Cisco IOS® MPLS Management Technical Deployment Overview

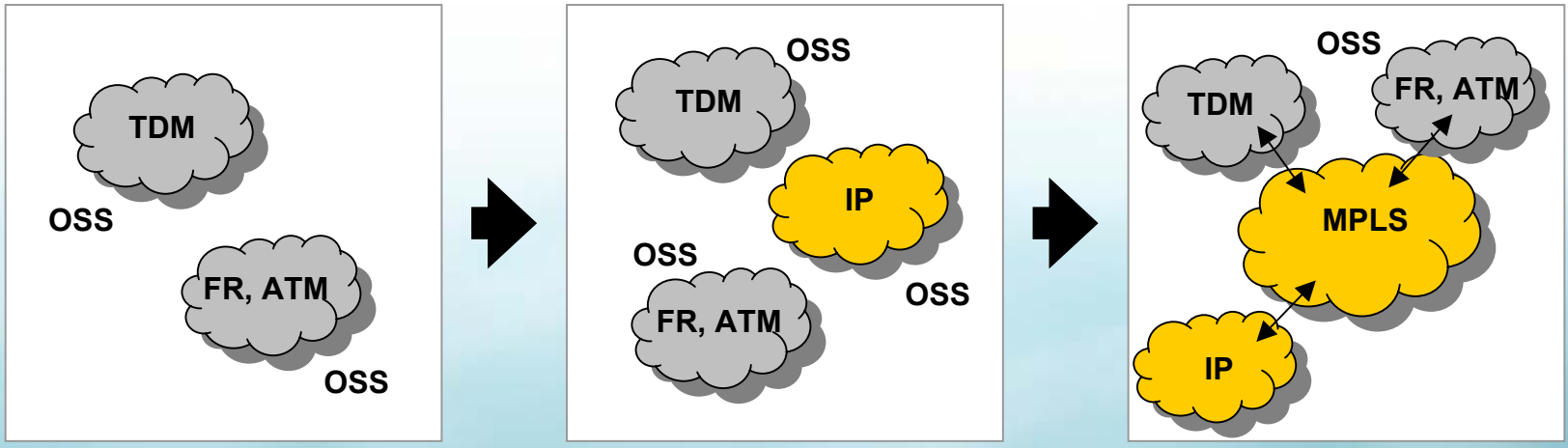
Enabling Innovative Services

February 2004

Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – *Primary & Backup*
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

Service Provider Problems



- **Operational Efficiencies**

  Increase management automation and availability

- **New Services Provisioning**

  Enable competitive differentiation and customer retention through profitable bundled services

- **Disparate Networks**

  Manage and consolidate traditional and emerging networks

Key Network Management Attributes

- Fault management
- Configuration
- Accounting
- Performance
- Security

MPLS Operations Administration & Management (OAM) are tools and techniques needed to address FCAPS in deploying and operating an MPLS network successfully

Cisco IOS MPLS Embedded Management and FCAPS

Fault Management	MPLS Ping/Traceroute, VCCV, Mib, Auto SAA
Configuration	MPLS TE Auto Tunnel, Auto Tunnel Mesh Groups, Auto SAA
Accounting	NetFlow, MIB
Performance	SAA, Auto SAA, NetFlow, Mib
Security	RSVP Message Authentication LDP Message Authentication MD5 Authentication for Routing Protocol: BGP, OSPF

Deployment Requirements: 3 Categories*

- ✓ VC/LSP Path Verification and Tracing
- ✓ Built-in Protocol Operations
- ✓ Standard Management APIs/NMS Applications
  - ✓ MIBs, CLI, XML, etc…

➢ ***These must be addressed before the majority of providers will deploy value added MPLS services***

*1st Tier PWE/MPLS SPs

Consequences of Not Addressing OAM Requirements

- Providers cannot guarantee SLAs to customers
- Providers cannot guarantee path liveliness/reachability
- Difficult to tell if VC interface is up/down
- Difficult to roll out new service

Take away:
Difficult at best to deploy services without OAM

Fault Management Detection and Isolation

Control Plane Verification

- Consistency check
- Authentication

Data Plane Verification

- Ability to verify connectivity, trace and SLA

  Paths from PE to PE – Global routing table as well as VPNs

  Paths from CE to CE within a VPN

  TE tunnels

  Pseudowires

VC/LSP Connection Verification and Trace Requirements

- **Automated detection and diagnosis of broken transport LSPs and VCs:**
  - **Point-to-point**
  - **Multipoint-to-point**
  - **Equal Cost Multi-Path (ECMP)**
  - **Capability to run diagnostic tools from both headend and midpoints**

Data plane OAM packets must follow same path they are testing

Built-In Protocol Requirements

- Detect errors, recover from them, and alert the network operator *before* customer calls.
- Detection of DoS attacks via an OAM filtering mechanism for security mgmt.
- inherent to separate data and control planes

  RSVP-TE

  MPLS Fast Reroute

  LDP

Standard Management API Requirements

- **Ability to suppress unnecessary alarms**
  - **Example: LSP carrying pseudowire VCs**
  - **SNMP**
  - **SysLog**
  - **Protocol Flooding**
- **Integration of standard PWE3 and other related MIBs for fault and statistics management.**

Performance Monitoring Requirements

Some questions to ask are:

- **How does the service provider decrease operational expense and the complexity of monitoring SLAs and verifying service?**
- **How does the SP verify connectivity, and rapidly find bad paths across the MPLS core with Cisco IOS® Software instrumentation?**
- **How can the SP perform troubleshooting diagnostic to automatically find trouble spots and quickly resolve MPLS network issues?**
- **How can the SP obtain network measurements of round trip time, packet loss and jitter between PE routers?**

Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – *Primary & Backup*
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

LSP Ping

- Similar to ICMP (IP) Ping
  - Sequence number
  - Timestamps
  - Sender identification
- Full identification of FEC based on the application
- Variable length for MTU discovery
- Support for tunnel/path tracing
- Multiple-reply modes
- Handles ECMP
- Cisco® implementation compliant with draft-ietf-mpls-lsp-ping-03.txt

MPLS Ping: Operation

- Ping Mode: Connectivity check of an LSP

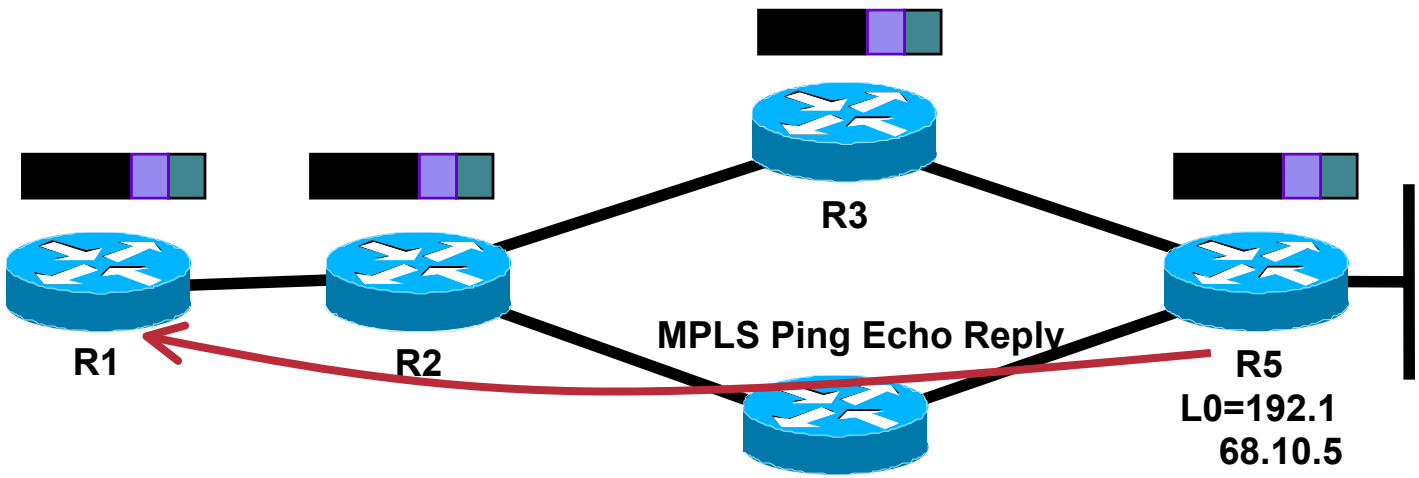
  Test if a particular "FEC" ends at the right egress LSR
- Traceroute Mode: Hop by Hop fault localization
- Uses two messages

  MPLS Echo Request

  MPLS Echo Reply
- Packet need to follow data path

MPLS Ping: Packet Flow

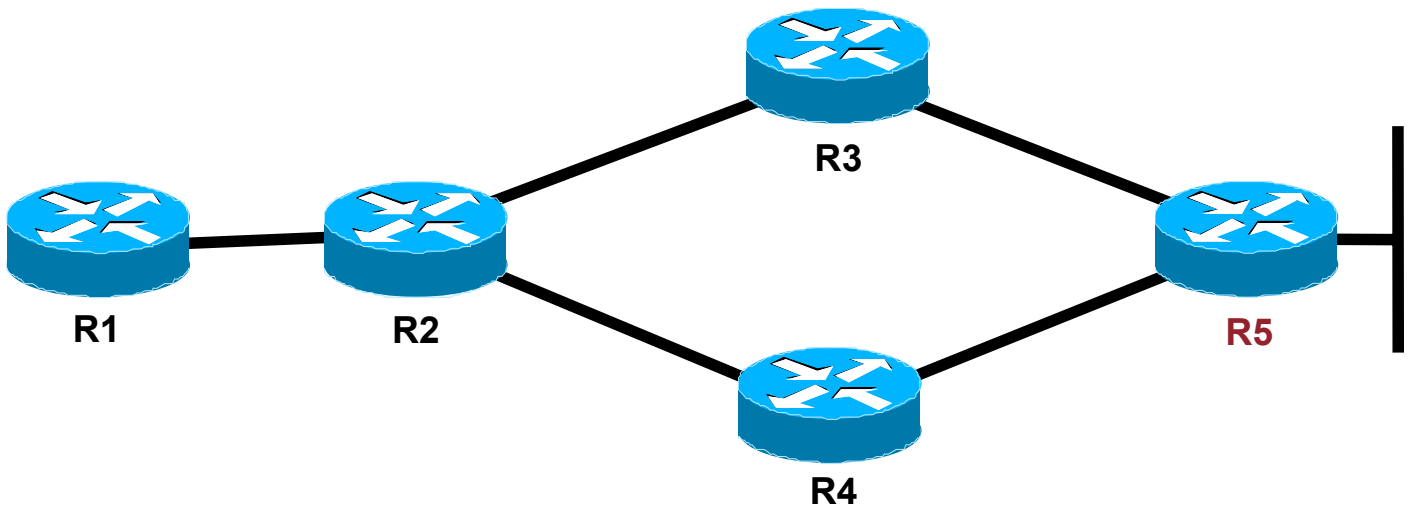
- Ping with label for FEC=192.169.10.0/24
- Label Switched at R2, R3
- R3 pops label off
- R5 processes packet



R1#ping mpls ipv4 192.168.10.5/32

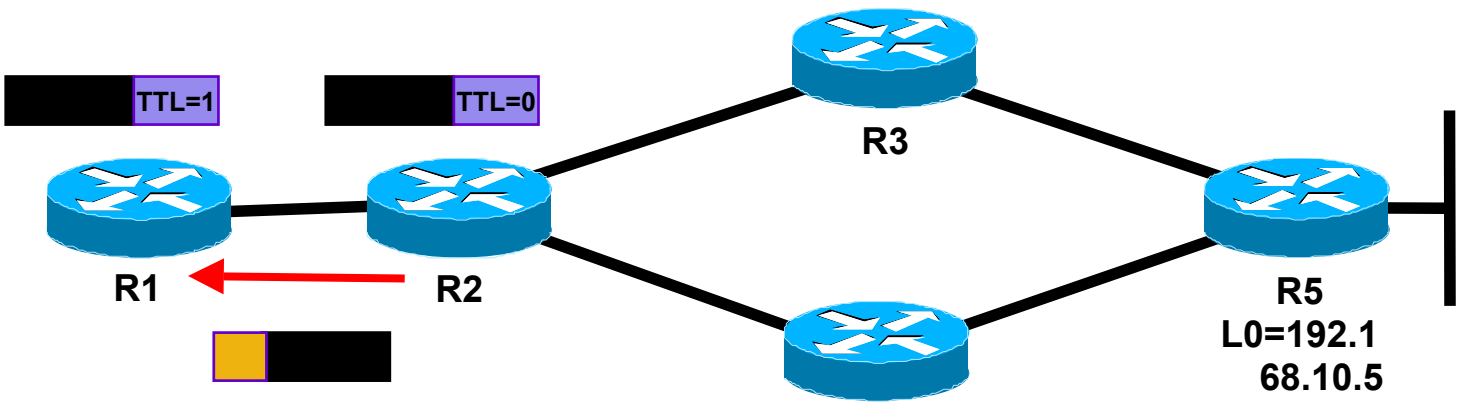
" Packet Flow Ping Mode: Egress Node

- Check packet integrity
- Check if FEC distribution protocol is associated with incoming interface
- Check if valid egress node for the FEC
- Send echo Reply according to value of Reply Mode



MPLS Traceroute: Packet Flow

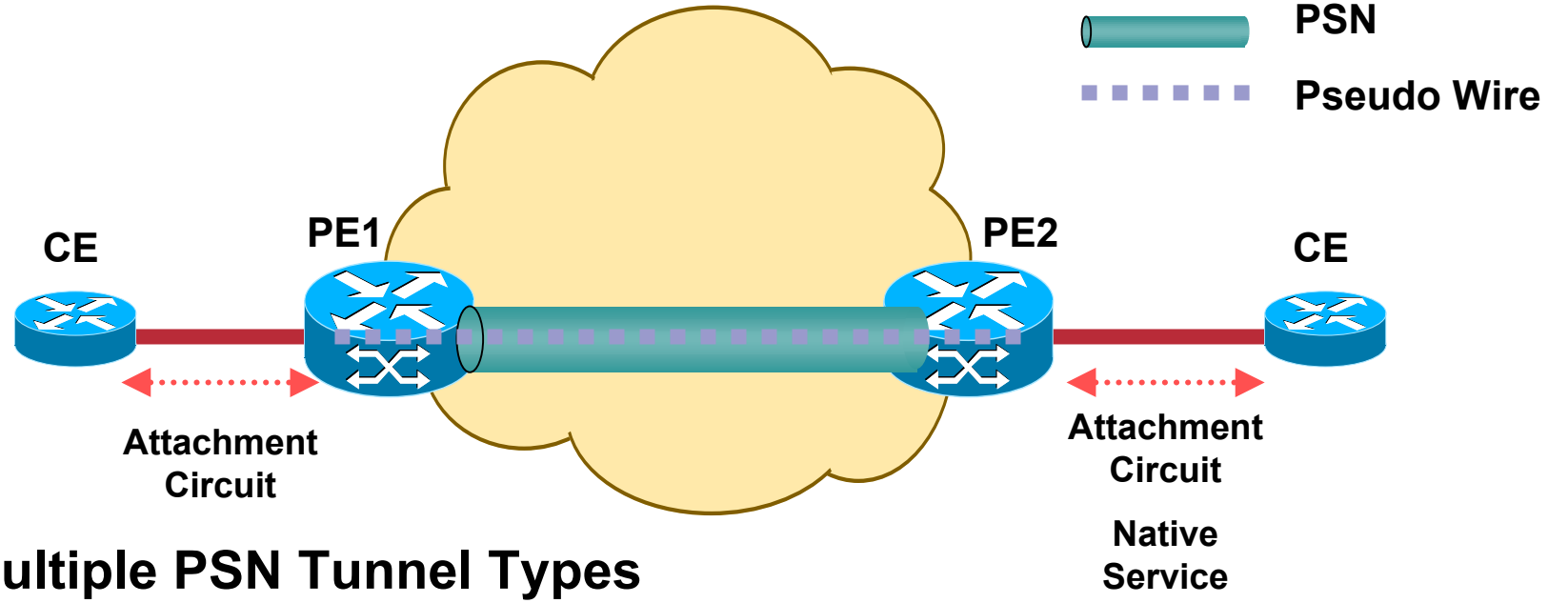
- MPLS Ping Packets are sent with TTL=1,2,3…,n
- Label switched if TTL > 1
- Processed where TTL expires
- Reply contains downstream mapping TLV (i.e. the label, interface for reaching the downstream router)



Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – *Primary & Backup*
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

Virtual Circuit Connection Verification (VCCV)



- **Multiple PSN Tunnel Types**
  - **MPLS, IPSEC, L2TP, GRE,…**
- **Motivation**

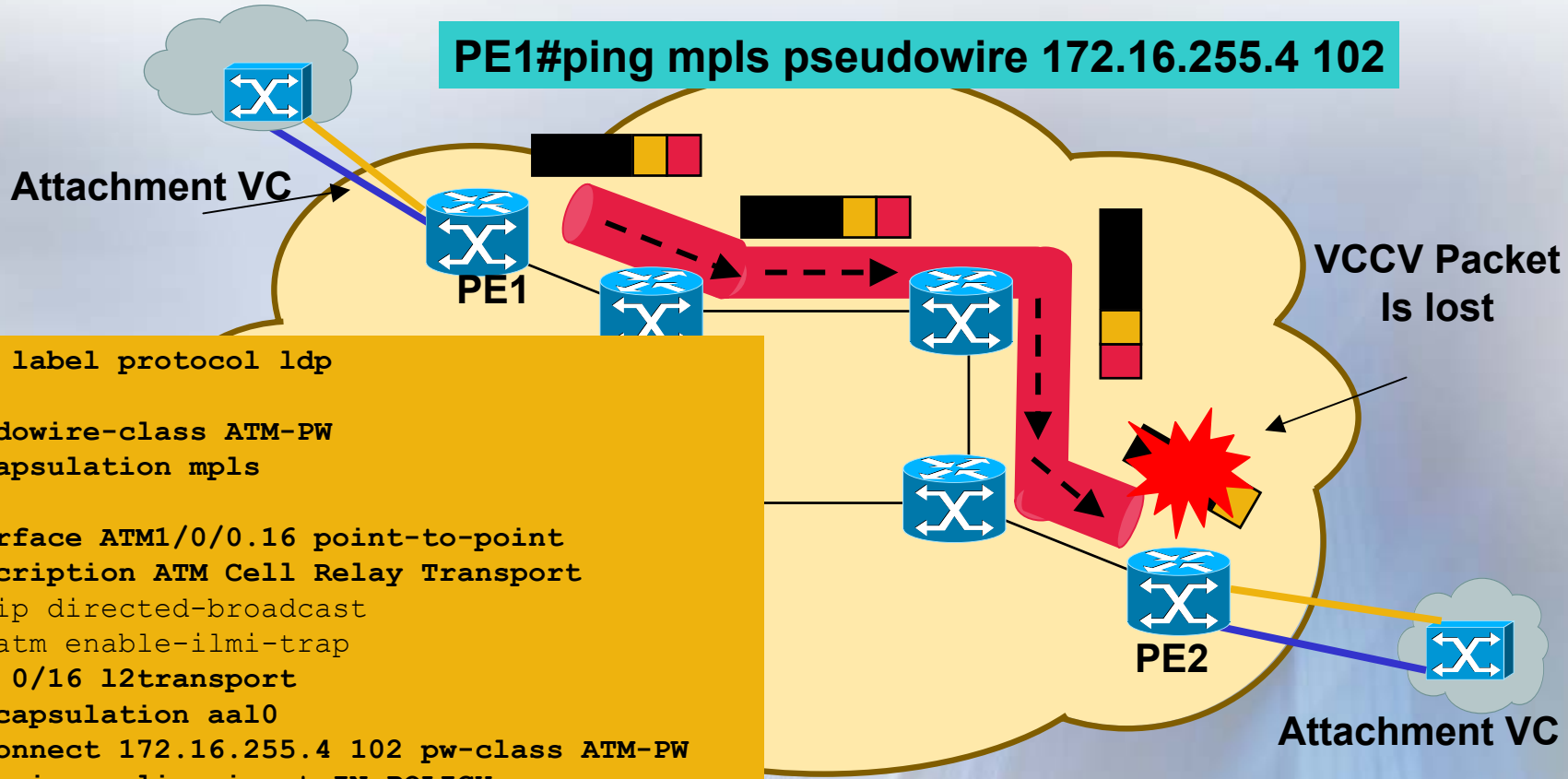
  One tunnel can serve many pseudo-wires.

  MPLS LSP ping is sufficient to monitor the PSN tunnel (PE-PE connectivity), but not VCs inside of tunnel.

VCCV Overview

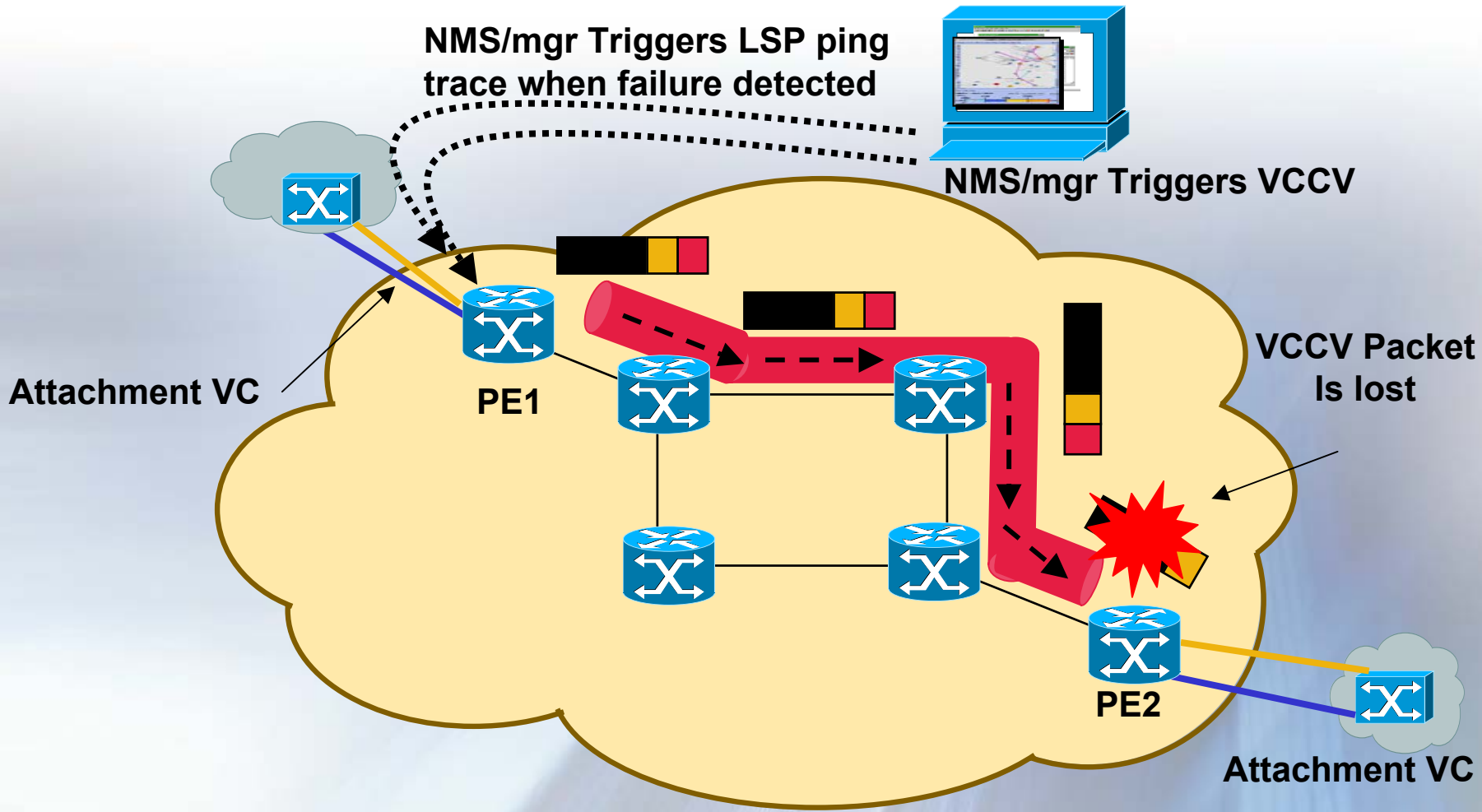
- Mechanism for connectivity verification of PseudoWire (PW)
- Really a control channel
- Features
  - Works over MPLS or IP networks
  - In-band Connectivity Verification (CV) via control word flag or out-of-band option by inserting router alert label between tunnel and PW labels
  - Works with ICMP Ping and/or LSP ping

Connectivity Trace Using VCCV




```
mpls label protocol ldp
!
pseudowire-class ATM-PW
 encapsulation mpls
!
interface ATM1/0/0.16 point-to-point
 description ATM Cell Relay Transport
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 0/16 l2transport
  encapsulation aal0
  xconnect 172.16.255.4 102 pw-class ATM-PW
  service-policy input IN-POLICY
  service-policy output OUT-POLICY
 !
!
```

Example of Operation CV/Trace Using VCCV and LSP Ping



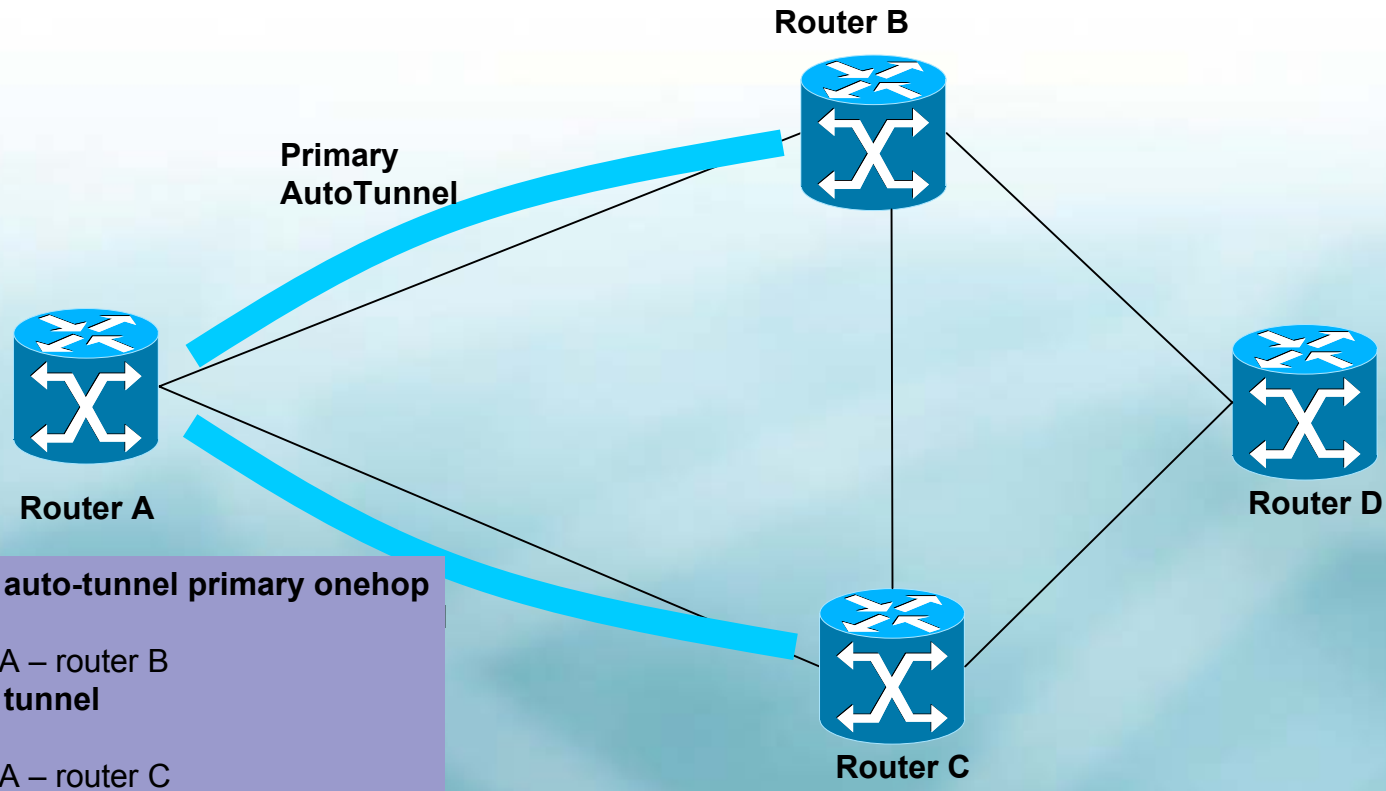
Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – *Primary & Backup*
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

MPLS TE AutoTunnel

- AutoTunnel automatically creates TE tunnels for primary and backup use
- Primary - AutoTunnel for primary TE tunnels has the following characteristics:
  - Sets up a TE tunnel to every adjacent neighbor or a “1-hop” tunnel
  - With FastReRoute, “1-hop” tunnel protects not only TE LSP traffic, but also IP Traffic. (Future versions will protect LDP LSP traffic as well)
  - Does not appear in configuration files – system generated
- Backup – AutoTunnel for backup TE tunnels has the following characteristics:
  - Sets up a Next hop and Next Next Hop
  - N:1 concept applies here as well i.e. 1 Backup tunnel protects multiple Primary tunnels
  - A “manually” configured backup tunnel is preferred to a Backup AutoTunnel

MPLS TE AutoTunnel: Primary

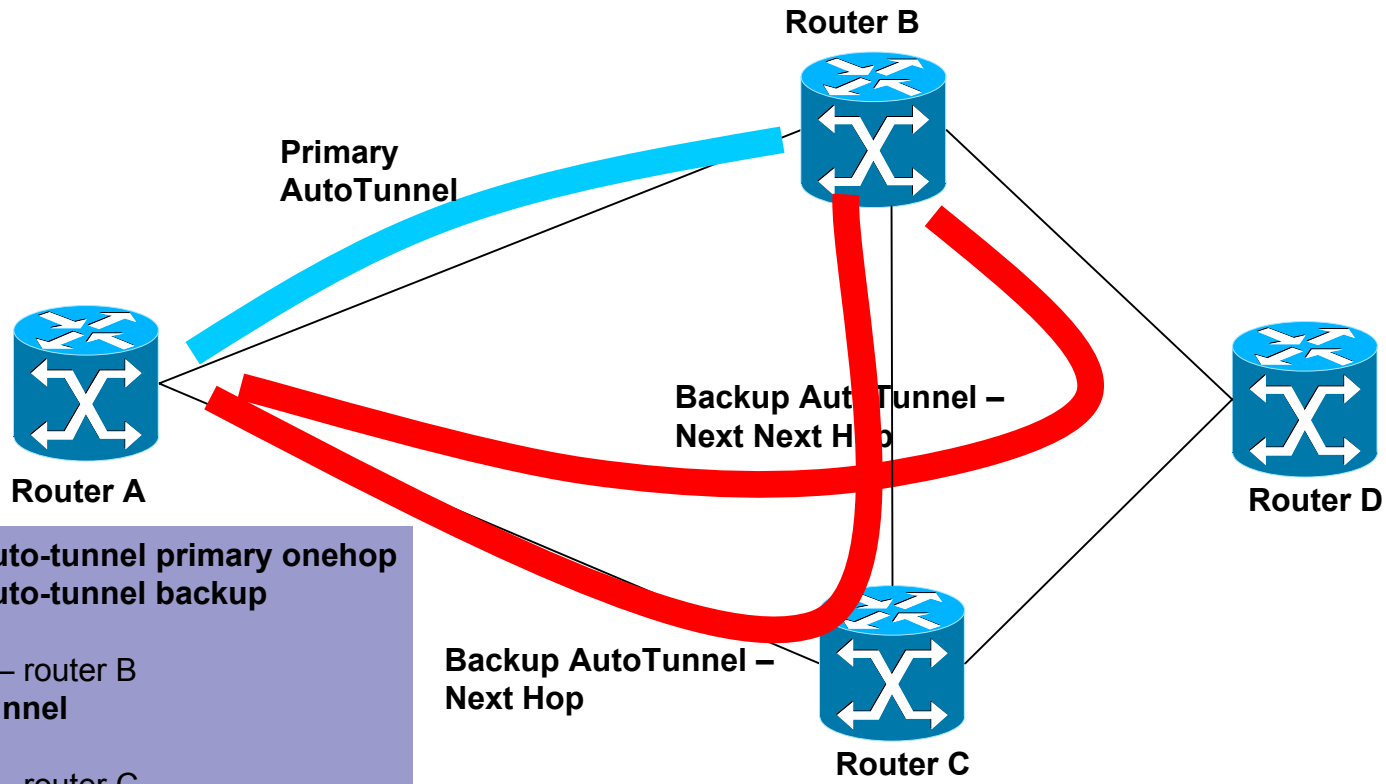



```
mpls traffic-eng auto-tunnel primary onehop

! Interface router A – router B
mpls traffic-eng tunnel

! Interface router A – router C
mpls traffic-eng tunnel
```

Router A creates 2 AutoTunnels for each adjacent neighbor – Router B and Router C

All AutoTunnels are zero bandwidth tunnels

MPLS TE AutoTunnel: Primary and Auto Backup

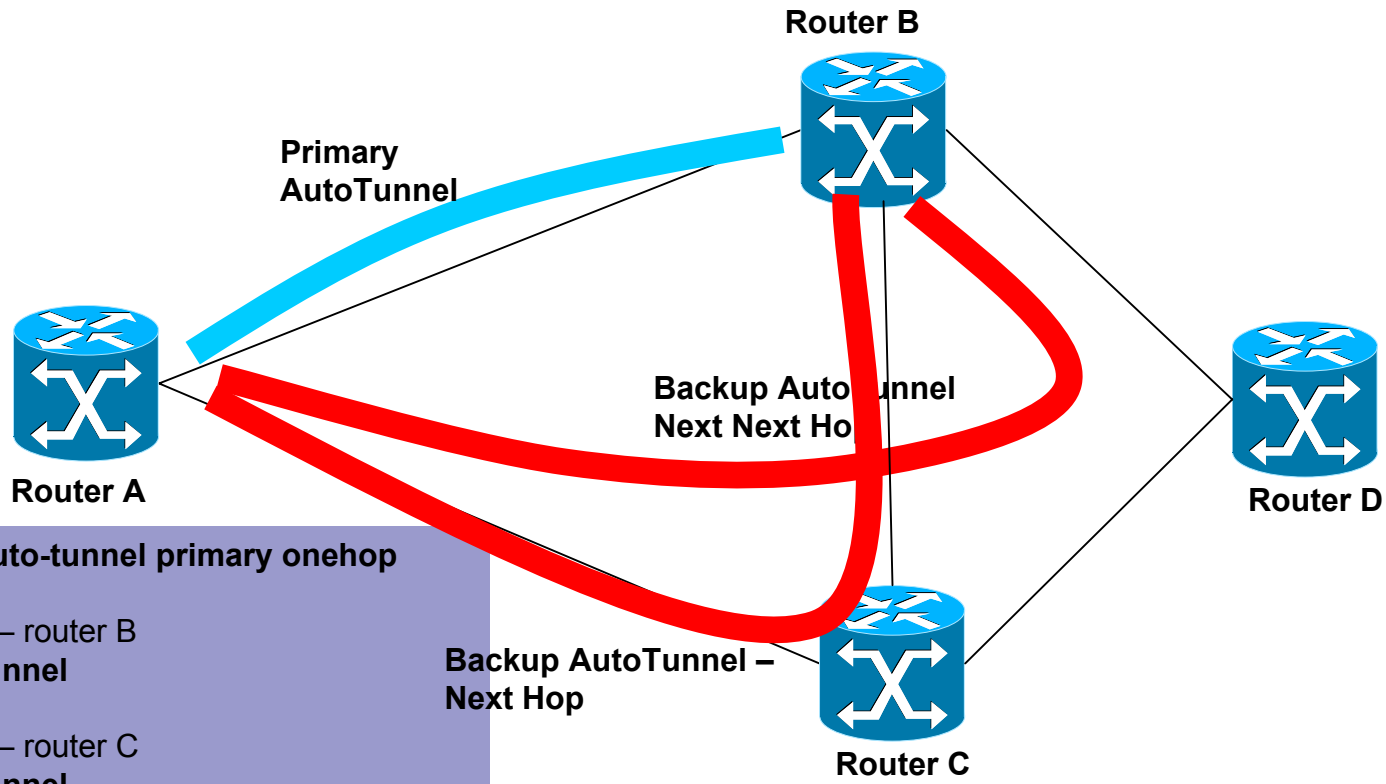



```
mpls traffic-eng auto-tunnel primary onehop
mpls traffic-eng auto-tunnel backup

! Interface router A – router B
mpls traffic-eng tunnel

! Interface router A – router C
mpls traffic-eng tunnel
```

Router A creates 2 Backup AutoTunnels for each connected link

All AutoTunnels are zero bandwidth tunnels

MPLS TE AutoTunnel: Primary and Manual Backup




```
mpls traffic-eng auto-tunnel primary onehop

! Interface router A – router B
mpls traffic-eng tunnel

! Interface router A – router C
mpls traffic-eng tunnel

!configure backup tunnel (Ra-Rc-Rb), (Ra-Rc-Rd-Rb)
```

On Router A define Manual Backup tunnels {RA, RC, RB} and/or {RA, RC, RD, RB}

Manual Tunnels take precedence over AutoTunnels – provides "tweaking" capability for customers

“Manual” TE vs AutoTunnel

Configuration Tasks – Before AutoTunnel

Configure Link

ip rsvp bandwidth....

mpls traffic-eng tunnel.....

….

Configure IGP

router ospf ....

mpls traffic-eng area...

.....

Configure TE Tunnels

int tun0

tunnel mode mpls .....

.....

int tun1

tunnel mode mpls .....

.....

Configuration Tasks – After AutoTunnel

Configure Link

ip rsvp bandwidth....

mpls traffic-eng tunnel….

….

Configure IGP

router ospf ....

mpls traffic-eng area...

.....

Configure TE AutoTunnel

mpls traffic-eng auto-tunnel primary onehop

mpls traffic-eng auto-tunnel backup

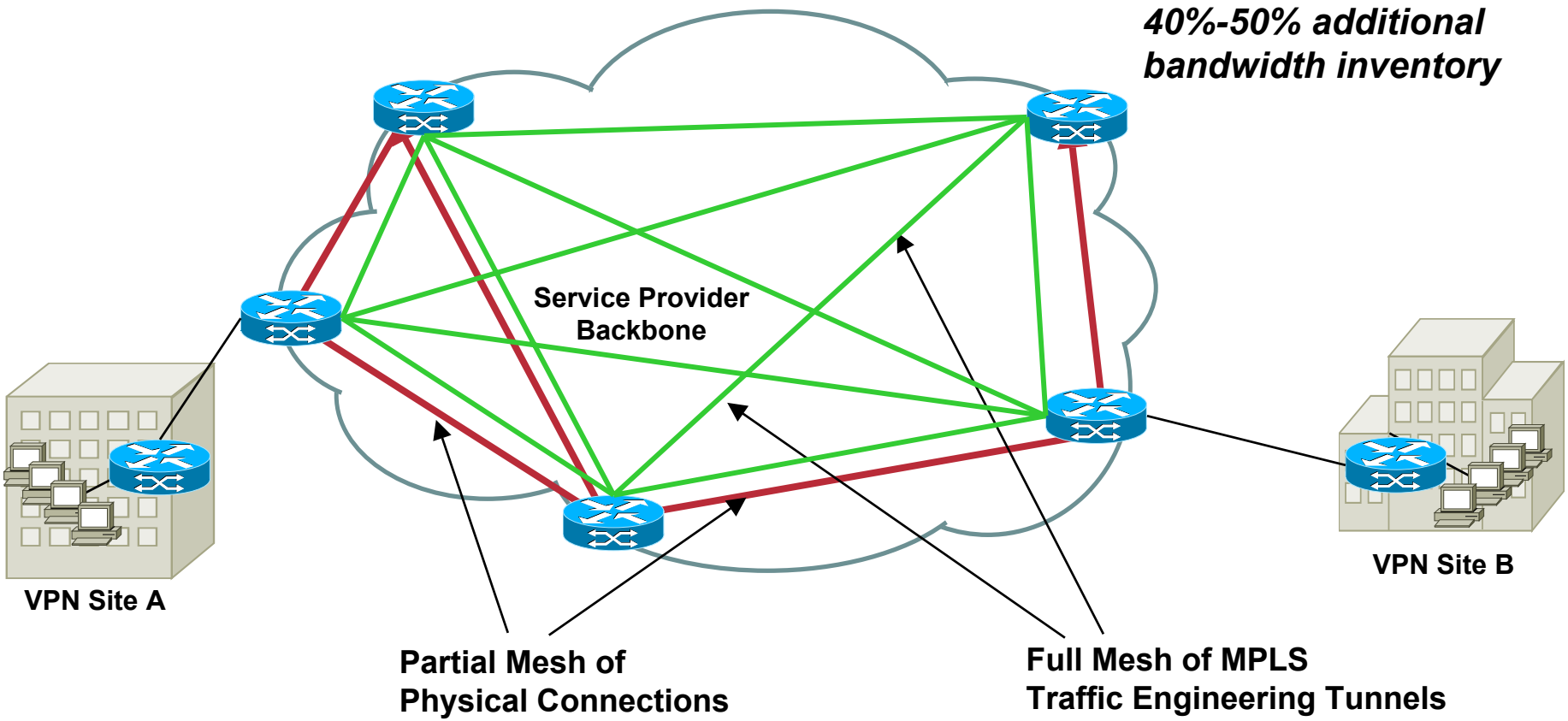
Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – *Primary & Backup*
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

Full-Mesh TE Deployment

Requirement: Need to increase "bandwidth inventory" across the network

Solution: Deploy MPLS TE with a full logical mesh over a partial physical mesh and use Offline Capacity Planning Tool



Operational Issues Raised by Full-Mesh TE

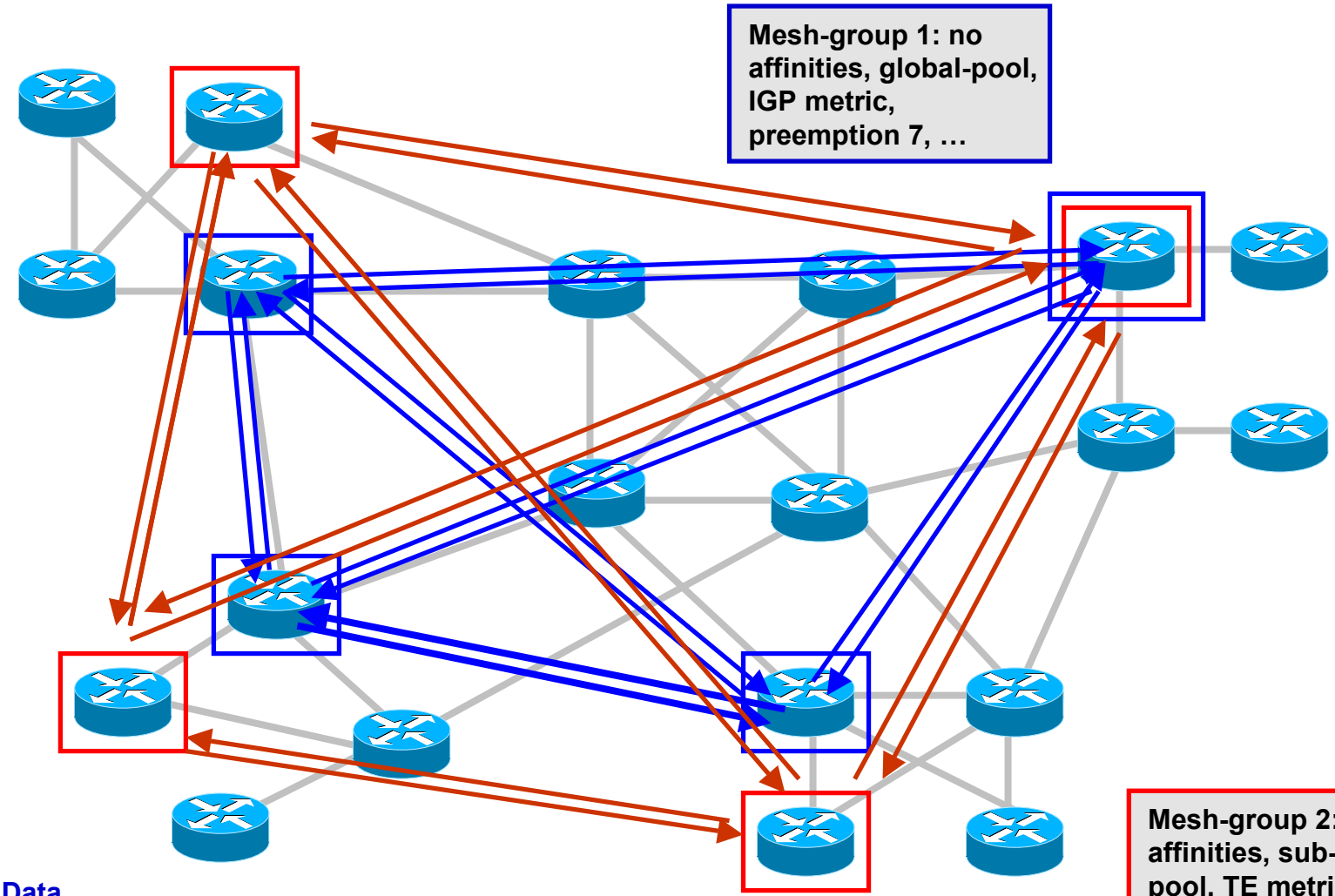
Scenario 1: Transitioning a MPLS network to a TE Full Mesh

- Typically zero bandwidth TE Tunnels are deployed to introduce minimal disruption to existing traffic flows.
- An offline capacity planning tool then modifies the bandwidth constraints of the TE Tunnels and increases network utilization.
- However, still is a lot of configuration = create a full mesh for 100 Routers means 10,000 TE Tunnels.

Scenario 2: Adding Routers to an existing TE Full Mesh

- For 100 Routers in an existing Full Mesh, the 101st Router is added
- TE Tunnels need to be built from the 101st router to every other 100 routers.
- Since TE Tunnels are unidirectional, a TE Tunnel needs to be built from each of the 100 routers

AutoTunnel Mesh Groups



MPLS AutoTunnel: Configuration

- **Enable TE on all routers (member of the mesh group)**
- **Enable AutoTunnel Mesh Groups (global level)**

  router(config)# mpls traffic-eng auto-tunnel mesh
- **Configure ACCESS-LIST (standard IP access list) which defines the set of possible tunnel destination**
- **Configure Auto-Template**

  router(config)#interface Auto-Template 1

  router(config-if)#ip unnumbered Loopback0

  router(config-if)#tunnel mode mpls traffic-eng

  router(config-if)#tunnel mpls traffic-eng autoroute announce

  router(config-if)#tunnel mpls traffic-eng priority 1 1

  router(config-if)#tunnel mpls traffic-eng auto-bandwidth

  router(config-if)#tunnel mpls traffic-eng path-option 1 dynamic

  router(config-if)#tunnel destination access-list 1
- **TE LSP will automatically be set up using the locally configured templates.**

Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – Primary & Backup
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

Service Assurance Agent (SAA) Measuring the Network

- Active Traffic Generation within Cisco IOS Software using SAA Probes
  - "Probe" software configured within Cisco IOS that generates traffic
  - Monitor network performance and health
  - Test and troubleshoot network problems
- Measurement of key end-to-end network metrics
  - Network delay
  - Packet loss
  - Network delay variation (jitter)
  - Connectivity

SAA L3 MPLS VPN Operations Today

SAA for MPLS VPN Operation

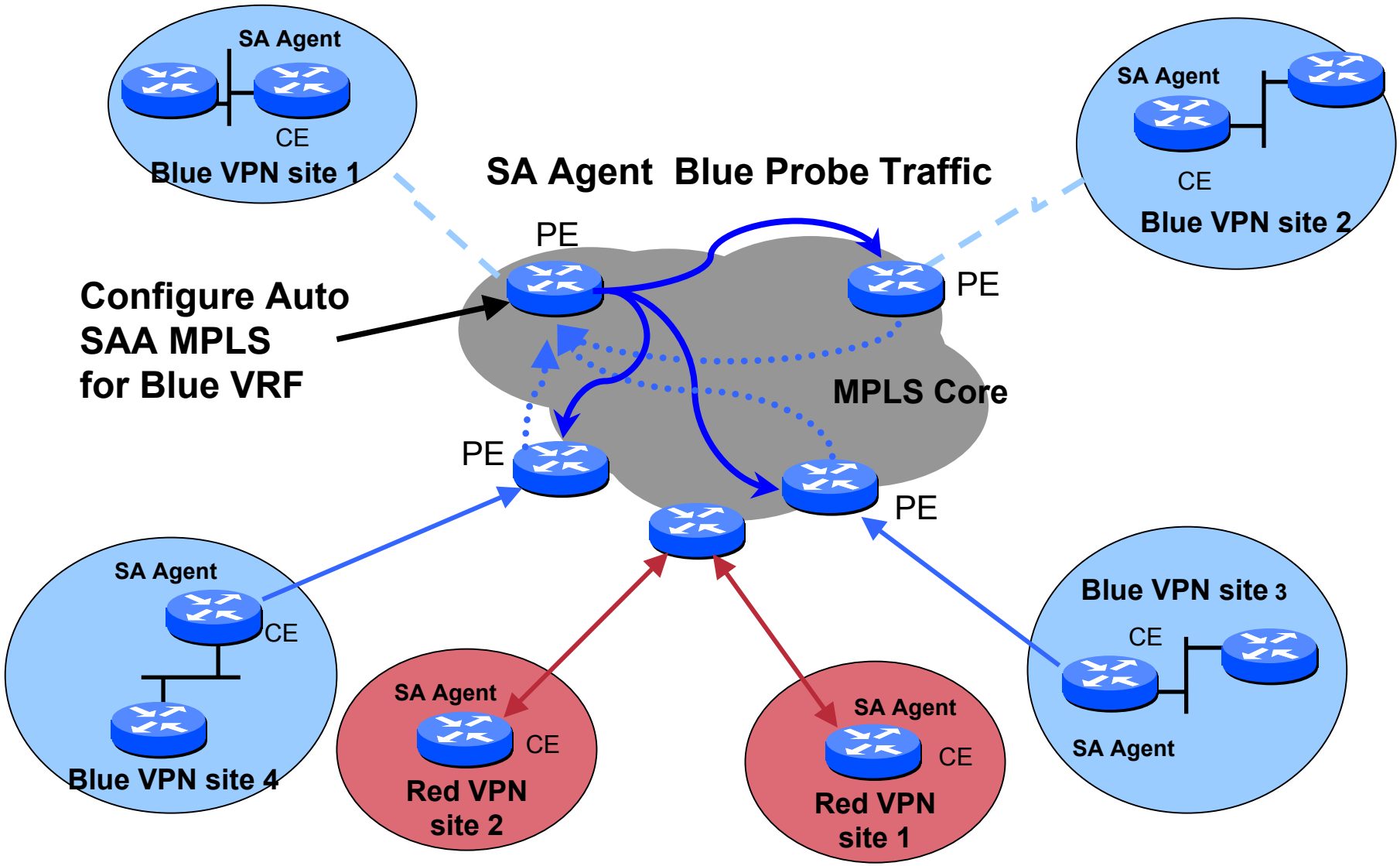
- VRF Aware monitoring
- L3 MPLS VPN SLA measurement
- PE router, multi-vrf CE or dedicated SAA router
- Supported releases 12.2(11)T train and 12.0(26)S, 12.2(20)S

Auto SAA MPLS L3 VPN

Auto SAA for MPLS L3 VPN Embedded Tool provides:

- Automatic connectivity testing of label switch paths
- Proactive monitoring of equal-cost traffic paths between the edges
- Troubleshooting and MPLS forwarding problem isolation
- Use of LSP ping for connectivity testing and network performance monitoring

Auto SAA MPLS L3 VPN



Auto SAA for MPLS Probe Generation

- **Scenario for Probe Generation**
  - ✓ **All PEs participating with VPNv4 are discovered**
  - ✓ **Probes are generated from source to all destination Pes using /32 IBGP VPNv4 loopbacks**
  - ✓ **It is assumed if a probe exists between two PEs it will not be generated again.**
  - ✓ **if a new EXP value is specified a new set of probes is generated**

SAA for MPLS Monitoring Thresholds

- Autoconfiguration will allow thresholds for reaction trigger and trap events
- Reaction trigger sends traps on connection loss, timeout, latency thresholds
- LSP Ping embedded LSP connectivity testing
- Probe will activate at a higher frequency based on threshold violation
  - The higher activation rate is used to isolate network problems

SAA for MPLS Probe Scheduling

Scheduling and Scalability

- Probes will be activated sequentially
- User specifies probe activation interval
  - ✓ Probes are spaced equally using the time interval
  - ✓ Example 60 probes are used to scan with an interval of 5 seconds. Probe activates 5s*60 total scan time of 300s.
  - ✓ Frequency is configurable to overlap activation of probes or create periods of no activation

Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – Primary & Backup
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

Why a New Version 9?

- Fixed export formats are not flexible and adaptable
- With each new version Cisco creates new export fields
- Partners need to reengineer for each new version

Solution: Build a flexible and extensible export format called version 9

NetFlow v9 and IETF

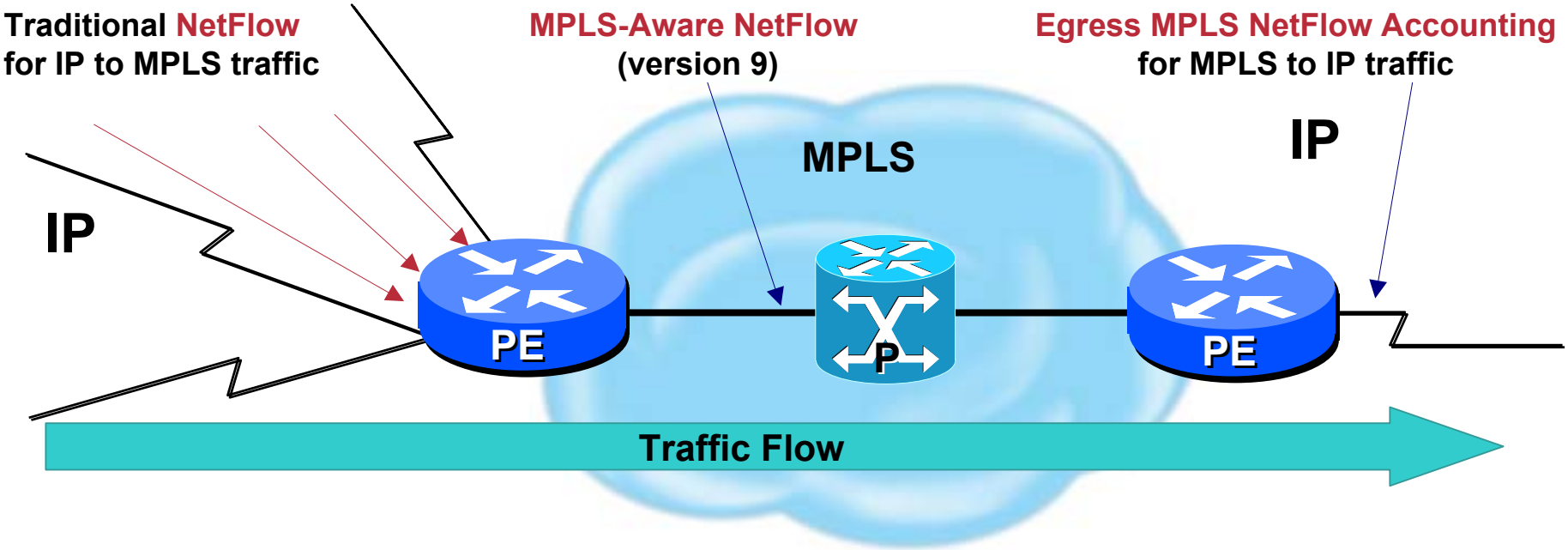
- Internet Protocol Flow Information eXport (IPFIX) is an IETF Working Group

  http://ipfix.doit.wisc.edu/

- NetFlow version 9 is the basis for the standard in the IETF
- Informational RFC on NetFlow version 9

  http://www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt

MPLS



Egress MPLS NetFlow Accounting

- IP information only
- Ideal for billing
- Current availability: Cisco IOS® Software Releases 12.0(10)ST and 12.1(5)T

MPLS-Aware NetFlow (version 9)

- Exports up to three MPLS labels, and IP packet information
- Ideal for Traffic Engineering

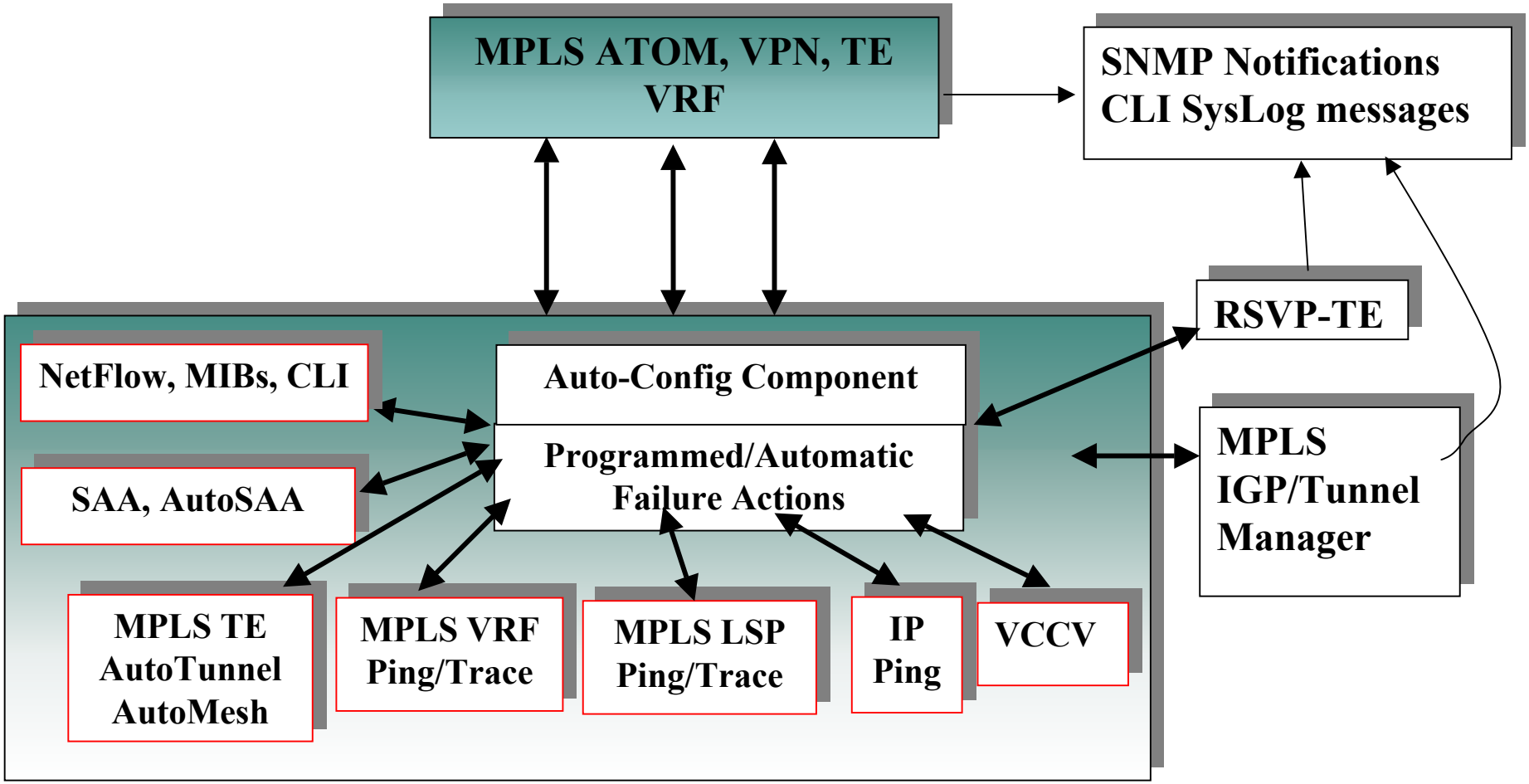
MPLS-Aware NetFlow

- Top Label Export and Destination Prefix advertised by LDP on the MPLS P routers
- Export up to 3 incoming MPLS labels, from positions 1-to-6 in the MPLS label stack
- Experimental bits and end-of-stack bit
- Export label Position
- Type of top label: LDP, BGP, VPN, ATOM, TE Tunnel
- Sampled MPLS-Aware NetFlow
- P router only

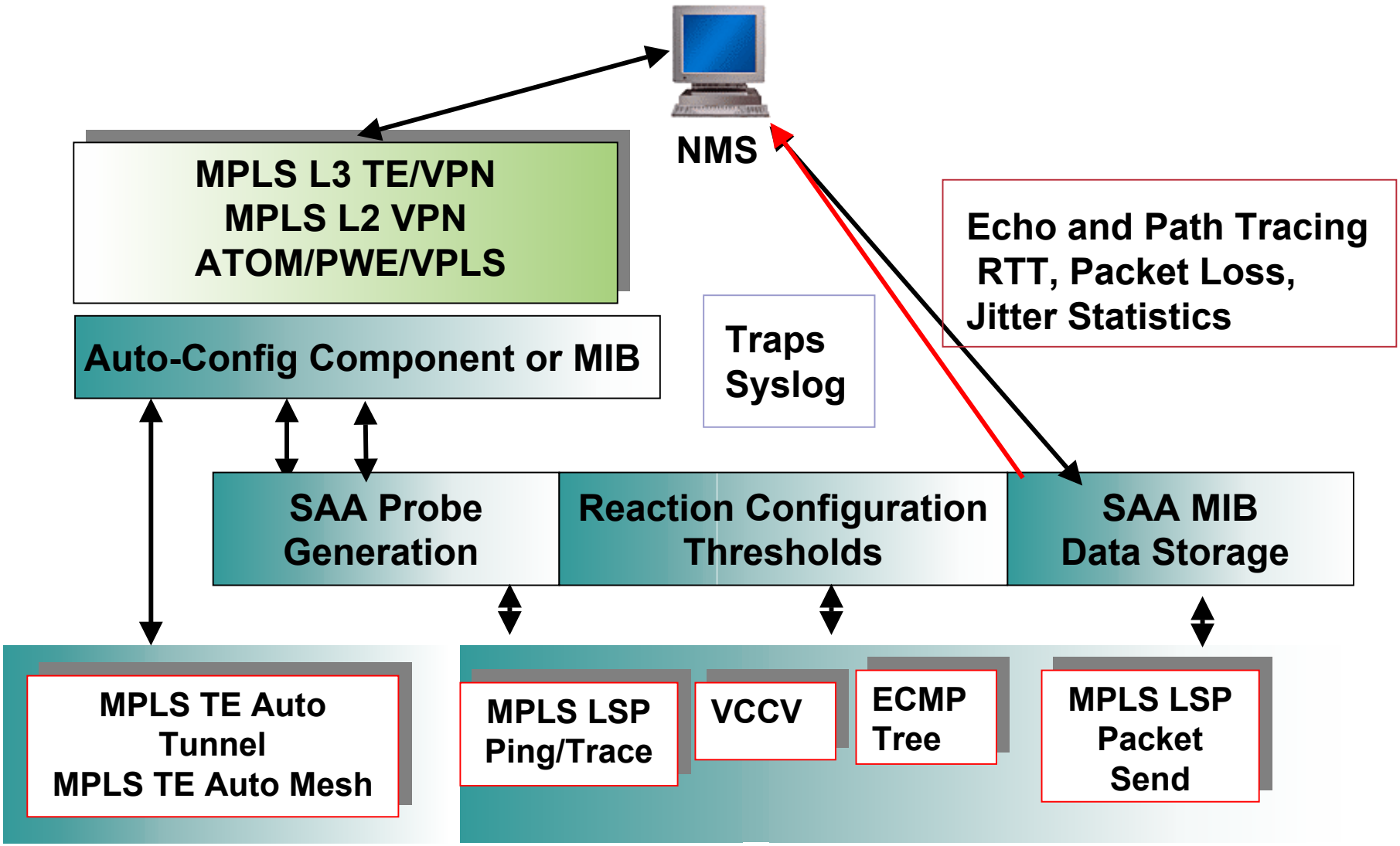
Agenda

- Introduction
- Technical Deployment Overview
  - MPLS Ping/Traceroute
  - VCCV
  - MPLS TE AutoTunnel – Primary & Backup
  - MPLS TE AutoTunnel – Mesh Groups
  - Auto SAA for MPLS
  - MPLS-Aware NetFlow
- Summary
  - Putting It All Together

MPLS Embedded Management



MPLS Embedded Management and Monitoring



Software and Hardware Details

Cisco.com

See reference slide for further details

- LSP Ping/Trace available as of 12.0(27)S with limited ECMP support
  - Supported FEC: LDP IPv4, TE IPv4
- VCCV available as of 12.0(27)S
  - Support both Router Alert (RA) and Control world option
  - On GSR
    - Control Word option: E3 line card is the imposition card
    - Router Alert option: All other line cards and when Egress not E3
- MPLS TE AutoTunnel, AutoMesh as of 12.0(27)S
- Auto SAA for MPLS L3 VPN as of 12.2(RLS5)S
- Note: MPLS L3 VPN Aware SAA Probes Supported as of 12.2(11)T and 12.0(26)S)

World-Class Customer Support

- 2,000 Technical Support Professionals
- 1,600+ Support Engineers* (400 CCIEs) on 24x7
- 630+ Depots and 10,000 Field Engineers in 120 countries*
- 85,000+ Assisted cases/ month
- 321,000 Customer issues resolved/month
- 75% TAC Web resolved: of 25% assisted, 64% were web-initiated
- 98% Material availability
- 92% Orders submitted online, 55% "no touch"
- 60% Change orders submitted online

Cisco.com

Customer Advocacy Mission

Accelerate customer success with Cisco through innovative services and world-class people, partners, process, and tools.

* Internal & Outsource Partners

Cisco leads in the MPLS Market

Cisco.com

Americas	EMEA	AsiaPac/Japan

Over 200 Customers (MPLS Core & L2/L3 Edge)

Cisco IOS MPLS