The bridge to possible

Deploying VPNs over Segment Routed Networks Made Easy

SDN Controller based approach

Krishnan Thirukonda, Principal Engineer
@KrishThirukonda

BRKMPL-2131

cisco Live!

Cisco Webex App

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

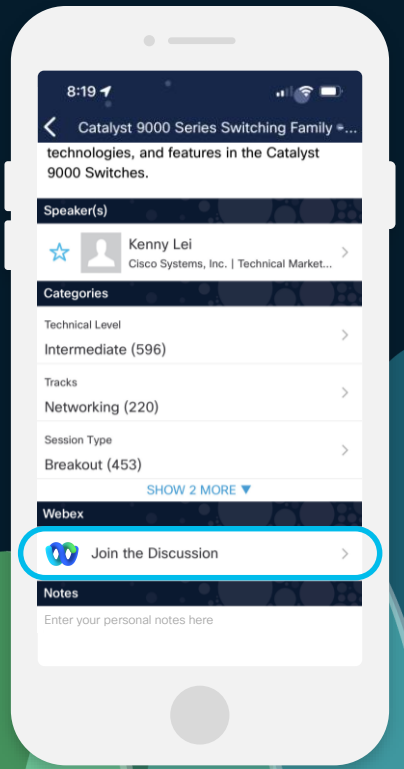
Questions?

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

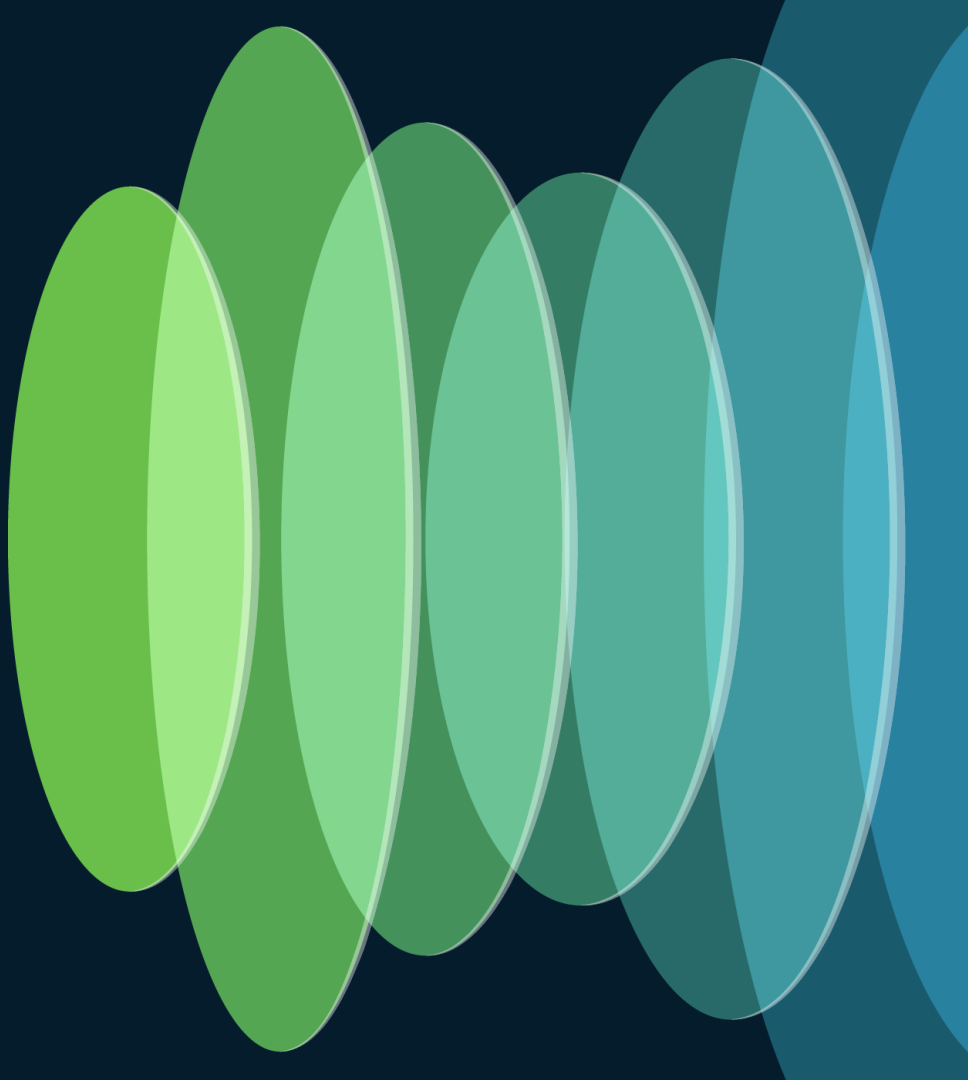
Webex spaces will be moderated by the speaker until June 7, 2024.



Agenda

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

Technology Review



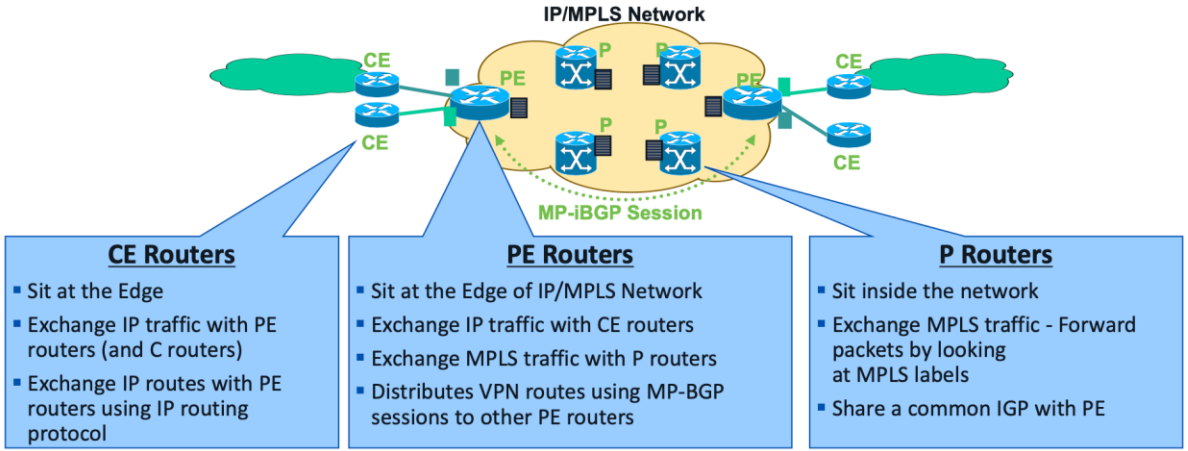
Services provided to end customers

- L2 and L3 VPNs
  - Overlay services over common IP/MPLS core or IPv6
  - Provides private networks with separation
  - Examples: BGP L3VPNs, EVPN or legacy
- Internet access
- Multicast Transport – Content Delivery, MVPN etc
- Private Line Emulation (PLE)

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
   !
  !
```

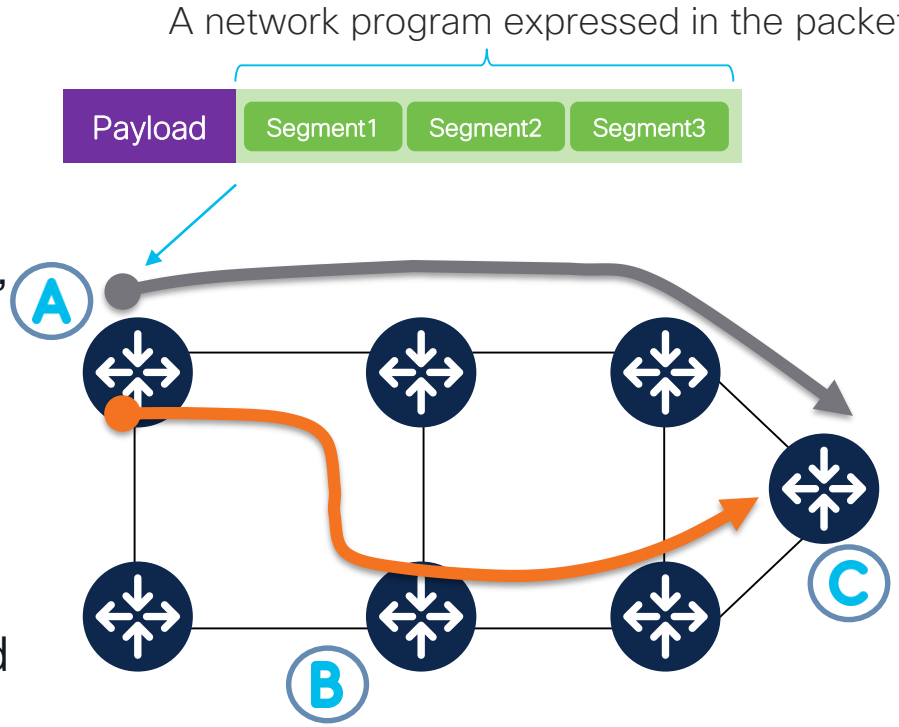
Transport paths in network

- Best Effort service uses IGP routing
- Large scale networks have multiple IGP domains with BGP Labelled Unicast (BGP-LU) or BGP-SR.
- Traffic Engineering for granular SLAs or tactical traffic management
  - RSVP-TE (MPLS Core)
  - SR-TE (MPLS Core)
  - SRv6 (IPv6 Core)

This focus in this session is on Segment Routing

What is Segment Routing?

- Source Routing principle => packets carry the path information
- An ingress node steers a packet through an ordered list of instructions, called segments
- A segment is locally defined and executed at a specific location in the network
- A segment can represent ANY function, topological or service-based or user-defined



One Architecture / Two Data-Plane instantiations

Segment Routing

SR-MPLS

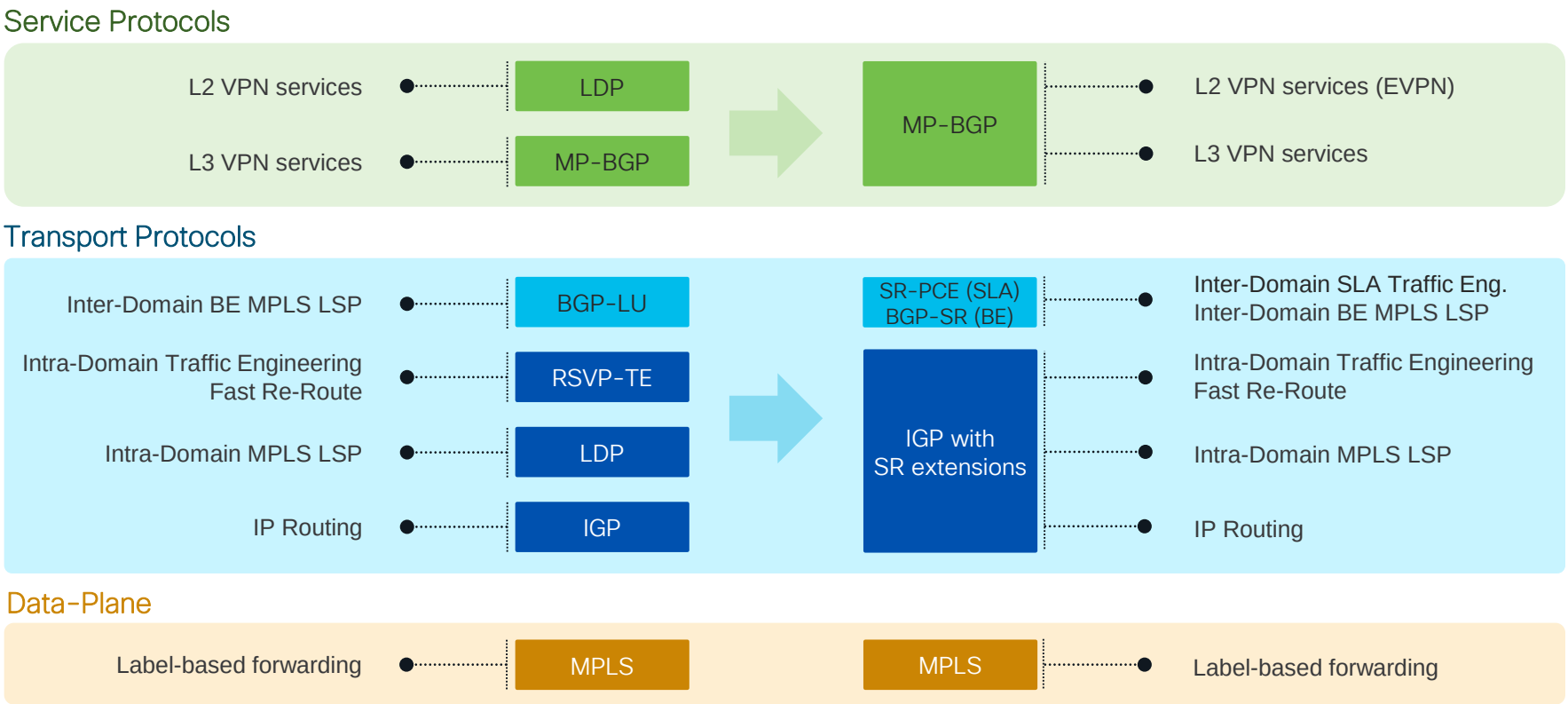
- Instantiation of SR on the MPLS data plane
- A segment is encoded with an MPLS label

SRv6

- Instantiation of SR on the IPv6 data plane
- One or more segments are encoded with an IPv6 address

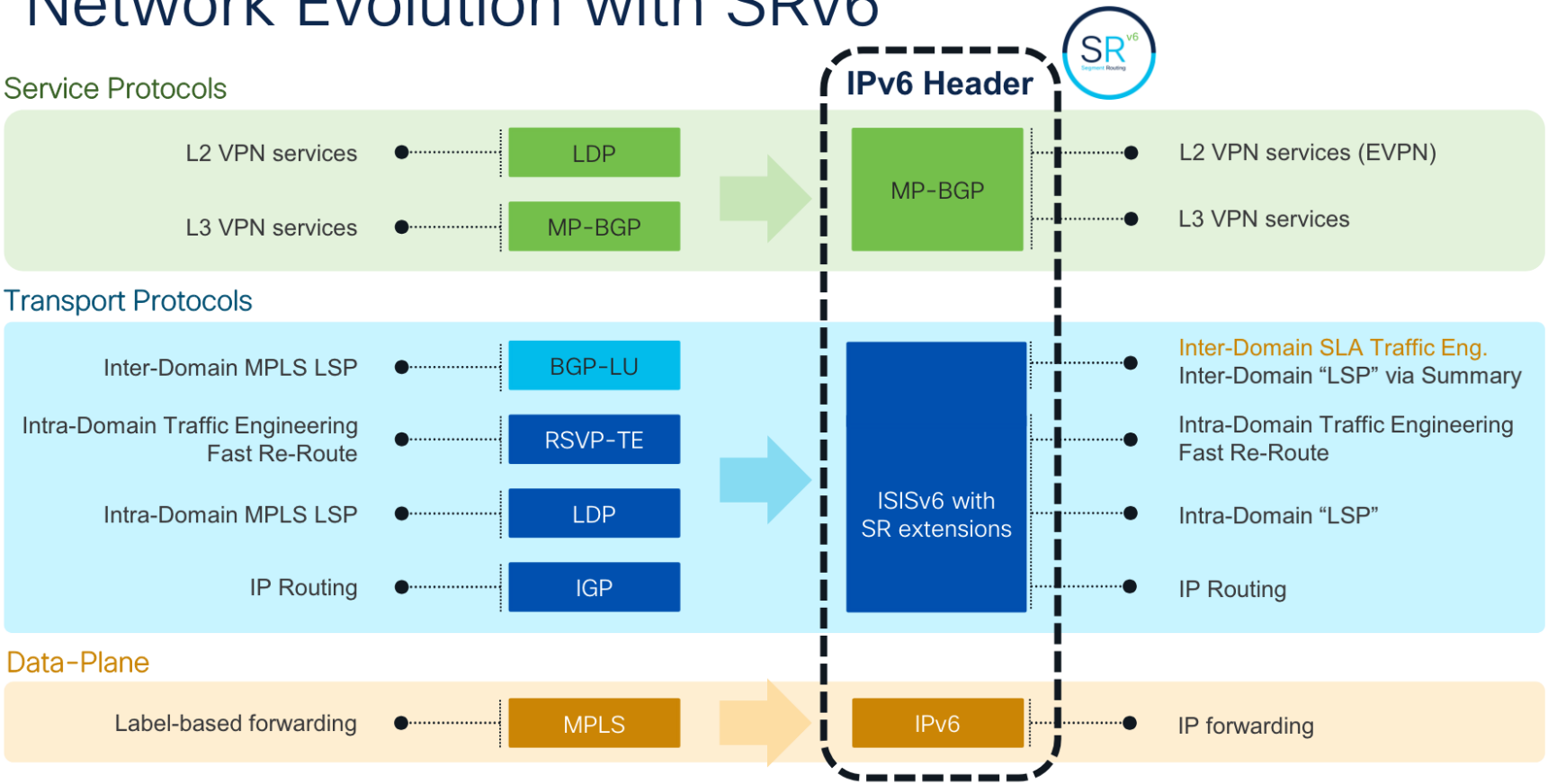
Refer: BRKSPG-2510 for deep dive of segment routing

Network Evolution with SR-MPLS



LDP: Label Distribution Protocol, **MP-BGP**: Multi-protocol BGP, **BGP-LU**: BGP Labeled-Unicast, **PCE**: Path Computation Element, **RSVP-TE**: Reservation Protocol Traffic Engineering

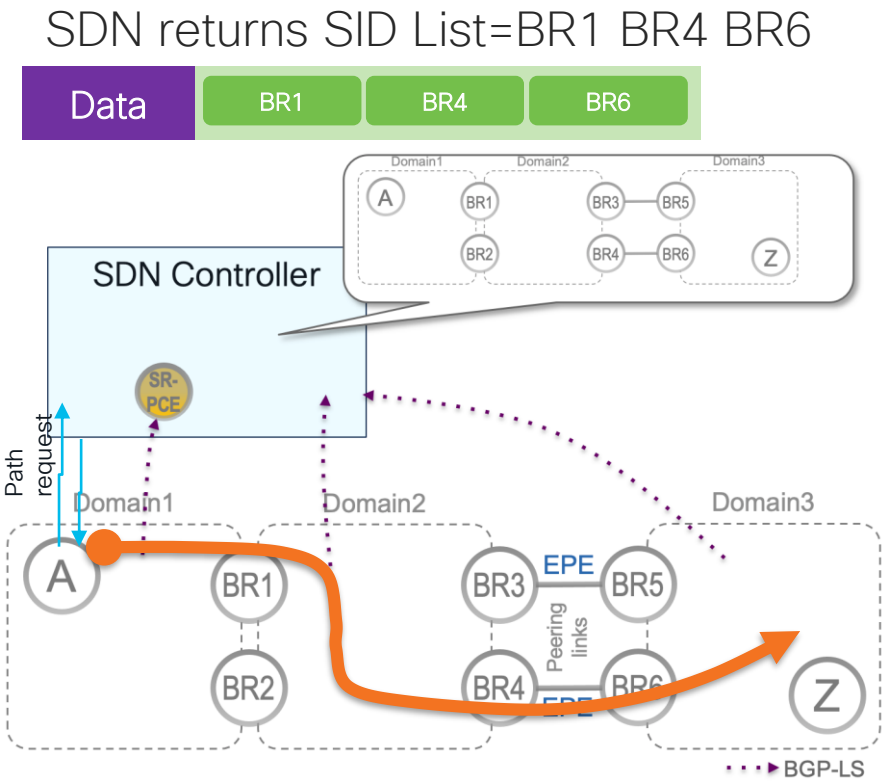
Network Evolution with SRv6



LDP: Label Distribution Protocol, **MP-BGP**: Multi-protocol BGP, **BGP-LU**: BGP Labeled-Unicast, **RSVP-TE**: Reservation Protocol Traffic Engineering

Programmability enabled by Segment Routing

- Underlay paths can be “programmed” on SR Networks
- Paths are SID Lists and computed based on different intent criteria
- Intent Examples: Low Latency Path, disjoint path, encrypted links only paths, BW available paths
- Inter-domain path calculation uses external path computation element, routers delegate path calculation to external path calculation engines
  - External path calculation engines use BGP-Link State to learn topologies from all IGP domains
  - Bandwidth Awareness using Telemetry
- Enables Software Defined Networking for Transport Networks to provide fine grained control



SR Traffic Engineering

- Simple, Automated and Scalable
  - No core state: state in the packet header
  - No tunnel interface: “SR Policy”
  - uniquely identified by a tuple (head-end, color, end-point)
    - Resolved to a SID List
  - On-demand policy instantiation & automated steering
- Multi-Domain
  - SR PCE for compute
  - Binding-SID (BSID) for scale

Reference

```
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

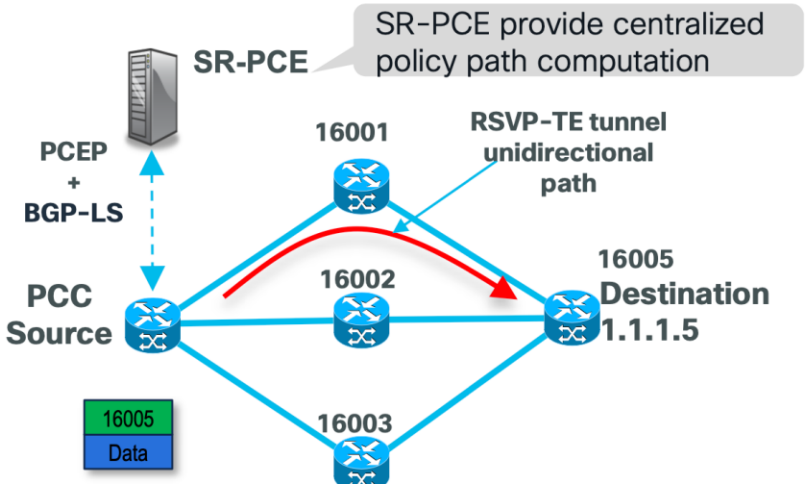
```
pce
 segment-routing
  traffic-eng
   peer ipv4 198.19.1.5
    policy srte_pce_node5_node4
     color 701 end-point ipv4 198.19.1.4
     candidate-paths
      preference 100
       dynamic mpls
        metric
         type te
```

PCE configured

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



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
  - Dynamic, locally calculated
  - Dynamic, PCE delegated
- Policy instantiation
  - Static OR 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

Service (VPN) To TE path binding & Steering

- SR-Policy: uniquely identified by a tuple (head-end, color, end-point), resolves to a SID-List to reach end-point w SLA
- Static Binding. Works well for p2p services
  - SR-Policy (headend => endpoint, color) is configured on PEs.
  - L2VPN with preferred-path <sr-policy name> in IOS-XR
- Route Policy to Color VPN Prefixes,
  - ODN templates to map colors to Service Level Objectives and Constraints.
- SRv6/FlexAlgo locators as next hop – VPN configurations extended

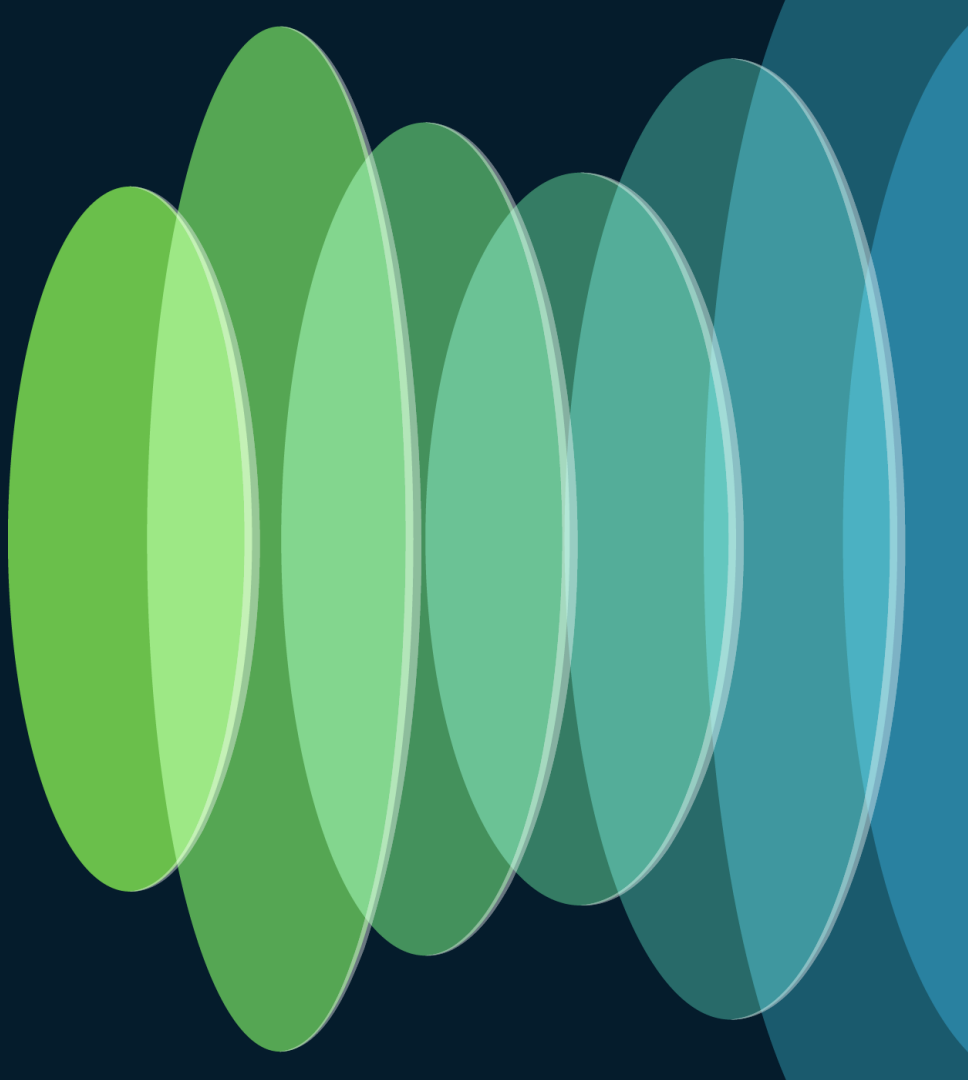
SR Policy pull model: On-Demand Nexthop (ODN)

- E1 maps color BLUE to the low-delay intent using a configured Template
- Upon receiving a service route via E2 with color BLUE, E1 automatically instantiates the SR Policy (E2, BLUE) which is resolved to a SID-List using path calculation.
  - This is called On-Demand Next-hop (ODN)
  - Each PE installs only the SR Policies that it needs
- E1 steers the traffic for prefix W/w onto SR Policy (E2, BLUE)

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

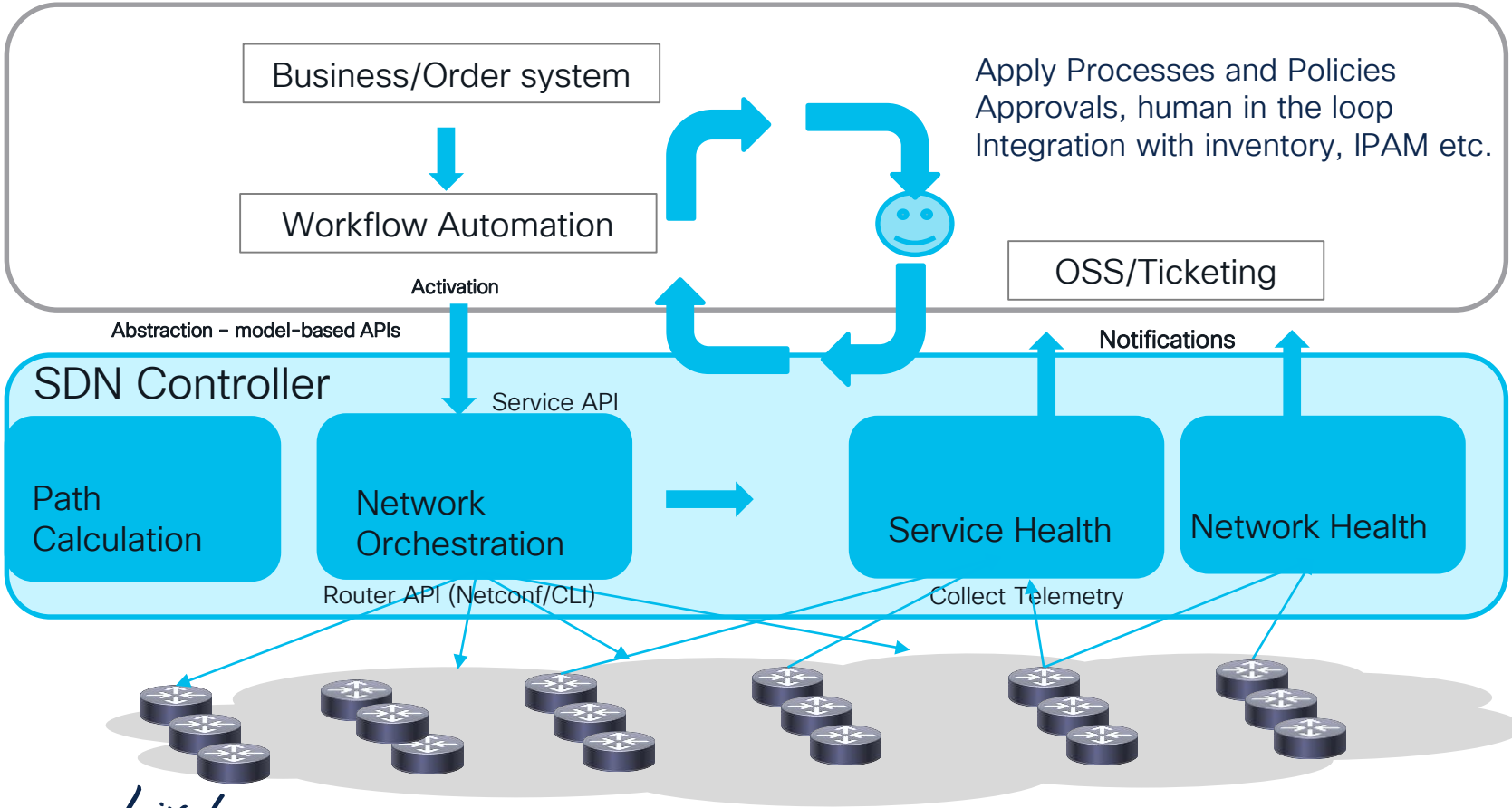
Automation Considerations



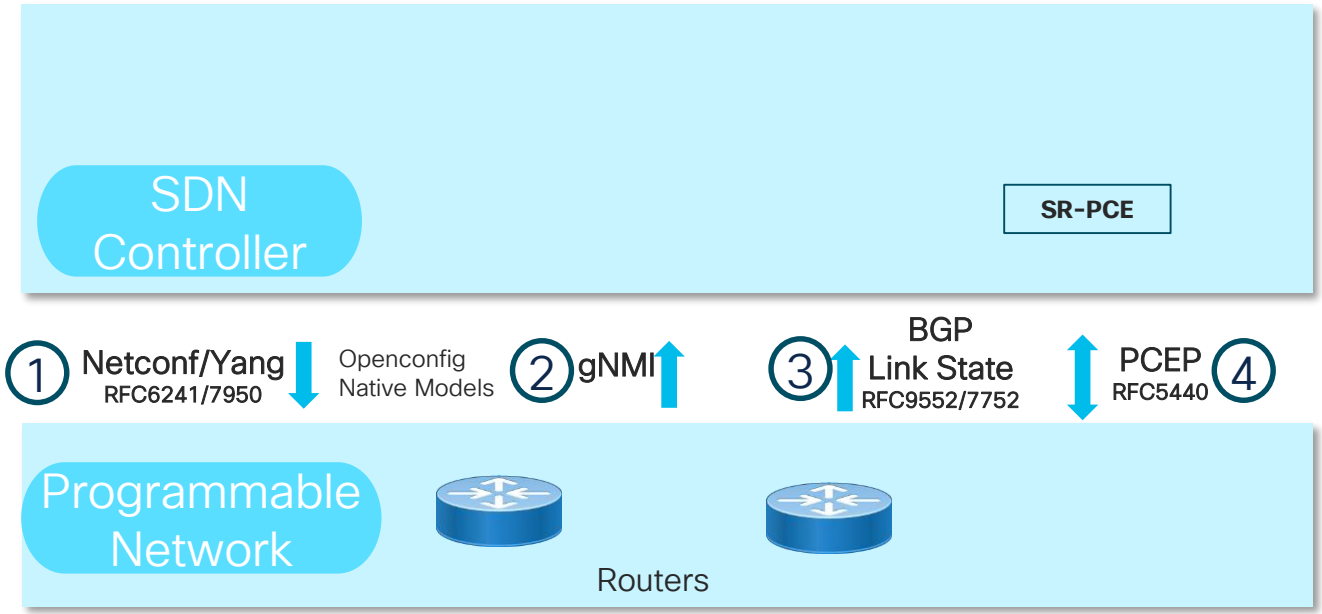
Different areas of automation

- Planning – Mid/Long Term capacity planning, update traffic trends
- 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, Maintenance, upgrades
  - Optimization – short term, avoid BW congestion, hot spots etc
- Fragmented solutions reduce efficiency, need integrated solution

Automation with SDN Controller



IP Domain SDN Controller South Interfaces



1. Netconf/Yang for configuration
2. gNMI (or SNMP) for Telemetry
3. BGP Link State for Topology information
4. PCE Protocol (PCEP) for path request/report

IP Domain SDN Controller – North Bound Interface

UI & Restconf/Yang API
RFC6040/7950

Restconf/Yang notifications, Kafka, gRPC, REST, Syslog, TRAP

L3NM
RFC 9182

Slice
draft-ietf-teas-ietf-network-slice-nbi-yang

L3NM
RFC9182

L2NM
RFC9291

Topology
RFC8345+

SAIN
RFC9417

PCE

SDN Controller

Netconf/Yang
RFC6241/7950

Openconfig
Native Models

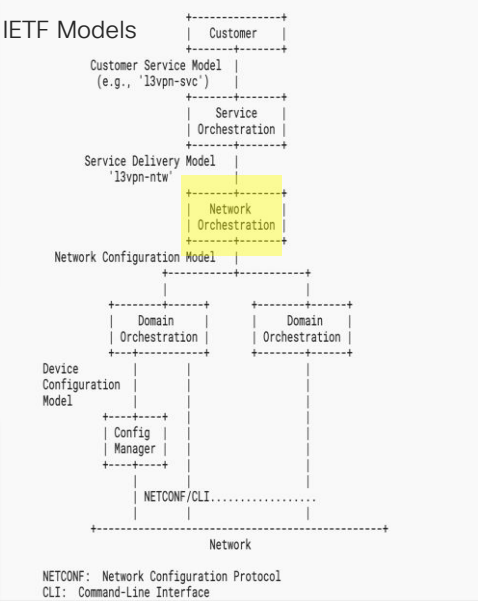
gNMI

BGP
Link State
RFC9552/7752

PCEP
RFC5440

Programmable Network

Routers



SDN Standardization Efforts

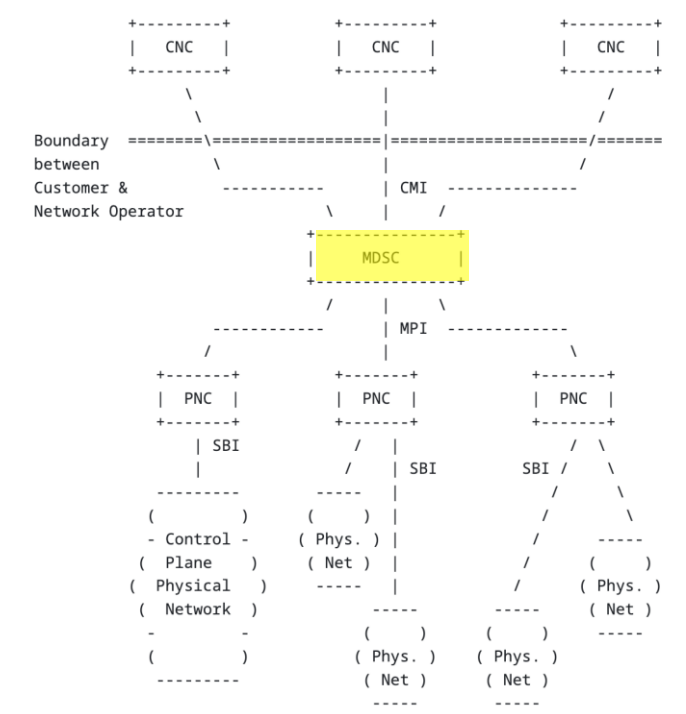


Figure 2: ACTN Base Architecture

Mandatory Use Case Requirements for SDN for Transport (MUST)

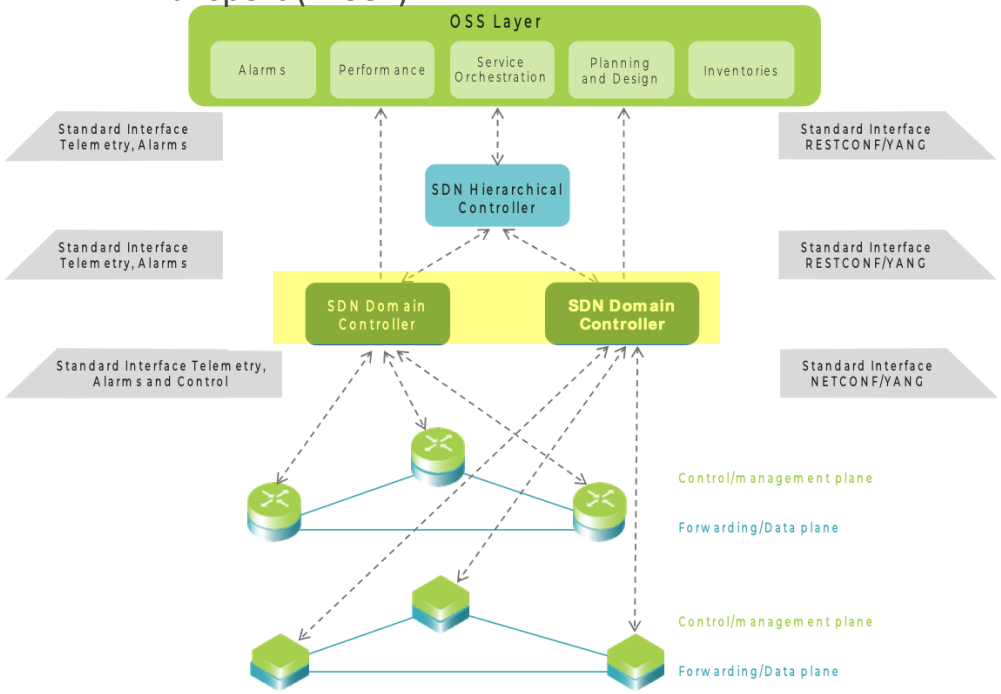


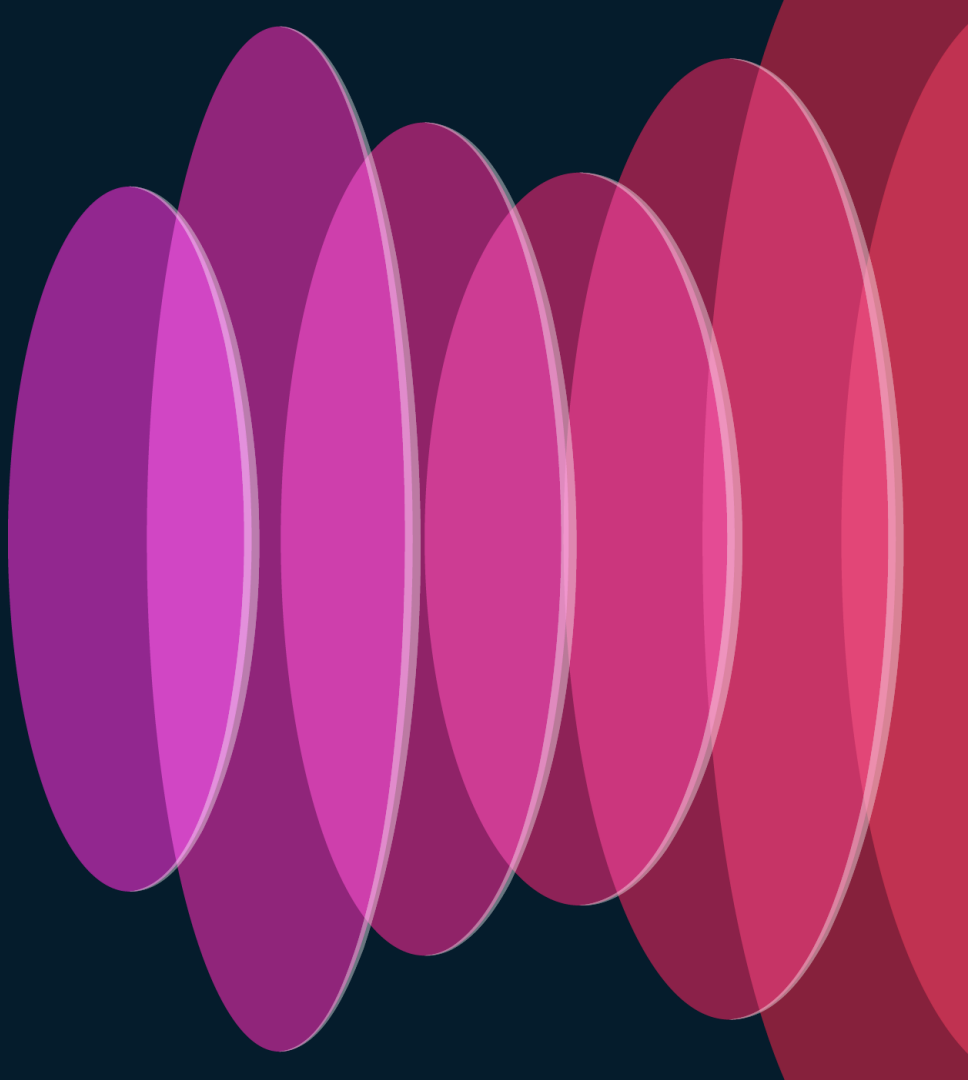
Figure 1: MUST general Hierarchical SDN architecture

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



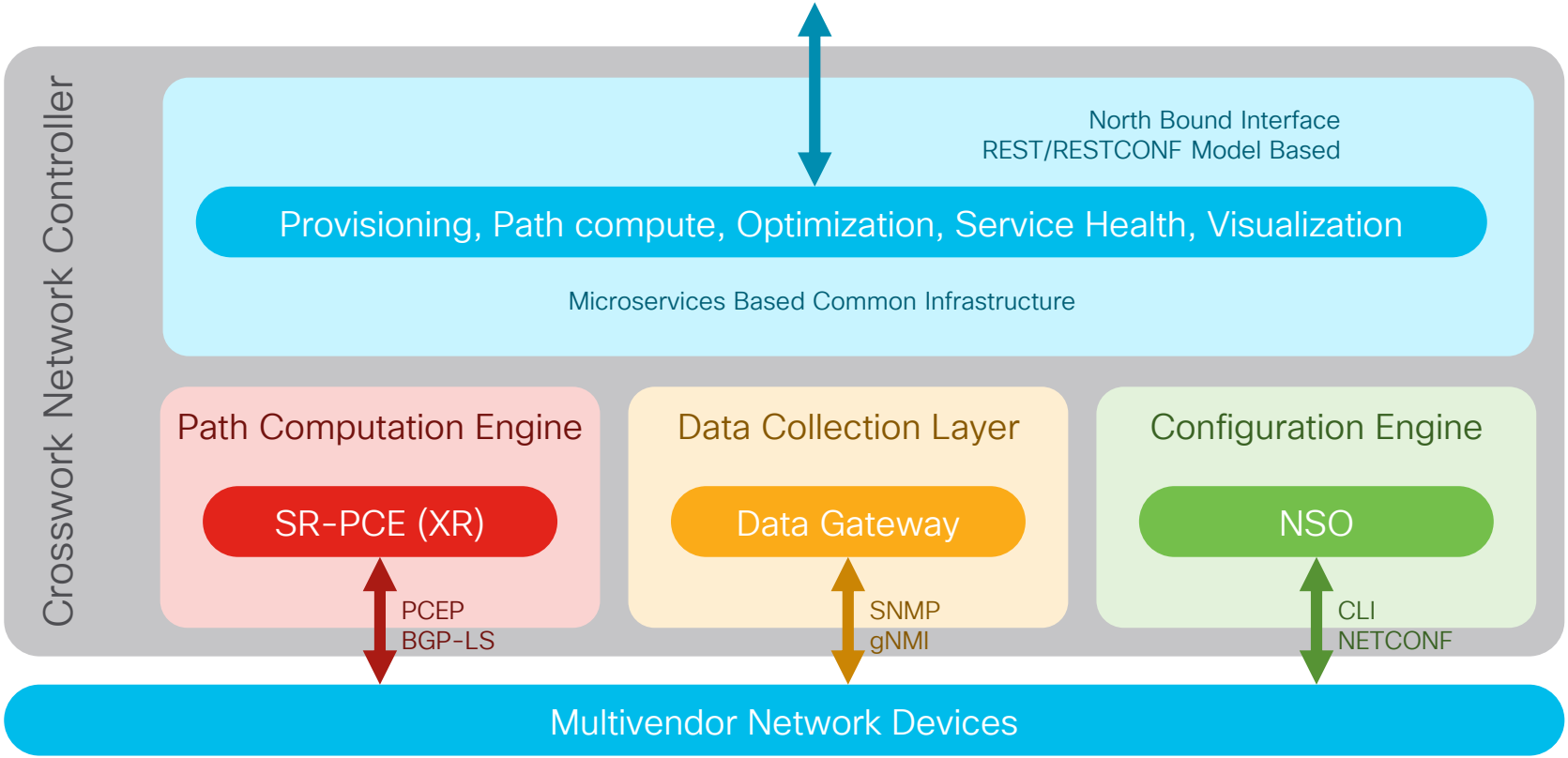
cisco Live!

Crosswork Network Controller (CNC)

Automation solution for deploying and operating IP transport networks

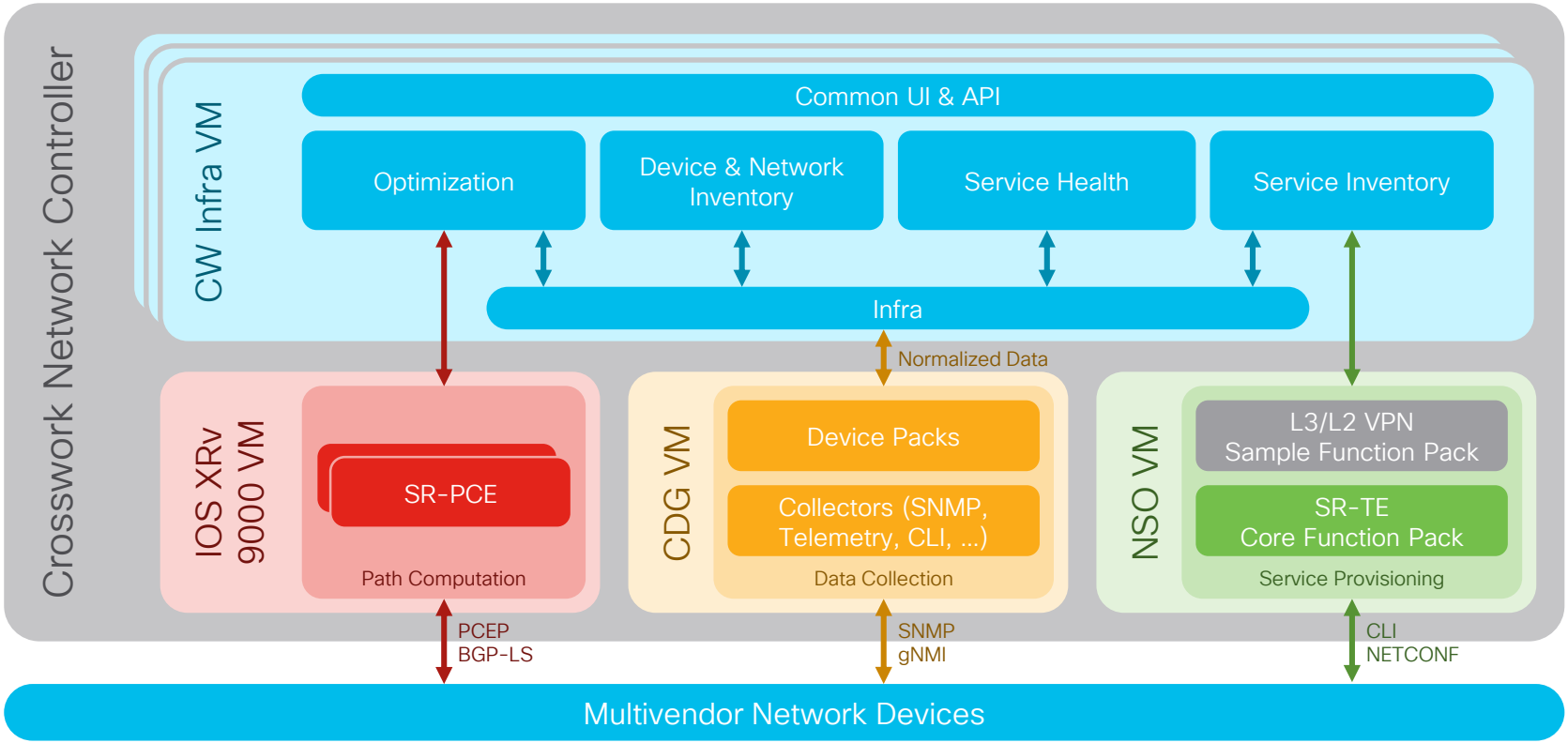
Intent-based Automated Provisioning	Service Provisioning (L2VPN, L3VPN)	Service-Oriented Transport Provisioning (SR-MPLS, SRv6, RSVP-TE)		
Dynamic Traffic Engineering	Bandwidth-Aware Path Control	Flexible Algorithm	Local Congestion Mitigation	
Closed Loop Automation	Real-time Network Optimization			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

Crosswork Network Controller – Architecture

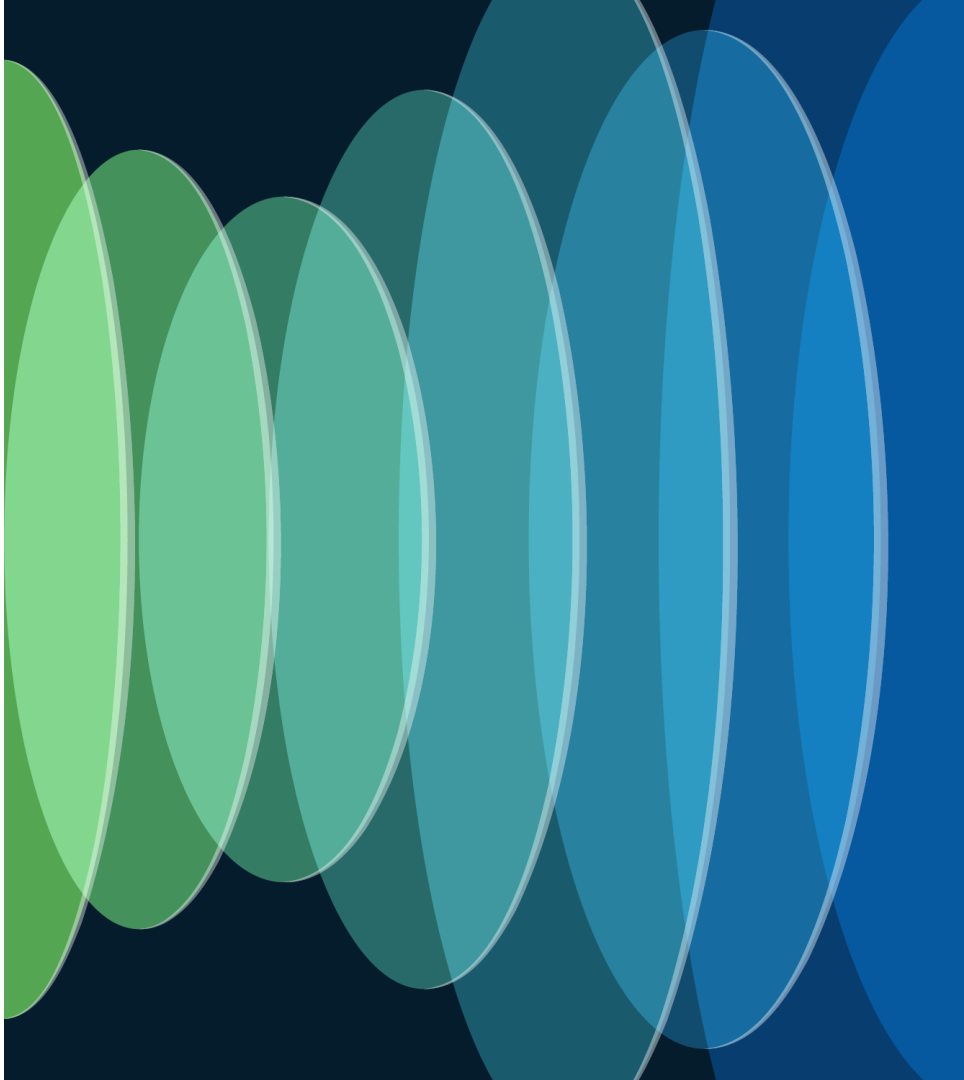


Ref: SR-PCE: Segment Routing Path Computation Engine NSO: Network Services Orchestrator

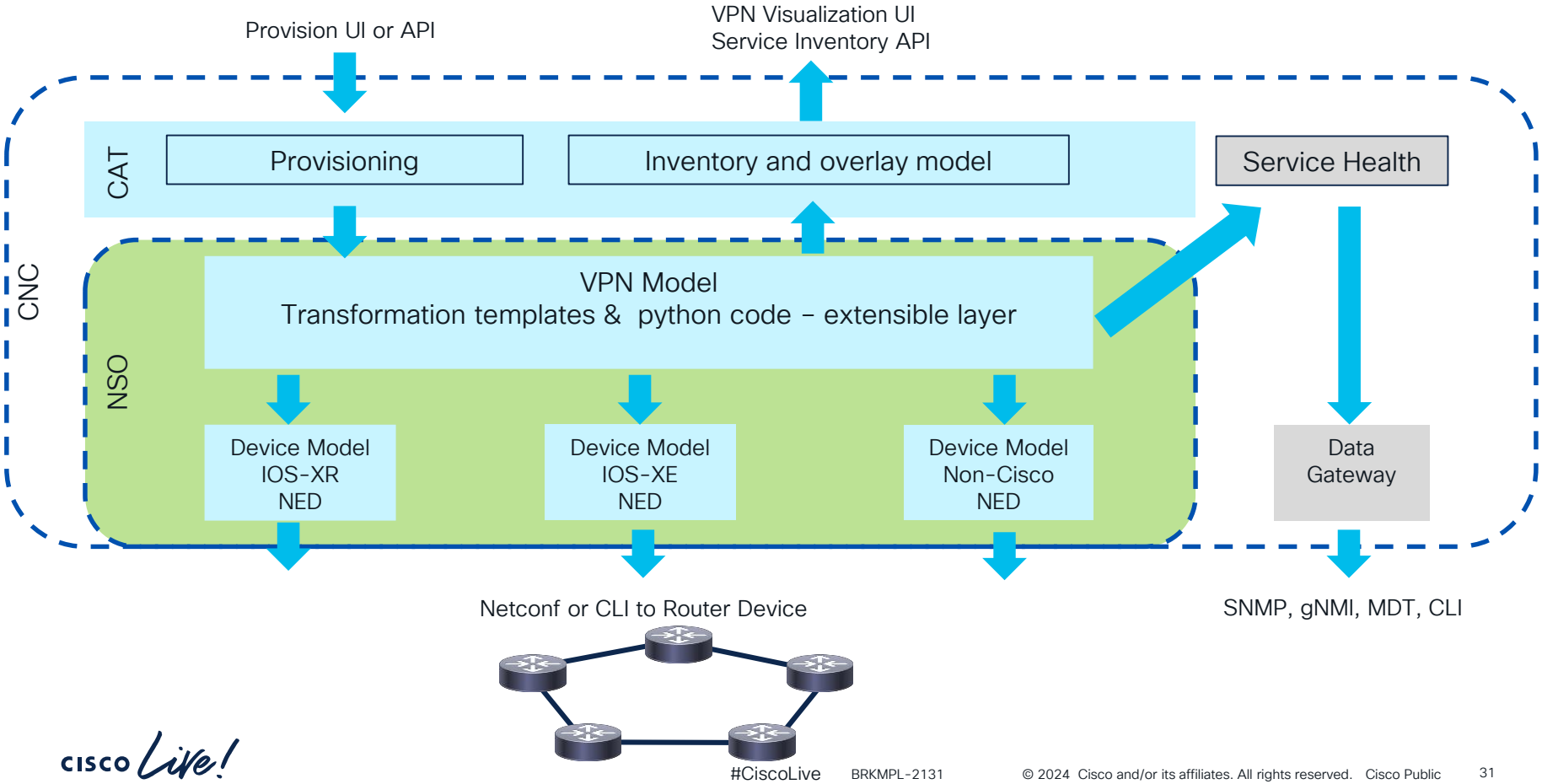
Crosswork Network Controller – Architecture



Service Provisioning



Provisioning components



CNC uses NSO as provisioning engine internally

NSO is a broadly deployed, highly scalable and very flexible provisioning platform

Service Manager

- Concept of an end-to-end “service”
- Full lifecycle management
- Service Models
- Service intent
- Service create code

Device Manager

- Single network-wide API
- Device models
- Syncs a local copy of all device configs

Configuration DB

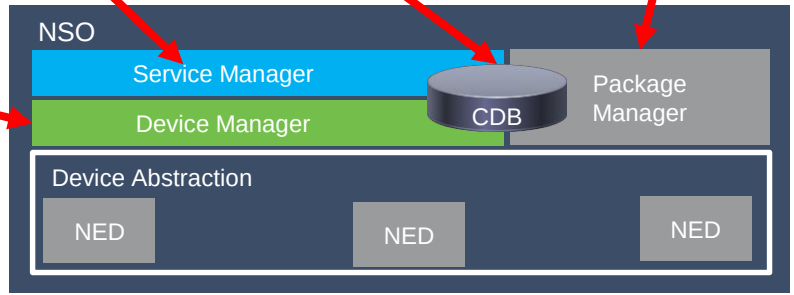
- YANG database
- Stores all device and service configs
- In memory DB

Package Manager

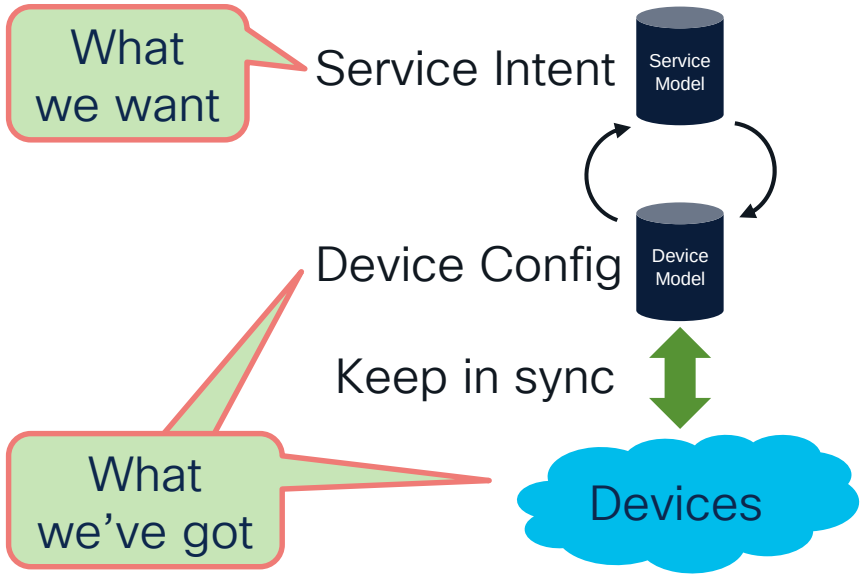
- Services and Device models and translation code in packages.

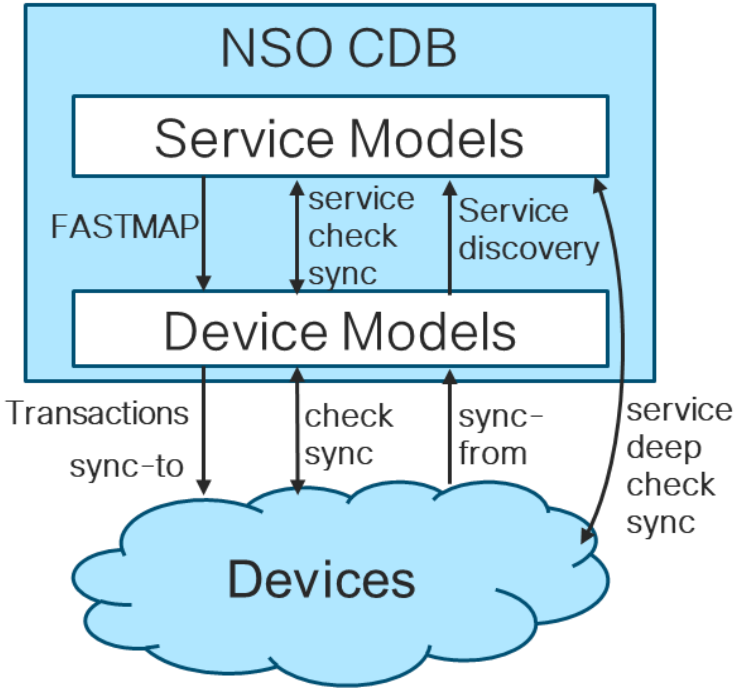
TSDN Function Packs

- Packages for CNC provisioning



Models and Sync Tools in NSO

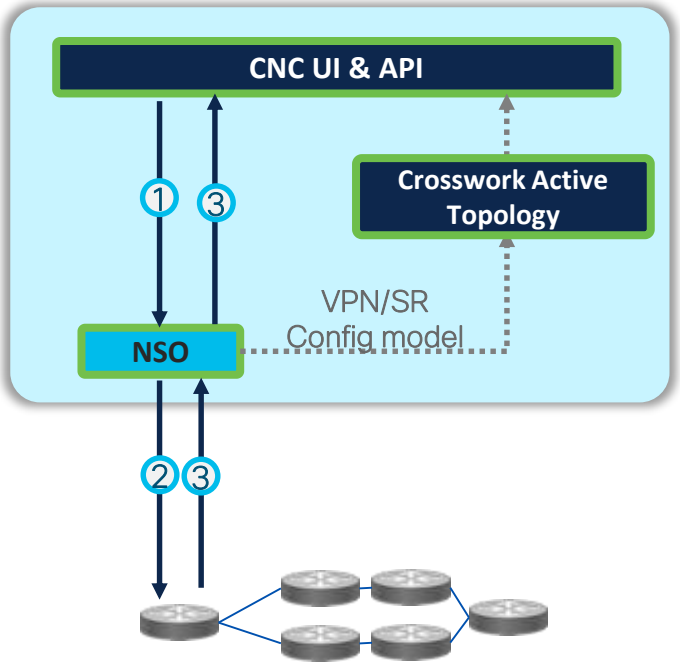




Industry's Broadest Multivendor Support

Over 170 Supported NEDs – Customization Available

Service Provisioning: NSO based Service



1. User requests VPN service with associated SR Policy
2. NSO creates device configurations for the VPN service and pushes it to the PE routers – IOS-XR and IOS-XE out of box.
3. Validation feedback is provided, visualization of paths

Service Provisioning UI loads and renders Service model YANG schema
CNC ships with NSO FPs for the following:
IETF-L2NM based on RFC9291 and IETF-L3NM based on RFC 9182
SR Policy Core FP. RSVP-TE sample FP.

VPN NSO FPs

IETF L2NM L2 VPN*

- T-LDP, EVPN VPWS, EVPN ELAN and ETREE
- SR-TE Policy or RSVT-TE or SRv6 locator
- ODN + l2vpn policy option for evpn
- L2VPN EVPN VPWS over SRV6

IETF L3NM VPN*

- VPN, Interface, BGP Neighbor
- SR-TE, SRv6 via l3vpn policy & ODN
- Tree-SID Provisioning

* function packs can be customized as needed for variations and non cisco devices

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

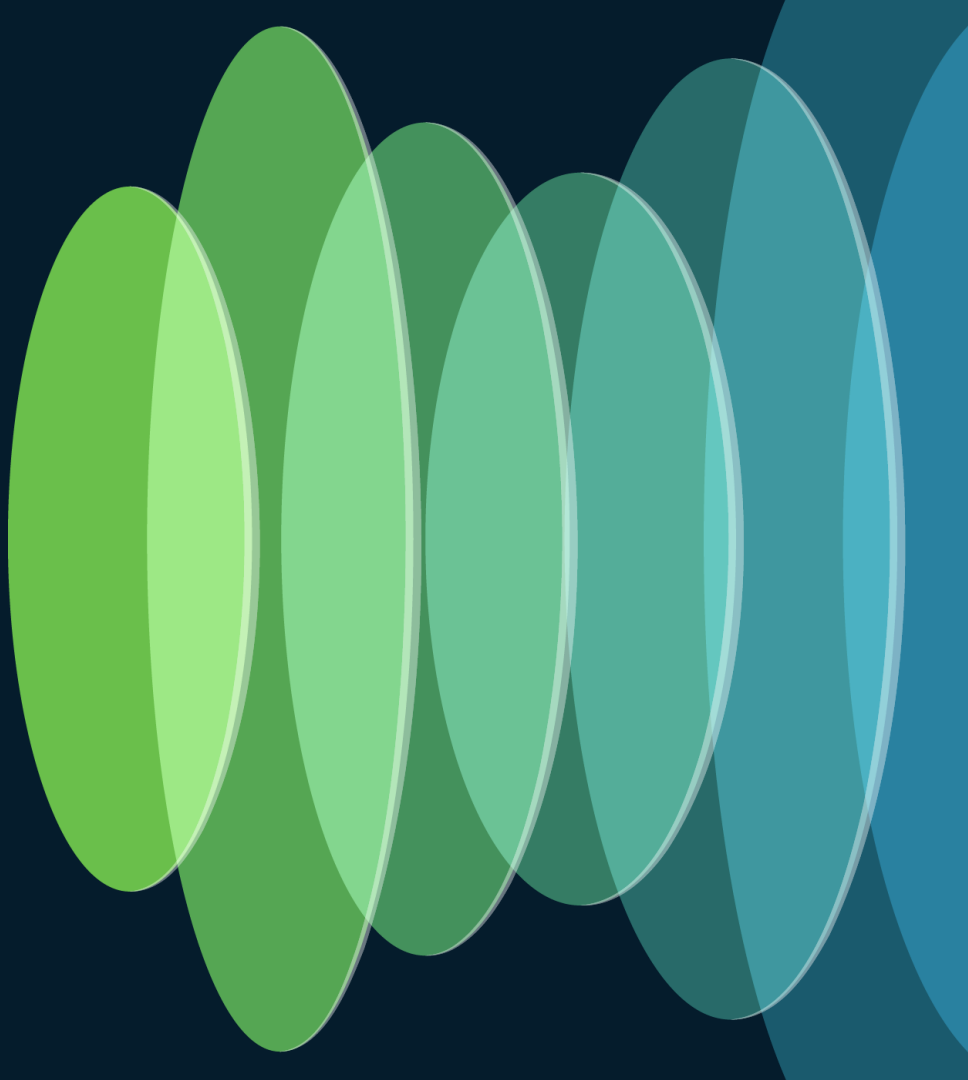
Extend as needed, starting from Cisco XR/XE out of box

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



Traffic Engineering – Why do we need it?

Service-Level Objective (SLO)

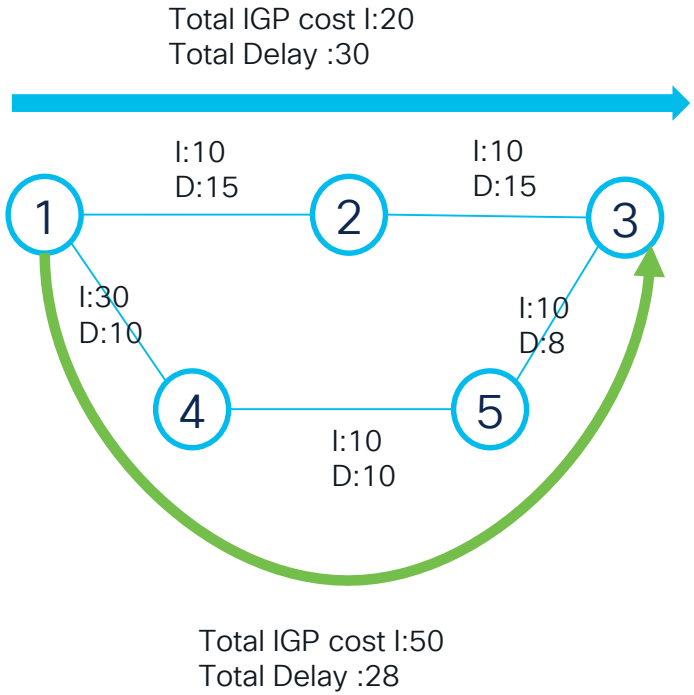
Link Preferences

High Availability

Bandwidth Applications

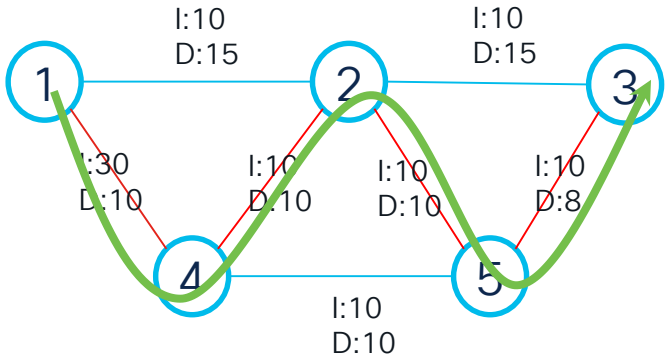
Congestion Mitigation

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

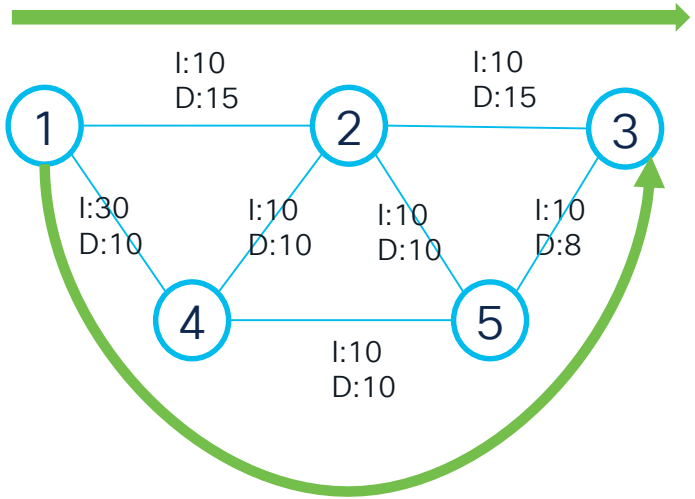


Total IGP cost I:50
Total Delay :28

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

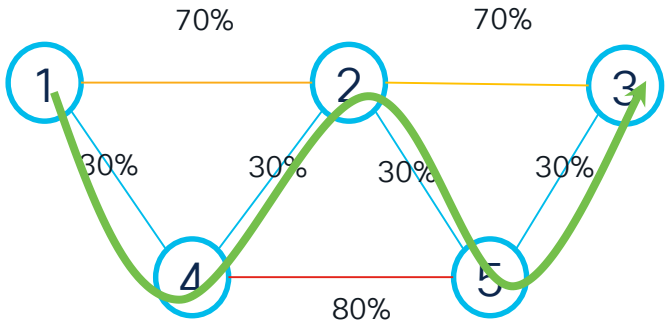
Highly Available Traffic using Disjoint paths

Send two copies with separated node/links/srlgs



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

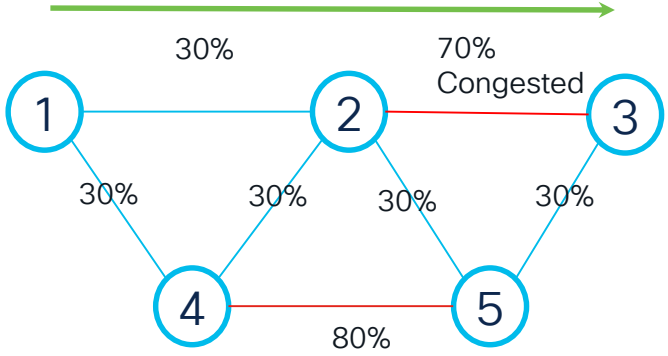
Bandwidth as Constraint



Link Utilization Tracked

Find and use Paths that have BW available for this traffic

BW Optimization Congestion Mitigation

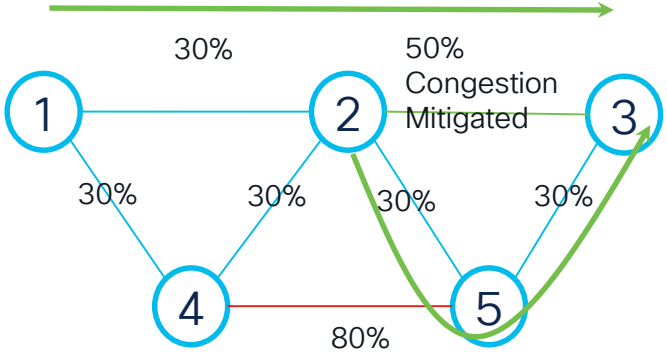


Link Utilization Tracked

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

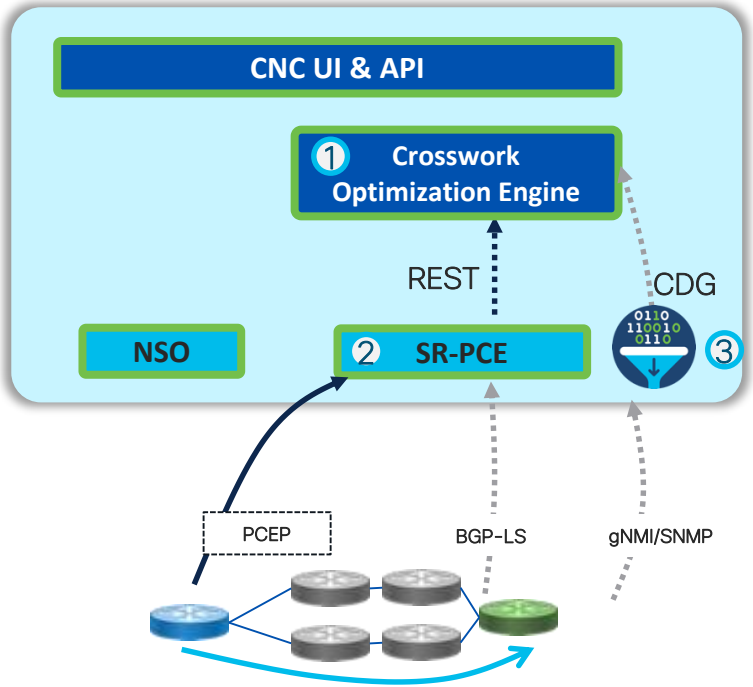
Automation needed

BW Optimization Congestion Mitigation



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

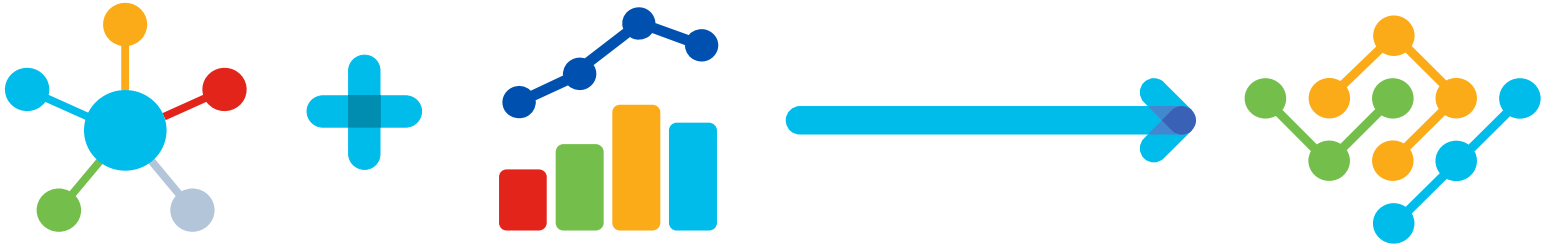
Path Calculation and Control Component View



1. Crosswork Optimization Engine
2. SR-PCE
3. Crosswork Data Gateway

Optimization Engine (OE)

- Builds and maintains real-time network model that includes topology and traffic
- Run simulations against real-time network model
- Performs bandwidth book-keeping (Bandwidth use cases)



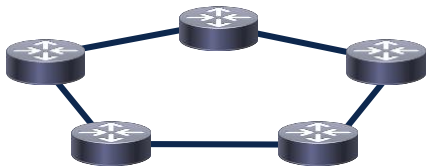
Topology

Interface and SR policy utilization

OE Real-Time network model

Optimization Engine (OE)

- Crosswork collects topology and LSPs using SR-PCE via internal API
- Crosswork enriches topology with additional attributes via SNMP using CDG
- Crosswork collects interface and SR policy statistics via Telemetry (gNMI/openconfig) or SNMP using CDG



Physical Network

Topology

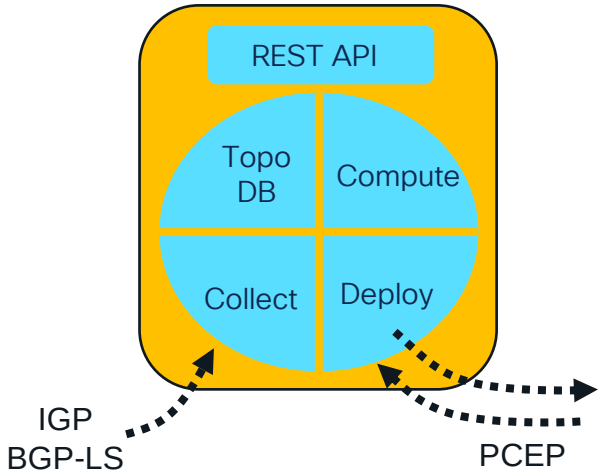
LSPs

Collection via SR-PCE

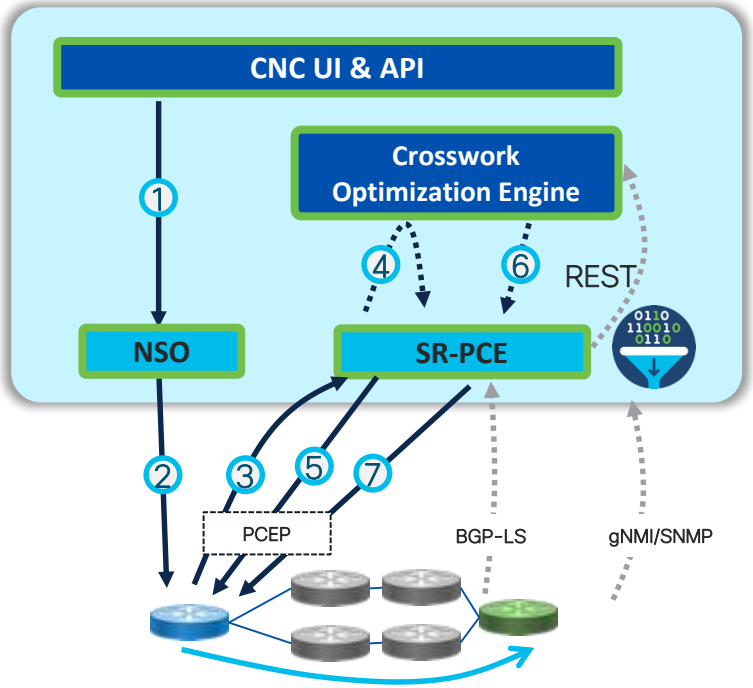
OE Real-Time network model

Segment Routing PCE (SR-PCE) on IOS-XR

- SR-PCE: IOS XR multi-domain stateful Segment Routing Path Computation Element (PCE)
  - **IOS XR**: Available on any physical/virtual IOS XR device, typically IOS-XRv9000 are deployed
  - **Multi-domain**: Real-time feed via BGP-LS/IGP from multiple domains; computes inter-area/domain/AS paths
  - **Stateful**: takes control of SRTE Policies, updates them when required
  - **SR PCE**: native SR-optimized computation algorithms
  - **Delegates** to OE when Bandwidth constraint is requested using API



Path computation – SR-PCE + Optimization engine



1. User requests VPN service & associated SLA from CNC.
2. NSO provisions Service, SR policy initialized at headend
3. Headend requests path from SR-PCE
4. If request includes bandwidth, SR-PCE gets path from OE
5. SR-PCE returns path to headend
6. If bandwidth path needs to change, OE pushes path to SR-PCE
7. SR-PCE updates headend via PCEP for path changes

SR Policy Optimization	
Objective	Latency/IGP/TE Metric Minimization
Constraints	Affinities, Disjoint Paths, Bandwidth

Path Computation & Optimization scenarios

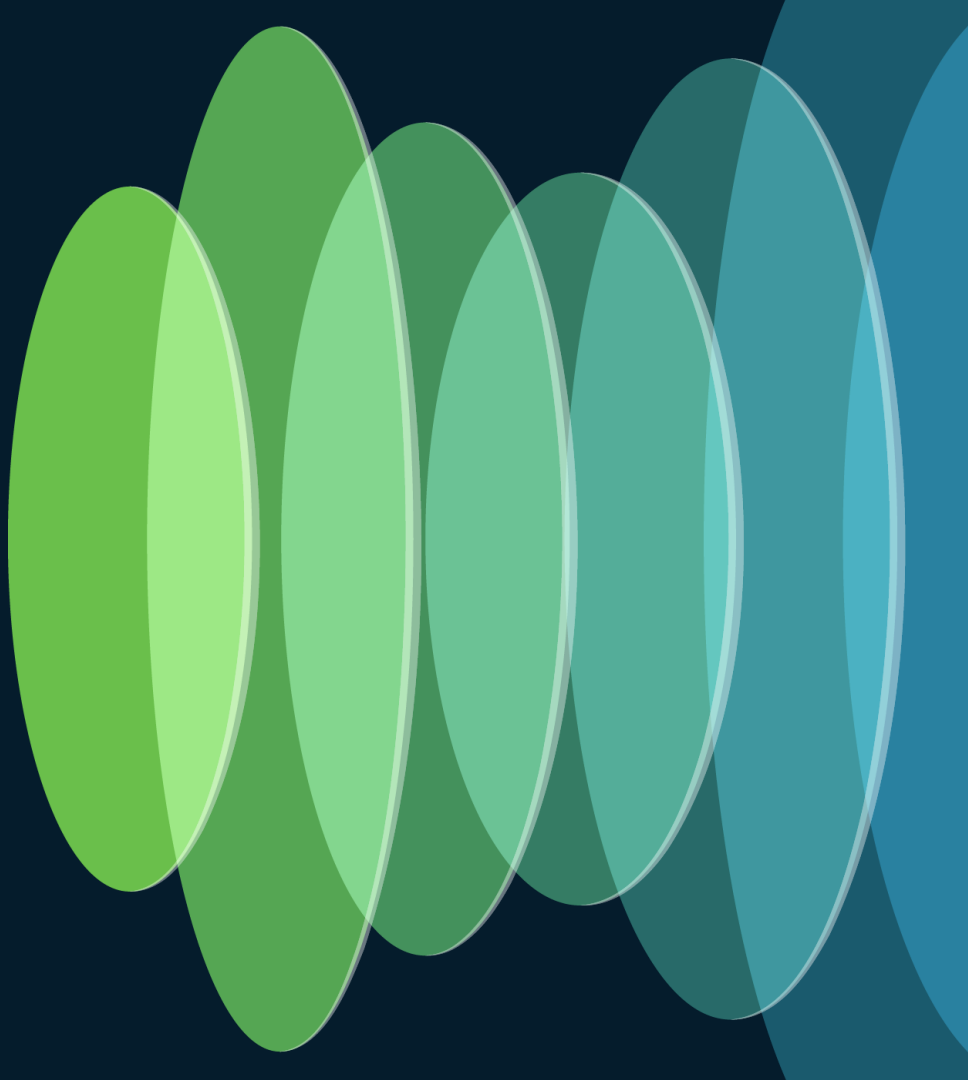
Use case	Optimization objective / constraint	Single IGP domain	Multi-IGP domain
Basic Reachability	IGP Metric	PCC or PCE	PCE
Low Latency	TE Metric	PCC or PCE	PCE
Low Latency	Delay Metric	PCC or PCE	PCE
Disjointness	IGP/TE/Delay + Association Group	PCC or PCE	PCE
Bandwidth on Demand (BWoD)	Bandwidth	PCE + COE	PCE + COE
Circuit Style SR-TE (CS SR-TE)	Bandwidth	PCE + COE	PCE + COE
Local Congestion Mitigation (LCM)	Bandwidth	PCE + COE	PCE + COE

PCC: Path computation client aka Head End Router, PCE: Engine, COE, Crosswork Optimization Engine

Crosswork Network Controller transport capabilities

- Segment Routing Traffic Engineering
- Segment Routing v6 Traffic Engineering (SRv6)
- TreeSID
- Bandwidth on Demand (BWoD)
- Circuit Style SR-TE (CS SR-TE)
- Local Congestion Mitigation (LCM)

Service Health



CNC Service Health Architecture

Uses Service Assurance for Intent Network concepts – IETF RFC 9417

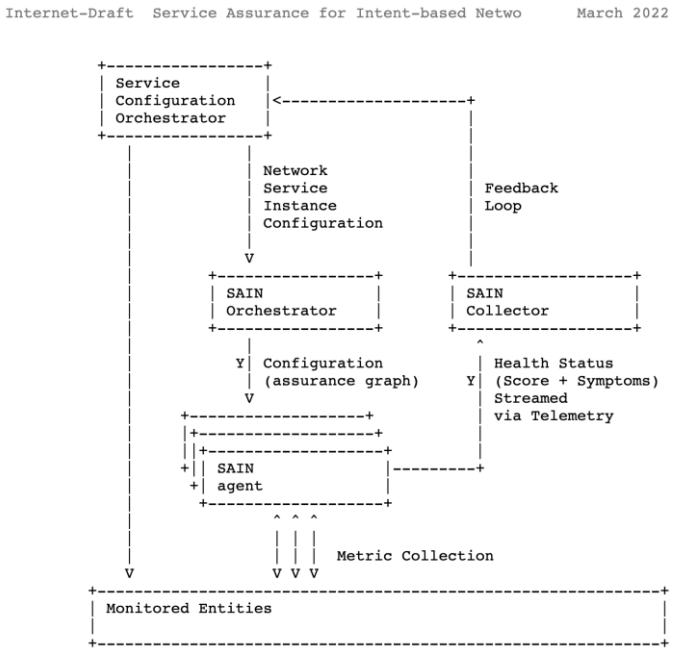
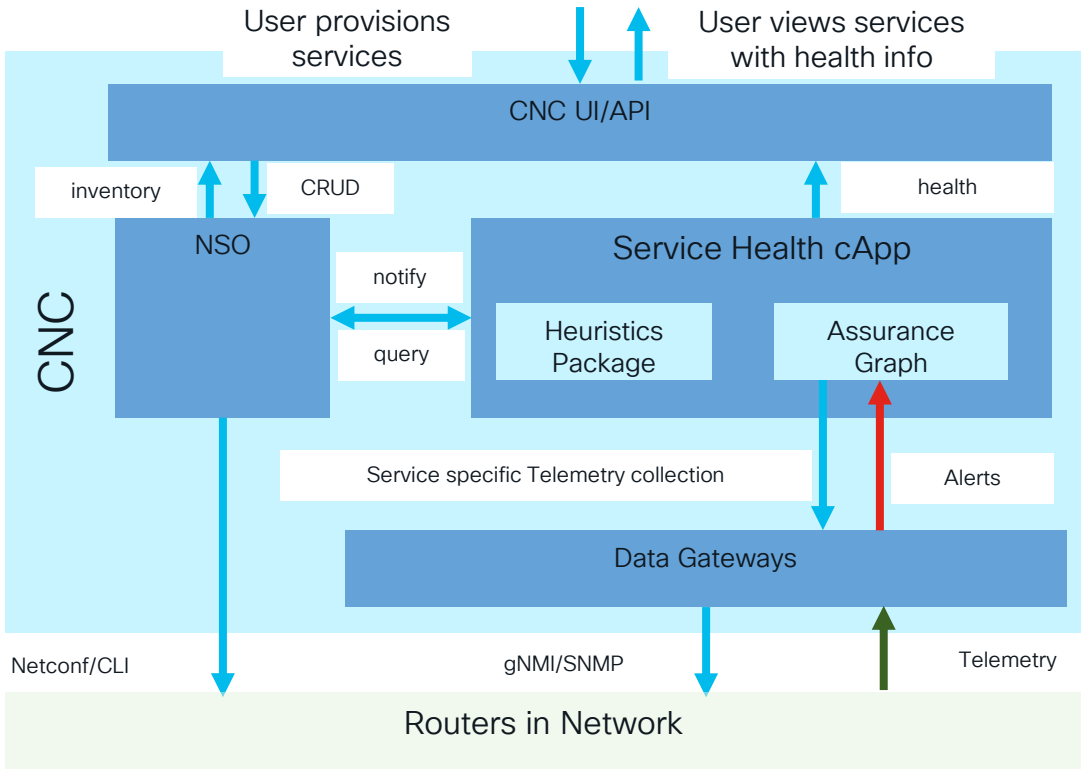


Figure 1: SAIN Architecture



From Heuristic Package to Assurance Graph

INTENT

Service Type and Device Config

RULES

Assurance Graph

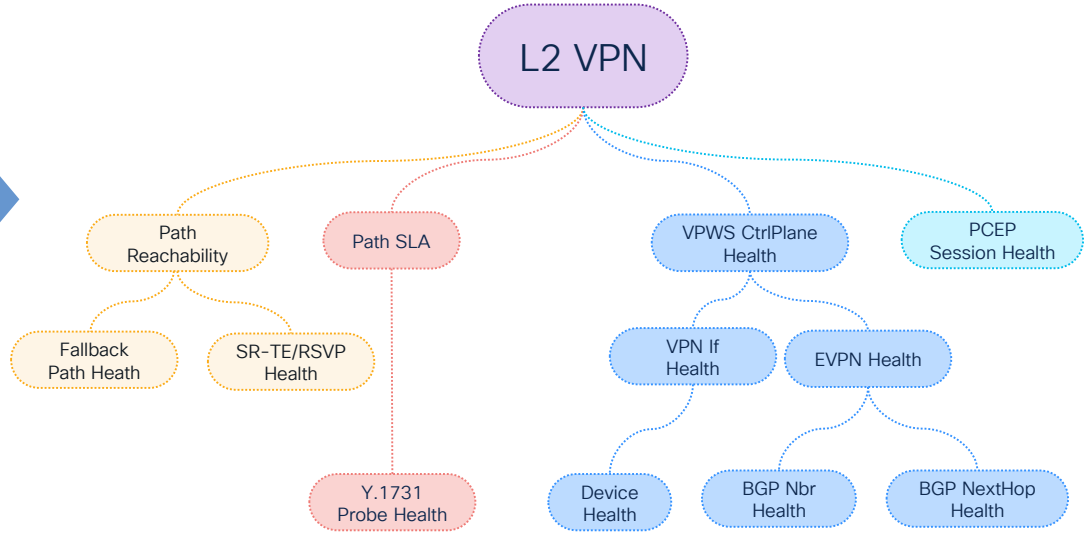
NSO Service and Device Configuration

Services

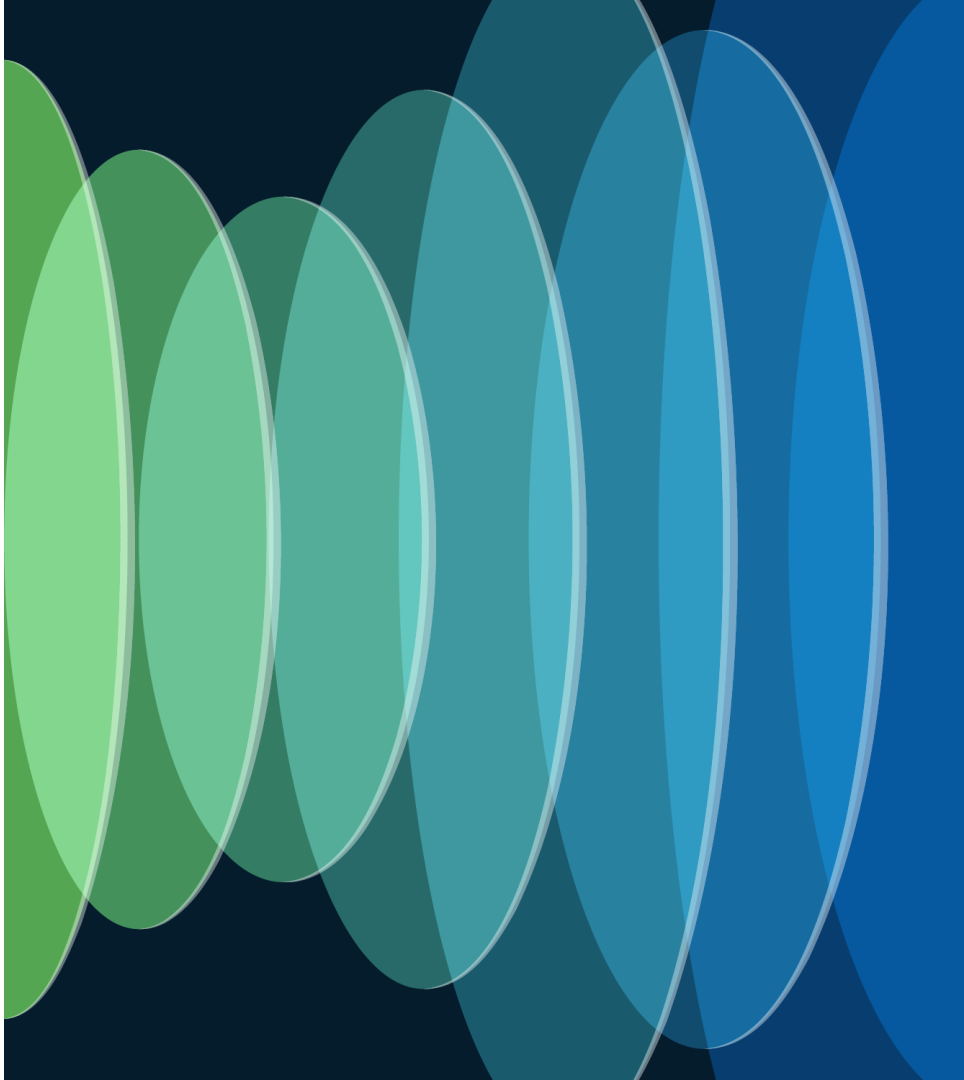
Subservices

Expressions

Metric



Demo



Conclusion

- SDN Controllers moves the Automation and Assurance boundaries offering single API and assurance platform reducing the cost & work needed in building automation.
  - Extensible modules allow for flexibility in supporting variations.
  - API integration to integrate with business processes
  - Telemetry via controller supports collect once and consume many places
  - Visualization is a big operations benefit
- Segment Routing Networks are programmable and enable delivery of granular SLAs with simplification and scale with SDN controllers
- Innovation with SDN Controllers is faster w simplified networks

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 2025.

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

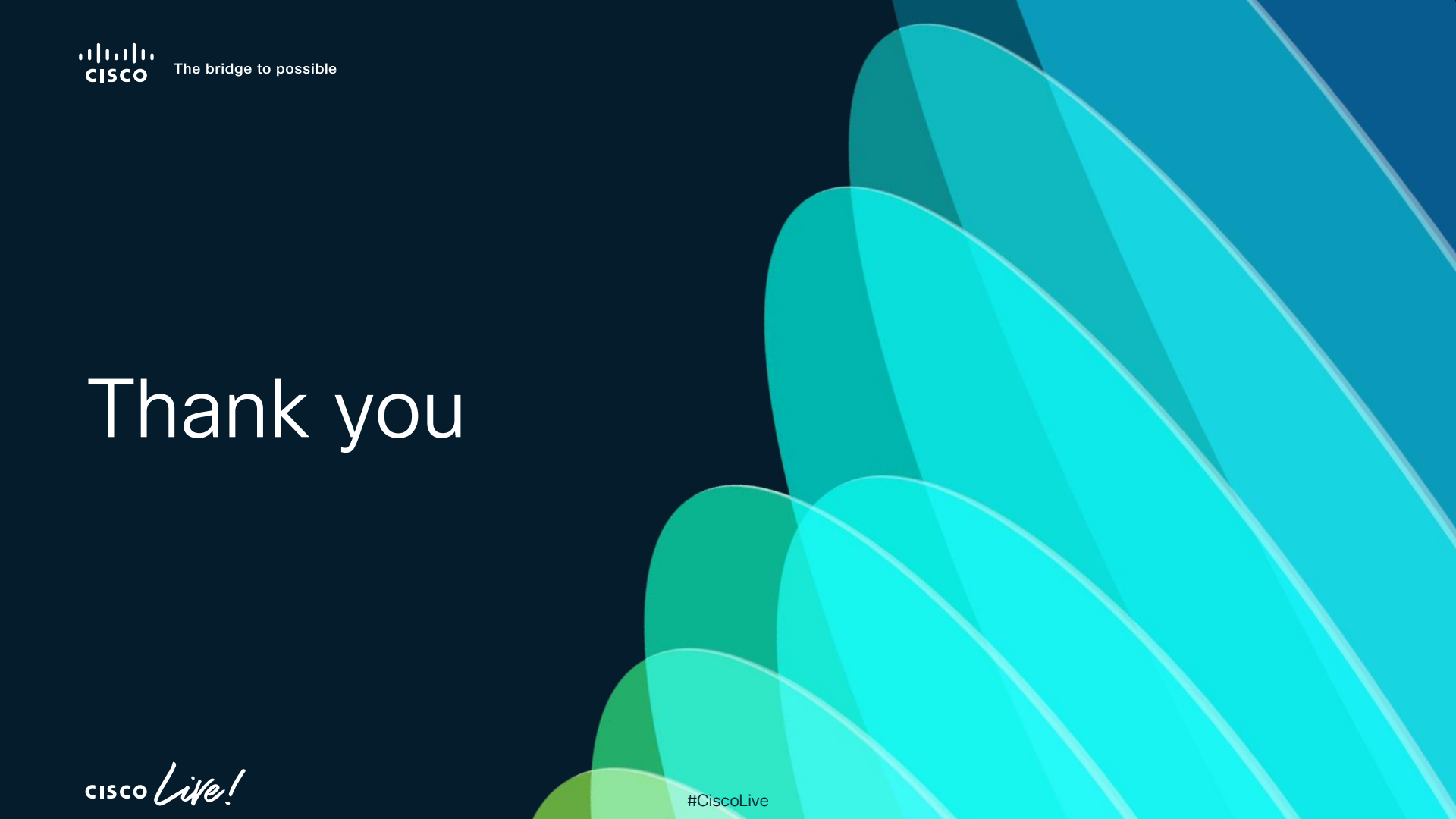
Contact me at: cnc-request@cisco.com

SR Learning Path

Session ID	Title	Session Type	Speakers	Schedule and location
TECSPG-1000	Segment Routing Masterclass	Technical Seminar	Jose Liste | Jakub Horn	Jun 2 | 9:00 am - 1:00 pm L2, Breakers BH
BRKMPL-2203	Introduction to SRv6 uSID Technology	Breakout	Jakub Horn	Jun 3 | 10:30 am - 12:00 pm L3, South Seas B
BRKMPL-2135	Preparing for a Successful Segment Routing Deployment -	Breakout	Jose Liste	Jun 3 |10:30 am - 12:00 pm L2, Surf EF
BRKENT-1520	Segment Routing Innovations in IOS XE	Breakout	Jason Yang | Sumant Mali	Jun 3 | 9:30 am - 10:30 am L3, Palm D
BRKMPL-2131	Deploying VPNs over Segment Routed Networks Made Easy	Breakout	Krishnan Thirukonda	Jun 3 | 01:00 PM / LL, Tradewinds DEF
BRKMPL-2177	Empower Your Network with Segment Routing and MPLS Network Migration	Breakout	Thomas Wang	Jun 3 | 9:30 am - 10:30 am LL, Tradewinds DEF
BRKMPL-2043	Simplify Your Journey to SR and SRv6 with Cisco Crosswork Automation	Breakout	Sujay Murthy | Eric Ortheau	Jun 4 | 04:00 PM / LL, Tradewinds ABC

SR Learning Path

Session ID	Title	Session Type	Speakers	Schedule and location
BRKSPG-2474	Reduced Resolution Time with Svc-centric Approach to Troubleshooting	Breakout	Paola Arosia	Tuesday, Jun 410:30 am - 11:30 am PDT L3, Palm A
LTRSPG-2006	Explore the Power of SRv6: Unleashing the Potential of Next-Generation Networking -	Instructor-led Lab	Jakub Horn | Marius Stoica | Alex Kiritchenko	Jun 5 | 8:00 am - 12:00 pm Luxor - L1, Lotus 3
BRKMPL-2133	Circuit-Style Segment Routing and Service Emulation -	Breakout	Thomas Wang	Jun 5 | 4:00 pm - 5:00 pm L2, Surf CD
BRKSPG-2263	Design, Deploy and Manage Transport Slices using SDN Controller and Assurance	Breakout	Sujay Murthy	Jun 6 | 09:30 AM / LL, Tradewinds ABC
BRKSPG-2870	Automate Transport Service Provisioning, Optimization, and Assurance with SDN Controller	Breakout	Deepak Bhargava	Jun 6 | 01:00 PM / L3, South Seas J
LABMPL-1201	SRv6 Basics	Walk-in Lab	Luc De Ghein	Walk in Lab area in WoS
LABSP-3393	Implementing Segment Routing v6 (SRv6) Transport on NCS 55xx/5xx and Cisco 8000: Advanced -	Walk-in Lab	Paban Sarma | Gautam Renjen | Alexey Babaytsev	Walk in Lab area in WoS
LABSPG-3000	Configure and Implement BGP-EVPN with Segment Routing using NCS 55xx/5xx Platforms	Walk-in Lab	Tejas Lad | Paban Sarma	Walk in Lab area in WoS


The bridge to possible
Thank you
cisco Live!
#CiscoLive