MPLS Layer 3 and Layer 2 VPNs over an IP only Core

Rahul Aggarwal
Juniper Networks

rahul@juniper.net

MPLS 2004

Juniper NETWORKS

Agenda

- MPLS VPN services and transport technology
- Motivation for MPLS VPN services over an IP only core
- IP only core transport requirements
- Applicability analysis of IP only core transport choices
- IETF status
- Conclusion

MPLS VPN Services

- BGP/MPLS Layer 3 VPNs
  - draft-ietf-l3vpn-rfc2547bis-02.txt
- BGP/MPLS Layer 3 Multicast VPNs
  - Draft-raggarwa-l3vpn-mvpn-vpls-mcast-00.txt
- Layer 2 point to point services
  - RSVP signaled: draft-raggarwa-pwe3-rsvp-te-00.txt
  - LDP signaled: draft-ietf-pwe3-control-protocol-10.txt
- Layer 2 VPNs
  - BGP signaled: draft-ietf-l2vpn-vpls-bgp-02.txt
- VPLS
  - BGP signaled: draft-ietf-l2vpn-vpls-bgp-02.txt
  - LDP signaled: draft-ietf-l2vpn-vpls-ldp-05.txt

Transport Technology Choices

- MPLS transport tunnels
  - Most commonly deployed for Layer 3 unicast VPNs and Layer 2 services
- IP transport tunnels
  - Currently commonly deployed for Layer 3 multicast VPNs
- Choice determined by application requirement
  - MPLS VPN service architecture doesn't enforce a particular transport technology

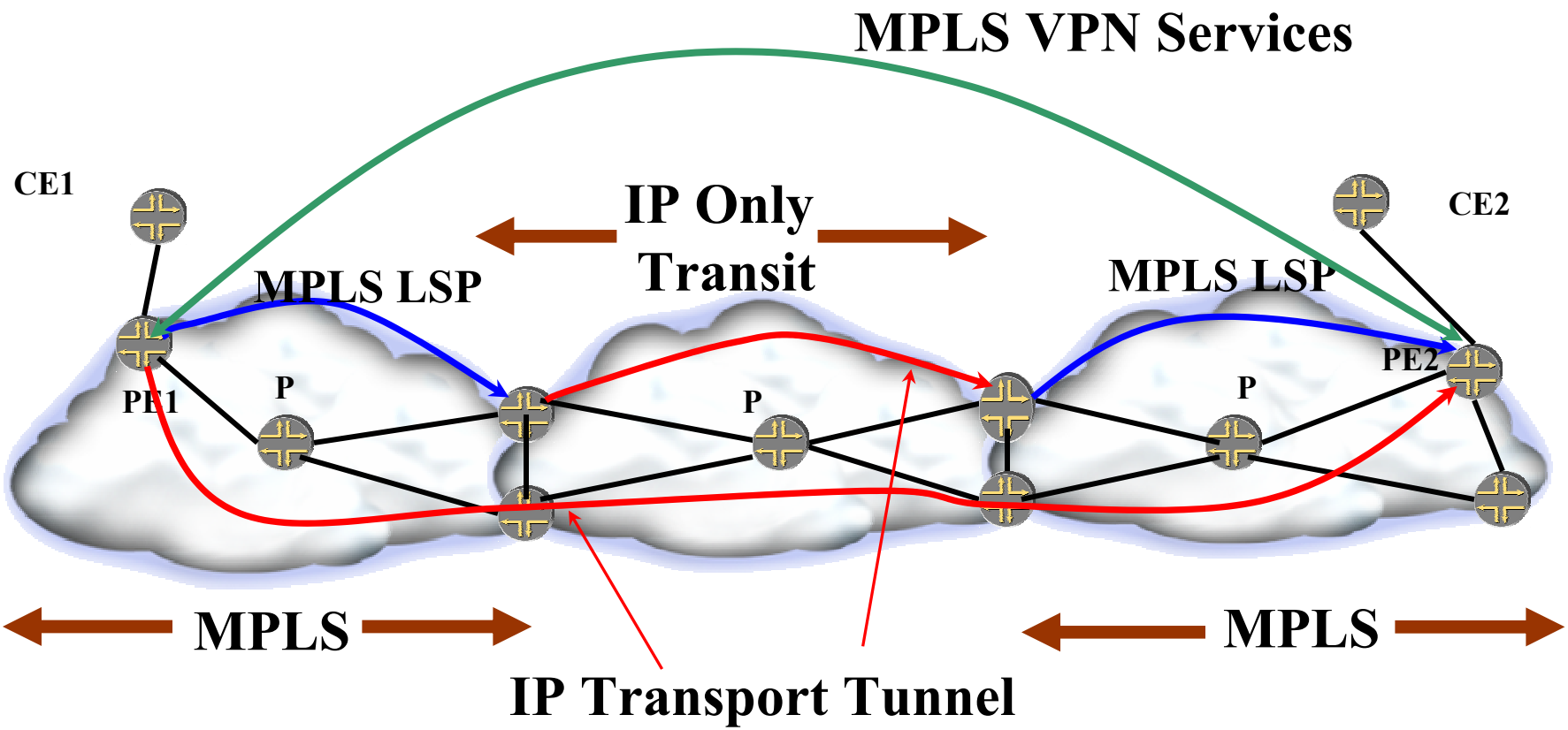
IP Transport Tunnels in Perspective

- Disadvantages
  - MTU decreased by at least 16 bytes
  - Multiple encapsulation options
  - No support for resource reservation
  - No support for explicit routing
  - Incipient fast reroute technology
- However IP transport tunnels have a role…

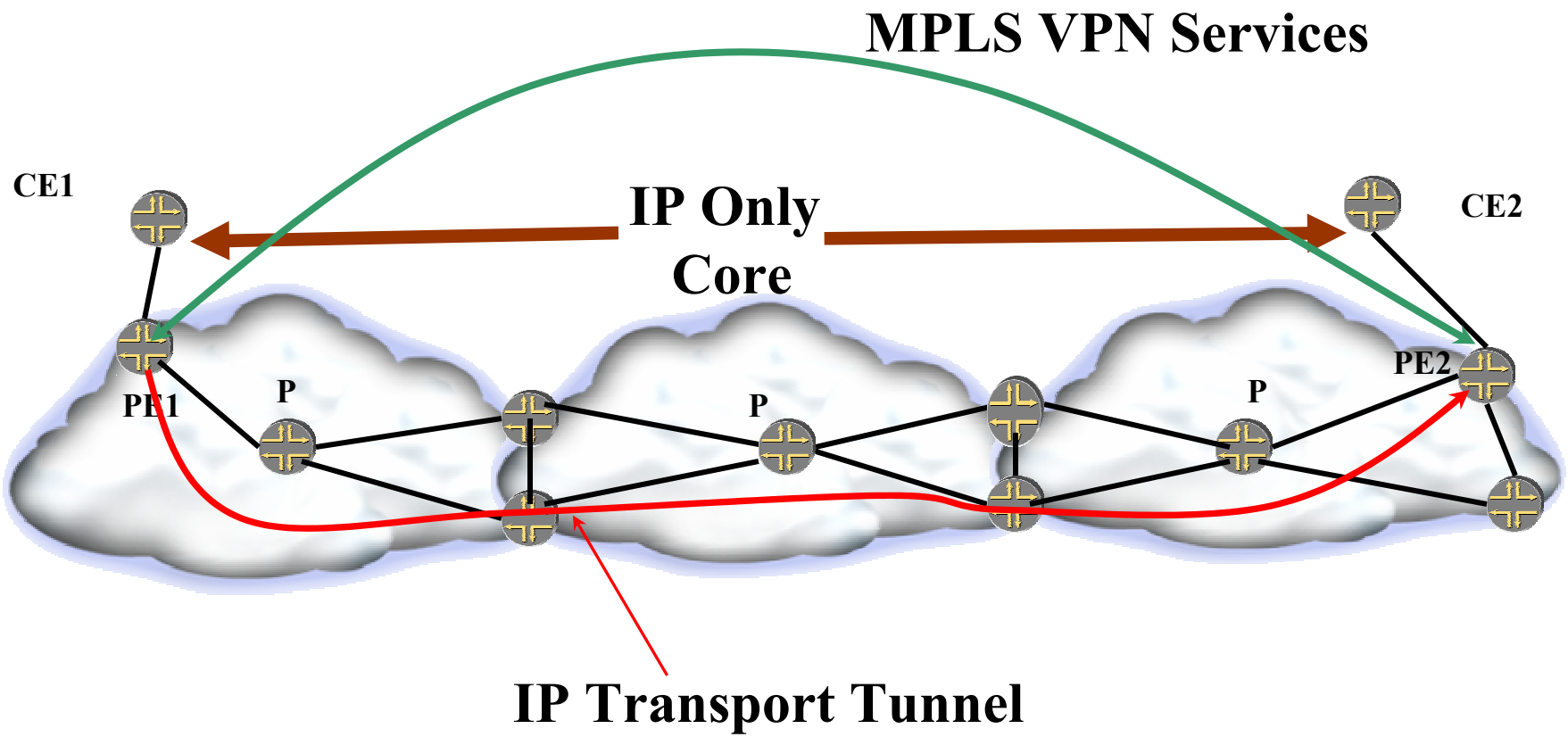
Why MPLS VPN Services over an IP Core ?

- Transit routers may not support MPLS
  - Legacy equipment in the network
- The Service Provider may not want to deploy MPLS
  - Some people have a "technology religion" !
- As a migration path to a MPLS core from an IP core
  - What to do in the interim ?

Extending the Reach of MPLS



Migration to MPLS



IP Only Core Transport Tunnel Requirements

- Multi-service transport tunnel technology
  - Ability to carry multiple services on the same transport tunnel
  - Avoid point solutions
- Minimize the number of additional mechanisms
  - Minimize changes to protocols already used by VPN services
  - Minimize introduction of new protocols
  - An IP transport technology shouldn't require a new signaling protocol to enable a VPN service

IP Only Core Transport Tunnel Requirements …

- Operational ease
  - Configuration and management
  - Tunnel liveliness mechanism
- Security considerations

IP Only Core Transport Choices Applicability Analysis

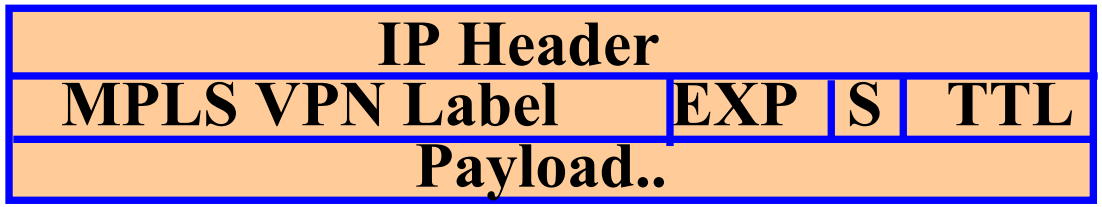
- MPLS over IP
- MPLS over GRE
- MPLS over IPsec
- MPLS over L2TPv3

- Let us analyze the applicability of these to various MPLS VPN applications
  - Will focus on BGP/MPLS unicast VPNs and VPLS
- A system wide view must be taken while evaluating the above – system = service provider infrastructure

IP Only Core Encapsulation

- MPLS over IP
  - draft-ietf-mpls-in-ip-or-gre-05.txt
- MPLS over GRE
  - draft-ietf-mpls-in-ip-or-gre-05.txt
- MPLS over IPsec
  - draft-ietf-mpls-in-ip-or-gre-05.txt
- MPLS over L2TPv3
  - draft-townsley-l2tpv3-mpls-01.txt

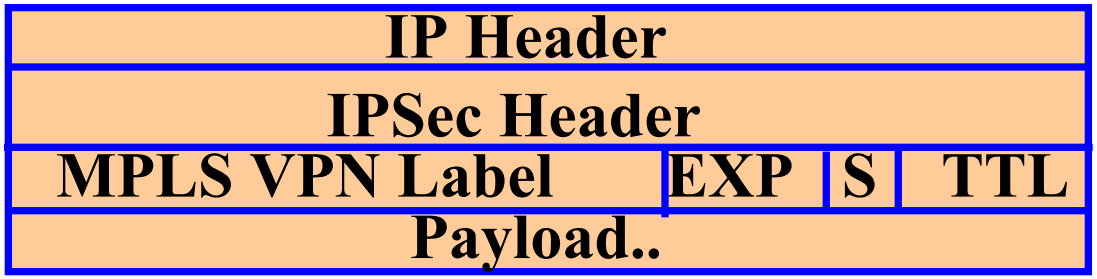
IP Only Core Encapsulation…



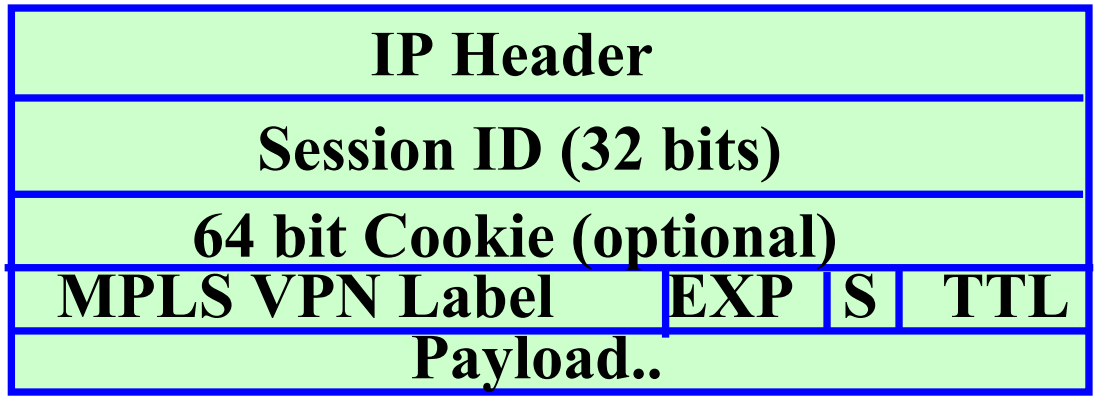
MPLS Over IP

MPLS Over GRE

IP Only Core Encapsulation…



MPLS Over IPSec (Transport Mode)



MPLS Over L2TPv3

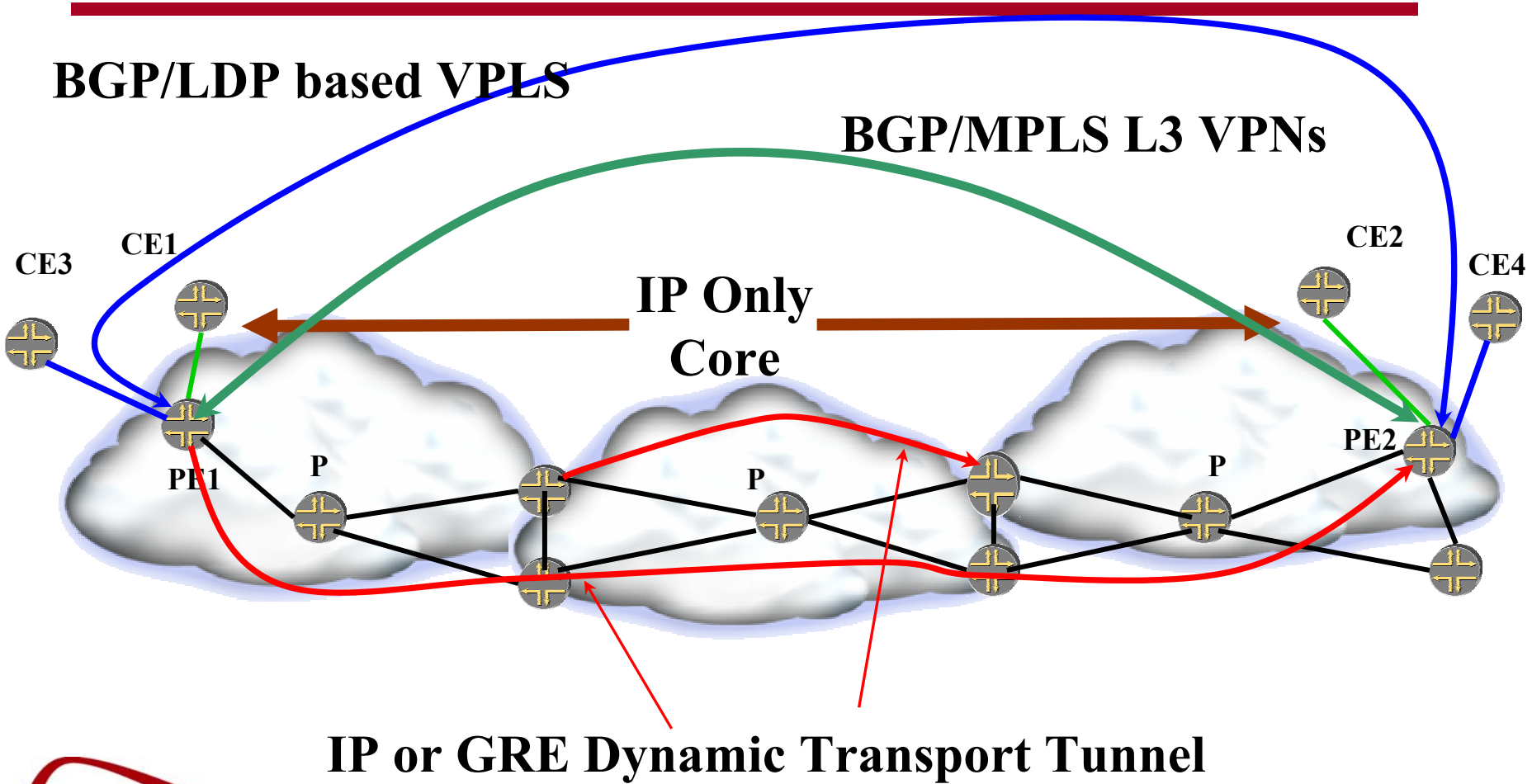
IP Only Core
BGP/MPLS Unicast VPNs

- MPLS over IP and MPLS over GRE
  - No change to BGP VPN mechanisms
  - draft-ietf-l3vpn-rfc2547bis-02.txt and draft-ietf-l3vpn-gre-ip-2547-02.txt
- MPLS over IPsec
  - Requires an additional protocol: IKE for key exchange
  - No change to BGP VPN mechanisms
- MPLS over L2TPv3
  - Requires additional mechanism in BGP to exchange L2TPv3 session and cookie information
  - draft-townsley-l3vpn-l2tpv3-00.txt
  - draft-nalawade-kapoor-tunnel-safi-01.txt

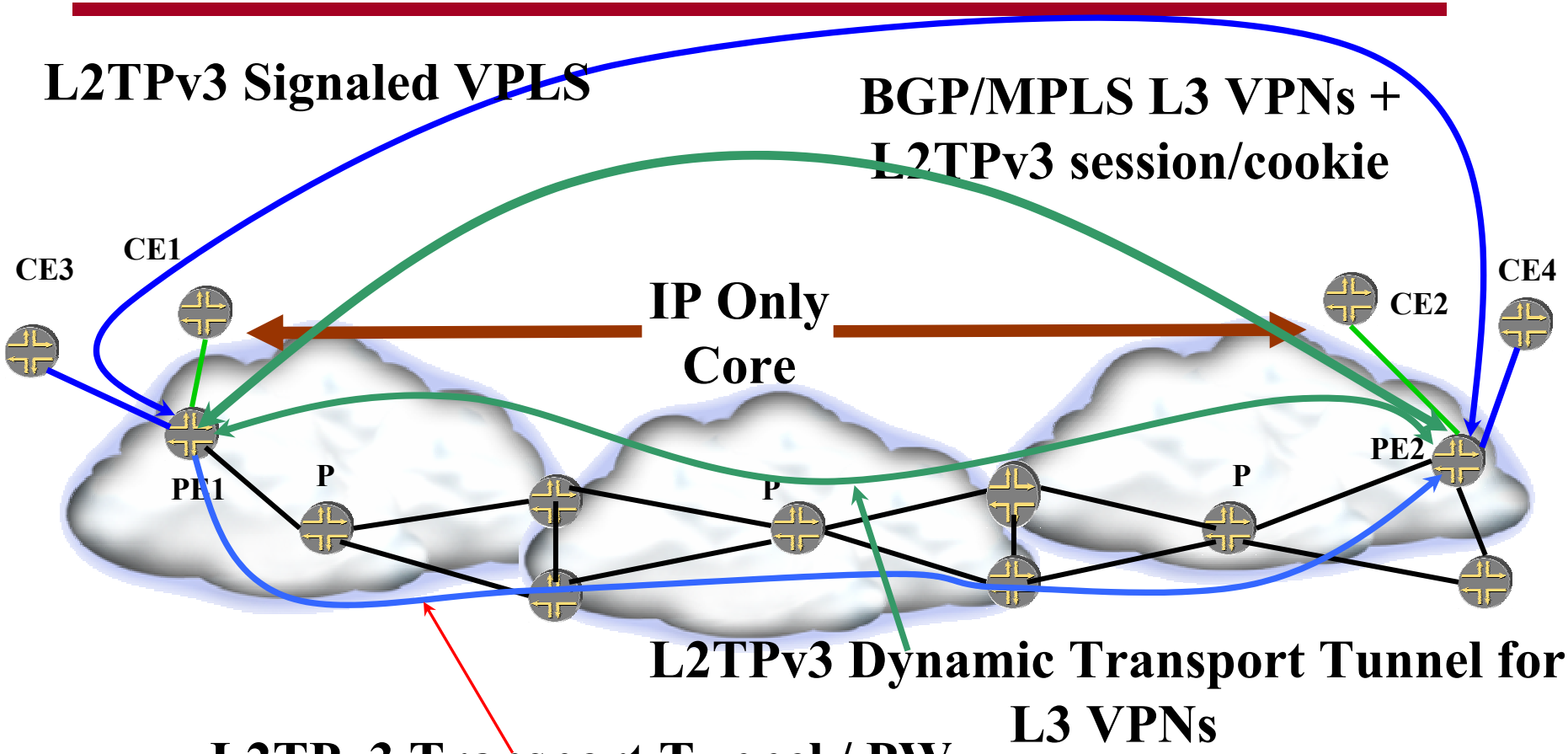
IP Only Core
VPLS over IP

- MPLS over IP and MPLS over GRE
  - BGP based VPLS with no changes to BGP mechanisms.
  - LDP based VPLS with no changes to LDP mechanisms and BGP based or manual auto-discovery
- MPLS over IPsec
  - IKE for key exchange
  - BGP based VPLS with no changes to BGP mechanisms.
  - LDP based VPLS with no changes to LDP mechanisms and BGP based or manual auto-discovery
- L2TPv3
  - Auto-discovery ? BGP ?
  - Currently requires L2TPv3 based signaling: draft-ietf-l2tpext-l2vpn-01.txt

Multi-Service IP Transport
MPLS over IP or GRE



Application Specific IP Transport
MPLS over L2TPv3



Meeting the Requirements
Multi-Service Transport Technology

- MPLS over IP and MPLS over GRE support all MPLS VPN services
  - IPsec supports only ingress replication with Multicast VPNs
- The same MPLS over IP, GRE and IPsec tunnel can be used for providing different MPLS VPN services
- The same L2TPv3 tunnel can NOT be used for providing different VPN services
- The "complete" VPLS solution with L2TPv3 is not clear
- Applicability of L2TPv3 to Multicast VPNs is not clear

Meeting the Requirements
Minimize Additional Mechanisms

- Minimize changes to the MPLS VPN enabling technology
  - MPLS over IP, GRE and IPsec do not require any changes
  - MPLS over L2TPv3 requires enhancements to BGP for BGP/MPLS L3VPNs
- Minimize the number of new protocols
  - MPLS over IP and GRE do NOT require new protocols
  - IPsec requires IKE
  - L2TPv3 requires L2TPv3 signaling for L2 transport
  - L2TPv3 doesn't reduce the BGP/MPLS L3VPN protocols or the L2 services auto-discovery protocol

IP Only Core Transport Configuration and Management

- MPLS over IP and GRE tunnels can be dynamically created between the ingress and egress PE routers
  - No additional mechanisms are required
  - Several vendors are shipping "soft-GRE" implementations
- IPsec tunnels require IKE configuration
- L2TPv3 tunnels can be dynamically created when L2TPv3 signaling is not used
  - Additional mechanisms are required to exchange L2TPv3 session and cookie

IP Only Core Transport
Tunnel Liveliness Mechanism

- BFD can be used for liveliness detection on the MPLS over IP, GRE, IPsec or L2TPv3 tunnel.
  - BFD session will be established between the tunnel endpoints
  - Provides scalable and sub-second liveliness detection
  - L2TPv3 keep-alives are insufficient on their own as they are not suited to sub-second liveliness detection

IP Only Core Transport Security Considerations

- System wide perspective
  - SP infrastructure including CE-PE link
- Look at some threats
  - DoS Attacks
  - VPN packet spoofing
- Does L2TPv3 add value ?
- The role of IPsec

Security Considerations
System Wide Perspective

- "The chain is as strong as its weakest link"
- Need to look at the whole system, and how to protect it against ALL security threats that are possible in practice
- This presentation will discuss only some of the security threats

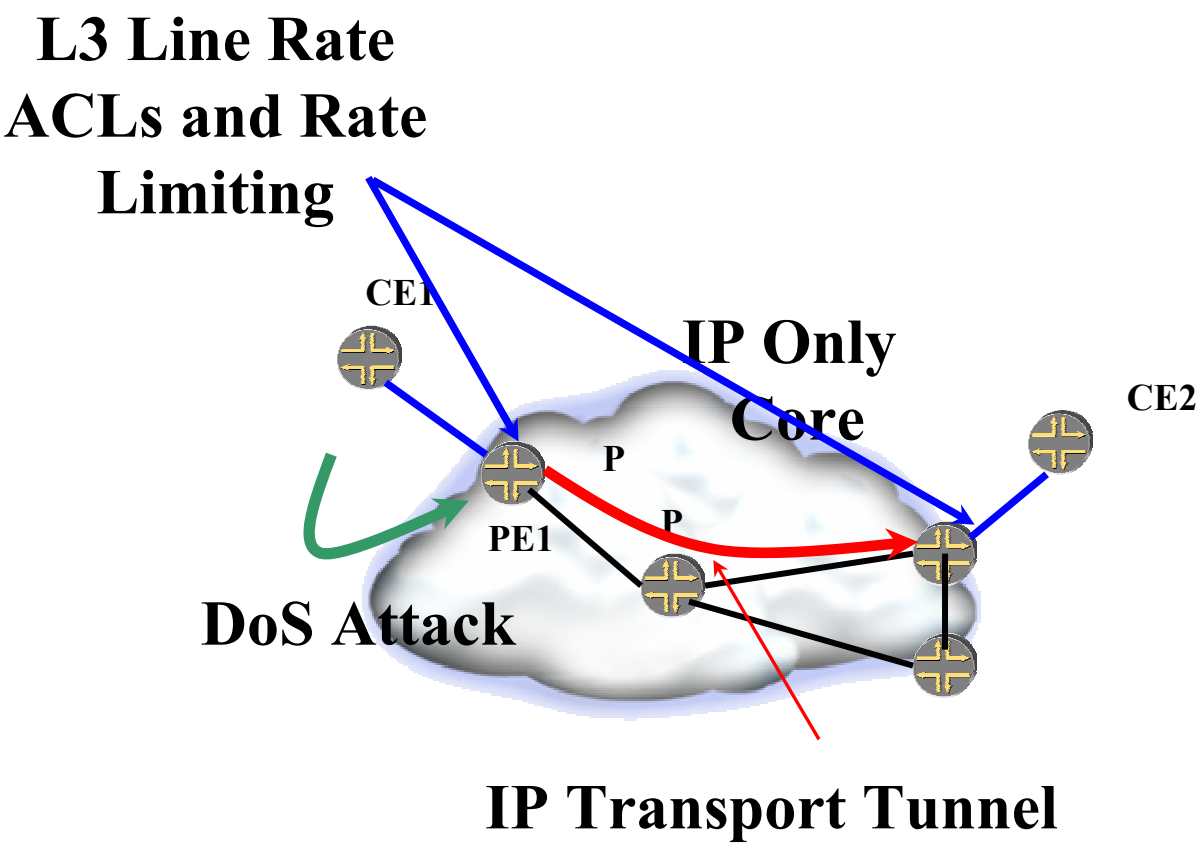
Security Considerations
Some Threats

- Denial of Service (DoS)
  - Attacks the router's control plane
  - Impacts ALL the customers on the attacked PE (not just one VPN)
- VPN packet spoofing
  - Impacts only the specific VPN

Security Considerations
Preventing DoS Against a Router

- Protect route processor
  - Limit access to known sources – **requires ACL**
  - Rate limit traffic to central processor
- Prevent source address spoofing
  - Filtering at ingress to service provider – **requires ACL**
- Must be at line rate

Protecting Against DoS Attacks

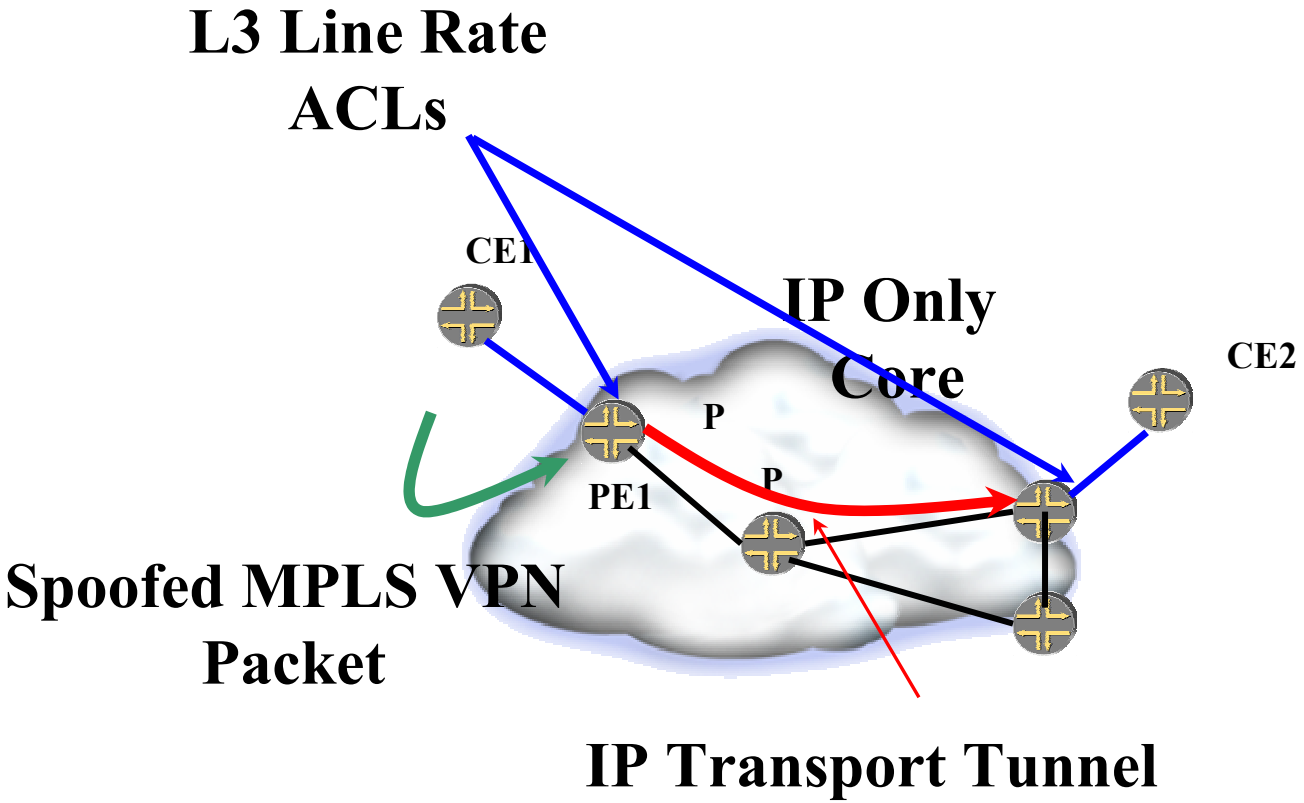


VPN Packet Spoofing
Are ACLs used for protecting against DoS sufficient ?

- To protect against DoS:
  - Each router limits traffic to lo0 to only sources within its own service provider
  - Each ingress router should reject packets whose source address is from the address block used by the service provider for its infrastructure
- To protect against VPN packet spoofing with 2547 over IP/GRE:
  - Filter out packets from "outside" which have source addresses that belong "inside", and
  - Filter out on each PE all packets which have source addresses that belong "outside"

Bottom line: requirements for protecting against VPN packet spoofing with 2547 over IP/GRE are satisfied by the mechanisms to protect against DoS

Protecting Against VPN Spoofing Attacks



Security Considerations
Does L2TPv3 Add Value ?

- 2547 over L2TP focuses only on protection against spoofing of VPN traffic:
  - "If the IP network which MPLS packets are being carried over is vulnerable to spoofing attacks which could bypass these boundary ACLs then the L2TPv3 Cookie provides ample protection…" (draft-townsley-l2tpv3-mpls-01.txt)
- 2547 over L2TP or L2TP PWs do NOT mitigate DoS attacks against the router
- Line rate boundary ACLs are required to prevent DoS attacks
  - Also protect against VPN packet spoofing

Bottom line: 2547 over L2TPv3 does not eliminate the need for (line rate) ACLs and doesn't provide a value add.

Security Considerations
The Role of IPsec

- Secures the CE to PE link
  - Required for securing the end-to-end MPLS VPN service
- Cryptographic authentication
  - Protection against packet spoofing between PE and CE
  - Ensures payload integrity
- Encryption
  - Ensures payload privacy

Meeting the Requirements Score Card

Multi-service Transport	MPLS over IP, GRE.
Minimize changes to the enabling MPLS VPN technology	MPLS over IP, GRE, IPsec
Minimize # of signaling protocols	MPLS over IP, GRE
Configuration and management	MPLS over IP, GRE, IPsec, L2TPv3
Tunnel liveliness mechanism	
Security considerations	All require boundary ACLs

Bottom line: MPLS over IP/GRE is the "multi-service" MPLS over IP transport technology. IPsec has limited applicability. L2TPv3 doesn't provide a value add.

IETF Status

- MPLS over IP/GRE/IPsec (draft-ietf-mpls-in-ip-or-gre-05.txt):
  - Passed WG Last Call
  - Passed IETF Last Call
  - In the IESG review
- 2547 Unicast VPNs over IP/GRE (draft-ietf-l3vpn-gre-ip-2547-02.txt)
  - L3VPN WG document
  - Passed IETF Last Call
  - In the IESG review

IETF Status…

- 2547 Multicast VPNs over IP/GRe
  - Only requires MVPN signaling and draft-ietf-l3vpn-gre-ip-2547-02.txt
- MPLS PWs over IP/GRE/IPsec
  - Only requires draft Martini and draft-ietf-mpls-in-ip-or-gre-05.txt
- L2VPNs over IP/GRE/IPsec
  - Only requires BGP signaling and draft-ietf-mpls-in-ip-or-gre-05.txt
- VPLS over IP/GRE/IPsec
  - Only requires BGP signaling and draft-ietf-mpls-in-ip-or-gre-05.txt

IETF Status…

- 2547 over L2TP:
  - draft-townsley-l3vpn-l2tpv3-00.txt – Not a WG document
  - draft-townsley-l2tpv3-mpls-01.txt – Not a WG document
  - draft-nalawade-kapoor-tunnel-safi-01.txt – Not a WG document

Conclusion

- MPLS VPN services over an IP only core have to be supported
- A system wide perspective must be taken while choosing the IP transport technology
- MPLS over IP and GRE is the "multi-service" MPLS over IP transport technology
- IPsec has its role
- L2TPv3 does not provide a value add