We’re ready.
Are you?

Understanding MPLS

Khurram Waheed
Systems Engineer

Cisco live!

Session Goals

- Understand the problems MPLS is addressing
- Understand major MPLS technology components
- Understand typical MPLS applications
- Understand benefits of deploying MPLS

Agenda

- Introduction
- MPLS Basics
- MPLS Layer-3 VPNs
- MPLS Layer-2 VPNs
- MPLS Traffic Engineering
- Summary

Introduction

Why Multi-Protocol Label Switching?

- **SP/Carrier perspective**
  - Reduce costs (CAPEX/OPEX); consolidate networks and maximise utilisation of resources.
  - Consolidated network for multiple Layer-2/3 services over same infrastructure
  - Support increasingly stringent SLAs (Voice + Video etc.)
- **Enterprise/end-user perspective**
  - Campus/LAN
  - Need for network segmentation (users, applications, etc.)

What is MPLS?

Brief Summary

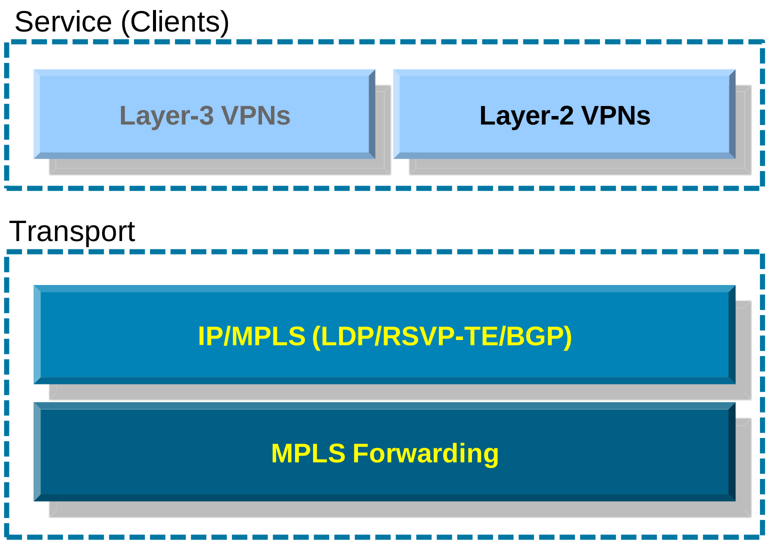
- **It’s all about labels …**
- **Use the best of both worlds**
  - Layer-2: efficient forwarding and traffic engineering
  - Layer-3: flexible and scalable
- **MPLS forwarding plane**
  - Use of labels for forwarding Layer-2/3 data traffic
  - Labeled packets are switched; instead of routed
    - Leverage 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 Basics

Topics

Basics of MPLS Signalling and Forwarding

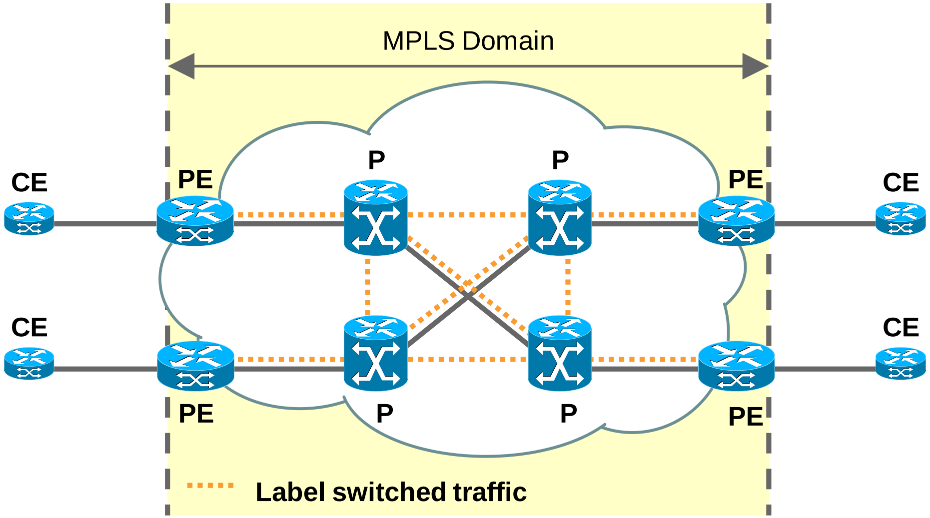
- MPLS Reference Architecture
- MPLS Labels
- MPLS Signalling and Forwarding Operations



MPLS Reference Architecture

Different Types of Nodes in an 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



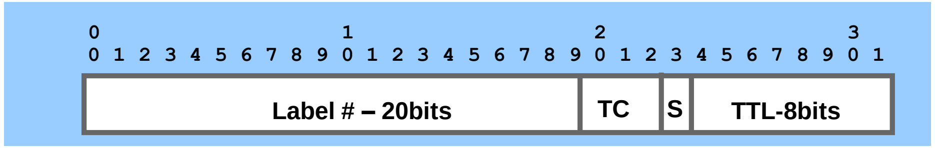
Cisco live!

MPLS Labels

Label Definition and Encapsulation

- 4 Bytes (32Bits) in size
- 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 for services (VPNs etc.)

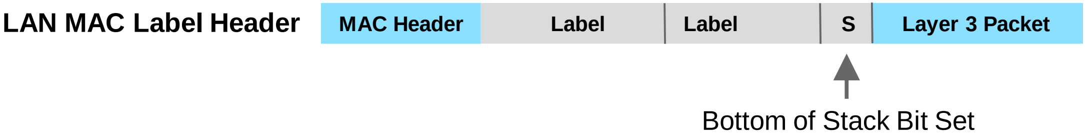
MPLS Label



TC = Traffic Class: 3 Bits; S = Bottom of Stack; TTL = Time to Live

MPLS Label Encapsulation

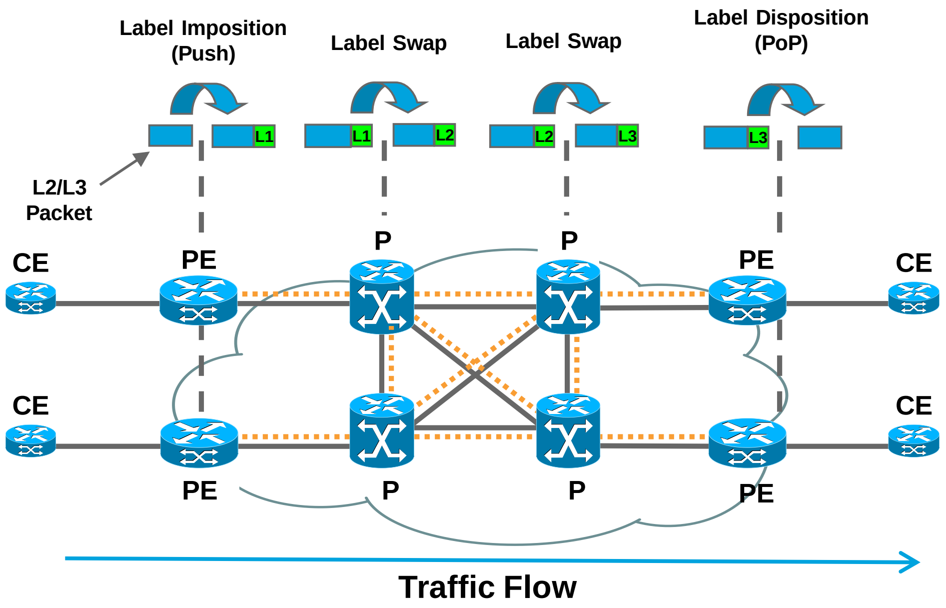
MPLS Label Stack



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 (SWAP)**
  - 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

Overview

- **IGP (OSPF/ISIS)**
  - Learns MPLS Loopback Interfaces (loopback0 etc.)
- **LSP signalling**
  - Either LDP or RSVP
  - Leverages IP routing (RIB from IGP)
- **Exchange of labels**
  - Label bindings
  - Downstream MPLS node advertises what label to use
- **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

MPLS Path (LSP) Setup

Signalling Options

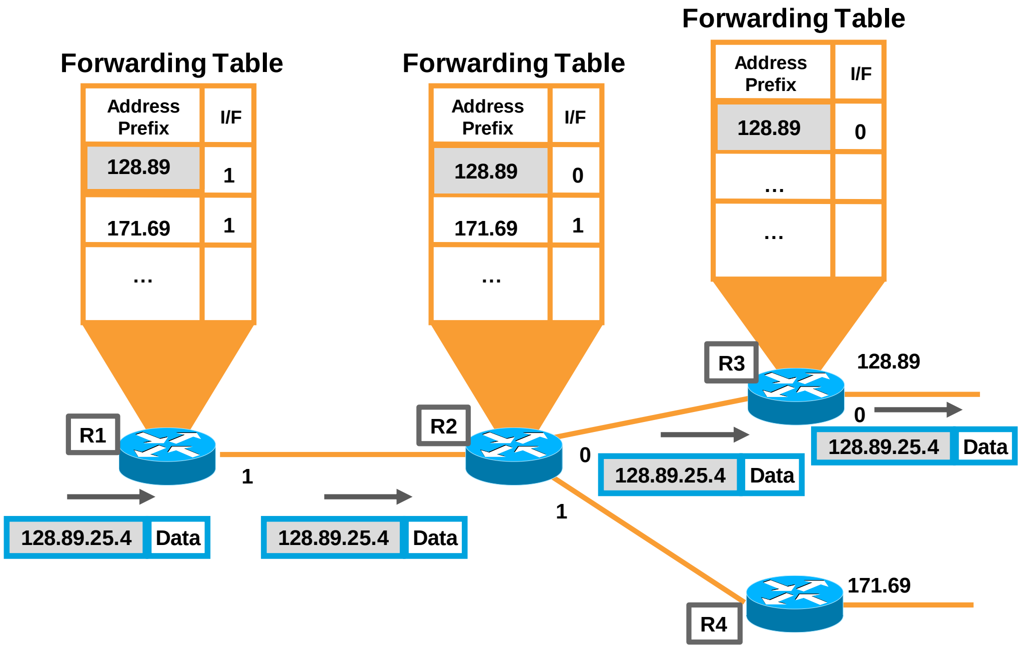
- **LDP signalling**
  - Leverages existing routing (RIB)
- **RSVP signalling**
  - Aka MPLS RSVP/TE
  - Enables enhanced capabilities, such as Fast Re-Route (FRR)

	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, etc.
- Establish IP reachability

Forwarding Table

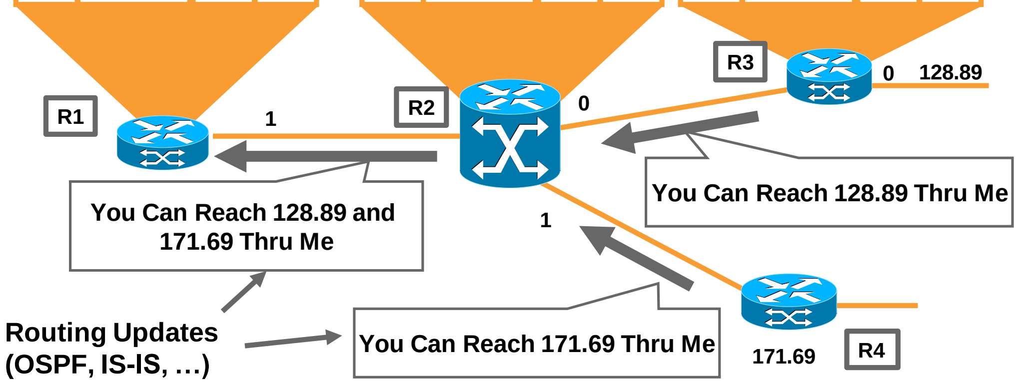
In Label	Address Prefix	Out I'face	Out Label
	128.89	1	
	171.69	1	
	…	…	

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: Assign Local Labels

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

Forwarding Table

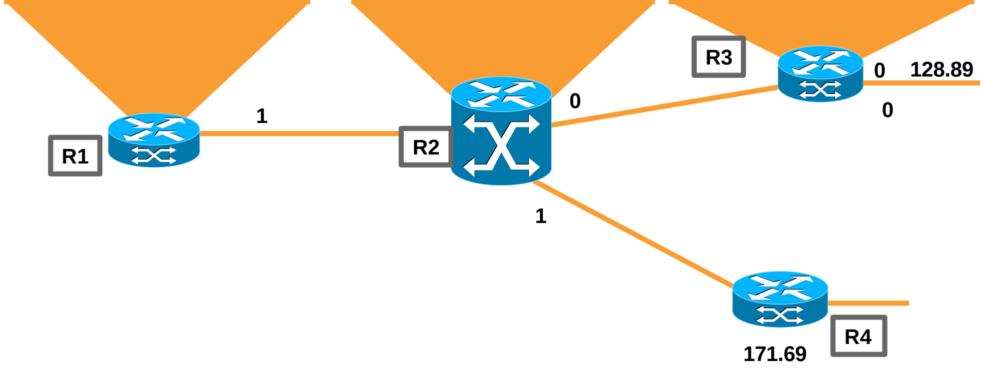
In Label	Address Prefix	Out I'face	Out Label
-	128.89	1	
-	171.69	1	
...	...	...	...

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	-
...	...	...	...



Cisco live!

MPLS Path (LSP) Setup

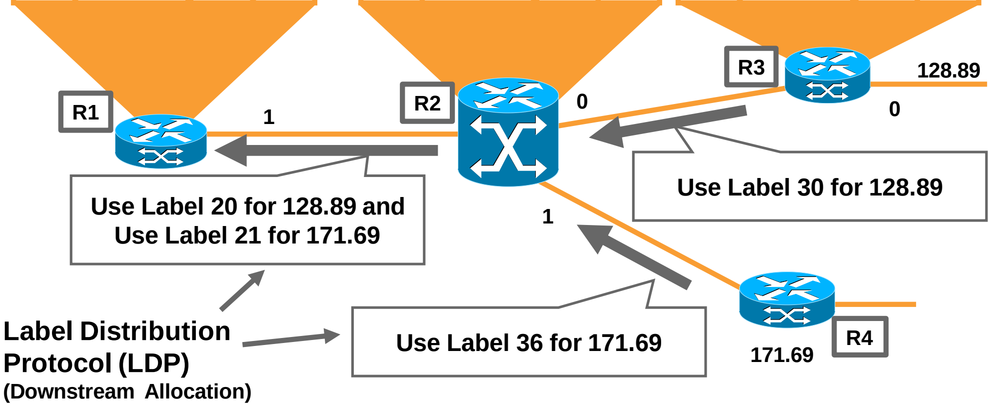
Step 2B: Assign Remote Labels

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

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

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

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



MPLS Traffic Forwarding

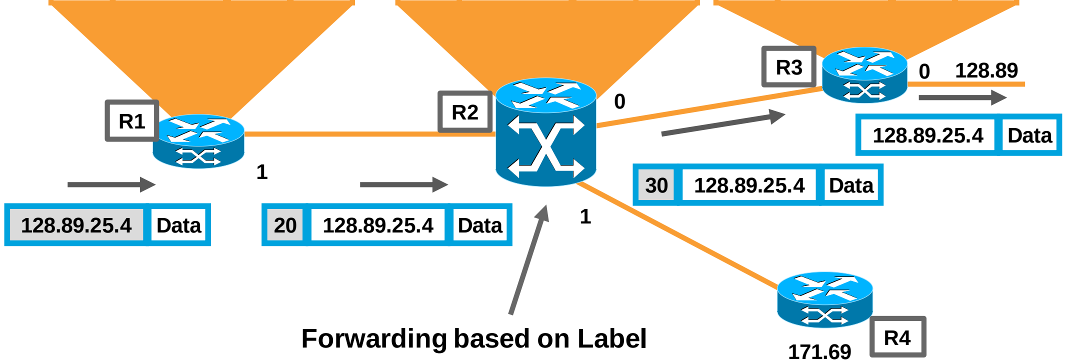
Hop-by-Hop Traffic Forwarding Using Labels

- 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)

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

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

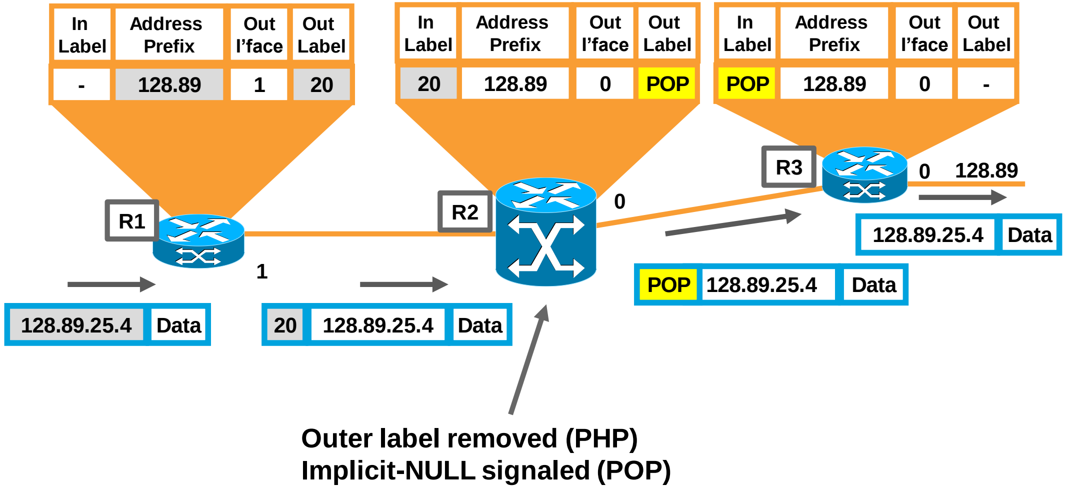
In Label	Address Prefix	Out I'face	Out Label
30	128.89	0	-
…	…	…	…



MPLS Penultimate Hop Popping

Forwarding Efficiency Gains with PHP

- Downstream node signals POP label (Implicit NULL)
- Last LSR (P) removes outer label before sending to LER (PE)
- Improves LER (PE) performance by not performing multiple label lookups to forward to final packet
- Explicit-NULL can be used for QoS requirements



Summary…So Far...

Key Takeaways

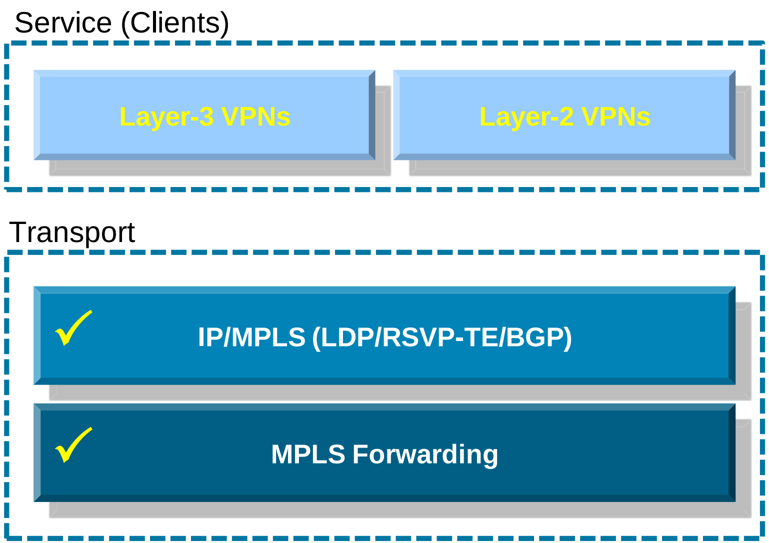
- MPLS networks consist of **PE** routers at in/egress and **P** routers in core
- Traffic is encapsulated with label(s) at ingress (PE router)
- Labels are removed at egress (PE router)
- MPLS forwarding operations include label imposition (**PUSH**), swapping (**SWAP**), and disposition (**POP**)
- Penultimate Hop Popping (**PHP**) is used to improve LER performance.
- **LDP** and/or **RSVP** can be used for signalling label mapping information to set up an end-to-end Label Switched Path (**LSP**)

MPLS Virtual Private Networks

MPLS Virtual Private Networks

Topics

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



What is a Virtual Private Network?

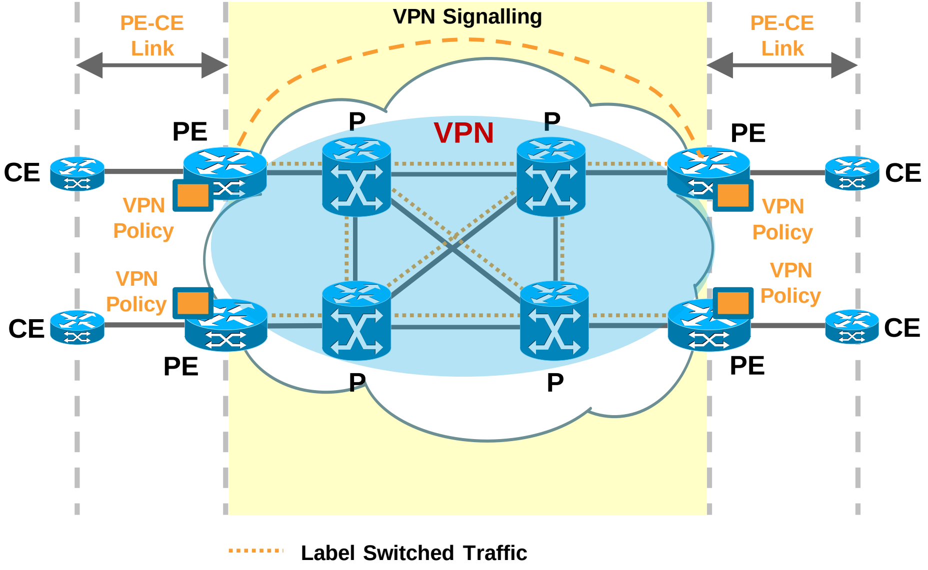
Definition

- **Set of sites which communicate with each other**
  - 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)

MPLS VPN Example

Basic Building Blocks

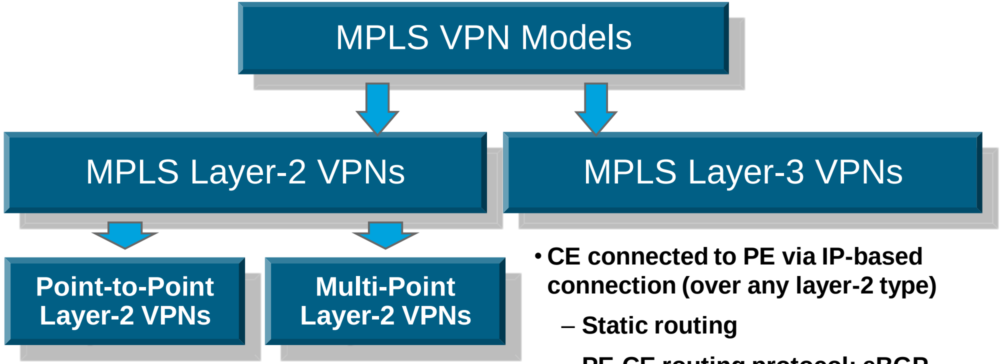
- **VPN policies**
  - Configured on PE routers (manual operation)
- **VPN signalling**
  - Between PEs
  - Exchange of VPN policies
- **VPN traffic forwarding**
  - Additional VPN-related MPLS label encapsulation
- **PE-CE link**
  - Connects customer network to MPLS network; either layer-2 or layer-3



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)



Point-to-Point Layer-2 VPNs

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

Multi-Point Layer-2 VPNs

- **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 SP involvement**

MPLS Layer-3 VPNs

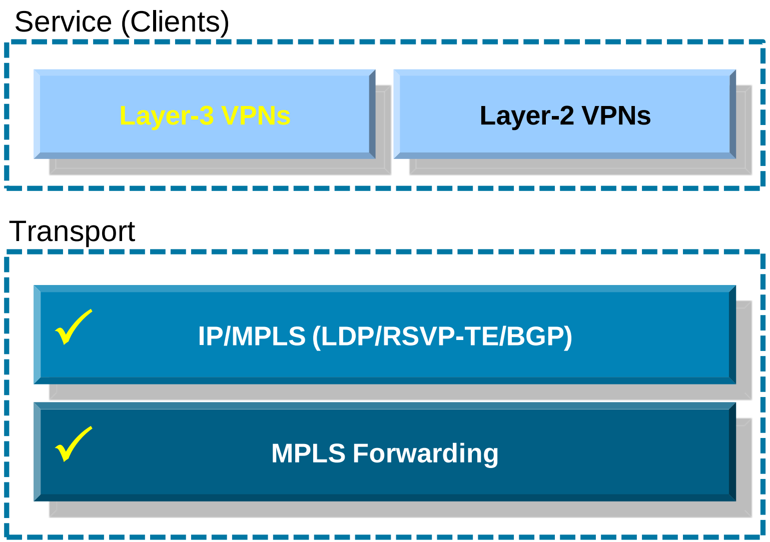
- **CE connected to PE via IP-based connection (over any layer-2 type)**
  - **Static routing**
  - **PE-CE routing protocol; eBGP, OSPF, IS-IS**
- **CE routing has peering relationship with PE router; PE routers are part of customer routing**
- **PE routers maintain customer-specific routing tables and exchange customer=specific routing information**

MPLS Layer-3 Virtual Private 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

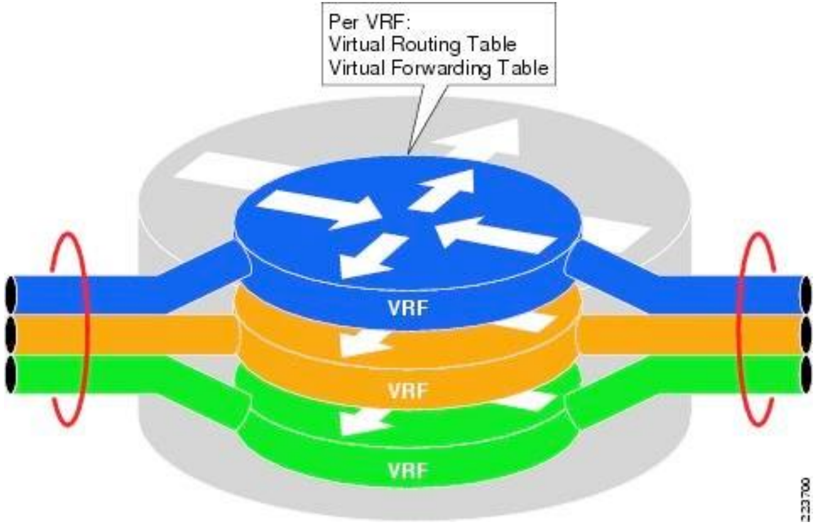
Technology Components

- **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 - VRF

Virtual Routing Table and Forwarding Separate to Customer Traffic

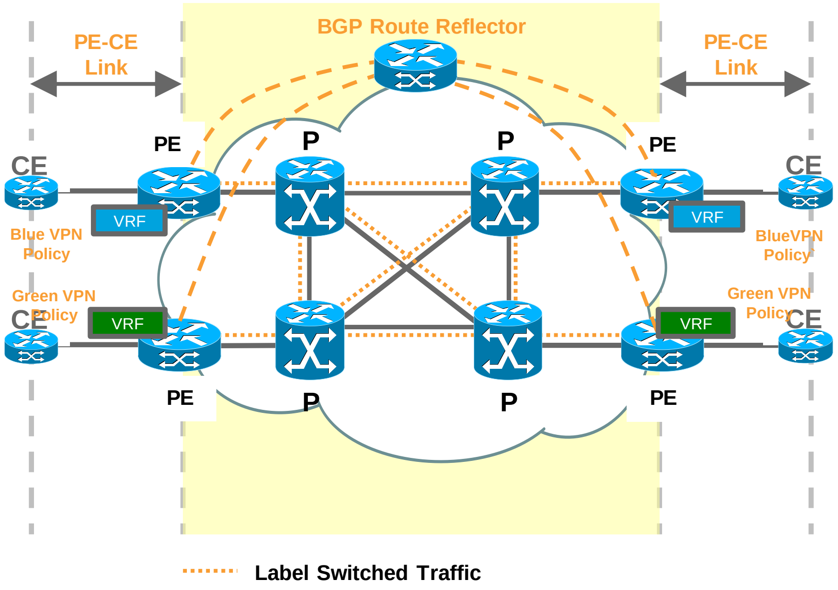
- Logical routing context within the same PE device
- Unique to a VPN
- Allows for customer overlapping IP addresses
- Deployment use cases
  - Business VPN services
  - Network segmentation
  - Data Centre access



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

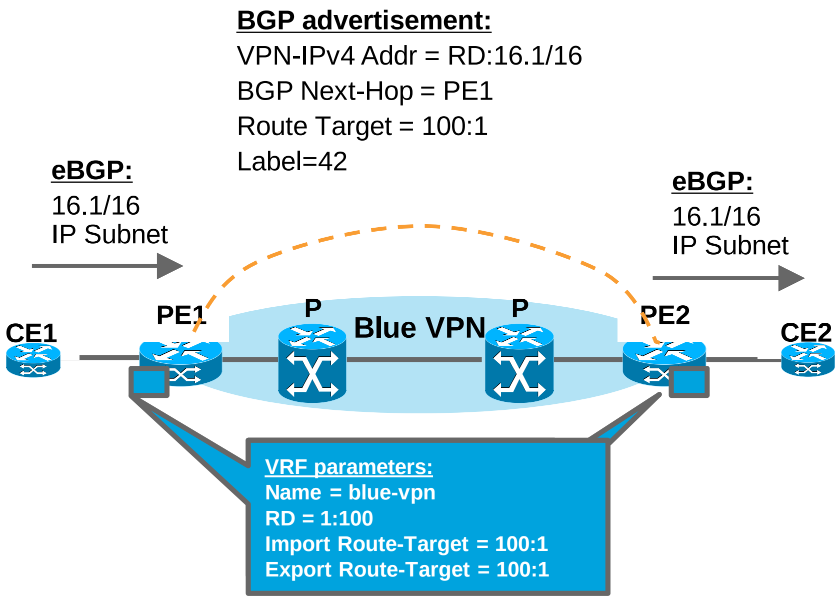
Selective distribute VPN routes:

- **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

Exchange of VPN Policies among PE Routers

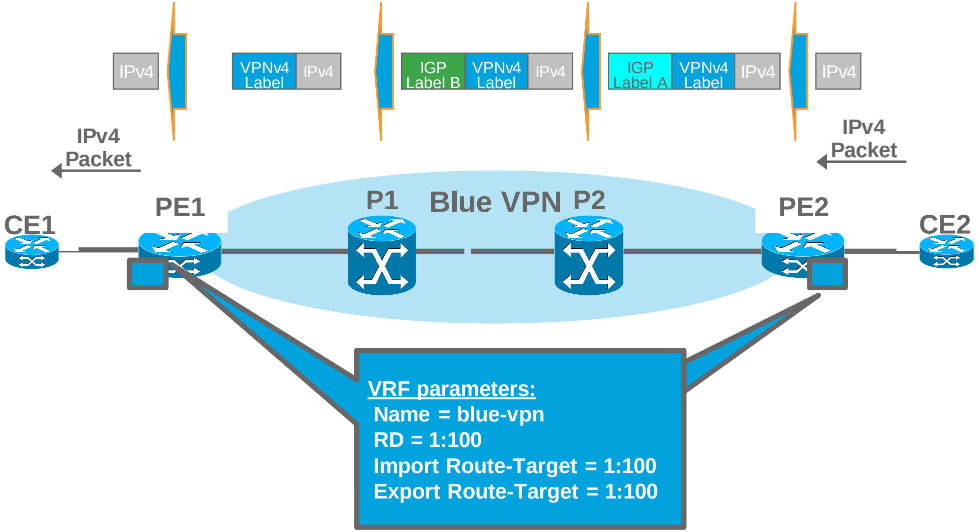
1. CE1 redistributes IPv4 route to PE1 via eBGP
2. PE1 allocates VPN label for prefix learnt from CE1, to create unique VPNv4 route
3. PE1 redistributes VPNv4 route into MP-iBGP, it sets itself as a next-hop and relays VPN site-routes to PE2
4. PE2 receives VPNv4 route and, via processing in local VRF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



VPN Forwarding Plane Processing

Forwarding of Layer-3 MPLS VPN Packets

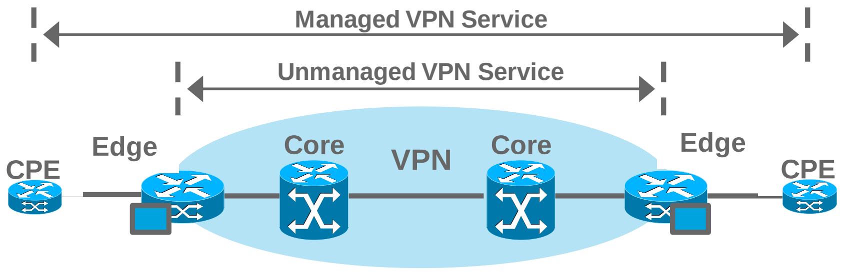
1. CE2 forwards IPv4 packet to PE2
2. PE2 imposes pre-allocated VPN label to IPv4 packet, received from CE2
   - Learned via MP-IBGP
3. PE2 also imposes outer IGP label 'A' (learned via LDP) and forwards labeled packet to P2
4. P2 router swaps outer IGP label and forwards labelled packet to P1. A>B
5. P1 router strips outer IGP label 'B' (PHP) and forwards packet to PE1
6. Router PE1 strips VPN label 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

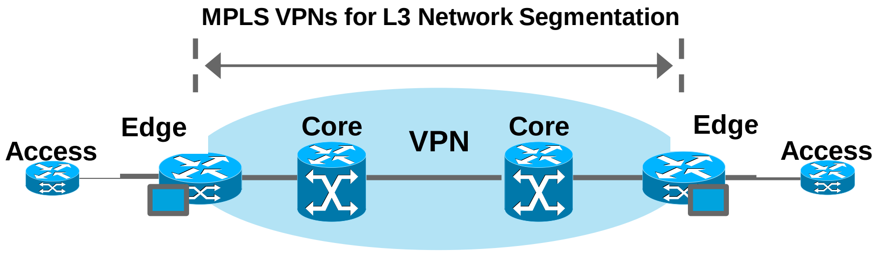


Network Segment	CPE	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	ASR9K ASR1K ISR	ASR9K ASR1K C6800	CRS ASR9K C6800

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

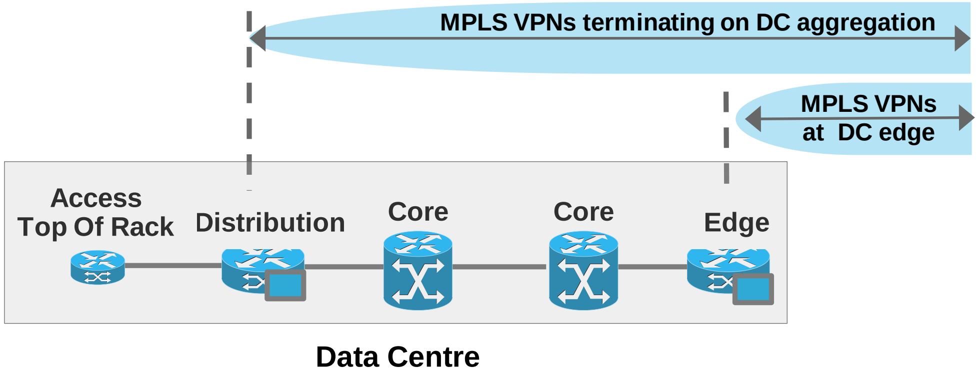


Network Segment	Access	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	ASR1K ISR	C6800 ASR1K ASR9K	CRS ASR9K C6800

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)



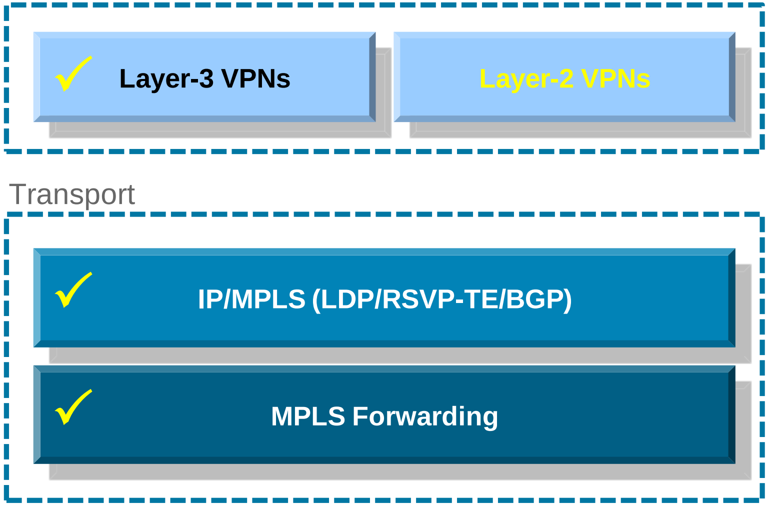
Network Segment	Distribution	Core	Edge
MPLS Node	CE or PE	P or CE	PE
Typical Platforms	N7K 6800	N7K 6800	ASR9K 6800

MPLS Layer-2 Virtual Private 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)

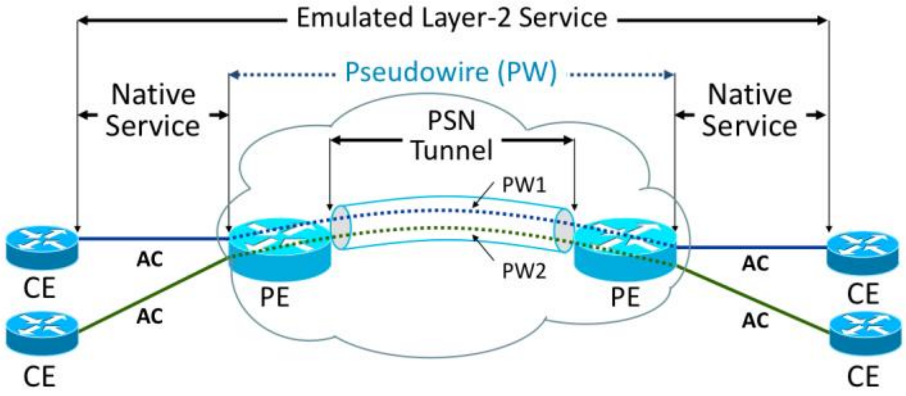
- **CE connected to PE via Ethernet connection (VLAN)**
- **CEs peer with each other via fully/partial mesh Layer-2 VPN connection**
- **CE-CE routing; no MPLS network involvement**

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

Virtual Private Wire Services (VPWS)

Overview of Pseudowire (PW) Architecture

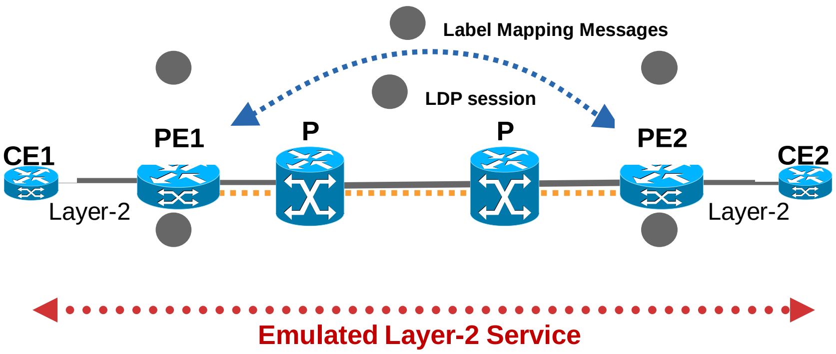
- Based on IETF's Pseudo-Wire (PW) Reference Model
- Enables transport of any Layer-2 traffic over MPLS
- Includes additional VC label encapsulation and translation of L2 frames
  - Ethernet, ATM, FR, or PPP
- PE-CE link is referred to as Attachment Circuit (AC)
- Support for L2 interworking
- PWs are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



VPWS Control Plane Processing

Signalling of a new Pseudowire

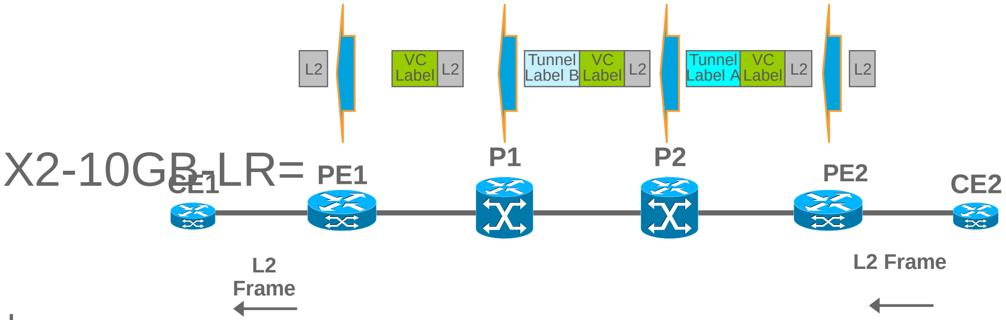
1. New Virtual Circuit (VC) cross-connect, connects customer-L2-interface (AC) to a new PW, via VC ID and remote PE ID
2. New targeted LDP session between PE1 and PE2 is established, in case one does not already exist
3. PE binds VC label with customer layer-2 interface and sends label-mapping to remote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



VPWS Forwarding Plane Processing

Forwarding of Layer-2 traffic over Pseudowire

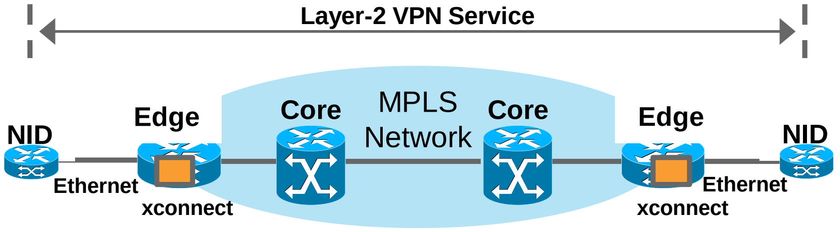
1. CE2 forwards L2 frame to PE2
2. PE2 pushes VC (inner) label to L2 frame received from CE2
3. PE2 pushes outer (Tunnel) label and forwards frame to P2
4. P2 and P1 forward frame using outer (tunnel) label (swap)
5. Router PE1 pops Tunnel label, and based on VC label, L2 frame is forwarded to customer interface to CE1, after VC label is removed



Cisco live!

Service Provider Deployment Scenario
PWs for offering Layer-2 Business VPN Services (VPWS)

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



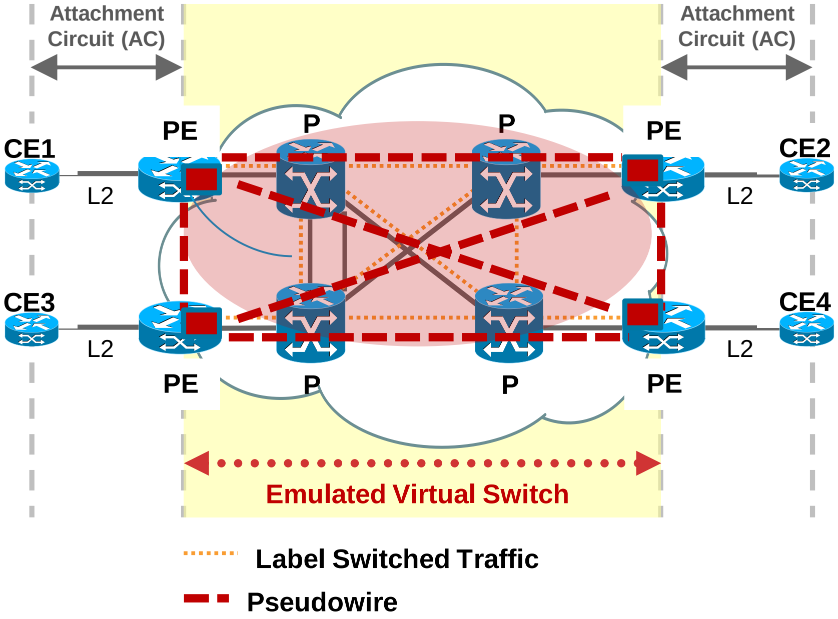
Network Segment	NID *	Edge	Core
MPLS Node	CE	U-PE	P
Typical Platforms	ASR901	ME3800X ASR903 ASR9K	CRS ASR9K

* NID : Network Interface Device

Virtual Private LAN Service

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 Service (VPLS)

Technology Components

- VPN policies
  - Virtual Switching Instance (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

VPLS Forwarding Plane Processing

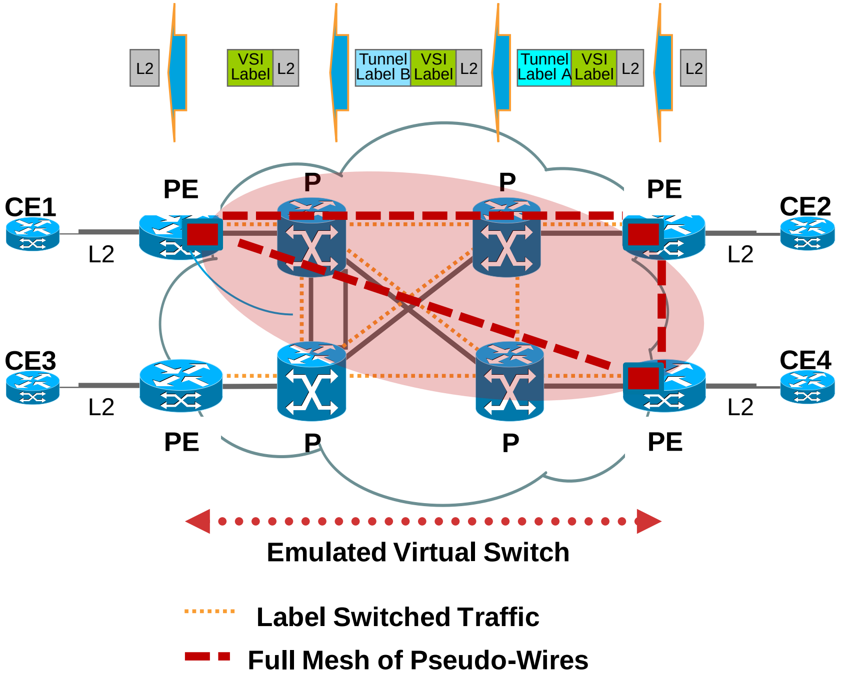
Forwarding of Layer-2 Traffic over VPLS Network

MAC learning:

- For new L2 frames
- VSI forwarding table updated
- Frames flooded to all PEs over PWs

Layer-2 Frame Forwarding:

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

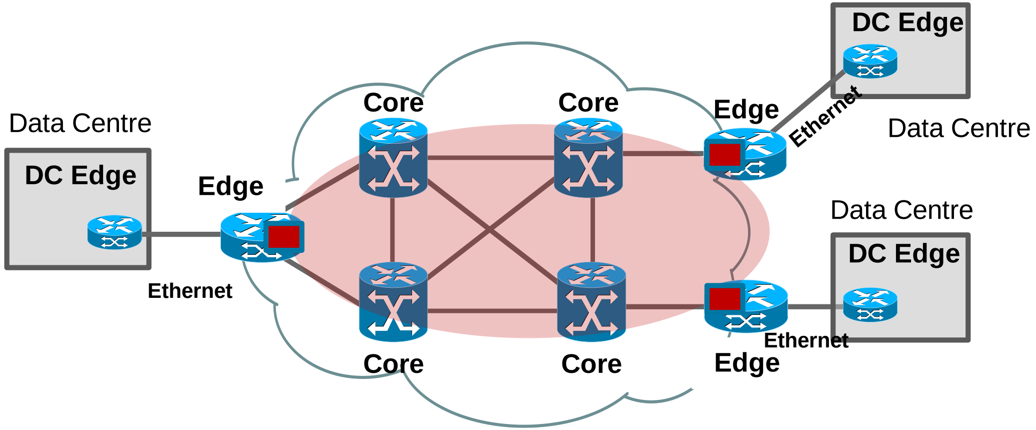


Cisco live!

Data Centre Deployment Scenario

PWs for offering Layer-2 Business VPN Services (VPWS)

- **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 6800	CRS ASR9K	ASR9K 6800

Summary Layer 2 VPN

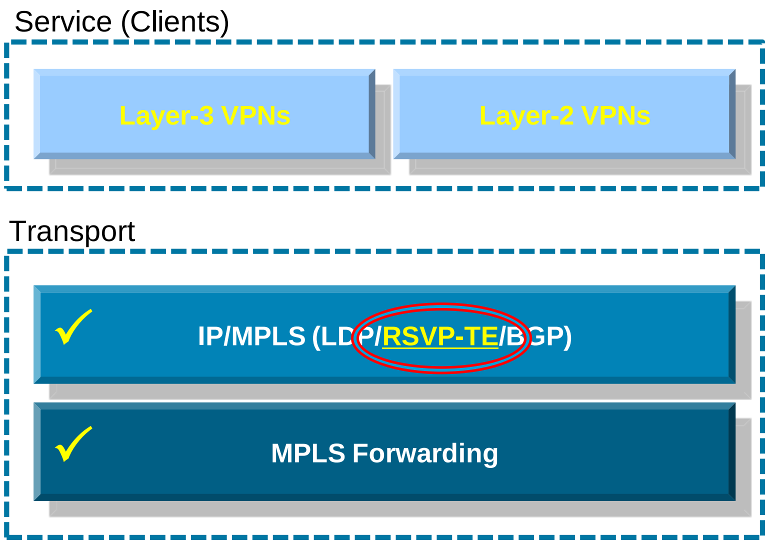
Technology Components

- 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 for 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

MPLS Traffic Engineering

MPLS Traffic Engineering
Topics

- What is MPLS TE
- The problem MPLS TE solves
- MPLS TE Signalling and Path Computation
- MPLS-TE Fast Re-Route (FRR)



Why MPLS Traffic Engineering?

Drivers for MPLS Traffic Management

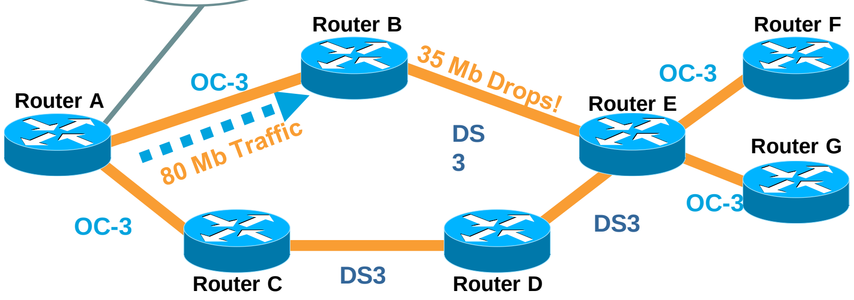
- **Need for better utilisation of available network bandwidth**
  - Optimise traffic distribution throughout network
  - Network capacity management
- **Protection against link and node failures**
  - Fast re-routing around failures to minimise (service) traffic loss
  - Optimise aggregate availability 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 Uitilisation 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



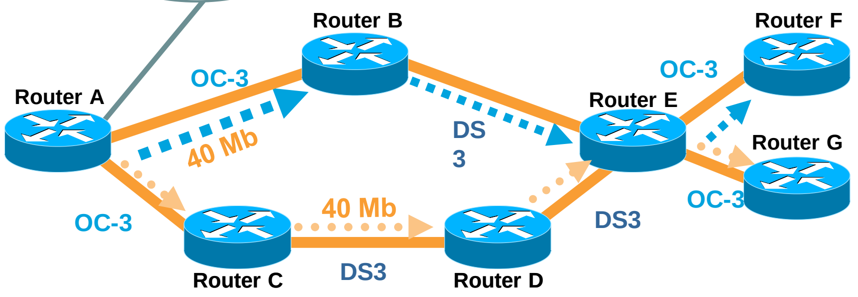
Cisco live!

How MPLS TE Solves the Problem

Optimised Path Computation via Additional Cost Metrics

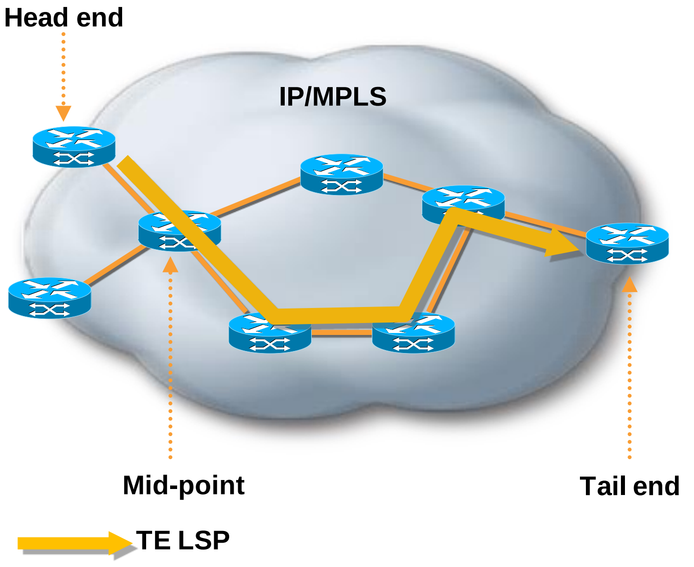
- Router A sees all links
- Router A computes paths on properties other than just shortest cost
  - Creation of 2 tunnels
- No link oversubscribed

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



MPLS Traffic Engineering
Technology Building Blocks

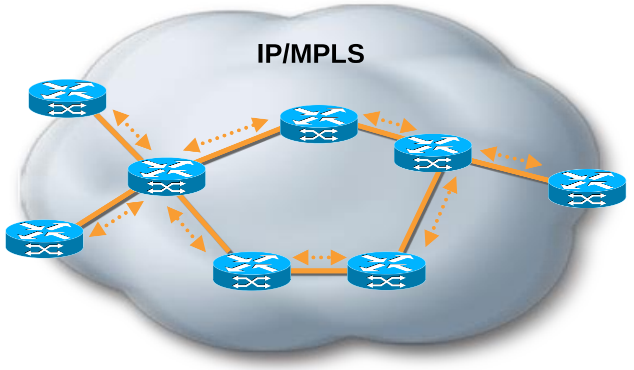
- **Link information Distribution***
  - ISIS-TE
  - OSPF-TE
- **Path Calculation (CSPF)***
  - At head-end node
- **Path Setup (RSVP-TE)**
- **Unidirectional forwarding traffic down Tunnel**
  - Auto-route
  - Static
  - PBR
  - CBTS / PBTS
  - Forwarding Adjacency
  - Tunnel select

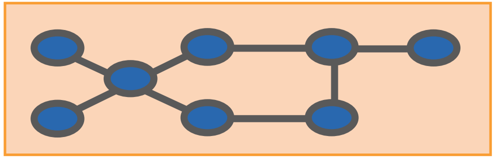


Distribution of Link Information

Additional Metrics for Path Computation

- **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**



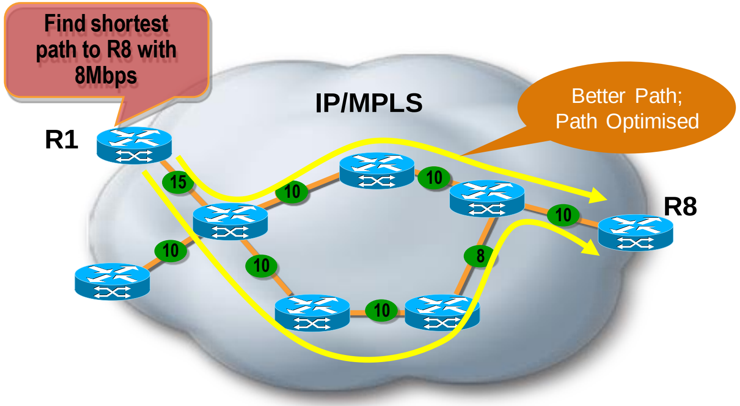


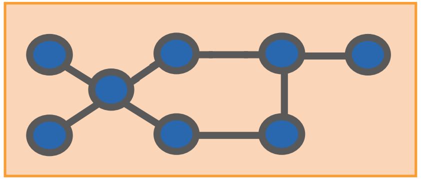
TE Topology database

Path Calculation

Calculation of Optimal Network Path, Based on Multiple Metrics

- 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
- Paths are optimised regularly (configurable)
- If better path available, traffic switched to new path
- Not required if using offline path computation





TE Topology database

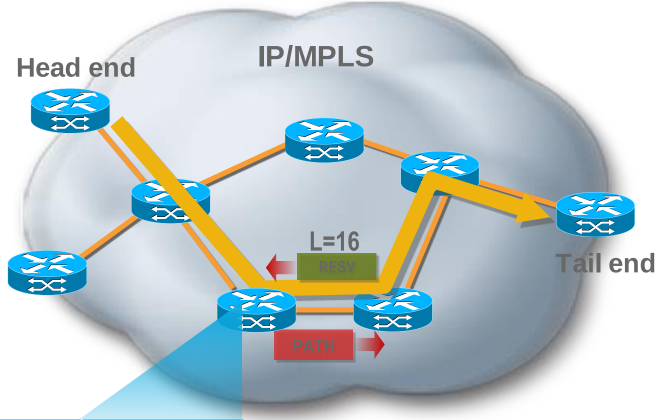
Link with insufficient bandwidth

Link with sufficient bandwidth

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



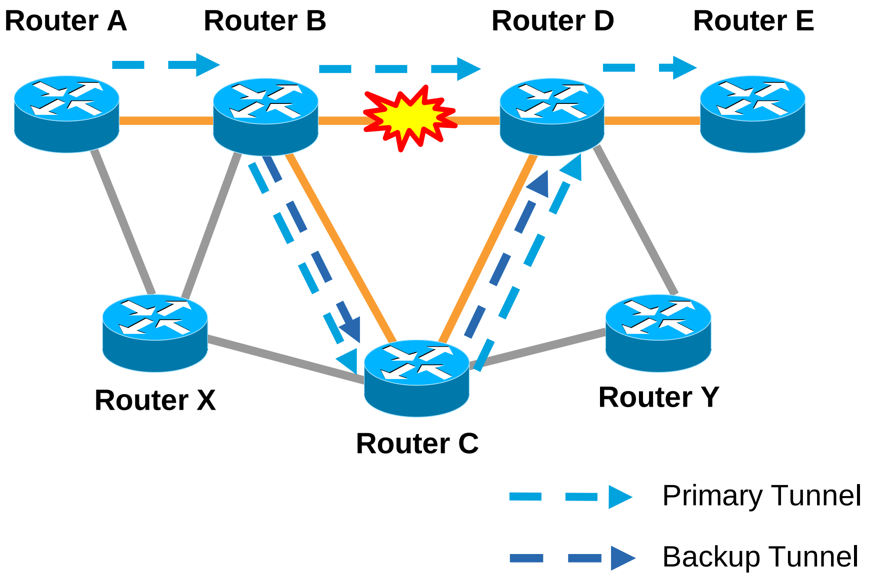
Input Label	Out Label, Interface
17	16, 0

TE LSP

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



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

Summary MPLS-TE

Technology Components

- MPLS-TE is signaled via RSVP
- Co-exists with basic MPLS (LDP)
- Uses IGP (OSPF/IS-IS) to build topology database
- Provides additional control over traffic path (constrained based forwarding – CSPF)
- Provides for Dynamic, Explicit or Loose path computation
- Provides Fast Re-Route capabilities (~<50ms)

Summary

Session 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

Cisco Live Sessions

Recommended

- **Segment Routing and SDN**
  - BRKRST-3370 – Advances In Routing
- **IPv6 Deployment**
  - BRKSPG-3300 – Service Provider IPv6 Deployment
- **Cloud Enablement Architecture**
  - BRKSPG-3864 - Cloud Enablement Architecture and NFV Services Delivery

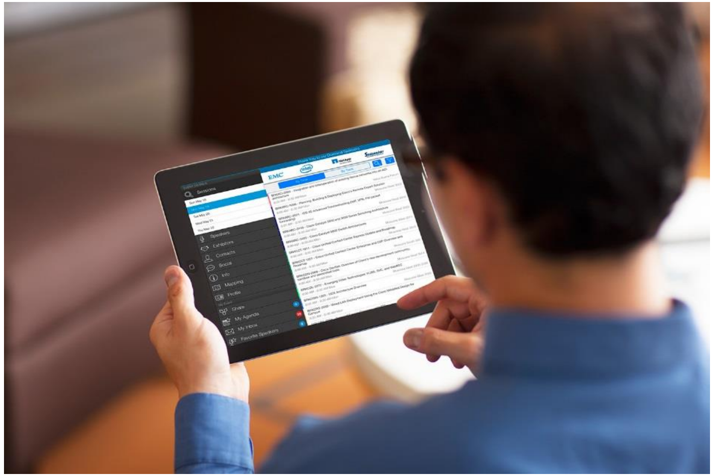
Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a **Cisco 2016 T-Shirt** by completing the 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 http://showcase.genie-connect.com/ciscolivemelbourne2016/
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected Friday 11 March at Registration



Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com

CiscoLive!

Thank you

cisco

References

Technology References

Acronyms Used in MPLS Reference Architecture

For your reference only

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

Technology References

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.
PLR	Point of Local Repair
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

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

Label Distribution Protocol

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

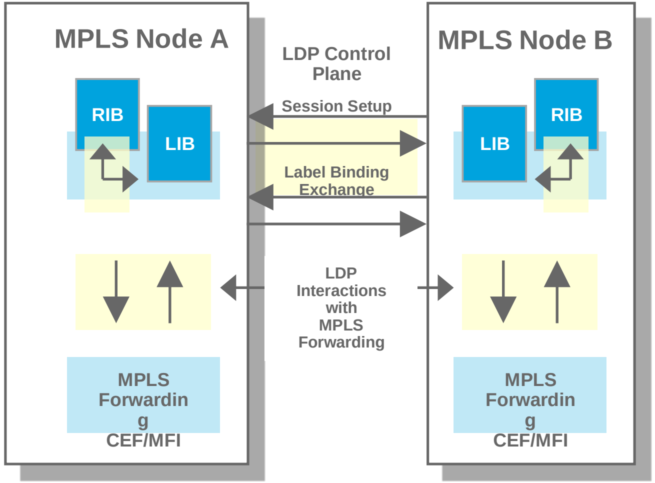
Some More Details

- 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

- 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

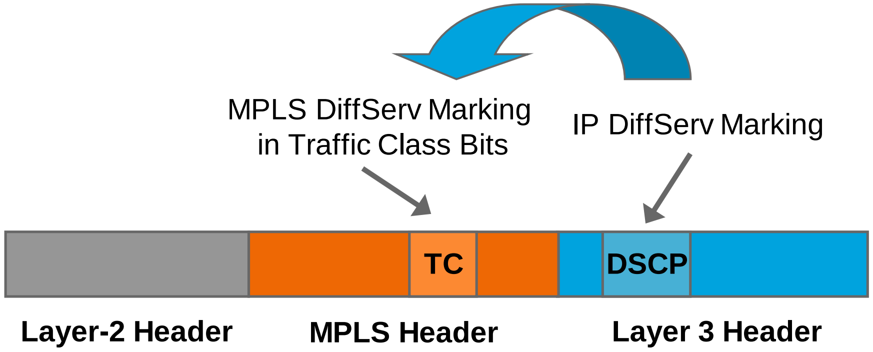
The Need for Differentiated Services

- 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 QoS

QoS Marking in MPLS Labels

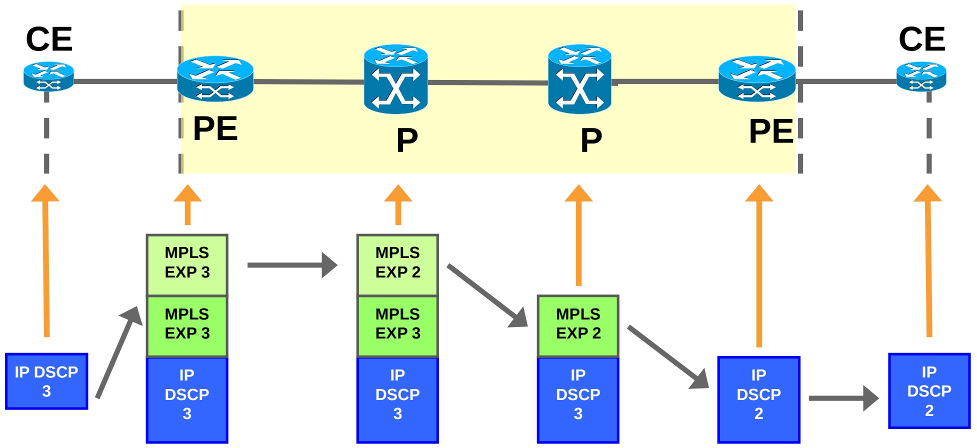
- MPLS label contains 3 TC bits
- Used for packet classification and prioritisation
  - Similar to Type of Service (ToS) field in IP packet (DSCP values)
- DSCP values of IP packet mapped into TC bits of MPLS label
  - At ingress PE router
- Most providers have defined 3–5 service classes (TC values)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



MPLS QoS Uniform Mode

QoS Field Assignments in MPLS Network

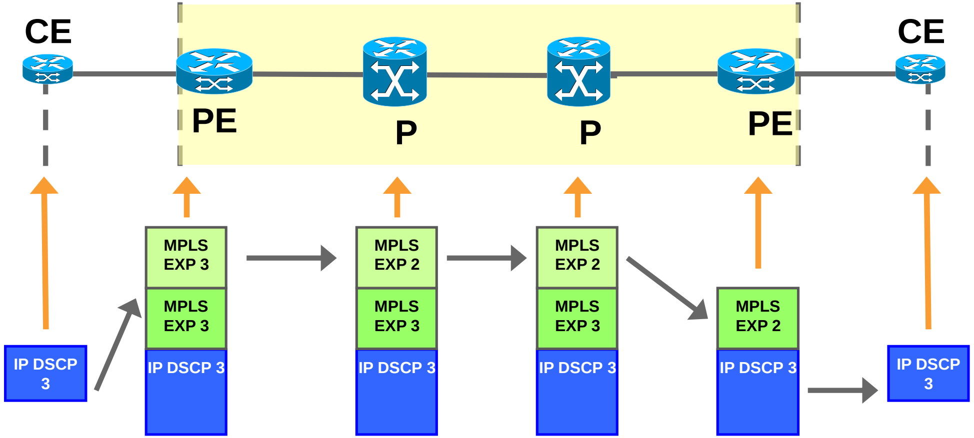
- LDP startup
  - Local labels assigned to RIB prefixes and stored in LIB
  - Peer discovery and session setup
  - Exchange of MPLS label bindings
- Programming of MPLS forwarding
  - Based on LIB info
  - CEF/MFI updates



MPLS QoS Pipe Mode

QoS Field Assignments in MPLS Network

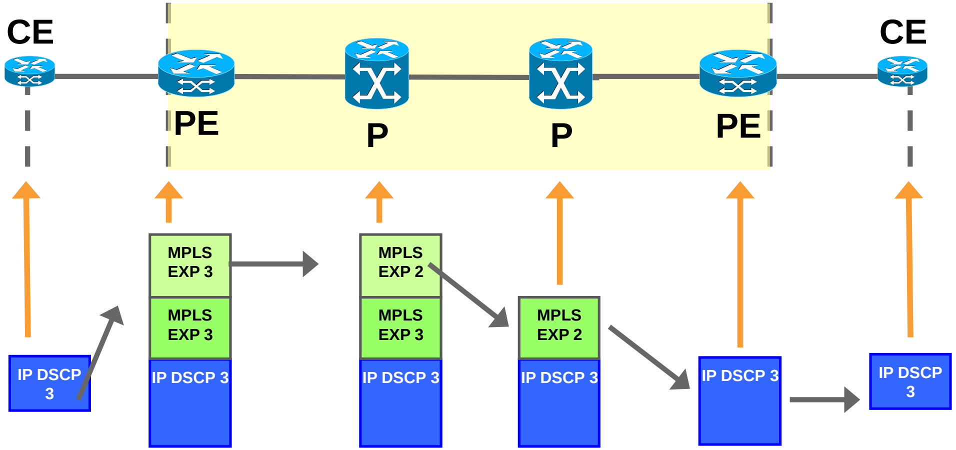
- End-to-end behaviour:
  - Original IP DSCP is preserved
- At ingress PE:
  - EXP value set based on ingress classification
- EXP changed in the MPLS core
  - Based on traffic load and congestion
- At egress PE:
  - EXP value not copied back into IP DSCP value



MPLS QoS Short Pipe Mode

QoS Field Assignments in MPLS Network

- 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

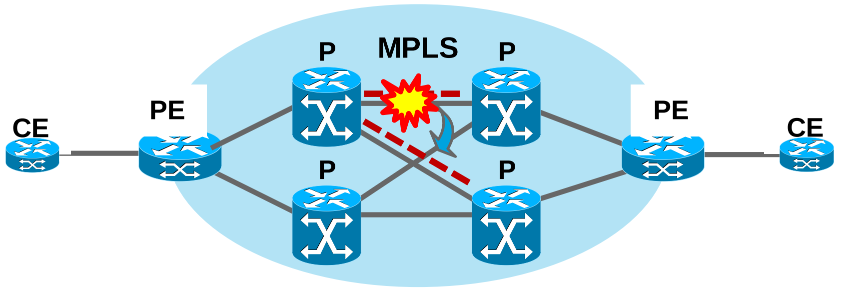


Cisco live!

Service Provider Deployment Scenario

Implementing Sub-Second Failure Detection 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

Summary Layer 3 VPN

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

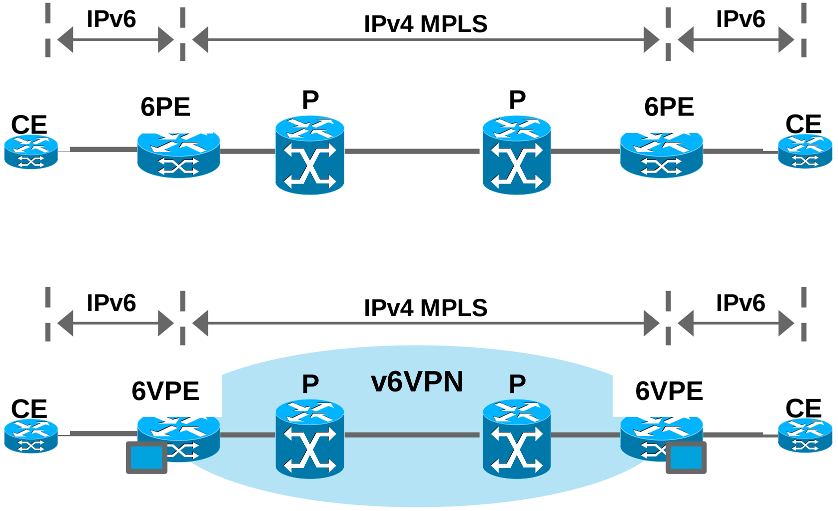
Advanced Topics

For your reference only

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



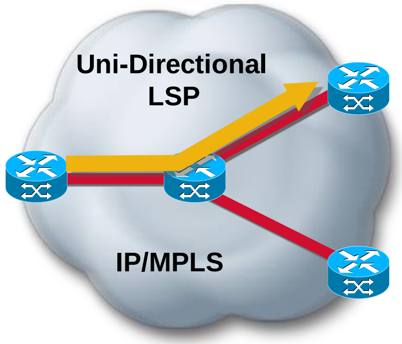
Label Switched Multicast (LSM)

For your reference only

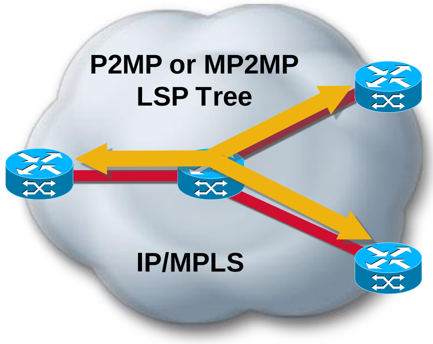
Point-to-Multipoint MPLS Signalling and Connectivity

- 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)



Cisco live!

MPLS SNMP MIBs

SNMP Management Access to MPLS Resources

- MPLS-LSR-STD-MIB
  - Provides LSP end-point and LSP cross-connect information
- 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 Troubleshooting 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!