

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright white sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Protect Your Network Using Programmability & Segment Routing

Michael Geller, Distinguished Architect
@michaelge11er
BRKSPG-2125

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

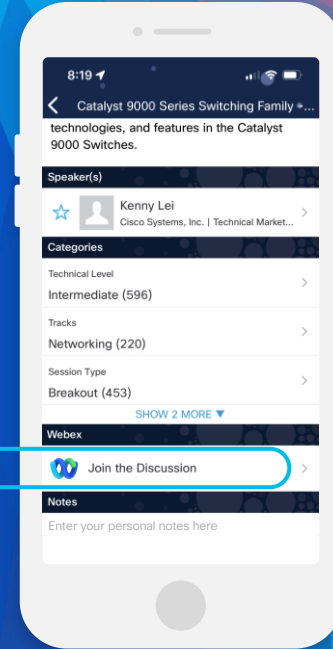
Questions?

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 December 22, 2023.

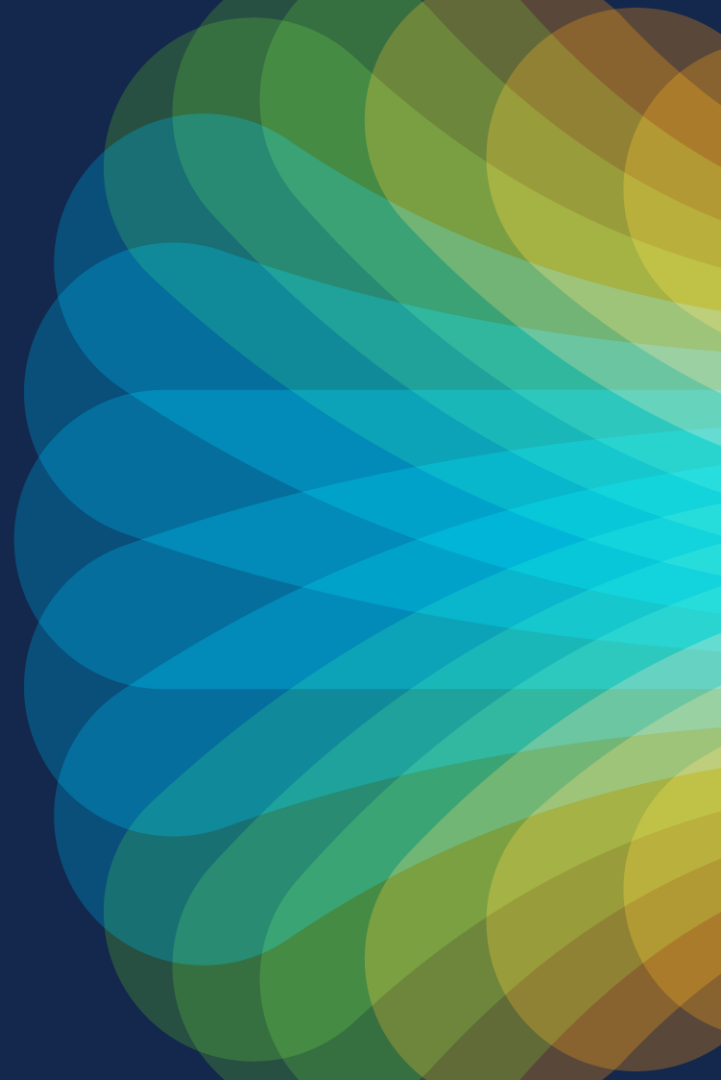


<https://cislive.ciscoevents.com/cislivebot/#BRKSPG-2125>

Agenda

- Introduction
- Protecting The “Clean Core”
- DDoS Protection Provided By The Transport Fabric
- How To Program Security Policy Into the Network Fabric
- Where to Learn More
- Conclusion

Introduction



My Personal & Professional Life

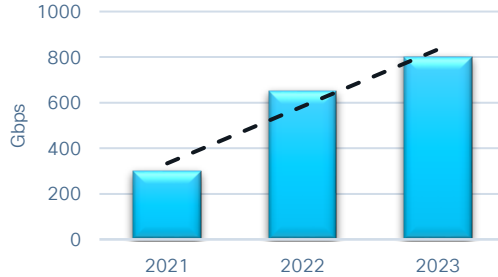


- Distinguished Architect @ Radware
- 25 Years in Cisco
- Distinguished Speaker
- Cloud and SP Security
 - “Securing critical apps and the networks that deliver them”
- Areas of focus: DDoS, 5G, AppSec, SecOPS
- 2 kids, 1 wife
- 5th Degree Black Belt, TKD



DDoS attacks keep growing and even faster

DDoS Attack Volume

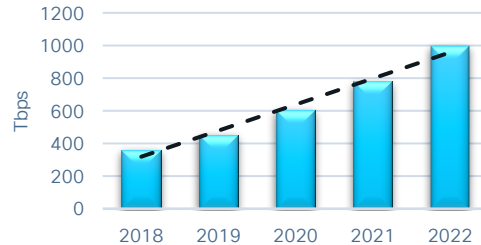


Source: GCore-Radar, March, 2023

DDoS attack volume have grown by a 66% CAGR during the last 3 years.



Global International Internet Traffic



Source: TeleGeography 2023

Internet traffic is projected to grow at an annual rate of ~25% from 2020-2030².



The proliferation of connected devices is a prime opportunity for cybercriminals to stage more and more massive DDoS attacks.



As low-latency applications move to the edge, networks become more vulnerable to DDoS attacks.

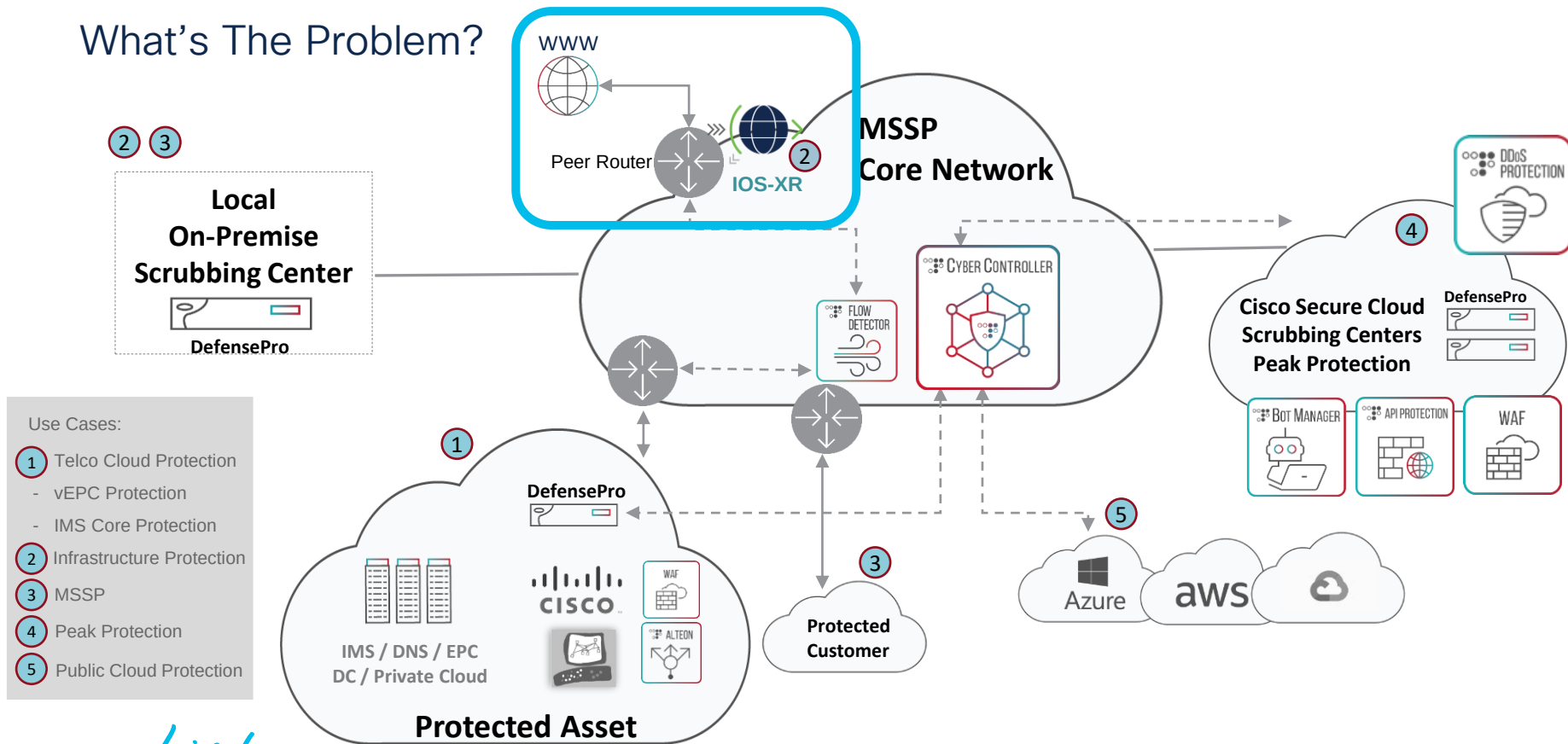


Problem & Approach

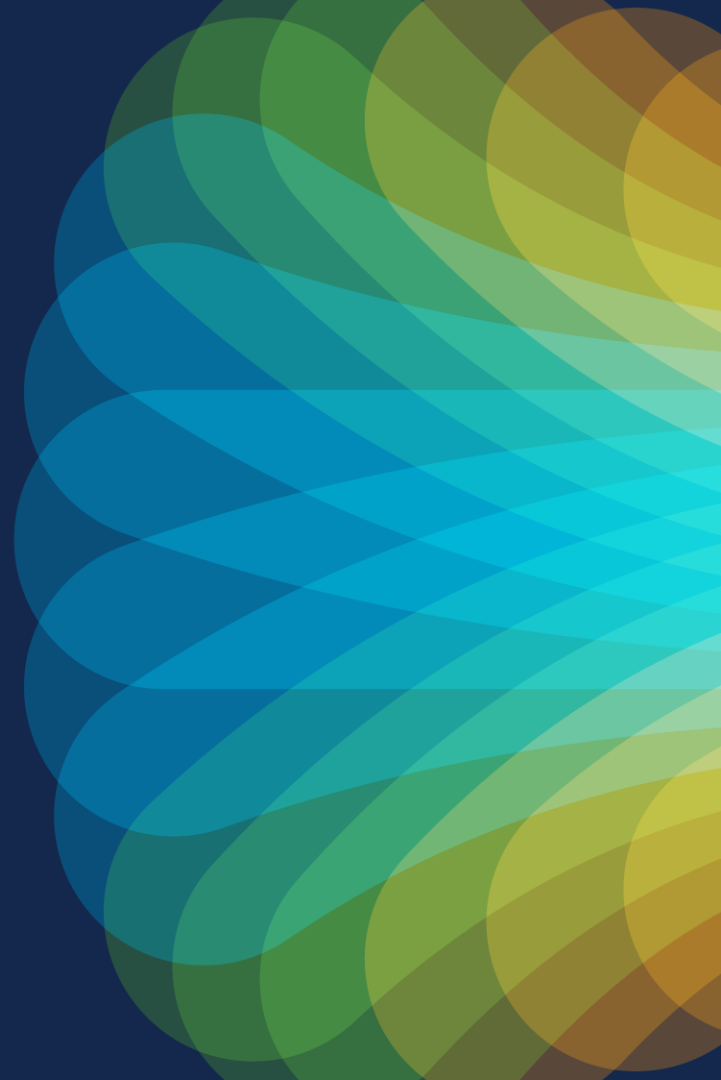
- Apps and Services run at the programmable network edge, how do I apply security in the transport fabric, at scale, without taking a huge latency penalty?
 - First, put a DDoS service natively in IOS-XR (Edge Protection)
 - Second, use SRv6 to program the network to deliver path-optimized, policy bound service chains, natively, protecting the “clean core”
 - Third, monitor and optimize constantly

Multi-Tier DDoS Protection

What's The Problem?

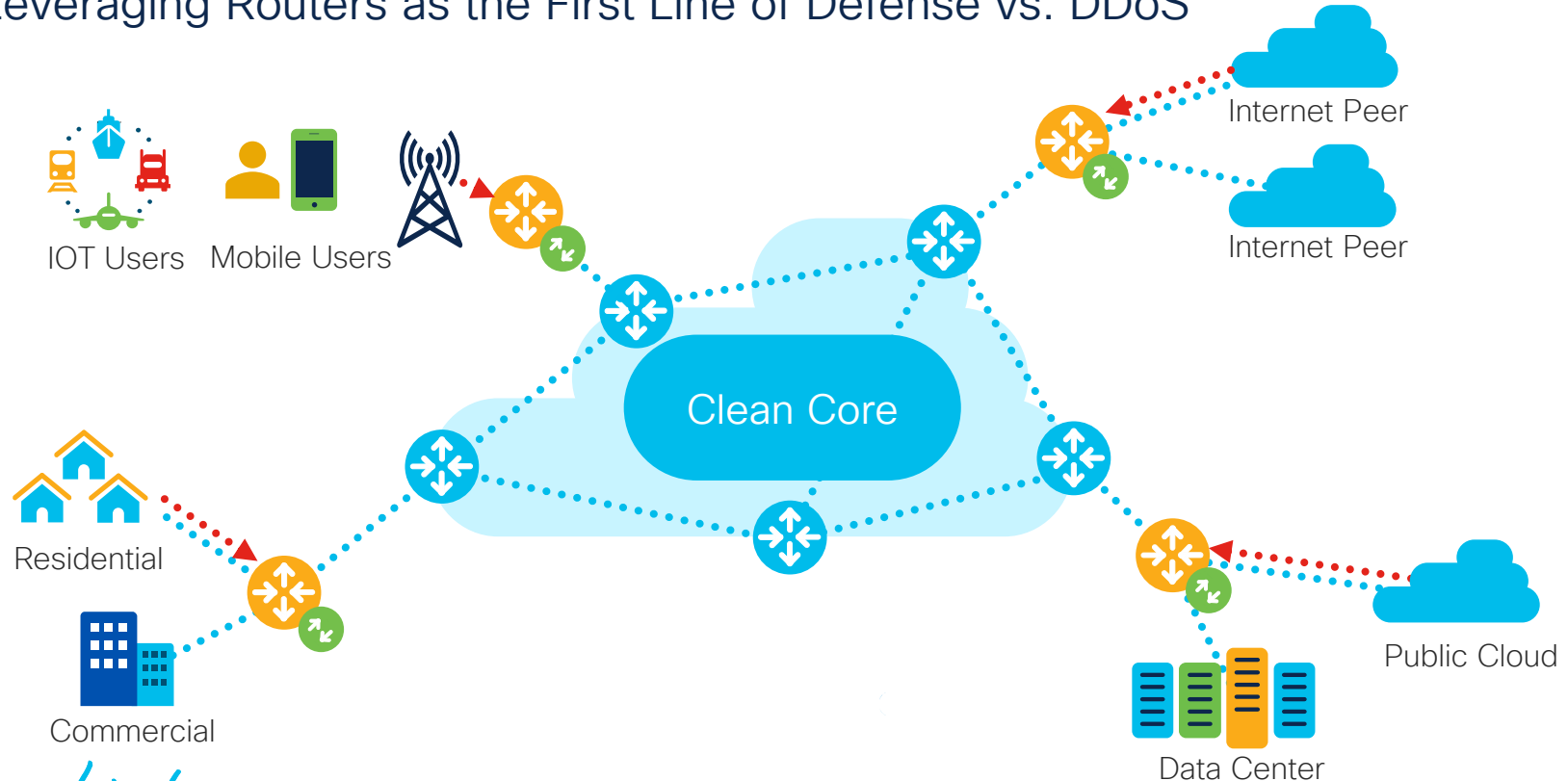


Protecting The Clean Core



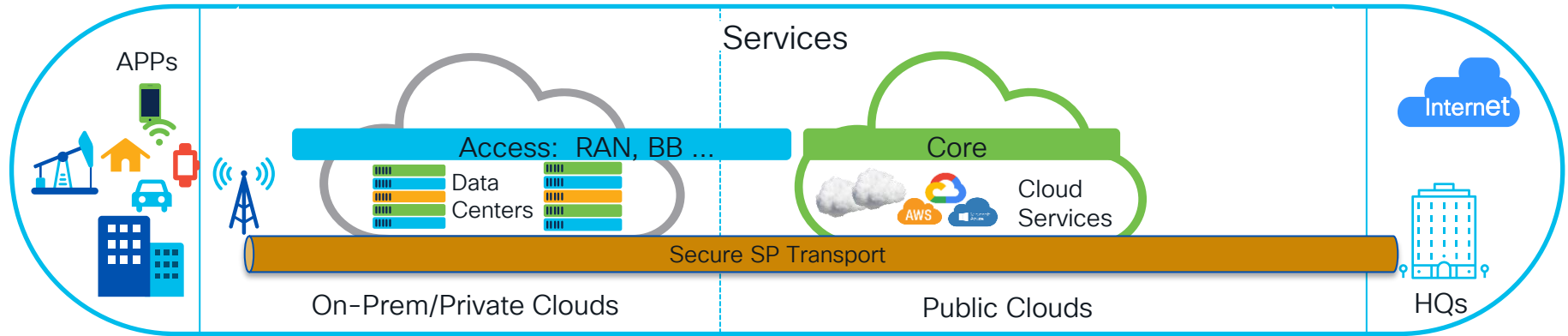
DDoS Edge Protection operation

Leveraging Routers as the First Line of Defense vs. DDoS

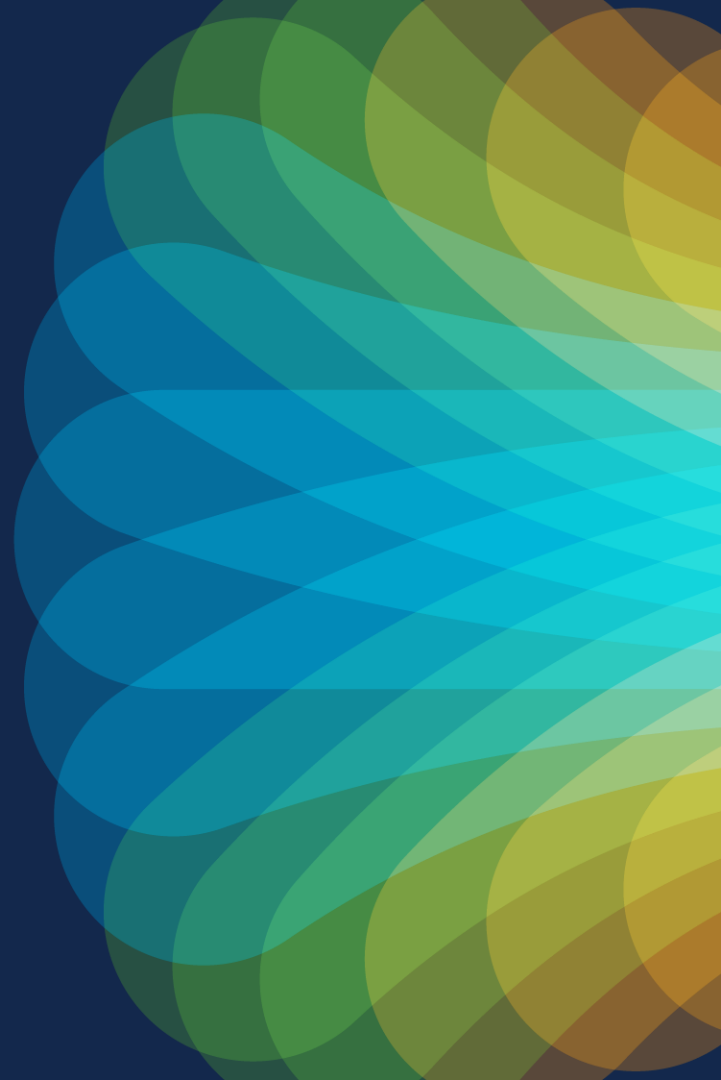


Protecting The Clean Core

Programming A Secure Path & Service



DDoS Protection Provided By The Transport Fabric



Keep attack traffic off your network by establishing a security perimeter at the edge

Use your routers as the first line of defense against DDoS attacks

Real-time on-box attack Detection and Mitigation

Protects quality of experience and the performance of low-latency applications

Software that requires no additional equipment, rack space, power, or cooling

Makes the solution cost-effective and scalable

Zero-day attack detection and mitigation using unsupervised machine learning

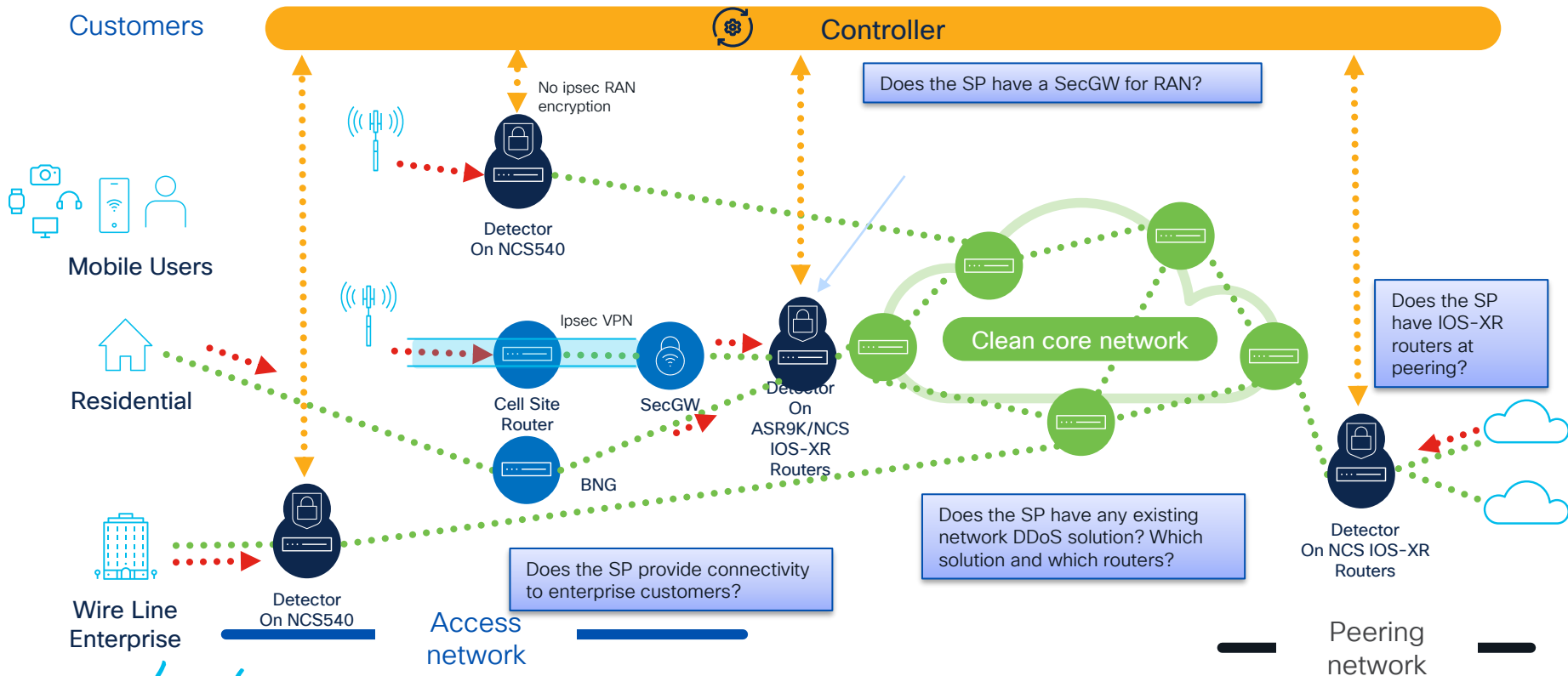
Ensures the flow of legitimate traffic while preventing malicious traffic from flooding the access network

Autonomous system with a central interface management function

Offers ease of management with complete control

Scale your DDoS capabilities simply and cost-effectively as you scale your networks

Cisco Secure DDoS Edge Protection detects and mitigates DDoS attacks on your routers in real-time



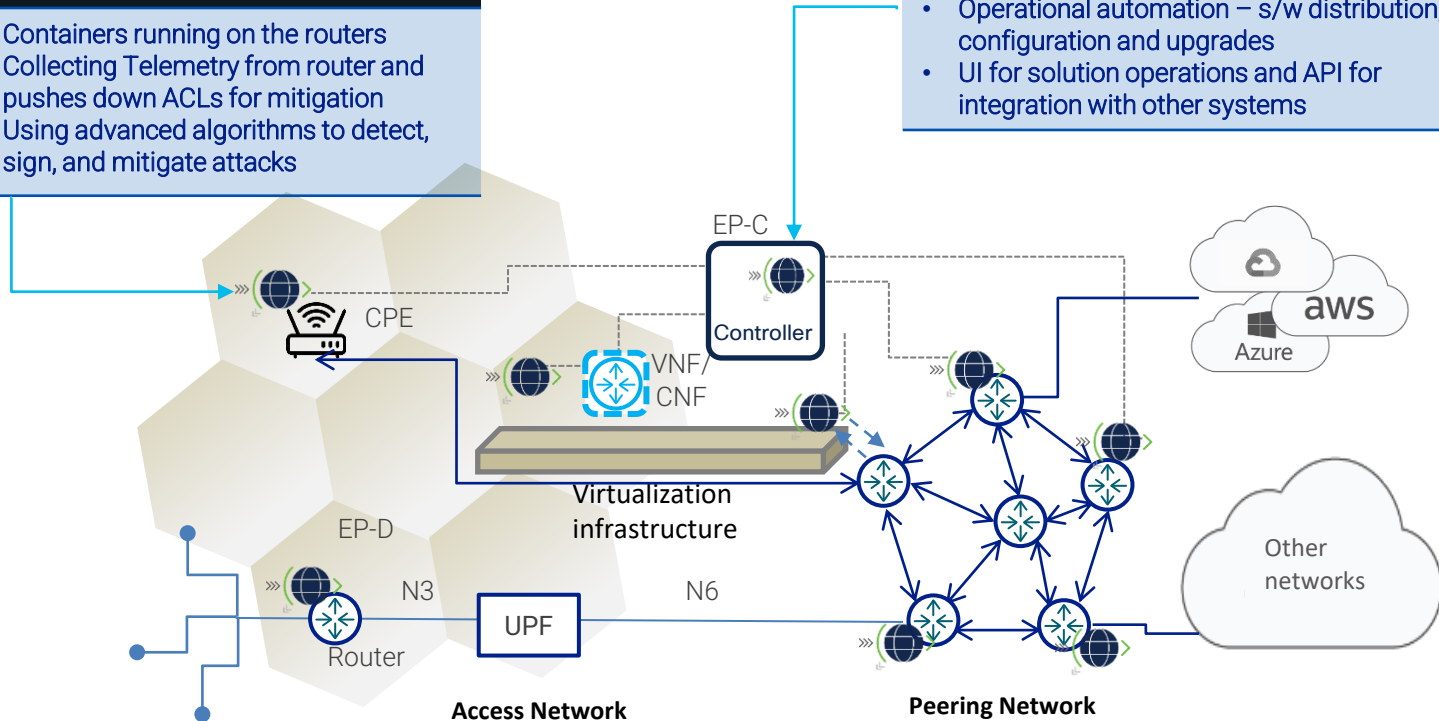
DDoS - Solution Architecture

Detectors

- Containers running on the routers
- Collecting Telemetry from router and pushes down ACLs for mitigation
- Using advanced algorithms to detect, sign, and mitigate attacks

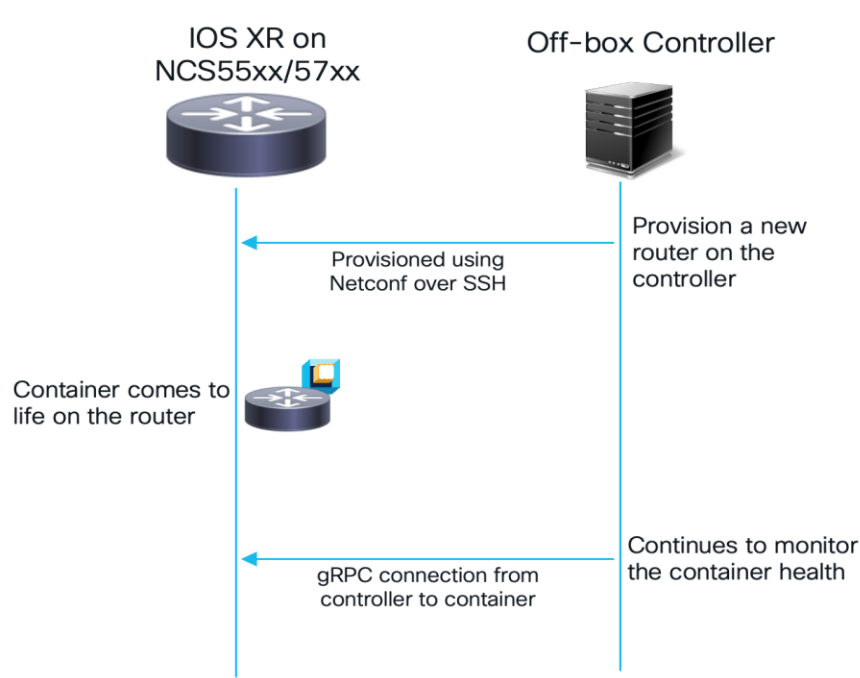
Controller:

- Manages 10,000s of detectors
- Manages security function on global view
- Operational automation – s/w distribution, configuration and upgrades
- UI for solution operations and API for integration with other systems

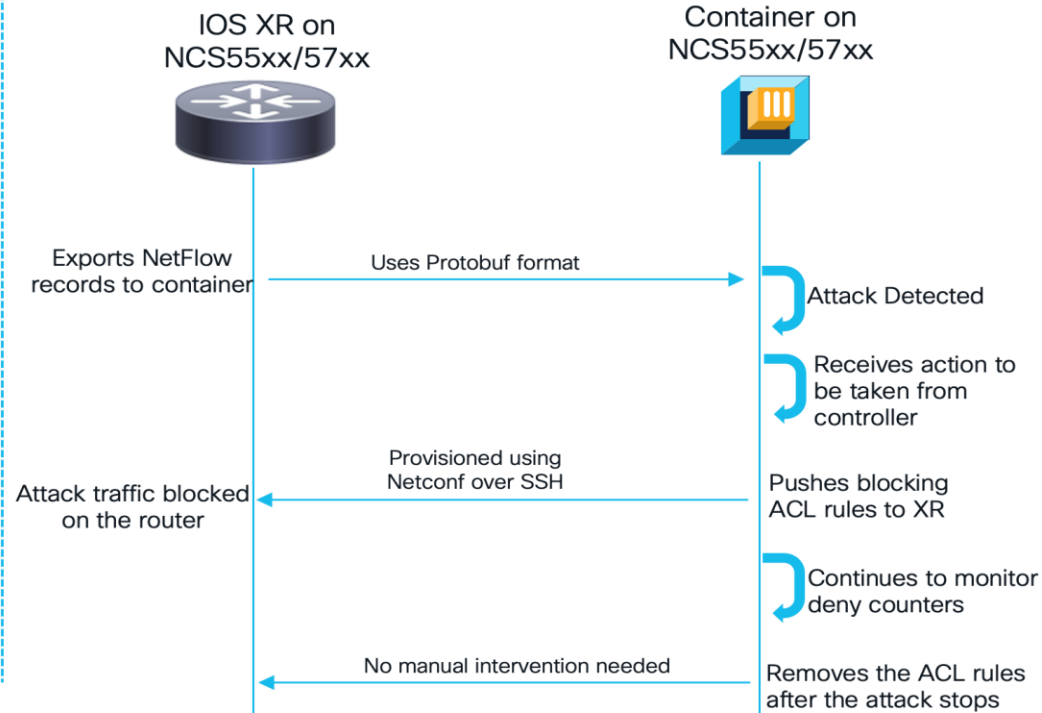


Detailed Flows

Provisioning Phase



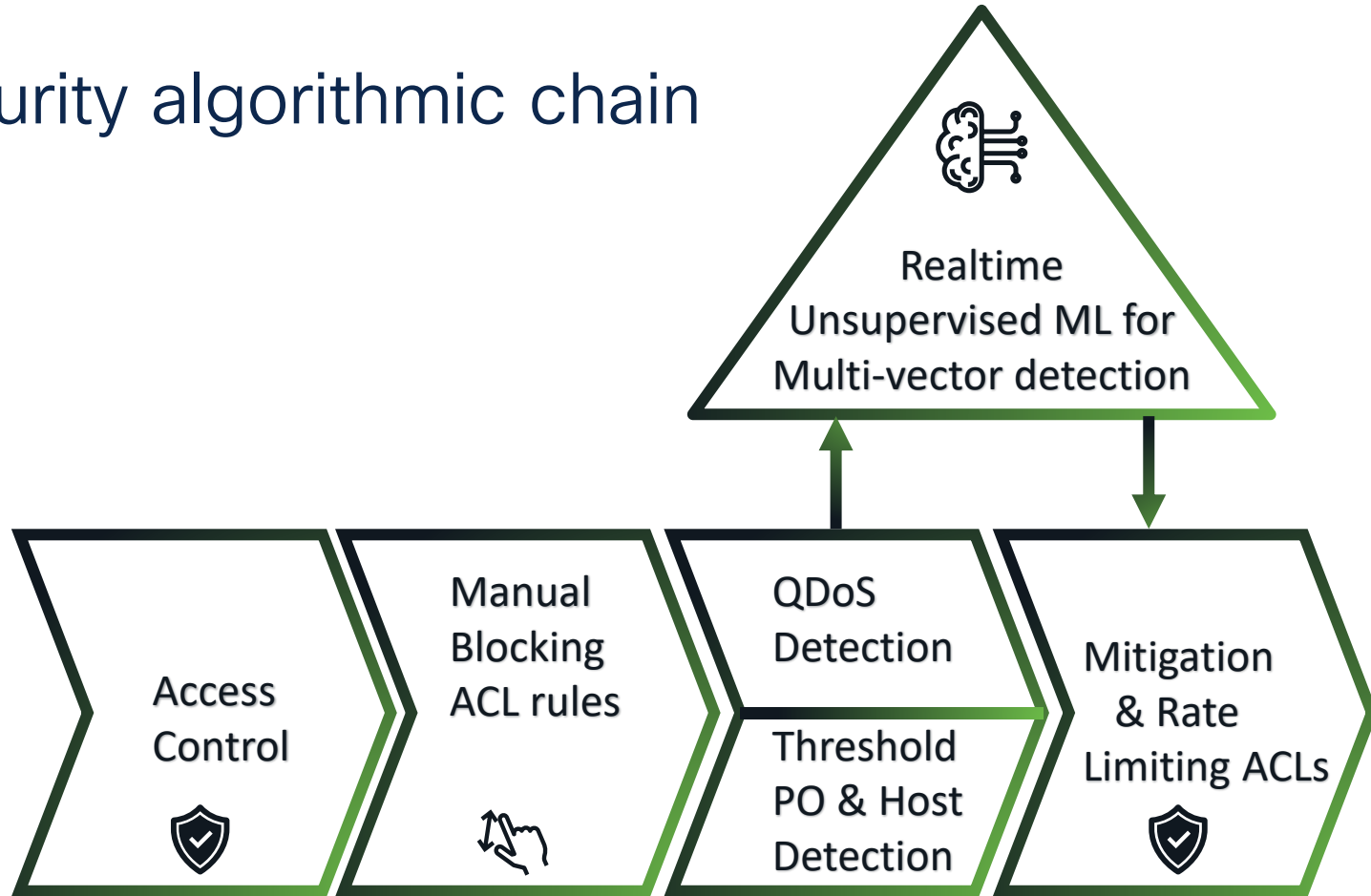
Detection & Mitigation Flows



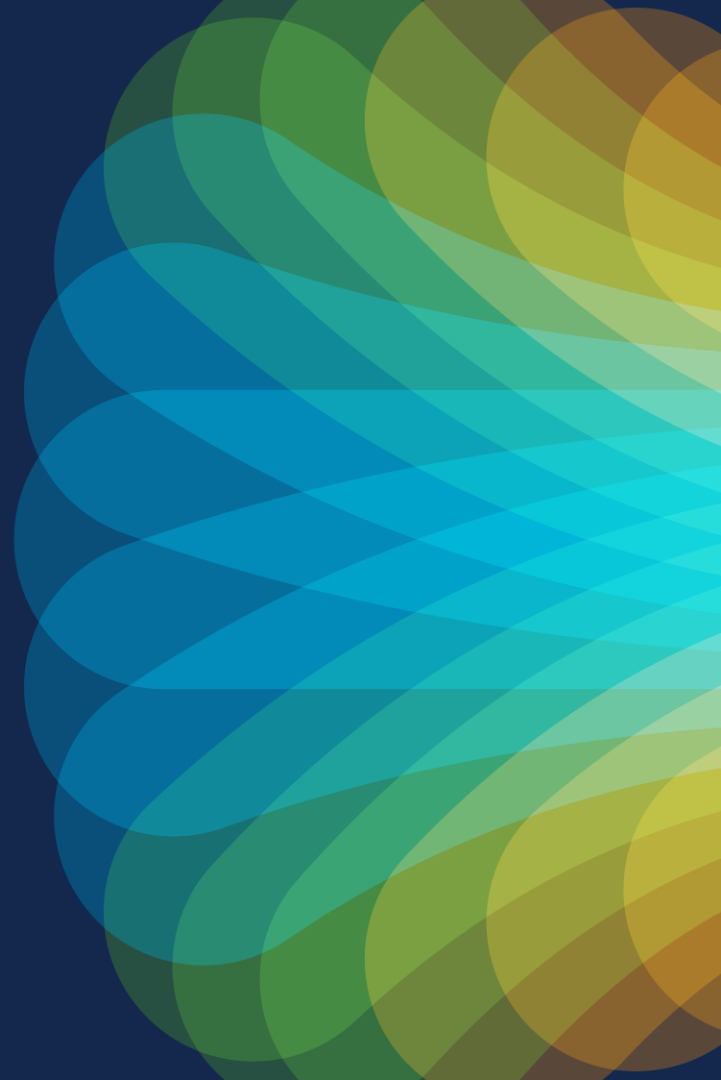
Router Model & IOS-XR Support

- 7.9.1 IOS-XR: NCS540 Tortin and Everglades (Mobile Access Use Case)
- 7.10.1 IOS-XR (July 2023): NCS540 Adadia →Crater Lake
- 7.11.1 IOS-XR (Nov 2023): NCS5500, NCS5700, NCS540 (Peering Use Case)
- 24.1.1 IOS-XR (Feb 2024): 8k

Security algorithmic chain

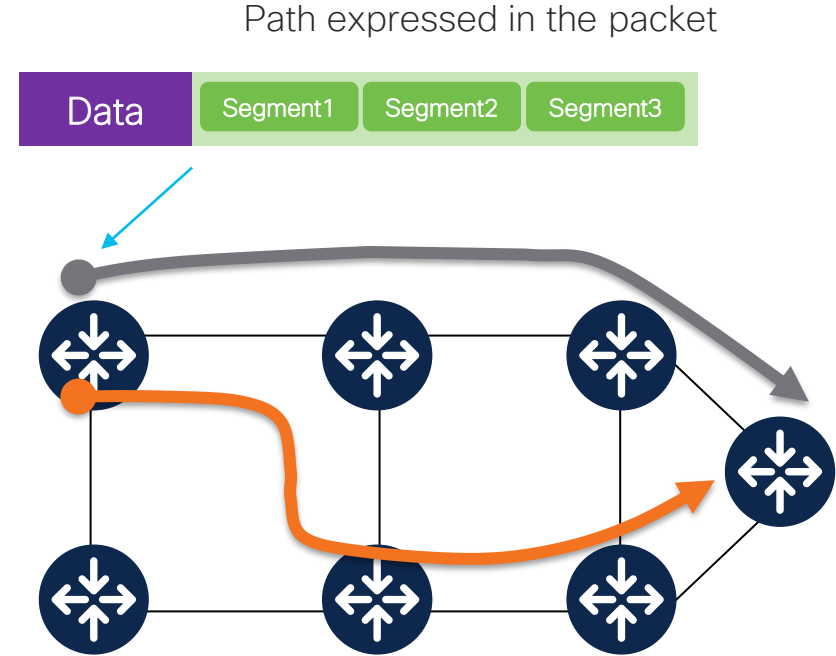


How To Program Security Policy Into the Network Fabric



What is Segment Routing?

- SR is an architecture based on the **Source Routing principle**
- It provides a **stateless IP fabric** with uncompromised **simplicity** and **scale**
- It delivers a unified, **end-to-end policy-aware** network infrastructure



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



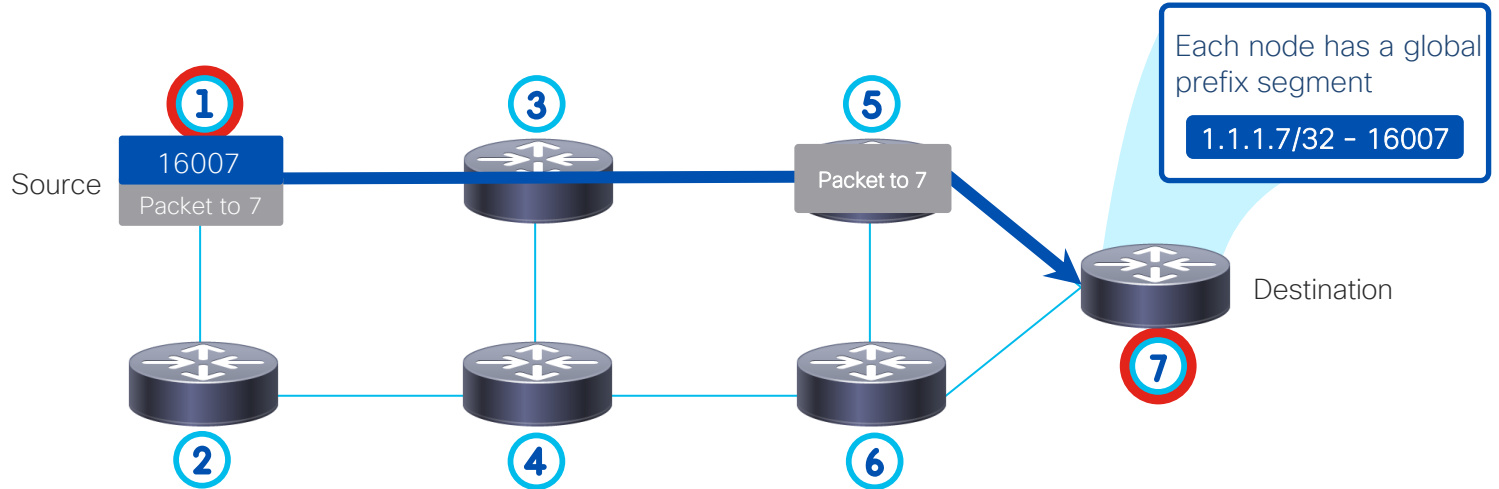
SRv6

- Instantiation of SR on the IPv6 data plane
- A segment is encoded with an IPv6 address

IGP Prefix Segment

Example

Send traffic from Node 1 to Node 7 over the IGP shortest path

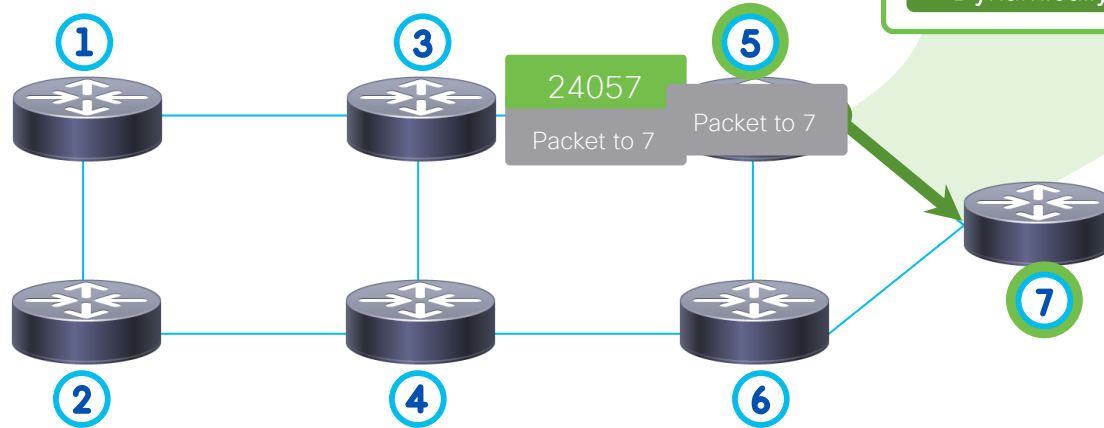


Only one segment is required

IGP Adjacency Segment

Example

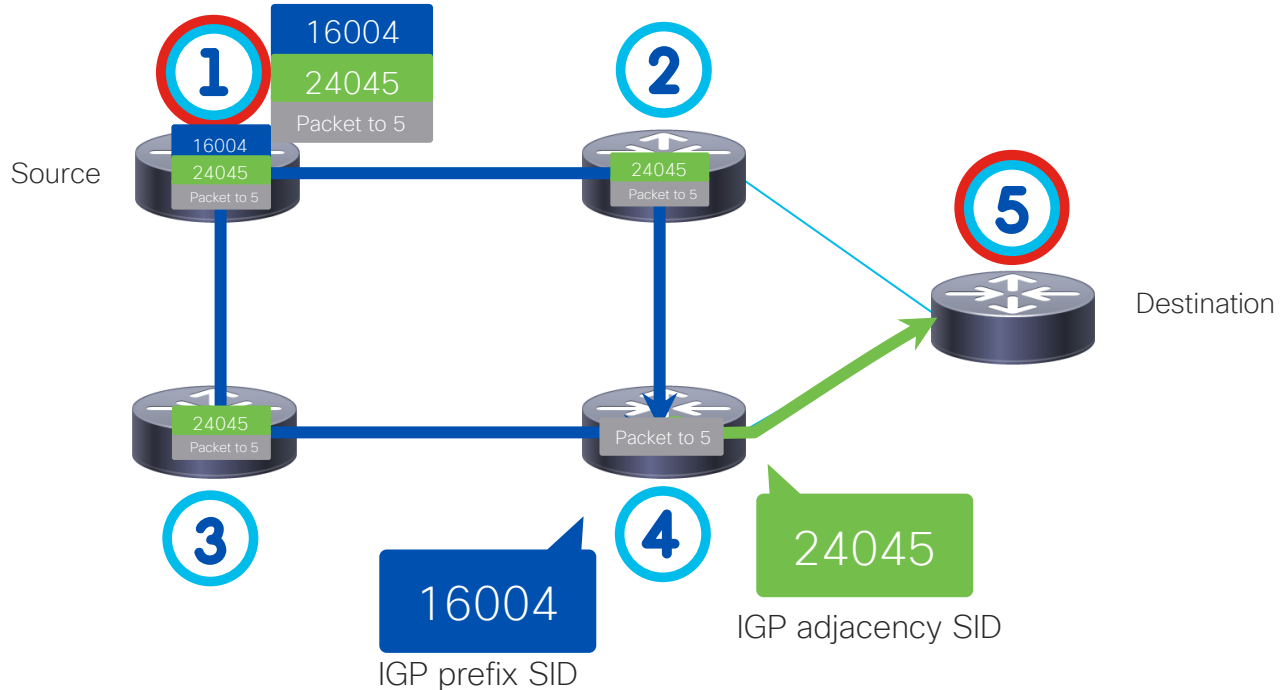
Send traffic from Node 5 to Node 7 over direct link



Combining Segments

Example

Send traffic from Node 1 to Node 5 avoiding the link between Node 2 to Node 5



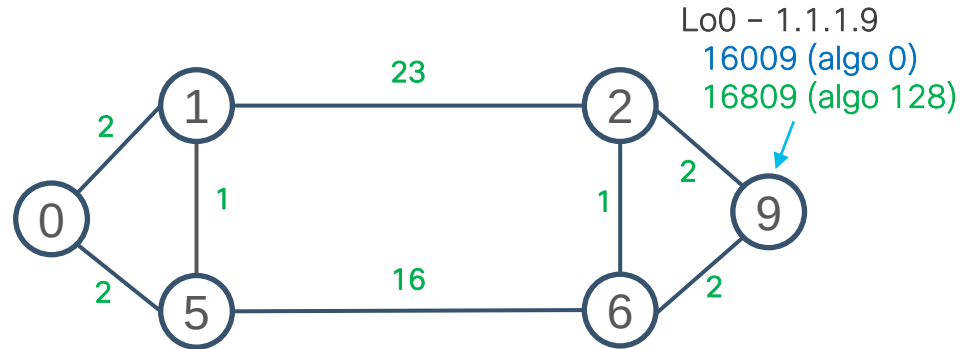
SR Flexible Algorithm – Flex Algo

Sub-Topology
Nodes & Links

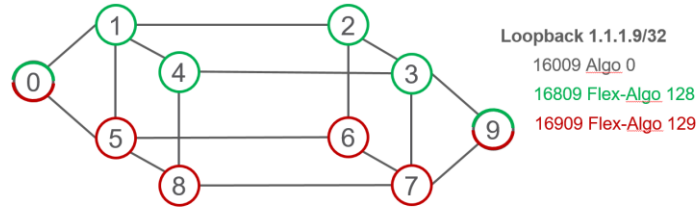
Metric
IGP, TE, Delay

FlexAlgo Protection
TI-LFA

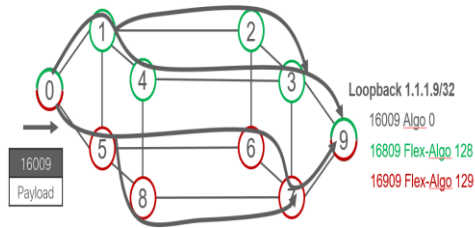
1 node-SID



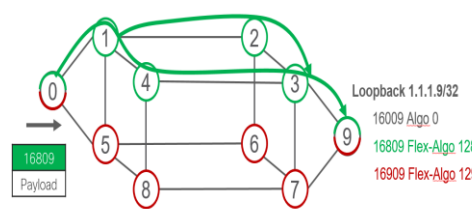
SR IGP Flex Algo – Dual Plane Data Network



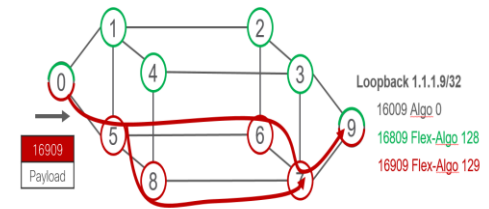
- All the nodes support Algo 0: minimize IGP metric
- **Green nodes** also support 128
- **Red nodes** also support 129



• Path to Node 9 across Algo 0

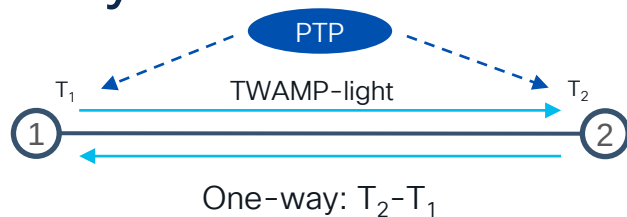
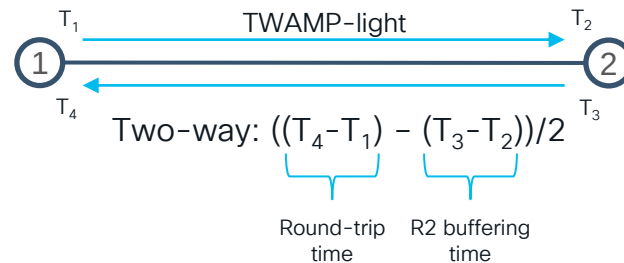


• Path to Node 9 across **Flex-Algo 128**



• Path to Node 9 across **Flex-Algo 129**

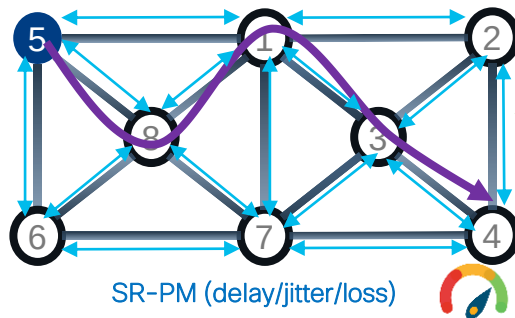
Delay Measurement – Performance Routing



min/max/avg Delay & Jitter
advertised in IGP

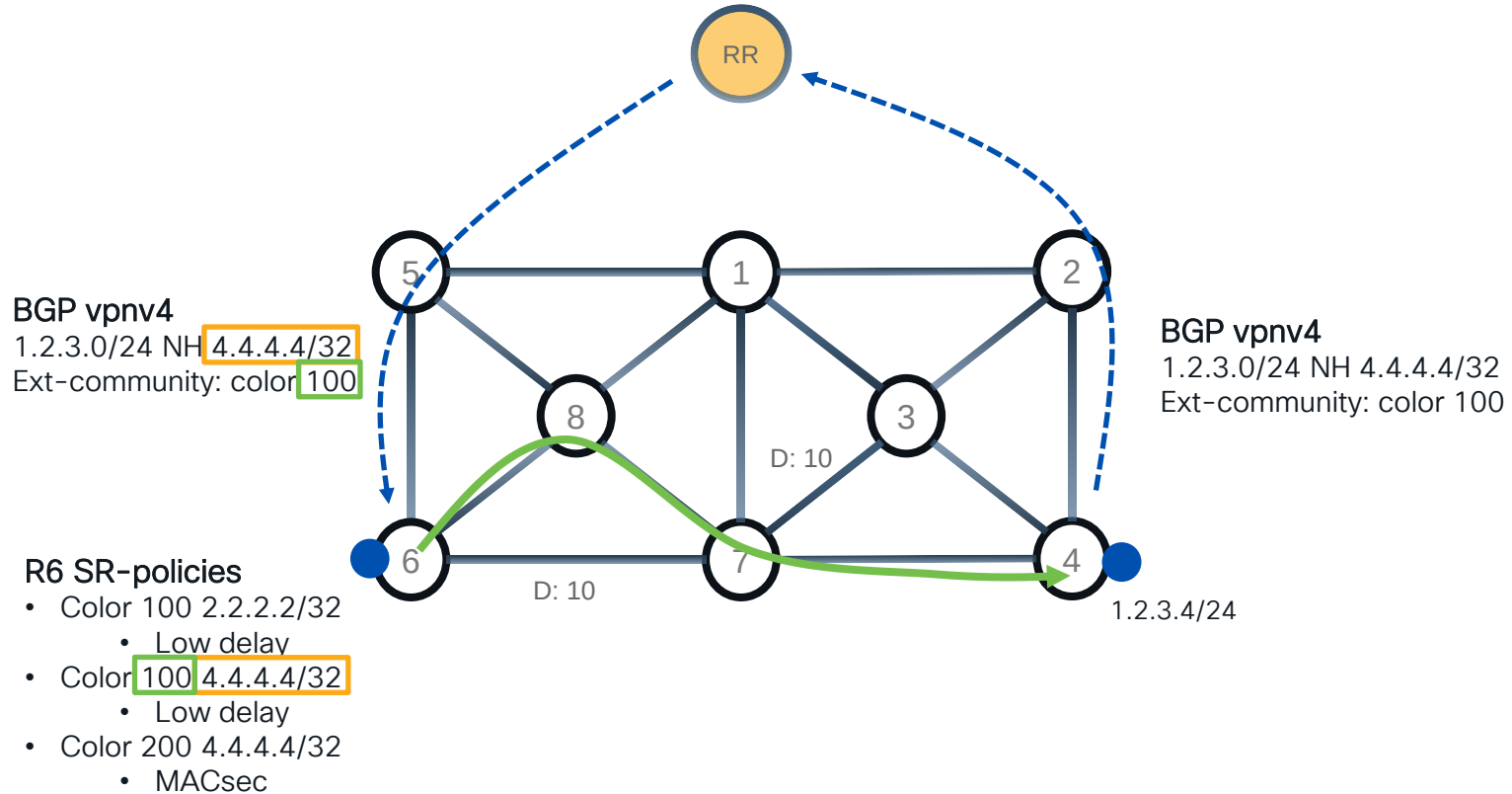
Advertisement
threshold to protect
the network

Minimum delay value used as the delay metric



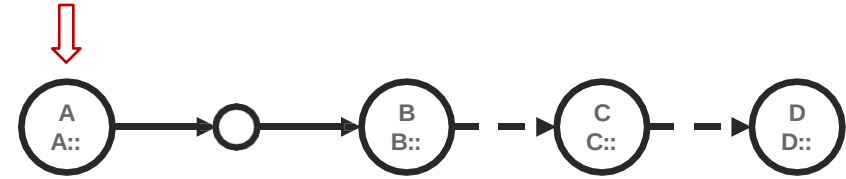
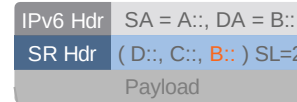
Delay normalization for delay based ECMP

Intent-based Automated Steering



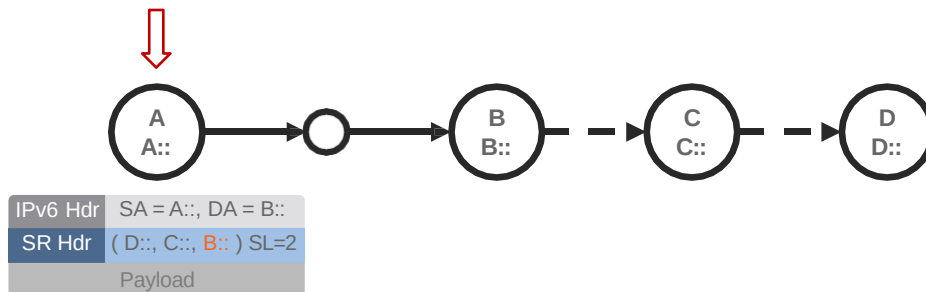
Source Node

- Source node is SR-capable
- SR Header (SRH) is created with
 - Segment list in reversed order of the path
 - Segment List [0] is the LAST segment
 - Segment List [$n - 1$] is the FIRST segment
 - Segments Left is set to $n - 1$
 - First Segment is set to $n - 1$
- IP DA is set to the first segment
- Packet is send according to the IP DA
 - Normal IPv6 forwarding



IPv6 Hdr	Version	Traffic Class	Flow Label	
	Payload Length		Next = 43	Hop Limit
	Source Address = A::			
	Destination Address = B::			
SR Hdr	Next Header	Len= 6	Type = 4	SL = 2
	First = 2	Flags		RESERVED
	Segment List [0] = D::			
	Segment List [1] = C::			
	Segment List [2] = B::			
Payload				

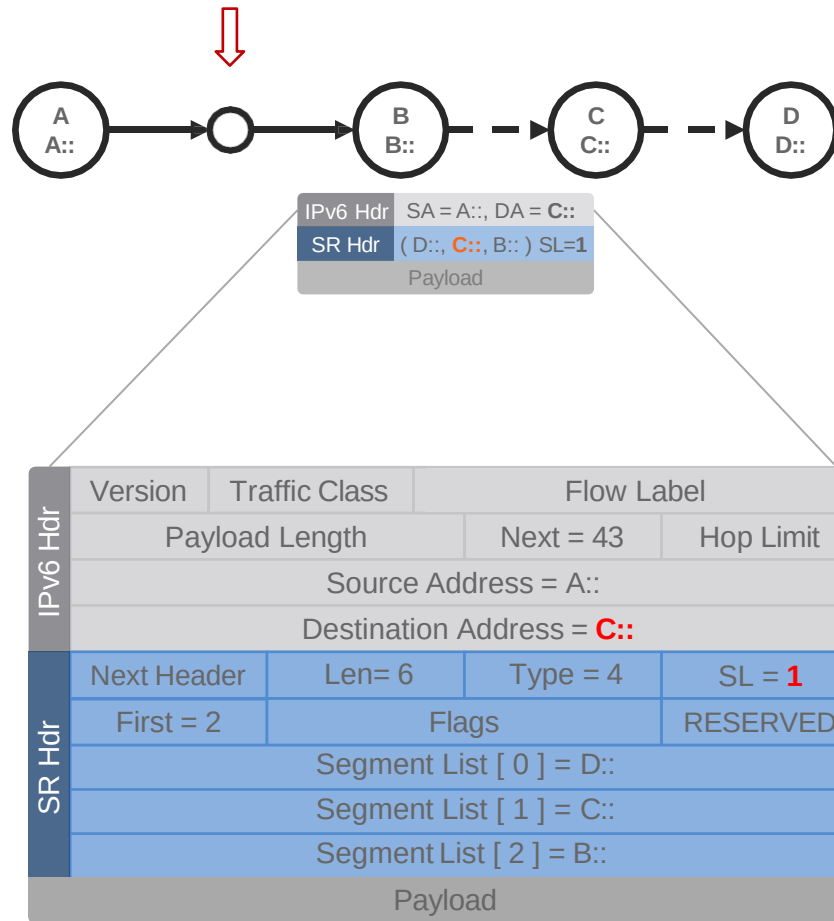
Non-SR Transit Node



- Plain IPv6 forwarding
- Solely based on IPv6 DA
- No SRH inspection or update

SR Segment Endpoints

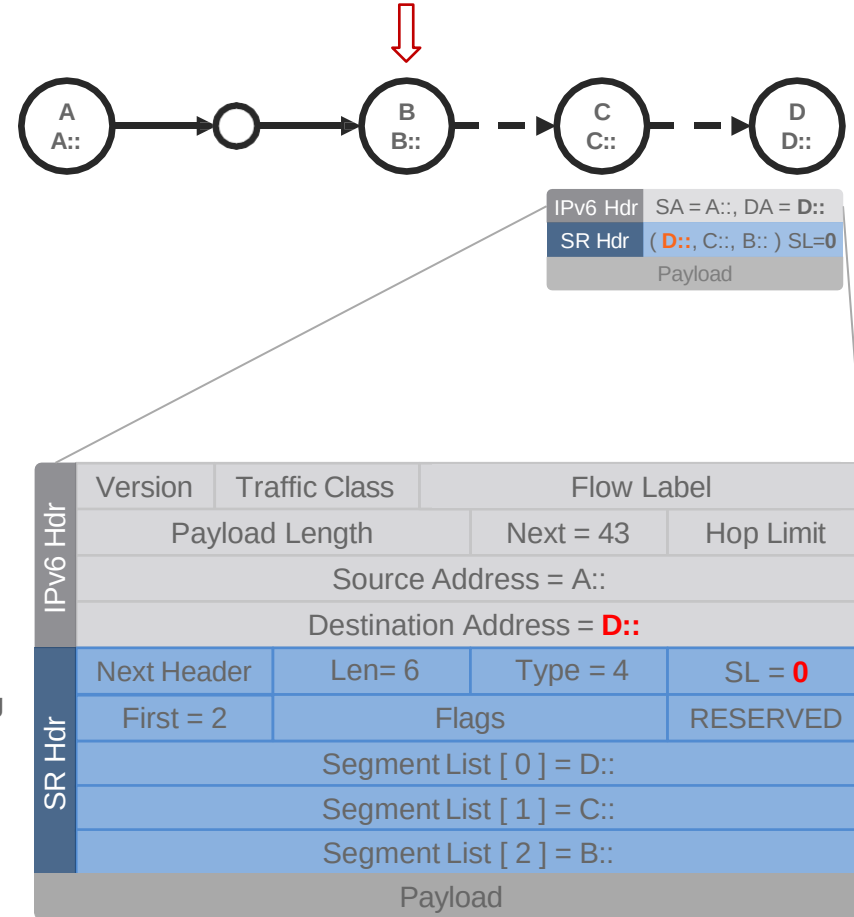
- SR Endpoints: SR-capable nodes whose address is in the IP DA
- SR Endpoints inspect the SRH and do:
 - IF Segments Left > 0, THEN
 - Decrement Segments Left (-1)
 - Update DA with Segment List [Segments Left]
 - Forward according to the new IP DA



SR Segment Endpoints

- SR Endpoints: SR-capable nodes whose address is in the IP DA
- SR Endpoints inspect the SRH and do:
 - IF Segments Left > 0, THEN
 - Decrement Segments Left (- 1)
 - Update DA with Segment List [Segments Left]
 - Forward according to the new IP DA
 - ELSE (Segments Left = 0)
 - Remove the IP and SR header
 - Process the payload:
 - Inner IP: Lookup DA and forward
 - TCP / UDP: Send to socket
 - ...

Standard IPv6 processing
The final destination does not have to be SR-capable.



Segment format (Base Format)

Locator

Function

1111 : 2222 : 3333 : 4444 : 5555 : 6666 : 7777 : 8888

Design

2001 : 0db8 : 0000: 0001 : 0042 : 0000:0000:0000

Prefix

Router ID

Function

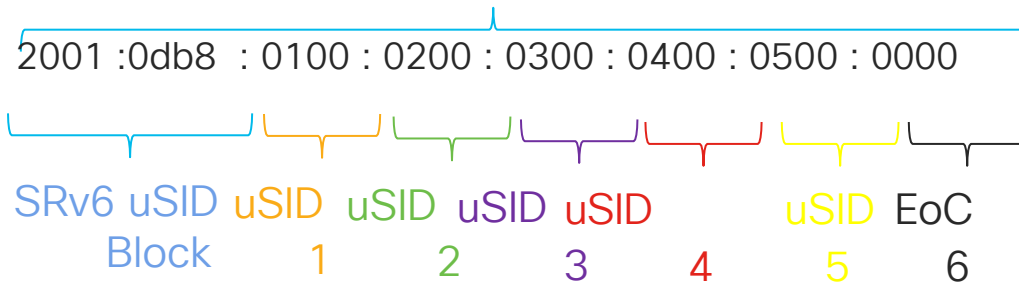
SA:2001::1	
DA:2001:db8:0:4:1:0:0:0	
NH:RH	
Type:4 (SRH)	
NH:IPv4 SL:1	
Segment List:	
[0]:	2001:db8:0:5:45:0:0:0
1 :	2001:db8:0:4:1:0:0:0
2 :	2001:db8:0:3:48:0:0:0
3 :	2001:db8:0:2:1:0:0:0
4 :	2001:db8:0:1:45:0:0:0
SA:7.5.4.3	
DA:11.6.19.71	
Port:UDP	
UDP Header/Data	

Srv6 uSID format

: 0100 : =SRV6 uSID

16 bits here, but can be anything

SRV6 uSID Carrier



32 bits here,
but can be anything

CISCO *Live!*

SRV6 Encapsulation

```
SA: 2001::1
DA: 2001:db8:0:4:1:0:0:0
NH: RH

Type: 4 (SRH)
NH: IPv4 | SL: 1
Segment List:
[0]: 2001:db8:0:5:45:0:0:0
1 : 2001:db8:0:4:1:0:0:0
2 : 2001:db8:0:3:48:0:0:0
3 : 2001:db8:0:2:1:0:0:0
4 : 2001:db8:0:1:42:0:0:0
```

```
SA: 7.5.4.3
DA: 11.6.19.71
Port: UDP
```

UDP Header/Data

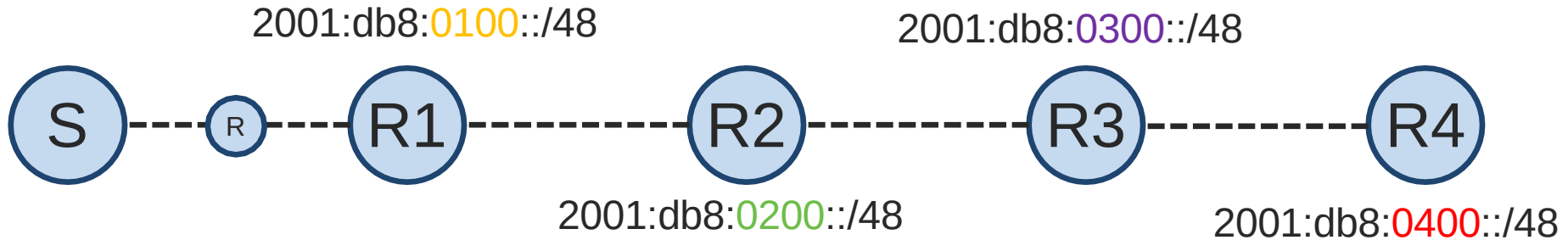
SRV6 uSID Encapsulation

```
SA: 2001::1
DA: 2001:db8:100:200:300:400:500::
NH: IPv4
```

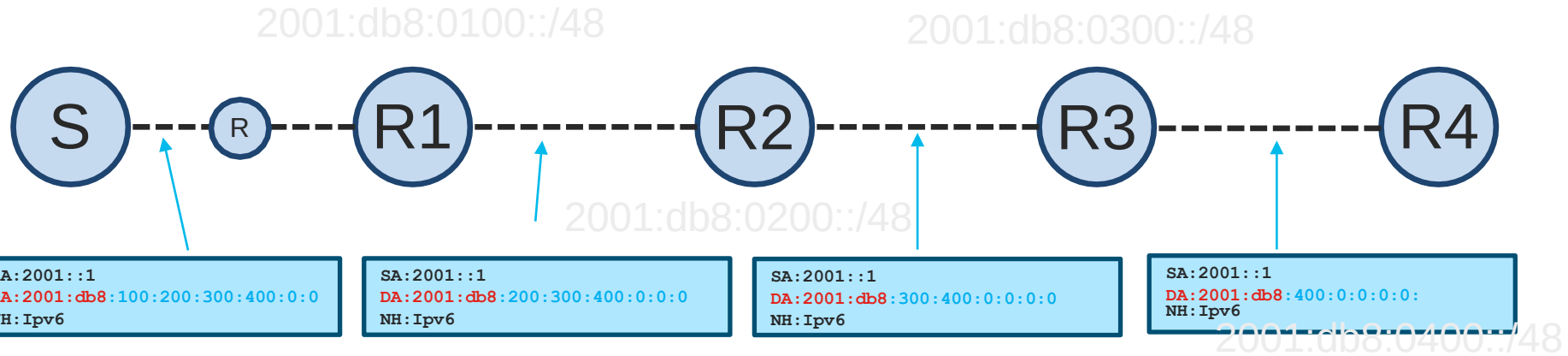
```
SA: 7.5.4.3
DA: 11.6.19.71
Port: UDP
```

UDP Header/Data

Srv6 uSID Locator Advertisement



Srv6 uSID Forwarding

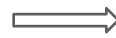


Shift & Forward

Incomming DA 2001:db8:100:200:300:400::

Shift 2001:db8:200:300:400::

Forward Lookup result for- 2001:db8:200::/48



Srv6 uSID More Than 6 SIDs?

100->200->300->400->500->600->700->800->900->a00->b00

Carrier 1 2001 : 0db8 : 0100 : 0200 : 0300 : 0400 : 0500 : 0600

Carrier 2 2001 : 0db8 : 0700 : 0800 : 0900 : 0a00 : 0b00 : 0000

SA:2001::1 DA:2001:db8:100:200:300:400:500:600 NH:RH
Type:4 (SRH) NH:IPv4 SL:0 Segment List: [0] : 2001:db8:700:800:900:a00:b00::
SA:7.5.4.3 DA:11.6.19.71 Port:UDP
UDP Header/Data

Shift & Forward
END of Carrier
-> is there SRH?
Decrement SL
Copy New SID (Carrier)
PSP

Srv6 uSID is SRv6

SA:2001::1

DA:2001:db8:100:200:300:400:500:600

NH:RH

Type: 4 (SRH)

NH:IPv4 | SL:1

Segment List:

[0]: 2001:1:0:1:44::

1 : 2001:db8:100:200:300:400:500:600

2 : 2001:1:0:2:1::

3 : 2001:db8:700:f111::

4 : 2001:db9:500:800:900::

SA:7.5.4.3

DA:11.6.19.71

Port:UDP

UDP Header/Data

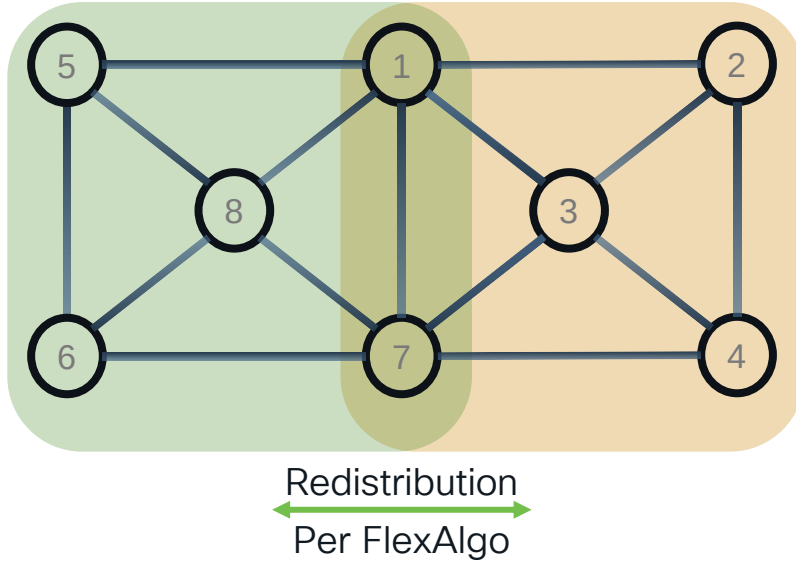
Any combination is allowed

SRv6 uSID Carrier

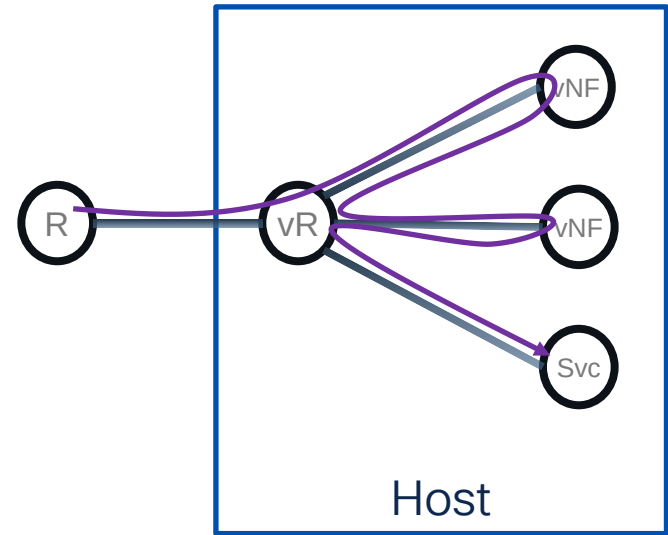
SRv6 SID

SRv6 advantages

Optimized Multi-domain SLA

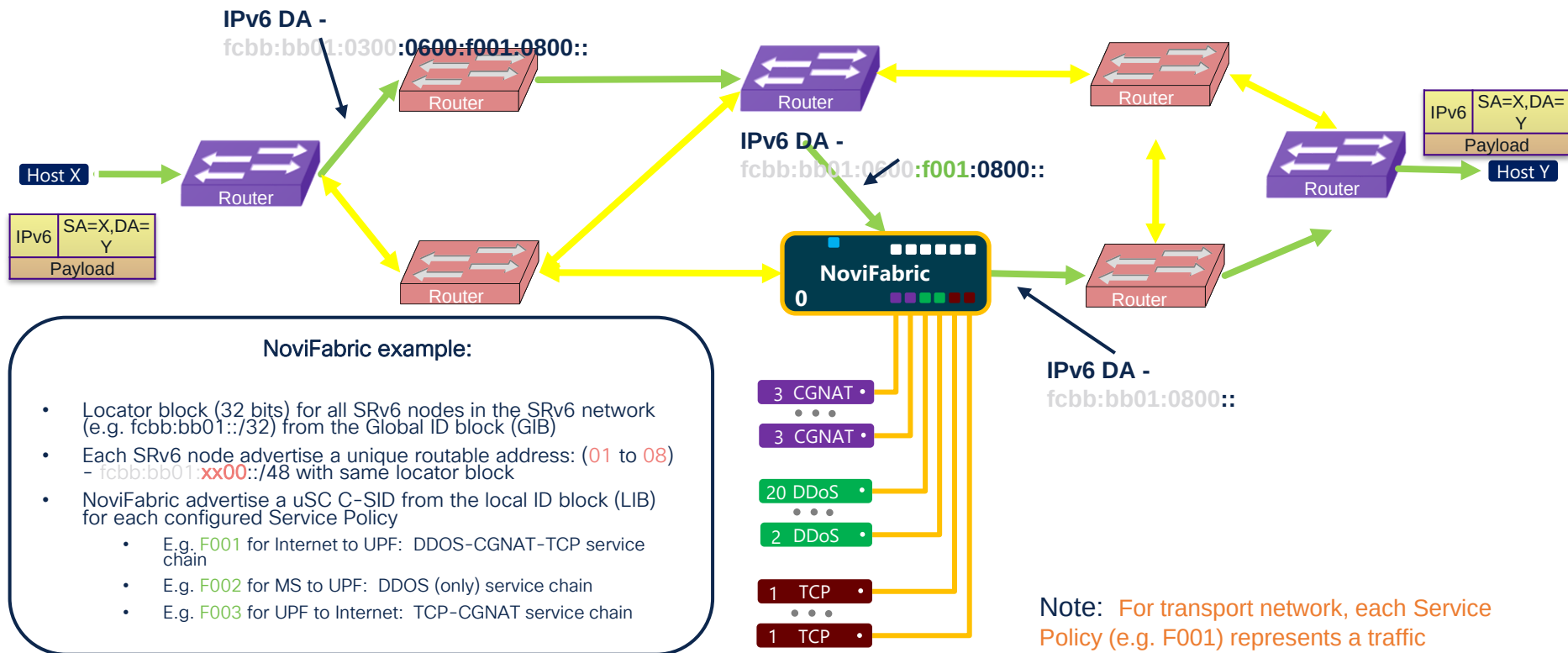


Optimized Service Chaining



Service And Policy Insertion with a Service Proxy - Noviflow

Segment Routing over IPv6 (SRv6) - NoviFabric



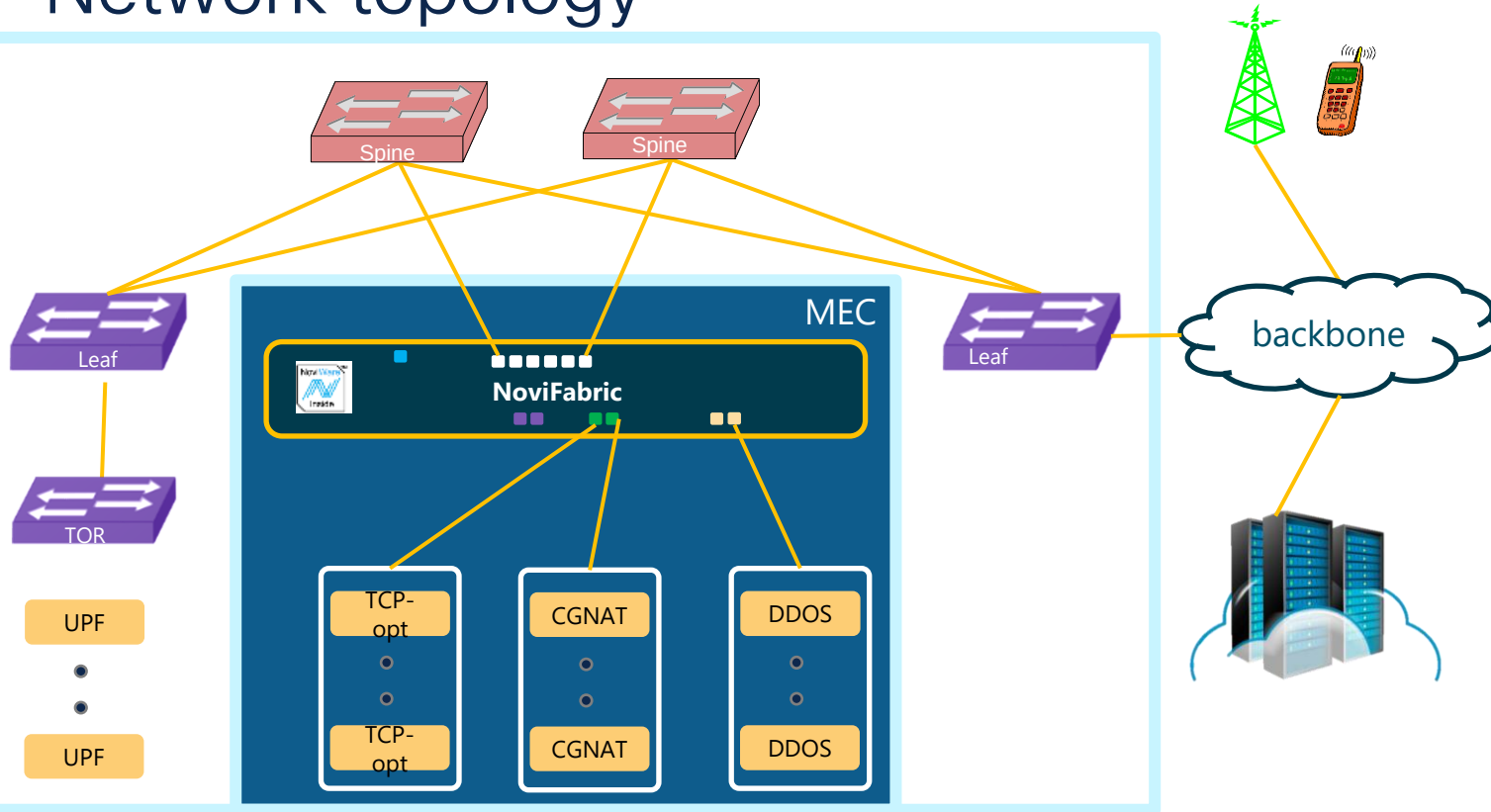
NoviFabric – SRv6 Service proxy

- Introduces a new variant of binding segment: **Service Chain Segment (End.SC)**
 - Act as an orchestrator and enforcement point for a Service policy.
 - Invokes, in order, the services listed in the service policy
 - Support for a mix of different service types (see side box)
- End.SC benefits
 - Greater scalability
 - Reduced overhead of SRH header
 - Network opacity (e.g. opaque execution of security services)
 - Service independence

Service types

- Type I – **SR aware** -- Service is a SR node (has its own SID).
 - Packet with SRv6 header is transmitted to and returned by the service
 - It executes SR process on the SR header and its own service behavior on encapsulated packet
- Type II – **SR passthrough** -- Service is not an SR node
 - Packet with SRv6 header is transmitted and returned by the service
 - Outer SRv6 header is left unchanged by the service
 - Service executes its own service behavior on the encapsulated packet
- Type III – **SR unaware** -- Service is not an SR node
 - Information from SRv6 header is embedded in packet transmitted to the service
 - SRv6 header is reconstructed based on policy information

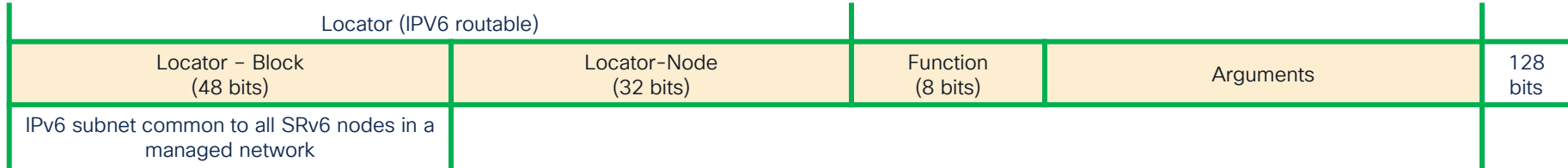
Network topology



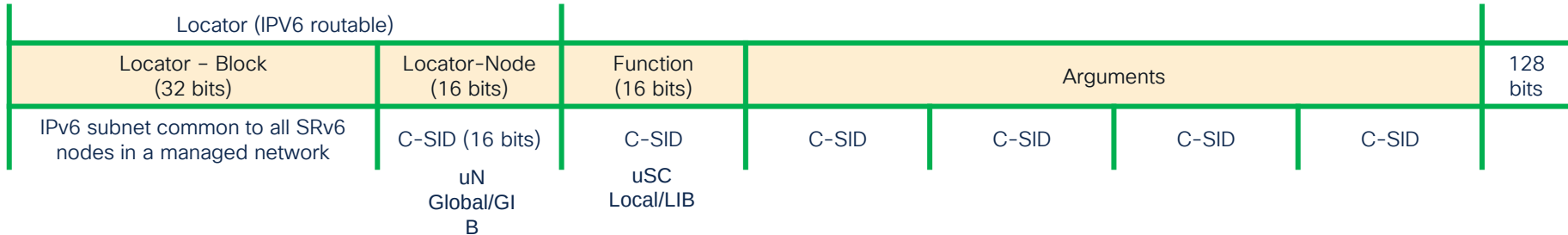
Supported SRv6 Segment ID (SID) format

Version	Traffic Class	Flow Label	Payload Length		Next Header=43	Hop Limit	8 bytes	IPv6 Header 40 bytes
Source IPv6 Address							16 bytes	
Destination IPv6 Address							16 bytes	
Next Header	Hdr Ext Len	Routing Type=4	Segments Left	Last Entry	Flags	Tags	8 Bytes	SRH Header (Hdr Ext Len) bytes
Segment List[0] (IPv6 address)							16 bytes	
...							...	
Segment List[n-1] (IPv6 address)							16 bytes	
Optional Type Length Value (TLV) objects							Variable	
Payload (Ethernet, IPv4 or IPv6)							Variable	Payload (variable length)

SID (uncompressed, full 128 bits)

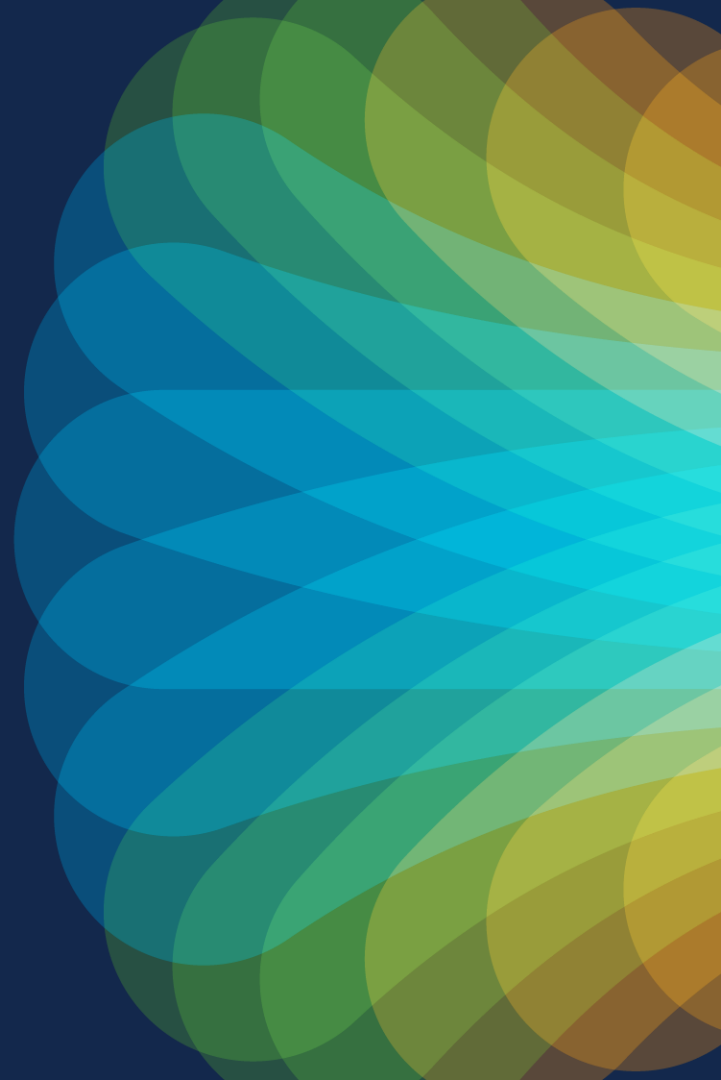


C-SID (Compressed SID, F3216)



Note: NEXT-C-SID flavor only

Where To Learn More?



Resources I Use Often

- Github for SRv6:
<https://github.com/topics/srv6>
- BGP colored Prefix Routing (CPR) for SRv6 based services:
<https://datatracker.ietf.org/doc/draft-wang-idr-cpr/>
- BGP Overlay Services Based on SRv6:
<https://datatracker.ietf.org/doc/rfc9252/>
- SRv6 for Zebra/Linux:
<https://github.com/coreswitch/zebra/blob/master/docs/srv6.md>

SRv6 University and E2E Network Transformation (Peering/DC/Transport)
[TECSPG-3052]
Brendon Mifsud, Principal Architect, Cisco Systems, Inc.
Cris He, Customer Delivery Architect, Cisco Systems, Inc.
Schedule Tuesday, Dec 5 | 9:00 AM - 1:00 PM AEDT | Meeting Room 209

FULL CONFERENCE **IT LEADERSHIP**
SRv6 for Next-Generation Transport Networks [BRKSPG-1676]
Dan Clark, Systems Architect, Cisco Systems
Schedule Wednesday, Dec 6 | 4:00 PM - 5:30 PM AEDT | Meeting Room 209

EXPLORER **FULL CONFERENCE** **IT LEADERSHIP**
Transform Your DCI with SRv6 - Crosswork, SP Routers, and IOS XR [DEMO-SP06]

EXPLORER **FULL CONFERENCE** **IT LEADERSHIP**
SRv6 uSID Traffic Engineering Lab [LABSPG-2787]

FULL CONFERENCE **IT LEADERSHIP**
Protect Your Network Using Programmability and Segment Routing [BRKSPG-2125]
Mike Geller, Distinguished Architect, Cisco Systems, Inc.
Schedule Wednesday, Dec 6 | 2:40 PM - 3:40 PM AEDT | Meeting Room 204

EXPLORER **FULL CONFERENCE** **IT LEADERSHIP**
Enable Seamless Hybrid Cloud - SP Routers, IOS XR, and Accedian [DEMO-SP07]

EXPLORER **FULL CONFERENCE** **IT LEADERSHIP**
Drive Operational Efficiency - Crosswork Network Controller [DEMO-SP03]

Learn More About The Solution

Cisco Secure DDoS Edge Protection Landing Page

<https://www.cisco.com/site/us/en/products/security/ddos-edge-protection/index.html>

Cisco Secure DDoS Protection web page

<https://www.cisco.com/go/secure-ddos>

Cisco “What is a DDoS Attack?” web page,

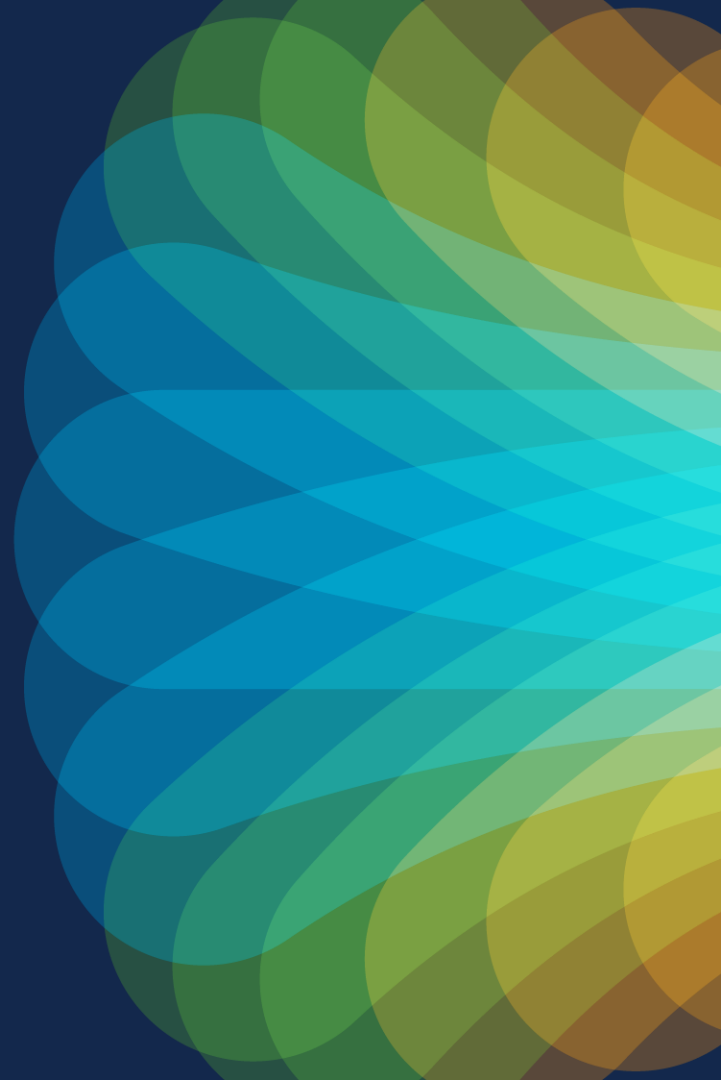
<https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html>

DDoS Edge Protection on DEVNET,

<https://developer.cisco.com/docs/secure-ddos-edge-protection>



Conclusion



CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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!*

#CiscoLiveAPJC

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a dark blue, sans-serif font, positioned to the left of a bright, multi-colored sunburst graphic that radiates from the right side of the image.

Let's go

#CiscoLiveAPJC