Cisco live!

What You Make Possible

TOMORROW
starts here.

cisco

Understanding MPLS

BRKMPL-1101

TOMORROW starts here.

Session Goals

Objectives

- Understand the problems MPLS is addressing
- Understand the major MPLS technology components
- Understand typical MPLS applications
- Understand benefits of deploying MPLS
- Learn about MPLS futures; where MPLS is going

Agenda

Topics

- Introduction
- MPLS Technology Basics
- MPLS Layer-3 VPNs
- MPLS Layer-2 VPNs
- Advanced Topics
- Summary

Introduction

Why Multi Protocol Label Switching?

- SP/Carrier perspective
  - Reduce costs (CAPEX); consolidate networks
  - Consolidated network for multiple Layer-2/3 services
  - Support increasingly stringent SLAs
  - Handle increasing scale/complexity of IP-based services
- Enterprise/end-user perspective
  - Campus/LAN
    - Need for network segmentation (users, applications, etc.)
  - WAN connectivity (connecting enterprise networks)
    - Need for easier configuration of site-to-site WAN connectivity

MPLS Applications

	Service Providers	Enterprise Data Centre	Data Centre Interconnects	EWAN Edge
Key Features	L2/L3VPN's TE/FRR QoS High Availability	VPN's TE/FRR High Availability	VPN's / VRF's VRF-Aware Security High Availability	VPN's / VRF's VRF Aware Security High Availability
Applications	Hosted Data Centres Data Centre interconnect Segmentation for IT Mergers, Acquisitions, spinoffs	Departmental segmentation Service multiplexing Security Mergers, Acquisitions, spinoffs	Disaster Recovery Vmotion support Branch Interconnects	Internet Access Branch Connectivity

- **Network Consolidation** – Merging Multiple parallel network into a shared infrastructure
- **Network segmentation** – By user groups or business function
- **Service and policy centralisation** – Security policies and appliances at a central location
- **New applications readiness** – Converged multi-service network
- **Increased network security** – User groups segmentation with VPNs

What is MPLS?

Brief Summary

- It's all about labels …
- Use the best of both worlds
  - Layer-2 (ATM/FR): efficient forwarding and traffic engineering
  - Layer-3 (IP): flexible and scalable
- MPLS forwarding plane
  - Use of labels for forwarding Layer-2/3 data traffic
  - Labeled packets are being switched instead of routed
    - Leverage layer-2 forwarding efficiency
- MPLS control/signalling plane
  - Use of existing IP control protocols extensions + new protocols to exchange label information
    - Leverage layer-3 control protocol flexibility and scalability

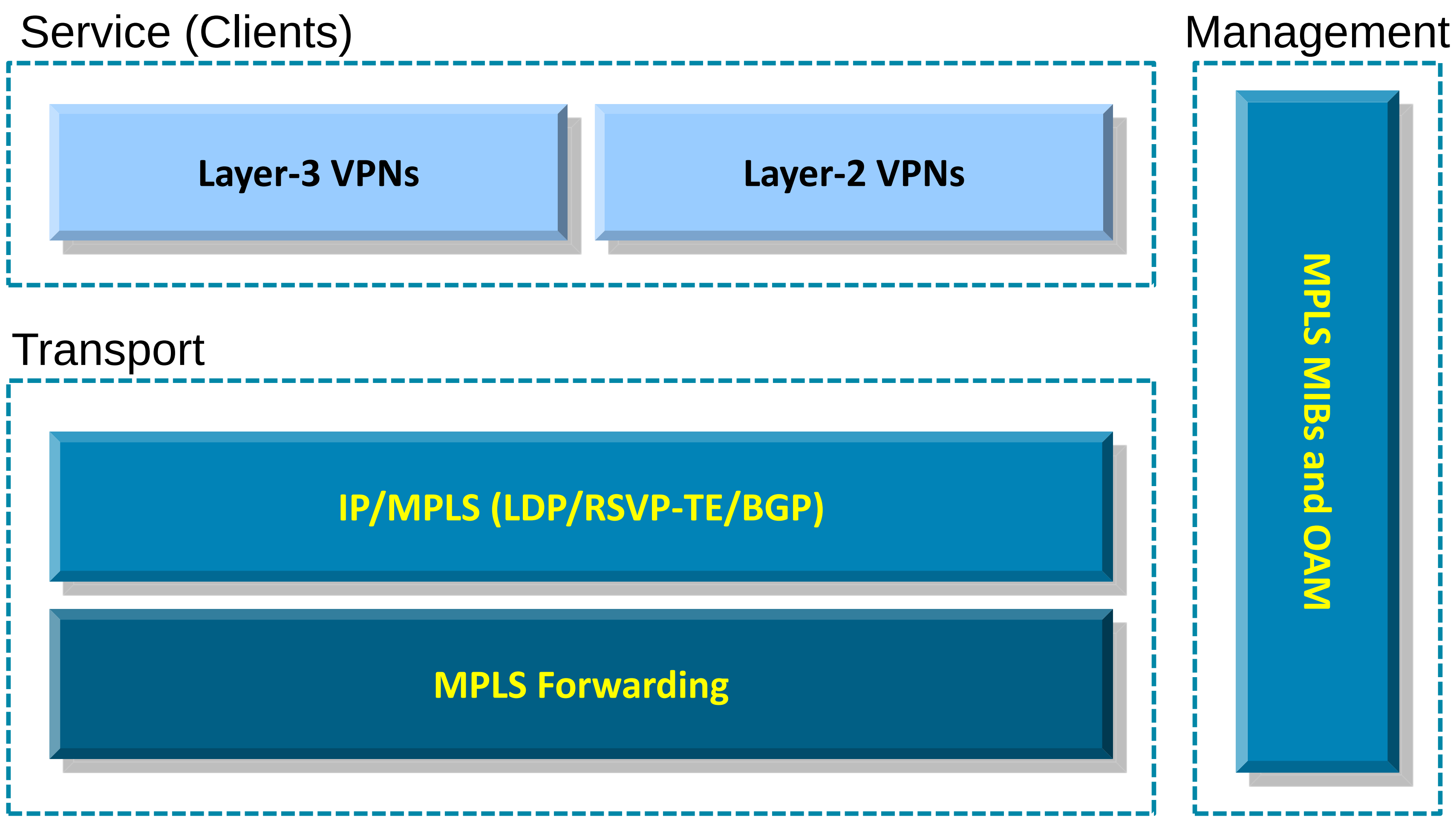
MPLS Technology Basics

Technology Building Blocks of MPLS

Topics

Basics of MPLS Signalling and Forwarding

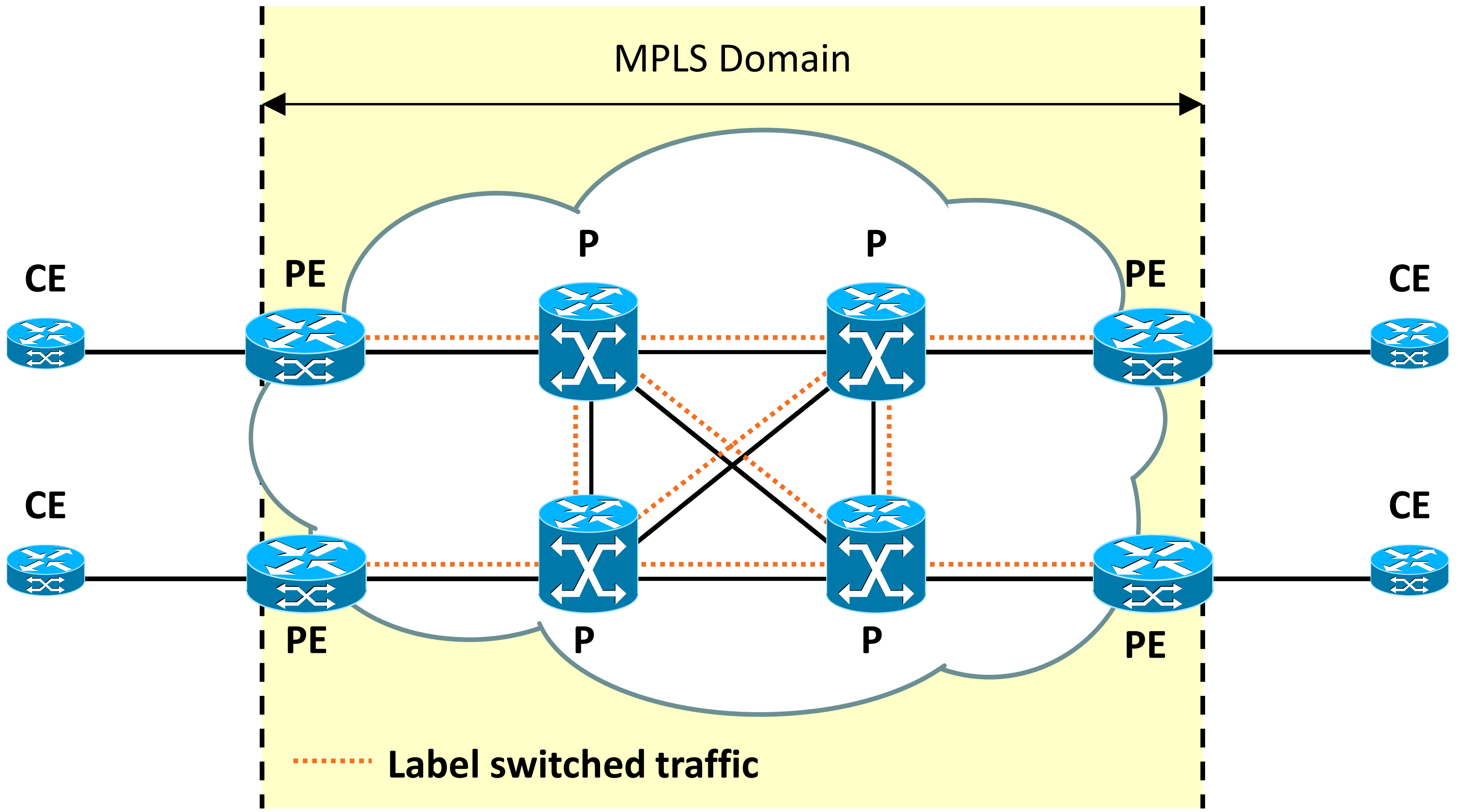
- MPLS reference architecture
- MPLS Labels
- MPLS signalling and forwarding operations
- MPLS Traffic Engineering
- MPLS OAM and MIBs



MPLS Reference Architecture

Different Type of Nodes in a MPLS Network

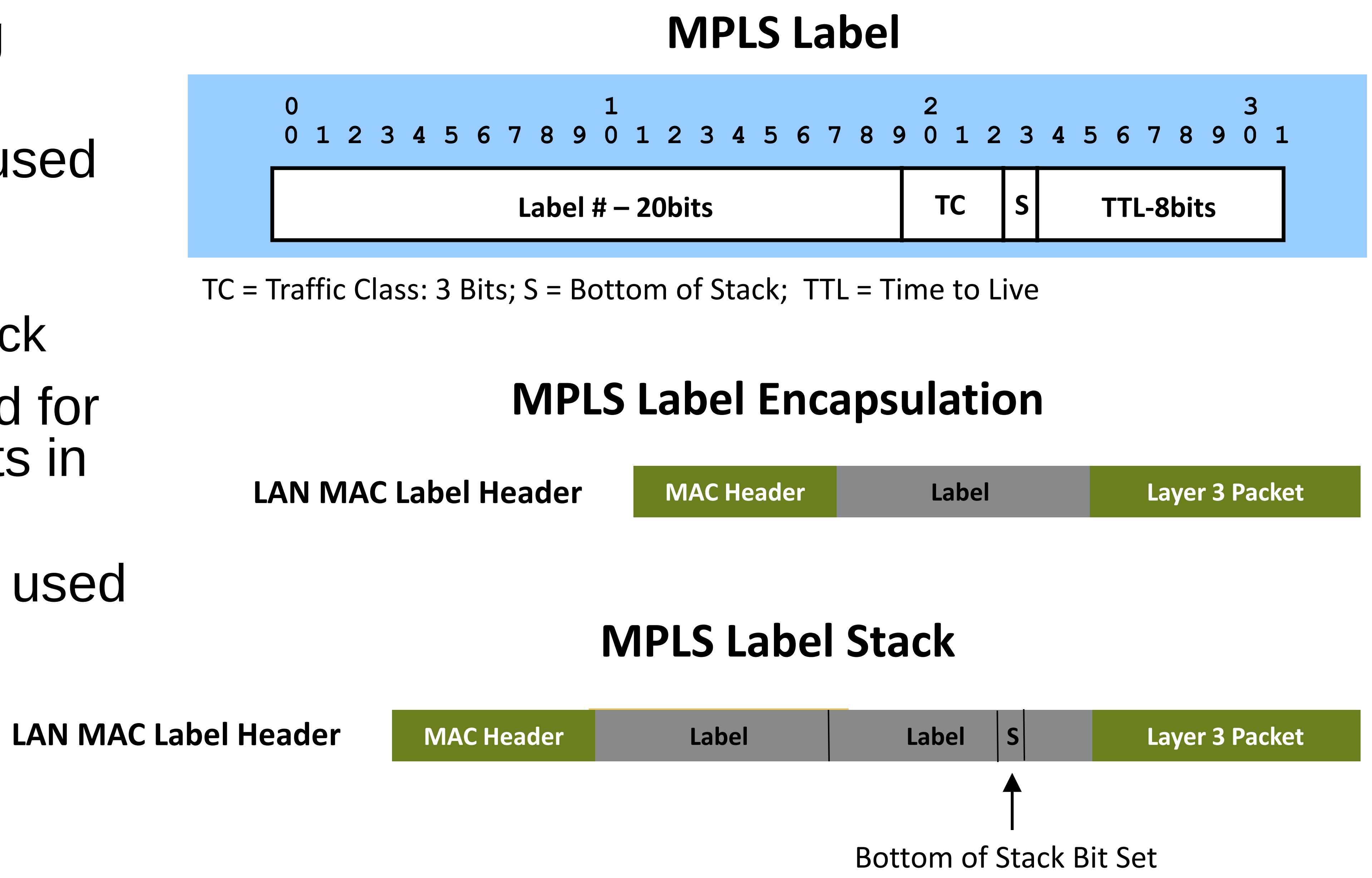
- P (Provider) router
  - – Label switching router (LSR)
  - – Switches MPLS-labeled packets
- PE (Provider Edge) router
  - – Edge router (LER)
  - – Imposes and removes MPLS labels
- CE (Customer Edge) router
  - – Connects customer network to MPLS network



MPLS Shim Labels

Label Definition and Encapsulation

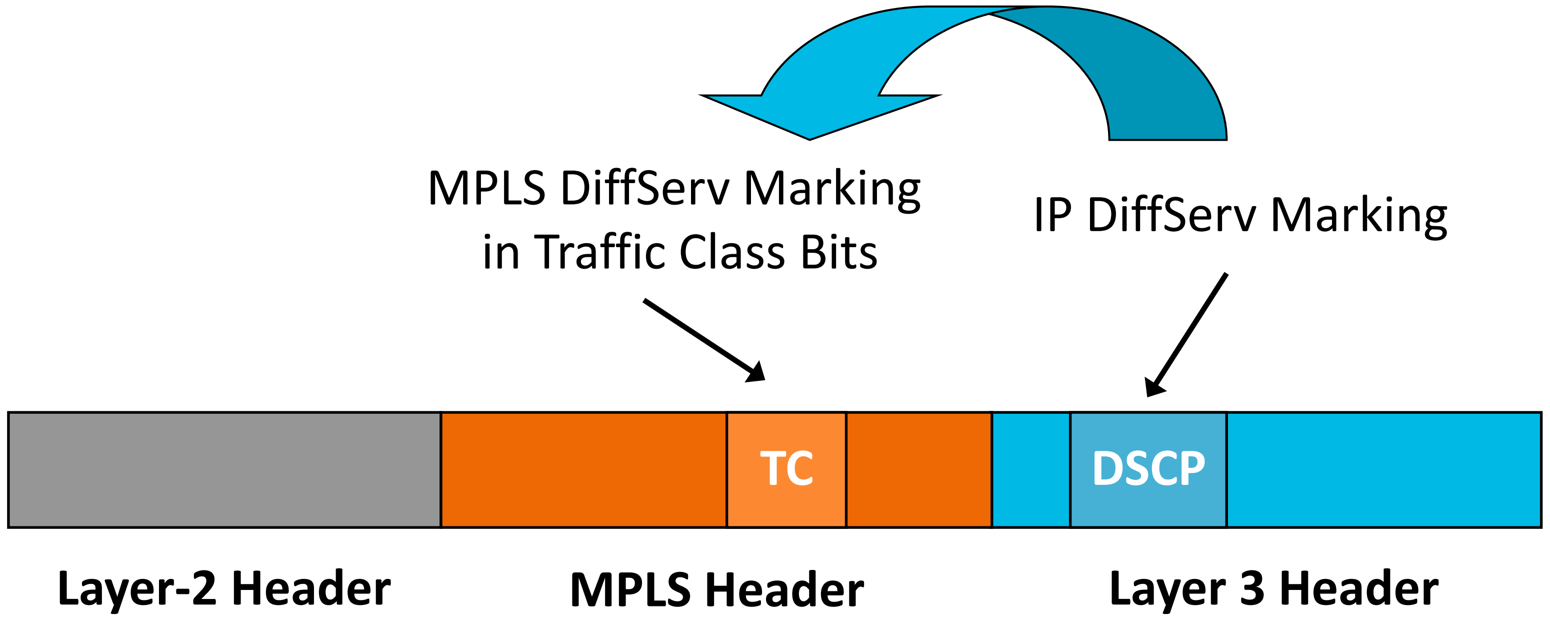
- Labels used for making forwarding decision
- Multiple labels can be used for MPLS packet encapsulation
  - Creation of a label stack
- Outer label always used for switching MPLS packets in network
- Remaining inner labels used to specific services (e.g., VPNs)



MPLS QoS

QoS Marking in MPLS Labels

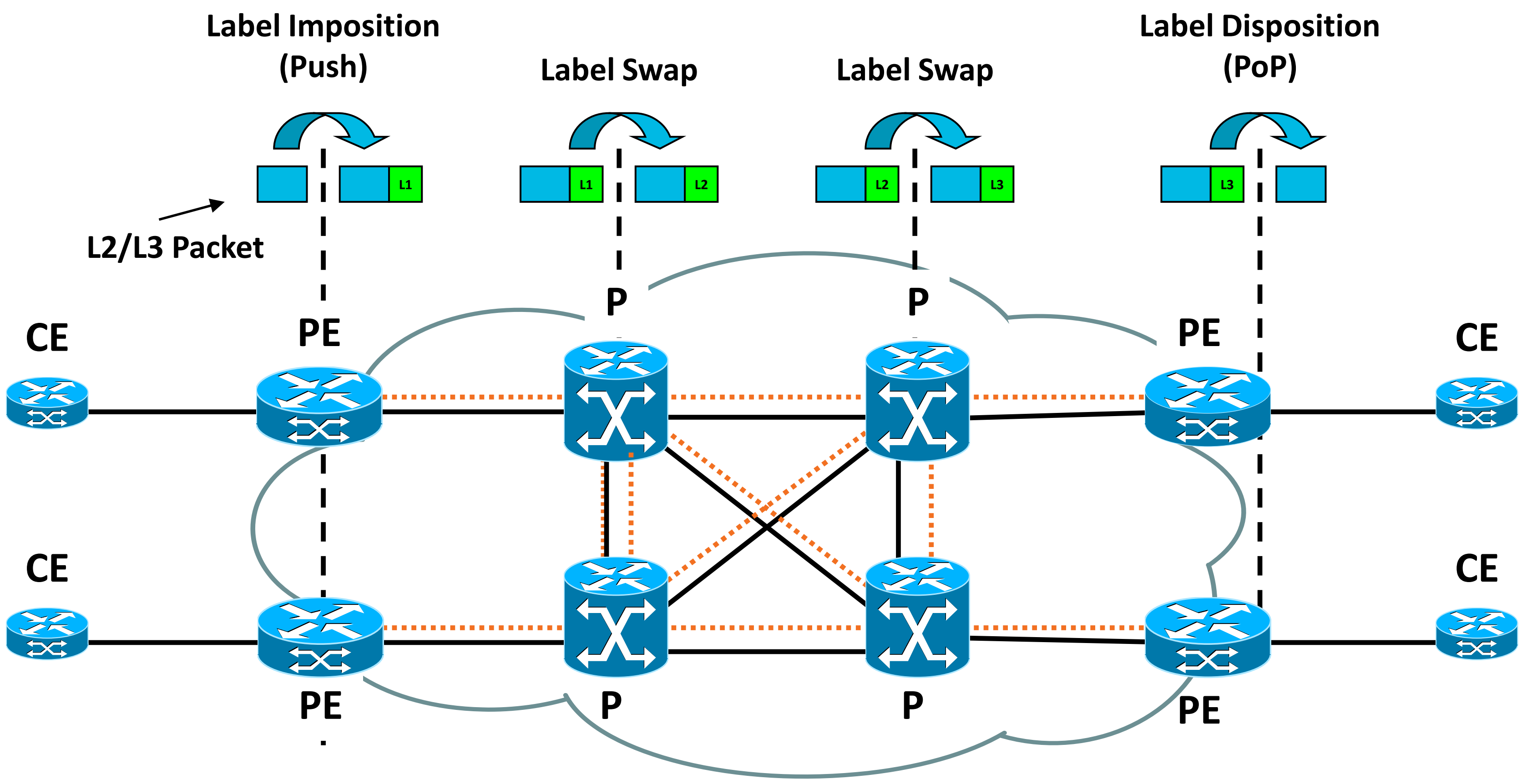
- MPLS label contains 3 TC bits
- Used for packet classification and prioritisation
  - Similar to Type of Service (ToS) field in IP packet (DSCP values)
- DSCP values of IP packet mapped into TC bits of MPLS label
  - At ingress PE router
- Most providers have defined 3–5 service classes (TC values)
- Different DSCP <-> TC mapping schemes possible
  - Uniform mode, pipe mode, and short pipe mode



Basic MPLS Forwarding Operations

How Labels Are Being Used to Establish End-to-end Connectivity

- Label imposition (PUSH)
  - By ingress PE router; classify and label packets
  - Based on Forwarding Equivalence Class (FEC)
- Label swapping or switching
  - By P router; forward packets using labels; indicates service class & destination
- Label disposition (POP)
  - By egress PE router; remove label and forward original packet to destination CE



MPLS Path (LSP) Setup and Traffic Forwarding

MPLS Traffic Forwarding and MPLS Path (LSP) Setup

- LSP signalling
  - Either LDP* or RSVP
  - Leverages IP routing
  - Routing table (RIB)
- Exchange of labels
  - Label bindings
  - Downstream MPLS node advertises what label to use to send traffic to node
- MPLS forwarding
  - MPLS Forwarding table (FIB)

	IP	MPLS
Forwarding	Destination address based Forwarding table learned from control plane TTL support	Label based Forwarding table learned from control plane TTL support
Control Plane	OSPF, IS-IS, BGP	OSPF, IS-IS, BGP LDP, RSVP
Packet Encapsulation	IP Header	One or more labels
QoS	8 bit TOS field in IP header	3 bit TC field in label
OAM	IP ping, traceroute	MPLS OAM

* LDP signalling assumed in next examples

MPLS Path (LSP) Setup

Signalling Options

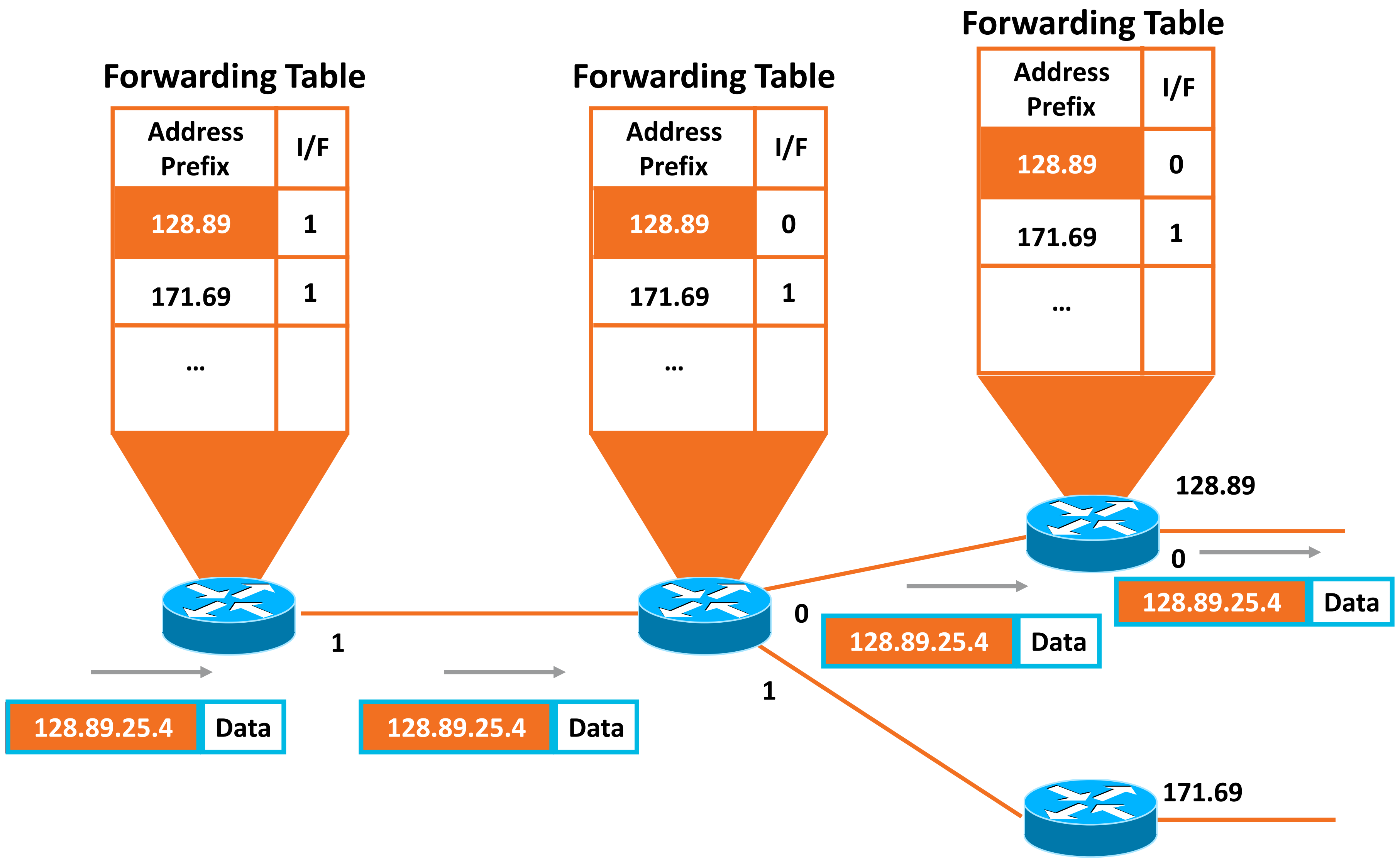
- LDP signalling
  - – Leverages existing routing
- RSVP signalling
  - – Aka MPLS RSVP/TE
  - – Enables enhanced capabilities, such as Fast ReRoute (FRR)

	LDP	RSVP
Forwarding path	LSP	LSP or TE Tunnel Primary and, optionally, backup
Forwarding Calculation	Based on IP routing database Shortest-Path based	Based on TE topology database Shortest-path and/or other constraints (CSPF calculation)
Packet Encapsulation	Single label	One or two labels
Signalling	By each node independently Uses existing routing protocols/information	Initiated by head-end node towards tail-end node Uses routing protocol extensions/information Supports bandwidth reservation Supports link/node protection

IP Packet Forwarding Example

Basic IP Packet Forwarding

- IP routing information exchanged between nodes
  - Via IGP (e.g., OSFP, IS-IS)
- Packets being forwarded based on destination IP address
  - Lookup in routing table (RIB)



MPLS Path (LSP) Setup

Step 1: IP Routing (IGP) Convergence

- Exchange of IP routes
  - OSPF, IS-IS, EIGRP, etc.
- Establish IP reachability

Forwarding Table

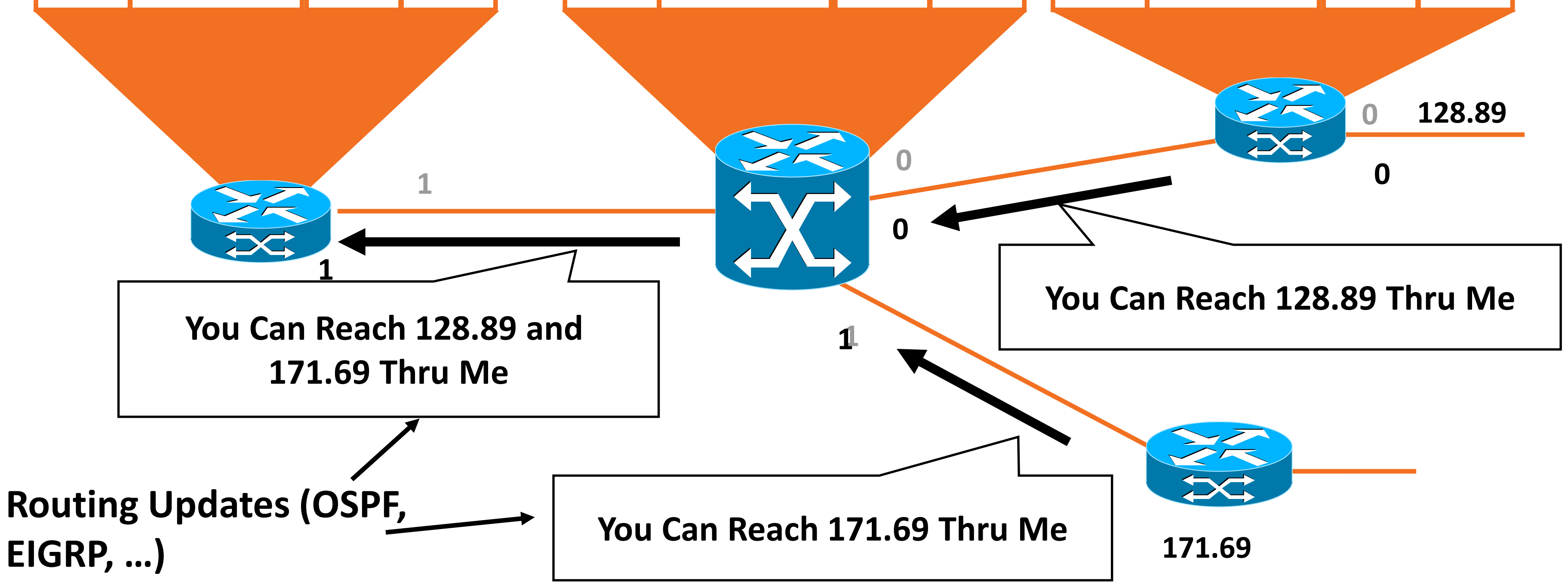
In Label	Address Prefix	Out I'face	Out Label
	128.89	1	
	171.69	1	
	…	…	

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
	128.89	0	
	171.69	1	
	…	…	

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
	128.89	0	
	…	…	



MPLS Path (LSP) Setup

Step 2A: Assignment of Local Labels

- Each MPLS node assigns a local label to each route in local routing table
  – In label

Forwarding Table

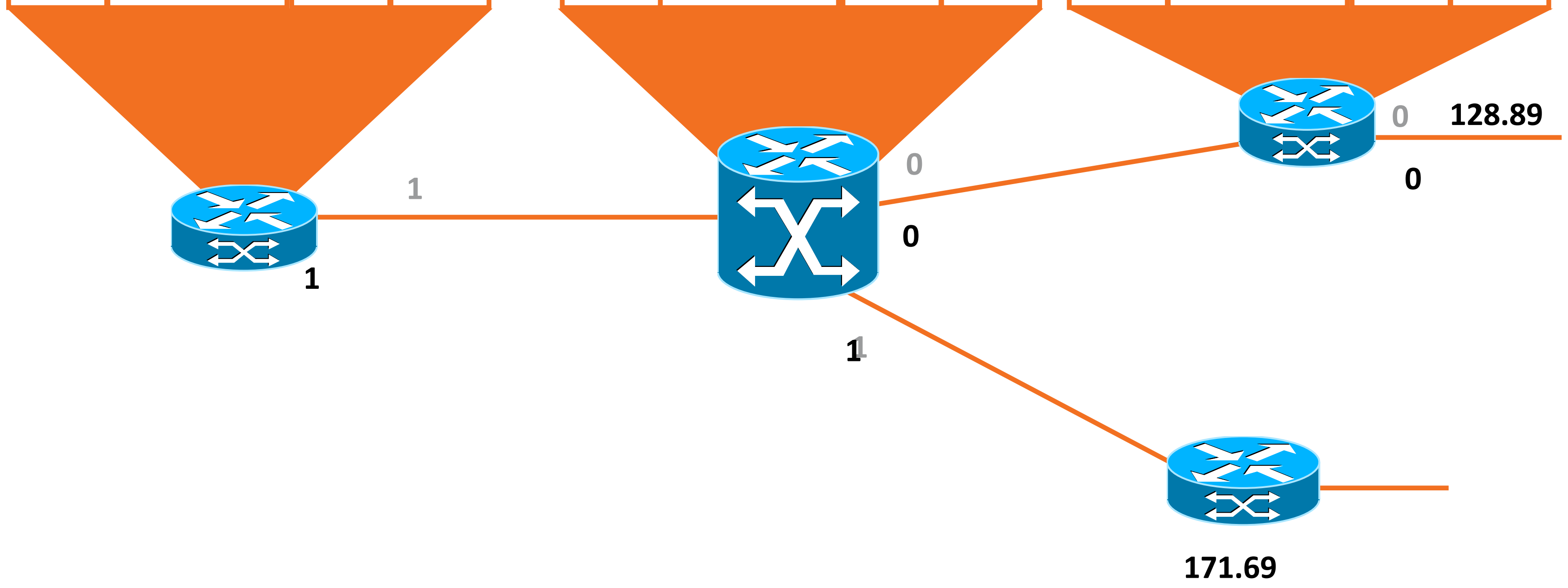
In Label	Address Prefix	Out I'face	Out Label
-	128.89	1	
-	171.69	1	
...	...	...	...

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
20	128.89	0	
21	171.69	1	
...	...	...	...

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
30	128.89	0	-
...	...	...	...



MPLS Path (LSP) Setup

Step 2B: Assignment of Remote Labels

- Local label mapping are sent to connected nodes
- Receiving nodes update forwarding table
  - Out label

Forwarding Table

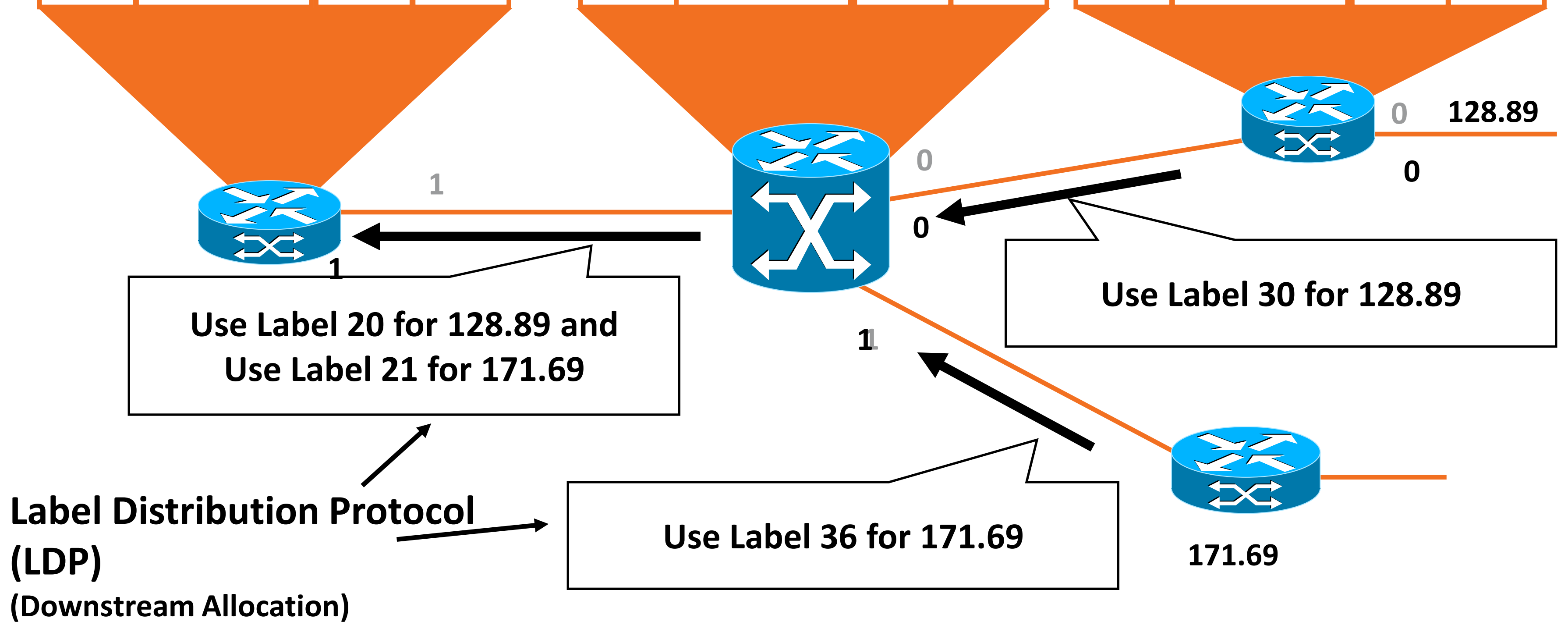
In Label	Address Prefix	Out I'face	Out Label
-	128.89	1	20
-	171.69	1	21
…	…	…	…

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
20	128.89	0	30
21	171.69	1	36
…	…	…	…

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
30	128.89	0	-
…	…	…	…



MPLS Traffic Forwarding

Hop-by-hop Traffic Forwarding Using Labels

- Ingress PE node adds label to packet (push)
  - Via forwarding table
- Downstream node use label for forwarding decision (swap)
  - Outgoing interface
  - Out label
- Egress PE removes label and forwards original packet (pop)

Forwarding Table

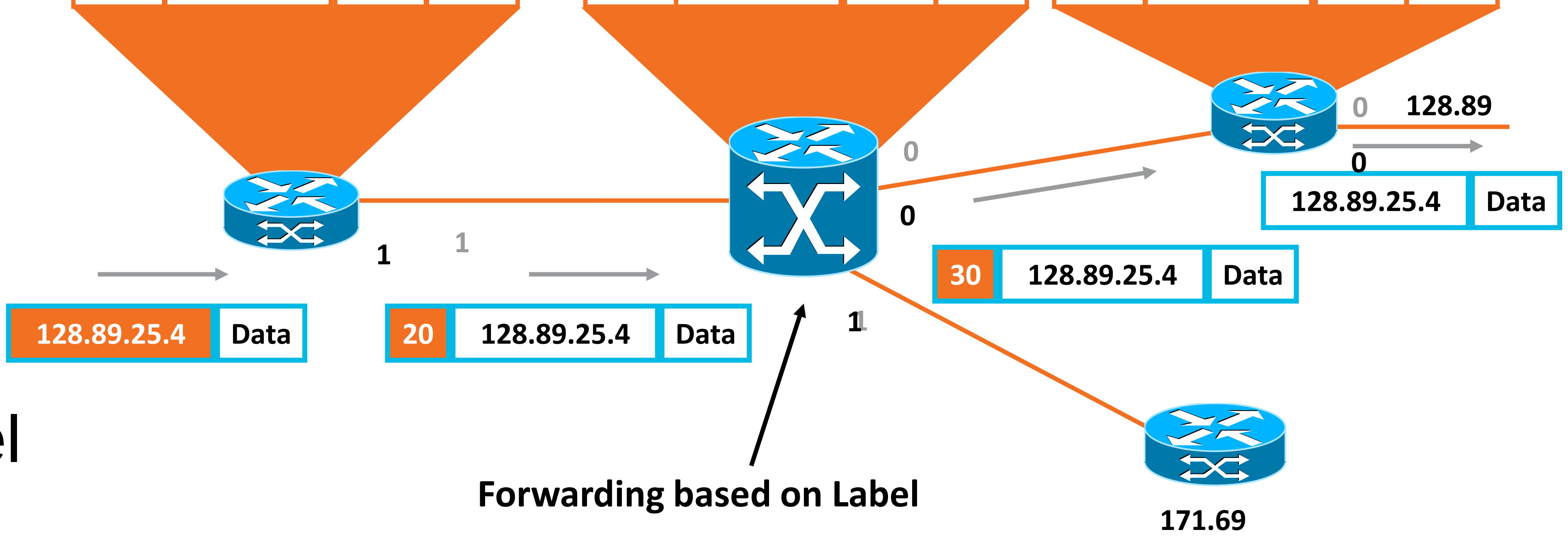
In Label	Address Prefix	Out I'face	Out Label
-	128.89	1	20
-	171.69	1	21
…	…	…	…

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
20	128.89	0	30
21	171.69	1	36
…	…	…	…

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
30	128.89	0	-
…	…	…	…



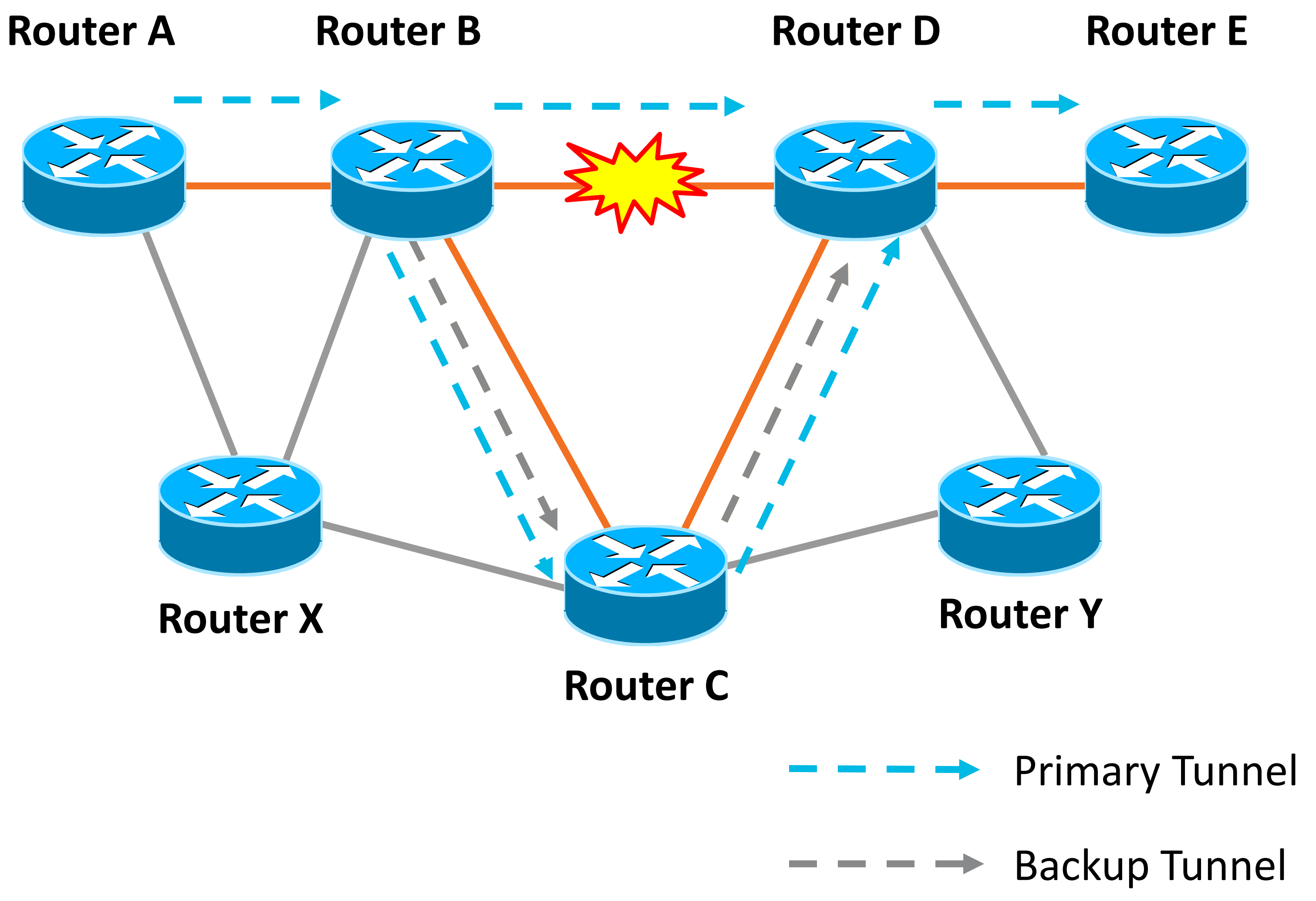
MPLS TE Fast ReRoute (FRR)

Implementing Network Failure Protection Using MPLS RSVP/TE

- Steady state
  - Primary tunnel:

    A → B → D → E
  - Backup tunnel:

    B → C → D (pre-provisioned)
- Failure of link between router B and D
- Traffic rerouted over backup tunnel
- Recovery time* ~ 50 ms



*Actual Time Varies—Well Below 50 ms in Lab Tests, Can Also Be Higher

MPLS SNMP MIBs

SNMP Management Access to MPLS Resources

- MPLS-LSR-STD-MIB
  - Provides LSP end-point and LSP cross-connect information
  - Frequently used: none ☹
- MPLS-LDP-STD-MIB
  - Provides LDP session configuration and status information
  - Frequently used: LDP session status Trap notifications
- MPLS-L3VPN-STD-MIB
  - Provides VRF configuration and status information and associated interface mappings
  - Frequently used: VRF max-route Trap notifications
- MPLS-TE-STD-MIB
  - Provides TE tunnel configuration and status information
  - Frequently used: TE Tunnel status Trap notifications

MPLS OAM

Tools for Reactive and Proactive Trouble Shooting of MPLS Connectivity

- MPLS LSP Ping
  – Used for testing end-to-end MPLS connectivity similar to IP ping
  – Can we used to validate reach ability of LDP-signaled LSPs, TE tunnels, and PWs
- MPLS LSP Trace
  – Used for testing hop-by-hop tracing of MPLS path similar to traceroute
  – Can we used for path tracing LDP-signaled LSPs and TE tunnels
- MPLS LSP Multipath (ECMP) Tree Trace
  – Used to discover of all available equal cost LSP paths between PEs
  – Unique capability for MPLS OAM; no IP equivalent!
- Auto IP SLA
  – Automated discovery of all available equal cost LSP paths between PEs
  – LSP pings are being sent over each discovered LSP path

Summary

Key Takeaways

- MPLS networks consist of PE routers at in/egress and P routers in core
- Traffic is encapsulated with label(s) at ingress (PE router)
- Labels are removed at egress (PE router)
- MPLS forwarding operations include label imposition (PUSH), swapping, and disposition (POP)
- LDP and RSVP can be used for signalling label mapping information to set up an end-to-end Label Switched Path (LSP)
- RSVP label signalling enables setup of TE tunnels, supporting enhanced traffic engineering capabilities; traffic protection and path management
- MPLS OAM and MIBs can be used for MPLS connectivity validation and troubleshooting

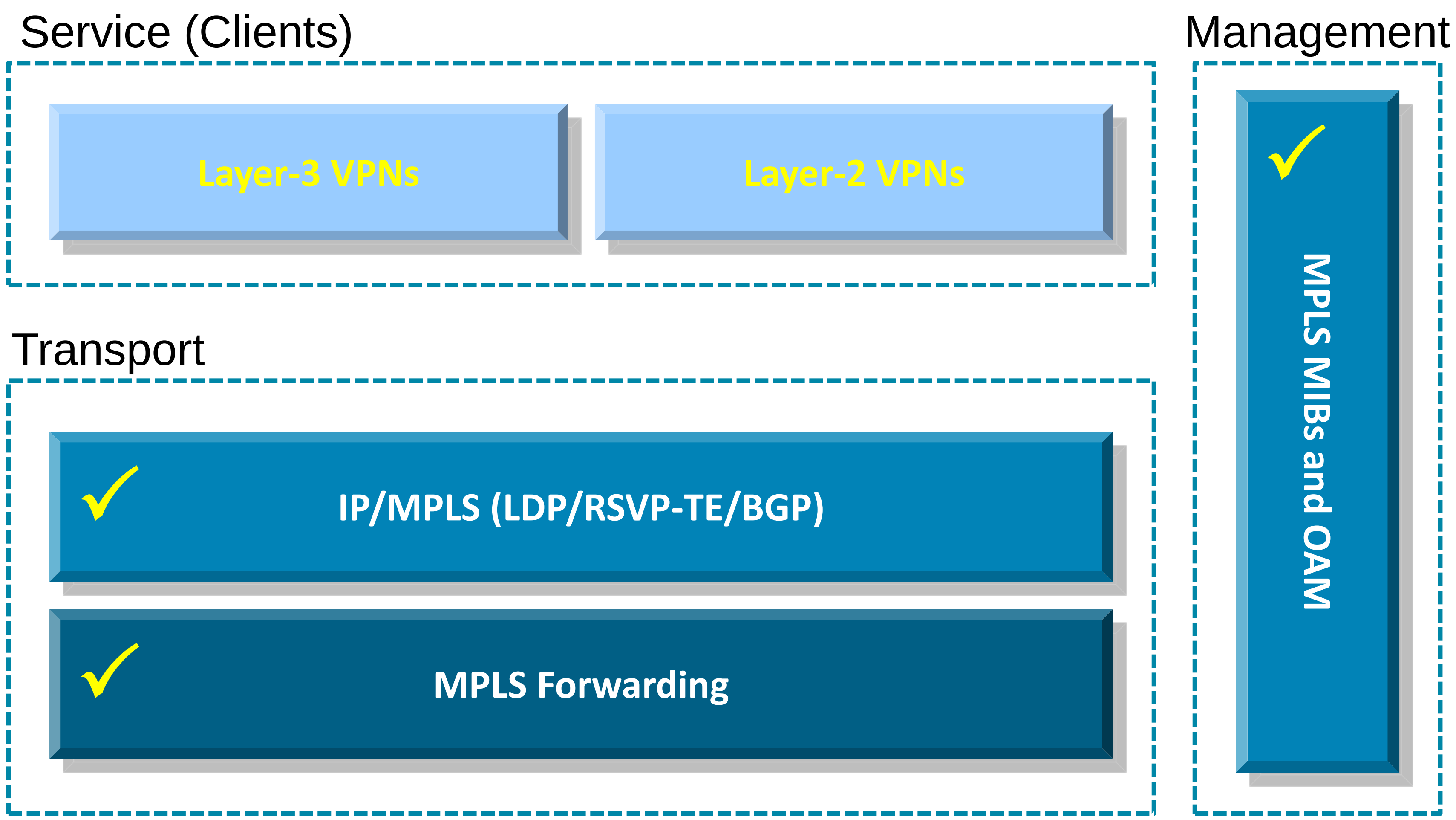
MPLS Virtual Private Networks

Technology Overview

MPLS Virtual Private Networks

Topics

- Definition of MPLS VPN service
- Basic MPLS VPN deployment scenario
- Technology options



What is a Virtual Private Network?

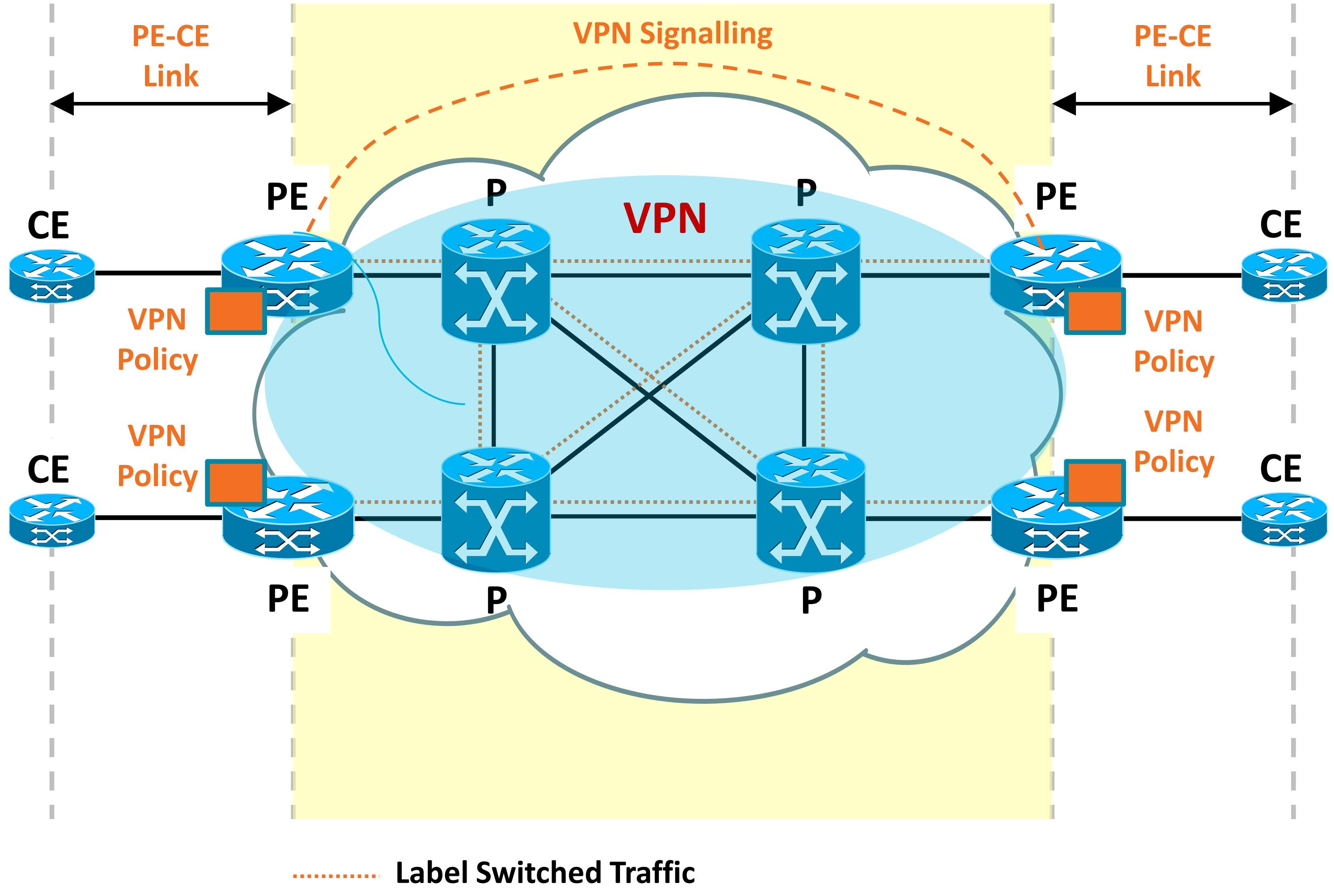
Definition

- Set of sites which communicate with each other in a secure way
  - – Typically over a shared public or private network infrastructure
- Defined by a set of administrative policies
  - – Policies established by VPN customers themselves (DIY)
  - – Policies implemented by VPN service provider (managed/unmanaged)
- Different inter-site connectivity schemes possible
  - – Full mesh, partial mesh, hub-and-spoke, etc.
- VPN sites may be either within the same or in different organisations
  - – VPN can be either intranet (same org) or extranet (multiple orgs)
- VPNs may overlap; site may be in more than one VPN

MPLS VPN Example

Basic Building Blocks

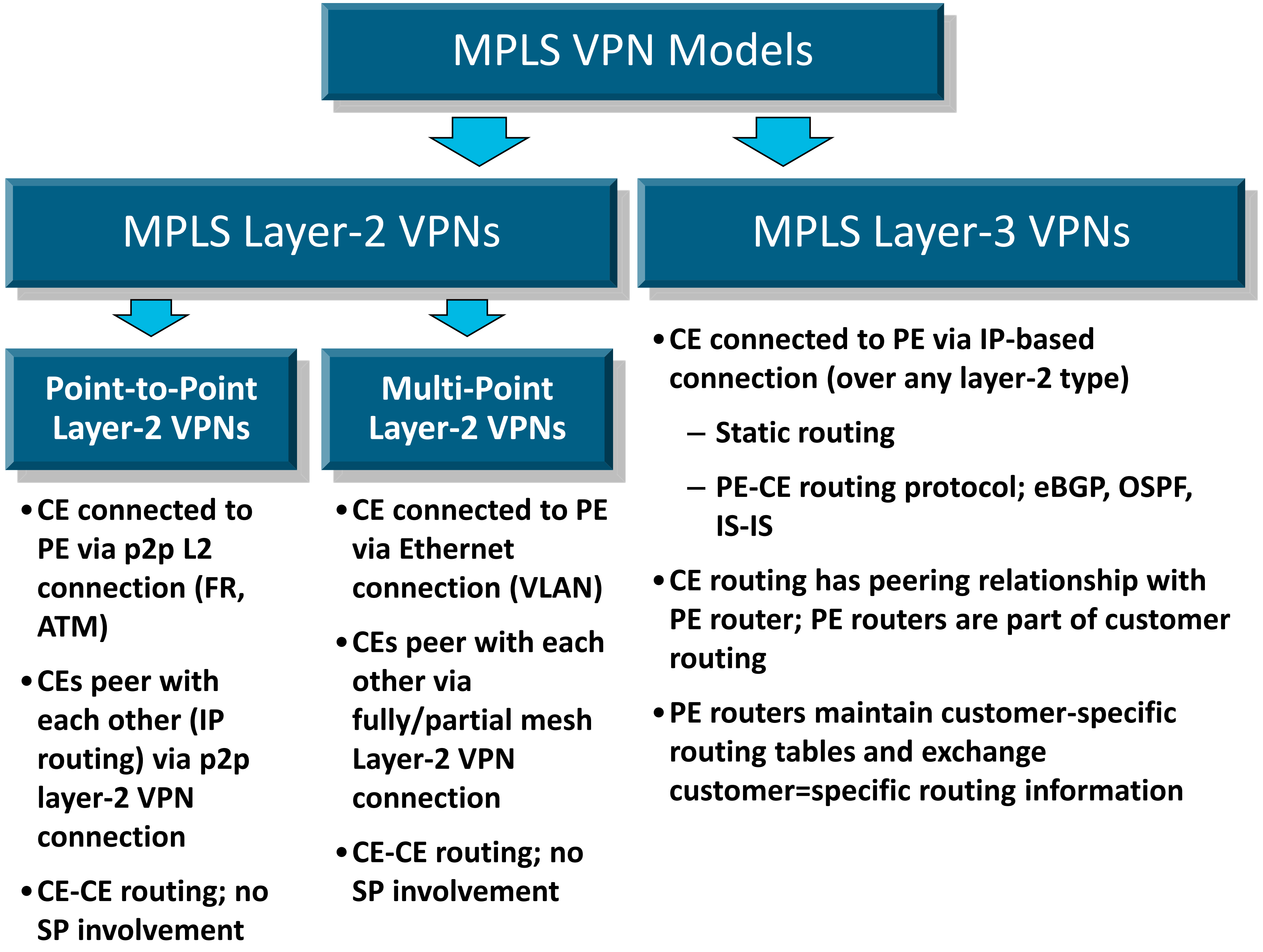
- VPN policies
  - – Configured on PE routers (manual operation)
- VPN signalling
  - – Between PEs
  - – Exchange of VPN policies
- VPN traffic forwarding
  - – Additional VPN-related MPLS label encapsulation
- PE-CE link
  - – Connects customer network to MPLS network; either layer-2 or layer-3



MPLS VPN Models

Technology Options

- MPLS Layer-3 VPNs
  - Peering relationship between CE and PE
- MPLS Layer-2 VPNs
  - Interconnect of layer-2 Attachment Circuits (ACs)



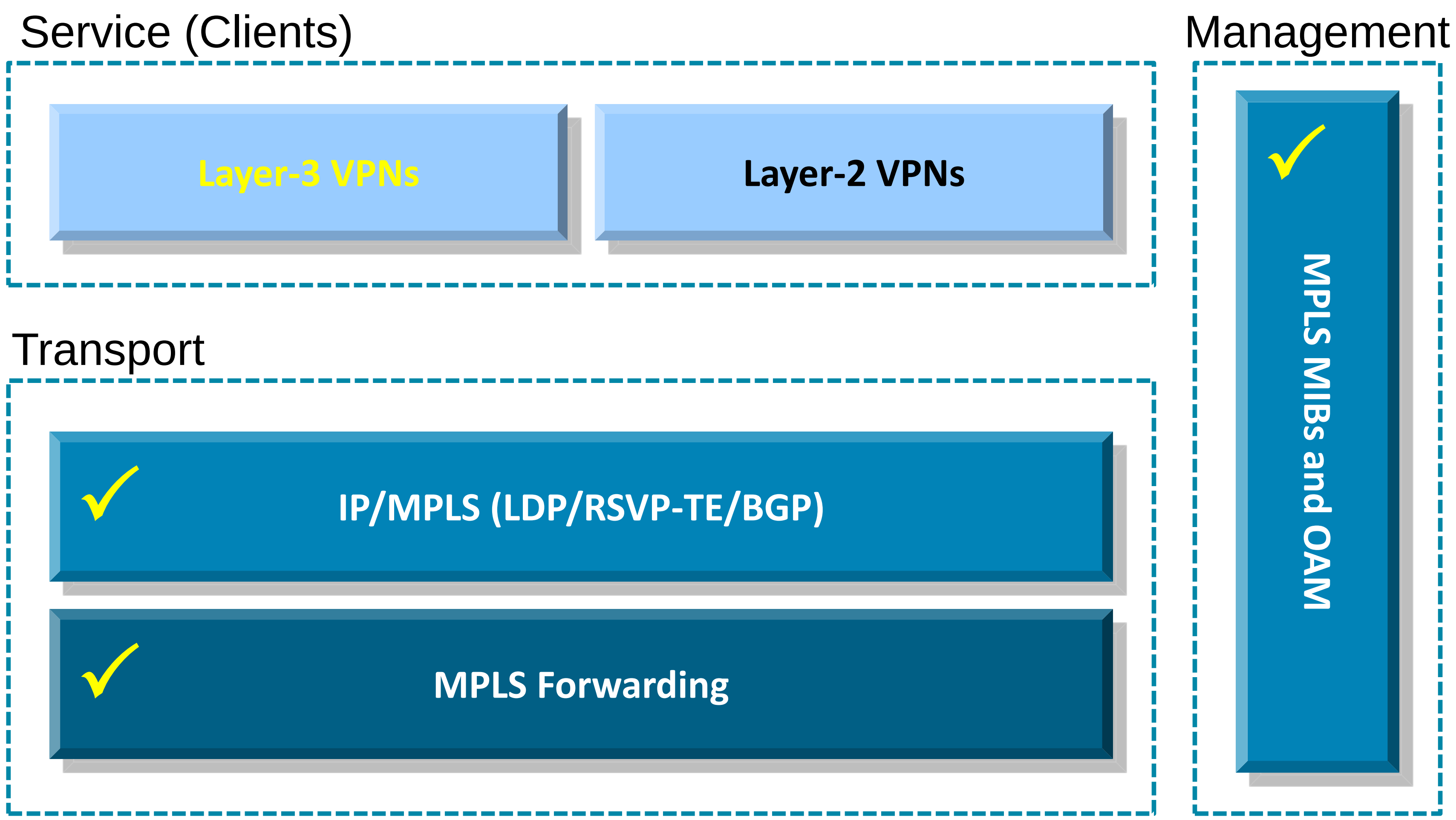
MPLS Layer-3 Virtual Private Networks

End-to-end Layer-3 Services Over MPLS Networks

MPLS Layer-3 Virtual Private Networks

Topics

- Technology components
- VPN control plane mechanisms
- VPN forwarding plane
- Deployment use cases
  - – Business VPN services
  - – Network segmentation
  - – Data Centre access



MPLS Layer-3 VPN Overview

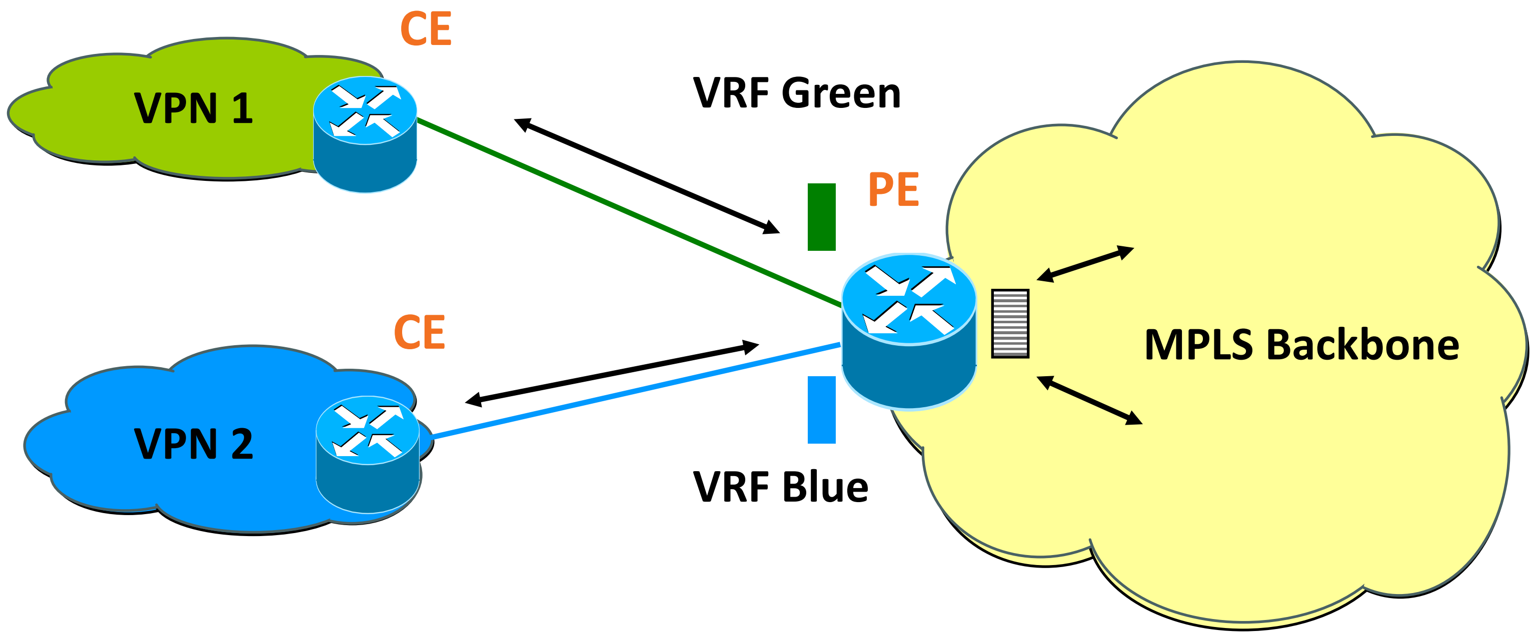
Technology Components

- VPN policies
  - – Separation of customer routing via virtual VPN routing table (VRF)
  - – In PE router, customer interfaces are connected to VRFs
- VPN signalling
  - – Between PE routers: customer routes exchanged via BGP (MP-iBGP)
- VPN traffic forwarding
  - – Separation of customer VPN traffic via additional VPN label
  - – VPN label used by receiving PE to identify VPN routing table
- PE-CE link
  - – Can be any type of layer-2 connection (e.g., FR, Ethernet)
  - – CE configured to route IP traffic to/from adjacent PE router
  - – Variety of routing options; static routes, eBGP, OSPF, IS-IS

Virtual Routing and Forwarding Instance

Virtual Routing Table and Forwarding to Separate Customer Traffic

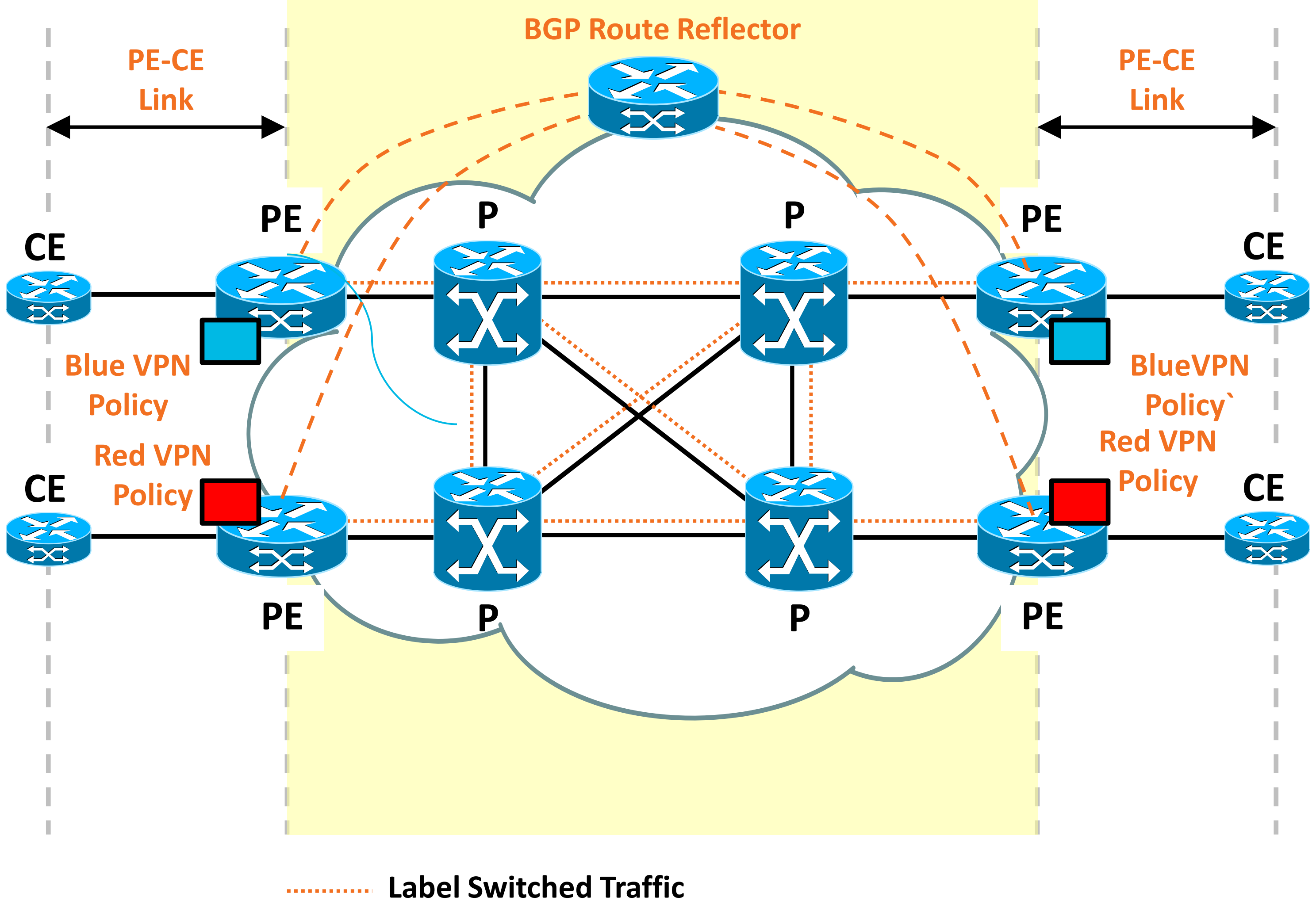
- Virtual routing and forwarding table
  - On PE router
  - Separate instance of routing (RIB) and forwarding table
- Typically, VRF created for each customer VPN
  - Separates customer traffic
- VRF associated with one or more customer interfaces
- VRF has its own routing instance for PE-CE configured routing protocols
  - E.g., eBGP



VPN Route Distribution

Exchange of VPN Policies Among PE Routers

- Full mesh of BGP sessions among all PE routers
  - BGP Route Reflector
- Multi-Protocol BGP extensions (MP-iBGP) to carry VPN policies
- PE-CE routing options
  - Static routes
  - eBGP
  - OSPF
  - IS-IS



VPN Control Plane Processing

VRF Parameters

Make customer routes unique:

- **Route Distinguisher (RD):** 8-byte field, VRF parameters; unique value to make VPN IP routes unique
- **VPNv4 address**: RD + VPN IP prefix

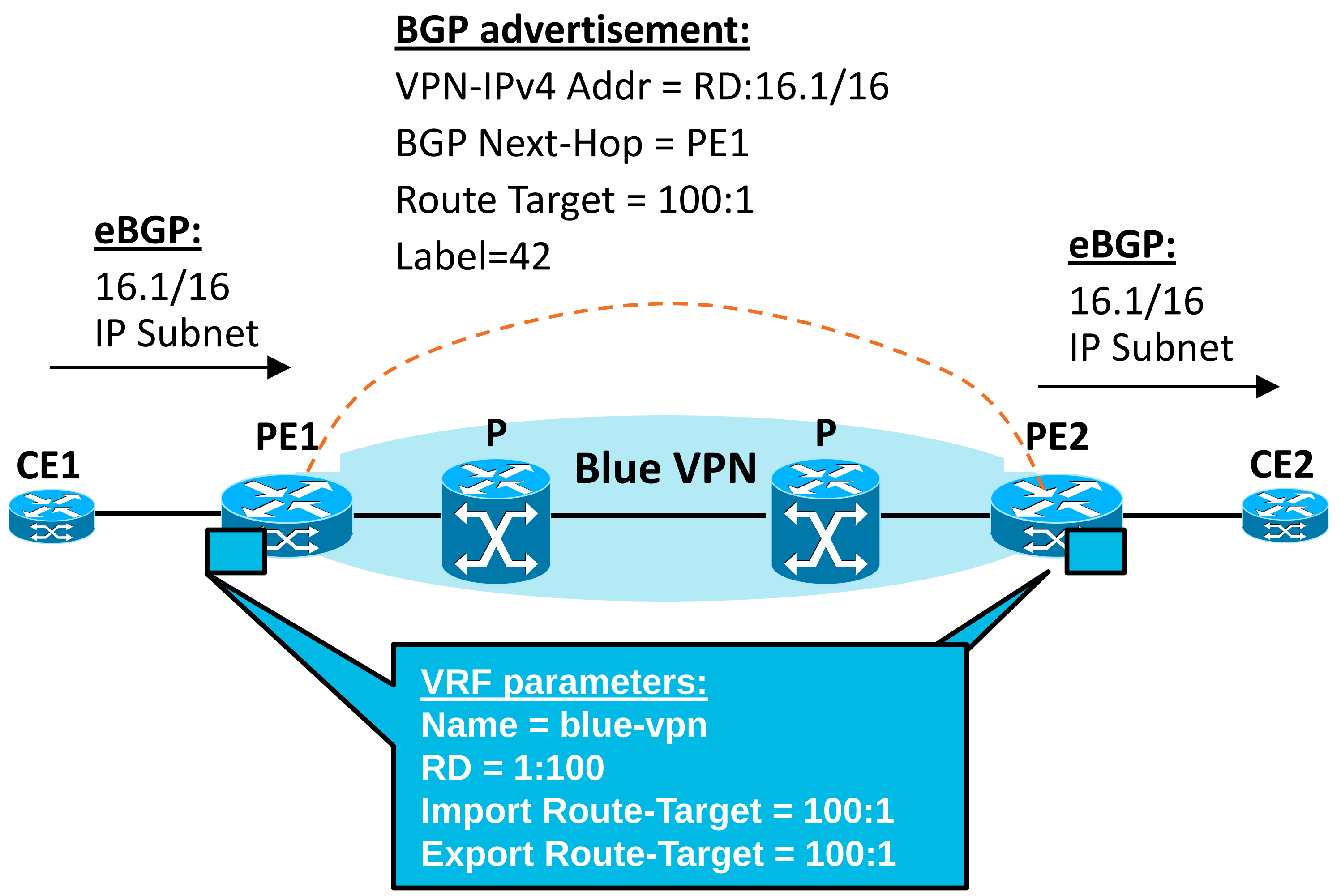
Selective distribute VPN routes:

- **Route Target (RT):** 8-byte field, VRF parameter, unique value to define the import/export rules for VPNv4 routes
- MP-iBGP: advertises VPNv4 prefixes + labels

VPN Control Plane Processing

Interactions Between VRF and BGP VPN Signalling

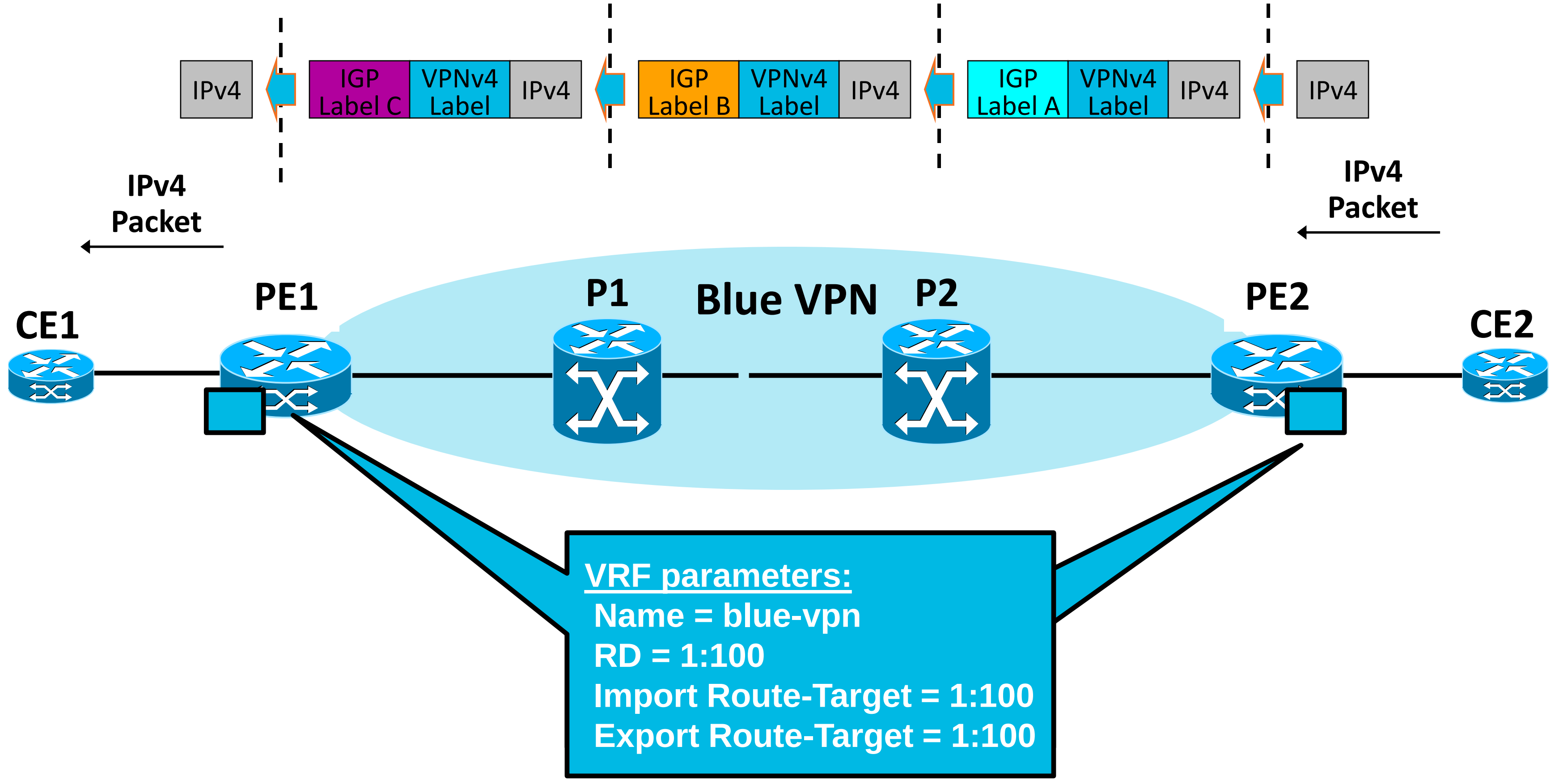
1. CE1 redistribute IPv4 route to PE1 via eBGP
2. PE1 allocates VPN label for prefix learnt from CE1 to create unique VPNv4 route
3. PE1 redistributes VPNv4 route into MP-iBGP, it sets itself as a next hop and relays VPN site routes to PE2
4. PE2 receives VPNv4 route and, via processing in local VRF (green), it redistributes original IPv4 route to CE2



VPN Forwarding Plane Processing

Forwarding of Layer-3 MPLS VPN Packets

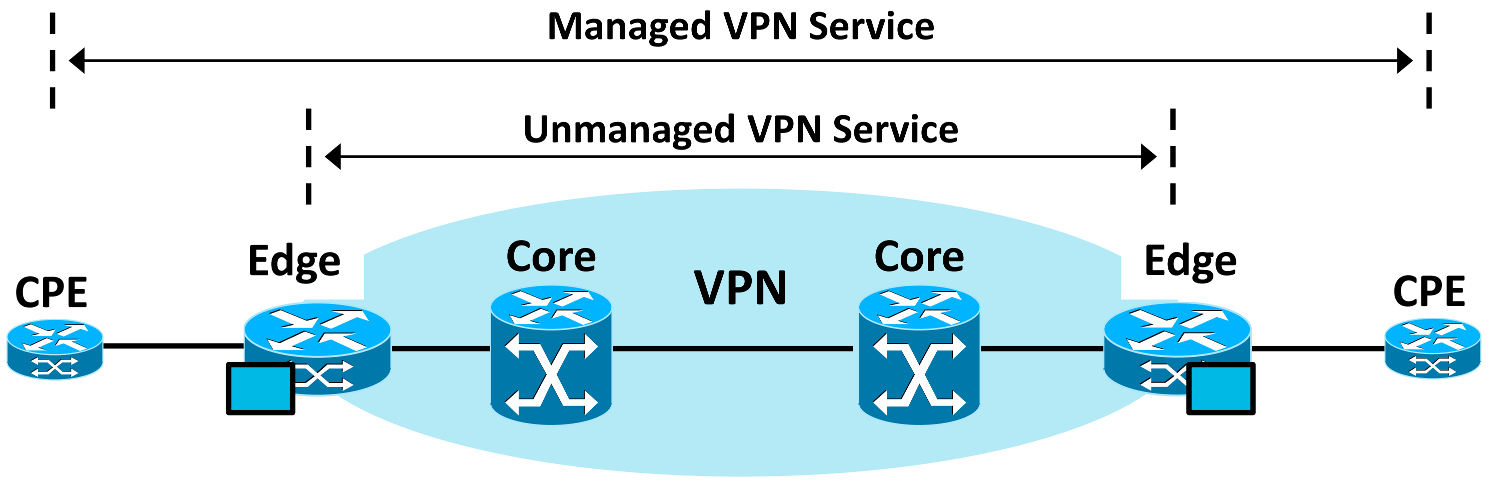
1. CE2 forwards IPv4 packet to PE2
2. PE2 imposes pre-allocated VPN label to IPv4 packet received from CE2
   - Learned via MP-IBGP
3. PE2 imposes outer IGP label A (learned via LDP) and forwards labeled packet to next-hop P-router P2
4. P-routers P1 and P2 swap outer IGP label and forward label packet to PE1
   - A->B (P2) and B->C (P1)
5. Router PE1 strips VPN label and IGP labels and forwards IPv4 packet to CE1



Service Provider Deployment Scenario

MPLS Layer-3 VPNs for Offering Layer-3 Business VPN Services

- Deployment Use Case
  - Delivery of IP VPN services to business customers
- Benefits
  - Leverage same network for multiple services and customers (CAPEX)
    Highly scalable
  - Service enablement only requires edge node configuration (OPEX)
  - Different IP connectivity can be easily configured; e.g., full/partial mesh

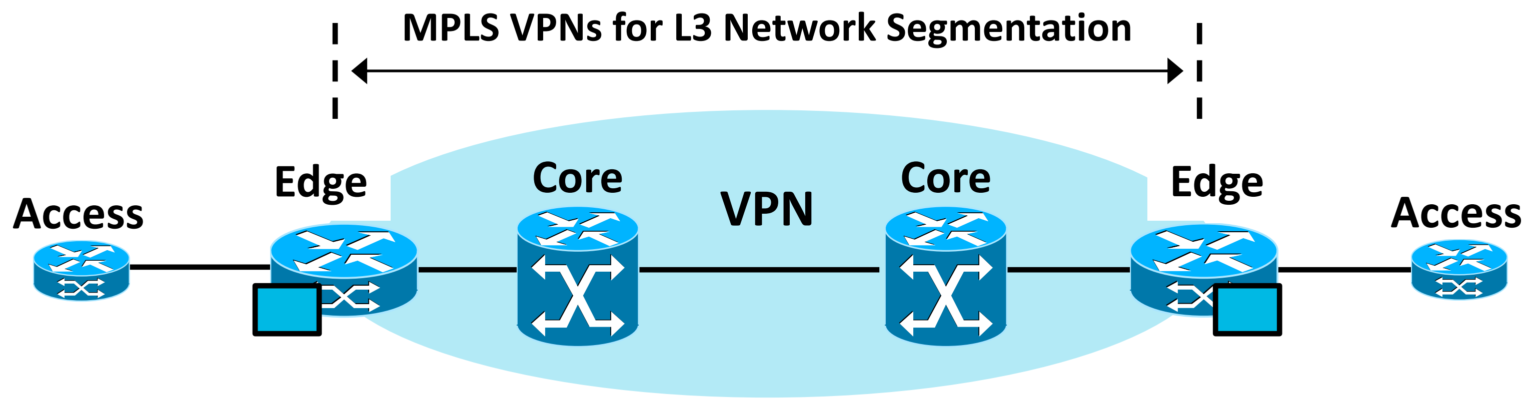


Network Segment	CPE	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	ASR1K ISR/G2 ASR901	ASR9K 7600 ASR1K ASR903 ME3800X	CRS-3 GSR ASR9K

Enterprise Deployment Scenario

MPLS Layer-3 VPNs for Implementing Network Segmentation

- Deployment Use Case
  - Segmentation of enterprise network to provide selective connectivity for specific user groups and organisations
- Benefits
  - Network segmentation only requires edge node configuration
  - Flexible routing; different IP connectivity can be easily configured; e.g., full/partial mesh

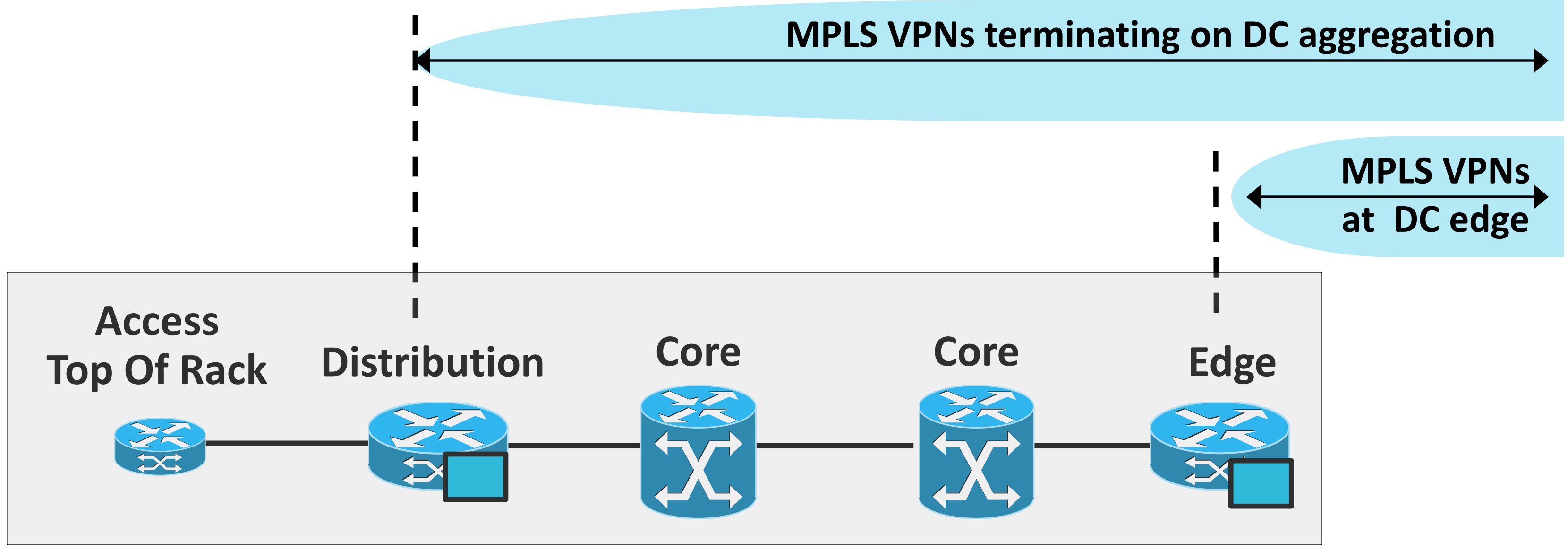


Network Segment	Access	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	ASR1K ISR/G2	7600 ASR1K	CRS-1 GSR ASR9K 7600 6500

Data Centre Deployment Scenario

MPLS Layer-3 VPNs for Segmented L3 Data Centre Access and Interconnect

- Deployment Use Case
  - Segmented WAN Layer-3 at Data Centre edge
  - Layer-3 segmentation in Data Centre
- Benefits
  - Only single Data Centre edge node needed for segmented layer-3 access
  - Enables VLAN/Layer-2 scale (> 4K)



Data Centre

Network Segment	Distribution	Core	Edge
MPLS Node	CE or PE	P or CE	PE
Typical Platforms	N7K 6500	N7K 6500	ASR9K 7600

Summary

Key Takeaways

- MPLS Layer-3 VPNs provide IP connectivity among CE sites
  - MPLS VPNs enable full-mesh, hub-and-spoke, and hybrid IP connectivity
- CE sites connect to the MPLS network via IP peering across PE-CE links
- MPLS Layer-3 VPNs are implemented via VRFs on PE edge nodes
  - VRFs providing customer routing and forwarding segmentation
- BGP used for signalling customer VPN (VPNv4) routes between PE nodes
- To ensure traffic separation, customer traffic is encapsulated in an additional VPN label when forwarded in MPLS network
- Key applications are layer-3 business VPN services, enterprise network segmentation, and segmented layer-3 Data Centre access

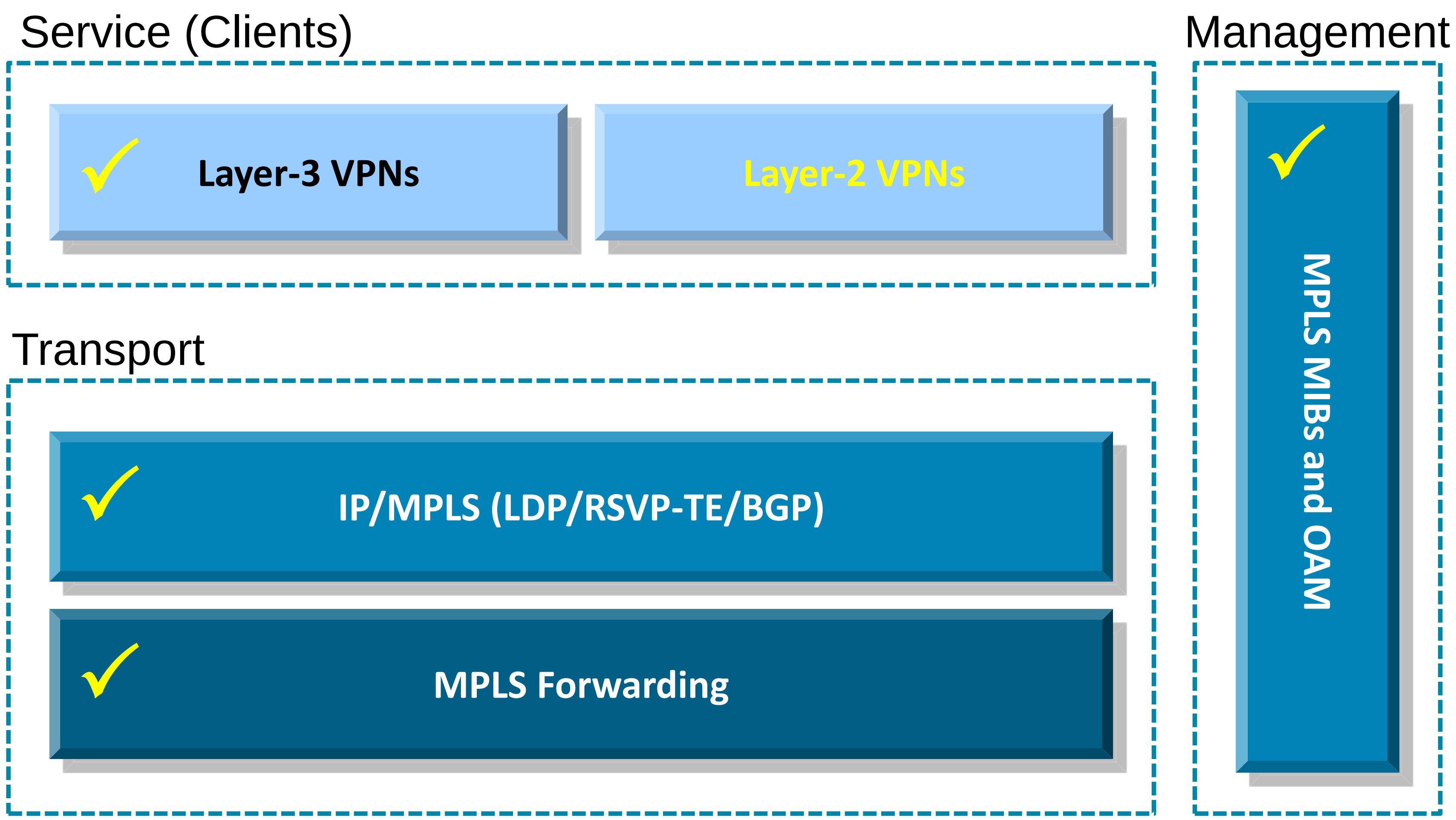
MPLS Layer-2 Virtual Private Networks

End-to-end Layer-2 Services Over MPLS Networks

MPLS Layer-2 Virtual Private Networks

Topics

- L2VPN technology options
- P2P VPWS services (PWs)
  - Overview & Technology Basics
  - VPN control plane
  - VPN forwarding plane
- MP2MP VPLS services
  - Overview & Technology Basics
  - VPN control plane
  - VPN forwarding plane
- Deployment use cases
  - L2 Business VPN services
  - Data Centre Interconnect



MPLS Layer-2 Virtual Private Networks

Technology Options

- VPWS services
  - Point-to-point
  - Referred to as Pseudowires (PWs)*
- VPLS services
  - Multipoint-to-Multipoint

MPLS Layer-2 VPNs

Point-to-Point Layer-2 VPNs (PWs)

- **CE connected to PE via p2p L2 connection (e.g., FR, ATM)**
- **CEs peer with each other (IP routing) via p2p layer-2 VPN connection**
- **CE-CE routing; no MPLS network involvement**

Multipoint-to-Multipoint Layer-2 VPNs (VPLS)

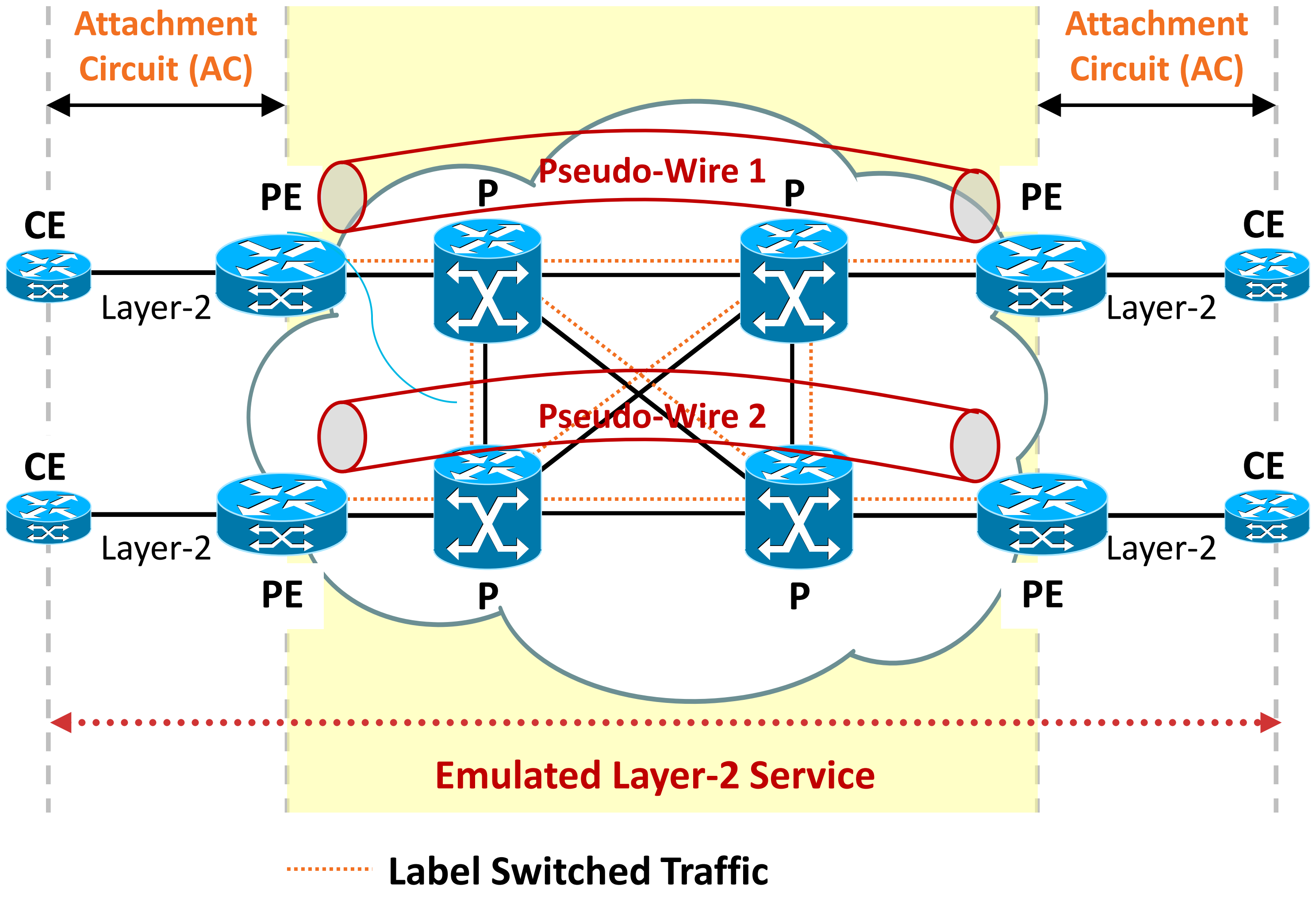
- **CE connected to PE via Ethernet connection (VLAN)**
- **CEs peer with each other via fully/partial mesh Layer-2 VPN connection**
- **CE-CE routing; no MPLS network involvement**

* Used to be referred to as Any Transport over MPLS or AToM as well.

Virtual Private Wire Services (VPWS)

Overview of Pseudowire (PW) Architecture

- Based on IETF's Pseudo-Wire (PW) Reference Model
- Enables transport of any Layer-2 traffic over MPLS
- Includes additional VC label encapsulation and translation of L2 packets
  – ATM, ATM, FR, or PPP
- PE-CE link is referred to as Attachment Circuit (AC)
- Support for L2 interworking
- PWs are bi-directional



Virtual Private Wire Services (VPWS)

Technology Components

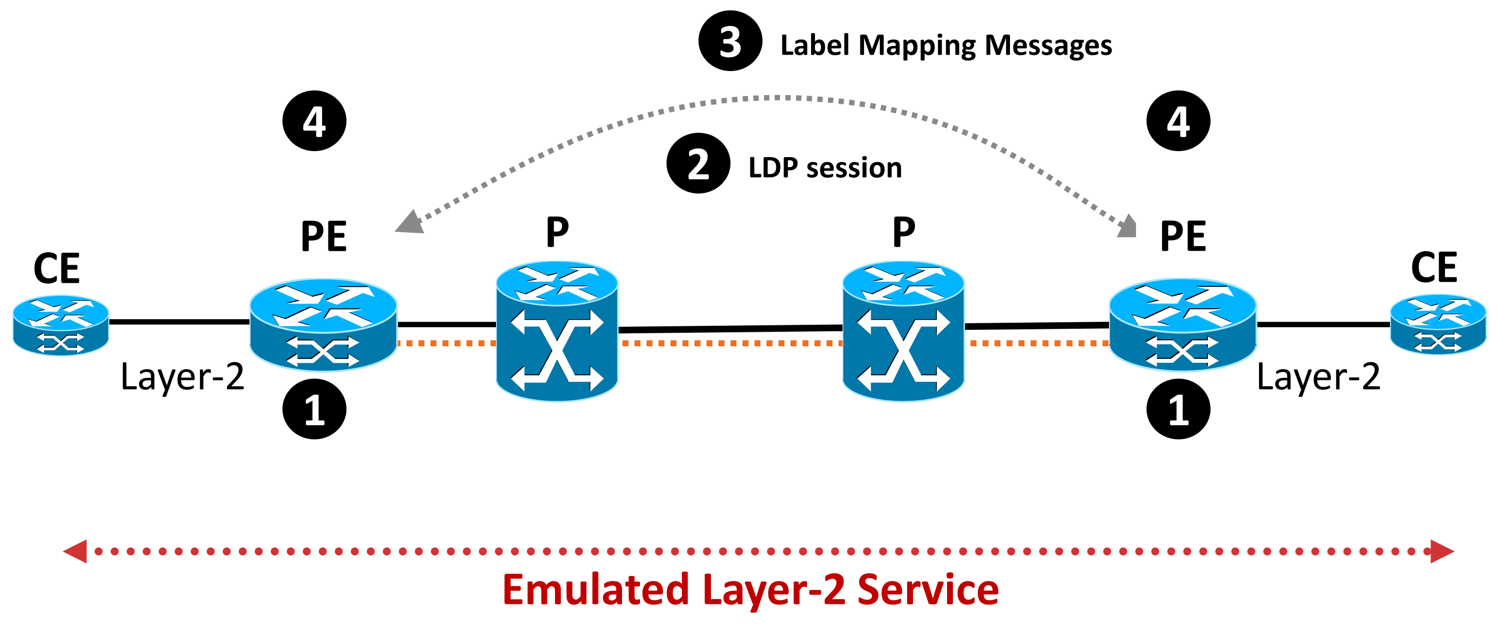
- VPN policies
  - Virtual cross-connect (Xconnect)
  - Maps customer interface (AC) to PW (1:1 mapping)
- VPN signalling
  - Targeted LDP* or BGP session between ingress and egress PE router
  - Virtual Connection (VC)-label negotiation, withdrawal, error notification
- VPN traffic forwarding
  - 1 or 2 labels used for encapsulation + 1 (IGP) label for forwarding: VC label + optional control word
  - Inner de-multiplexer (VC) label: identifies L2 circuit (packet)
  - Control word: replaces layer-2 header at ingress; used to rebuild layer-2 header at egress
  - Outer tunnel (IGP) label: to get from ingress to egress PE using MPLS LSP
- PE-CE link
  - Referred to as Attachment Circuit (AC)
  - Can be any type of layer-2 connection (e.g., FR, ATM)

* LDP is assumed as signalling protocol for next examples

VPWS Control Plane Processing

Signalling of a New Pseudo-Wire

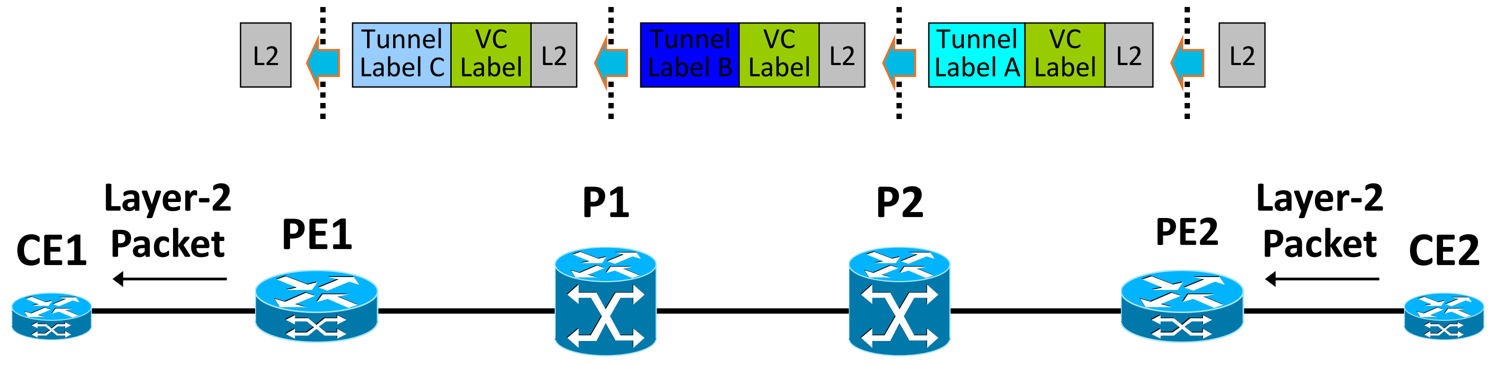
1. New Virtual Circuit (VC) cross-connect connects customer L2 interface (AC) to new PW via VC ID and remote PE ID
2. New targeted LDP session between PE1 and PE2 is established, in case one does not already exist
3. PE binds VC label with customer layer-2 interface and sends label-mapping to remote PE
4. Remote PE receives LDP label binding message and matches VC ID with local configured VC cross-connect



VPWS Forwarding Plane Processing

Forwarding of Layer-2 Traffic Over PWs

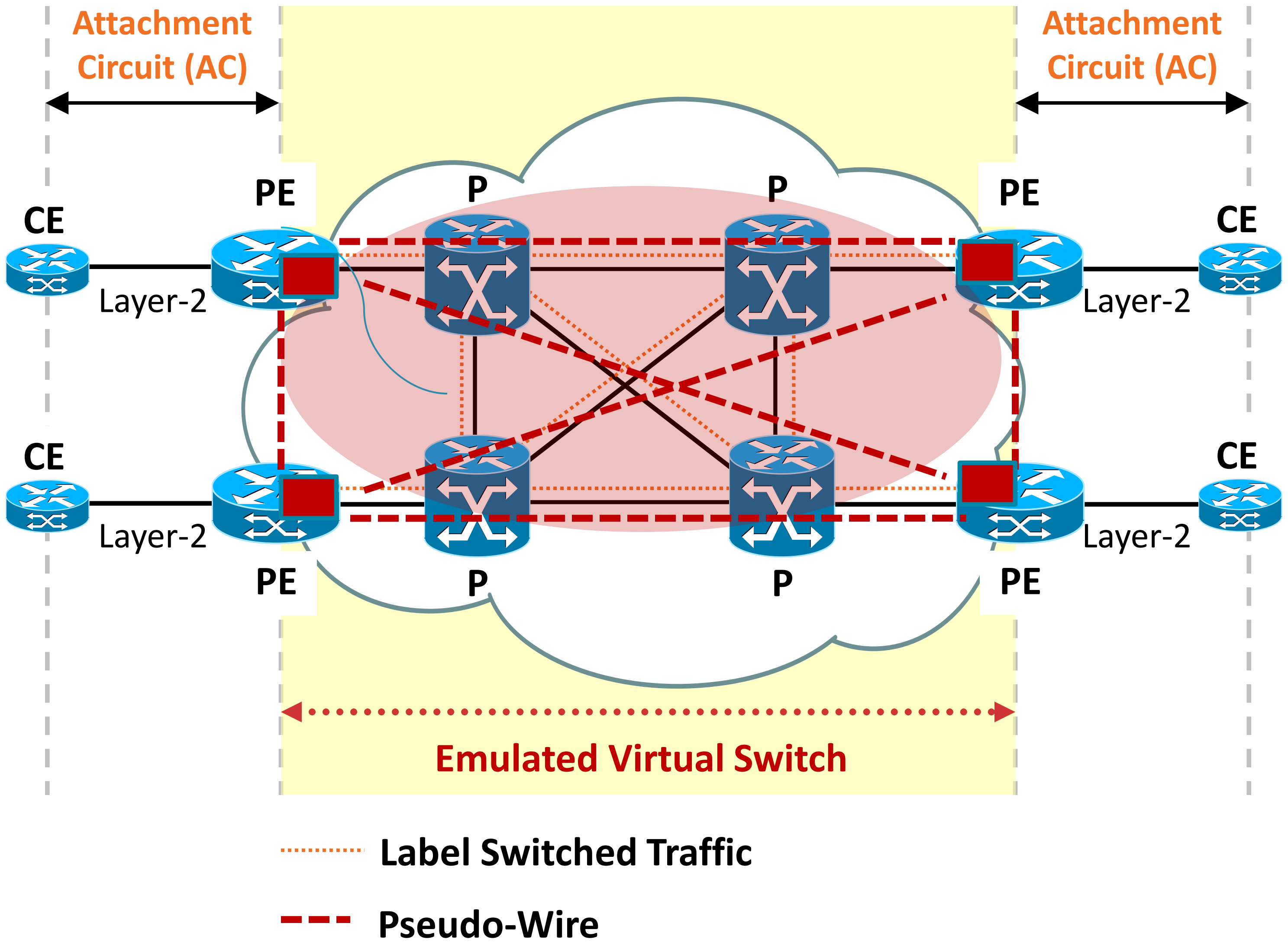
1. CE2 forwards L2 packet to PE2.
2. PE2 pushes VC (inner) label to L2 packet received from CE2
   - Optionally, a control word is added as well (not shown)
3. PE2 pushed outer (Tunnel) label and forwards packet to P2
4. P2 and P1 forward packet using outer (tunnel) label (swap)
5. Router PE2 pops Tunnel label and, based on VC label, L2 packet is forwarded to customer interface to CE1, after VC label is removed
   - In case control word is used, new layer-2 header is generated first



Virtual Private LAN Services

Overview of VPLS Architecture

- Architecture for Ethernet Multipoint Services over MPLS
- VPLS network acts like a virtual switch that emulates conventional L2 bridge
- Fully meshed or Hub-Spoke topologies supported
- PE-CE link is referred to as Attachment Circuit (AC)
  - Always Ethernet



Virtual Private LAN Services (VPLS)

Technology Components

- VPN policies
  - Virtual Switching Instance or VSI
  - One or more customer interfaces are connected to VSI
  - One or more PWs for interconnection with related VSI instances on remote PE
- VPN signalling
  - Full mesh of targeted LDP* (VC exchange) and/or BGP sessions (discovery and VC exchange)
  - Virtual Connection (VC)-label negotiation, withdrawal, error notification
- VPN traffic forwarding
  - 1 VC label used for encapsulation + 1 (IGP) label for forwarding
  - Inner de-multiplexer (VC) label: identifies VSI
  - Outer tunnel (IGP) label: to get from ingress to egress PE using MPLS LSP
- PE-CE link
  - Referred to as Attachment Circuit (AC)
  - Ethernet VCs are either port mode or VLAN ID

* LDP is assumed as signalling protocol for next examples

VPLS Forwarding Plane Processing

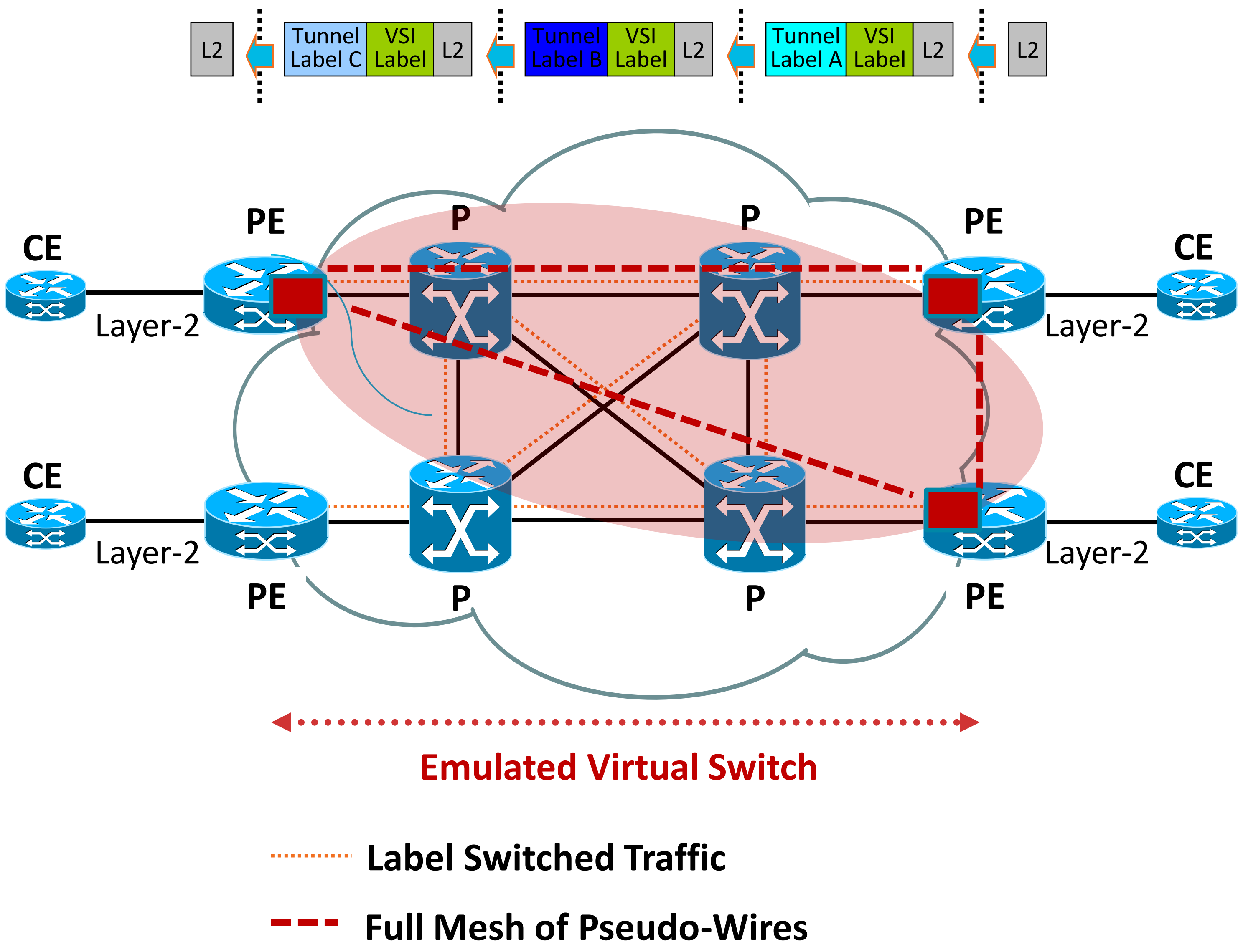
Forwarding of Layer-2 Traffic Over VPLS Network

MAC learning:

- For new L2 packets
- VSI forwarding table updated
- Packets flooded to all PEs over PWs

Layer-2 Packet Forwarding:

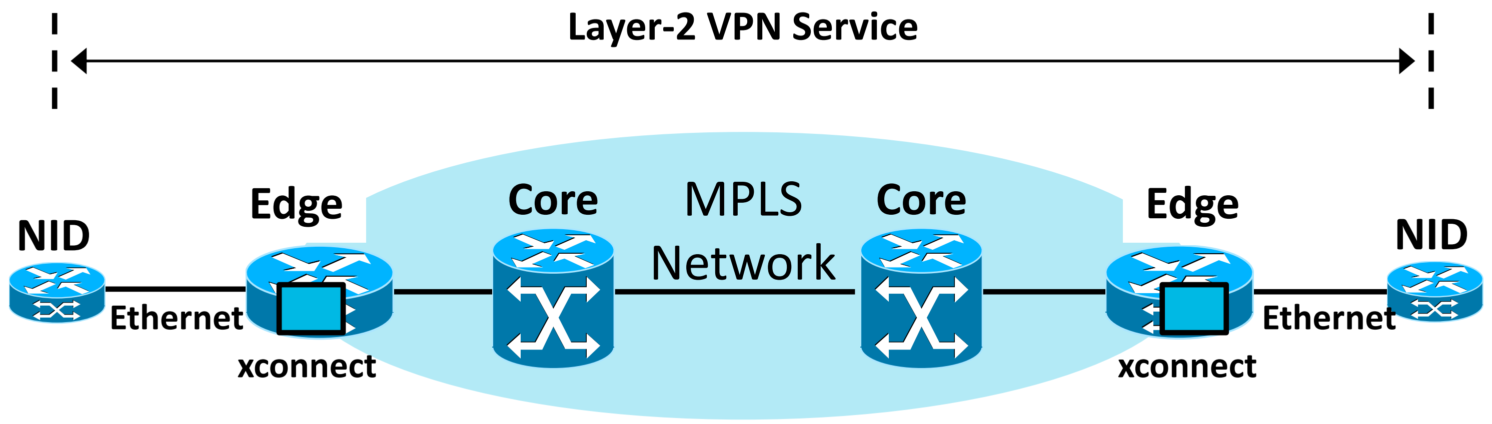
- For L2 packets with known destination MAC addresses
- Lookup in VSI forwarding table
- L2 packet forwarded onto PWs to remote PE/VSI



Service Provider Deployment Scenario

PWs for Offering Layer-2 Business VPN Services

- Deployment Use Case
  – Delivery of E-LINE services to business customers
- Benefits
  – Leverage same network for multiple services and customers (CAPEX)
  Highly scalable
  – Service enablement only requires edge node configuration (OPEX)



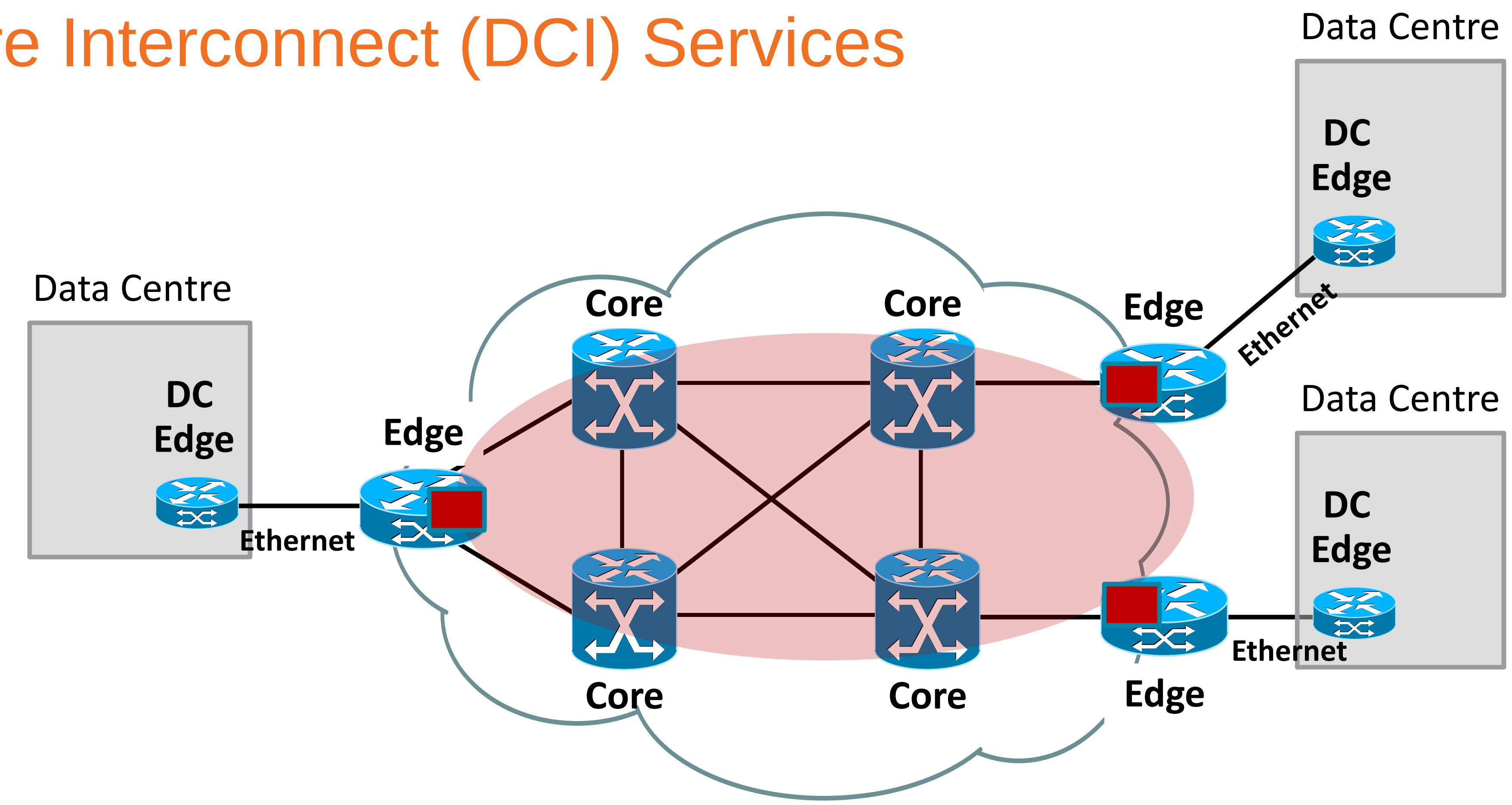
Network Segment	NID *	Edge	Core
MPLS Node	CE	U-PE	P
Typical Platforms	M3400 ASR901	ME3800X ASR903 ASR9K	CRS-1 GSR ASR9K

* NID : Network Interface Device

Data Centre Deployment Scenario

VPLS for Layer-2 Data Centre Interconnect (DCI) Services

- Deployment Use Case
  - E-LAN services for Data Centre interconnect
- Benefits
  - Single WAN uplink to connect to multiple Data Centres
  - Easy implementation of segmented layer-2 traffic between Data Centres



Network Segment	DC Edge	Core	Edge
MPLS Node	CE	P	PE
Typical Platforms	ASR9K 7600 6500	CRS-1 GSR ASR9K	ASR9K 7600

Summary

Key Takeaways

- L2VPNs enable transport of any Layer-2 traffic over MPLS network
- L2 packets encapsulated into additional VC label
- Both LDP and BGP can be used L2VPN signalling
- PWs suited for implementing transparent point-to-point connectivity between Layer-2 circuits (E-LINE services)
- VPLS suited for implementing transparent point-to-multipoint connectivity between Ethernet links/sites (E-LAN services)
- Typical applications of L2VPNs are layer-2 business VPN services and Data Centre interconnect

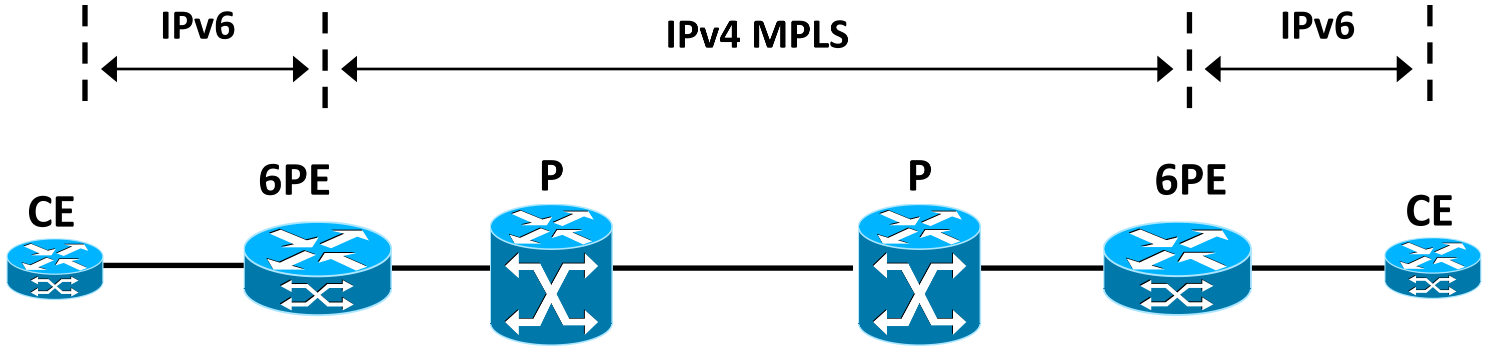
Advanced Topics

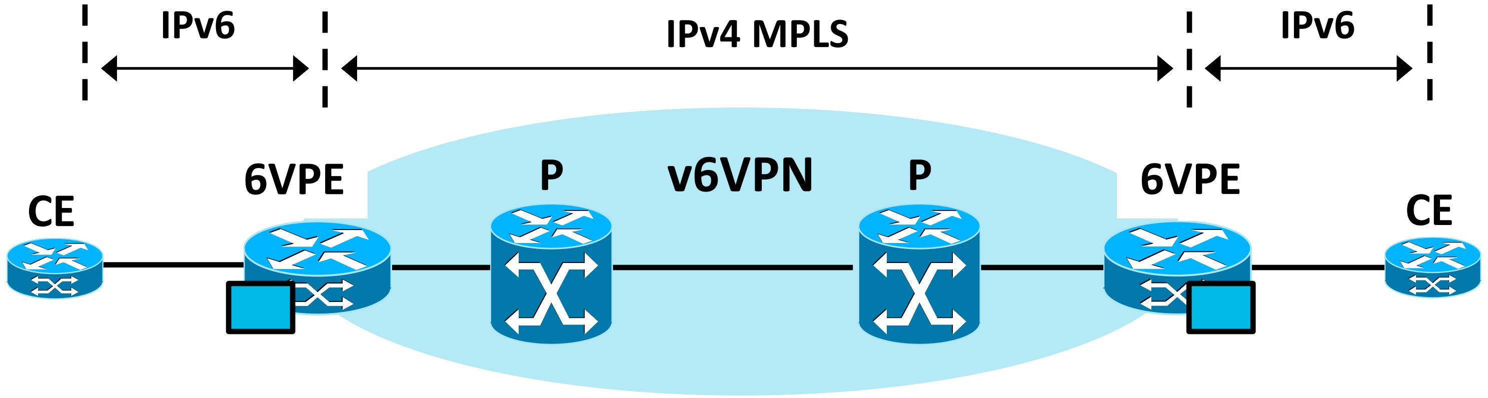
Latest MPLS Technology Developments, Trends, and Futures

MPLS And IPv6

IPv6 Support for Native MPLS Deployments and MPLS Layer-3 Services

- IPv6 traffic carried over IPv4 MPLS network
- Encapsulation of IPv6 into IPv4 LSP (6PE)
- Encapsulation of IPv6 into MPLS layer-3 VPN (6VPE)
  - Translation of IPv6 to IPv4 at PE edge



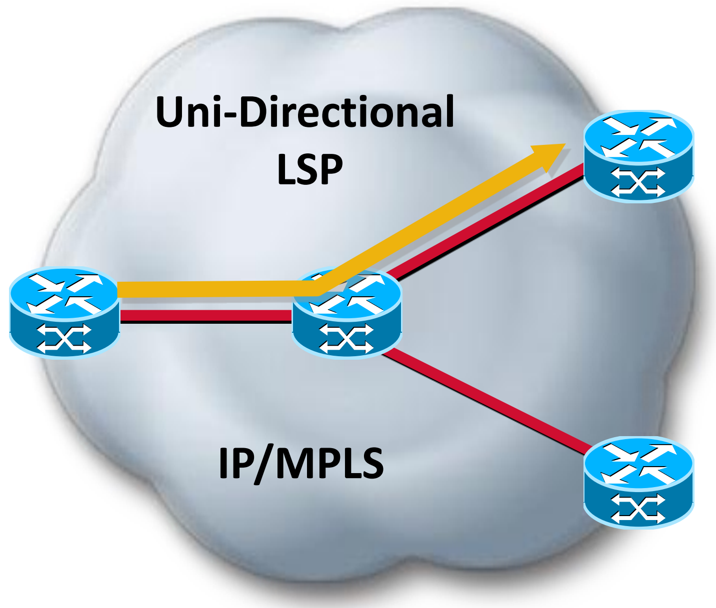


Label Switched Multicast (LSM)

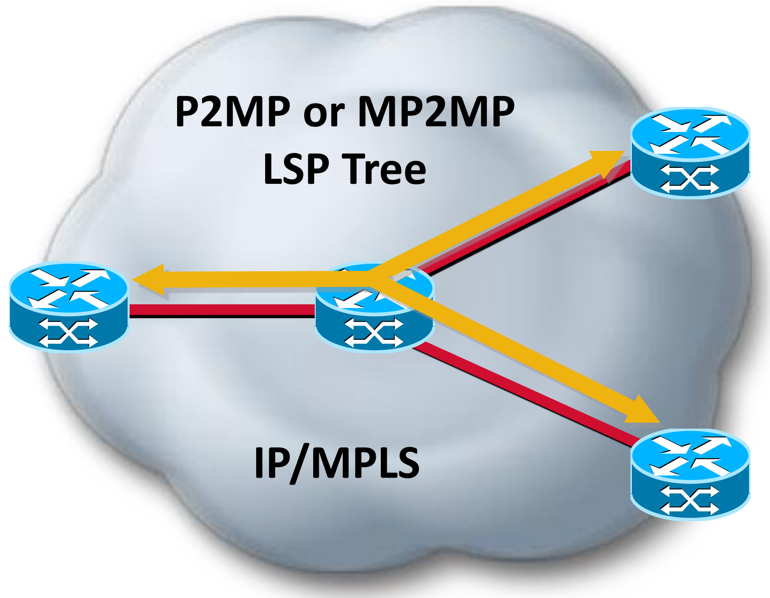
Point-to-Multi-Point MPLS Signalling and Connectivity

- What is Label Switched Multicast?
  - MPLS extensions to provide P2MP connectivity
  - RSVP extensions and multicast LDP
- Why Label-Switched Multicast?
  - Enables MPLS capabilities, which can not be applied to IP multicast traffic (e.g., FRR)
- Benefits of Label-Switched Multicast
  - Efficient IP multicast traffic forwarding
  - Enables MPLS traffic protection and BW control of IP multicast traffic

MPLS / IP



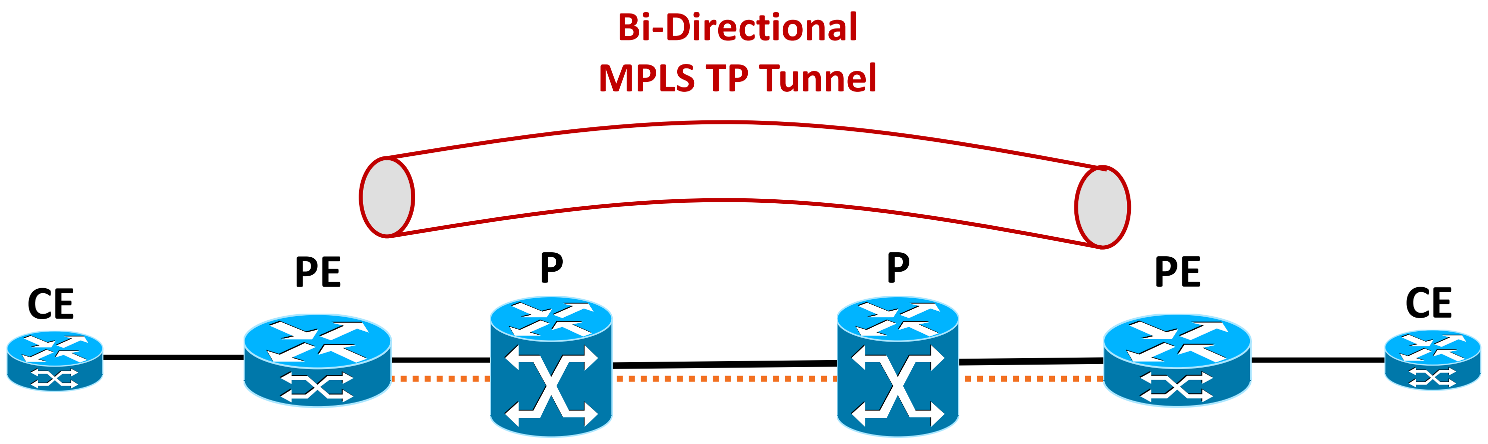
Label Switched Multicast (LSM)

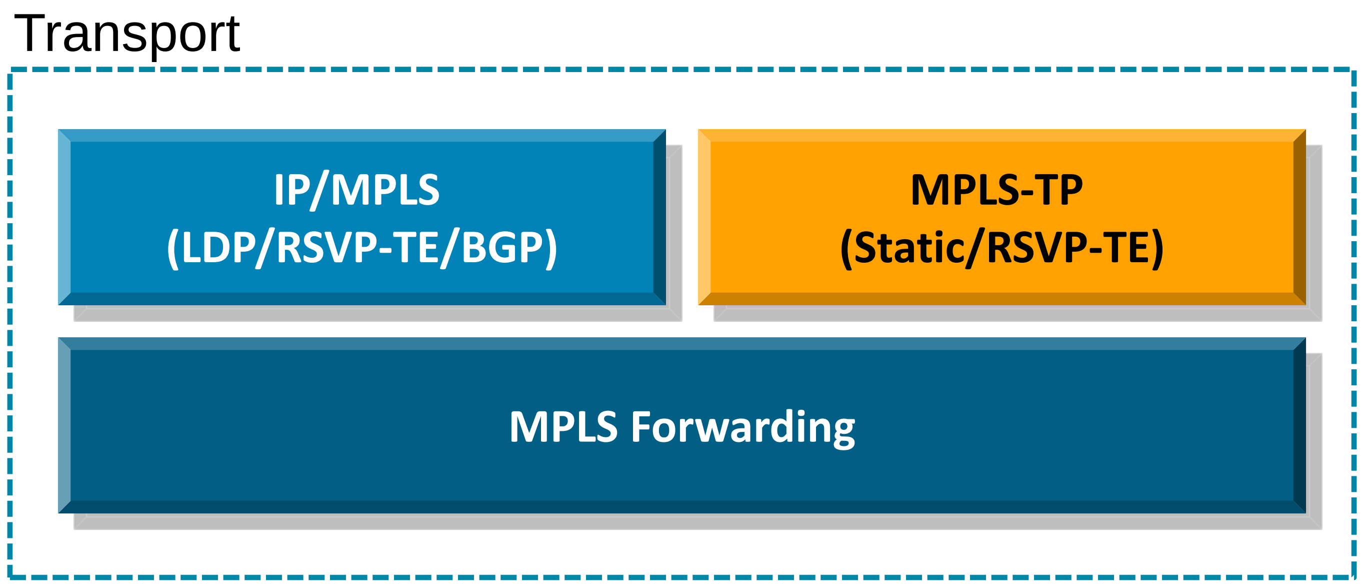


MPLS Transport Profile (TP)

Bi-Directional MPLS Tunnel Extensions For Transport Oriented Connectivity

- What is MPLS TP?
  - Point-to-point static LSPs which are co-routed
  - Bi-directional TP tunnel
- Why MPLS TP?
  - Migration of TDM legacy networks often assume continuation of connection-oriented operations model
  - MPLS TP enables packet-based transport with connection-oriented connectivity
- Benefits of MPLS TP
  - Meets transport-oriented operations requirements
  - Enables seamless migration to dynamic MPLS





Summary

Final Notes and Wrap Up

Summary

Key Takeaways

- It’s all about labels …
  - Label-based forwarding and protocol for label exchange
  - Best of both worlds … L2 deterministic forwarding and scale/flexible L3 signalling
- Key MPLS applications are end-to-end VPN services
  - Secure and scalable layer 2 and 3 VPN connectivity
- MPLS supports advanced traffic engineering capabilities
  - QoS, bandwidth control, and failure protection
- MPLS is a mature technology with widespread deployments
  - Defacto for most SPs, large enterprises, and increasingly in Data Centres
- Ongoing technology evolution
  - IPv6, optimised video transport, TP transport evolution, and cloud integration

Consider MPLS When …

Decision Criteria

- Is there a need for network segmentation?
  – Segmented connectivity for specific locations, users, applications, etc.
- Is there a need for flexible connectivity?
  – E.g., Flexible configuration of full-mesh or hub-and-spoke connectivity
- Is there a need for implementing/supporting multiple (integrated) services?
  – Leverage same network for multiple services
- Are there specific scale requirements?
  – Large number of users, customer routes, etc.
- Is there a need for optimised network availability and performance?
  – Node/link protection, pro-active connectivity validation
  – Bandwidth traffic engineering and QoS traffic prioritisation

References

Further Readings on MPLS Technology

Terminology Reference

For your reference only

Acronyms Used in MPLS Reference Architecture

Terminology	Description
AC	Attachment Circuit. An AC Is a Point-to-Point, Layer 2 Circuit Between a CE and a PE.
AS	Autonomous System (a Domain)
CoS	Class of Service
ECMP	Equal Cost Multipath
IGP	Interior Gateway Protocol
LAN	Local Area Network
LDP	Label Distribution Protocol, RFC 3036.
LER	Label Edge Router. An Edge LSR Interconnects MPLS and non-MPLS Domains.
LFIB	Labeled Forwarding Information Base
LSP	Label Switched Path
LSR	Label Switching Router
NLRI	Network Layer Reachability Information
P Router	An Interior LSR in the Service Provider's Autonomous System
PE Router	An LER in the Service Provider Administrative Domain that Interconnects the Customer Network and the Backbone Network.
PSN Tunnel	Packet Switching Tunnel

Terminology Reference

For your reference only

Acronyms Used in MPLS Reference Architecture

Terminology	Description
Pseudo-Wire	A Pseudo-Wire Is a Bidirectional “Tunnel" Between Two Features on a Switching Path.
PWE3	Pseudo-Wire End-to-End Emulation
QoS	Quality of Service
RD	Route Distinguisher
RIB	Routing Information Base
RR	Route Reflector
RT	Route Target
RSVP-TE	Resource Reservation Protocol based Traffic Engineering
VPN	Virtual Private Network
VFI	Virtual Forwarding Instance
VLAN	Virtual Local Area Network
VPLS	Virtual Private LAN Service
VPWS	Virtual Private WAN Service
VRF	Virtual Route Forwarding Instance
VSI	Virtual Switching Instance

Further Reading

For your reference only

MPLS References at Cisco Press and cisco.com

- http://www.cisco.com/go/mpls
- http://www.ciscopress.com
- MPLS and VPN Architectures — Cisco Press®
  - – Jim Guichard, Ivan Papelnjak
- Traffic Engineering with MPLS — Cisco Press®
  - – Eric Osborne, Ajay Simha
- Layer 2 VPN Architectures — Cisco Press®
  - – Wei Luo, Carlos Pignataro, Dmitry Bokotey, and Anthony Chan
- MPLS QoS — Cisco Press ®
  - – Santiago Alvarez

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Label Distribution Protocol

For your reference only

Overview

- MPLS nodes need to exchange label information with each other
  - Ingress PE node (Push operation)
    - Needs to know what label to use for a given FEC to send packet to neighbour
  - Core P node (Swap operation)
    - Needs to know what label to use for swap operation for incoming labeled packets
  - Egress PE node (Pop operation)
    - Needs to tell upstream neighbour what label to use for specific FEC type LDP used for exchange of label (mapping) information
- Label Distribution Protocol (LDP)
  - Defined in RFC 3035 and RFC3036; updated by RFC5036
  - LDP is a superset of the Cisco-specific Tag Distribution Protocol
- Note that, in addition LDP, also other protocols are being used for label information exchange
  - Will be discussed later

Label Distribution Protocol

For your reference only

Some More Details

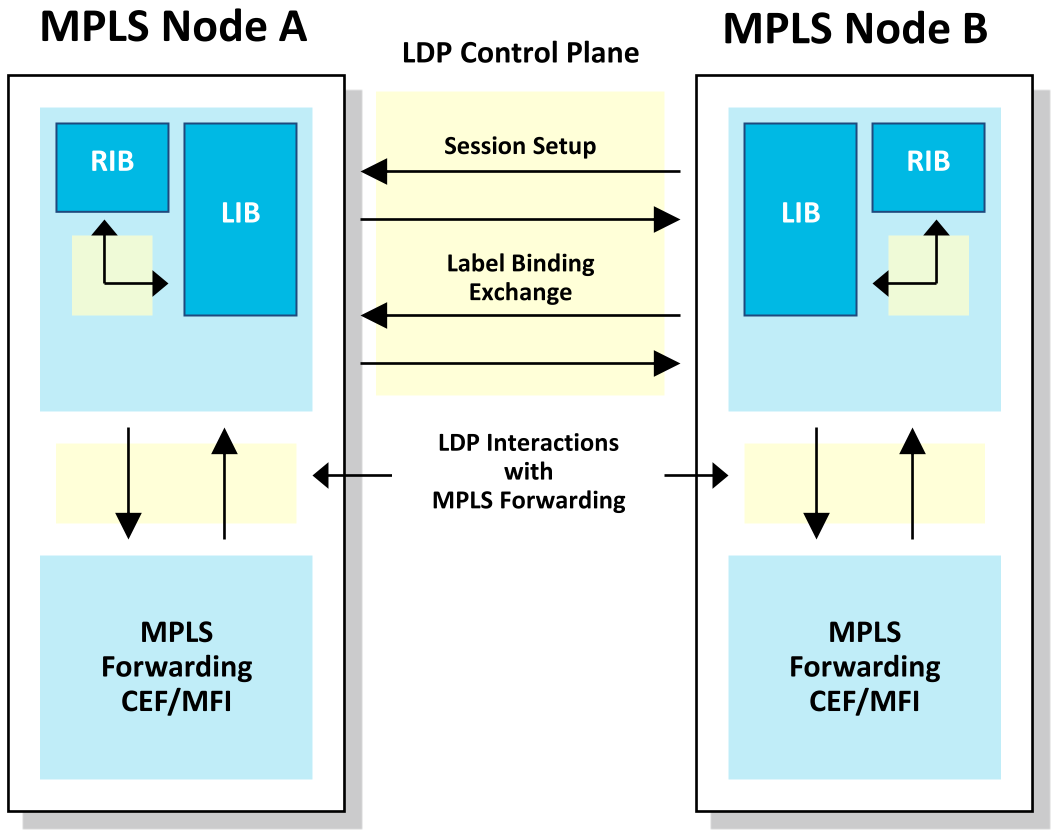
- Assigns, distributes, and installs (in forwarding) labels for prefixes advertised by unicast routing protocols
  - OSPF, IS-IS, EIGRP, etc.
- Also used for Pseudowire/PW (VC) signalling
  - Used for L2VPN control plane signalling
- Uses UDP (port 646) for session discovery and TCP (port 646) for exchange of LDP messages
- LDP operations
  - LDP Peer Discovery
  - LDP Session Establishment
  - MPLS Label Allocation, Distribution, and Updating MPLS forwarding
- Information repositories used by LDP
  - LIB: Label Information Database (read/write)
  - RIB: Routing Information Database/routing table (read-only)

Label Distribution Protocol

Operations Details

For your reference only

- LDP startup
  - Local labels assigned to RIB prefixes and stored in LIB
  - Peer discovery and session setup
  - Exchange of MPLS label bindings
- Programming of MPLS forwarding
  - Based on LIB info
  - CEF/MFI updates



Why MPLS QoS

For your reference only

The Need for Differentiated Services

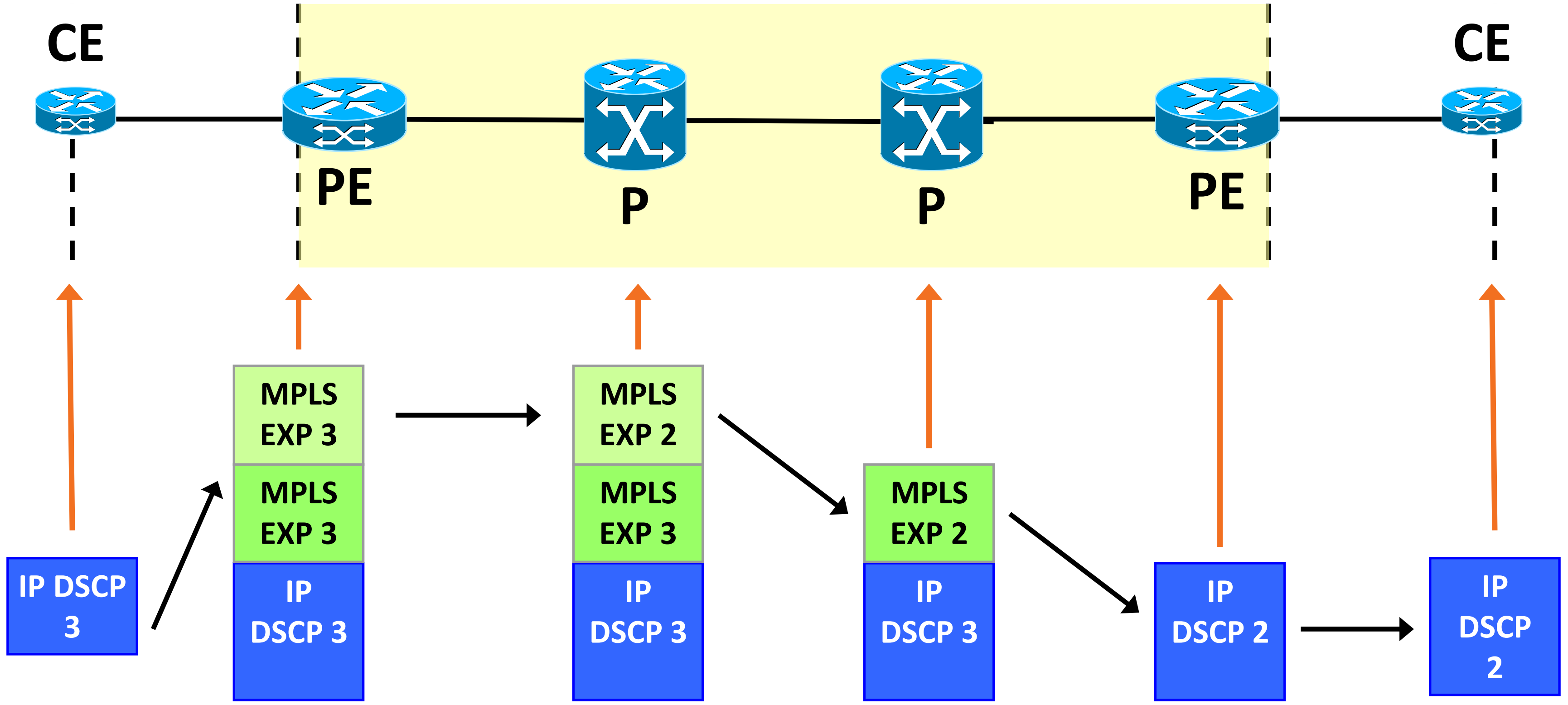
- Typically different traffic types (packets) sent over MPLS networks
  - E.g., Web HTTP, VoIP, FTP, etc.
- Not all traffic types/flows have the same performance requirements …
  - Some require low latency to work correctly; e.g., video
- MPLS QoS used for traffic prioritisation to guarantee minimal traffic loss and delay for high priority traffic
  - Involves packet classification and queuing
- MPLS leverages mostly existing IP QoS architecture
  - Based on Differentiated Services (DiffServ) model; defines per-hop behaviour based on IP Type of Service (ToS) field

MPLS Uniform Mode

QoS Field Assignments in MPLS Network

For your reference only

- End-to-end behaviour:
  - Original IP DSCP value not preserved
- At ingress PE:
  - IP DSCP value copied in EXP value of MPLS label
- EXP value changed in the MPLS core
  - Based on traffic load and congestion
- At egress PE:
  - EXP value copied back into IP DSCP value

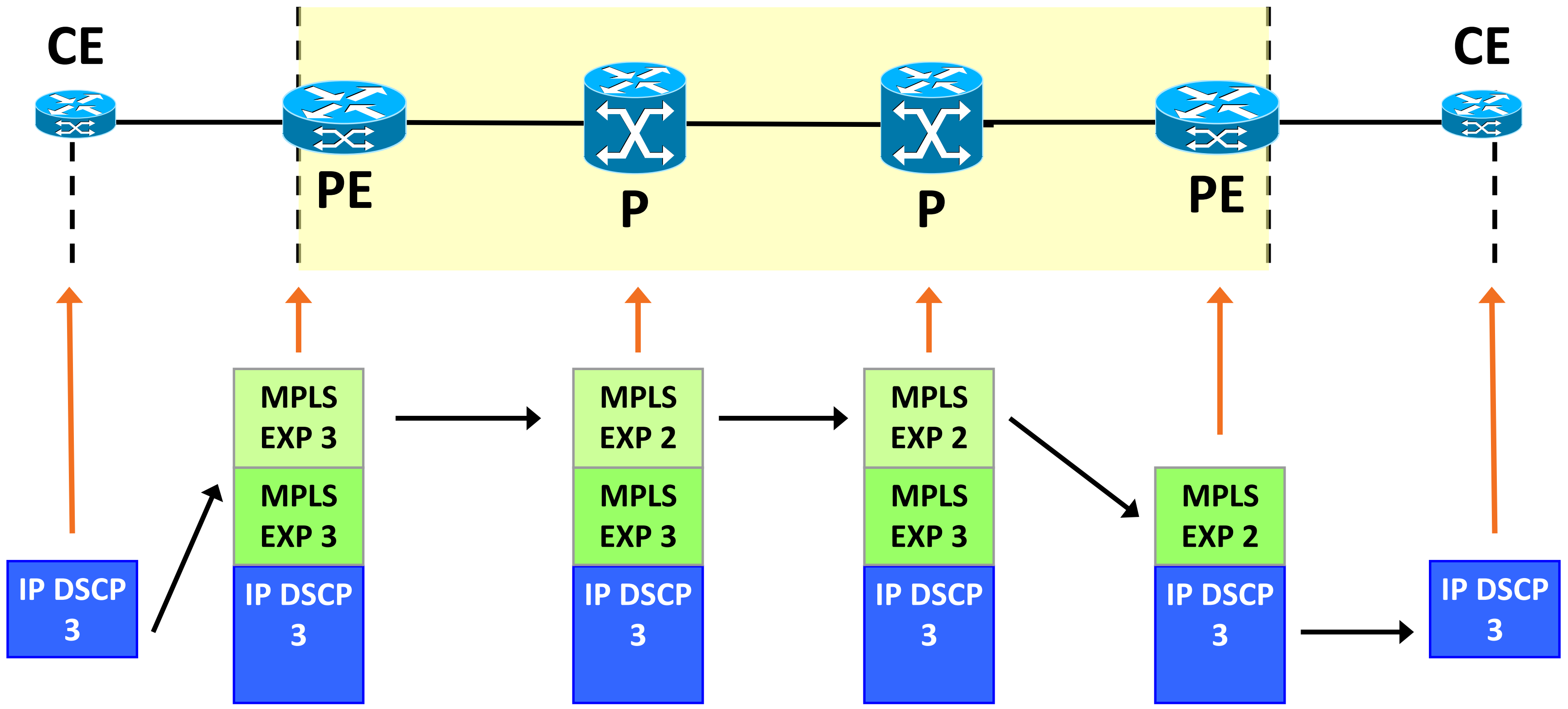


MPLS Pipe Mode

QoS Field Assignments in MPLS Network

For your reference only

- End-to-end behaviour:
  - Original IP DSCP is preserved
- At ingress PE:
  - EXP value set based on ingress classification
- EXP changed in the MPLS core
  - Based on traffic load and congestion
- At egress PE:
  - EXP value not copied back into IP DSCP value

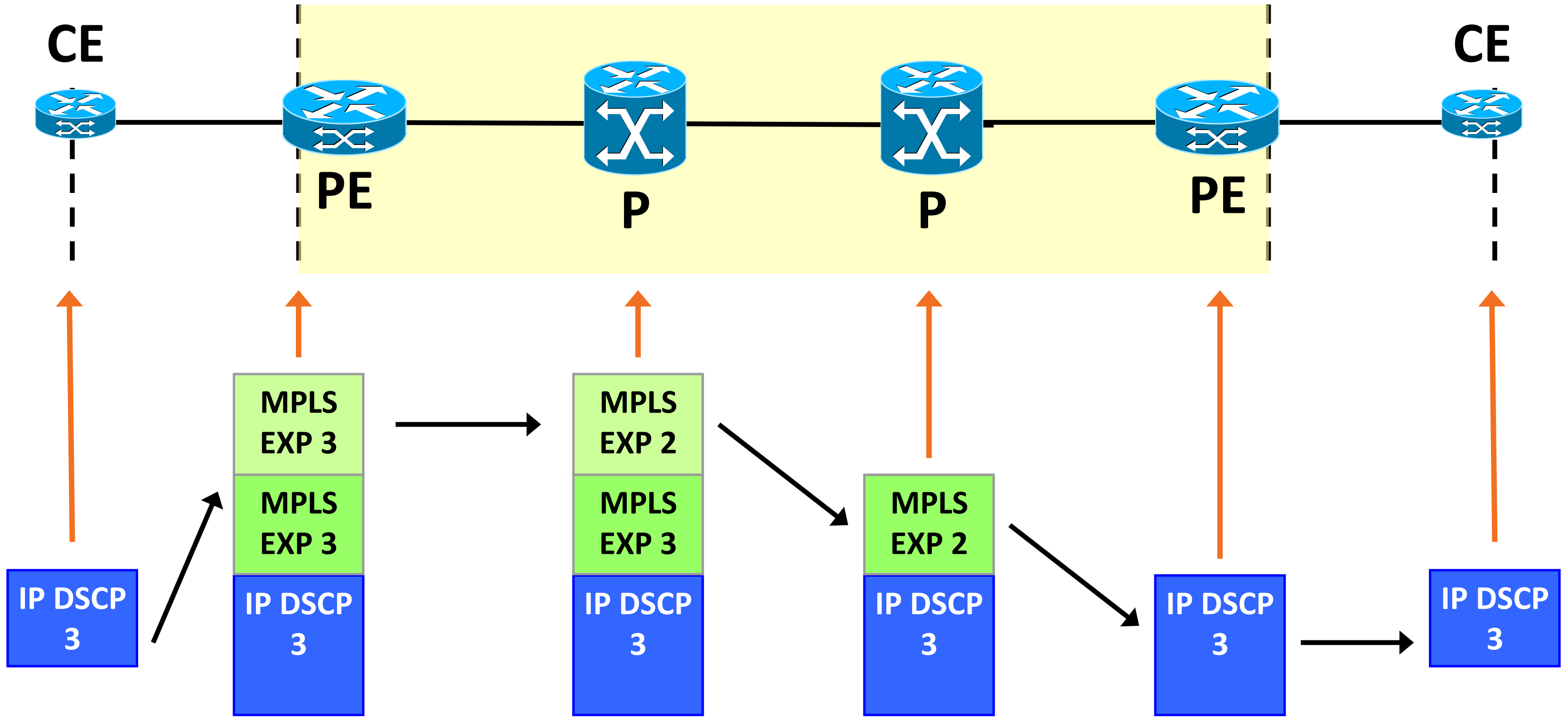


MPLS Short Pipe Mode

QoS Field Assignments in MPLS Network

For your reference only

- End-to-end behaviour:
  - Original IP DSCP is preserved
- At ingress PE:
  - EXP value set based on ingress classification
- EXP changed in the MPLS core
  - Based on traffic load and congestion
- At egress PE:
  - Original IP DSCP value used for QoS processing



Why MPLS Traffic Engineering?

For your reference only

Drivers for MPLS Traffic Management

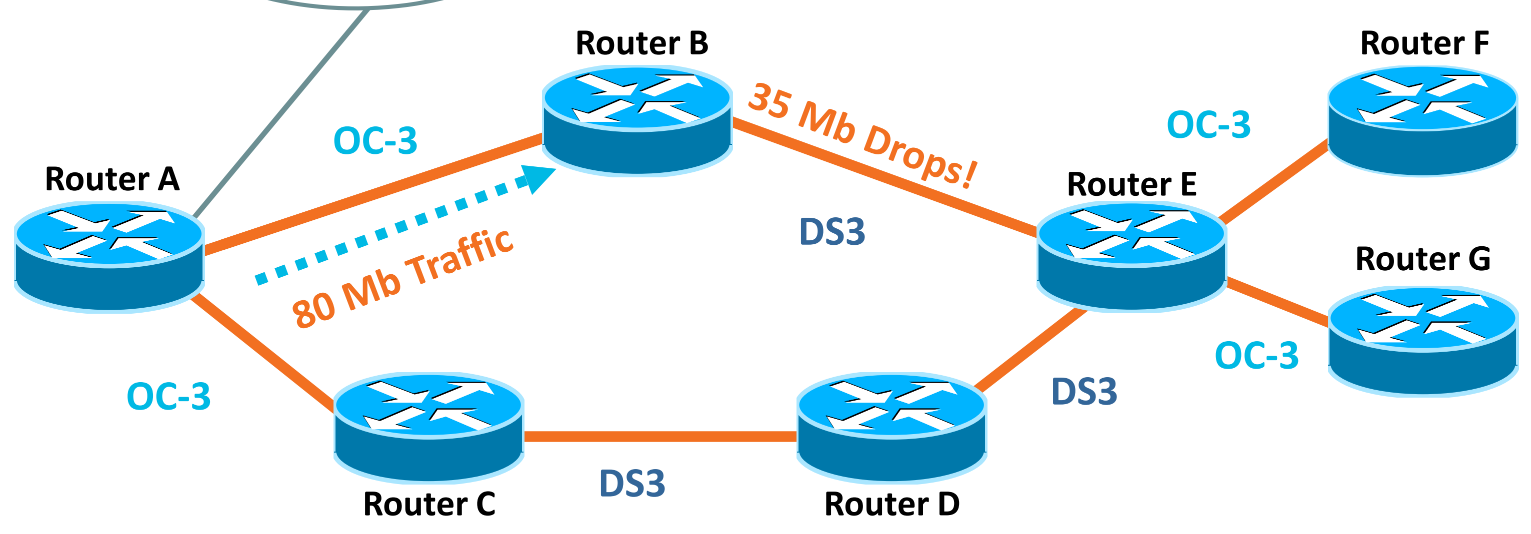
- Need for better utilisation of available network bandwidth
  - Optimise traffic distribution throughout network
  - Network capacity management
- Protection against link and node failures
  - Fast rerouting around failures to minimise (service) traffic loss
  - Optimise aggregate availability of network
- Delivery of premium services and enhanced SLAs
  - Ability to support guaranteed high availability and bandwidth for services
- Congestion in network due to changing traffic patterns
  - Optimise high bandwidth traffic flows; streaming video, database backup, etc.

The Problem with Shortest-Path Forwarding

Alternate Path Under Utilisation As a Result of Least-Cost Routing

- Some links are DS3, some are OC-3
- Router A has 40M of traffic for router F, 40M of traffic for router G
- Massive (44%) packet loss at router B→router E!
- Changing to traffic forwarding to A->C->D->E won't help

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	B	30
G	B	30



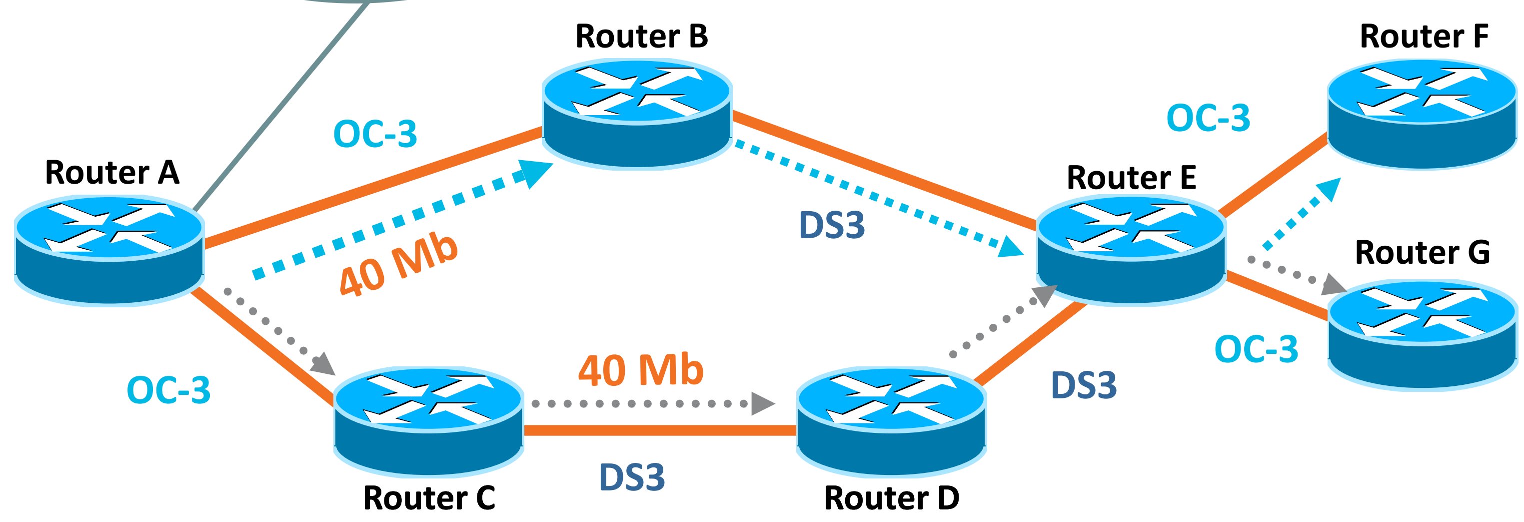
How MPLS TE Solves the Problem

For your reference only

Optimised Path Computation Via Additional Costs Metrics

- Router A sees all links
- Router A computes paths on properties other than just shortest cost
  - – Creation of 2 tunnels
- No link oversubscribed!

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	Tunnel 0	30
G	Tunnel 1	30

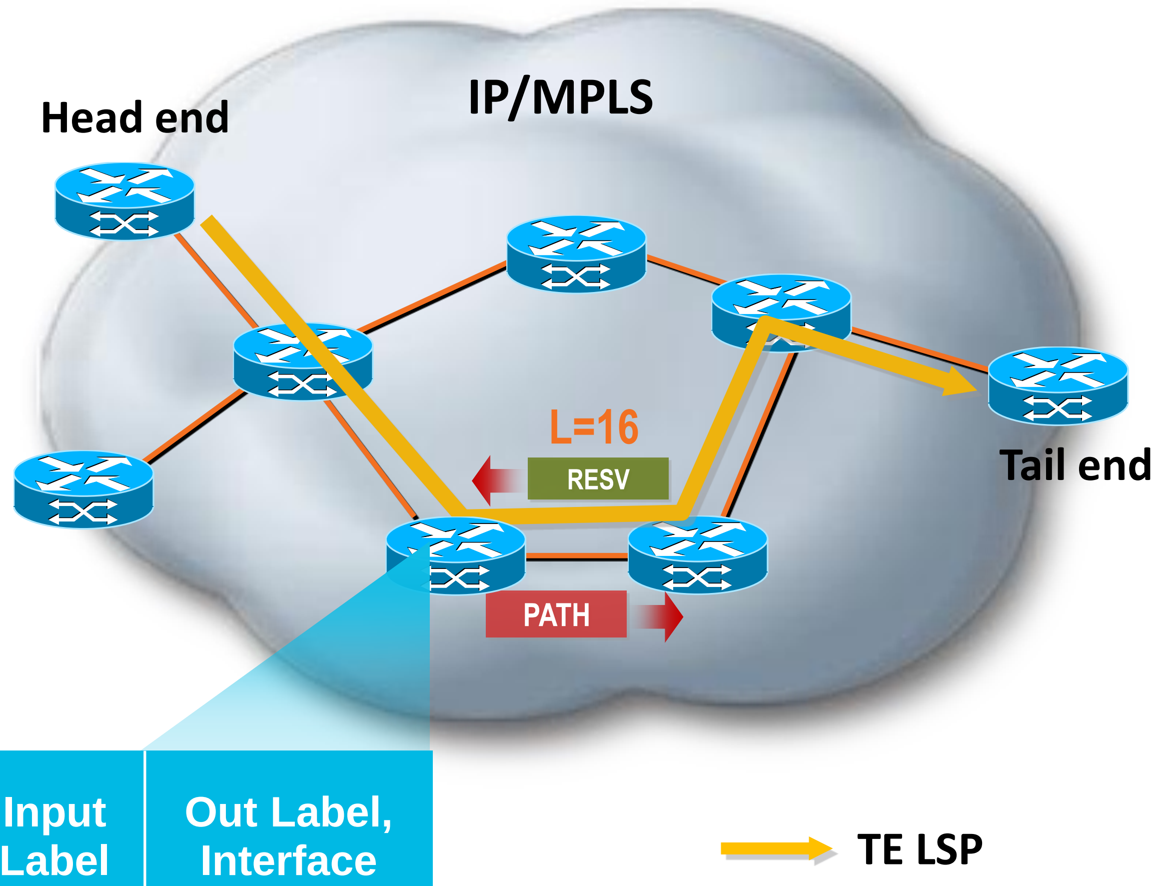


TE Tunnel Signalling

RSVP Signalling of MPLS Connectivity

For your reference only

- Tunnel signaled with TE extensions to RSVP
- Soft state maintained with downstream PATH messages
- Soft state maintained with upstream RESV messages
- New RSVP objects
  - LABEL_REQUEST (PATH)
  - LABEL (RESV)
  - EXPLICIT_ROUTE
  - RECORD_ROUTE (PATH/RESV)
  - SESSION_ATTRIBUTE (PATH)
- LFIB populated using RSVP labels allocated by RESV messages



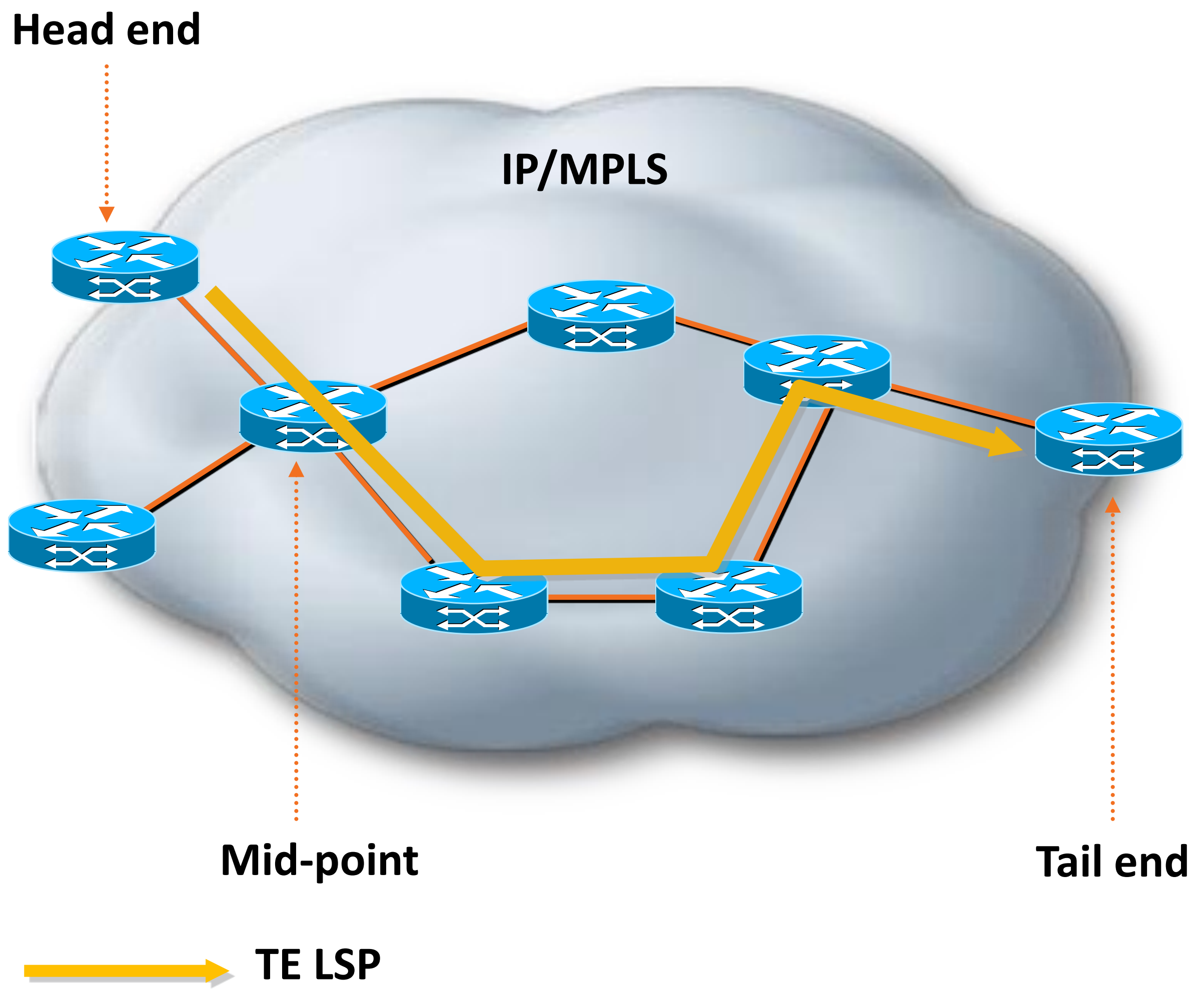
Input Label	Out Label, Interface
17	16, 0

MPLS Traffic Engineering

Technology Building Blocks

For your reference only

- Link information Distribution*
  - ISIS-TE
  - OSPF-TE
- Path Calculation (CSPF)*
  - At head-end node
- Path Setup (RSVP-TE)
- Unidirectional forwarding traffic down Tunnel
  - Auto-route
  - Static
  - PBR
  - CBTS / PBTS
  - Forwarding Adjacency
  - Tunnel select



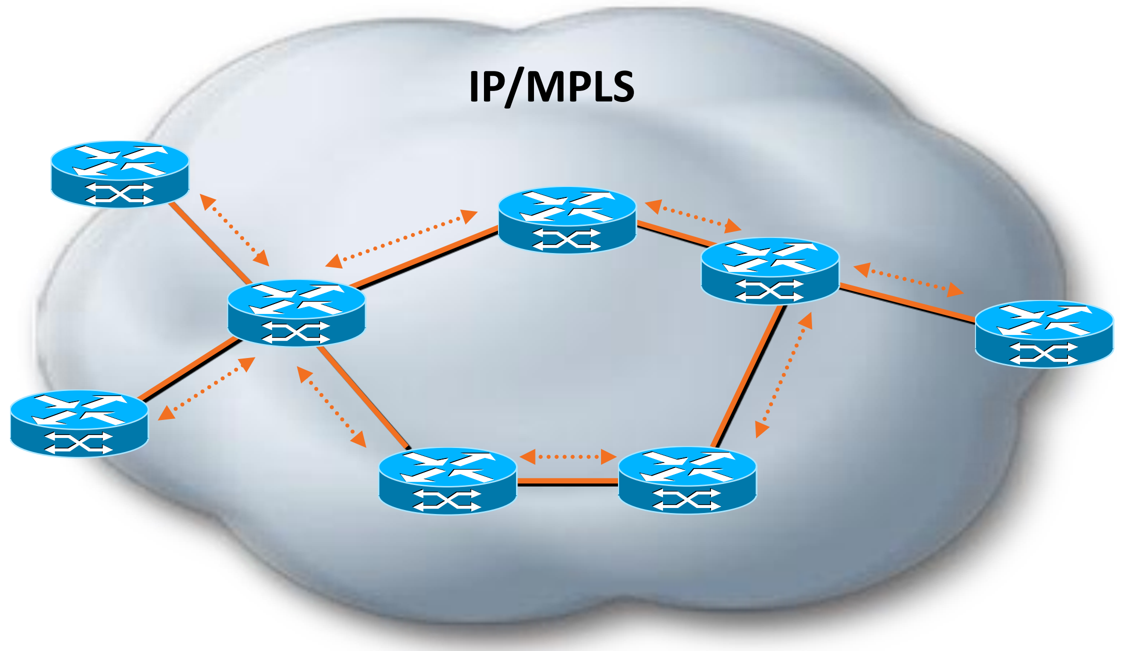
* Optional

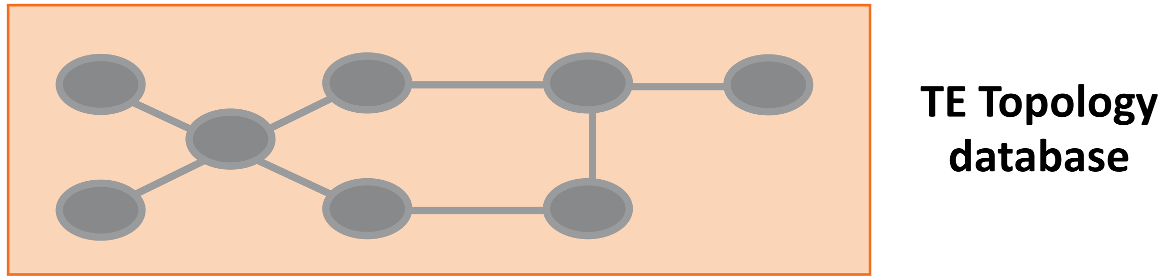
Distribution of Link Information

Additional Metrics for Path Computation

For your reference only

- Additional link characteristics
  - Interface address
  - Neighbour address
  - Physical bandwidth
  - Maximum reservable bandwidth
  - Unreserved bandwidth (at eight priorities)
  - TE metric
  - Administrative group (attribute flags)
- IS-IS or OSPF flood link information
- TE nodes build a topology database
- Not required if using off-line path computation



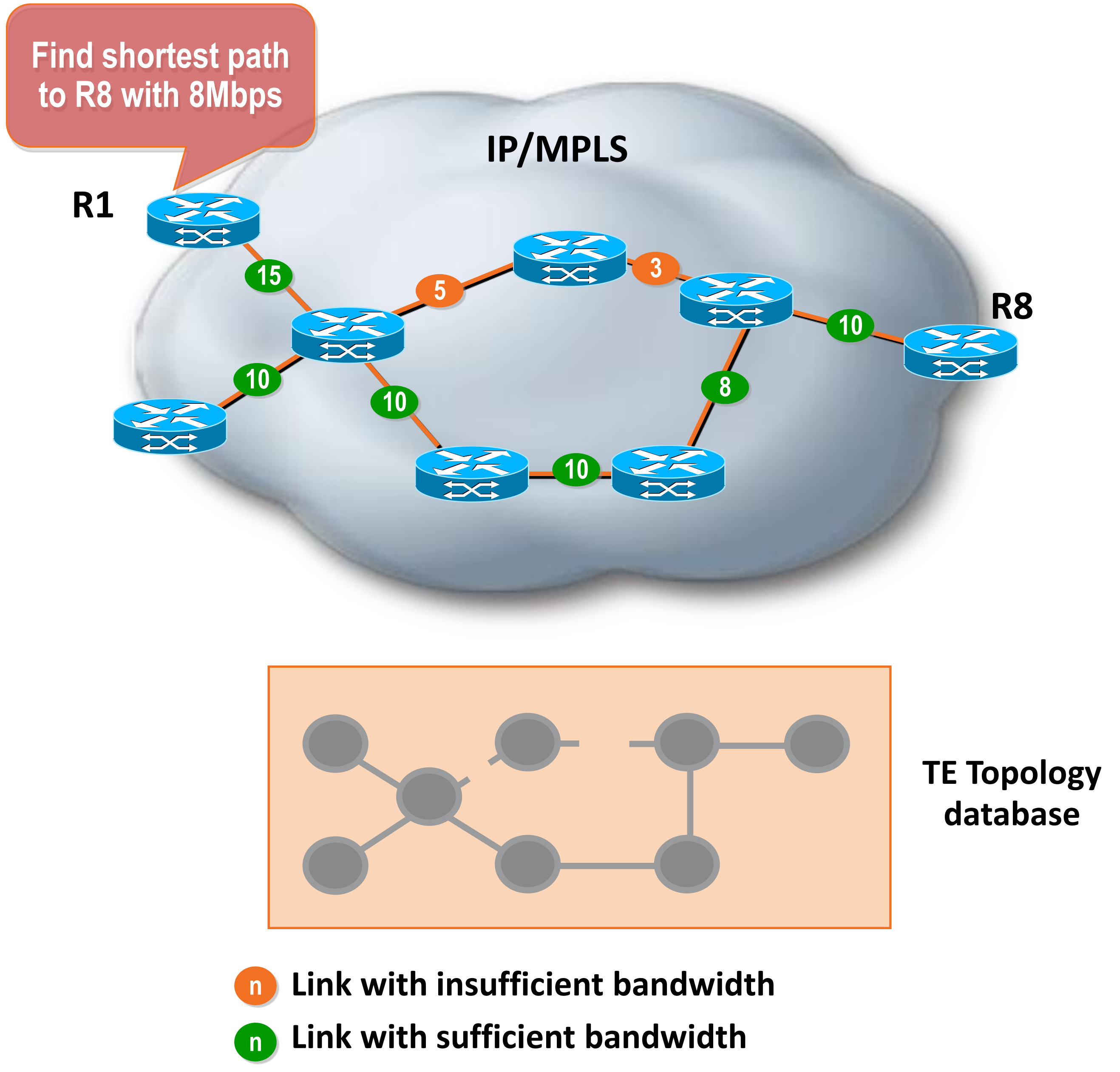


Path Calculation

Calculation of Optimal Network Path, Based on Multiple Metrics

For your reference only

- TE nodes can perform constraint-based routing
- Constraints and topology database as input to path computation
- Shortest-path-first algorithm ignores links not meeting constraints
- Tunnel can be signaled once a path is found
- Not required if using offline path computation

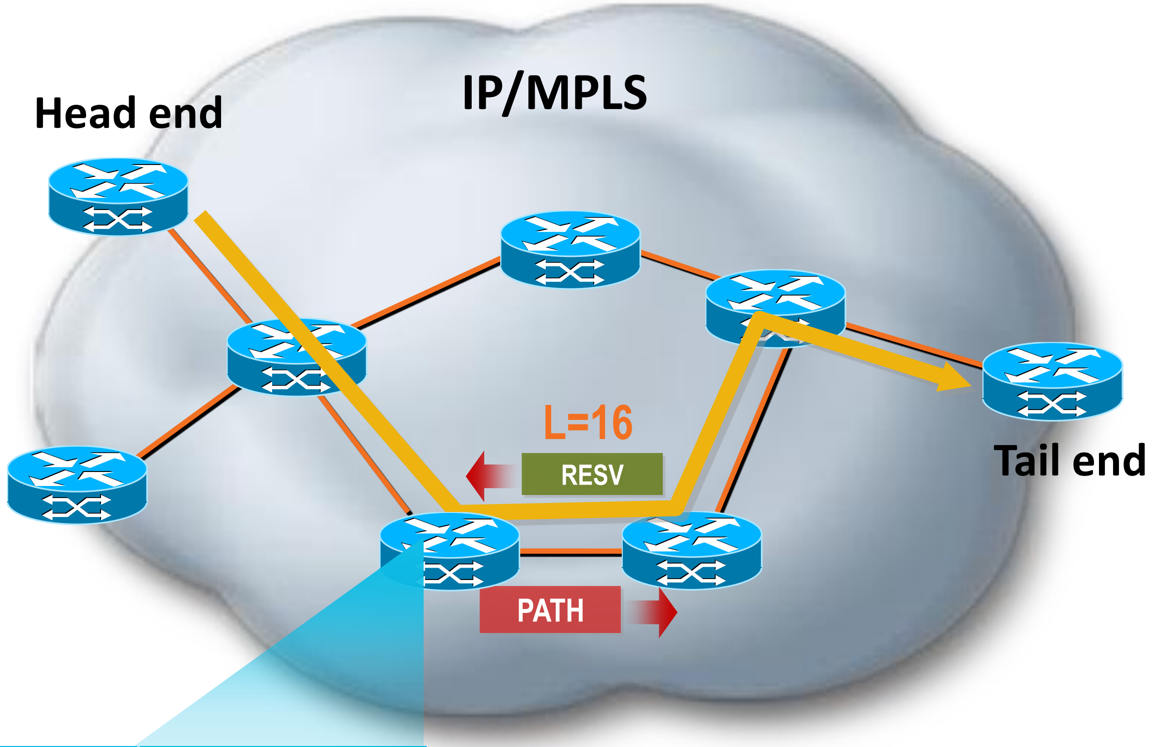


For your reference only

TE Tunnel Signalling

End-to-end Signalling of TE Tunnel in MPLS Network

- Tunnel signaled with TE extensions to RSVP
- Soft state maintained with downstream PATH messages
- Soft state maintained with upstream RESV messages
- New RSVP objects
  - LABEL_REQUEST (PATH)
  - LABEL (RESV)
  - EXPLICIT_ROUTE
  - RECORD_ROUTE (PATH/RESV)
  - SESSION_ATTRIBUTE (PATH)
- LFIB populated using RSVP labels allocated by RESV messages



Input Label	Out Label, Interface
17	16, 0

TE LSP

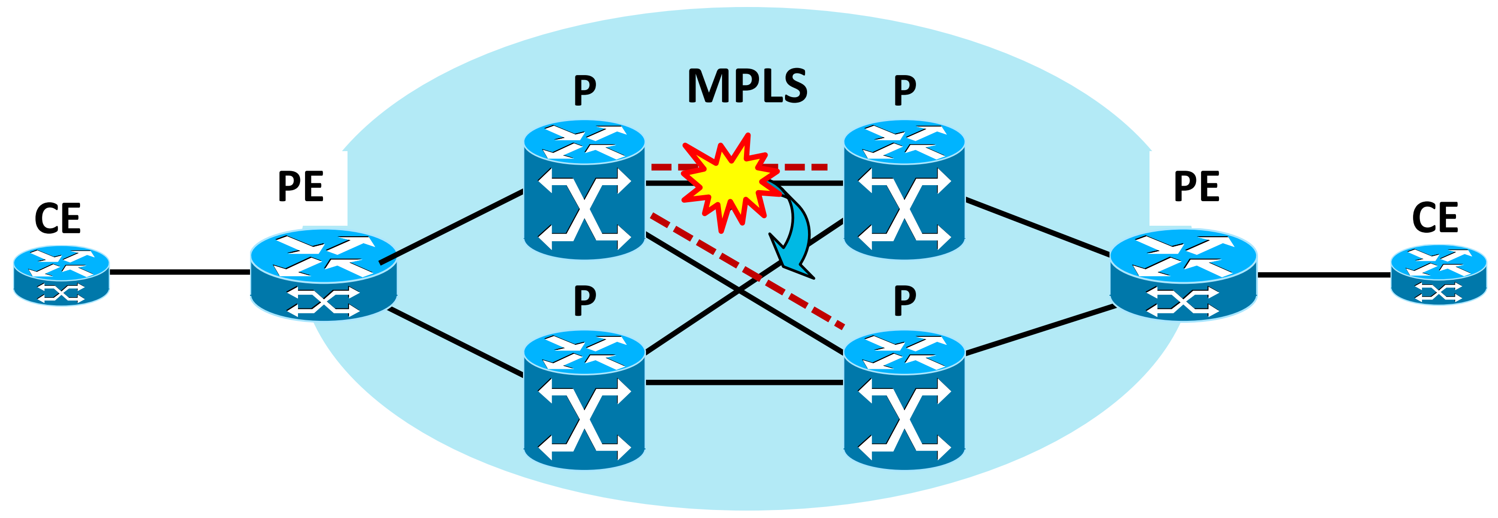
Service Provider Deployment Scenario

For your reference only

Implementing Sub-Second Failure Protection Using MPLS TE FRR

- Deployment Use Case
  - Implementing sub-second failure protection in MPLS core network
- Benefits
  - Sub-second failover protection against link failures in core network

    Can be less than 50 ms
  - Predictable traffic flows after core link failures



Network Segment	CPE	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	ASR1K ISR/G2	ASR9K 7600 ASR1K ASR903 ME3800X	CRS-1 GSR ASR9K

MPLS Management

Overview

For your reference only

Basic CLI (Craft interface):

- CLI used for basic configuration and trouble shooting (show commands)

Traditional management tools:

- SNMP MIBs to provide management information for SNMP (NMS) management applications
- MIB counters, Trap notifications, etc.

New management tools:

- MPLS OAM; used for reactive trouble shooting
  – LSP Ping and LSP Trace for trouble shooting MPLS label switched paths
- Automated MPLS OAM; used for proactive trouble shooting
  – Automated LSP ping/trace via Auto IP SLA