Possibilities

#CiscoLive

Introduction to MPLS

DGTL-BRKMPL-1100

Travis Jones
Systems Architect

CCIE #4603 – DC, R&S, SP, Security, & Voice

CCDE 2013::60

cisco Live!

June 2-3, 2020 | ciscolive.com/us

cisco

Agenda

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

Session Goals

Objectives

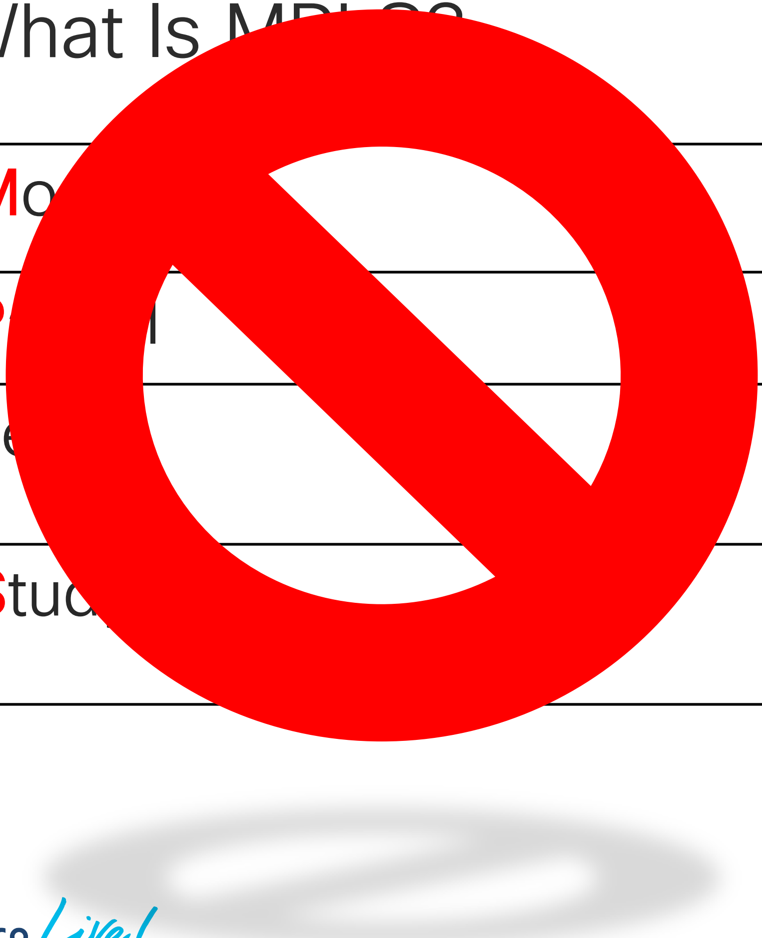
- Definition and history of MPLS
- Learn about MPLS customer and market segments
- Understand the problems MPLS is addressing
- Understand the major MPLS technology components
- Understand typical MPLS applications
- Understand benefits of deploying MPLS
- Learn about MPLS futures; where MPLS is going

Introduction

What Is MPLS?

Most	
Painful	
Learn	
Study	

What Is



Mo	
P l	
Le	
Stu	

What Is MPLS?

Definition

Multi **P**rotocol	Multi-Protocol: The ability to carry any payload Have: IPv4, IPv6, Ethernet, ATM, FR
Label	Uses Labels to tell a node what to do with a packet; separates forwarding (hop by hop behavior) from routing (control plane)
Switching	Routing based on IPv4 or IPv6 lookup. Everything else is Switching.

What is MPLS?

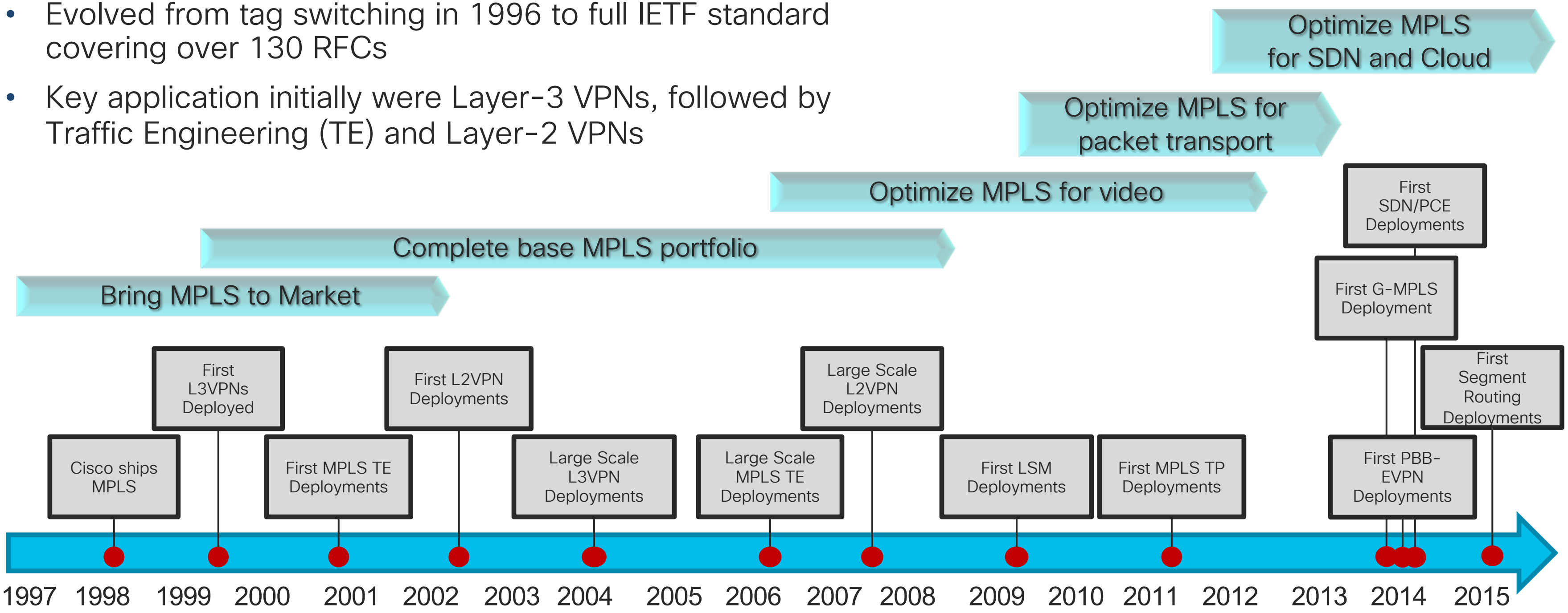
Brief Summary

- 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
- MPLS control/signaling plane
  - Use of existing IP control protocols extensions + new protocols to exchange label information

Evolution of MPLS

Technology Evolution and Main Growth Areas

- Evolved from tag switching in 1996 to full IETF standard covering over 130 RFCs
- Key application initially were Layer-3 VPNs, followed by Traffic Engineering (TE) and Layer-2 VPNs

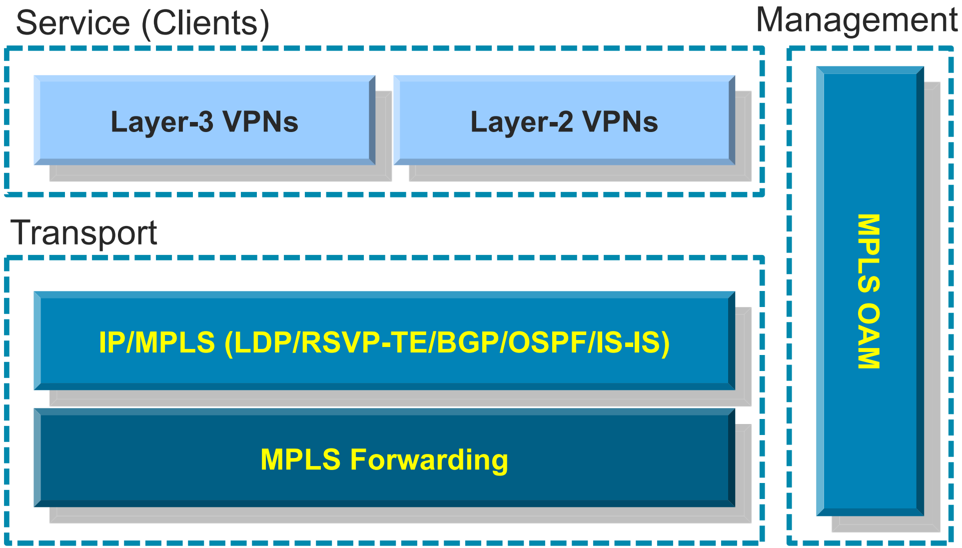


MPLS Technology Basics

Topics

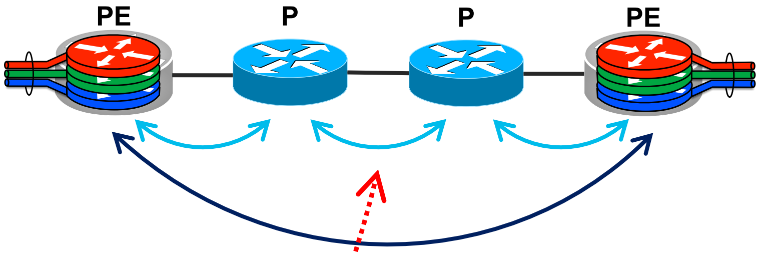
Basics of MPLS Signaling and Forwarding

- MPLS Reference Architecture
- MPLS Labels
- MPLS signaling and forwarding operations
- MPLS Traffic Engineering
- MPLS QoS
- MPLS OAM



MPLS Reference Architecture

Node Types & Protocols



- P (Provider) router = Label Switching Router (LSR)
  - Runs an IGP and LDP
- PE (Provider Edge) router = edge router (LER)
  - Imposes and removes MPLS labels
  - Runs an IGP, LDP and MP-BGP
- CE (Customer Edge) router
  - Not required
- Label Distribution Protocol
  - UDP/TCP port 646 (multicast/unicast)
  - IGP to label binding
- Multi-Protocol BGP
  - Address-family support (IPv4, IPv6, multicast, EVPN etc...)
  - Used for VRF / VPN route exchange

MPLS Labels

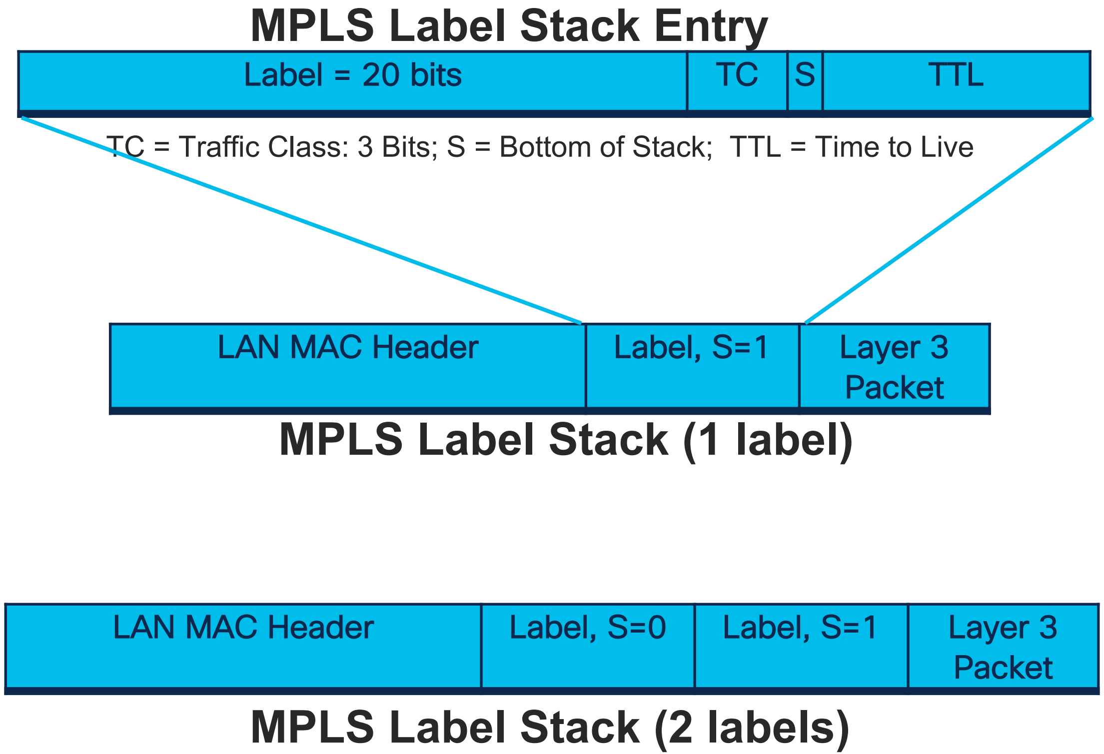
MPLS Label Characteristics

- MPLS Label has local significance
- One router assigns the MPLS label independently
- There is no global assignment for the whole network
  - No global authority
- 20 bits for the label gives label range of 0-1048575
  - Default label range might be lower
  - Label range is limited on some platforms
- Normal MPLS labels are: 16-1048575
- Reserved label range is: 0-15

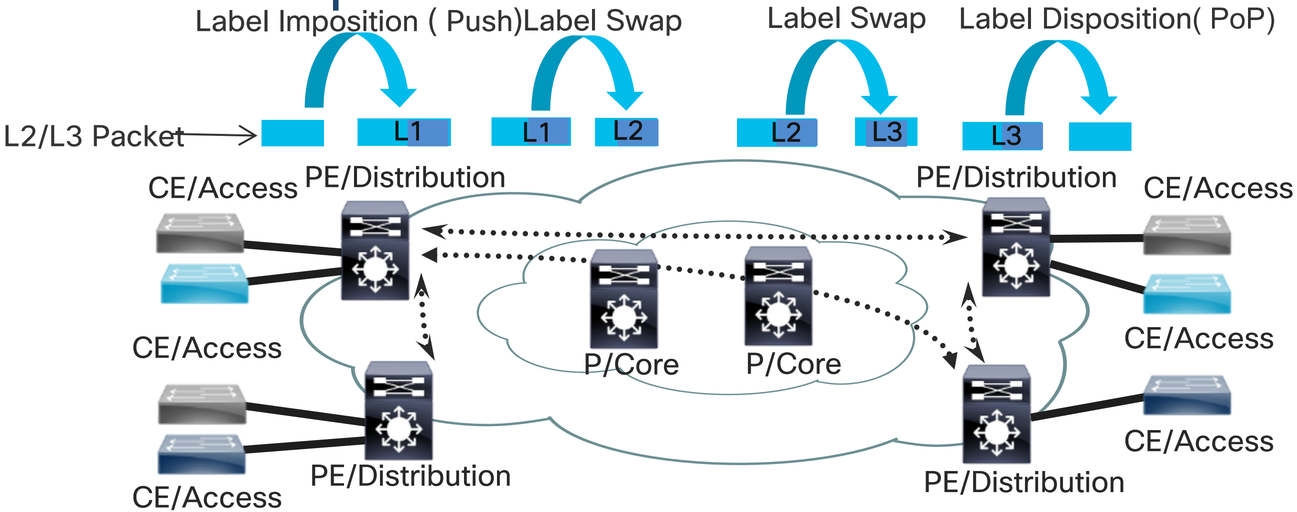
MPLS Labels

Label Definition and Encapsulation

- Labels used for making forwarding decision
- Multiple labels can be used for MPLS packet encapsulation
  - No limit on the number of labels in a stack
- Outer label always used for switching MPLS packets in network
- Inner labels usually used for services (e.g. L2/L3 VPN)



MPLS Label Operations



- Label imposition (Push)

  By ingress PE router; classify and label packets

- 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 signaling protocols
  - Either LDP* or RSVP
  - Leverages IP routing
  - Routing table (Routing Information Base – RIB)
- Exchange of labels
  - Label bindings
  - Downstream MPLS node advertises what label to use to send traffic to node
- MPLS forwarding
  - MPLS Forwarding table (Forwarding Information Base – 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	LDP, RSVP, BGP, OSPF, IS-IS
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 signaling assumed for next the examples

MPLS Path (LSP) Setup

Signaling Options

- LDP signaling
  - Leverages existing routing
- RSVP signaling
  - AKA MPLS RSVP / TE
  - Enables enhanced capabilities, such as Fast ReRoute (FRR)
- Can use both protocols simultaneously
  - They work differently, they solve different problems
  - Dual-protocol deployments are very common

	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
Signaling	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 Routing

IGP vs. BGP

- Exchange of IP routes for Loopback Reachability
  - OSPF, IS-IS, EIGRP, etc.
- iBGP neighbor peering over IGP transport
- Route towards BGP Next-Hop

Forwarding Table

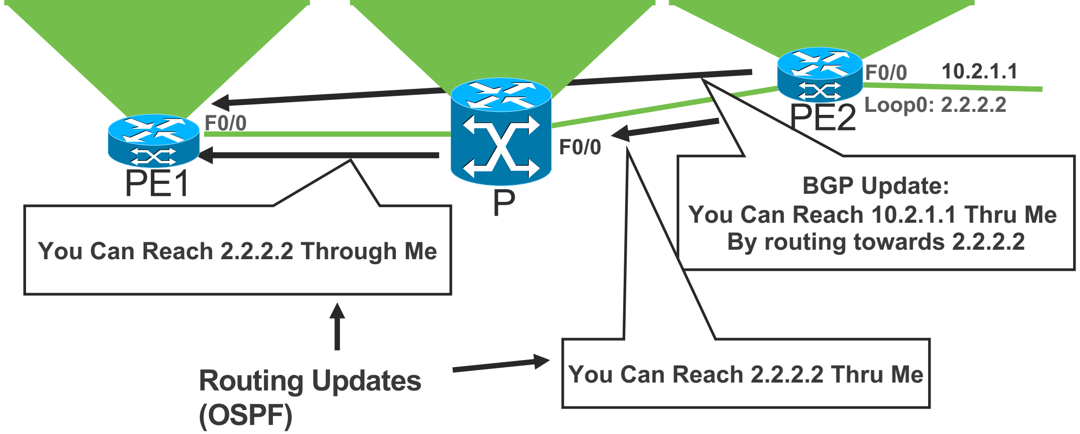
In Label	Address Prefix	Out I'face	Out Label
	10.2.2.2	F0/0	
	10.2.1.1	F0/0	
	...	...	

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
	10.2.2.2	F0/0	
	10.2.1.1	N/A	
	...	...	

Forwarding Table

In Label	Address Prefix	Out I'face	Out Label
	10.2.1.1	F0/0	
	...	...	



MPLS Label Switched Path (LSP) Setup with LDP

Assignment of Remote Labels

- Local label mappings are sent to connected nodes
- Receiving nodes update forwarding table
  - Out label
- LDP label advertisement happens in parallel (downstream unsolicited)

Forwarding Table (PE1)

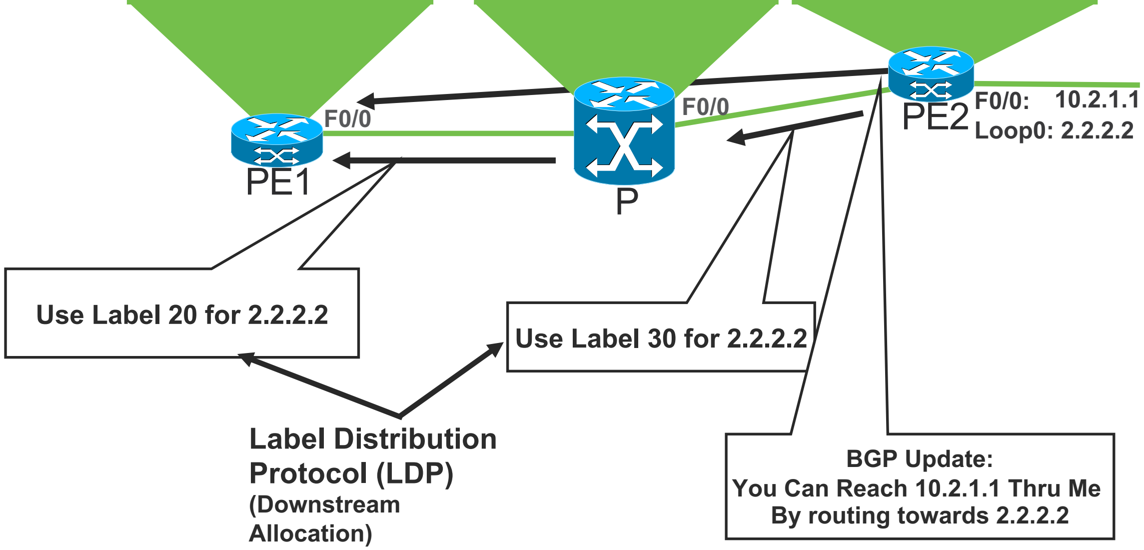
In Label	Address Prefix	Out I'face	Out Label
-	2.2.2.2	F0/0	20
-	...	...	...
...	...	...	...

Forwarding Table (P)

In Label	Address Prefix	Out I'face	Out Label
20	2.2.2.2	F0/0	30
...	...	...	...
...	...	...	...

Forwarding Table (PE2)

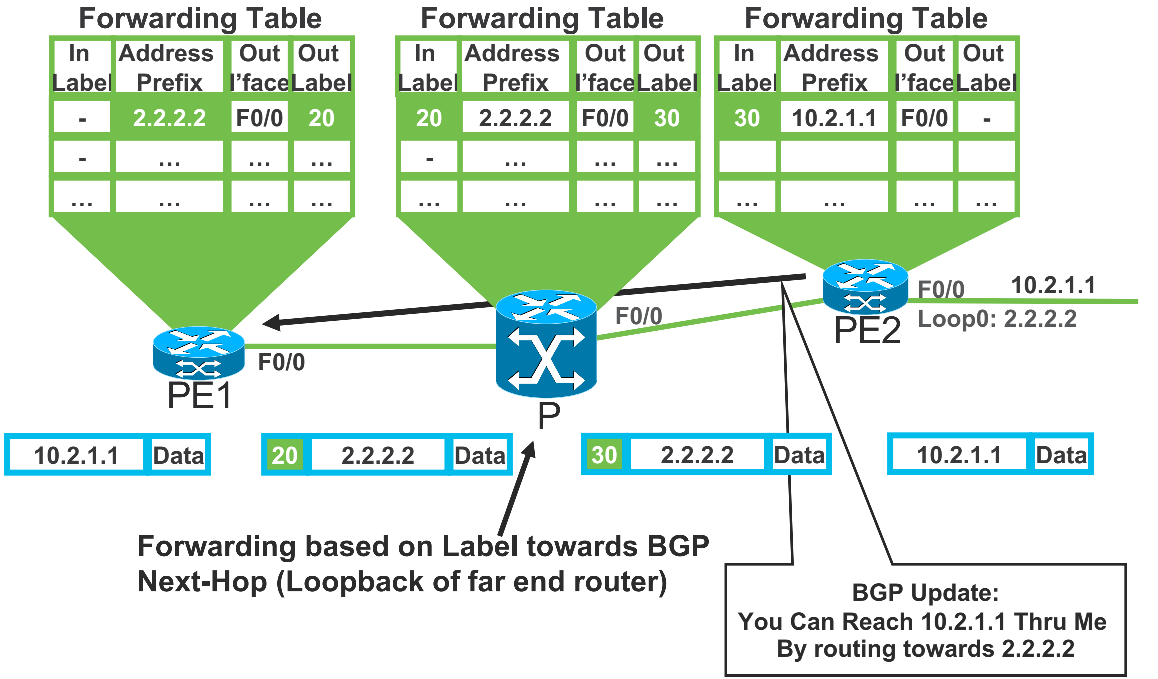
In Label	Address Prefix	Out I'face	Out Label
30	10.2.1.1	F0/0	-
...	...	...	...



MPLS Traffic Forwarding with LDP

Hop-by-hop Traffic Forwarding Using Labels

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



MPLS Traffic Forwarding with LDP

Quick recap

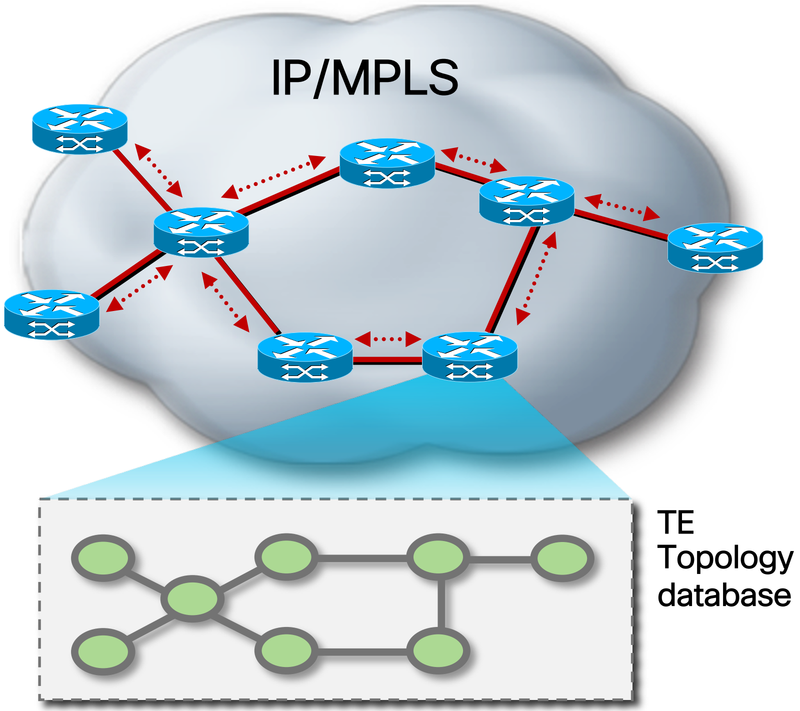
- Routing protocol distributes routes
- LDP distributes labels that map to routes
- Packets are forwarded using labels
- ...
- So what?
- ...
- MPLS's benefit shows up later, in two places:
  - Divergence from IP routed shortest path
  - Payload-independent tunneling

MPLS Path (RSVP) Setup

- MPLS-Traffic Engineering (TE) lets you deviate from the IGP shortest-cost path
- This gives you lots of flexibility around how you send traffic across your network
- Three steps:
  - Information distribution
  - Path calculation
  - LSP signaling

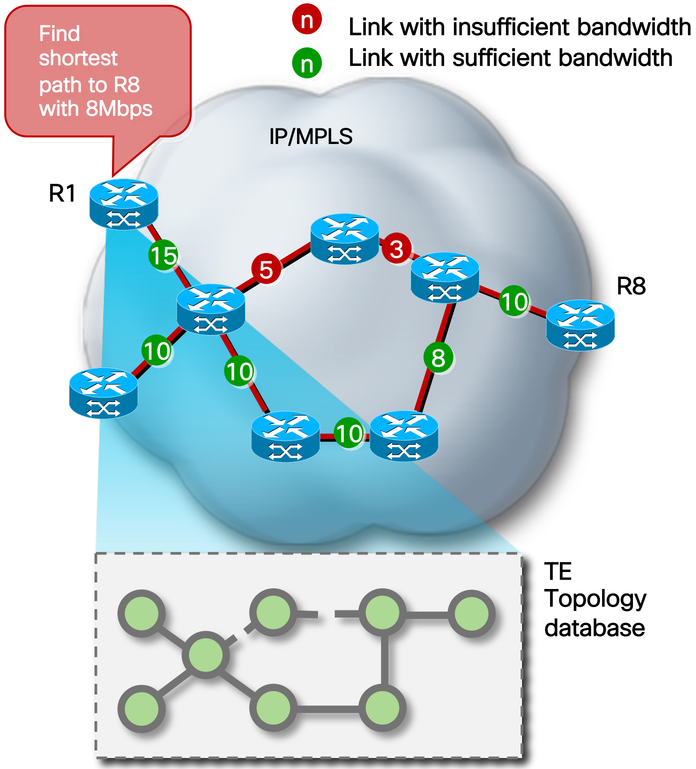
MPLS Path (RSVP) Setup

- Flood link characteristics in the IGP (ISIS or OSPF)
  - Reservable bandwidth
  - Link colors
  - Other properties



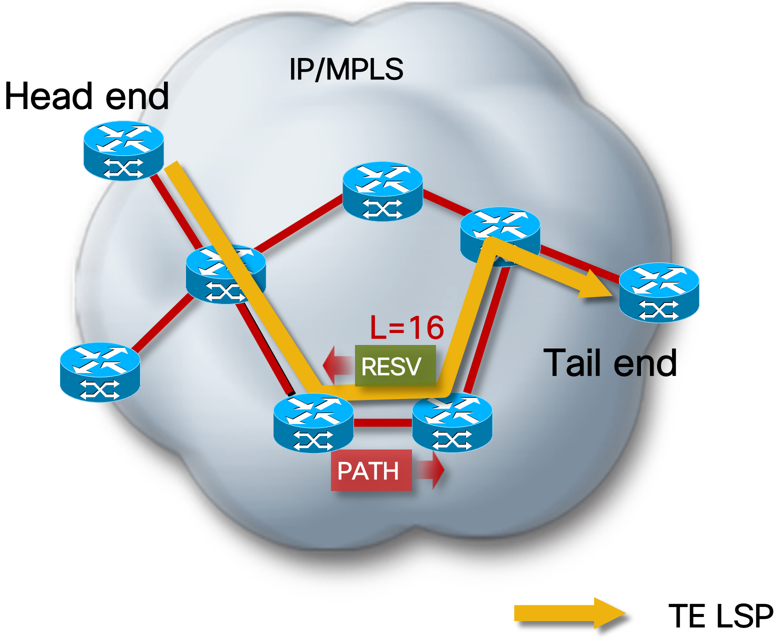
MPLS Path (RSVP) Setup

- IGP: Find shortest (lowest cost) path to all nodes
- TE: Per node, find the shortest (lowest cost) path which meets constraints



MPLS Path (RSVP) Setup

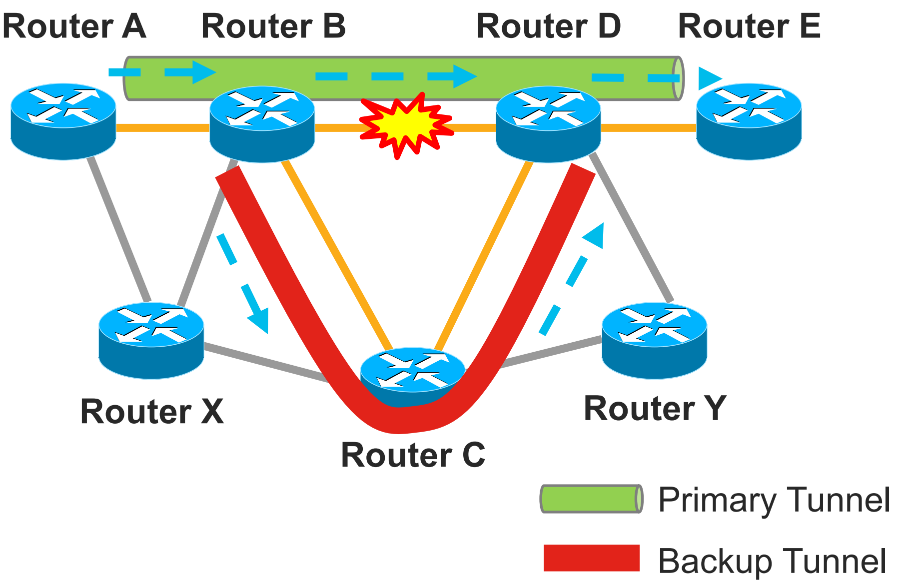
- Set up the calculated path using RSVP (Resource ReSerVation Protocol)
- Once labels are learned, they're programmed just like LDP labels
  - At the forwarding level, you can't tell whether your label came from RSVP or LDP
  - All the hard work is in the control plane
  - No per-packet forwarding hit for any of this



MPLS TE Fast ReRoute (FRR)

Implementing Network Failure Protection Using MPLS RSVP/TE

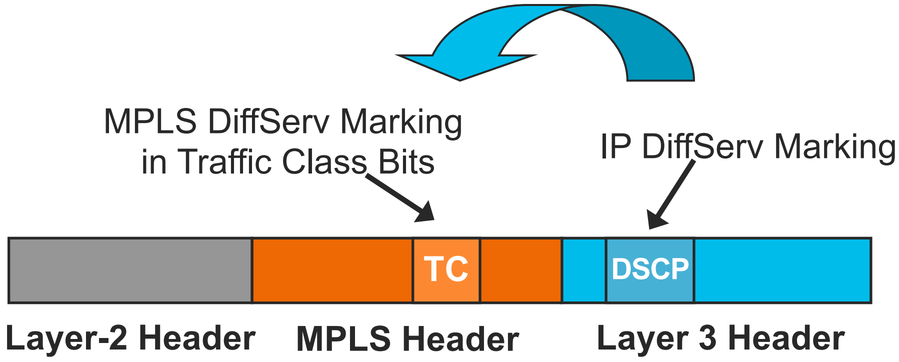
- Steady state
  - Primary tunnel:
    - A → B → D → E
  - Backup tunnel:
    - B → C → D (pre-provisioned)
- Failure of link between router B and D
- Traffic rerouted over backup tunnel
- Recovery time 50 ms
  - Actual Time Varies—Well Below 50 ms in Lab Tests



MPLS QoS

QoS Marking in MPLS Labels

- MPLS label has 3 Traffic Class (TC) bits
- Used for packet classification and prioritization
  - 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)



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 reachability 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

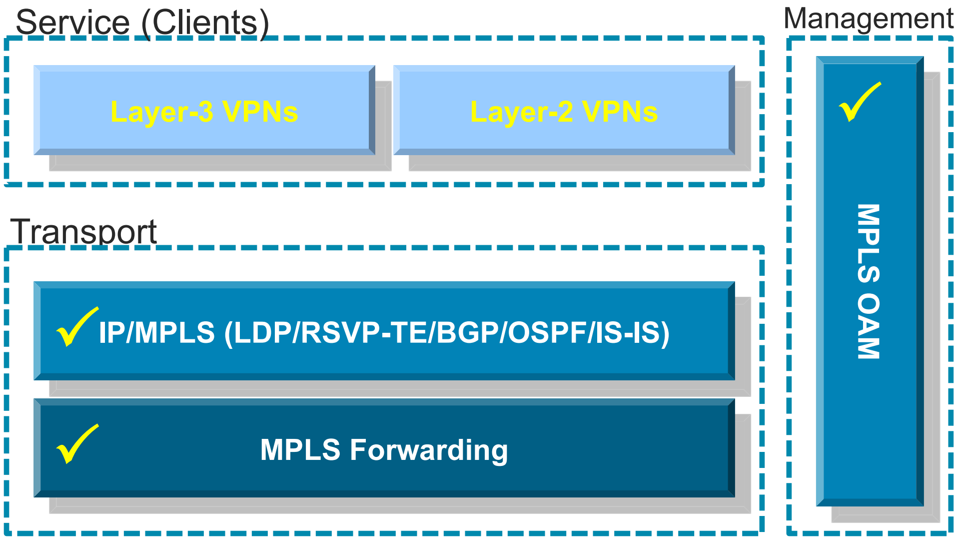
- MPLS networks consist of PE routers at in/egress and P routers in core
- Traffic is encapsulated with label(s) at ingress (PE router)
- Labels are removed at egress (PE router)
- MPLS forwarding operations include label imposition (PUSH), swapping, and disposition (POP)
- LDP and RSVP can be used for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

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?

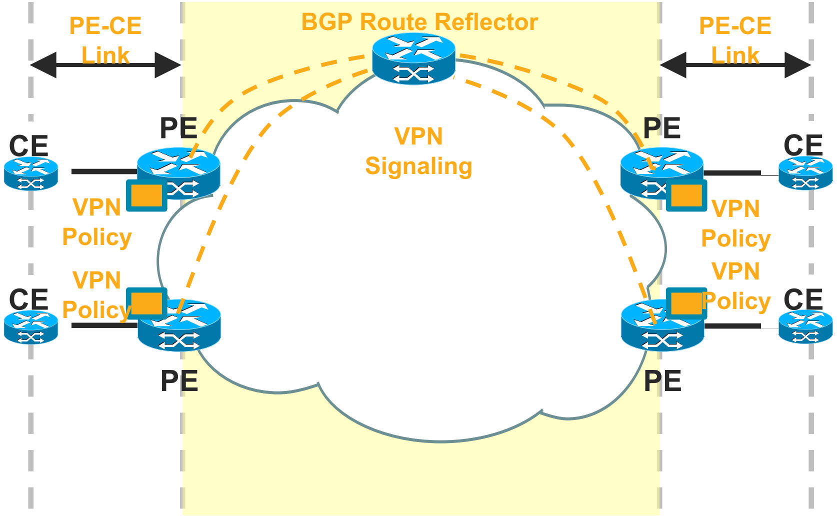
Definition

- Set of sites which communicate with each other 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 organizations
  - 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

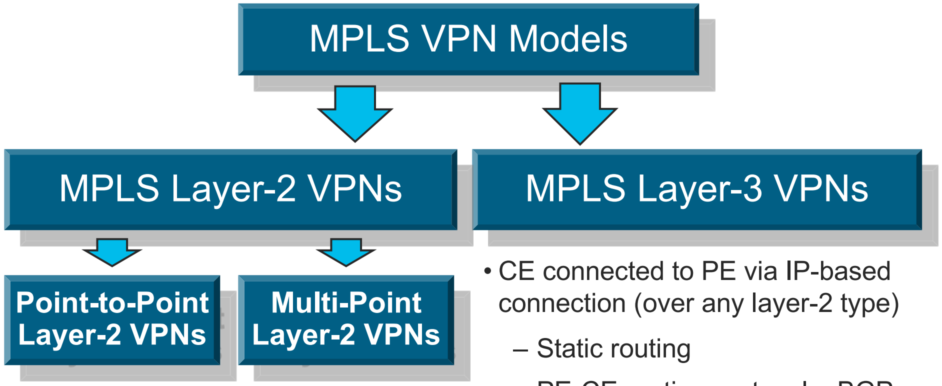
- VPN policies
  - Configured on PE routers (manual operation)
- VPN signaling
  - Between PEs
  - Exchange of VPN policies
- VPN traffic forwarding
  - Additional VPN-related MPLS label encapsulation
- PE-CE link
  - Connects customer network to MPLS network; either layer-2 or layer-3



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)
  - Peering relationship between CE's
  - SP not involved in routing



Point-to-Point Layer-2 VPNs
- CE connected to PE via L2 (Eth, FR, ATM, etc) connection
- CE-CE L2 p2p connectivity
- CE-CE routing; no SP involvement

Multi-Point Layer-2 VPNs
- CE connected to PE Ethernet connection
- CE-CE L2 (Eth) mp connectivity
- CE-CE routing; no SP involvement

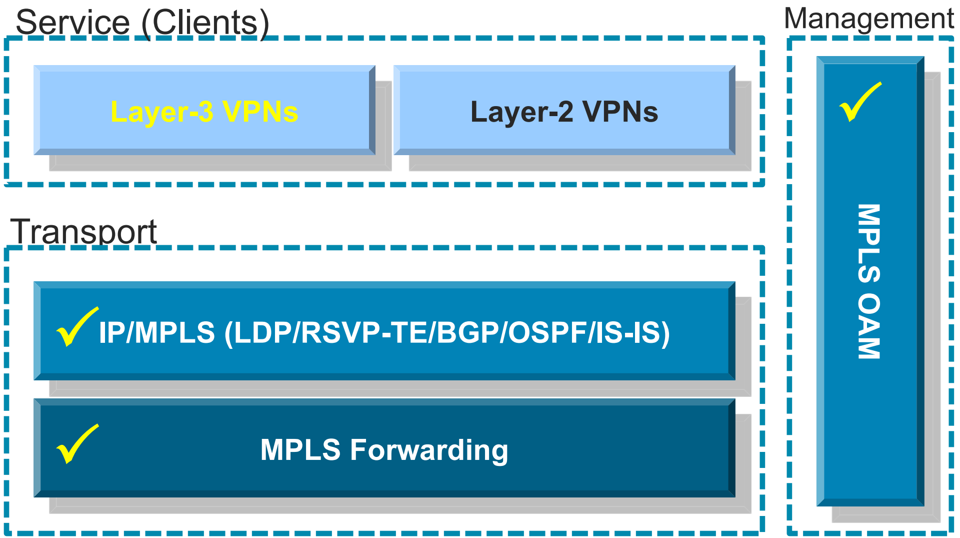
MPLS Layer-3 VPNs
- CE connected to PE via IP-based connection (over any layer-2 type)
  - – Static routing
  - – PE-CE routing protocol; eBGP, OSPF, IS-IS
- CE routing has peering relationship with PE router; PE routers are part of customer routing
- PE routers maintain customer-specific routing tables 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 Center access



MPLS Layer-3 VPN Overview

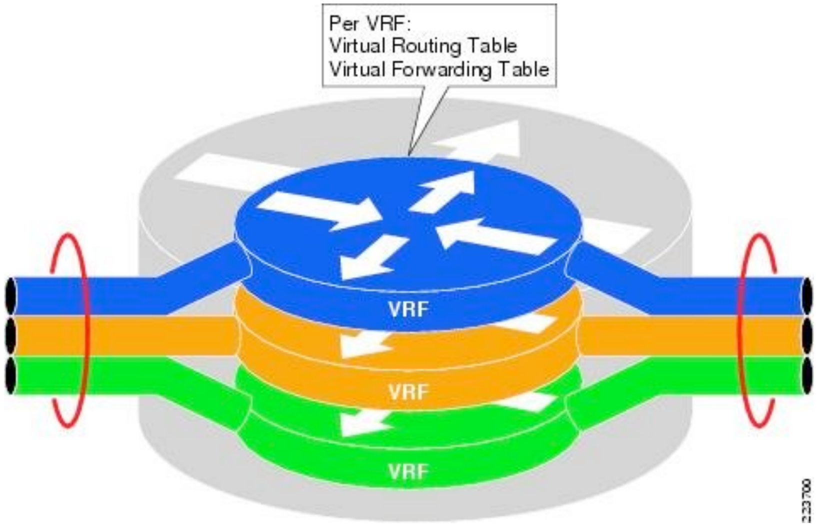
Technology Components

- VPN policies
  - Separation of customer routing via virtual VPN routing table (VRF)
  - In PE router, customer interfaces are connected to VRFs
- VPN signaling
  - Between PE routers: customer routes exchanged via BGP (MP-BGP)
- 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

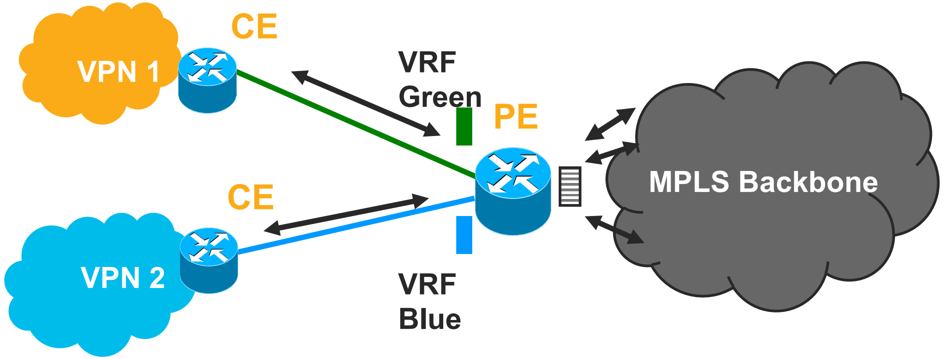
- Logical routing context within the same PE device
- Unique to a VPN
- Allows for customer overlapping IP addresses
- Deployment use cases
  - Business VPN services
  - Network segmentation
  - Data Center access



Virtual Routing and Forwarding Instance

Virtual Routing Table and Forwarding to Separate Customer Traffic

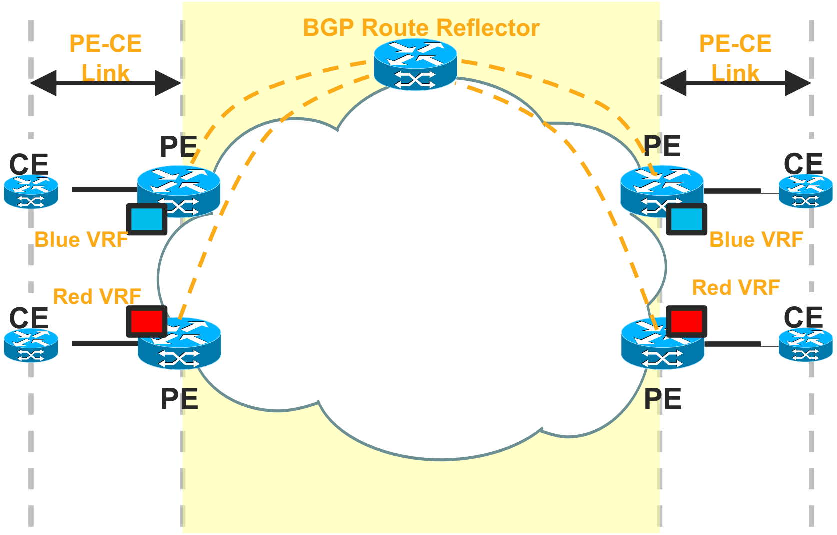
- Virtual routing and forwarding table
  - On PE router
  - Separate instance of routing (RIB) and forwarding table
- Typically, VRF created for each customer VPN
  - Separates customer traffic
- VRF associated with one or more customer interfaces
- VRF has its own routing instance for PE-CE configured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



VPN Route Distribution

Exchange of VPN Policies Among PE Routers

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



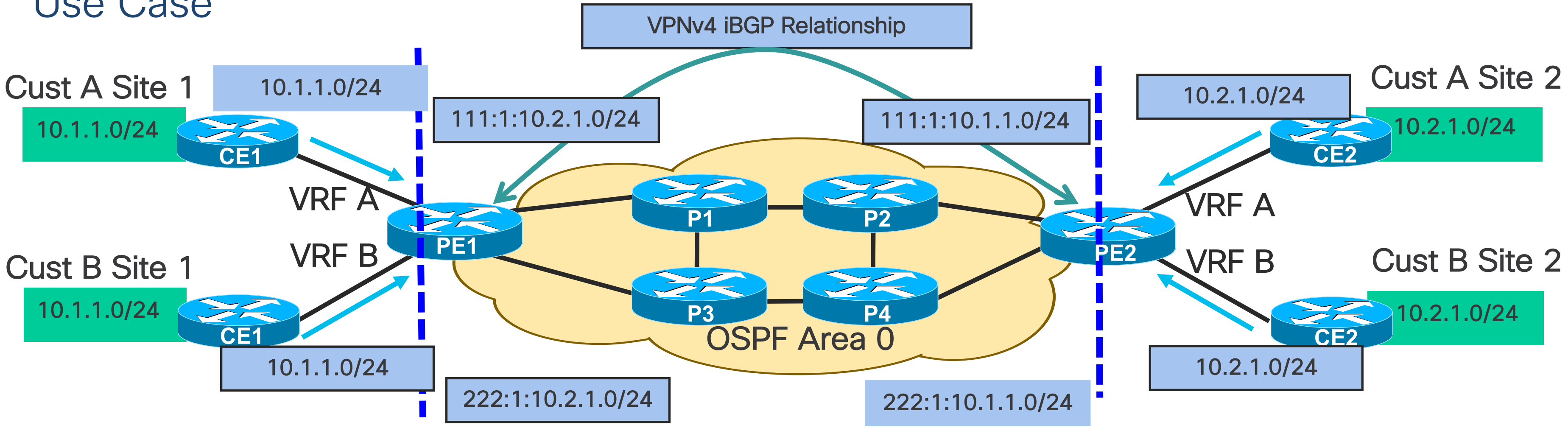
VPN Control Plane Processing

Exchange of routing information

- 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

Why an RD and VPNv4 Address?

Use Case

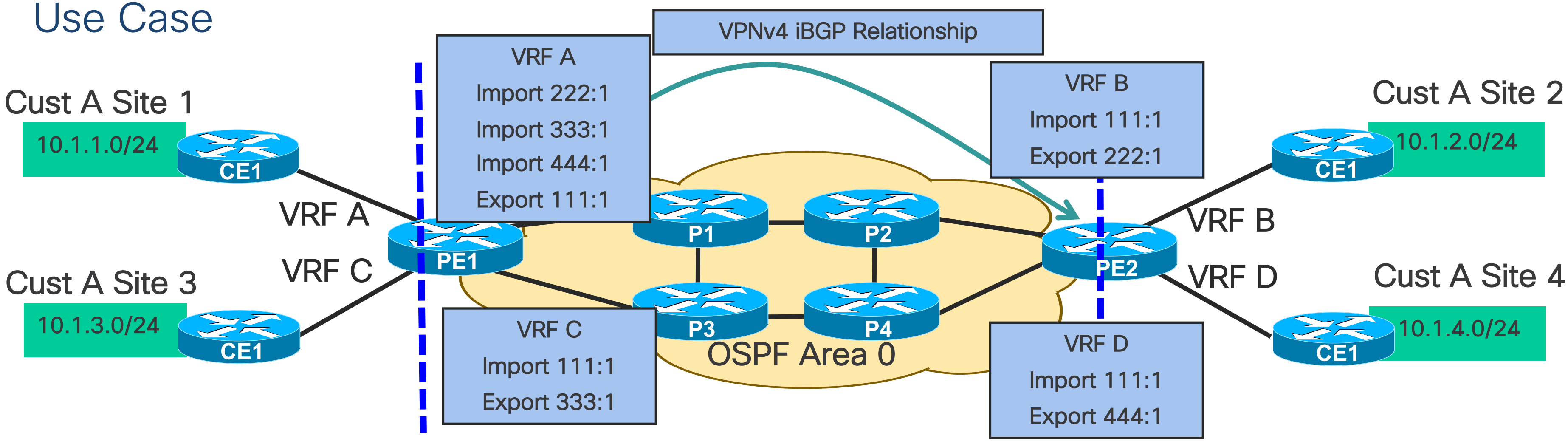


1. PE routers service multiple customers
2. Once PE redistributes customer routes into MP-BGP, they must be unique
3. RD is prepended to each prefix to make routes unique

VPNv4 prefixes are the combination of a 64-bit RD and a 32-bit IPv4 prefix. VPNv4 prefixes are 96-bits in length

Why are Route Targets Important?

Use Case



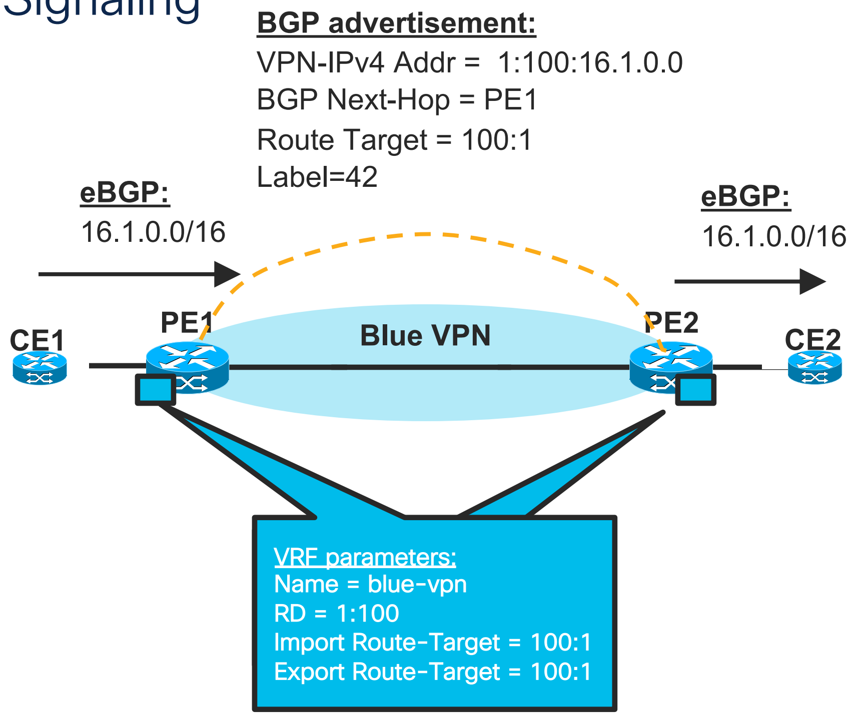
1. Route Targets dictate which VRF will receive what routes
2. Can be used to allow specific sites access to centralized services
3. Cust A Site 2, Site 3 and Site 4 will not be able to exchange routes with each other

Route Targets are a 64-bit value and are carried in BGP as an extended community

VPN Control Plane Processing

Interactions Between VRF and BGP VPN Signaling

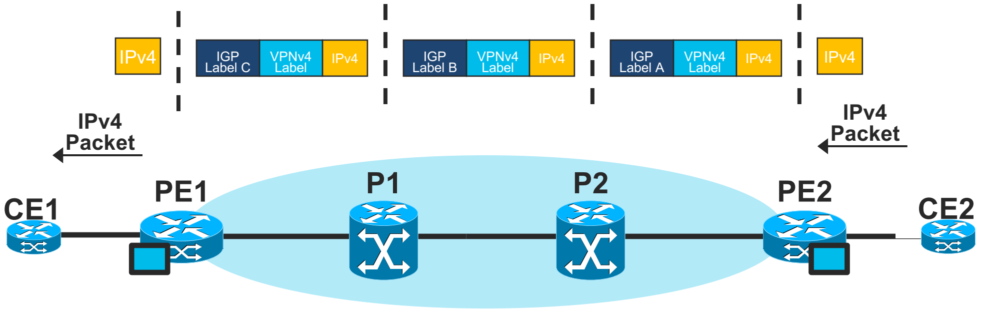
- CE1 redistribute IPv4 route to PE1 via eBGP
- PE1 allocates VPN label for prefix learnt from CE1 to create unique VPNv4 route
- PE1 redistributes VPNv4 route into MP-iBGP, it sets itself as a next hop and relays VPN site routes to PE2
- PE2 receives VPNv4 route and, via processing in local VRF (blue),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



VPN Forwarding Plane Processing

Forwarding of Layer-3 MPLS VPN Packets

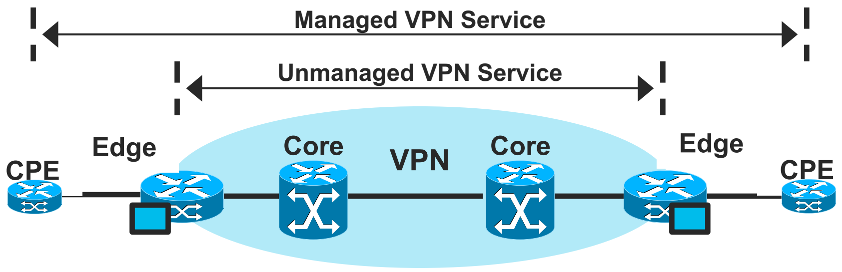
- CE2 forwards IPv4 packet to PE2
- PE2 imposes pre-allocated VPN label to IPv4 packet received from CE2
  - Learned via MP-IBGP
- PE2 imposes outer IGP label A (learned via LDP) and forwards labeled packet to next-hop P-router P2
- P-routers P1 and P2 swap outer IGP label and forward label packet to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

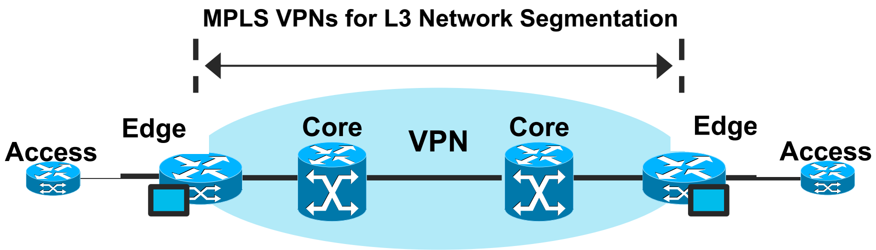


Network Segment	CPE	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	ASR1K ISR4K ASR90X	ASR9K ASR90X ASR1K ASR903 ME3800X	CRS-3 GSR ASR9K NCS5K

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 organizations
- Benefits
  - Network segmentation only requires edge node configuration
  - Flexible routing; different IP connectivity can be easily configured; e.g., full/partial mesh

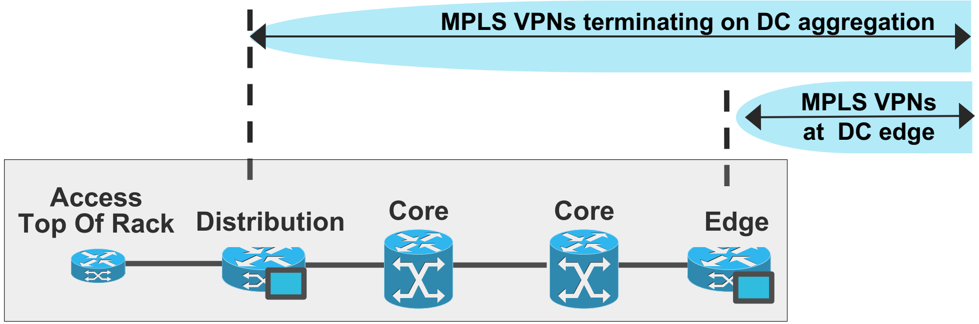


Network Segment	Access	Edge	Core
MPLS Node	CE	PE	P
Typical Platforms	CAT2K CAT3K ISR4K CAT9k	N7K ASR1K CAT6K CAT3K CAT9K	ASR9K CAT6K N7K NCS5K

Data Center Deployment Scenario

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

- Deployment Use Case
  - Segmented WAN Layer-3 at Data Center edge
  - Layer-3 segmentation in Data Center
- Benefits
  - Only single Data Center 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

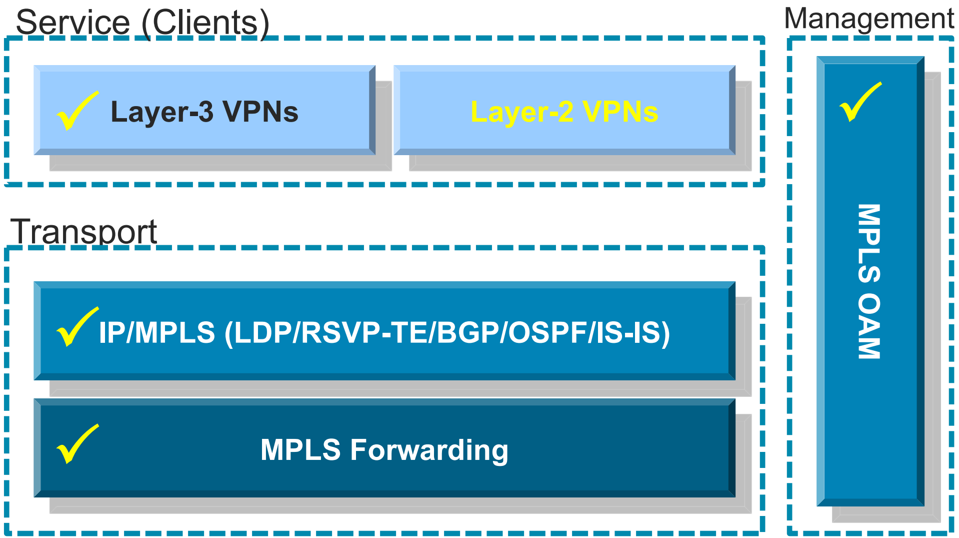
- MPLS Layer-3 VPNs provide IP connectivity among CE sites
  - MPLS VPNs enable full-mesh, hub-and-spoke, and hybrid IP connectivity
- CE sites connect to the MPLS network via IP peering across PE-CE links
- MPLS Layer-3 VPNs are implemented via VRFs on PE edge nodes
  - VRFs providing customer routing and forwarding segmentation
- BGP used for signaling 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 Center access

MPLS Layer-2 Virtual Private Networks

MPLS Layer-2 Virtual Private Networks

Topics

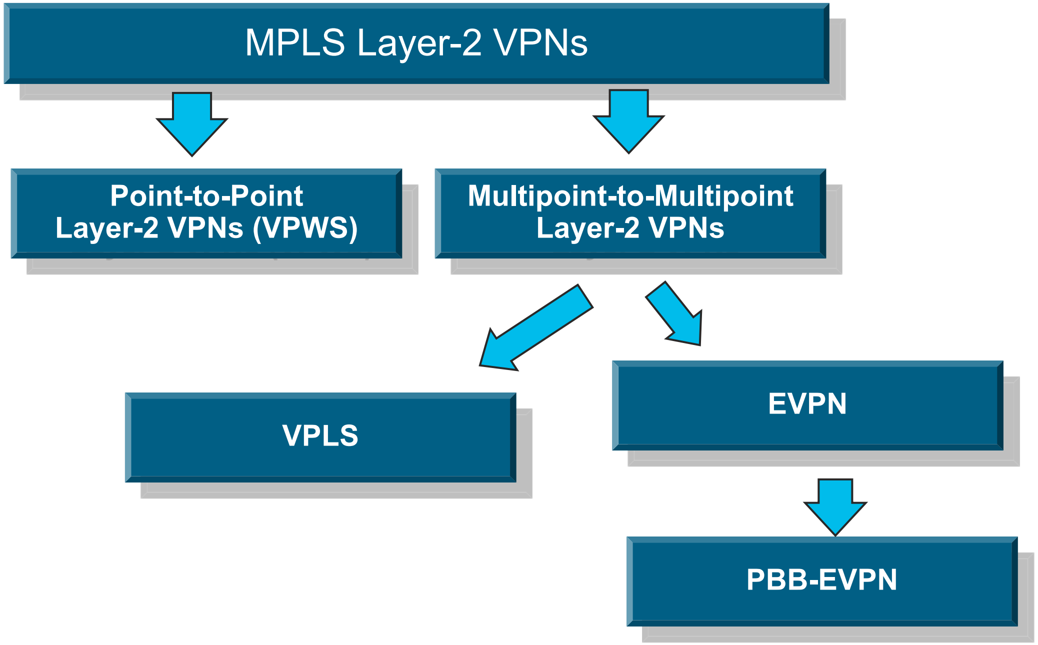
- L2VPN technology options
- P2P services (VPWS)
  - Overview & Technology Basics
  - VPN control plane
  - VPN forwarding plane
- MP2MP services (VPLS / xEVPN)
  - Overview & Technology Basics
  - VPN control / forwarding plane
- Deployment use cases
  - L2 Business VPN services
  - Data Center Interconnect



MPLS Layer-2 Virtual Private Networks

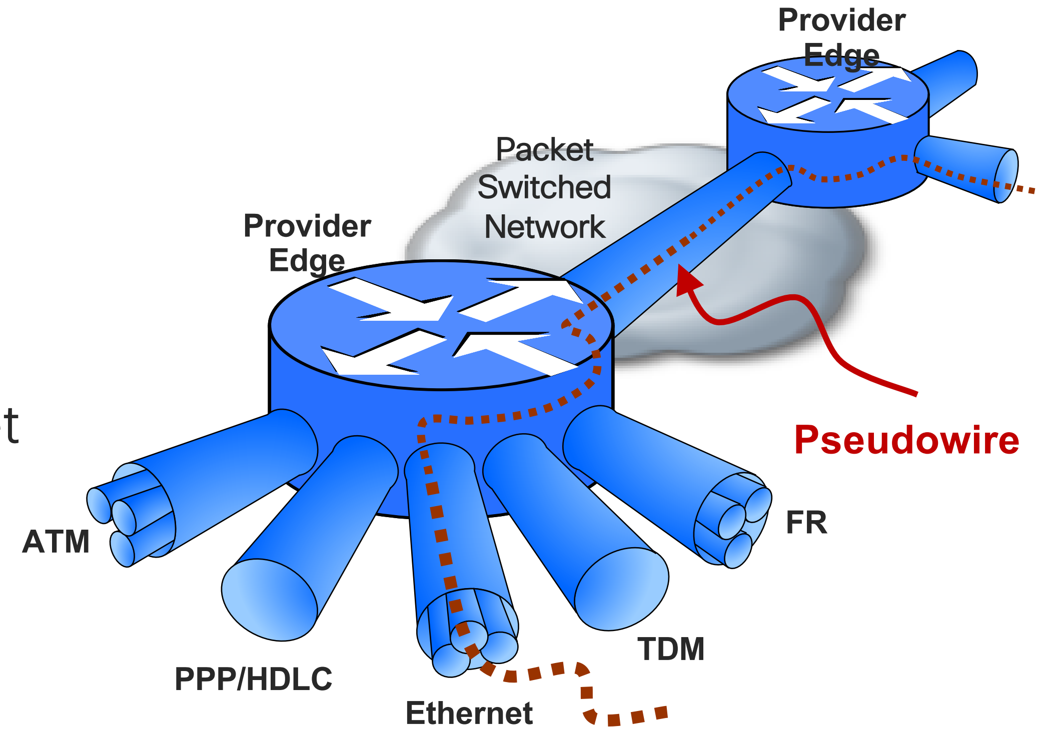
Technology Options

- VPWS services
  - Point-to-point
  - Referred to as Pseudowires (PWs)
- VPLS services
  - Multipoint
- EVPN
  - Multipoint with BGP-based MAC learning
- PBB-EVPN
  - Combines scale tools from PBB (aka MAC-in-MAC) with BGP-based MAC learning from EVPN



Layer 2 VPN Enabler

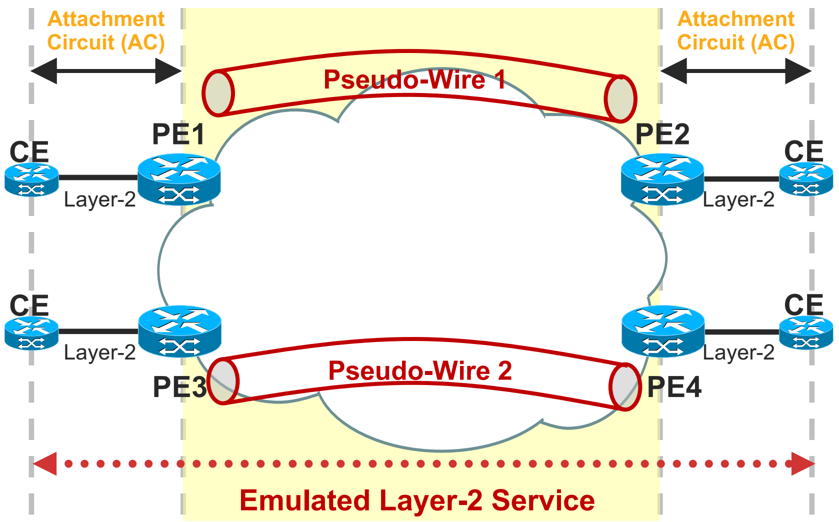
- L2VPNs are built with Pseudowire (PW) technology
- PWs provide a common intermediate format to transport multiple types of network services over a Packet Switched Network (PSN)
- PW technology provides Like-to-Like transport and also Interworking (IW)



Virtual Private Wire Services (VPWS)

Overview of Pseudowire (PW) Architecture

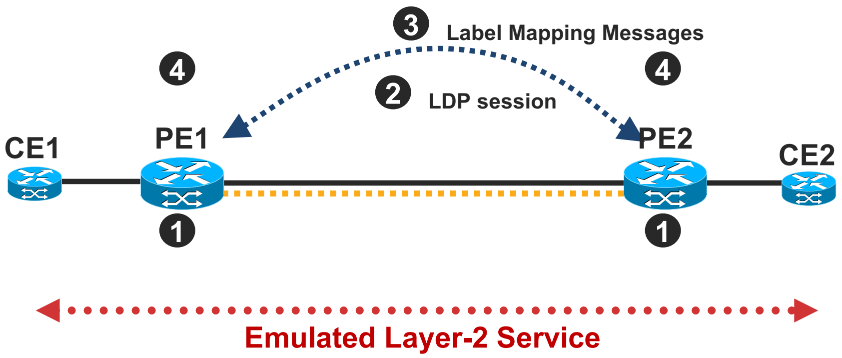
- Based on IETF's Pseudo-Wire (PW) Reference Model
- Enables transport of any Layer-2 traffic over MPLS
- PE-CE link is referred to as Attachment Circuit (AC)
- Provides a p2p service
- Discovery: manual (config)
- Signaling: LDP
- Learning: none



VPWS Control Plane Processing

Signaling of a New Pseudo-Wire

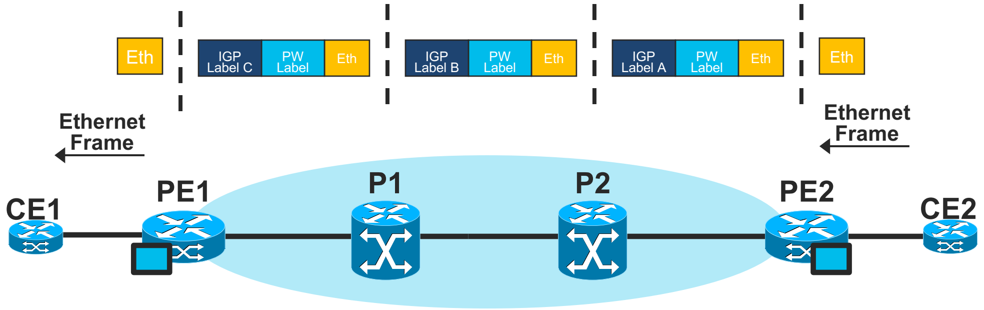
- (1) New Virtual Circuit (VC) cross-connect connects customer L2 interface (AC) to new PW via VC ID and remote PE ID
- (2) New targeted LDP session between PE1 and PE2 is established, in case one does not already exist
- (3) PE binds VC label with customer layer-2 interface and sends label-mapping to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

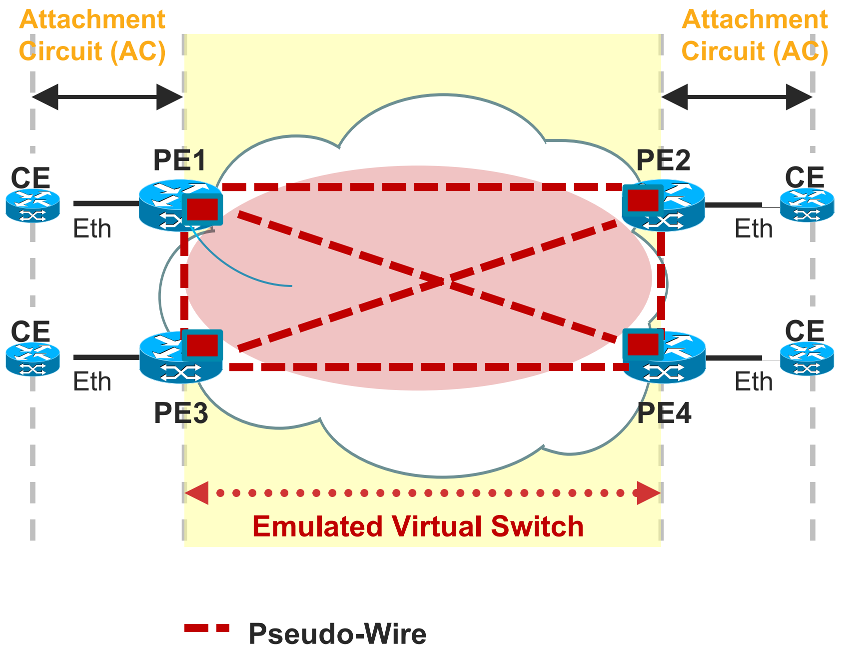
- CE2 forwards L2 packet to PE2.
- PE2 pushes VC (inner) label to L2 packet received from CE2
- PE2 pushed outer (Tunnel) label and forwards packet to P2
- P2 and P1 forward packet using outer (tunnel) label (swap)
- Router PE1 pops Tunnel label and, based on VC label, L2 packet is forwarded to customer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



Virtual Private LAN Services

Overview of VPLS Architecture

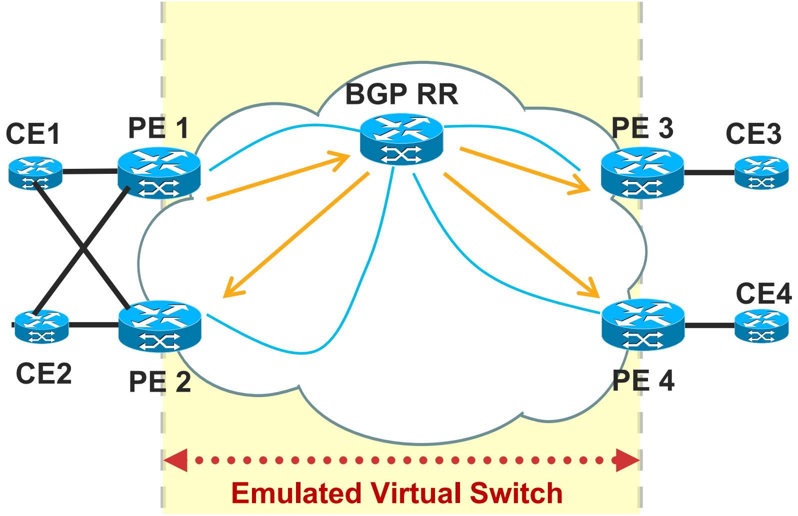
- VPLS network acts like a virtual switch that emulates conventional L2 bridge
- Fully meshed or Hub-Spoke topologies supported
- Provides a multipoint ethernet service
- Discovery: manual or auto (BGP)
- Signaling: LDP or BGP (PW label)
- Learning: data plane



EVPN

- Ethernet VPN
- Provides a multipoint ethernet service
- Discovery: BGP, using MPLS VPN mechanisms (RT)
- Signaling: BGP (MAC prefixes)
- Learning: Control plane (BGP)
- Allows for multihomed CEs

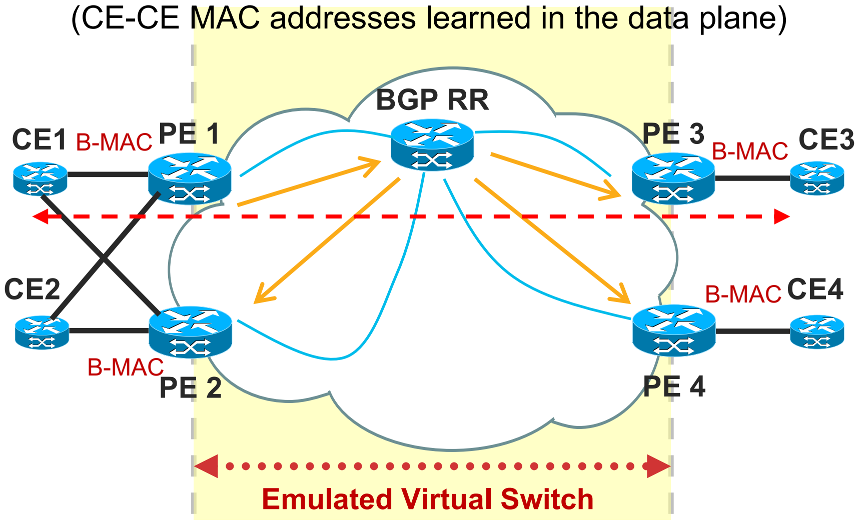
BGP advertisement:
L2VPN/EVPN Addr = **CE1.MAC**
BGP Next-Hop = PE1
Route Target = 100:1
Label=42



PBB-EVPN

- Combines Provider Backbone Bridging (MAC-in-MAC) with EVPN
  - Scales better than EVPN
  - Removes the need to advertise Customer MAC addresses in BGP
- Provides multipoint ethernet service
- Discovery: BGP, using MPLS VPN mechanisms (RT)
- Signaling: BGP (B-MAC prefixes)
- Learning: Control plane (BGP) and forwarding plane
- Allows for multihomed CEs

BGP advertisement:
L2VPN/EVPN Addr = **PE1.B-MAC**
BGP Next-Hop = PE1
Route Target = 100:1
Label=42

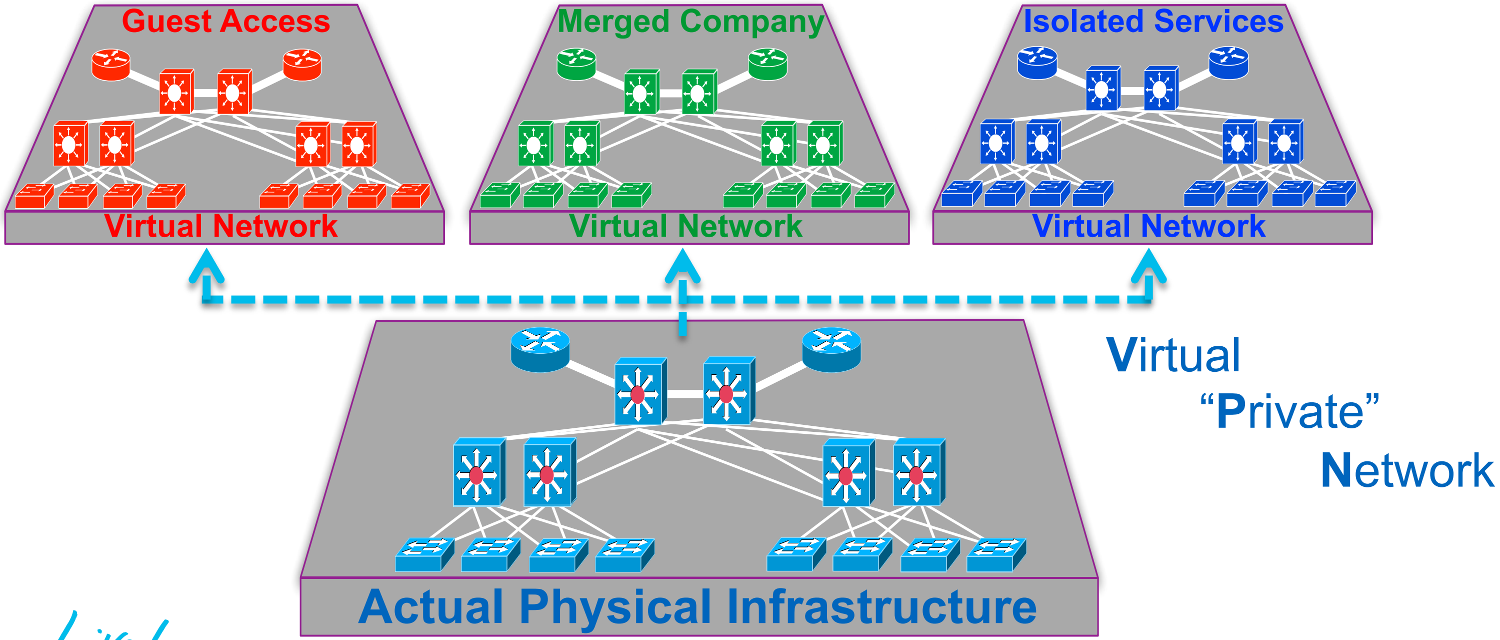


C-MAC = Customer MAC address
B-MAC = Backbone MAC address

MPLS Use Cases

Why Virtualize?

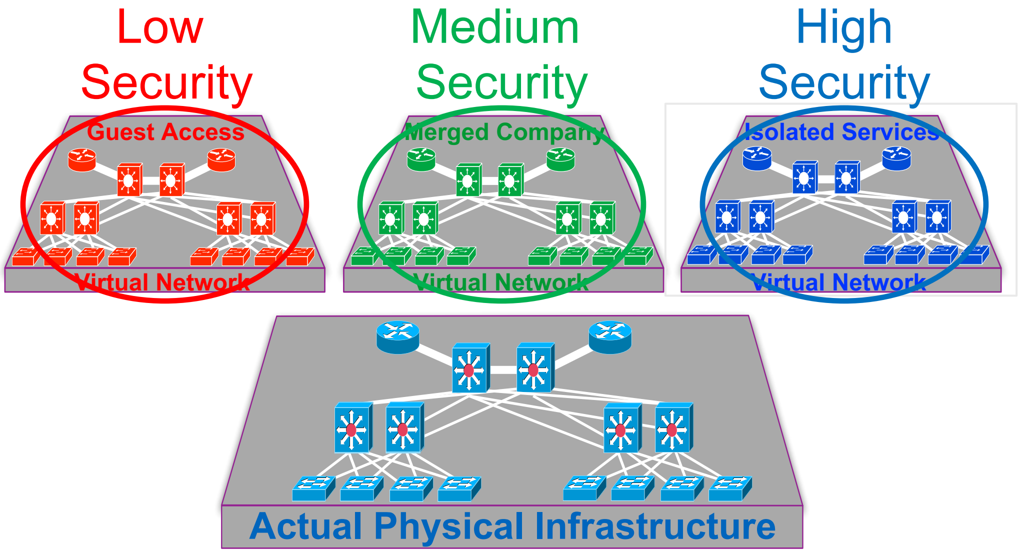
- Logical Segmentation
  - Traffic isolation per application, group, service etc…
  - Logically separate traffic using one physical infrastructure



Enterprise MPLS Deployment Scenario

Secure Segmentation

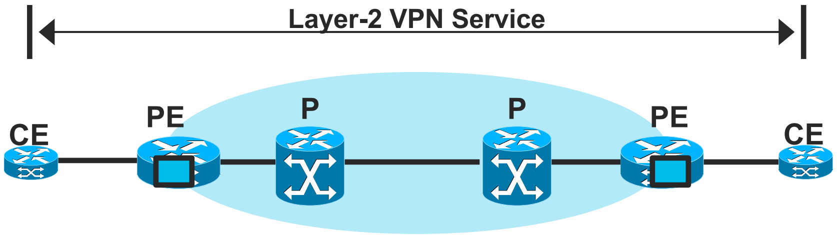
- Service isolation
  - Telephony systems, building control, surveillance
  - Security policies are unique to each virtual group/service
- Meet regulatory compliance requirements
  - HIPAA
  - PCI
  - SOX
  - etc…



Service Provider Deployment Scenario

PWs for Offering Layer-2 Business VPN Services

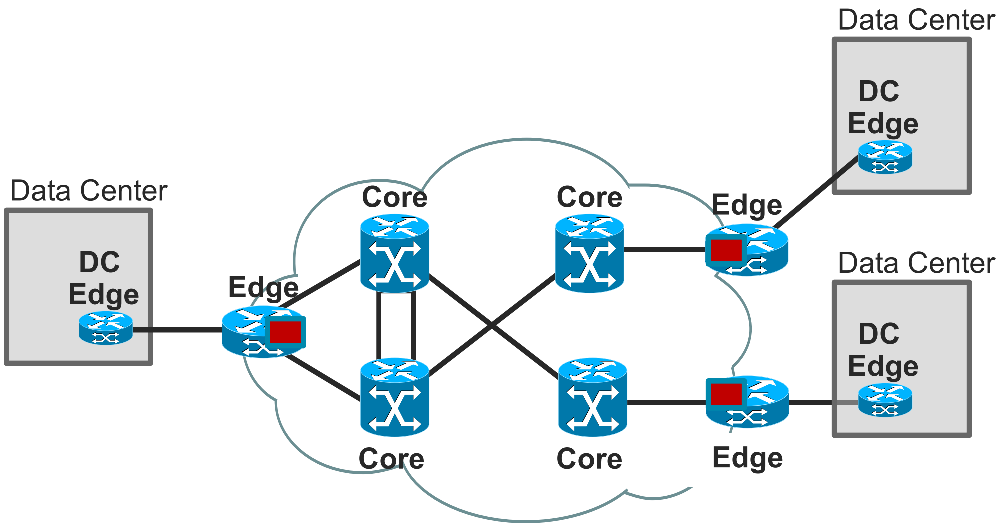
- Deployment Use Case
  - Delivery of E-LINE services to business customers
- Benefits
  - Leverage same network for multiple services and customers (CAPEX)
    - Highly scalable
  - Service enablement only requires edge node configuration (OPEX)



Data Center Deployment Scenario

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

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



Summary

Key Takeaways

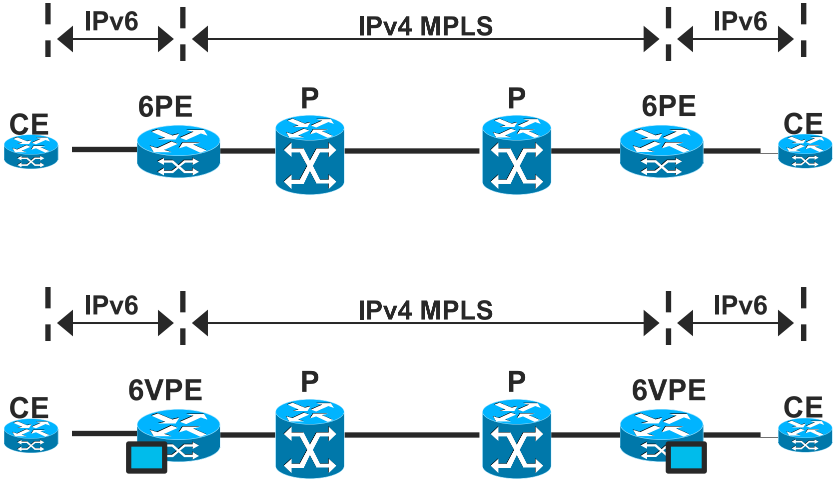
- L2VPNs enable transport of any Layer-2 traffic over MPLS network
- L2 packets encapsulated into additional VC label
- Both LDP and BGP can be used Pseudowire (PW) signaling
- PWs suited for implementing transparent point-to-point connectivity between Layer-2 circuits (E-LINE services)
- VPLS suited for implementing transparent point-to-multipoint connectivity between Ethernet links/sites (E-LAN services)
- EVPN / PBB-EVPN are next-generation L2VPN solutions based on BGP control-plane for MAC distribution/learning over the core
- Typical applications of L2VPNs are layer-2 business VPN services and Data Center interconnect

Advanced Topics

MPLS And IPv6

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

- MPLS allows IPv6 to be deployed as an edge-only service, no need to run v6 in the core
  - Easier to deploy
  - Security mechanism
- 6PE: All IPv6 can see each other (single VPN)
  - IPv6+label (no RD, no RT)
- 6VPE: Separate IPv6 VPNs
  - VPNv6, includes RD and RT

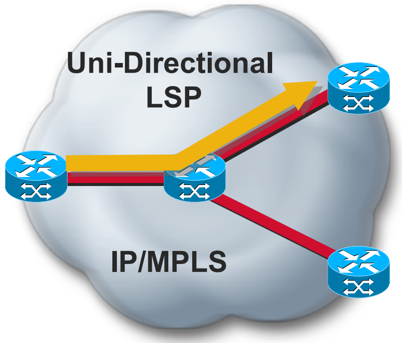


Label Switched Multicast (LSM)

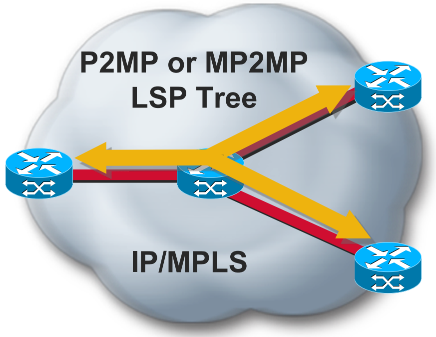
Point-to-Multi-Point MPLS Signaling and Connectivity

- 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



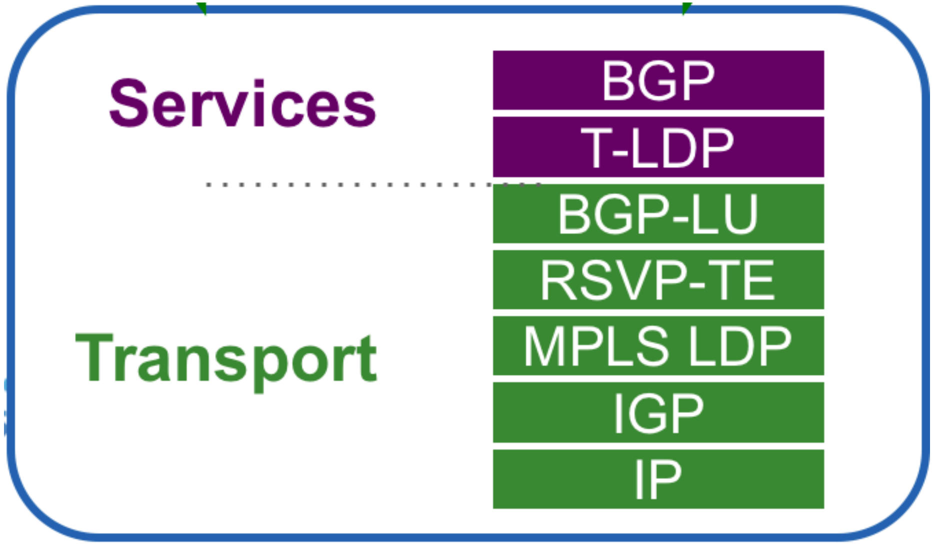
Label Switched Multicast (LSM)



Network Transport Evolution – Segment Routing

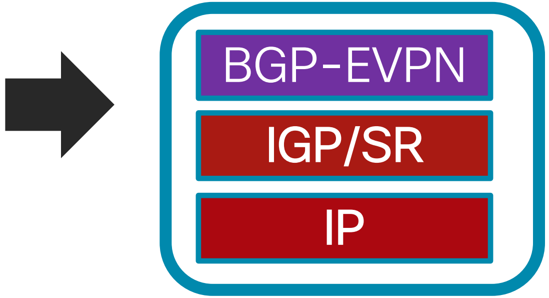
Simplify – Optimize – Enable

Unified MPLS



SR

Enabled Transport

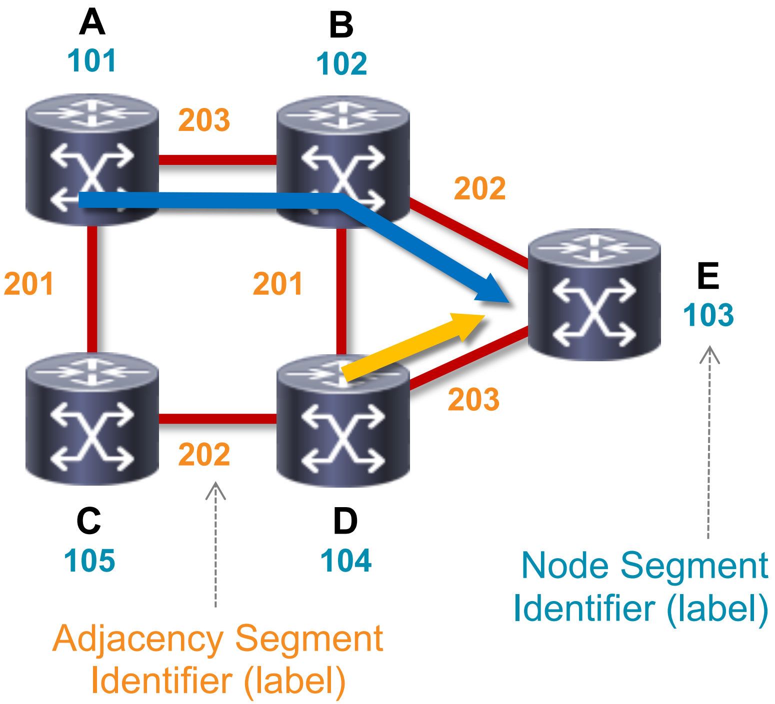


Do more with less !!

Segment Routing

Control Plane

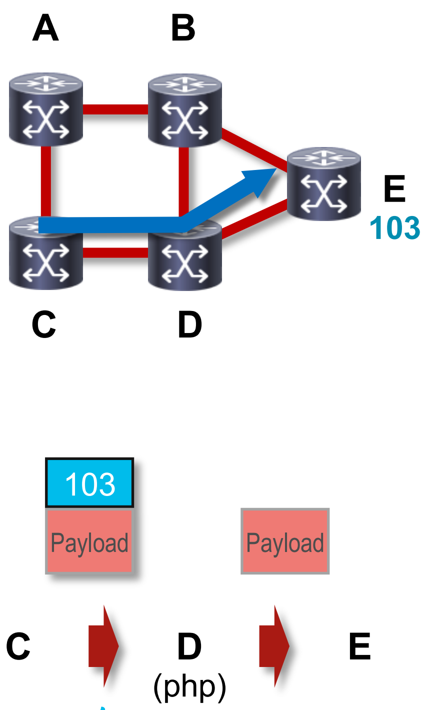
- Segment routing provides
  - Rich forwarding behaviors
- Simple IS-IS / OSPF extensions program MPLS forwarding plane
- IGP advertises
  - Node segment id (label) per node (globally significant)
  - Adjacency segment id (label) per link (locally significant)
- Packet with node segment id forwarded along shortest path to destination



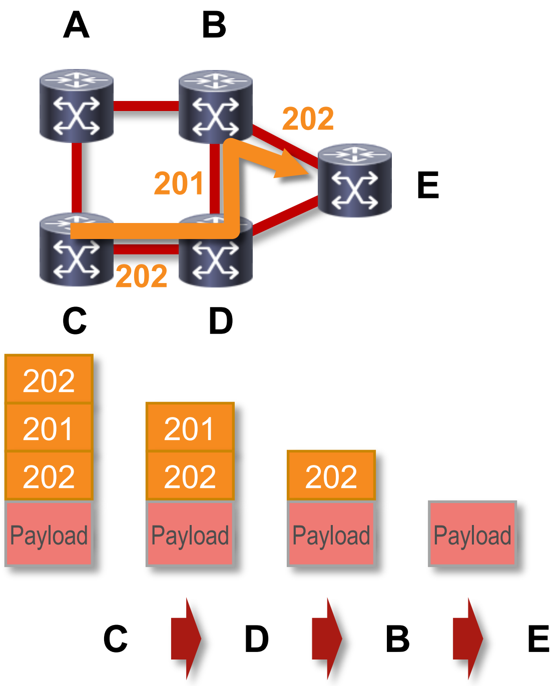
Segment Routing

Forwarding Plane

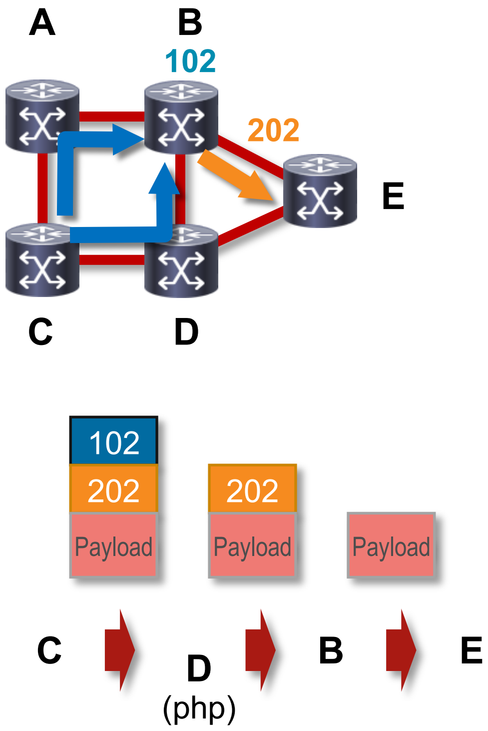
Node Path



Adjacency Path



Combined Path



Summary

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 signaling
- 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
  - De facto for most SPs, large enterprises, and increasingly in Data Centers
- Ongoing technology evolution
  - Control-plane simplification (Segment Routing) and WAN orchestration (PCE/SDN)

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 optimized network availability and performance?
  - Node/link protection, pro-active connectivity validation
  - Bandwidth traffic engineering and QoS traffic prioritization

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

Thank you

Possibilities

#CiscoLive

Terminology Reference

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

Acronyms Used in MPLS Reference Architecture (cont.)

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