
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Deploying VPNs Over Segment Routed Networks Made Easy

SDN Approach

Krishnan Thirukonda
@KrishThirukonda

BRKMPL-2131

cisco Live!

#CiscoLive

Cisco Webex App

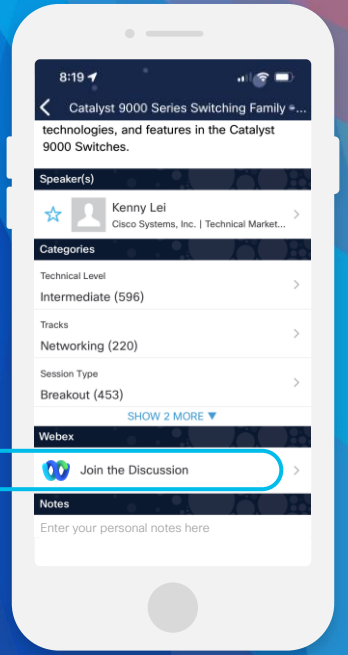
Questions?

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 9, 2023.

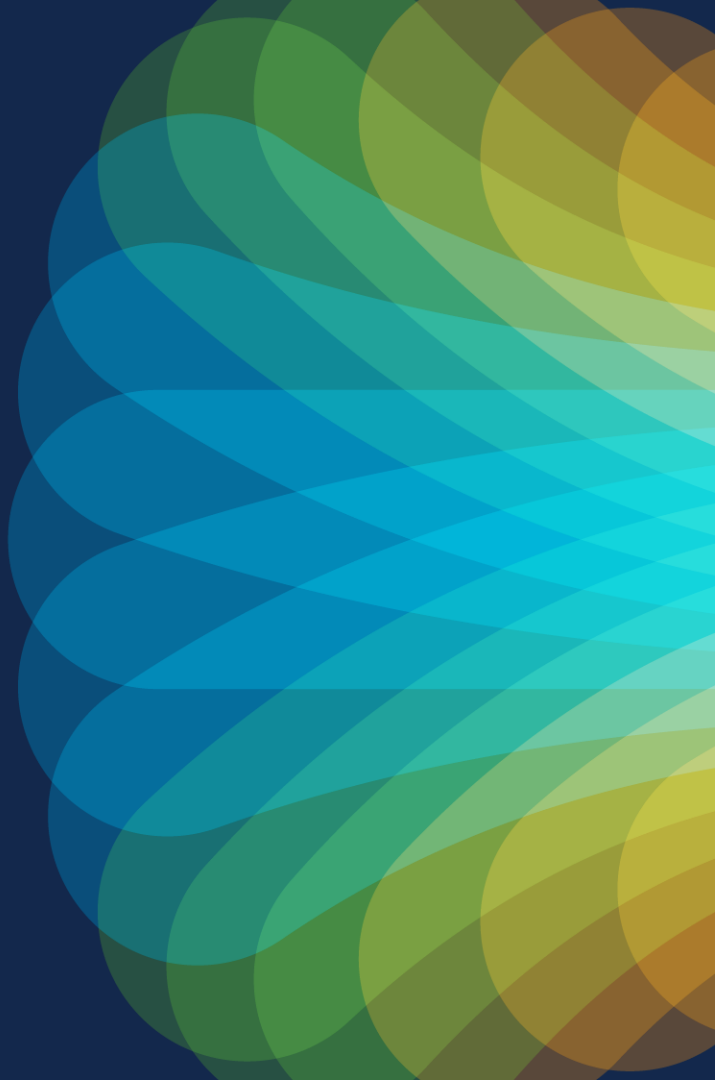


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMPL-2131

Agenda

- Technology Review
- Automation Considerations
- Cisco Controller for Transport SDN
  - Demo
- Conclusion

Technology Review



Technology Review – Transport Services

- L2 and L3 VPNs
  - Overlay services over common IP/MPLS core or IPv6
  - Provides private networks with separation
  - Examples:
    - RFC 2547/4364 BGP L3VPNs
    - EVPN
    - L2VPN using VPLS or VPWS with T-LDP or …
- Internet access
- Multicast Transport – Content Delivery, MVPN etc

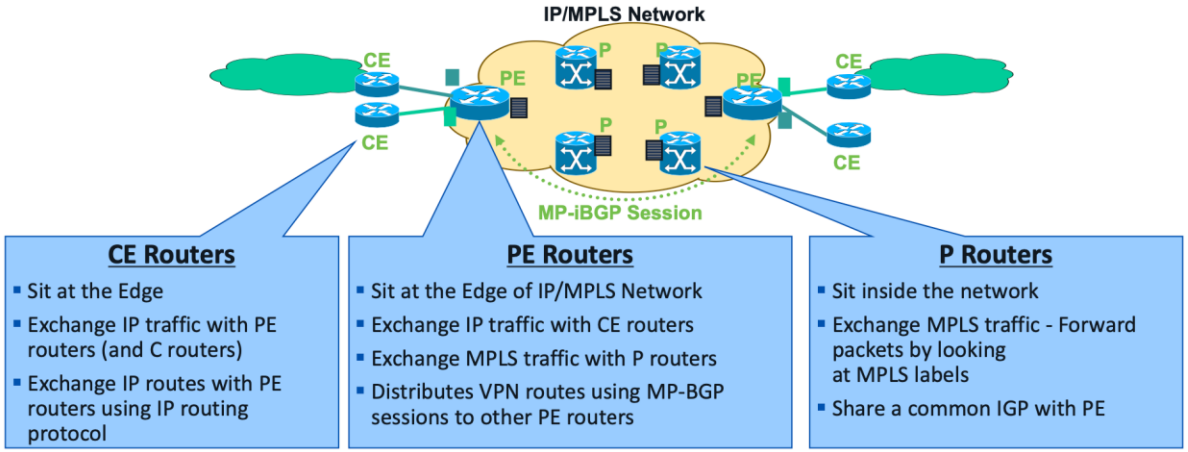
- Traffic Engineering
  - RSVP-TE (MPLS Core)
  - SR-TE (MPLS Core)
  - SRv6 (IPv6 Core)

This focus in this session is on Segment Routing

IP/VPN Technology Overview

Network Topology / Connection Model

Reference



Refer: BRKMPL-2102

Define VRF, RT & Policy

```
vrf vpn-101
 address-family ipv4 unicast
  import route-target
   65000:101
  !
  export route-policy SET_COLORv4_VPN-101-
ROUTE-POLICY
  export route-target
   65000:101
  !
```

PE-CE interface (& Qos)

```
interface HundredGigE0/0/0/1.101
 description T-SDN Interface
 vrf vpn-101
 ipv4 address 30.1.1.1 255.255.255.0
 encapsulation dot1q 101
!
```

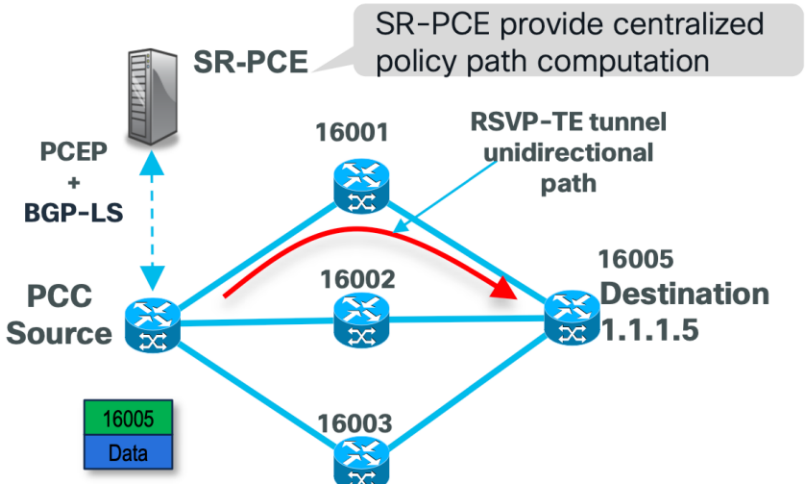
PE-CE Routing

```
router bgp 65000
 vrf vpn-101
  rd 65000:101
  address-family ipv4 unicast
   redistribute connected
  !
  neighbor 30.1.1.2
   remote-as 65003
   address-family ipv4 unicast
    route-policy PASS_ALL in
    route-policy PASS_ALL out
   !
  !
```

SR-TE vs RSVP-TE

- Source Routing
  - Source chooses a path and encodes it in the packet header as an ordered list of segments
  - The rest of the network nodes execute the SR encoded instructions
- Stateless SR-TE Policy
  - Policy label stack with Node-SID, or Adj-SID
  - Each Policy assigned unique Binding-SID
  - Node-SID ECMP Load-balance by IGP Nature
  - SR-PCE controller-based Inter-domain SR policy path calculation available
- Failure Protection - TiLFA
  - Local reroute comparable to MPLS TE Link / Node without RSVP signaling
  - IGP algorithm, support Microloop avoidance

	SR-TE	RSVP-TE
TE state only at head-end	Yes	No
ECMP-capability for TE	Yes	No
Engineered for SDN	Yes	Yes/No



Reference

Deploying Services with SR-TE

- L2VPN P2P with SR-TE static
- L2VPN EVPN with SR-TE with On-Demand Nexthop (ODN)
- L3VPN with On-Demand Nexthop SR-TE
- L3VPN or L2VPN with SRv6+FlexAlgo
- Internet E-PE
- Multicast with TREE-SID

- Signaling options:
  - NETCONF (PCC initiated)
  - PCEP (PCE initiated)
- Policy Path Options
  - Explicit candidate Paths – hops specified
  - Dynamic, locally calculated
  - Dynamic, PCE delegated
- Policy instantiation
  - Static
  - On demand
- Traffic Steering
  - Automated
  - Steering profile

- Dynamic Path Constraints
  - Metric minimization objective: latency, TE metric , hop count
  - SR IGP Flex Algo
  - Max Segment Depth
  - Affinity
  - Disjoint
  - Protected/unprotected
  - Bandwidth

Per service (VPN) To SR-TE Binding & Steering

- Preferred-path configuration. Works well for p2p services
  - L2VPN with preferred-path <tunnel> or <sr-policy> in configuration
- L3VPN and any multipoint VPN with RSVP-TE
  - use different loopbacks & BGP/Policy, CBTS, PBTS, SPP etc, limited
- On-Demand Next Hop with SR-TE :
  - BGP Color community colors advertised VPN Routes using route-policy
  - Service Level Objective (SLO) of the color configured in a template
  - PE instantiates sr-policy using template, on-demand when prefix arrives
  - Traffic Auto Steered for the colored Prefix to the Policy

Traffic Engineering – Why do we need it?

Service-Level Objective (SLO)

Link Preferences

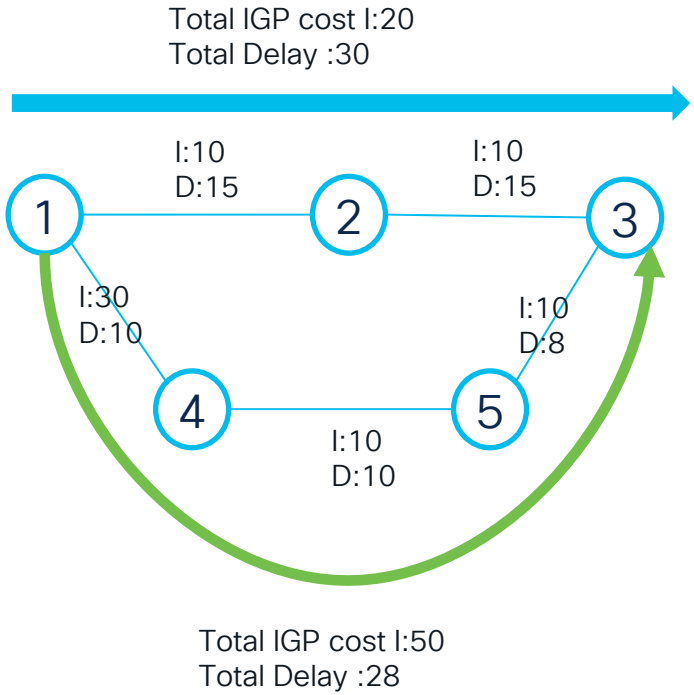
High Availability

Bandwidth Applications

Congestion Mitigation

SLO: Path Optimization Objective

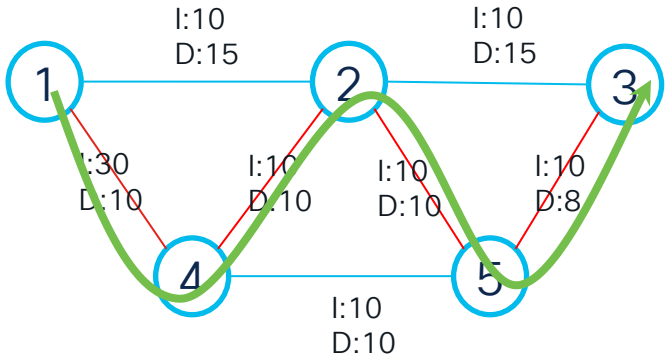
Ex: Find paths with lowest latency



Low Latency SLA traffic should go 1-4-5-3

Affinity to certain links

Example: Encrypted links etc

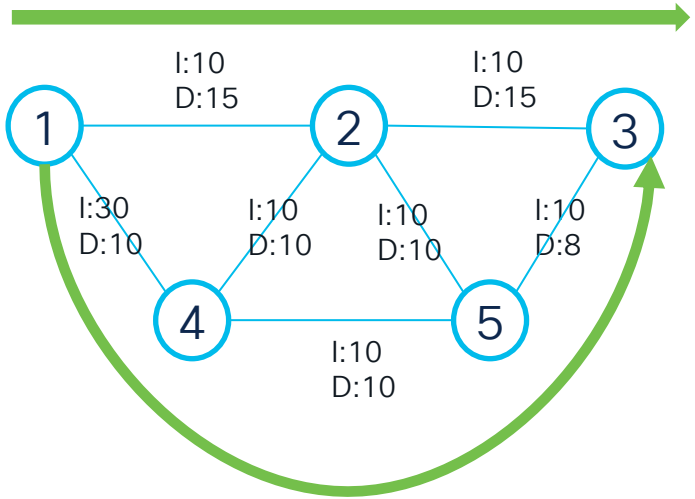


Total IGP cost I:50
Total Delay :28

Traffic that requires property=red goes through 1-4-2-5-3

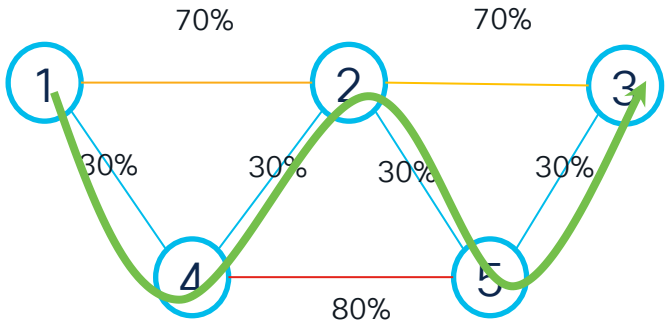
Highly Available Traffic using Disjoint paths

Send two copies with separated node/links/srlgs



Copy A via 1-2-3
Copy B via 1-4-5-3

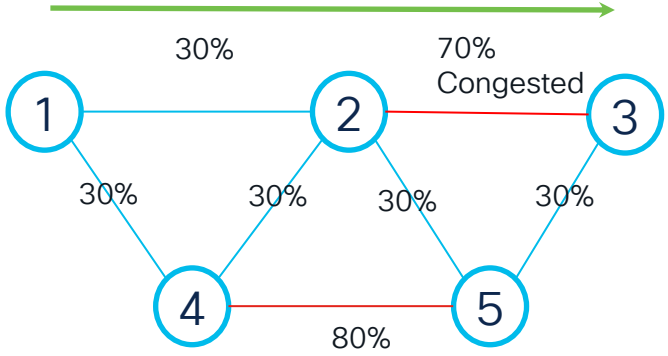
Bandwidth as Constraint



Link Utilization Tracked

Find and use Paths that have BW available for this traffic

BW Optimization Congestion Mitigation

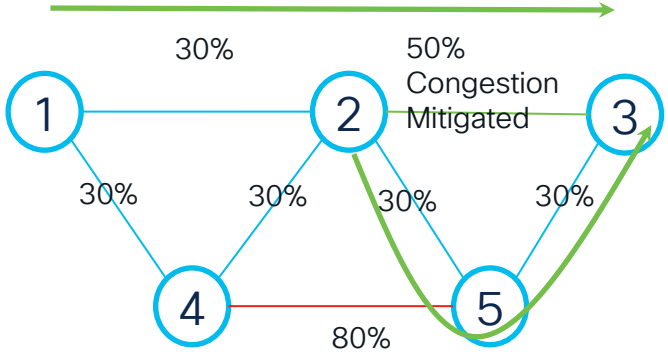


Link Utilization Tracked

At congestion points, create policies and bypass some traffic. Local vs Global Congestion Mitigation options.

Automation needed

BW Optimization Congestion Mitigation



Local Congestion Mitigation migrates some of the Optimizable traffic away from the congested link and brings

Path Calculation Options

- Explicit – Nail up paths – specify a list of hops
- Dynamic – Using CSPF* find path for specified constraints
  - Headend Based/Local – Headend router does path calculation using its TE DB
  - Centralized/Delegated – Headend requests path from external PCE
    - TE DB is Traffic Engineering database learnt via TE extensions to ISIS and OSPF
    - External PCE has TE DB from many ISIS and OSPF domains, can support multi-domain path calculation
- Path Provisioning
  - Headend Configured/PCC initiated
    - Configured on headend routers, headend may delegate to PCE using PCEP
    - Static Policy or On-Demand Nexthop Template
  - PCE Configured/PCE Initiated
    - Configured on PCE via CLI or API, PCE programs Headend using PCEP Protocol

*CSPF : Constrained Shortest Path First

SR-TE Policy Provisioning – IOS-XR Examples

- PCC-initiated Policies configured on headend routers
  - Crosswork Network Controller includes configuration engine to provision these
- PCE-initiated Policies configured on the IOS-XR SR-PCE
  - CNC UI/API includes capability to provision these

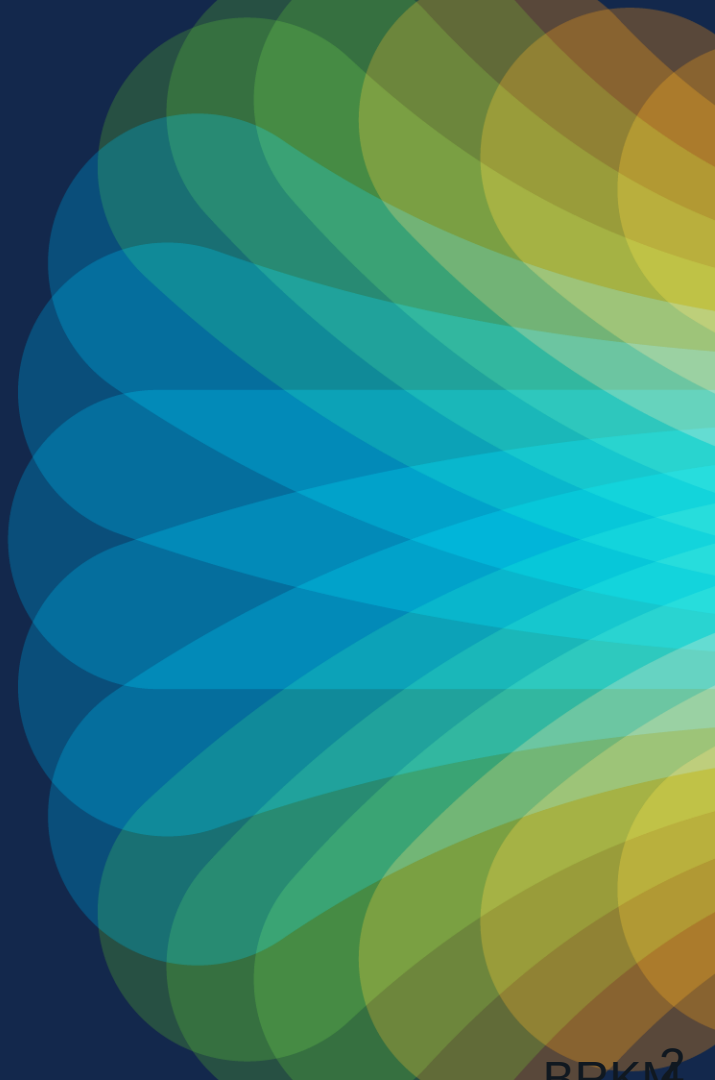
```
segment-routing
 traffic-eng
 policy srte_pcc_node5_node4
  color 700 end-point ipv4 198.19.1.4
  candidate-paths
   preference 100
    dynamic
     pcep
     !
     metric
      type te
```

PCC configured

```
pce
 segment-routing
  traffic-eng
   peer ipv4 198.19.1.5
    policy srte_pce_node5_node4
     color 701 end-point ipv4 198.19.1.4
     candidate-paths
      preference 100
       dynamic mpls
        metric
         type te
```

PCE configured

Automation Considerations



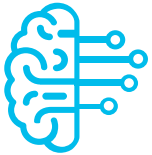
SDN for transport networks

Automated Transport Service Provisioning – VPNs

Operational Assist – Visualization and Dashboards

Service Health monitoring/Assurance

Traffic Engineering for fine grained SLAs



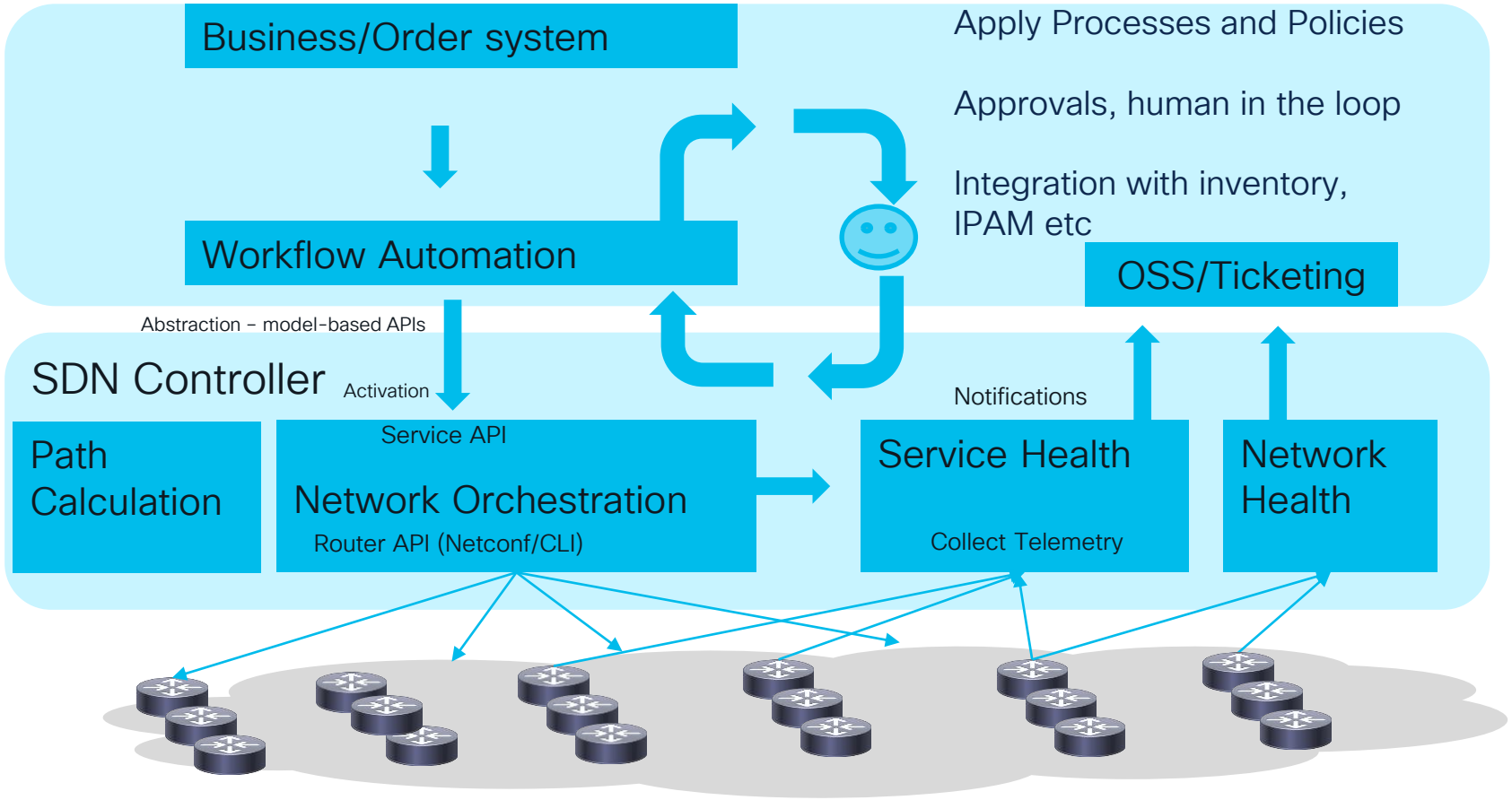
Real Time Automated Optimization – maintain SLAs under changing conditions

Bandwidth aware path calculation and Congestion Mitigation

Network Operations and Automation

- Day 0 – Zero Touch Provisioning ZTP (IETF RFC 8572)
- Day 1 – Config and Image Compliance, commissioning, integration
- Day 2 – In Service operations
  - Service Life Cycle Create, Update & Delete
  - Monitor Service Health
  - Monitor Network Health, Fault and Performance, Fault Auto remediation
  - Optimization – short term, avoid BW congestion, hot spots etc
  - compliance and planned maintenance config
- Planning – Mid/Long Term capacity planning, collect traffic trends

Service Life Cycle Workflow

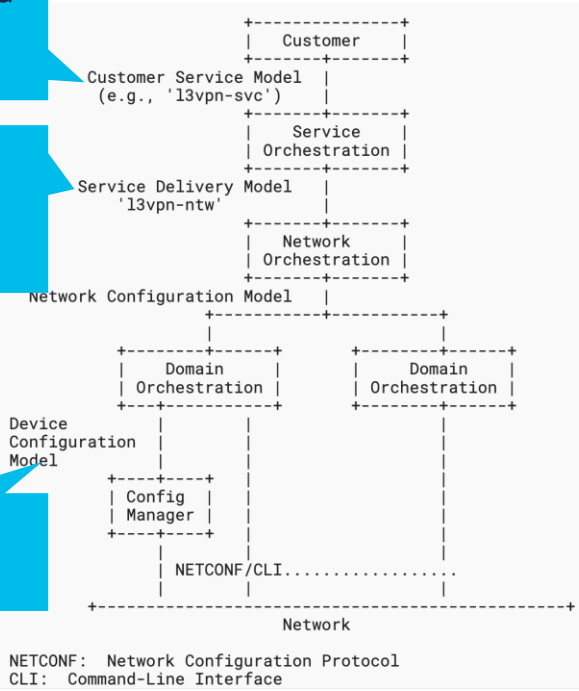


Models to abstract layers – standardization

RFC 8299 YANG Data Model for L3VPN Service Delivery

RFC 9182 A YANG Network Data Model for Layer 3 VPNs

Device Yang models Openconfig or native



Reference: RFC 9182 Figure 1

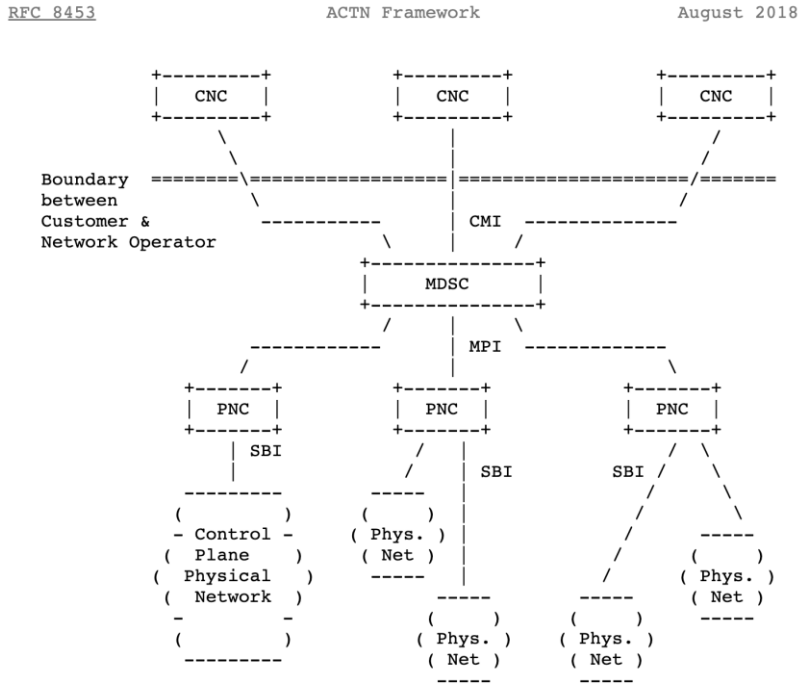


Figure 2: ACTN Base Architecture

Reference: RFC 8453

Reference to IETF Standards/Drafts for models

- RFC 8466: A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery
- RFC 9291: A YANG Network Data Model for Layer 2 VPNs
- RFC 8453 Framework for Abstraction and Control of TE Networks (ACTN)
- RFC 8299 YANG Data Model for L3VPN Service Delivery
- RFC 9182 A YANG Network Data Model for Layer 3 VPNs
- IETF Draft Network Slice Service YANG Model

Crosswork Network Controller

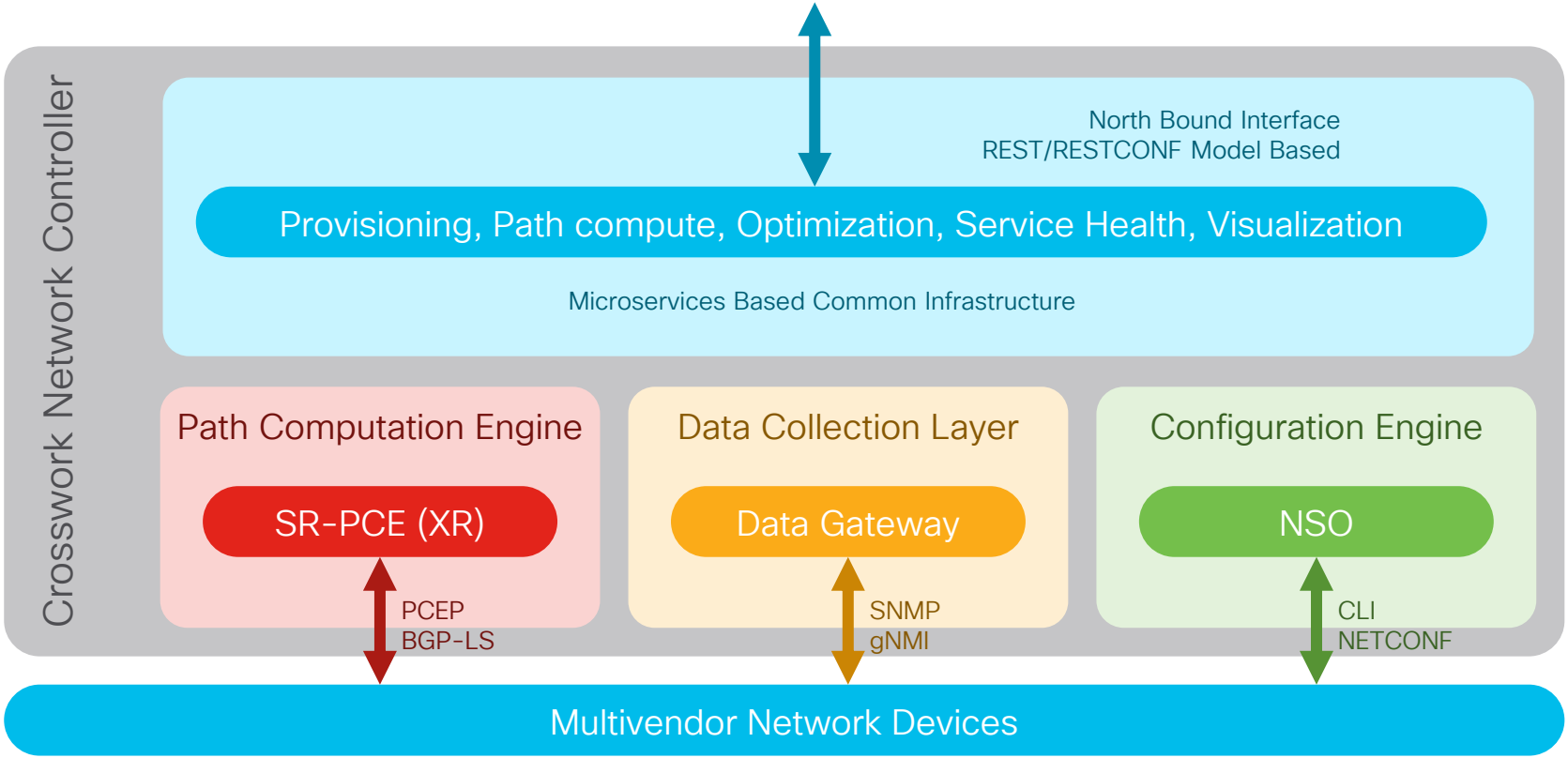
SDN Controller for Transport networks

Crosswork Network Controller (CNC)

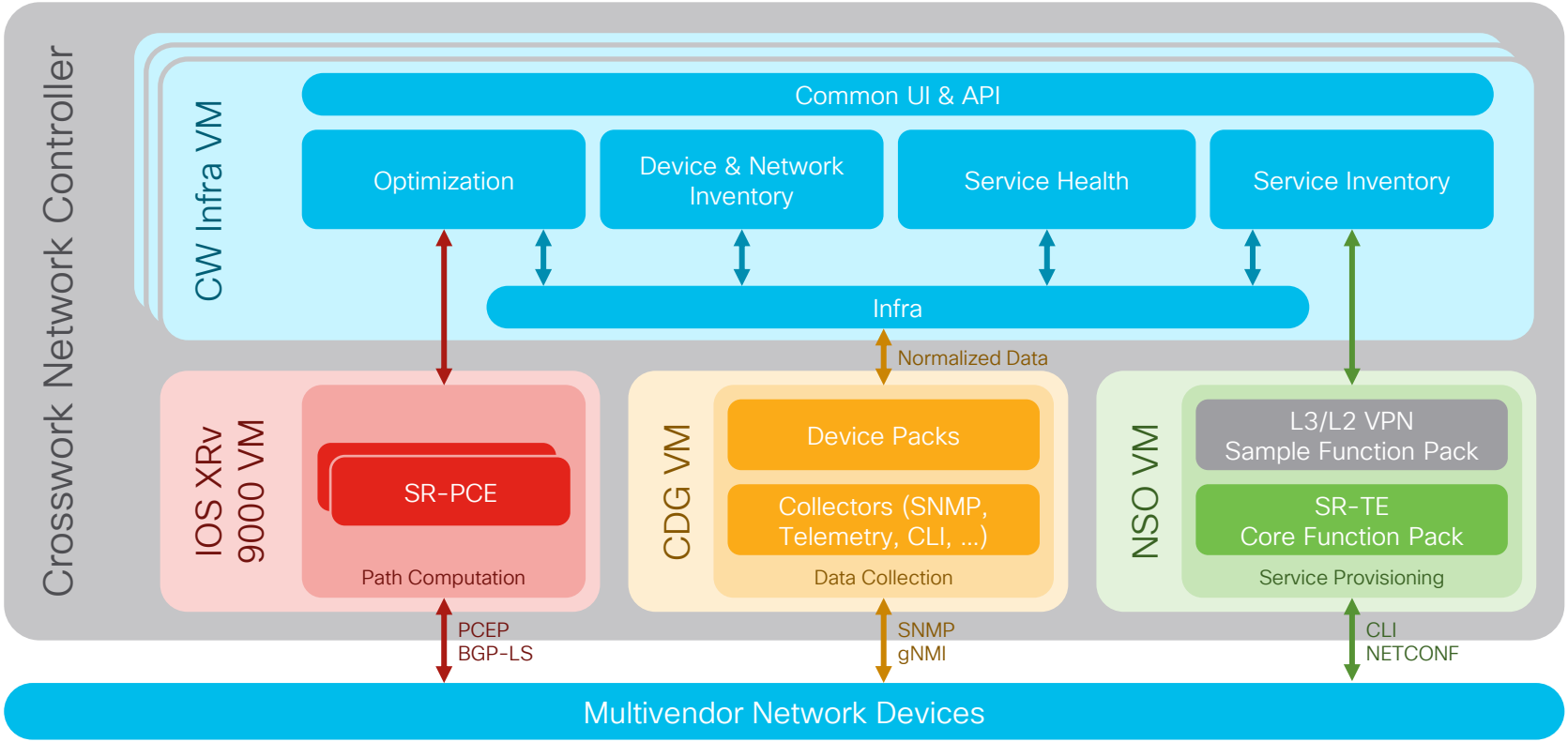
Automation solution for deploying and operating IP transport networks

Intent-based Automated Provisioning	Service Provisioning (L2VPN, L3VPN)	Service-Oriented Transport Provisioning (SR-MPLS, SRv6, RSVP-TE)		
Dynamic Traffic Engineering	Bandwidth-Aware Path Control	Flexible Algorithm	Local Congestion Mitigation	
Closed Loop Automation	Real-time Network Optimization			
Integrated Service Lifecycle Management	Visualization	Path Calculation	Service Health Monitoring	Network State Monitoring

Crosswork Network Controller – Architecture

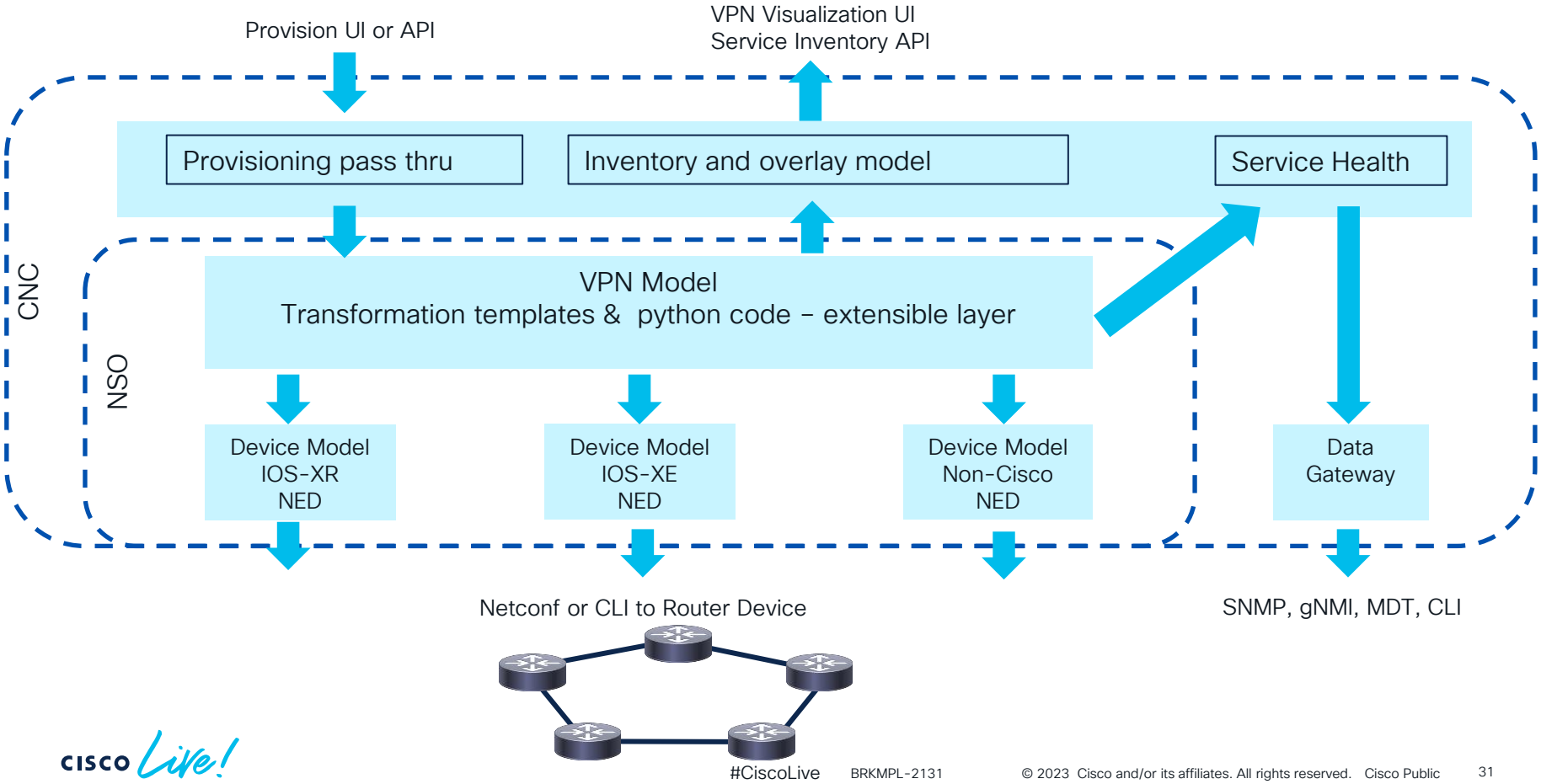


Crosswork Network Controller – Architecture



Provisioning

Looking under the hood



Industry's Broadest Multivendor Support

Reference

Over 170 Supported NEDs – Customization Available

Extensibility & Flexibility

IETF Based VPN Model

Extend & implement NSO Template and CNC UI

Pre-existing NSO VPN Deployments

Integration with CNC

Multi-vendor support

NSO template and mapping code

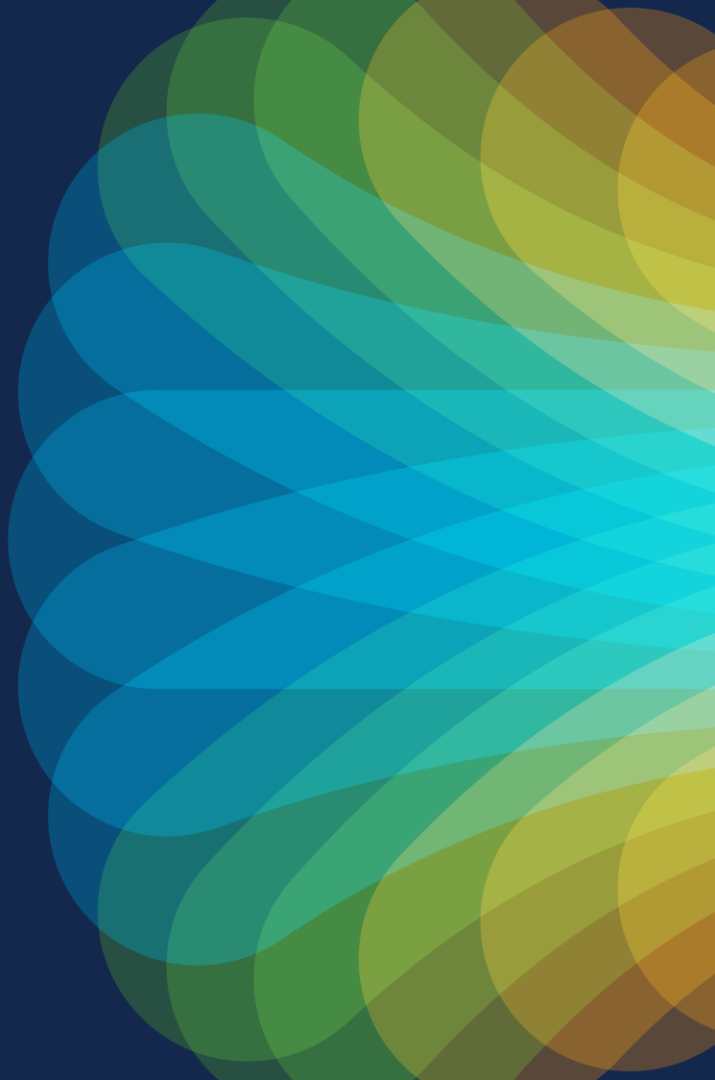
Extend as needed, starting from Cisco XR/XE out of box

Test and validation

Presentations on extensions and multivendor support:

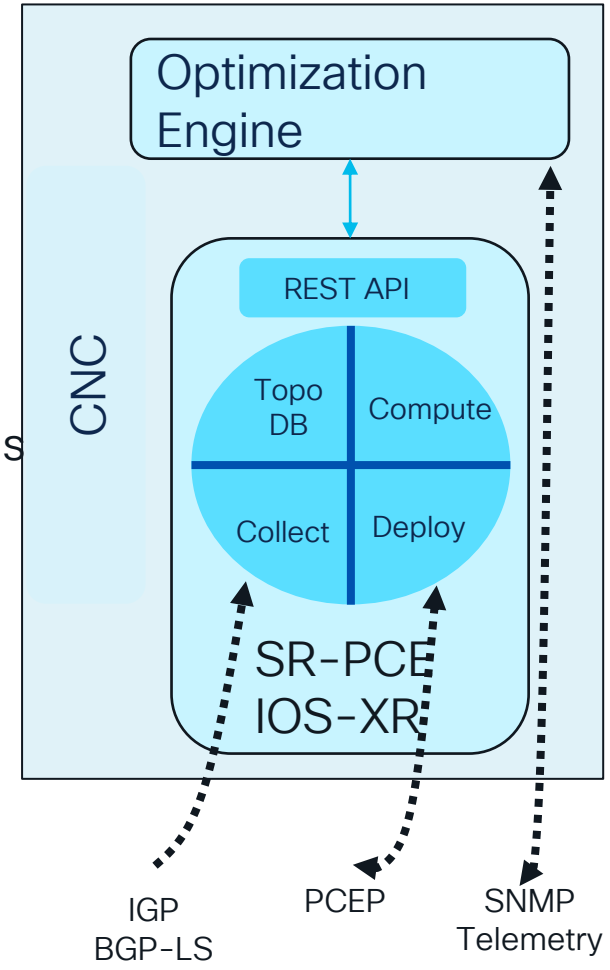
Adapting VPN to CNC: https://community.cisco.com/t5/nso-developer-hub-documents/automationdevdays22-cnc-nso-service-customization-nbsp/ta-p/4614587
Multi Vendor support: https://community.cisco.com/t5/nso-developer-hub-documents/automationdevdays22-cnc-multi-vendor-non-cisco-device/ta-p/4614579

Path Control & Optimization

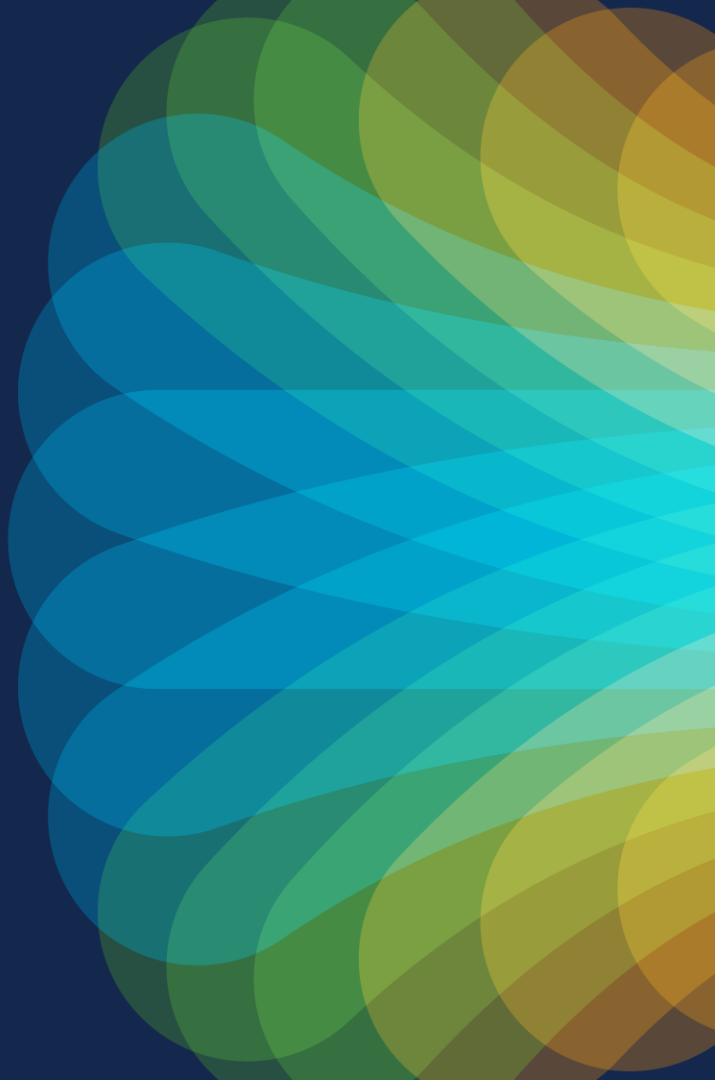


CNC Path Computation

- SR-PCE – IOS-XR based
  - IOS XR: Any Cisco XR router or XR9000v
  - Multi-domain: Real-time feed via BGP-LS/IGP
  - Stateful: updates SR-Policies when required
  - SR PCE: native SR-optimized computation algorithms computes inter-area/domain/AS paths
  - Real time optimization – always on closed loop
- Crosswork Optimization Engine
  - Visualization and UI/API
  - Bandwidth aware path calculation
  - Builds Traffic Model via Telemetry
  - Internal API integration with Cisco SR-PCE XR



Service Health



CNC Service Health Architecture

Uses Service Assurance for Intent Network concepts – IETF Draft

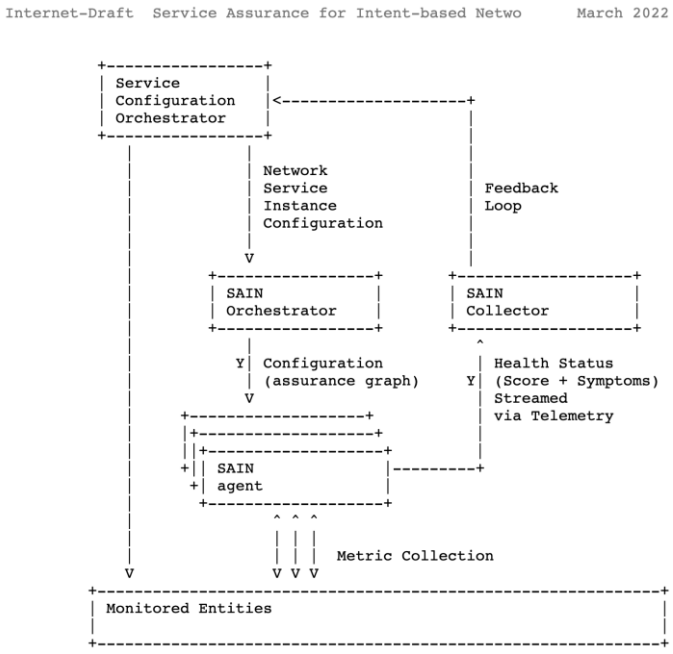
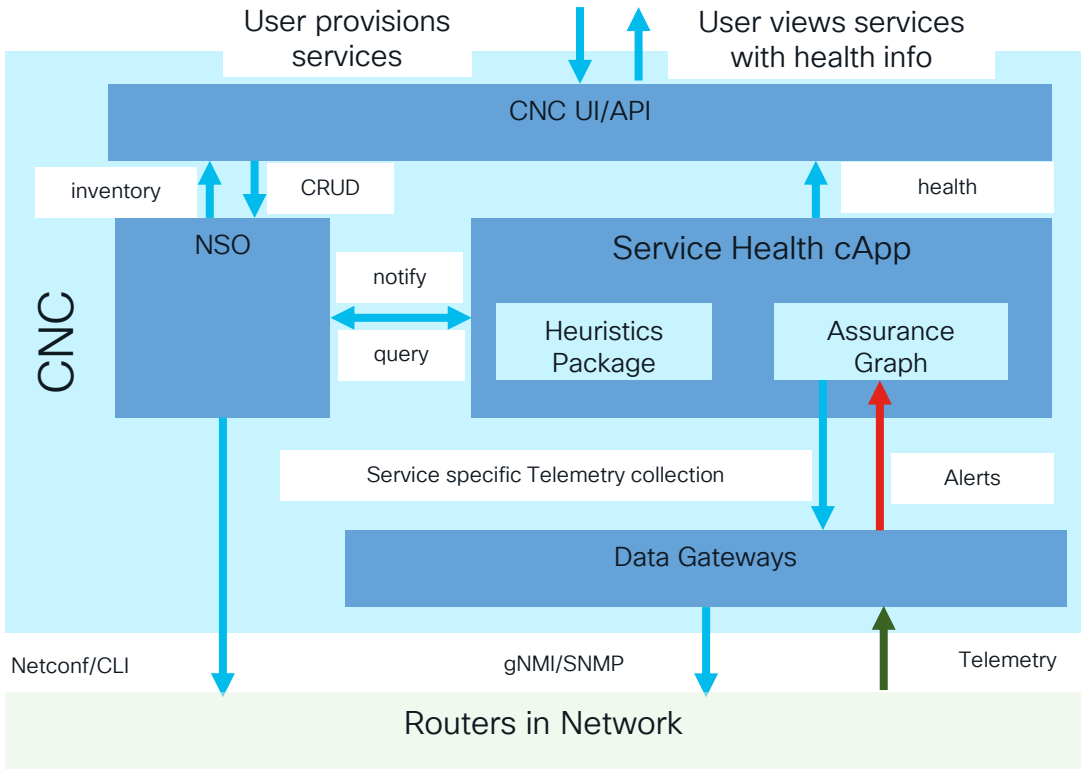


Figure 1: SAIN Architecture



From Heuristic Package to Assurance Graph

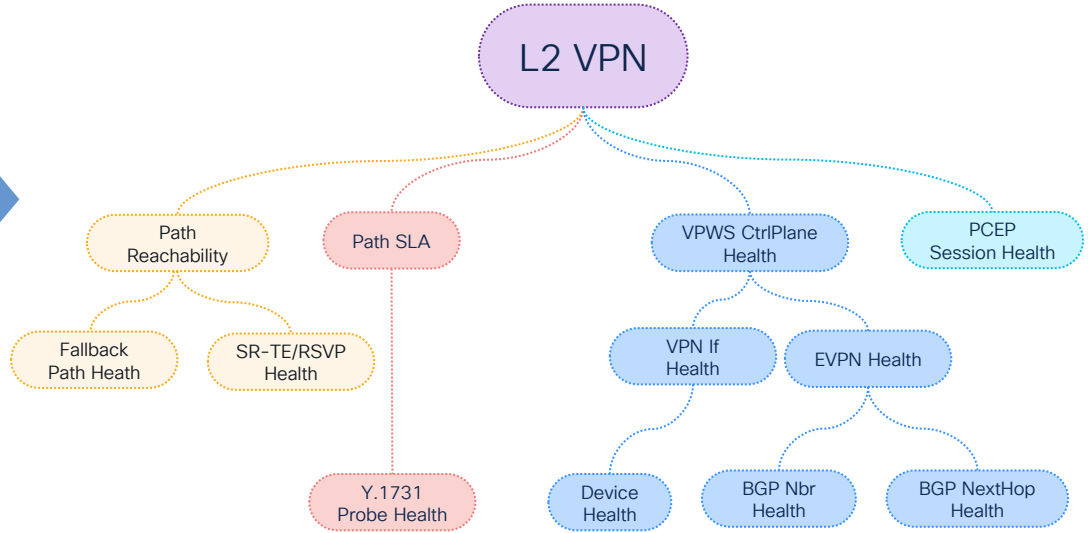
NSO Service and Device Configuration

Services

Subservices

Expressions

Metric



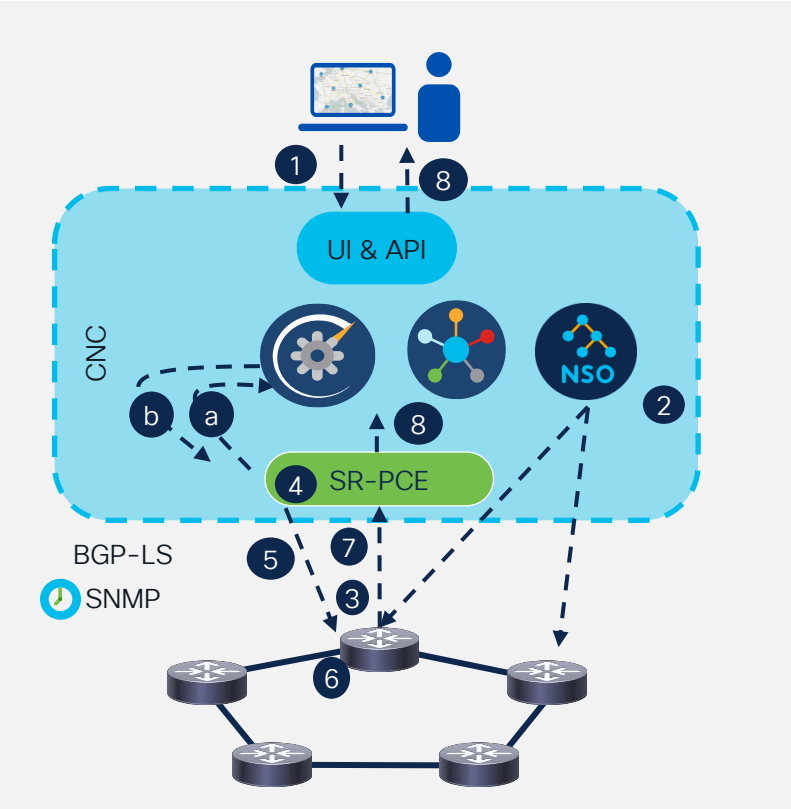
Demo Scenarios

- SR-TE Visualizations – low latency, disjoint and BWoD
- Create SR-TE Policy with affinity and visualize
- View L2VPN VPWS Service and path between PE
- Update L2VPN VPWS service to use SR-TE Policy with Affinity.
- Create L3vpn service with traffic going via low latency paths
- Service health monitoring for above two services

Demo

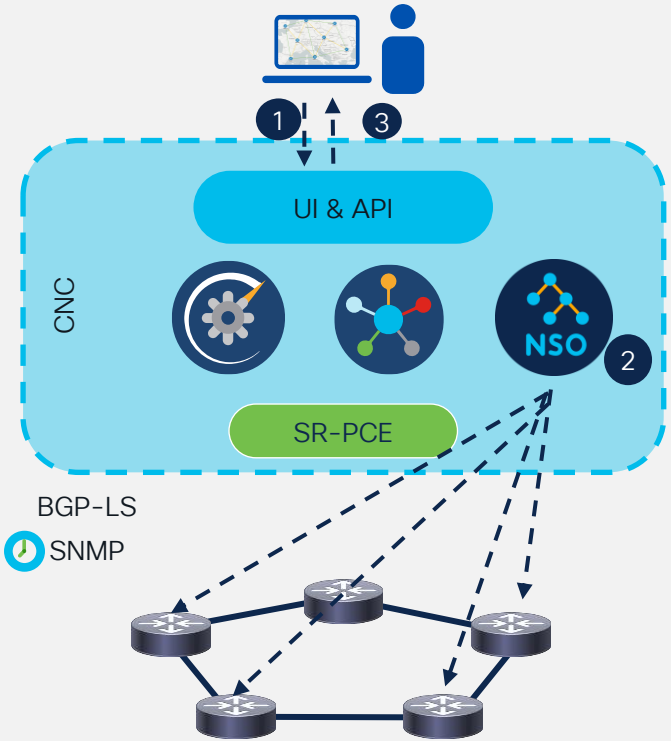
Service Provisioning – SR TE Services

Reference



1. User requests SR policy via UI or API
2. CNC/NSO calculates device configurations for SR-TE service, pushes it to headend devices.
3. Headend - PCEP Path Request to SR-PCE
4. SR-PCE calculates the Path or delegates
   a. If the path constraint includes bandwidth SR-PCE delegates to CNC/Optimization Function
   b. CNC/Optimization returns path
5. SR-PCE returns the calculated Path via PCEP
6. Headend uses the Path and brings up SR POLICY and forwarding
7. Headend sends a PCEP Path Report to SR-PCE on the path being used.
8. CNC provides visualization of policies and paths

Service Provisioning – VPN Services



1. User requests VPN service with SR policy
2. CNC/NSO calculates device configurations for VPN service & associated policies, pushes it to PE devices.
3. CNC visualization of VPNs & associated TE underlay paths
4. Additional transport visualization if VPN is bound to a SR Policy or RSVP-TE Tunnel.

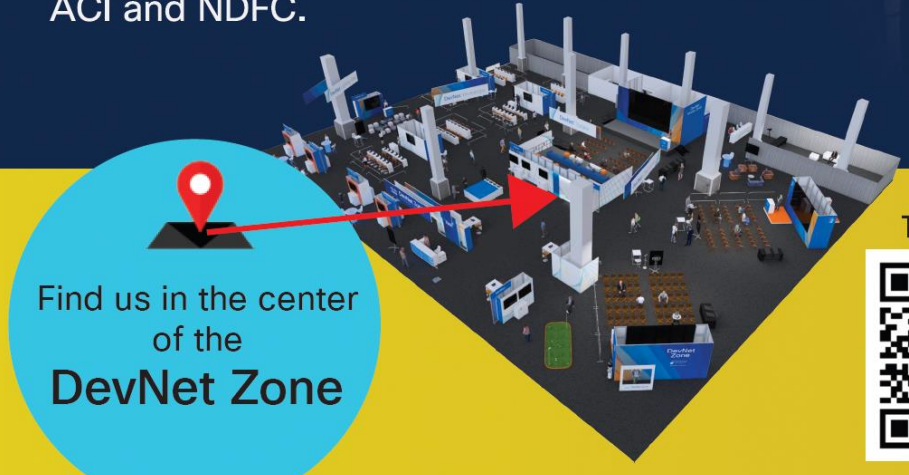
Cisco
Developer

Cisco
DSE Automation

Visit us at ‘Share Your Experience’

Booth #214 in the DevNet Zone

Win prizes by participating in hands-on activities about API quality, developer experience, and insights while working with Crosswork Network Controller, ACI and NDFC.



Find us in the center of the **DevNet Zone**

Take one of these survey and collect the prize at the booth

CNC

ACI

NDFC

Sessions with Crosswork and Assurance

- Not So Trivial Pursuits: How to Assure IP Networks Today and In The Future - IBOSPG-1205
- Reduce Resolution Time with a Service-Centric Approach to Troubleshooting BRKSPG-2474
- Design, Deploy and Manage Transport Slices using SDN Controller and Assurance - BRKSPG-2263
- Simplify your journey to SR and SRv6 with Crosswork Automation - BRKSPG-2043
- Cisco Crosswork Network Controller Integration with External Systems using API's - DEVLIT-2839
- Crosswork Network Controller integration with Service Now for Closed Loop Remediation - DEVWKS-2290

Cisco Webex App

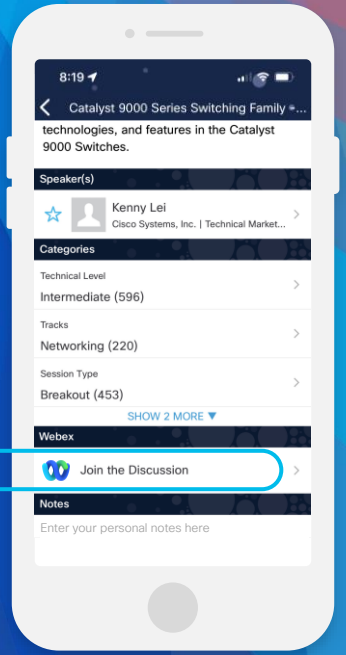
Questions?

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 9, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMPL-2131

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

The bridge to possible

Thank you

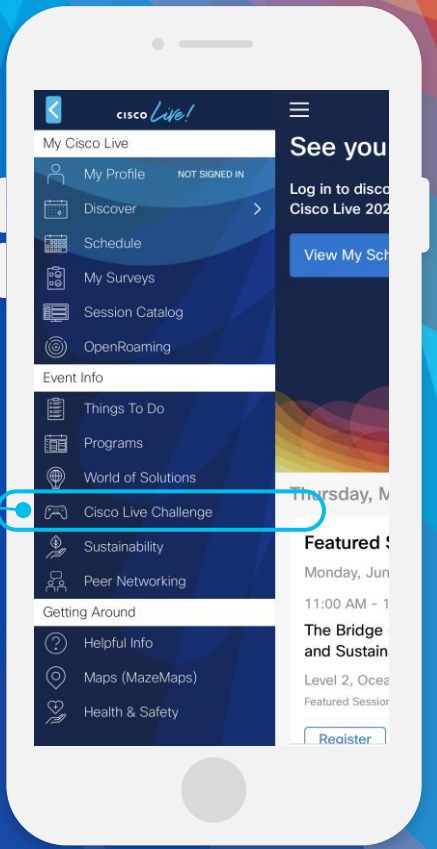
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive