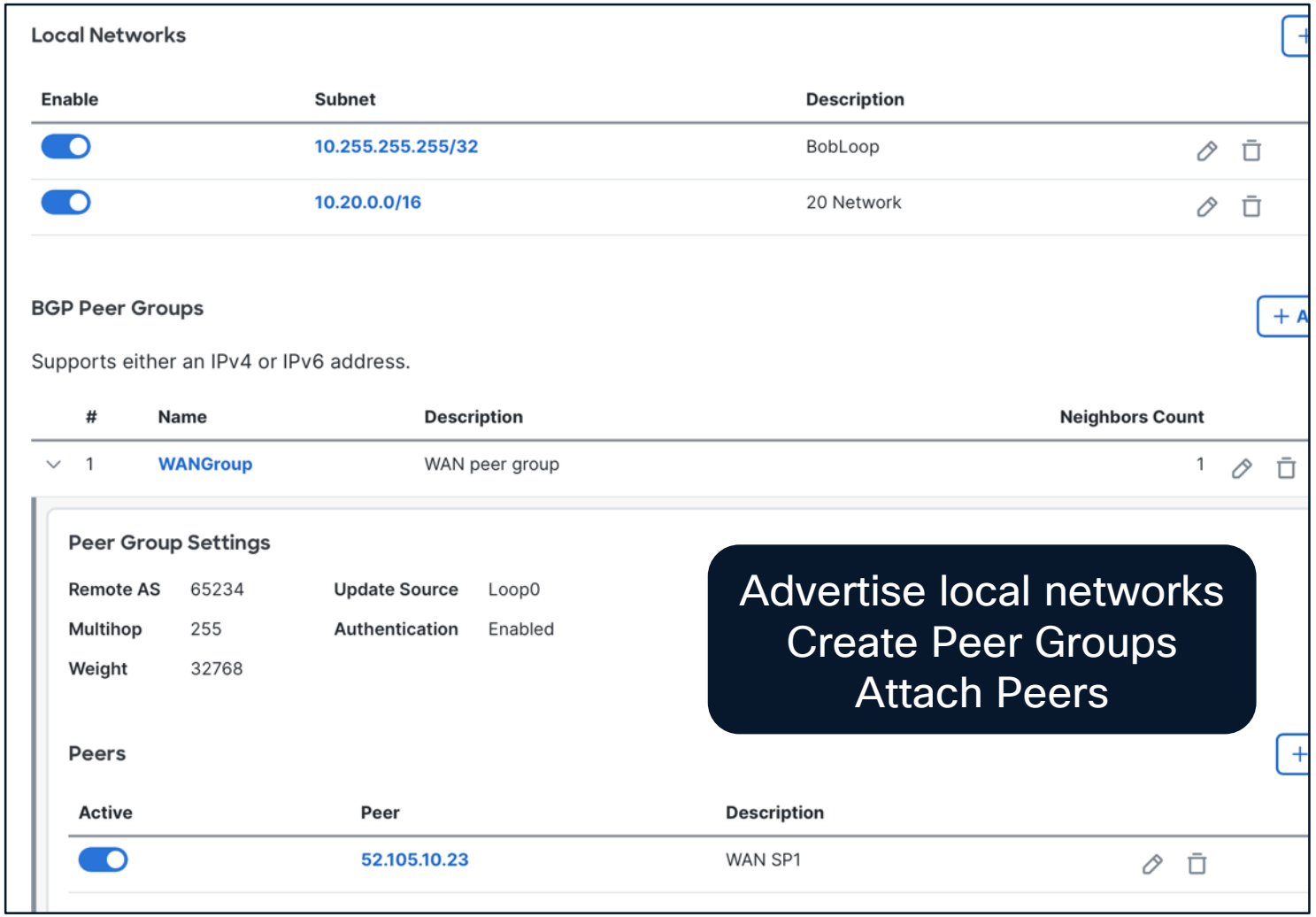
Route Filtering



Prefix-lists

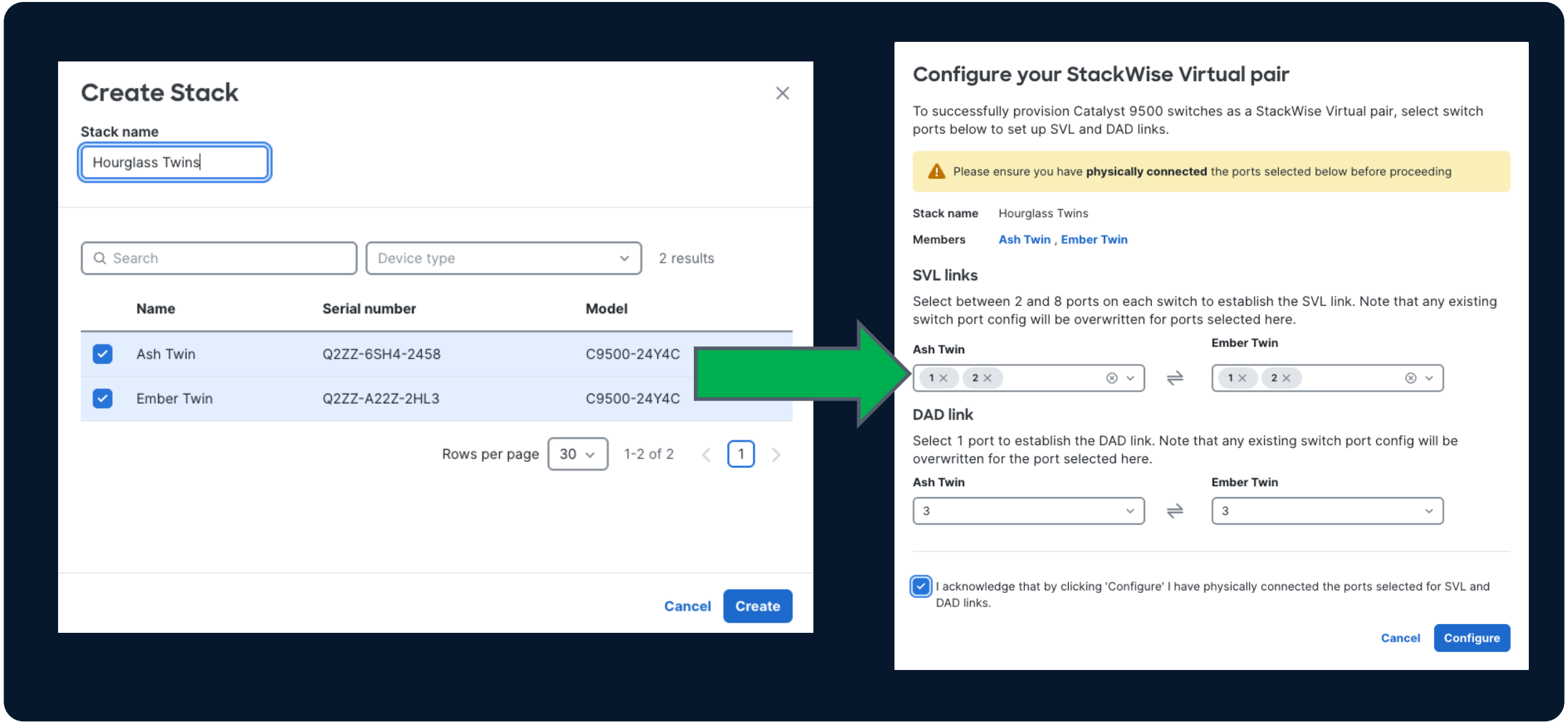
AS-path access-lists

Peering Config

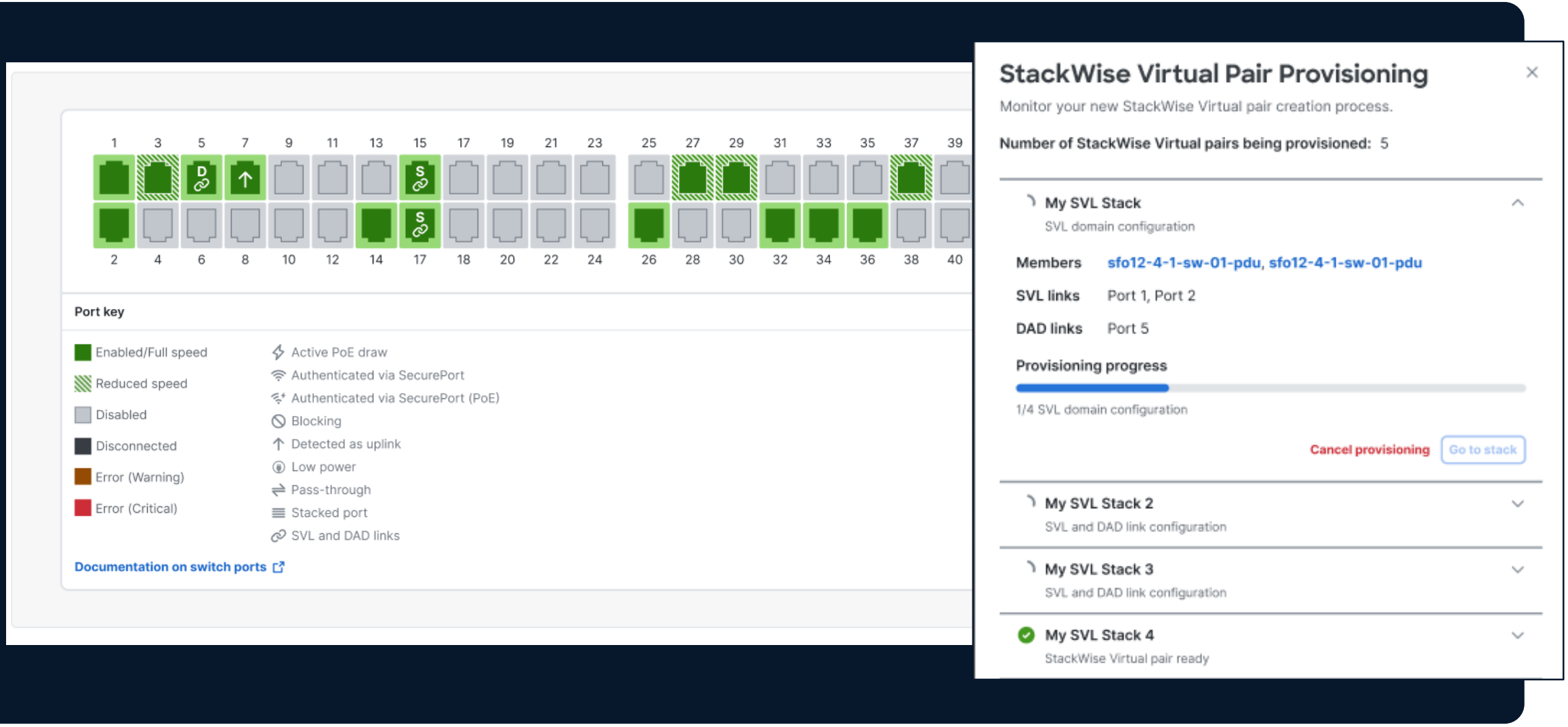


Advertise local networks
Create Peer Groups
Attach Peers

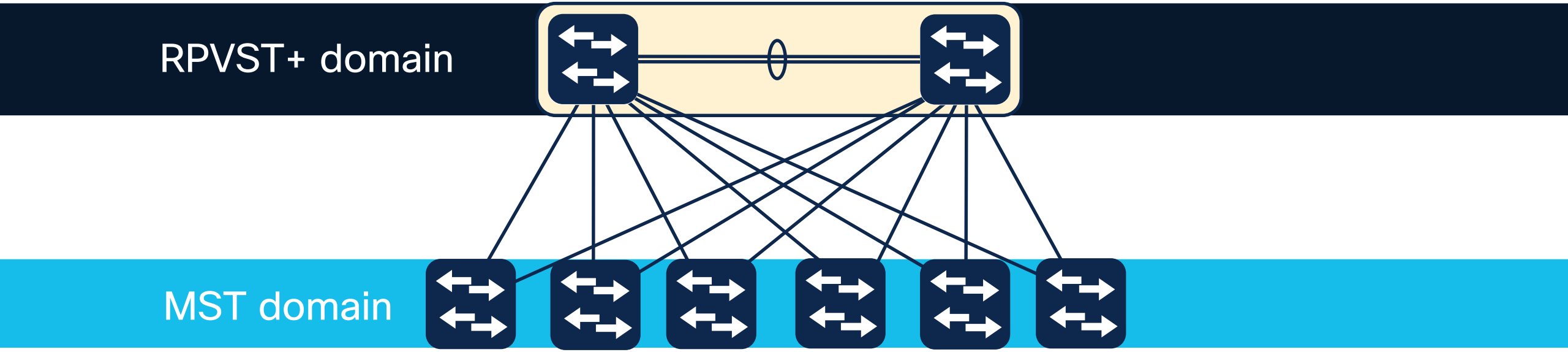
StackWise Virtual Setup



StackWise Virtual Config



Mixed Spanning-tree Versions

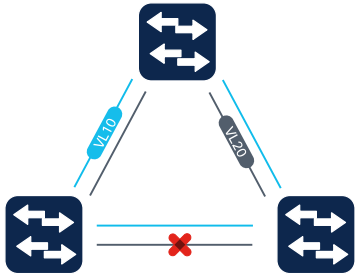


Rules of MST PVST+ interaction

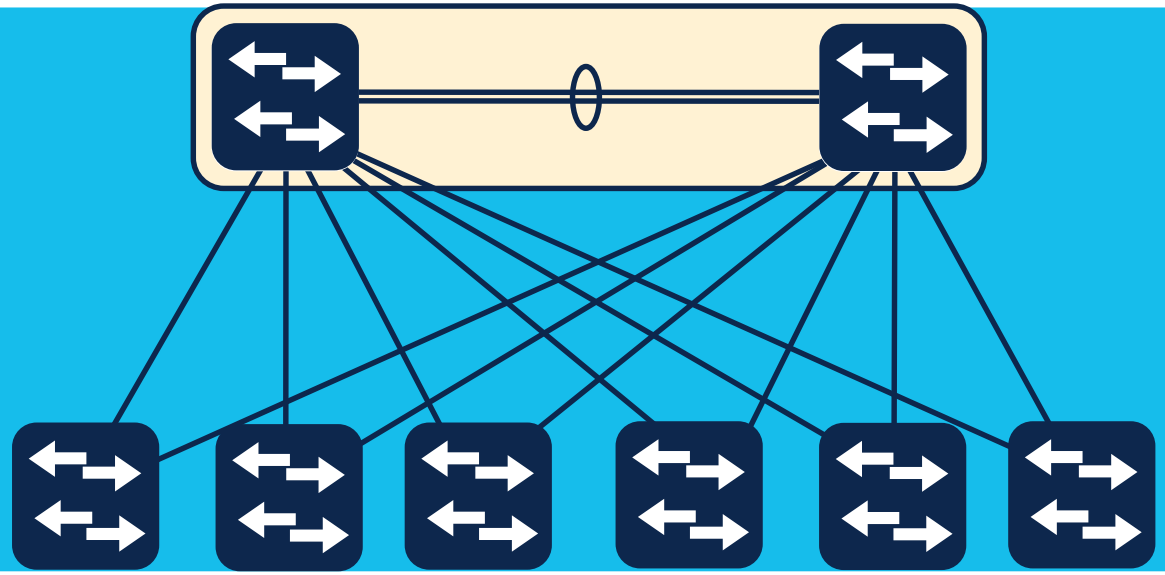
- If the MST bridge is the root, this bridge must be the root for all VLANs
- If the PVST+ bridge is the root, this bridge must be the root for all VLANs (this includes the CST, which always runs on VLAN 1, regardless of the native VLAN, when the CST runs PVST+)
- The simulation fails and produces an error message if the MST bridge is the root for the CST, while the PVST+ bridge is the root for one or more other VLANs. A failed simulation puts the boundary port in root inconsistent mode.

REF: Understanding Multiple Spanning Tree Protocol (802.1s)

RPVST+



RPVST+ domain



VLANs and PVST+ Instances

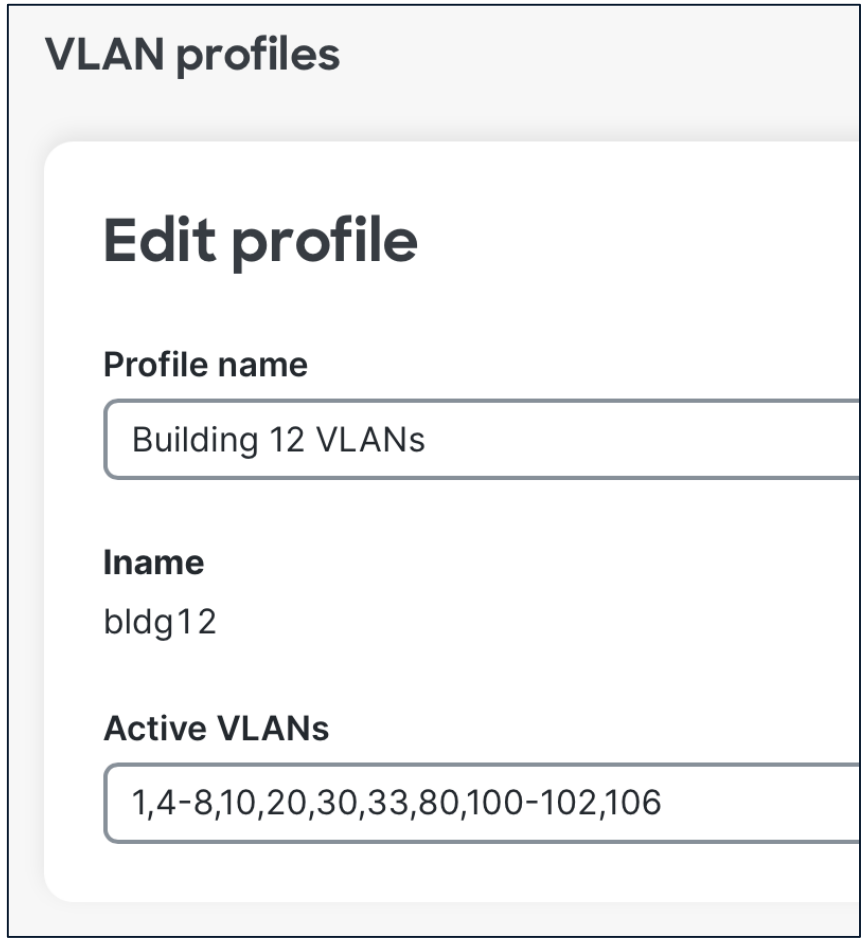
Time to use VLAN Database

Cloud-managed switches start with max supported active VLANs

- Catalyst 9300 = 1000
- Catalyst 9200 = 512

Catalyst switches can't run that many PVST+ instances

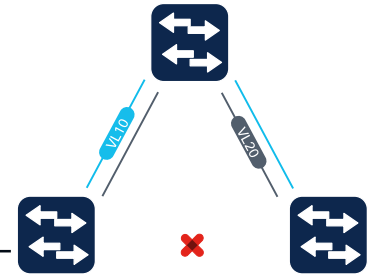
- Catalyst 9300 max 300 PVST instances
- Catalyst 9200 max 128 PVST instances
- Max 13000 STP Virtual ports*



The secret to a happy life is pruning unneeded VLANs

**STP virtual ports = trunks * active VLANs on trunk + number of non-trunk ports.*

RPVST+ Config



Switching > Switch Settings

Set the STP mode for the entire network

Set bridge priorities per switch & VLAN

STP configuration

STP configuration mode

- (•) Enable Spanning Tree
  - **Select Spanning Tree mode for Catalyst switches:**
  - ( ) Enable Multiple Spanning Tree (MST)
  - (•) Enable Rapid per-VLAN Spanning Tree (RPVST+)

ⓘ Operating network with a mix of RPVST+ and RSTP may cause unexpected issues, please refer to **Documentation** for best practices for operating mixed STP environments.

- ( ) Disable Spanning Tree

STP bridge priority ⓘ

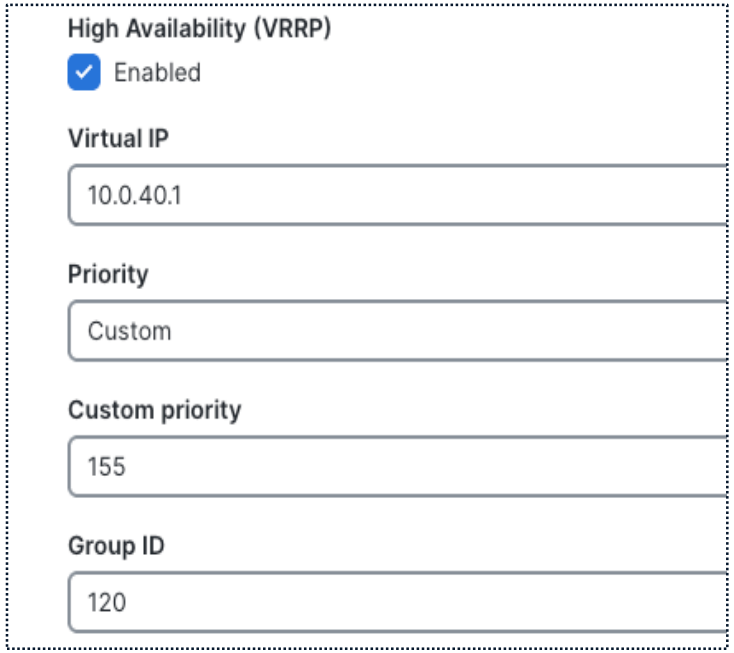
Switches/Stacks	Bridge priority	VLAN list	Actions
Default	32768		
Rocky_and_Bullwinkle	8192	1-4094	✎ 🗑

+ Set the bridge priority for another switch or stack

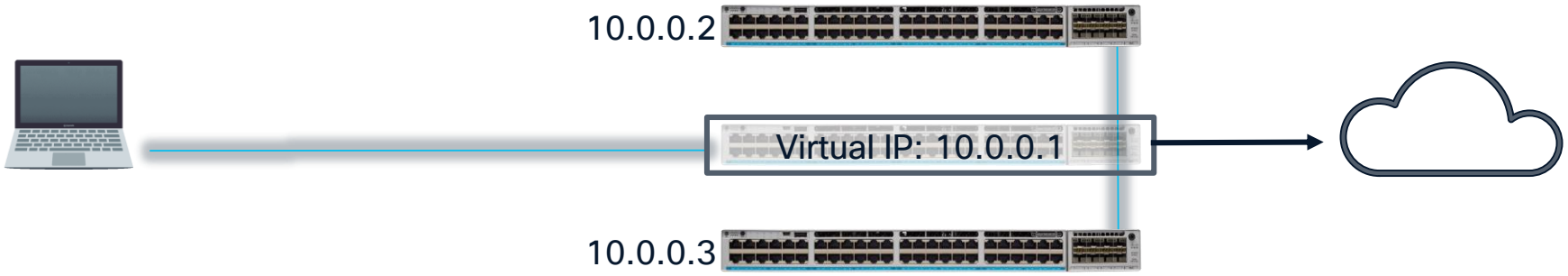
VRRP

Flexible, interoperable HA *Coming 17.18.2

1. Create/Edit a Layer3 SVI on each switch
2. Enable "VRRP" for IPv4 or IPv6
3. Configure both switches with matching Group-ID and VIP
4. Assign Priority to control Active



- IPv4 and IPv6 Support
- Per-Interface Control
- Compatible with OSPF/BGP/VRF
- Standards-based compatibility



Enterprise Switching Architectures

Enterprise Campus

Campus Core

Low-latency, high-availability

Core-Access Interconnect

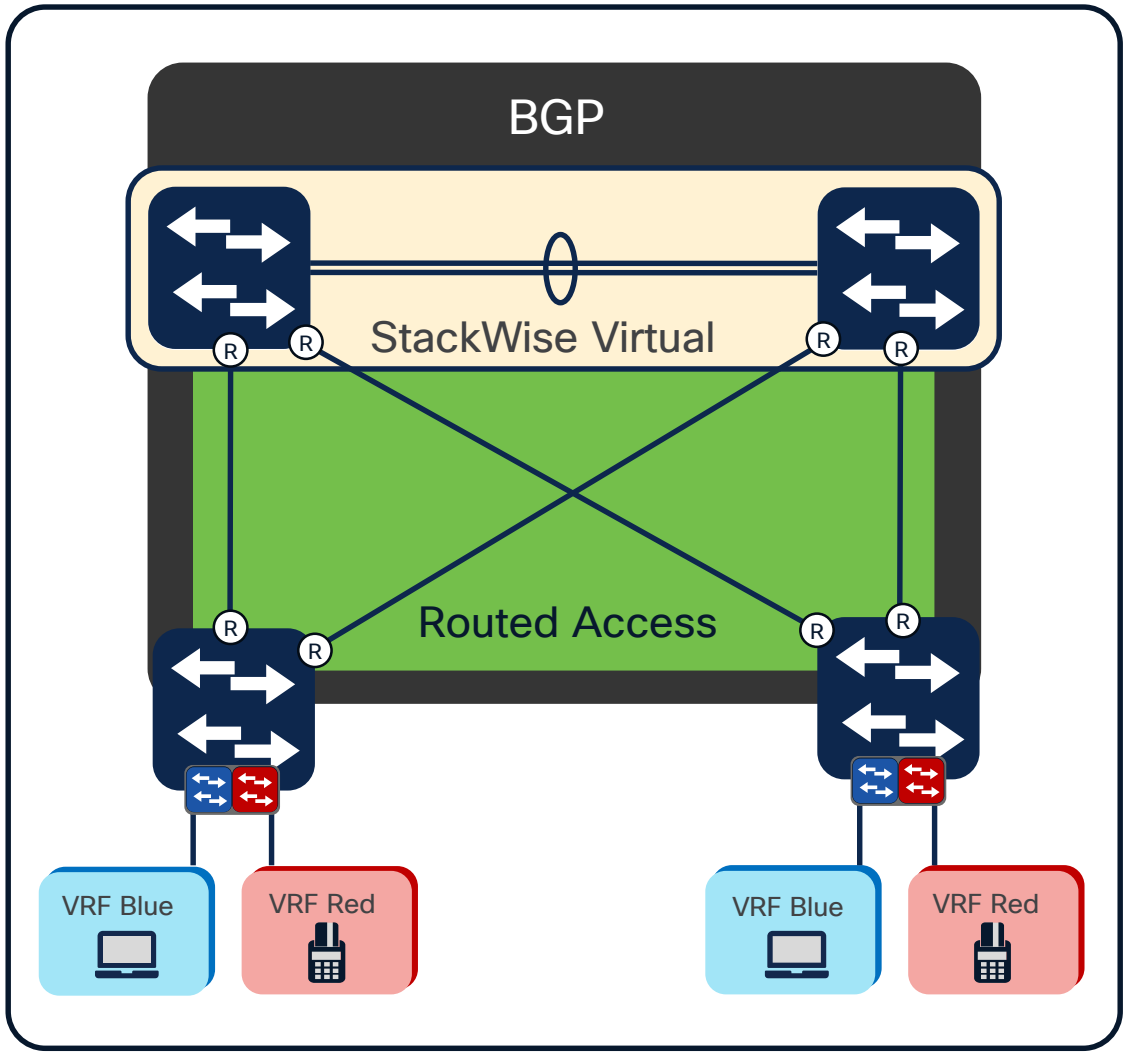
L3 routed access, limited STP

RPVST+ is still common

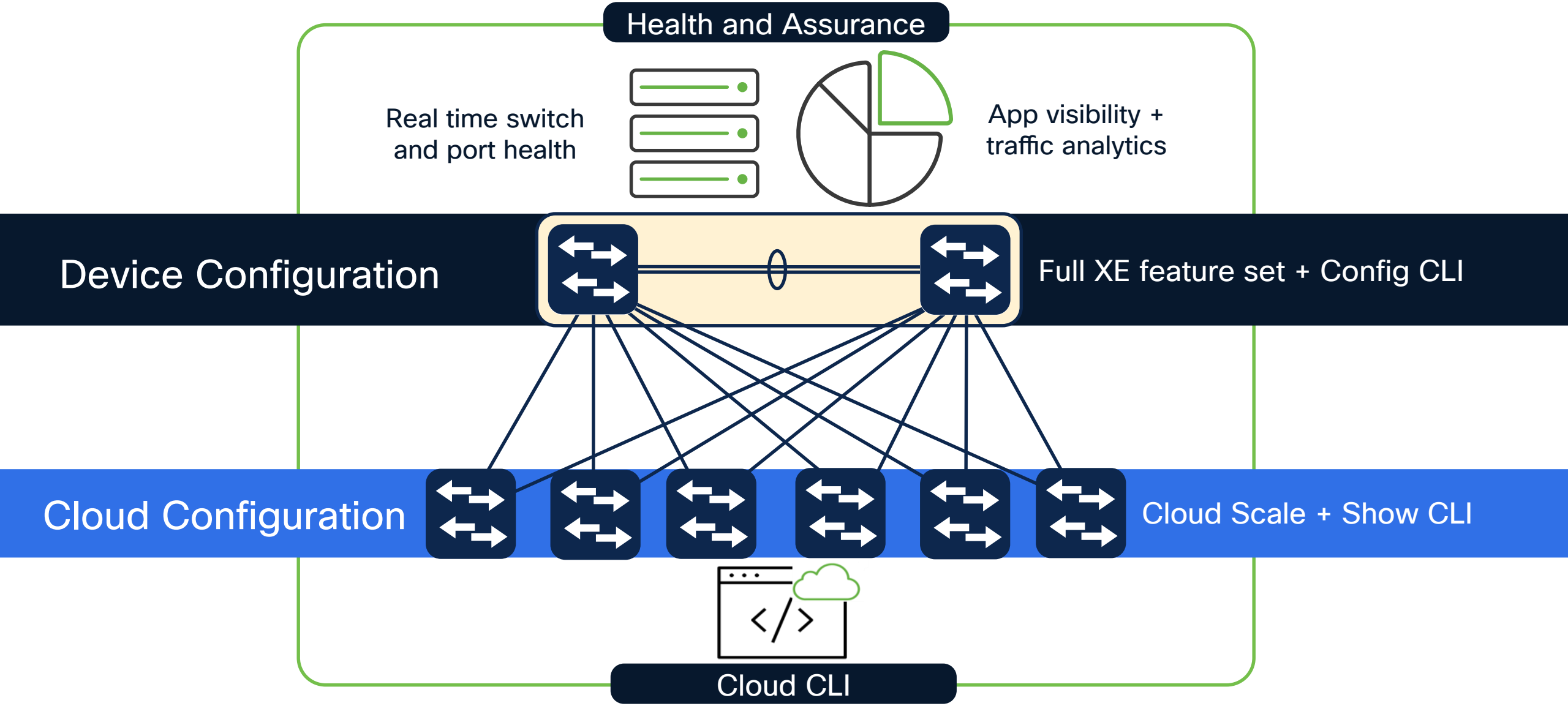
Campus Access

VRF segmented access layer

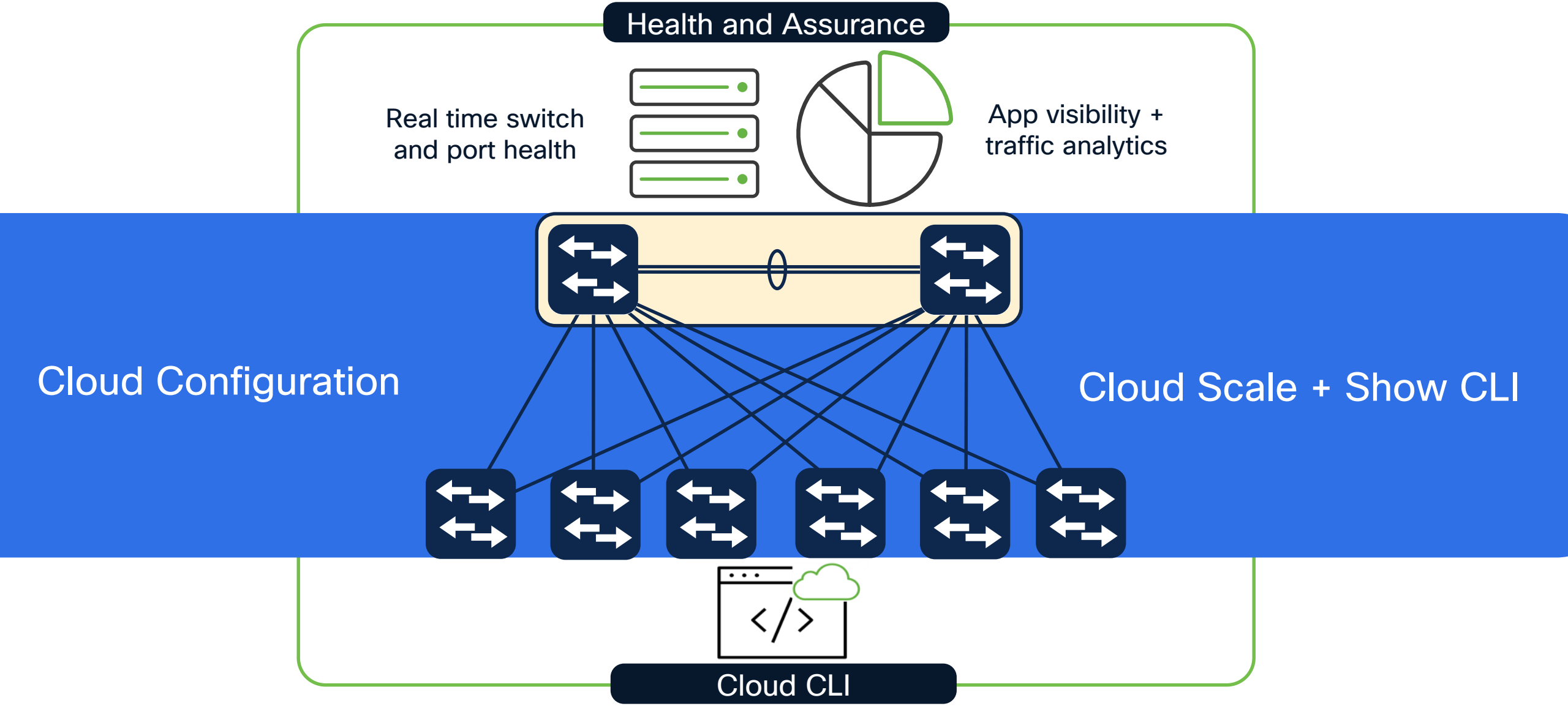
RPVST+ is common



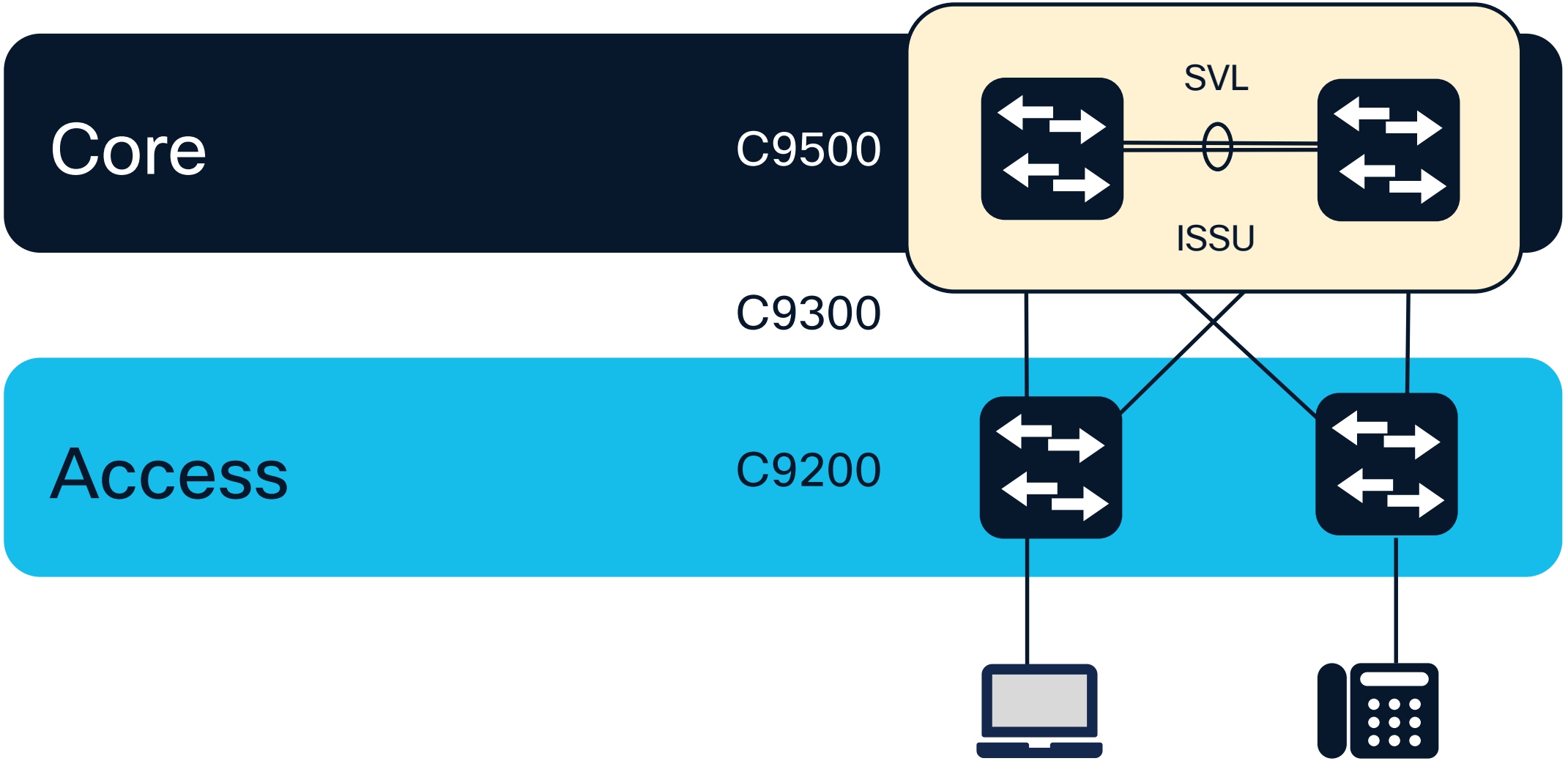
Flexible Config for Enterprise Cloud-management



Full cloud config for Enterprise Cloud-management



Core and Access Platforms



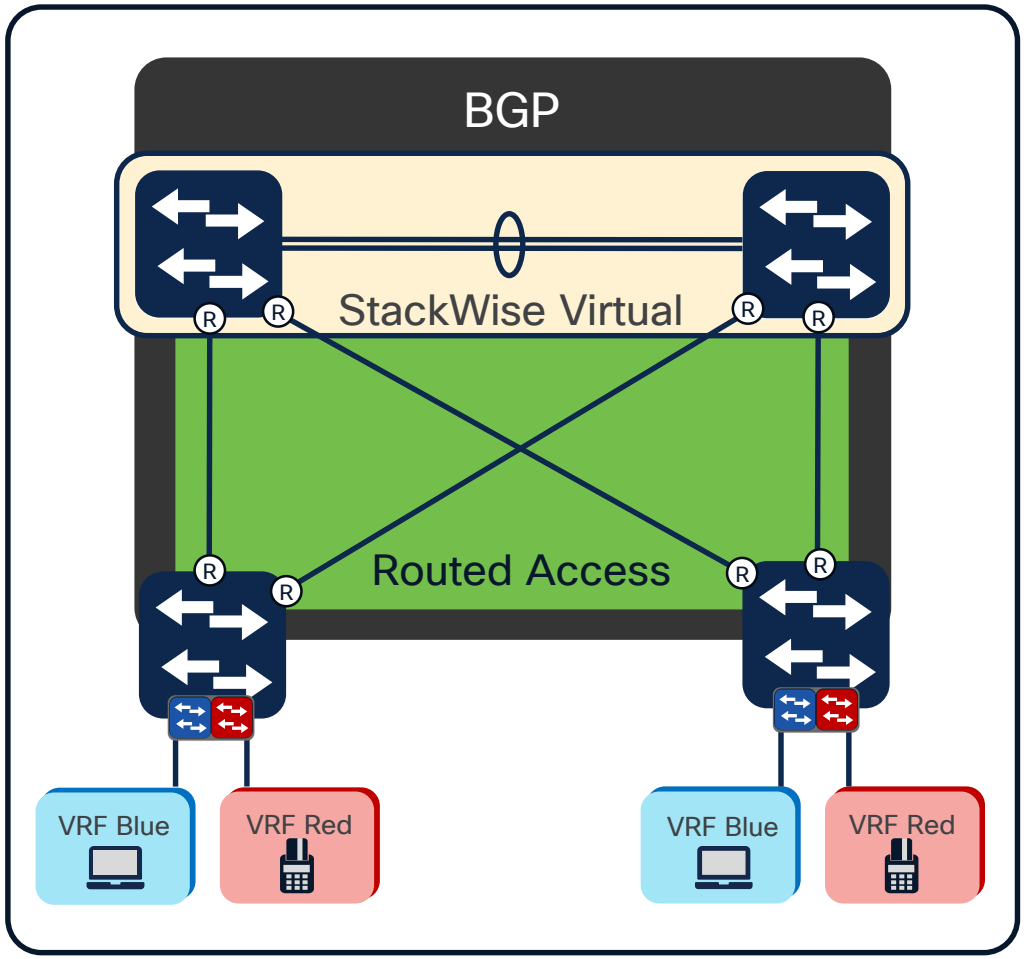
Enterprise Cloud-managed switching

Advanced Routing

Routed Ports	Loop-free routed access
VRF Lite	Scalable macro segmentation
BGP	Flexible, open dynamic routing

High-Availability

Rapid PVST+	Enhanced L2 loop prevention
StackWise Virtual (SVL) ISSU	Sub-second downtime firmware upgrades



Advanced L3

Routed Ports

Leverage Layer 3:

- Limit spanning-tree issues
- Smaller broadcast domains
- Faster Convergence
- Fewer VLANs

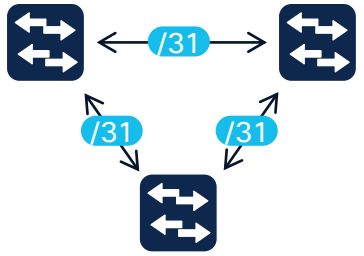
VRF

- Simple Macro Segmentation

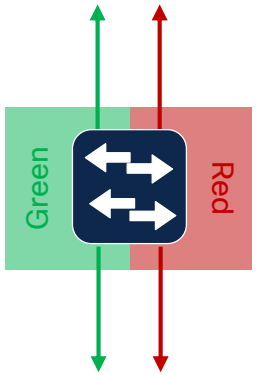
BGP

- Highly Flexible Reachability

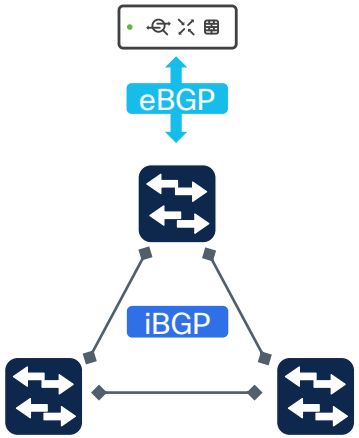
Routed Interfaces



VRF Lite



BGP



High Availability

Stackwise Virtual and ISSU

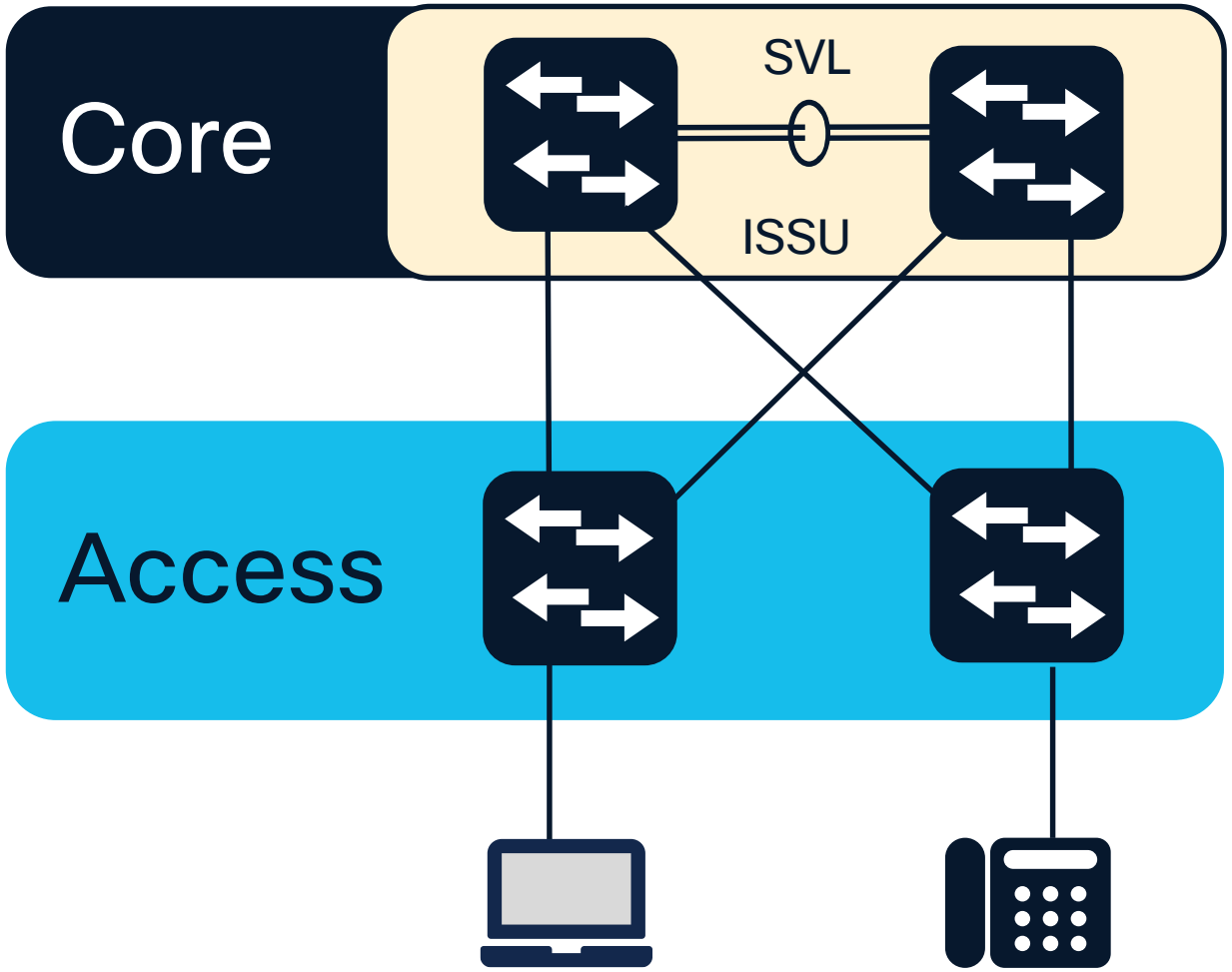
- Sub-second downtime upgrades

Staged Upgrades

- Roll incremental upgrades across a campus network

RPVST+

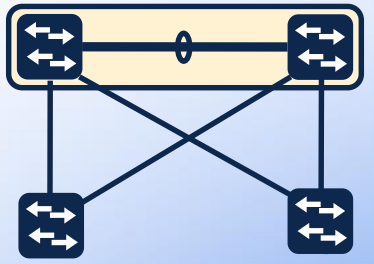
- Interoperability with all Catalyst based platforms
- Per-VLAN high availability



Is cloud ready for you?

Cloud manage your Catalyst

Check out the Cloud CLI



Look to the core in 17.18

Complete your session evaluations

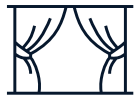
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

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

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

Thank you

cisco Live !


CISCO