MPLS Inter-Carrier Interconnect (MPLS-ICI)

An IP/MPLS Forum Sponsored Tutorial

Hari Rakotoranto
IP/MPLS Forum Ambassador
Product Manger
Cisco Systems

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. Summary

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. Summary

Introduction to the IP/MPLS Forum

- IP/MPLS Forum is an international, industry-wide, non-profit association of service providers, equipment vendors, testing centers and enterprise users
  - Created with the name change of the MFA Forum (Oct 2007) to reflect renewed focus on driving global industry adoption of IP/MPLS solutions in the market, by focusing on standardized solutions initiatives for IP/MPLS such as inter carrier interconnect (ICI), mobile wireless backhaul, and security.
- Objectives: Unify service providers, suppliers and end users on common vision of IP/MPLS based solutions

Awareness	Migration	Systems-Level Solutions
• Promote global awareness of the benefits of IP/MPLS • Empower the telecom industry to migrate from legacy technologies to IP/MPLS-based next generation networking	• Guide the telecom end user to make the leap from legacy technologies to IP/MPLS-based services	• Drive implementation of standards for IP/MPLS based solutions • Validate implementations and advance interoperability of standardized IP/MPLS based solutions

- Deliverables: Technical Specifications, Test Plans, Technical Tutorials, Collateral

Introduction to the IP/MPLS Forum

- **Current Work Items**
  - Framework and Reference Architecture for MPLS in Mobile Backhaul Networks
  - MPLS Inter-Carrier Interconnect
  - Generic Connection Admission Control (GCAC) Requirements for IP/MPLS Networks
  - Layer 2 VPNs using BGP for Auto-discovery & Signaling (BGP L2 VPN)
  - MPLS Over Aggregated Interface
  - Voice Trunking format over MPLS
  - TDM Transport over MPLS using AAL1

  The Forum is also planning several industry-driven future Work Items.
- **Service Provider Council**
- **Public Interoperability Events**
- **Technical Tutorials -** to broaden the understanding of the technology and benefits of the solutions
- Next meeting: June 24-26, Vancouver, Canada
- Please join us!
  - **To join the Forum contact Alysia Johnson, Executive Director**

E-Mail: ajohnson@ipmplsforum.org
Phone: 510 492-4057

Technical Tutorials

Introduction to MPLS	½ and full day
MPLS L2/L3 VPNs	½ day
MPLS VPN Security	½ day
Traffic Engineering	½ day
GMPLS	½ day
Migrating Legacy Services to MPLS	½ day
MPLS OAM	½ day
Voice over MPLS	½ day
Multi-service Interworking over MPLS	½ day
Multicast in MPLS/VPLS Networks	½ day
IP/MPLS in the Mobile RAN	½ day
MPLS Inter-Carrier Interconnect	½ day

New tutorials based upon demand

MPLS-ICI Tutorial Contributors

- Nabil Bitar – Verizon
- Rao Cherukuri – Juniper Networks
- Dave Christophe – Alcatel-Lucent
- Anne Exter - Verizon
- Hari Rakotoranto – Cisco Systems
- Paresh Khatri – Alcatel-Lucent
- David Sinicrope – Redback Networks

Agenda

1. Introduction to the IP/MPLS Forum
2. **Today's Challenges**
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. Summary

Today's Challenges

- **Migration away from traditional multiple packet networks towards a converged packet-switched MPLS system. Multiple business drivers:**
  - **CAPEX reduction - Reduce the number of networks by converging several independent networks over a common IP/MPLS network**
  - **OPEX reduction - Fewer networks to manage results in less operational staff, fewer systems and therefore less operational cost**
  - **Improved Return on Investment (ROI): One network that supports multiple services will recoup its costs faster, compared to several separate networks**
- **The Challenge is extending these cost benefits across multiple, inter-connected carrier networks to provide a converged network environment**

Today's Challenges *(continued)*

- Delivery of new value-added capabilities to enable new multi-media content with QoS requirements:
  - IP-VPNs
  - Traffic-engineered data trunks
  - Layer 2 VPN delivery via pseudowires
  - BGP-labeled routes
  - IMS/VoIP
- Delivery of new applications
  - IPTV
  - Gaming
- The Challenge is extending these services and application across multiple, inter-connected carrier networks to provide a seamless service experience

Today’s Challenges *(continued)*

- **Enterprise customers need to seamlessly connect various global locations**
  - **All service providers do not have a complete international footprint**
  - **Some enterprises choose to use multiple service providers even when a single service provider has the required footprint**
  - **Service providers must interconnect their MPLS-based networks with partner providers in order to fulfil enterprise demands for global connectivity and offer a ubiquitous and seamless services experience**
  - **As a result of mergers and acquisitions, some carriers could be providing services across multiple networks**

Today's Solutions

- Bilateral agreements
  - Limited to:
    - Basic IP interconnect OR
    - NNIs for the transport of native layer 2 services such as ATM and Frame Relay OR
    - Ethernet NNIs OR
    - MPLS inter-connects using proprietary bilateral agreements
  - MPLS inter-connects are limited
    - Concerns about security and the need for a greater degree of co-operation required at the control plane layer
    - Differing QoS attributes and capabilities between different providers (standardization may not be possible for all but the most generic cases)
  - Different agreements used by different providers

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. **MPLS-ICI Overview**
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. Summary

Objectives

MPLS Inter-Carrier Interconnect Technical Specification - IP/MPLS Forum work in progress

- To provide a framework to facilitate bilateral agreements between Service Providers and expand the scope of MPLS interconnects to carry a variety of Layer 1, 2 and 3 services
- To address the following inter-connect issues:
  - Methods for the establishment of Label Switched Paths (LSPs)
  - Signaling and routing protocols
  - Resiliency
  - Traffic management and Quality of Service (QoS)
  - Security
  - Operations, Administration and Maintenance (OAM)
  - Packet forwarding
  - Security requirements

Objectives *(continued)*

- **To provide a vital tool in reducing service providers' costs and adding value to their customers by enabling "next-generation" services such as VoIP, IPTV, Layer 2 VPN, IP-VPN and many other services on a seamless, global basis**

Services Covered

- Four common MPLS services are addressed in the first phase:
  - Inter-carrier (BGP/MPLS) IP VPN services
    - RFC4364 – Multi-AS Backbone Option A
    - RFC4364 – Multi-AS Backbone Option B
  - Labeled IPv4 routes using BGP
    - RFC3107 (Carrying Label Information in BGP-4) – For label switching IPv4 inter-domain traffic.
  - Pseudowires (e.g., emulated Layer 1 and Layer 2 services over an MPLS network)
  - Inter-domain traffic-engineered trunks for traffic with specific bandwidth and QoS requirements
- Makes use of existing standards for signaling, routing, security and OAM mechanisms

Future Phases

- Future phases may cover:
  - Methods to use dynamically established multi-segment pseudowires
  - Other advanced OAM capabilities
  - New applications or services

Challenges

- The MPLS-ICI specification helps with technical inter-connectivity issues but other challenges may still remain:
  - Inter-provider commercial arrangements still maintain complexity due to differences in provider QoS offerings and capabilities
  - All carriers are different!

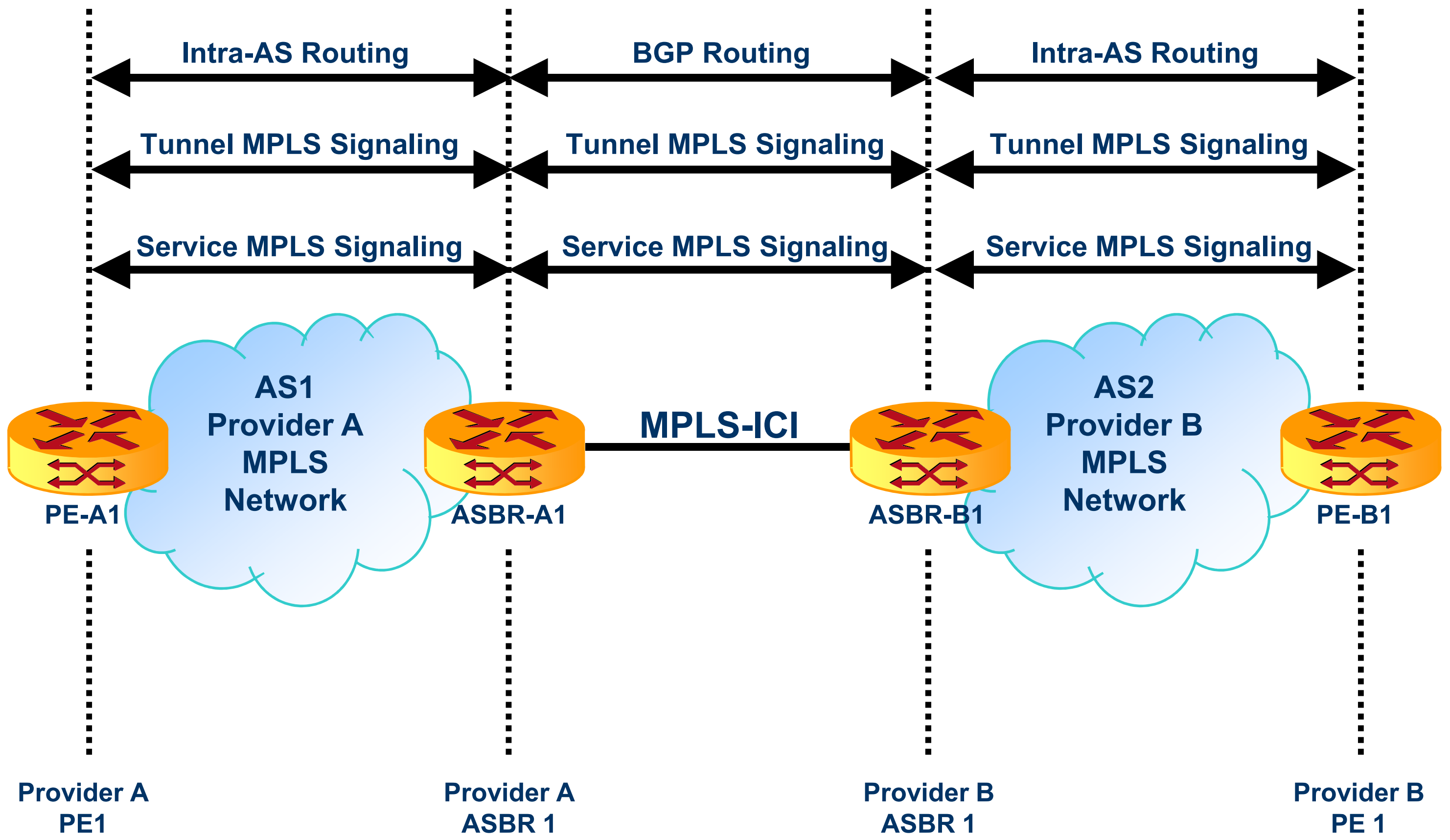
MPLS-ICI Technical Overview

- MPLS-ICI is a bi-directional logical link between two carriers' autonomous system border routers (ASBRs) over which packets of an MPLS service and associated control protocols are exchanged
- Focus of MPLS-ICI Technical Specification:
  - Actions and policies associated with processing and forwarding packets over an MPLS-ICI
  - Control plane protocols involved in:
    - Setup of a label switched path (LSP) over an MPLS-ICI
    - Signaling
    - Routing
    - Management
    - Security
- Assumes two different carriers at the end-points of the MPLS-ICI
- Does not preclude end-end LSPs traversing more than two carriers
  - But, an inter-carrier interconnection is, by definition, between two carriers' ASBRs

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. **Reference Architecture**
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. Summary

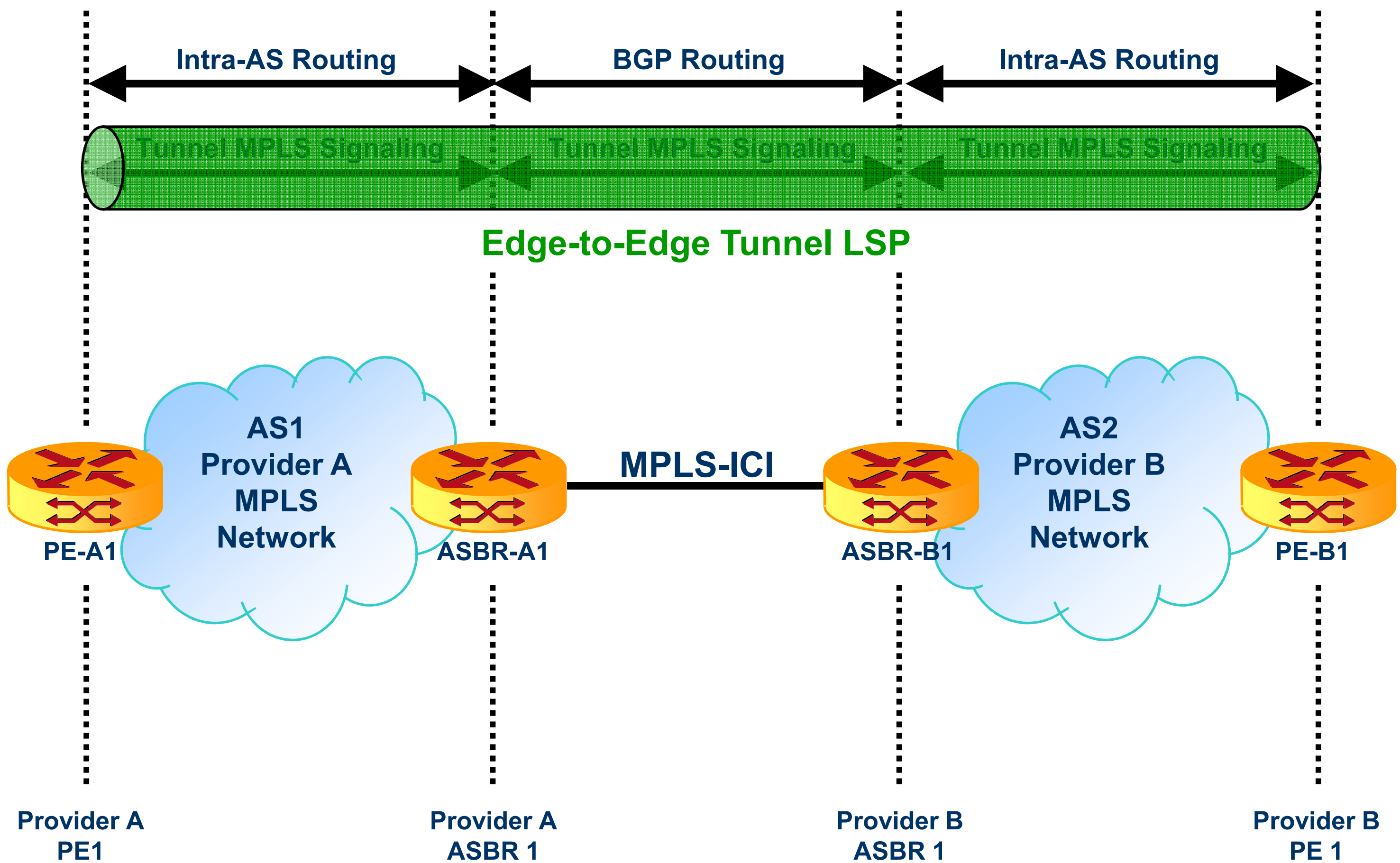
Reference Architecture



Reference Architecture

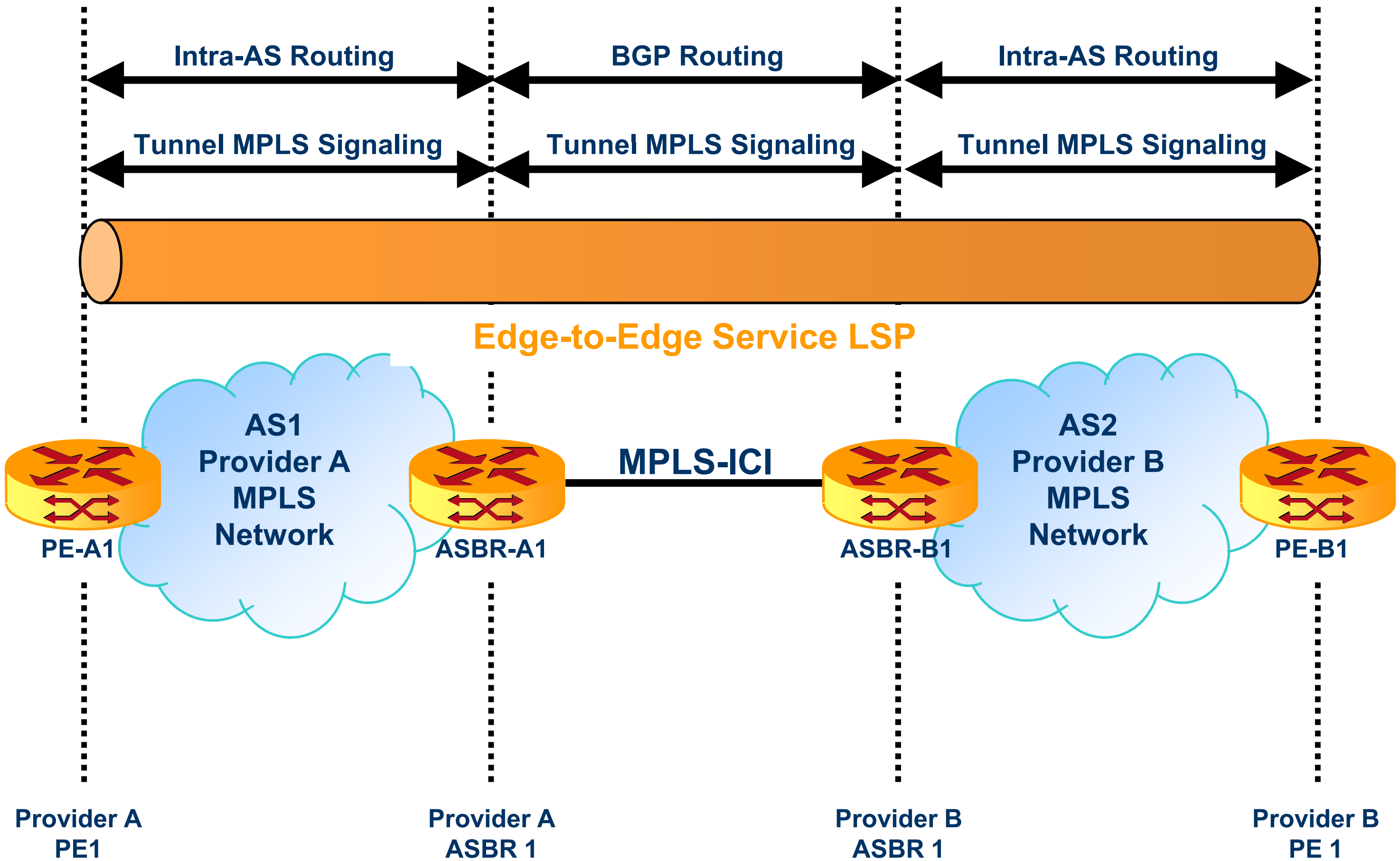
- Control plane processes operate in specific areas
  - Routing ASs
    - iBGP
    - eBGP
    - IGP
  - LSP segments
    - Tunnel LSP segments
    - Service LSP segments e.g. pseudowire LSP segment or BGP/MPLS IPVPN LSP segment
  - Each segment spans a single provider or the MPLS-ICI
  - Prevents sensitive information such as link state details and topology information about the network crossing the AS boundaries
- Edge-to-edge MPLS services are constructed by concatenating individual tunnel or service LSP segments at their respective layers

Reference Architecture



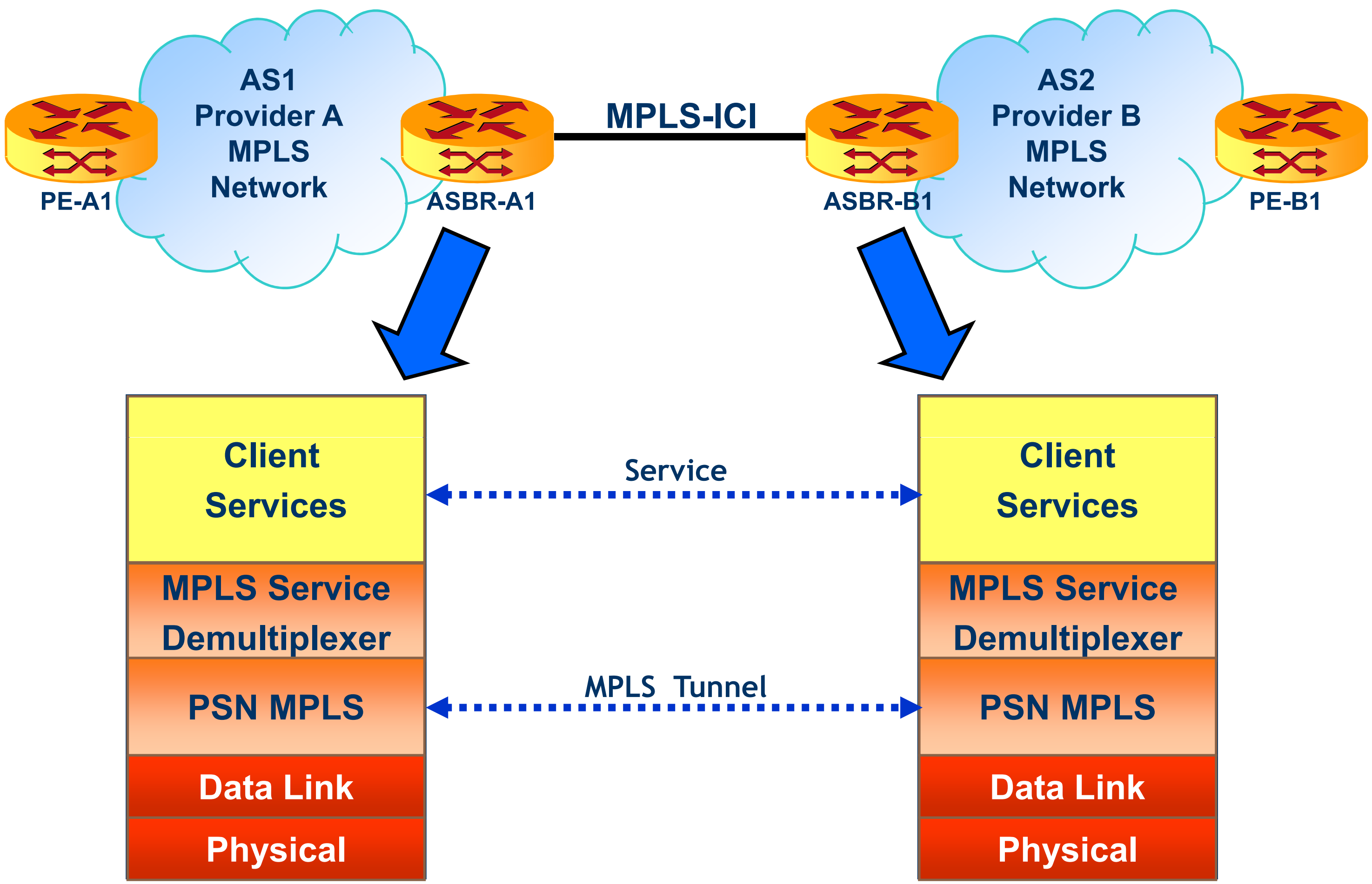
Edge-to-Edge Tunnel LSP

Reference Architecture



Edge-to-Edge Service LSP

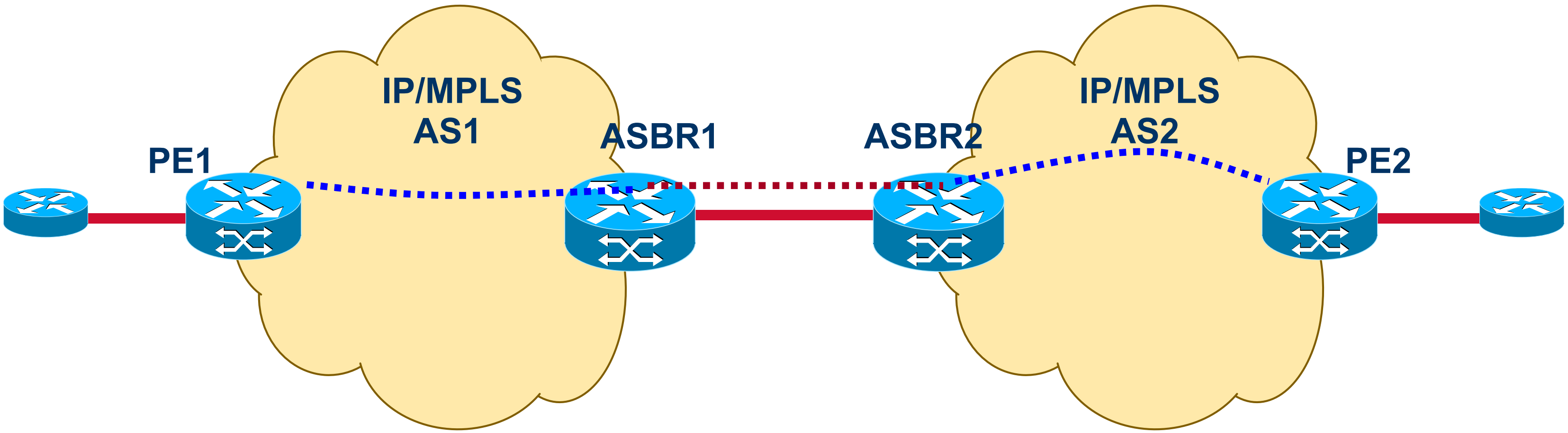
Reference Architecture



Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. **Mechanisms for LSP Establishment**
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. Summary

LSP Setup at ICI



- **Three mechanisms of LSP establishment across a provider domain boundary are defined:**
  - **All-static configuration**
  - **Statically configured and signalled establishment**
  - **Dynamic establishment**

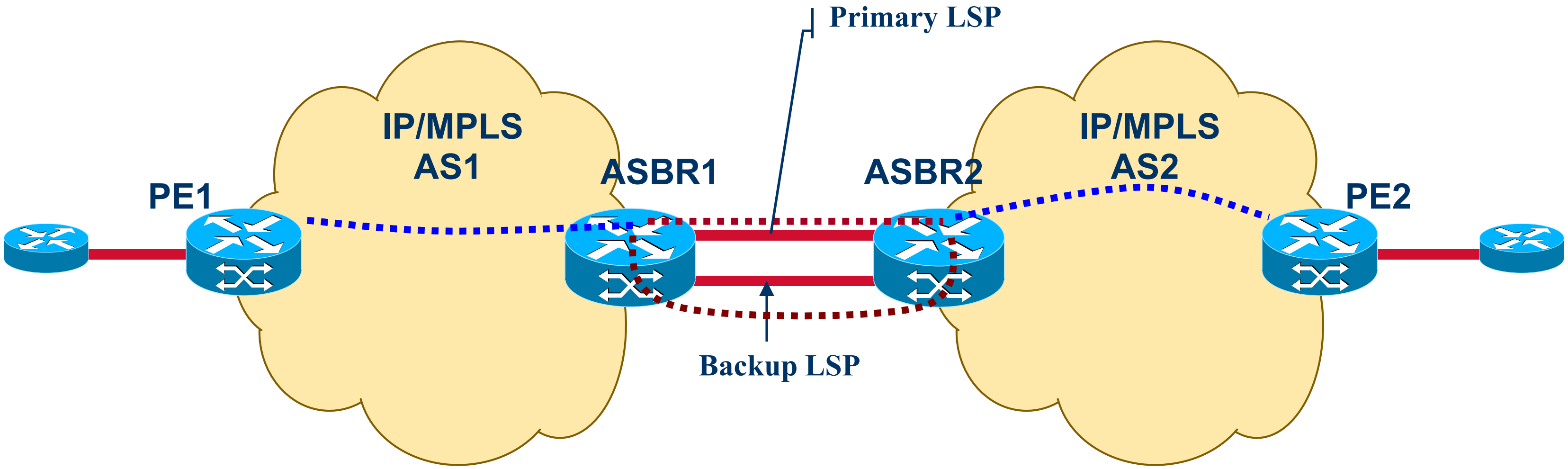
LSP Setup at ICI - Drivers

- Satisfy various interconnect models that fit providers' policies on security, information sharing and setup control
- May help the timely development of solutions
  - e.g., Static configuration may involve the least amount of development and have the least amount of interoperability issues
- Different scenarios for InterCarrier LSP setup are applications dependent

Resiliency / Protection at ICI

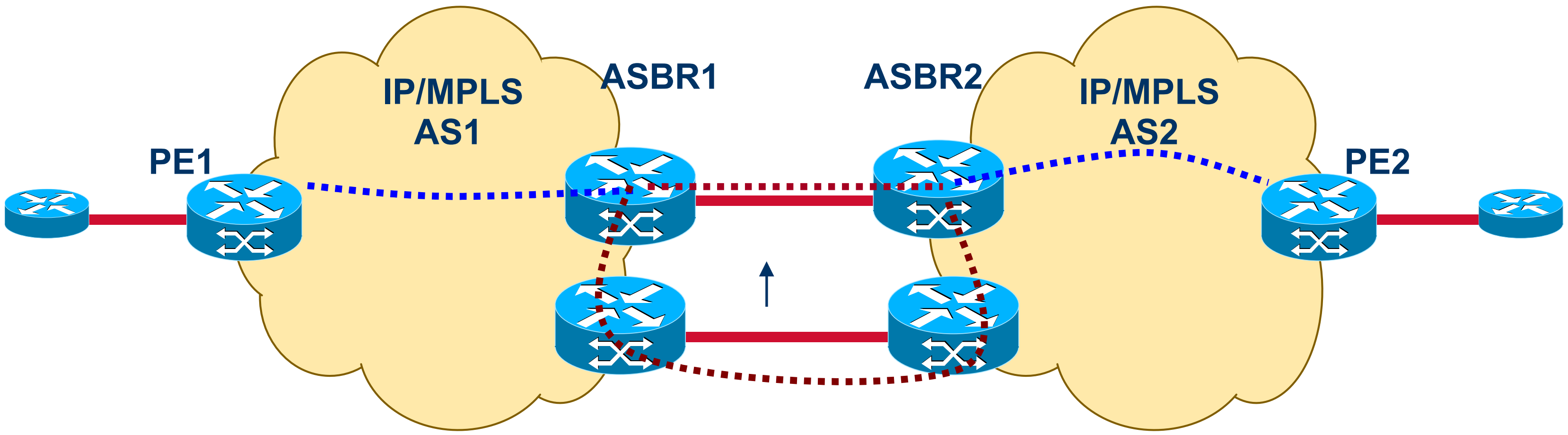
- **Resiliency:**
  - **Across the MPLS-ICI interface (e.g. against link failure between ASBRs)**
  - **Usually on a per LSP basis**
- **Protection Models:**
  - **Reroute around a link failure**
  - **One hop MPLS-ICI protection**
  - **Multi-hop LSP protection over an MPLS-ICI (including TE tunnel)**

Protection Model – One hop protection



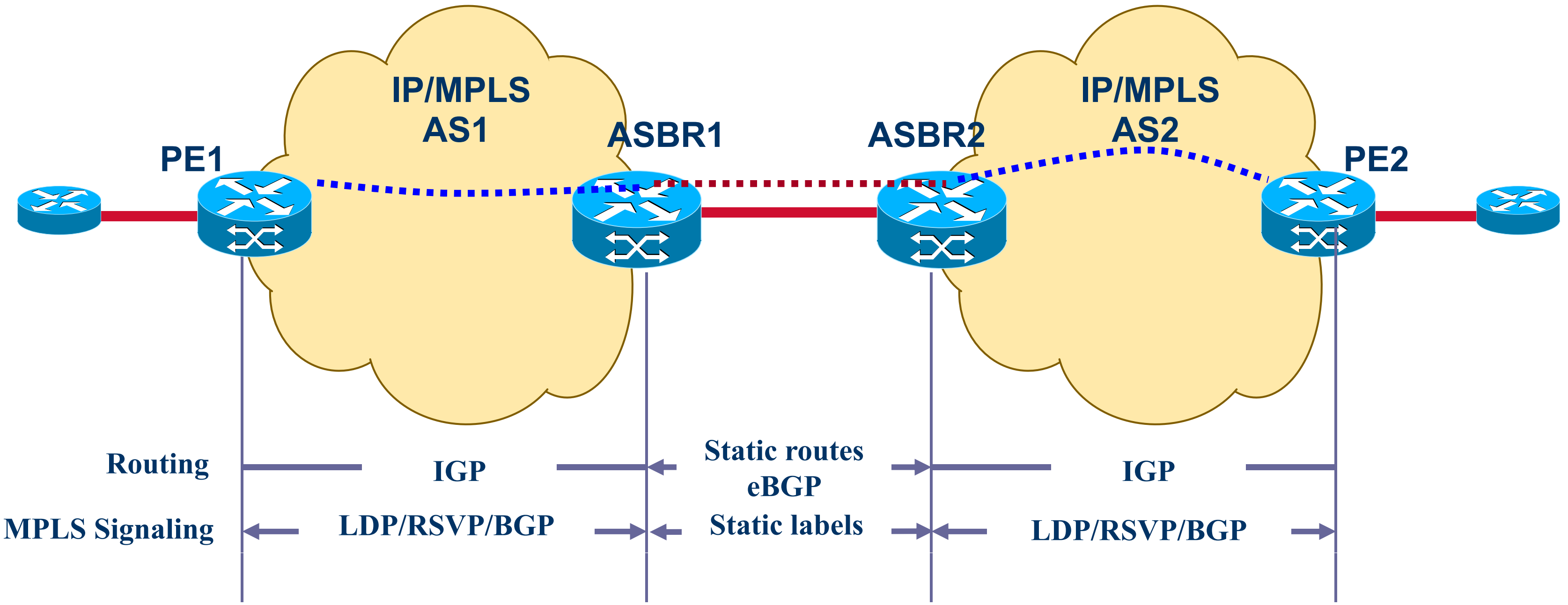
- Multiple parallel links between ASBRs
- Require configuration of primary and backup standby LSPs between ASBRs
- Failure detection protocols run between ASBRs
- Upon failure, each ASBR is in charge of forwarding traffic into the redundant path

Protection Model – Multi-Hop protection



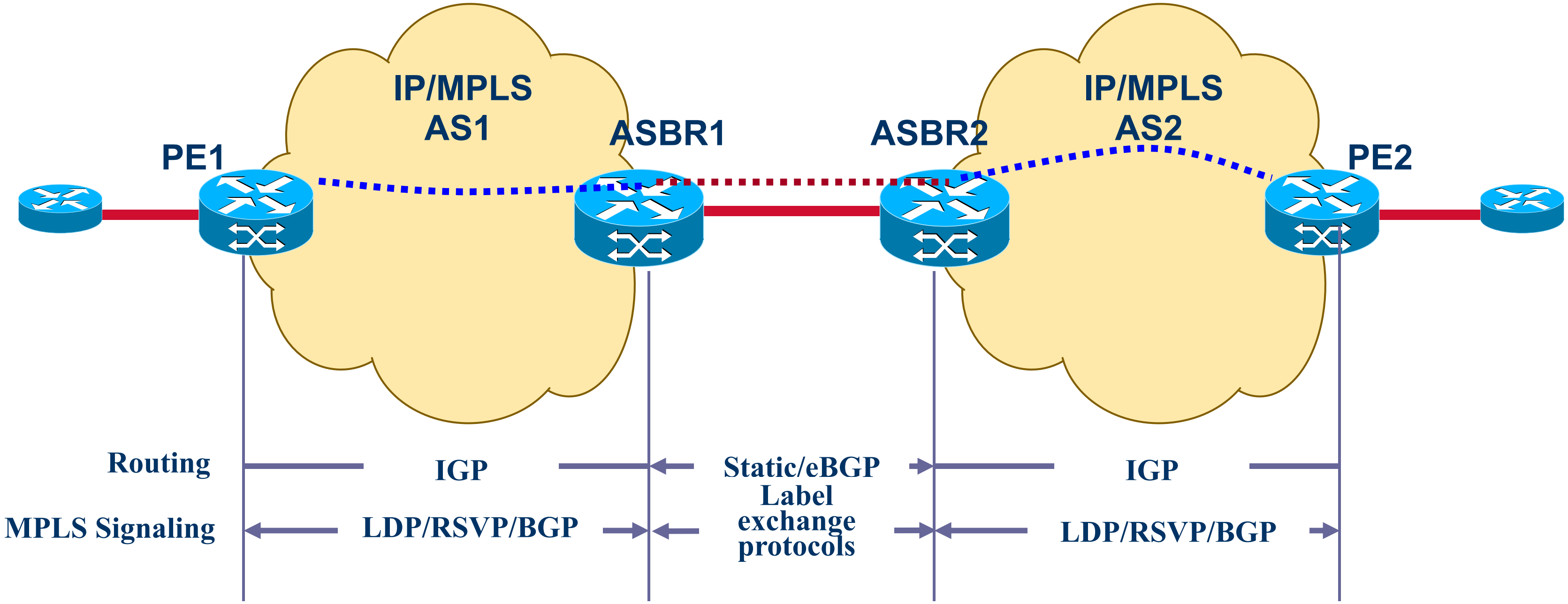
- Require configuration of primary and redundant tunnel LSPs between ASBRs
- Redundant LSP might span across multiple hops
- Upon failure, each ASBR is in charge of forwarding traffic into the redundant path

LSP Setup Mechanisms – All Static configuration



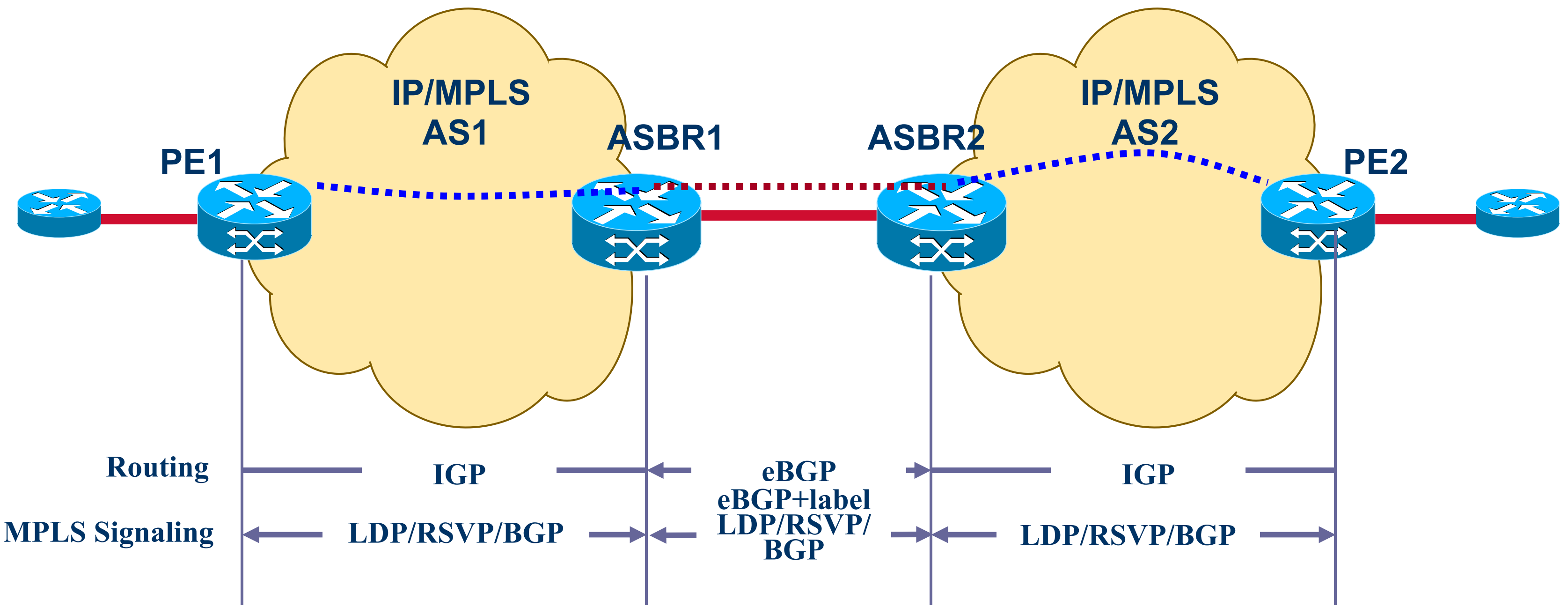
- Mainly applies to Static LSPs for PW and MPLS tunnels
- Matches current practices in establishing Inter-Carrier L2 circuits
  - Reduces some of the security concerns associated with dynamic signaling and provides for simplicity in admission control at the boundaries
- How it works:
  - Configuration of the endpoints of an LSP (segment) on the ASBRs, each belonging to a respective carrier
  - No MPLS signaling
  - MPLS labels are manually assigned
  - Manual resiliency configuration

LSP Setup Mechanisms – Statically Configured & Signaled establishment



- **How it works:**
  - Pre-determined routing
  - Configuration of the endpoints of an LSP (segment) on the ASBRs, each belonging to the respective carrier
  - Signaling protocol manages label assignment

LSP Setup Mechanisms – Dynamic setup



- **How it works:**
  - **Dynamic routing and signaling**
  - **Label distribution protocol used on the ICI interface: eBGP+label, LDP, RSVP**

Routing Considerations

- How to enable routing on the MPLS ICI interface while sharing no topology information across the two carriers?
- How to support the various methods of setting up LSPs
  - Depends on the use cases
- Focused on BGP as the routing protocol between two carrier domains – natural choice

Signaling Considerations

- MP-BGP for signaling
  - Support for IPVPN routes (RFC 4364)
  - BGP+label (RFC 3107) for IPV4 routes on the inter-carrier interfaces
- Inter-domain RSVP-TE
  - To set up data trunks with TE-constraints
  - More on this later

MPLS-ICI Alternatives Side by Side

Alternative	Characteristics
Static setup	• **Administratively/manually configure the endpoints of an LSP (segment) on each ASBR** • **MPLS labels are administratively/manually assigned** • **Used to satisfy security requirements** - **No signaling between domains** - **Require hiding PE reachability**
Statically configured & Signaled LSP setup	• **Administratively/manually configure the endpoints of an LSP (segment) on each ASBR** • **Signaling protocol manages MPLS label assignment** • **No reachability information shared between ASs**
Dynamic setup	• **Dynamic routing and signaling - simple provisioning on ASBRs** • **Signaling can be End-to-End or on per Segment basis** • **Dynamically established resiliency and/or re-rerouting under failures**

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. **CAC and Forwarding**
7. OAM
8. Security
9. Applications
10. References
11. Summary

Connection Admission Control (CAC)

- Connection Admission Control (CAC) must be supported at the MPLS ICI to ensure
  - Consistent admission of traffic on to resources
  - SLA of traffic is met
- CAC can be provided
  - By the ASBRs themselves or
  - Via an element manager or bandwidth management system
- Use of offline CAC tools is not prohibited

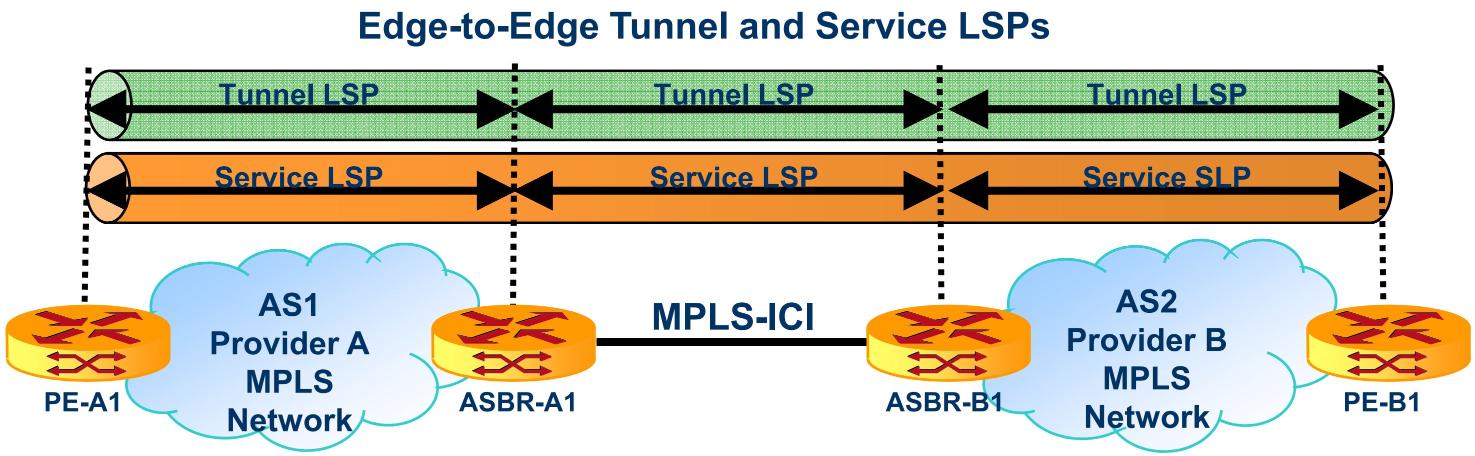
Traffic Management and Forwarding

- MPLS-ICI provides
  - Traffic policing
  - Traffic shaping
  - QoS marking and mapping
    - Marking of QoS via EXP bits
      - QoS markings must be mapped between one provider and another
      - QoS marking must be mapped to DiffServ classes for proper queuing
    - Basic Diffserv (or MPLS-Diffserv as in RFC3270)
    - MPLS TE
    - Diffserv-aware TE (DS-TE)
    - Aggregate RSVP (RFC 3175)
    - Inter-AS TE
  - Path MTU Handling
    - Path MTU discovery supported
    - Label stack depth must be accounted for
  - Load Balancing and ECMP
  - Time to Live

Agenda

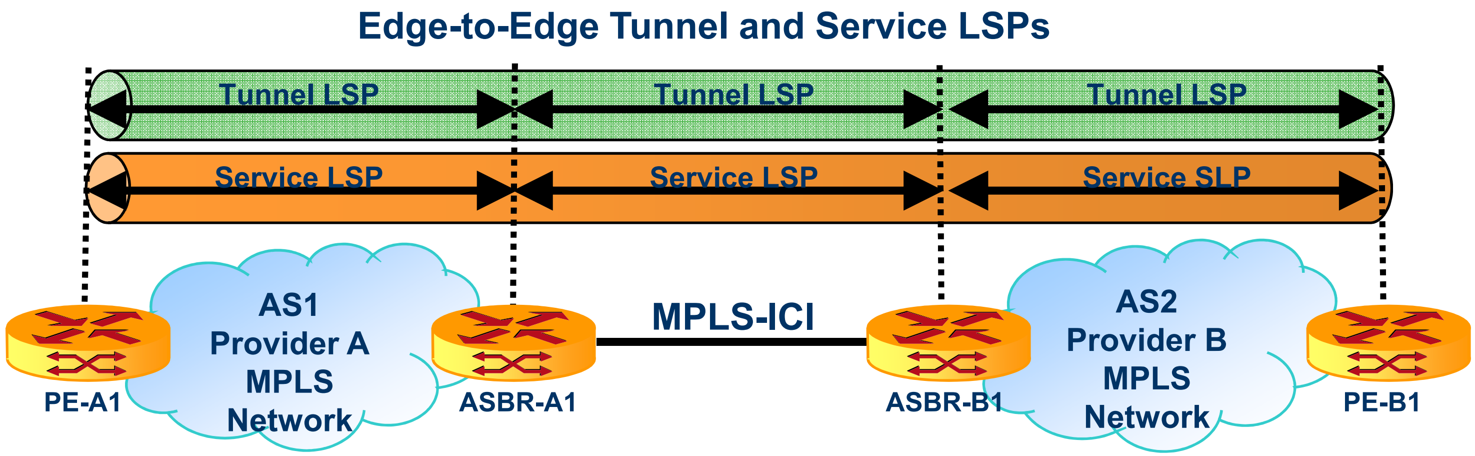
1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. **OAM**
8. Security
9. Applications
10. References
11. Summary

OAM Overview



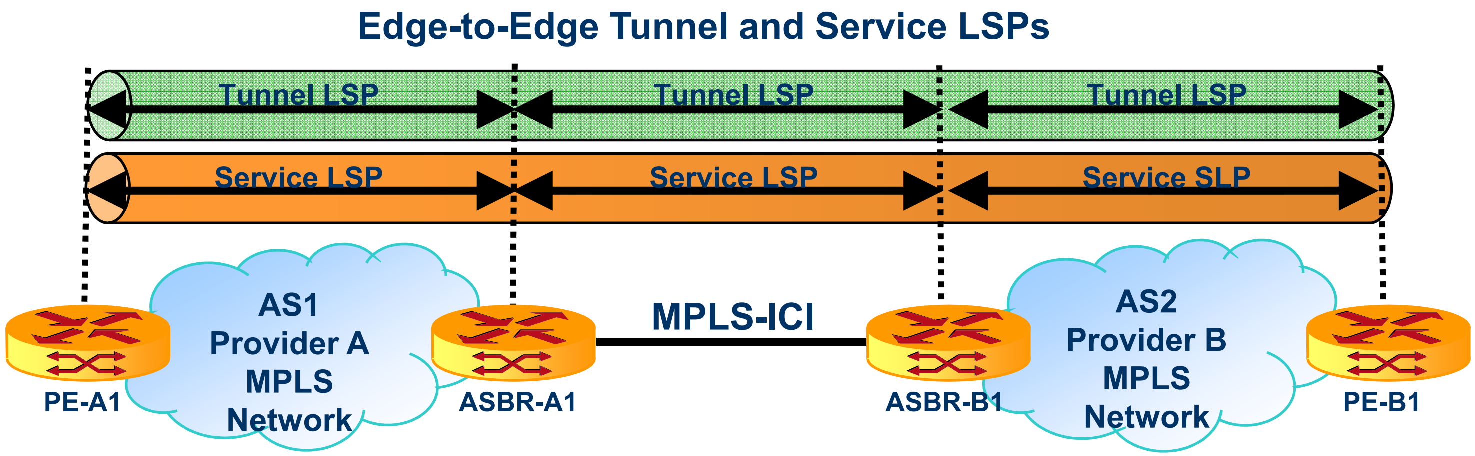
- Focus is on OAM capabilities that apply to:
  - LSP segments established across MPLS-ICI
  - Other segments of the same LSP extending beyond MPLS-ICI
- LSP segment established across M-ICI is a segment of LSP that extends PE to PE and is dynamically or statically established and stitched
- ASBR OAM capabilities for MPLS-ICI support:
  - Always on defect detection and handling
  - On demand diagnostics
- Capabilities apply to OAM packets that are destined to ASBRs interconnected by a MPLS-ICI
- Complements existing OAM capabilities within AS

OAM
Connection Verification



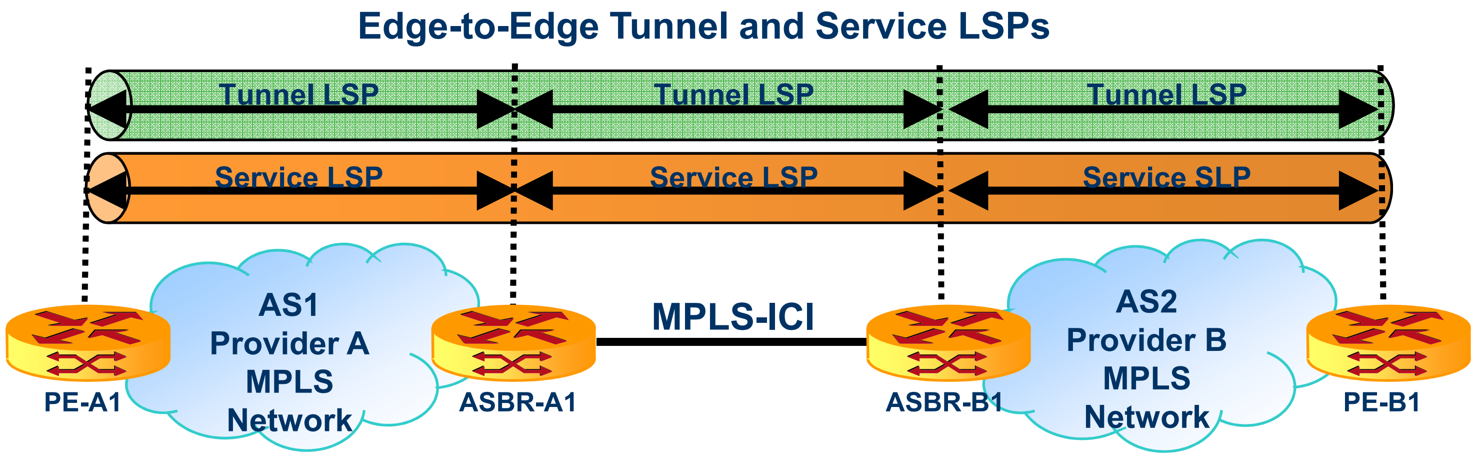
- **Always on defect detection and handling**
- **ABSR supports Bidirectional Forwarding Detection (BFD) in asynchronous mode that includes support of:**
  - **Timer Parameters:**
    - Time interval between successively transmitted protocol messages per LSP
    - Minimum receive interval for protocol messages per LSP
    - Failure detection criteria in terms of the number of successive messages that must be lost to trigger the declaration of an LSP down that is configurable per LSP
  - **Failure notification:**
    - Sending an SNMP trap upon LSP failure detection
    - Notify all client protocols that depend on the liveliness of the LSP being monitored when that LSP fails

OAM
Connection Verification (continued)



- ABSR acting as an endpoint for LSP or LSP segment must be able to divert OAM related DoS attacks by:
  - Dropping the BFD protocol messages received on an LSP if the protocol is not enabled for that LSP
  - Policing BFD protocol messages to enforce the message rate configured for all LSPs on an MPLS-ICI
    - Per-LSP policing is optional
- Policing BFD messages used for liveliness check may result in a false failure detection → Set policing parameters so "legitimate" messages used for liveliness check are not impacted by policing unless they exceed their allocated rate

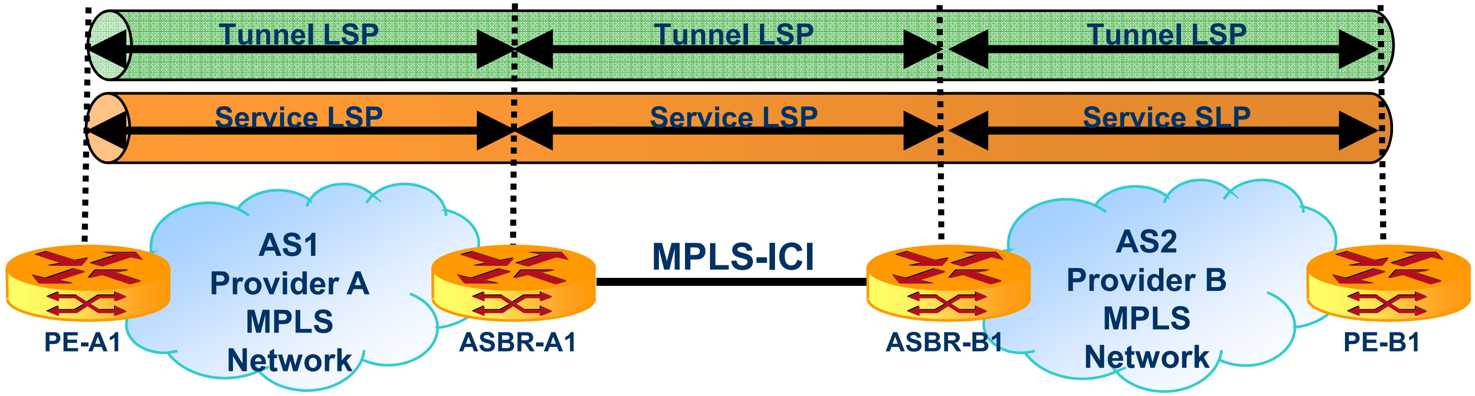
OAM
Connection Verification (continued)



- ABSR allows an MPLS BFD session per LSP
- An LSP extended between ASBRs can be stitched to other LSP segments to form an end-end LSP → a BFD session that runs end-to-end between the LSP endpoints that is transparent to the ASBRs
- ASBR supports the co-existence of an end-to-end BFD session and a BFD session between the ASBRs for an LSP segment
- MPLS packets carrying the BFD messages corresponding to the ASBR BFD sessions have TTL set to 1 to force these messages to be processed at the ASBRs rather than be switched across

OAM
Connection Verification (continued)

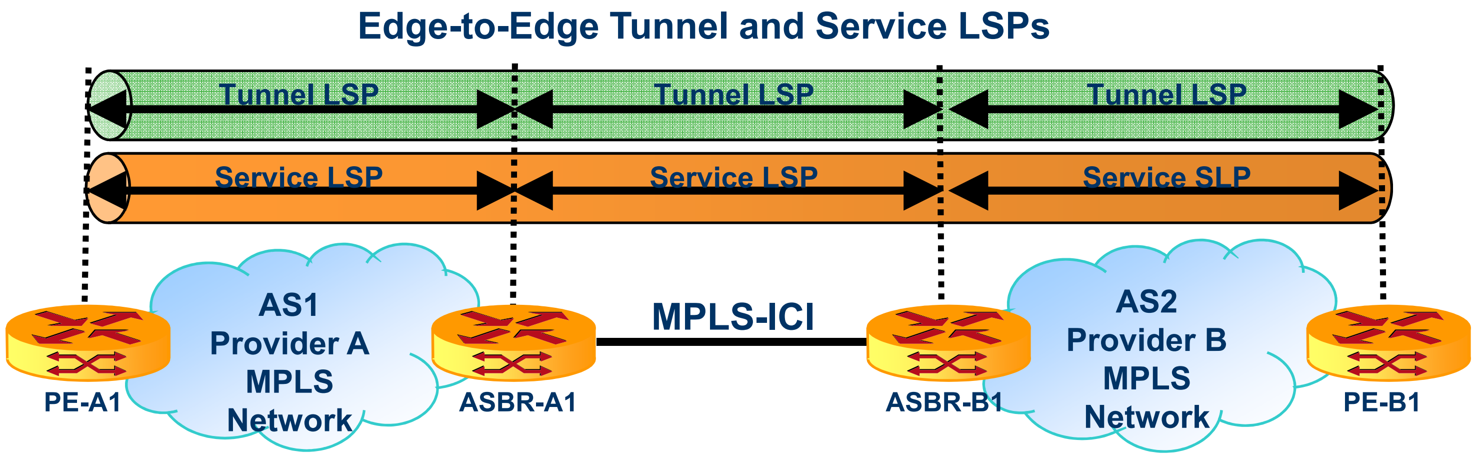
Edge-to-Edge Tunnel and Service LSPs



- ASBR supports the authentication option for multi-hop and single-hop BFD sessions between two ASBRs
- Where applicable, authentication must be enabled by configuration and the same key or password sharable for all sessions between the same ASBR pair using the same authentication method
- ASBR supports the bootstrapping method via MPLS ping for exchanging Your Discriminator and My Discriminator values used in BFD control messages
- ASBR supports the configuration of:
  - **Local Discriminator for a BFD session** (My Discriminator value in the BFD messages the ASBR sends to the peer ASBR at the other end, and Your Discriminator value in the BFD messages it receives for the session)
  - **Peer ASBR Discriminator for a BFD session** (My Discriminator value in the BFD messages the ASBR receives from the peer ASBR at the other end, and Your Discriminator value in the BFD messages it sends for the session)

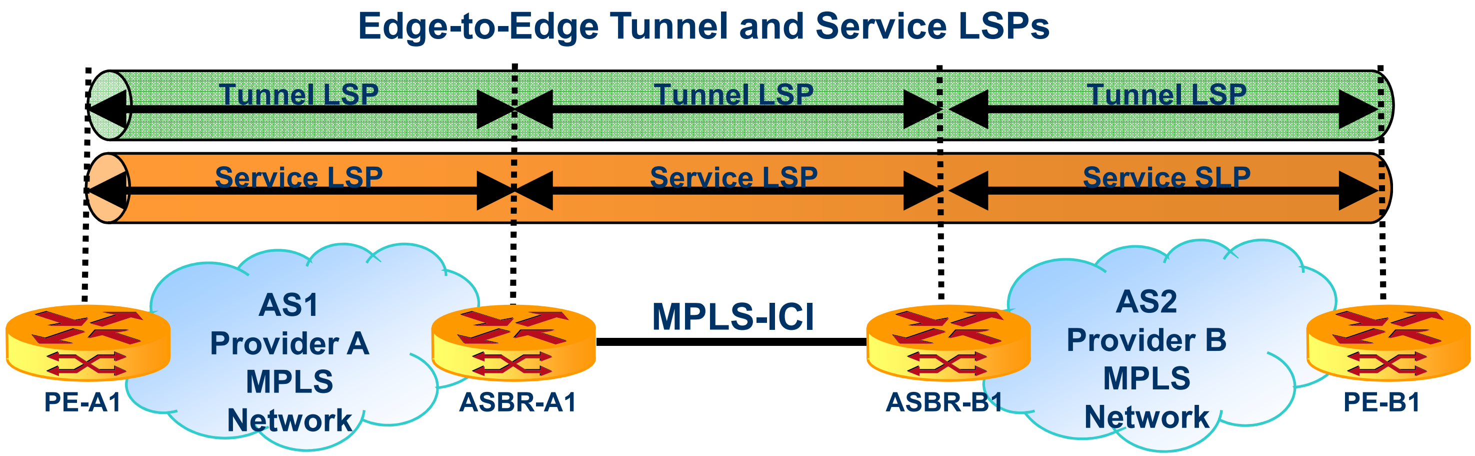
OAM

On Demand Diagnostics



- ASBR supports:
  - LSP ping [RFC4379] in both ping and trace modes to verify unidirectional connectivity and perform path tracing of MPLS label switched paths on MPLS-ICI segments
  - BFD in echo mode for performing loopback tests
- LSP ping
  - Support of LSP ping in ping mode enables the checking of:
    - Liveliness of the LSP
    - Data plane state against the control plane state for that LSP
  - Applies to LSPs with endpoints on the ASBRs at either end of an MPLS-ICI

OAM
On Demand Diagnostics

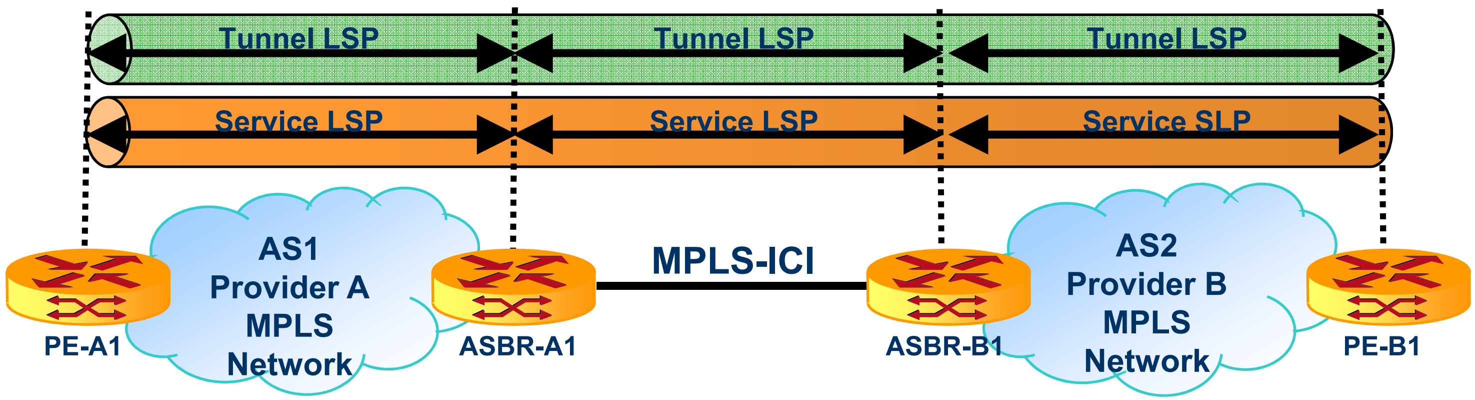


- LSP ping *(continued)*
  - LSP may be a segment of an end-to-end LSP that extends beyond the MPLS-ICI
  - LSP ping messages for LSPs that do not terminate on an ASBR MPLS-ICI transit the MPLS-ICI
  - ASBR supports the associated LSP ping Forwarding Equivalence Class (FEC) sub-Type Length Value (sub-TLV) and stackings for specific applications

LSP ping FEC and sub-TLV

Application	Sub-type	Length	Field Value
TE-Tunnels	3	20	RSVP IPv4 LSP
IP VPN	6	13	VPN IPv4 prefix
Pseudowires	8	14	L2 VPN endpoint
Pseudowires	10	14	“FEC 128” Pseudowire
Pseudowires	11	16	“FEC 129” Pseudowire
Labeled IPv4 routes	12	5	BGP labeled IPv4 prefix

OAM
On Demand Diagnostics

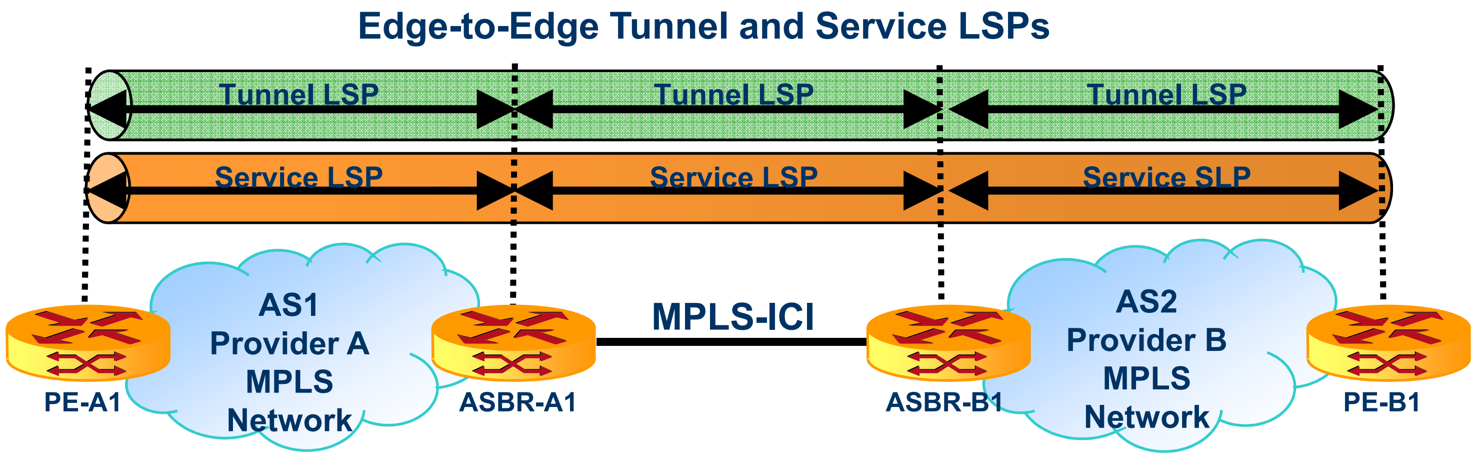


- ASBR LSP ping support *(continued)*
  - LSP ping reply modes specified in RFC4379
  - Reply mode should not include the router alert option → Prevent ping replies originated in one provider domain to be processed on every router in another provider domain on the path
  - Configure to drop or rate-limit received echo reply packets with the router alert option → avert overloading or attacking ASBR control plane and that of other routers within the ASBR AS
  - Alternative to avoiding DoS attacks is to transparently pass the packets with the router alert option → also prevents processing other packets with the router alert option

LSP Ping Reply Modes

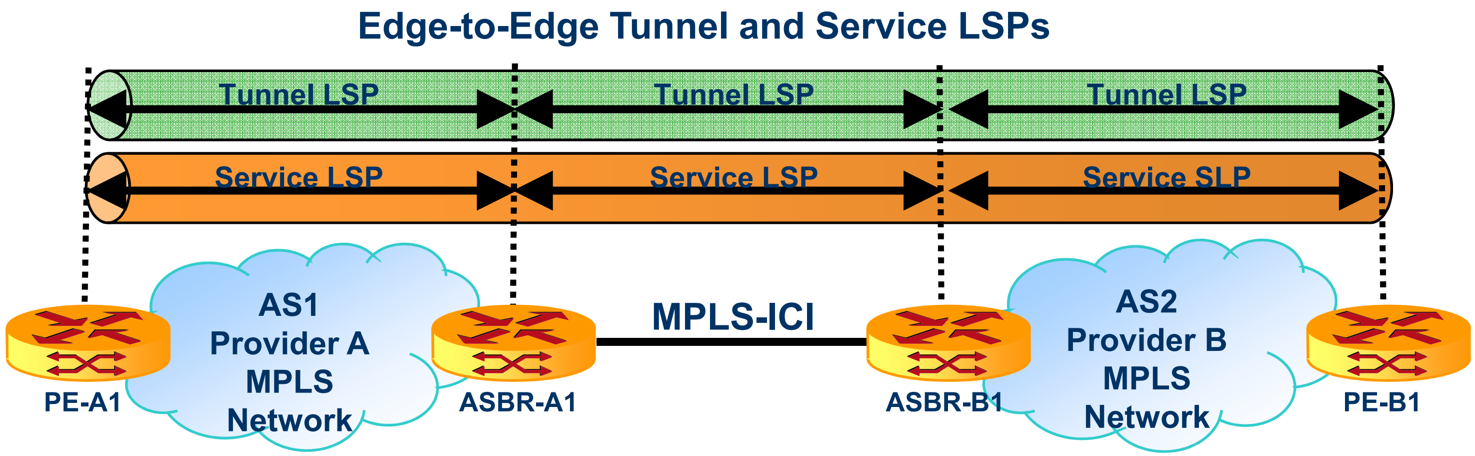
Value	Meaning
1	Do not reply
2	Reply via IPV3 UDP packet
3	Reply via applications level control channel

OAM
On Demand Diagnostics



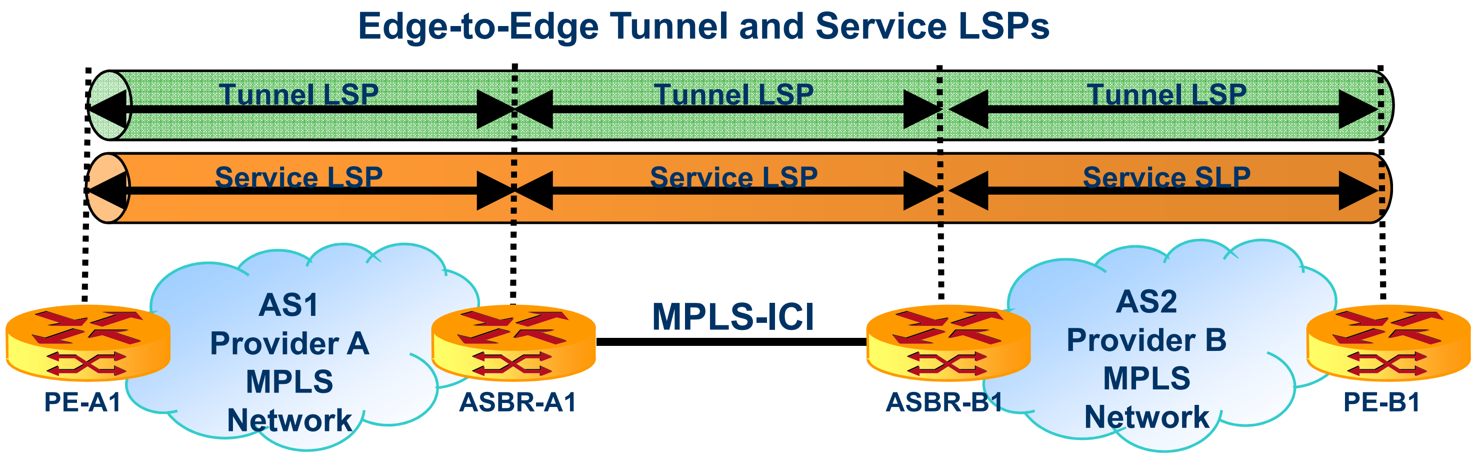
- ASBR LSP ping supports in ping mode:
  - Timer parameters: time interval between successive echo requests per LSP or globally when initiating an LSP ping test
  - Failure detection criterion in terms of the number of successively missed echo request replies that trigger declaration of an LSP down
    - This must be configurable per LSP
  - Failure notification:
    - Send an SNMP trap upon LSP failure detection
    - Notify all client protocols that depend on liveliness of LSP being monitored when that LSP fails

OAM
On Demand Diagnostics



- ASBR acting as an endpoint for an LSP must be able to avert OAM-related DoS attacks by:
  - Dropping the LSP ping messages received on an LSP if the protocol is not enabled for that LSP
  - Policing LSP ping echo requests to enforce the message rate configured for all LSPs
    - Per-LSP policing is optional
- Trace mode capability of LSP ping can be used for fault isolation
  - Enables identification of the path(s) traversed by an LSP and hop-by-hop fault localization
  - ASBR provides rate limiting or dropping of LSP tracing messages arriving at an ASBR from another provider
  - Dropping an LSP ping message disrupts the end-to-end path trace
  - ASBR supports the option to respond at the domain boundary without including a downstream label map

OAM
On Demand Diagnostics



- ASBR is configurable to respond to path trace messages from another provider ASBR by either:
  - Responding without a downstream label map to the next hop, or
  - Responding with a downstream label map to the next hop
- A router inside an AS with knowledge that the LSP being traced is a cross-AS LSP may:
  - Drop the LSP ping echo request, or
  - Respond to the LSP ping echo request without the downstream label map

OAM
MIBs

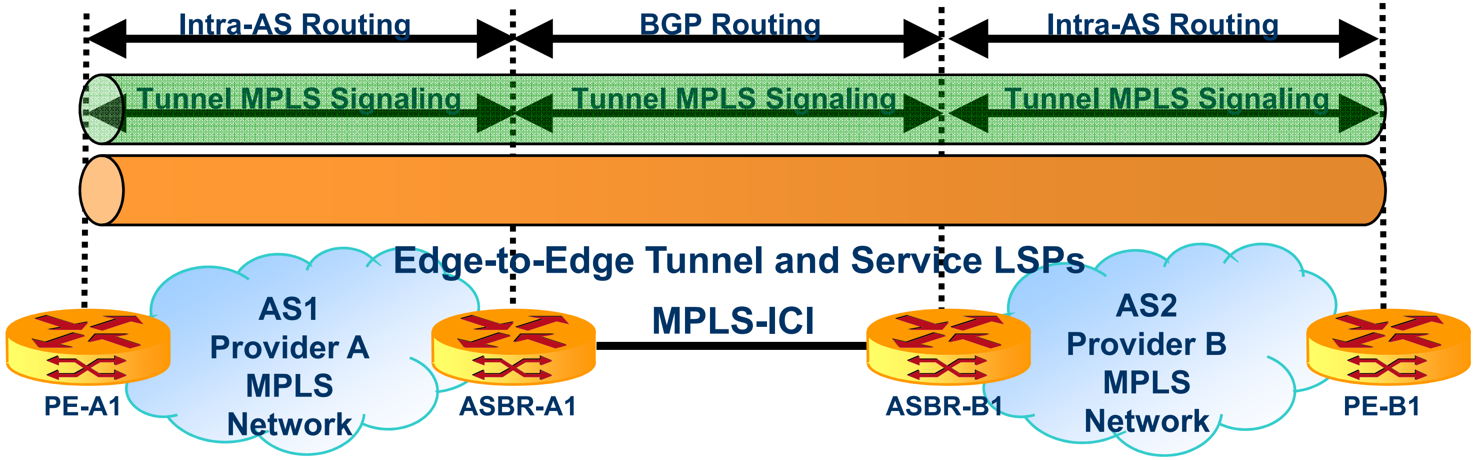
- ASBR supports a management information model (MIB) that provides configuration and management of BFD consistent with [BFDMIB] for the following groups:
  - bfdSessionGroup
  - bfdSessionPerfGroup
  - bfdSessionPerfHCGroup
  - bfdNotificationGroup
- When using the BFD MIB, ASBR shall support:
  - Only SNMPv3 for configuration of the BFD MIB
  - SNMPv2 is sufficient when read-only operations are performed
- Mechanism with a comparable level of security should be used when other network management protocols are used

[BFDMIB] “Bidirectional Forwarding Detection Management Information Base”, draft-ietf-bfd-mib-03.txt. IETF work in progress

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. **Security**
9. Applications
10. References
11. Summary

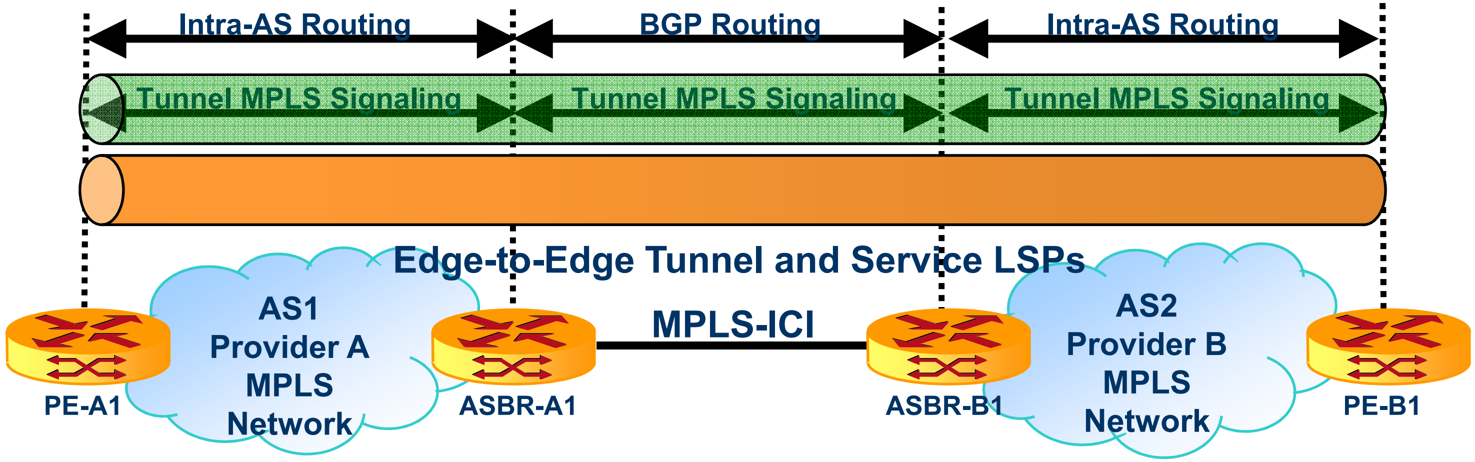
Security and Confidentiality Overview



- A key area of focus with MPLS internetworking across providers
- Prevent propagation of security vulnerabilities and exposures from a peers' network
- Security threats can originate from accidental, administrative and intentional sources
  - Intentional threats include spoofing and DoS attacks
  - Level and nature of threats may vary over time and by network
- Specific capabilities are important at the MPLS-ICI and at devices which support ICI (Ex: ASBRs) → control plane and data plane protection
- Complements security considerations addressed in individual protocol specification and/or security framework

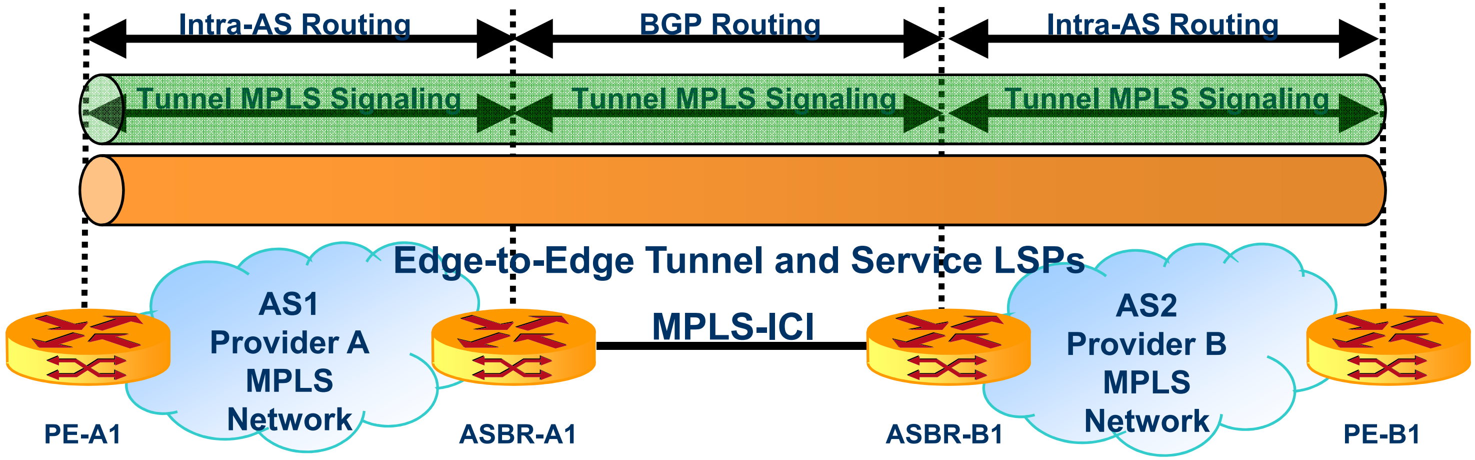
References: RFC 4111, RFC 3871, RFC 4778

Security and Confidentiality
Control Plan Protection



- **Authentication of Signaling Sessions**
  - **ABSR supports:**
    - **MD5 authentication for relevant TCP protocols within scope of MPLS-ICI (LDP, BGP)**
    - **MD5 authentication for RSVP-TE integrity object**
    - **Exchange all signaling and routing protocol messages over a single IPSec tunnel in tunnel or transport mode with authentication but with NULL encryption between peering ASBRs**
    - **IPSec supported with HMAC-MD-5 and optionally SHA-1**
  - **Protect against large volume and maliciously created OAM messages which might overwhelm ASBR or bring down a service**
    - **BFD: support authentication using MD-5 and TTL processing as an anti-replay measure**
    - **LSP ping does not support authentication**

Security and Confidentiality
Control Plan Protection continued

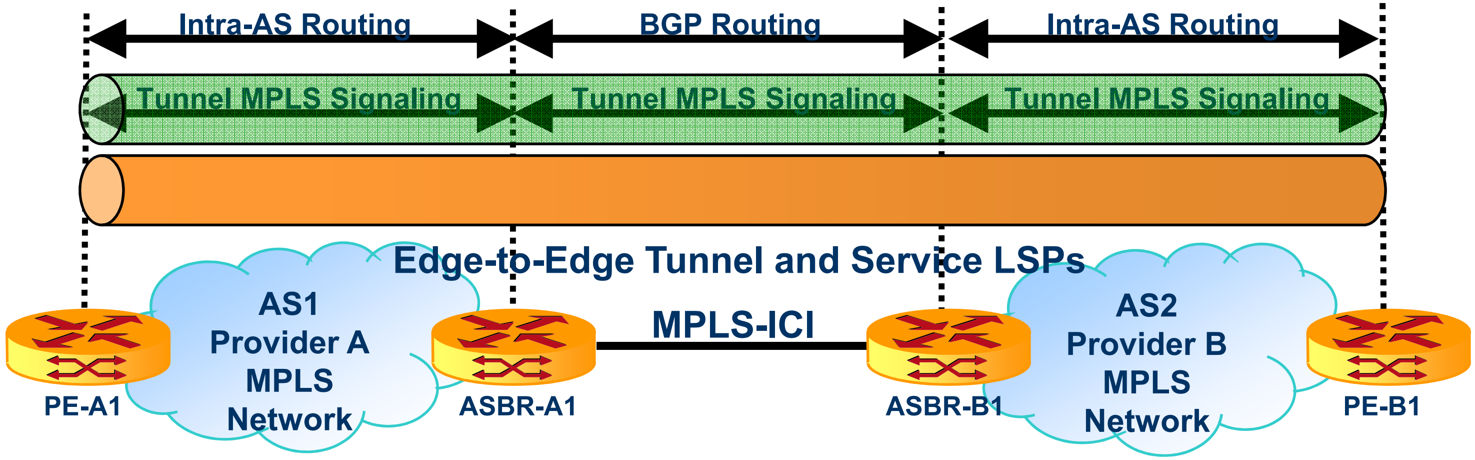


- **Protection against DoS attacks in the control plane**
  - **ASBR supports:**
    - **Filter signaling, routing and OAM packets destined for self and provide rate limiting**
    - **Packet filters that are separately applied per interface with minimal/no impact on performance**

    Enables filtering, and rate-limiting of signaling, routing and OAM messages sent by a peer to an associated traffic profile

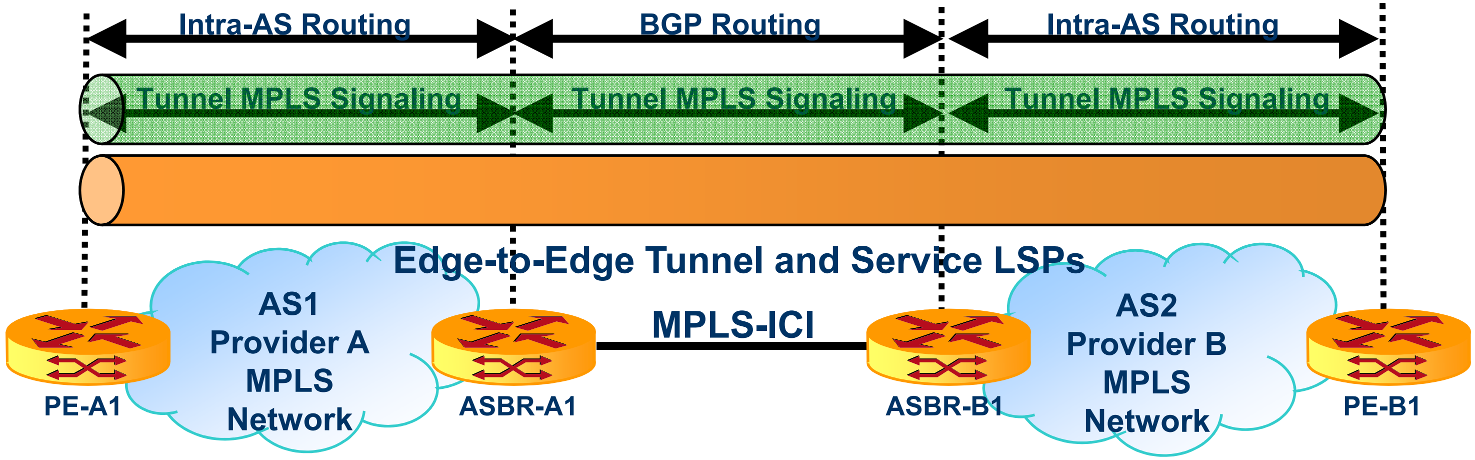
    - **Execution of management commands to take action such as turning on filters and/or disconnecting an interface while under a control plane DoS attack**
    - **Limiting number of BGP routes received from a specific peer and with IP VPNs, the number of routes learned per IP VPN**
- **Protection against malformed routing, signaling and OAM packets – treated in accordance with relevant protocol specifications**

Security and Confidentiality
Control Plan Protection continued



- **Ability to enable/disable specific protocols per interface**
  - **ABSR drops signaling/routing messages without performance impact if not configured on interface**
- **Protection against incorrect cross-connects through support of:**
  - **LSP Ping to verify end-to-end connectivity (PW, Tunnel, VPN LSP, etc) and verify PE to PE connectivity for L3 VPNs**
  - **BGP: ASBRs and Route Reflectors can restrict which route target attributes are sent to/accepted from a BGP peer across an ICI; and inform what it will accept → Reduces incorrect VPN cross-connect and disclosing confidential information**

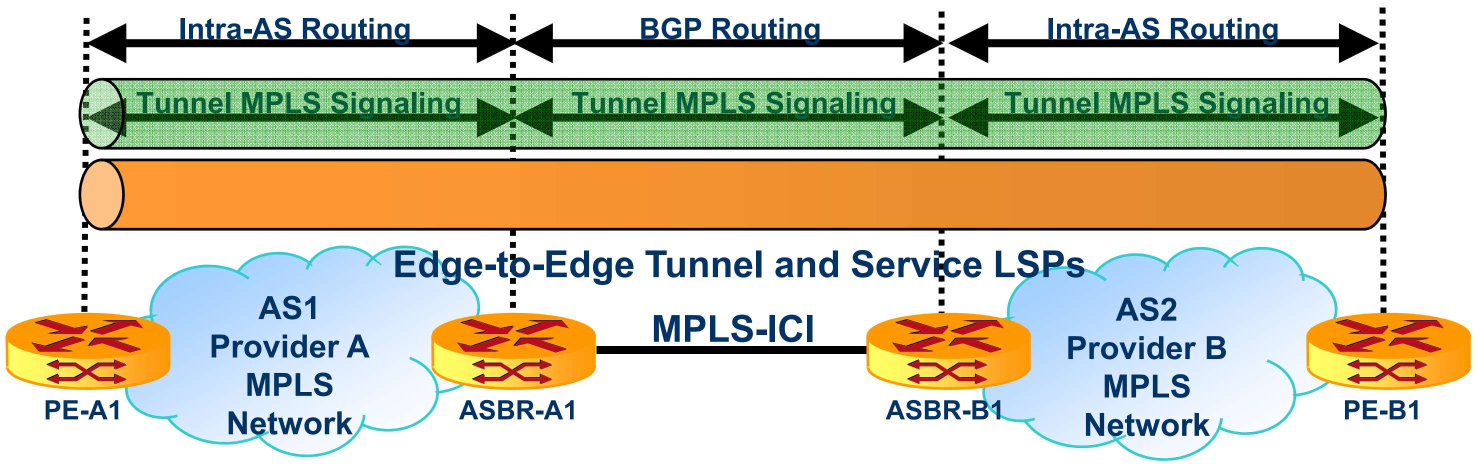
Security and Confidentiality
Control Plan Protection continued



- Protect confidential information by ASBRs with ability to identify and prohibit specific messages (performance, OAM) and LSP trace routes by:
  - Limiting addresses to which traceroute replies can be sent
  - Progressing messages only from trusted partner and targeted to specific agreed to address
  - Implementing traffic policing, reject or apply policies to messages
  - Controlling information provided about the path in RSVP-TE record route or LSP ping trace

  Balance against the impact on trouble shooting capabilities/efficiency

Security and Confidentiality
Data Plan Protection



- Protect against DoS in the data plane via traffic policing
- Protect against label spoofing by having the ASBR:
  - Verify top label received across MPLS-ICI was actually assigned to an LSP arriving from SP across MPLS-ICI; and drop if not
    - Top label: received top label and every label exposed by label popping for forwarding decision
  - Dropping MPLS labeled packets if all labels in stack are not process by ASBR
    - Detected if S-bit is set to 0
    - May prevent some applications across an interface

- Guarantees every label that enters the domain was actually assigned to that SP
- Avoid potential security attack on a service within its domain

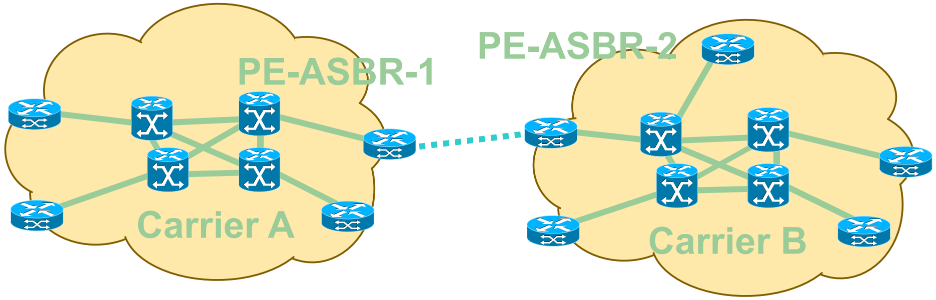
Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. **Applications**
10. References
11. Summary

MPLS-ICI Use Cases

- **Inter-Provider BGP/MPLS IPVPN: Extension of IPVPN services to out of franchise territories**
- **Inter-Provider MPLS Pseudowires (PWs): Extension of L2 VPNs and L2/L1 circuits over MPLS PWs to out of franchise territories**
- **Data trunks-TE tunnels: Efficient packet transport over TE-tunnels**

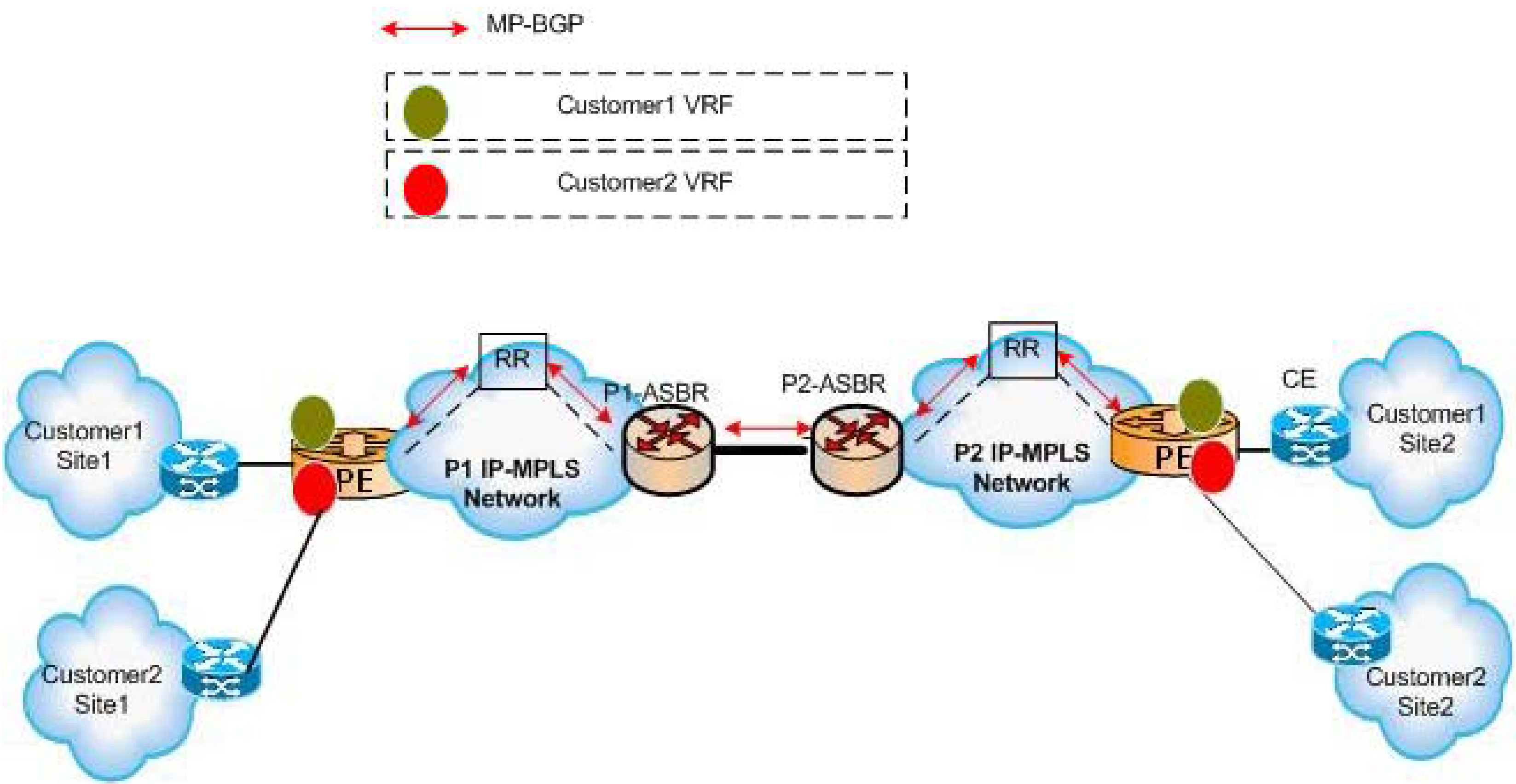
Use Case 1: Inter-Provider VPNs



- To interconnect two or more independently managed MPLS VPNs (same provider or different provider)
  - Fast geographic service coverage expansion
  - Fast service expansion with new actuations
  - Two MPLS VPN providers peering to cover geographically dispersed sites for a common customer base
- Requires:
  - eBGP between two providers to advertise IPv4 routes (RFC4364 Option A)
  - or MP-eBGP between two providers to advertise labeled IPVPN routes and/or labeled IPv4 routes (RFC4364 Option B)
  - Support for data-plane CoS mapping between providers

Use Case 1: Inter-provider IPVPN

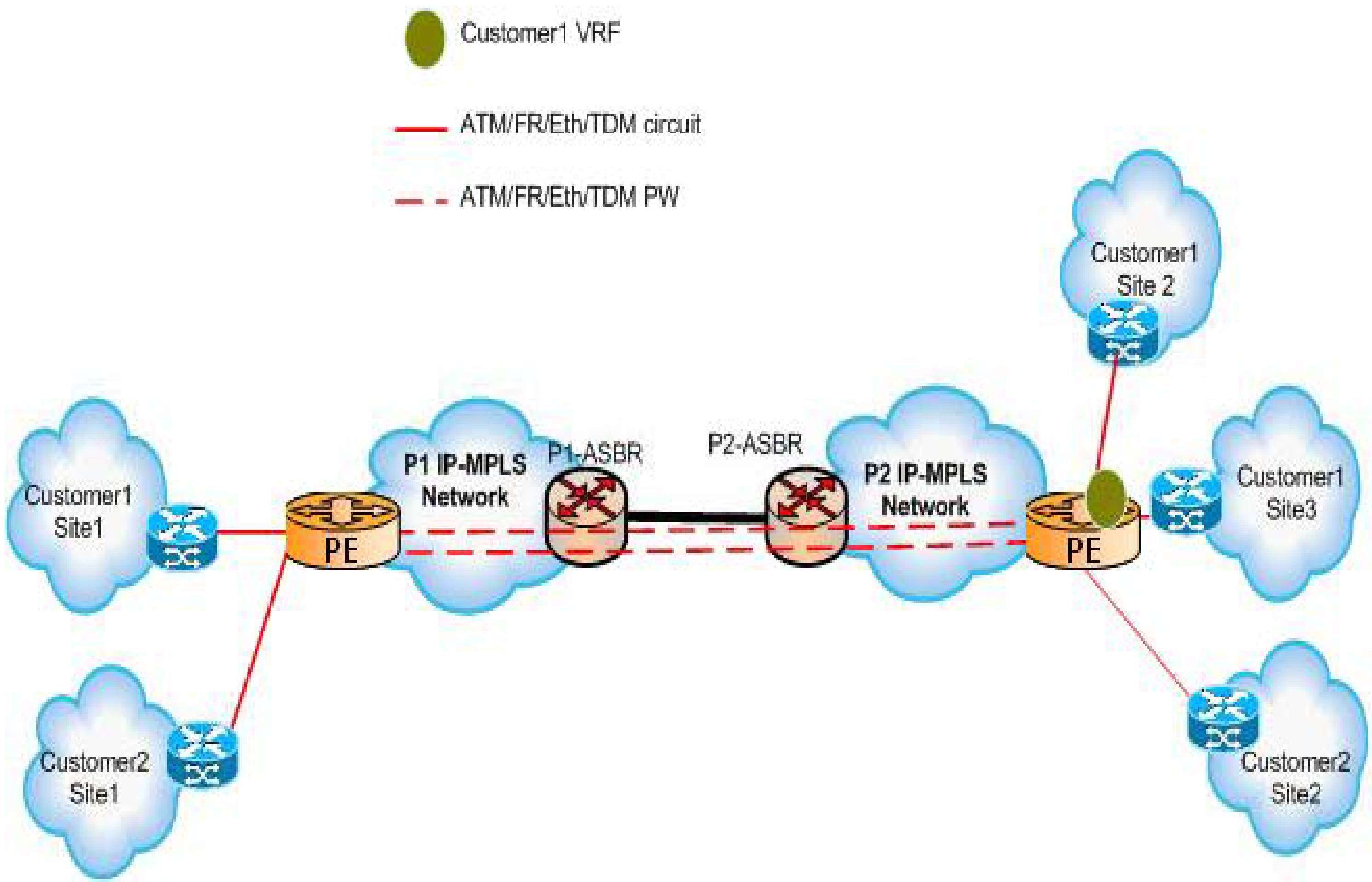
- **IPVPN Services: A typical Scenario**



Use Case 2: MPLS Pseudowires (PWs)

- **Motivation**
  - Carriers have many existing L1 and L2 (TDM, FR, ATM, Ethernet) customers, and will continue to sell L1 and L2 services
  - Carriers are also deploying IP-MPLS networks in their backbone and converging multiple services, including L1 and L2, on these backbones
  - Intra-carrier multi-service convergence over IP-MPLS networks will naturally lead to extending multi-service convergence over the InterCarrier Interconnect
- **Requires**
  - Support for PW setup (Layer-2 peering, Single-Hop, stitched Multi-Hops)
  - Support for data plane QoS mapping between providers

Use Case 2: MPLS PWs

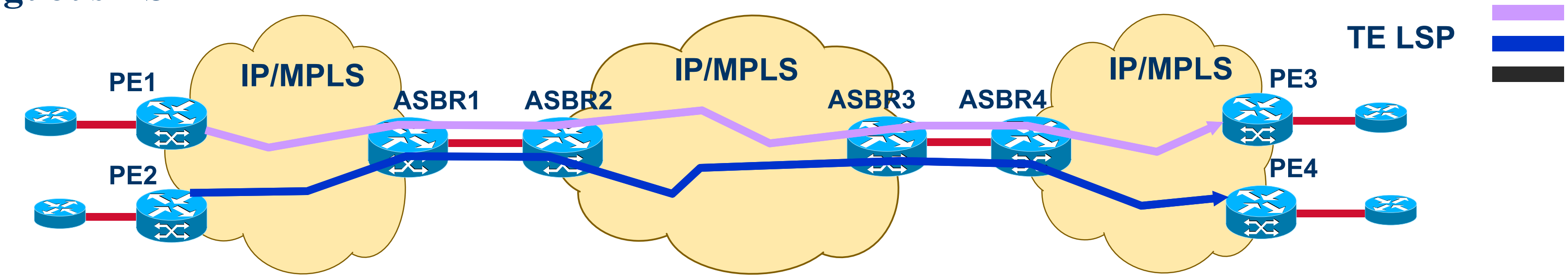


Use Case 3: Data Trunks

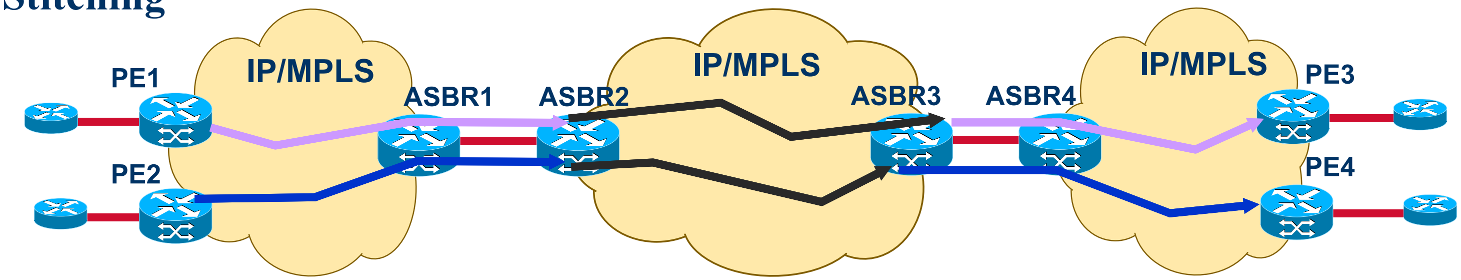
- **Motivation**
  - Interconnect two or more islands of a provider network using MPLS tunnels over another provider network
  - Interconnect a router in one provider's network to a router in another provider network by an MPLS tunnel
- **Requires**
  - Interdomain RSVP-TE: Often these tunnels have TE constraints (e.g. bandwidth, resiliency)
  - Support for data plane and control plane QoS mapping between providers

Use Case 3: Data Trunks - Inter-AS TE

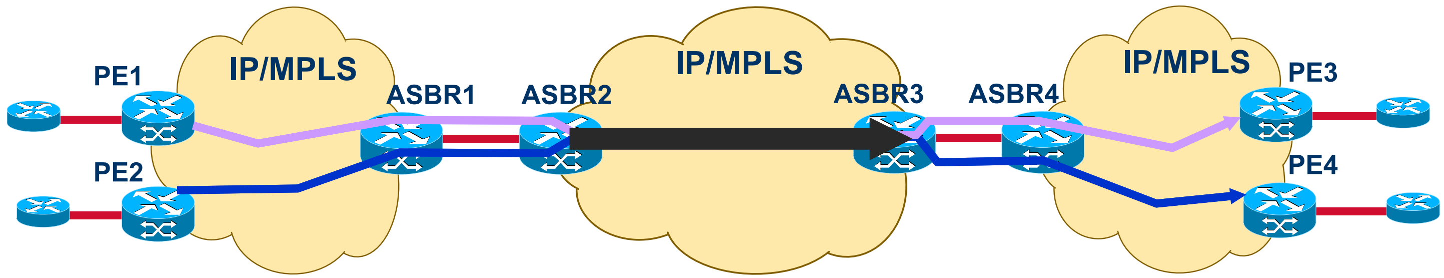
Contiguous LSP



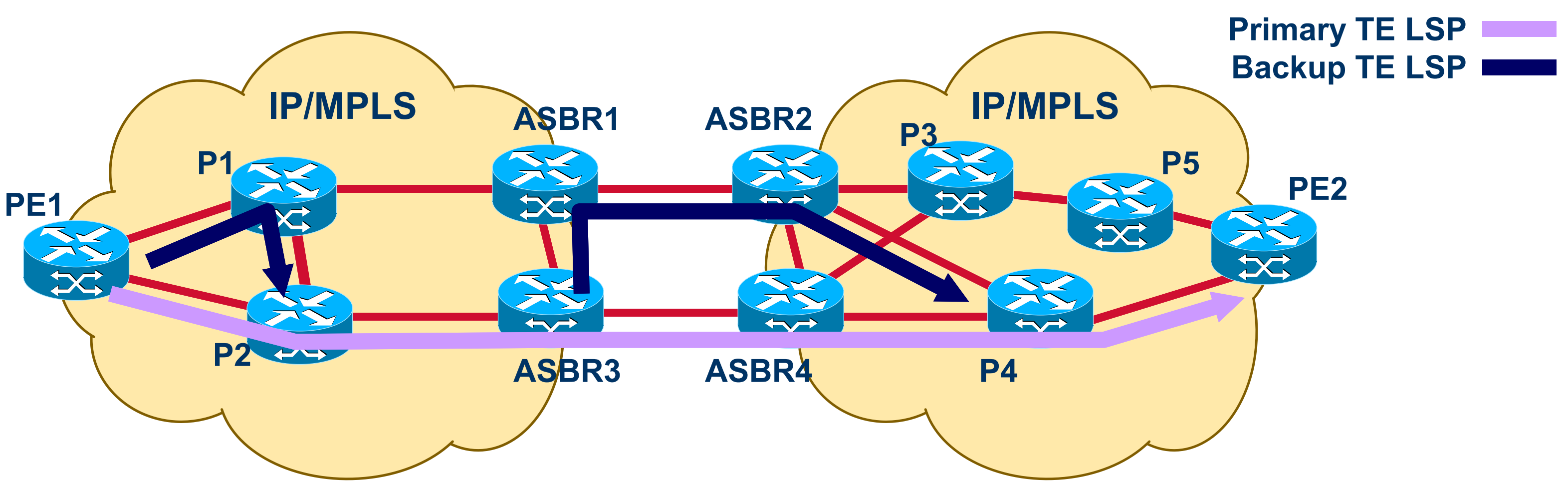
LSP Stitching



Hierarchical LSP



Inter-AS TE – Contiguous LSP Fast Re-Route



- FRR operation unmodified
- Link and node protection can include ASBRs and ASBR-to-ASBR links
- Node-Id flag helps the point of local repair (PLR) detect a merge point (MP)
- Node-Id flag defined in draft-ietf-nodeid-subobject

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. **References**
11. Summary

For More Information. . .

http://www.ipmplsforum.org

Addressing Inter Provider Connections with MPLS-ICI whitepaper available on the IP/MPLS Forum website:
http://www.ipmplsforum.org/education/mpls_white_papers.shtml

Agenda

1. Introduction to the IP/MPLS Forum
2. Today's Challenges
3. MPLS-ICI Overview
4. Reference Architecture
5. Mechanisms for LSP Establishment
6. CAC and Forwarding
7. OAM
8. Security
9. Applications
10. References
11. **Summary**

Summary

- MPLS-ICI Facilitates the rollout of Inter-Carrier MPLS-based services in a multi-vendor environment:
  - BGP/MPLS IP VPN
  - L2 Pseudowires (emulated Layer 1 and Layer 2 services over an MPLS network)
  - Inter-domain MPLS tunnel
  - Inter-domain traffic-engineered trunks for traffic with specific bandwidth and QoS requirements
- Identifies protocols/procedures/features required for Inter-Carrier MPLS Internetworking, both generic and application-specific
- Makes use of existing standards for signaling, routing and OAM mechanisms
- Helps with technical inter-connectivity issues and to reduce overall service cost
- Other challenges may still remain:
  - Inter-provider commercial arrangements
  - All carriers are different!

Thank you **for attending the**

MPLS Inter-Carrier Interconnect (MPLS-ICI) Tutorial

Please visit the IP/MPLS Forum Booth in the Exhibit Area