Implementing MPLS VPN in Provider's IP Backbone

Luyuan Fang

luyuanfang@att.com

AT&T

Outline

- BGP/MPLS VPN (RFC 2547bis)
- Setting up LSP for VPN - Design Alternative Studies
  - Interworking of LDP / RSVP / VPN protocols
  - Interoperability in heterogeneous IP network
- MPLS VPN Deployment Issues
  - Scalability
  - VPN security
  - Load sharing between PE-CE links
- MPLS VPN network management
  - Provisioning
  - Performance
  - Fault Management

BGP/MPLS VPN (RFC 2547bis)

AT&T

- MPLS VPN: Deliver network based VPN services over shared IP network.
- Security: Controlled access. VRF - "VPN Routing and Forwarding" tables, contains customer VPN routes. VPNs are isolated.
- Scalability: Provider backbone (P) routers are not VPN aware; Provider Edge (PE) router only holds the routing information of VPN directly connected.
- Customer addresses can overlap. Support non-unique, private (RFC1918) addressing in customer networks.
- Easy configuration for customers, no special changes required on customer side (for Enterprise VPN).

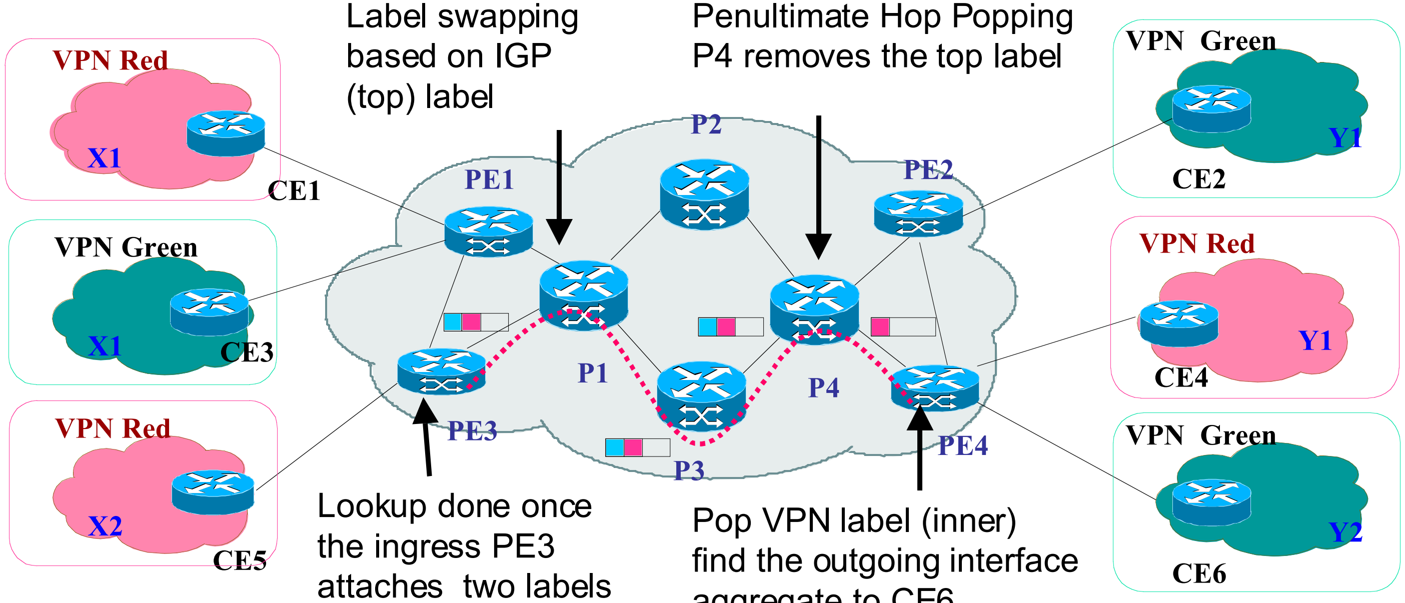
BGP/MPLS VPN

Configuration:

- IGP (e.g. OSPF, or ISIS) routing in the core
- MPLS (e.g. LDP) enabled for all P and PE
- MP-iBGP fully meshed between PEs
- PE-CE can be e-BGP, OSPF, RIP or Static

Two level Labels: 🟦🟥□

- Top label 🟦: LDP label forwarding through the core, PE-PE
- Inner label 🟥: VPN label identify the destination VPN, forwarding to CE



Label swapping based on IGP (top) label

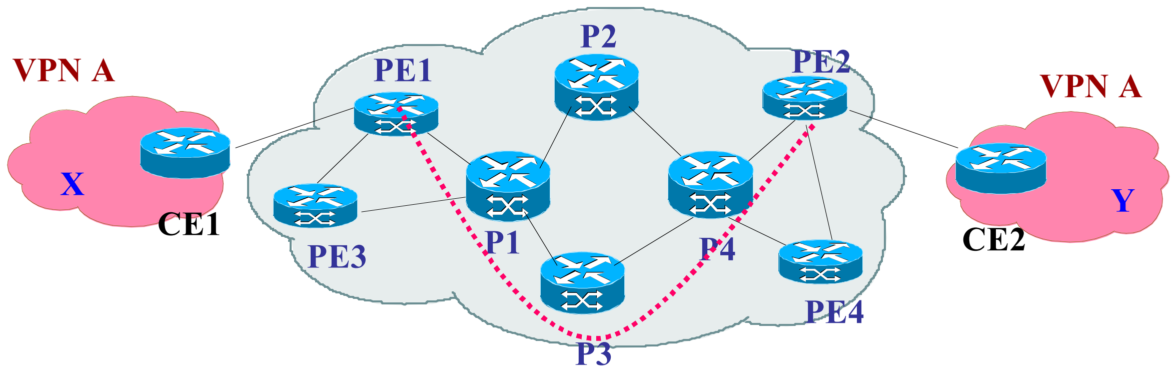
Penultimate Hop Popping P4 removes the top label

Lookup done once the ingress PE3 attaches two labels on each packet

Pop VPN label (inner) find the outgoing interface aggregate to CE6

Setting up LSP for VPN
- Design Alternatives Study

- Example 1: VPN / LDP
  - MPLS (LDP) enabled in the entire backbone network, including all P and PE routers for setting up the Label Switched Path (LSP)
  - VPN enabled on VPN PE routers

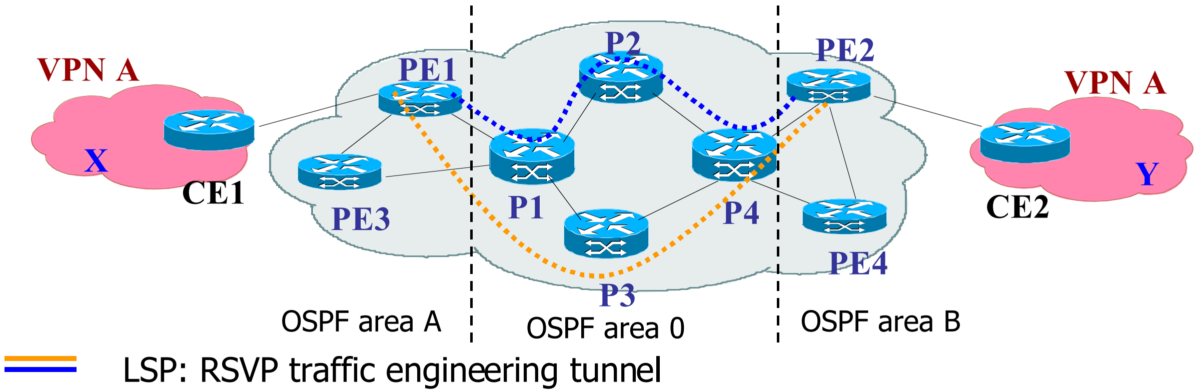


LSP = IGP path (e.g. OSPF shortest path), in this case

  - Advantage: simplicity
  - Consider: availability of LDP

Setting up LSP for VPN
- Design Alternatives Study

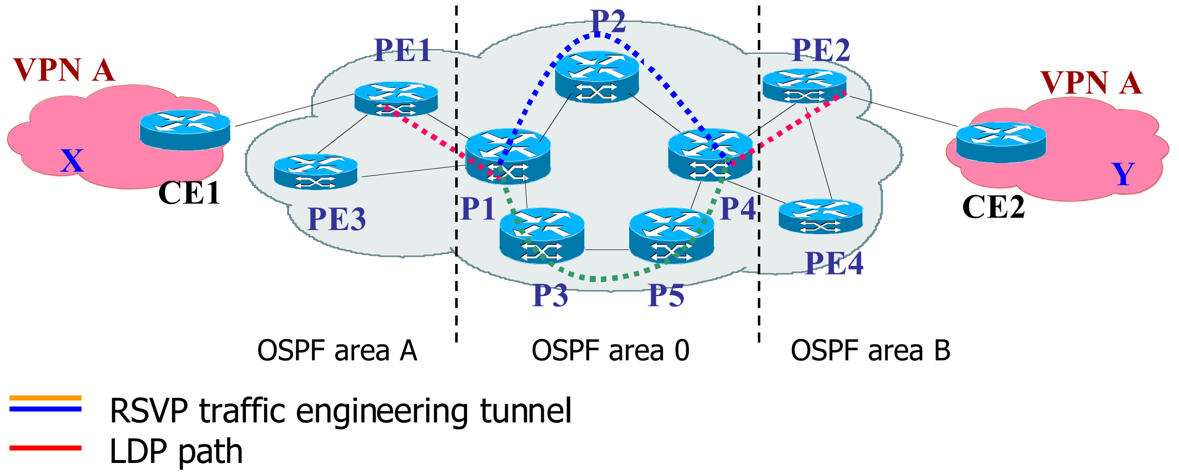
- Example 2: VPN / RSVP
  - Using RSVP TE Tunnel through Multi OSPF areas (PE-PE) for setting up the LSP, with back-up tunnel for failure protection
  - RSVP tunnels are unidirectional, alternative path can be taken for each direction
  - VPN enabled on VPN PE routers



  - *Advantage:* Better TE control, including fast reroute when available
  - *Consider:* Availability of RSVP across multi-OSPF area; many long tunnels required throughout the network may or may not be desirable.

Setting up LSP for VPN
- Design Alternatives Study

- Example 3: VPN / LDP / RSVP
  - Config LDP for PE1 and P1, P4 and PE2.
  - Build short RSVP TE Tunnel in OSPF area 0 (P1-P3-P5-P4), note P1 and P4 may be from one vendor, acting as the head-end, P3 and P5 may be from another vendor. P3 and P5 does not need to enable LDP.
  - Interoperability on RSVP is required, not LDP in this example .
  - VPN enabled on VPN PE routers.



  - *Advantage:* LDP does not need to be available everywhere. Short tunnel.
  - *Consider:* There are no end-to-end TE control.

MPLS VPN Deployment Issues

- MPLS Feature availability
  - VPN, LDP, RSVP, CR-LDP: individually, and Interworking
  - Design largely based on feature availability Vs. optimal
- Multi-vendor inter-operability
  - Required in an heterogeneous IP network
- Incremental deployment plans
  - Fully enable MPLS in the entire IP backbone Vs. partially enable MPLS.
  - TE tunnels, use only as needed Vs. fully meshed
  - Incrementally deploy BGP/MPLS VPN on PE routers

MPLS VPN Deployment Issues

- Scalability
  - The use of Route Reflector
  - Performance impact on PEs needs to be measured
- Load sharing between PE-CE links
  - Assign different RDs to different sites Vs. single RD for each VPN.
- Security
  - One VPN’s route does not exist in other non-connected VPN’s VRF or the global routing table
  - FR/ATM equivalent security - more study needed
- Multi-AS inter-working
  - Feature needed today for building VPN to traverse multi-AS / multi-provider’s network

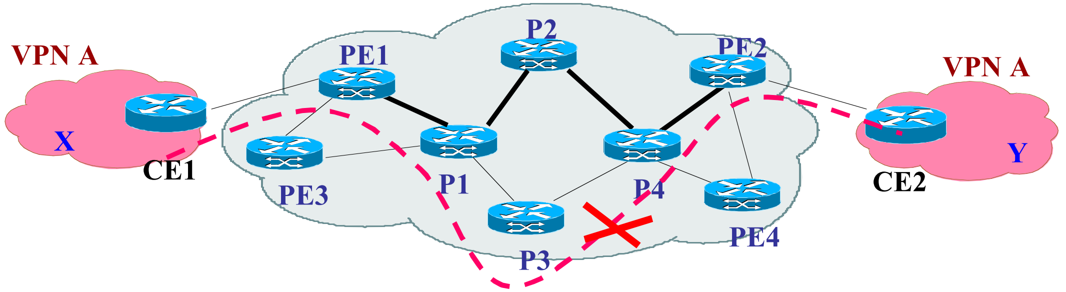
MPLS VPN network management

- Available MIBs today
  - LSR MIB, VPN MIB, MBGP MIB, RSVP TE MIB,TDP MIB, FTN MIB,…
- Configuration and Provisioning
  - Auto-provisioning tools needed for large scale VPN deployment
- Performance
  - All MPLS features impact on performance, including basic VPN on PE routers, need to be studied
  - More study needed for VPN supporting QoS
  - Network performance: delay, jitter, loss, throughput, availability
  - Element performance: utilization
- Security

MPLS VPN network management

- Traffic Management / Engineering
  - Characterize traffic for VPNs
  - Profiling, correlation, and optimization
- Fault management
  - Monitoring and troubleshooting
  - VPN failure detection and recovery

Example:



Config: LDP in the core for all P and PE router; IGP: OSPF; iBGP full mesh between PEs
LSP: OSPF shortest path: PE1-P1-P3-P4-PE2; no TE tunnels.

Problem: All links and nodes are up, but P3 label switching fails. LSP failure results in VPN failure.

Solution required: PE1 and PE2 to to be notified of the LSP failure
LSP needs to be re-established through recovery mechanism, force LSP <> OSPF path

Summary

- Implementing BGP/MPLS VPN in large IP backbone can be feasible
  - Illustrations of alternatives and examples presented here have been experimented through lab testing and inter-lab trial
- Deployment Challenges
  - Feature availability
  - Interoperability
  - Manageability
- Requirements on BGP/MPLS VPN implementation, service deployment and management