MPLS VPN Security Best Practice Guidelines

MPLScon 2006

May 24 2006

Monique Morrow and Michael Behringer

Distinguished Consulting Engineer and
Distinguished Systems Engineer

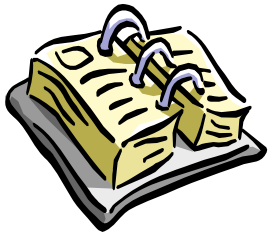
Cisco Systems, Inc.

mmorrow@cisco.com

mbehring@cisco.com

(www.cisco.com)

MPLS VPN Security - Agenda

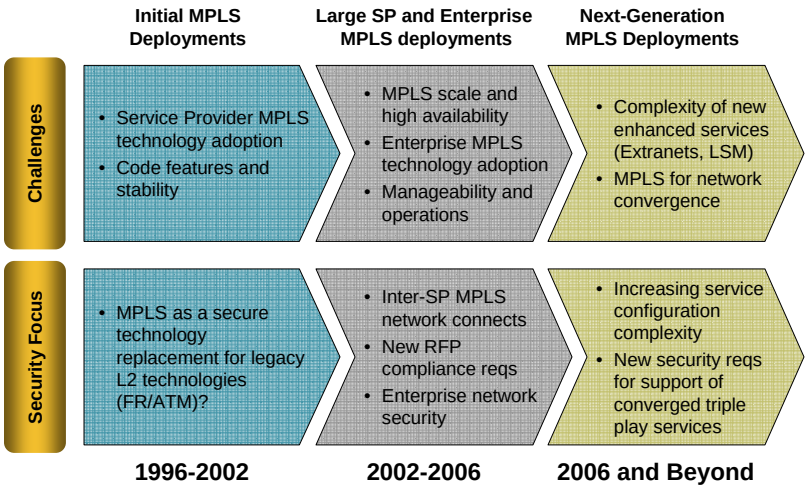


- MPLS Security evolution and drivers
- Secure MPLS VPN Design Considerations
- Ongoing standardization work
- Summary

MPLS Security

- **Protection mechanisms for MPLS-specific network resources**
  - **Protection of MPLS forwarding and signaling**
- **MPLS security protection areas**
  - **Integrity and privacy of MPLS VPN service traffic**
  - **MPLS node access and resiliency**
- **Focus areas in MPLS network infrastructure**
  - **MPLS core (LSPs between PE pairs)**
  - **MPLS service edge (PE-CE link)**
  - **MPLS network interconnect (Inter-AS/SP)**
- **Incremental value-add and integral part of scalable and robust MPLS technology solution**

MPLS Evolution



MPLS Security Drivers

MPLS Customers	MPLS Security Drivers	Examples
Service Provider Segment		
Tier-1 (Global)	Network convergence	Triple play and public/private services convergence
Tier-2 (National)	Network convergence and network interconnect	Inter-AS/SP network inter-connect
Enterprise Segment		
Financials	Regulatory compliance Extranet security	Sarbanes-Oxley Act Financial application access
Education/Research	User traffic segmentation Regulatory compliance	Secure campus connectivity
Other	Extranet security MPLS technology value-add	Extranet partner connectivity
Government Segment		
Government agencies and institutions	Regulations driving new network security reqs	US Homeland Security

Why Is MPLS VPN Security Important?

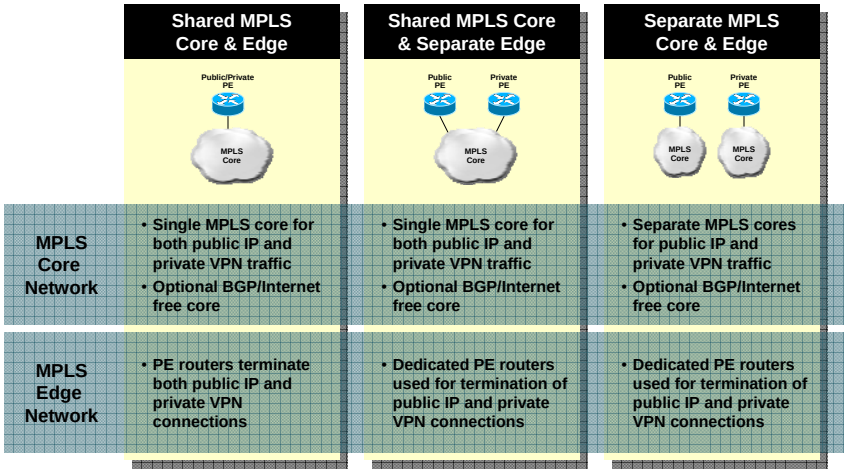
- **Customer buys "Internet Service":**
  - **Packets from SP are not trusted**
  - **Perception: Need for firewalls, etc.**
- **Customer buys a "VPN Service":**
  - **Packets from SP are trusted**
  - **Perception: Few or no further security measures required**

SP Must Ensure Secure MPLS Operations

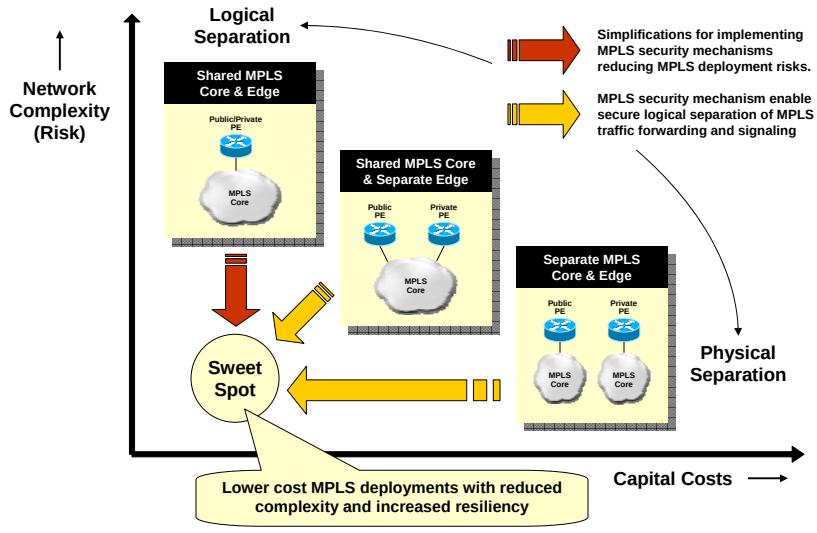
Security Risk

- MPLS security architecture components
  - Network design
  - Implementation
  - Operation
- Level of MPLS network deployment complexity determines perceived security risks
- Influencing factors of MPLS deployment complexity
  - Network architecture (e.g., physical v.s. logical separation)
  - Networking services run on top of MPLS network
- Types of networking services
  - Public IP services (Internet)
  - Private (VPN) connectivity services

MPLS Deployment Scenarios



Network Complexity versus Capital Costs



Secure MPLS/VPN Core Design

- Don't let packets into the core (for MPLS: PE routers)
  - No way to attack core, except through routing, thus:
- Secure the routing protocol
  - Neighbor authentication, maximum routes, dampening,…
- Design for transit traffic
  - QoS to give VPN priority over Internet
  - Choose correct router for bandwidth
  - Separate PEs where necessary
- Operate Securely

→ **Still "Open": Routing Protocol**

→ **Only Attack Vector: Transit Traffic**

→ **Now Only Insider Attacks Possible**

→ **Avoid Insider Attacks**

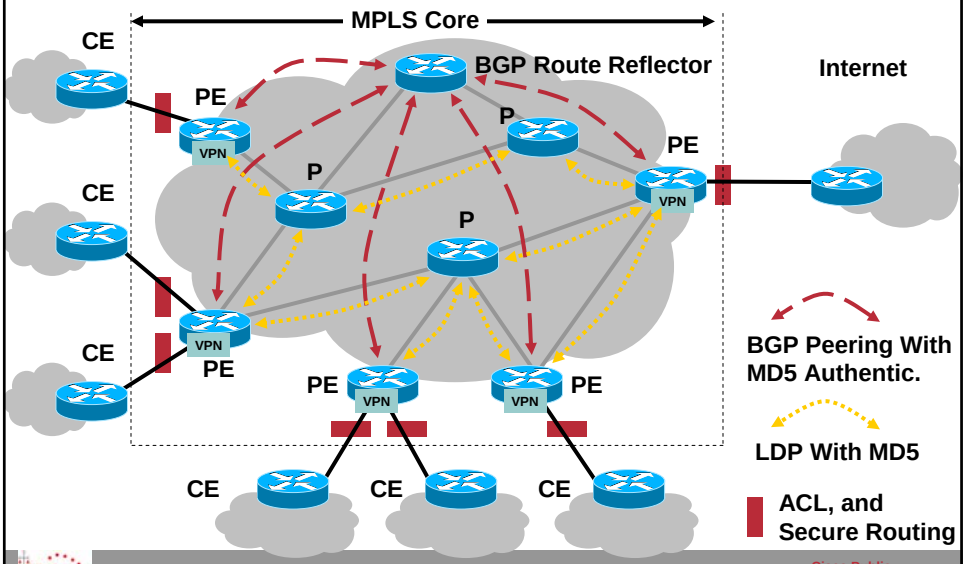
Security Recommendations for ISPs

- Secure devices (PE, P): They are trusted
- Core (PE+P): Secure with ACLs on all interfaces

  Ideal: deny ip any <core-networks>
- Static PE-CE routing where possible
- If routing: Use authentication (MD5)
- Separation of CE-PE links where possible (Internet/VPN)
- LDP authentication (MD5)
- VRF: Define maximum number of routes

Note: Overall security depends on weakest link

Securing the MPLS Core



Feature Portfolio

	MPLS Traffic Forwarding (Data Plane)	MPLS Signaling (Control Plane)
MPLS Core Network		
Access Control	▪ Native MPLS traffic separation	• Session authentication for core signaling protocols
Data Integrity & Privacy	▪ PE-PE packet/path integrity ▪ MPLS TTL propagation	• Control plane message validation/authentication
MPLS Service Edge		
Access Control	• IP/MPLS packet filtering • VRF-context packet forwarding	• Session authentication for PE-CE signaling protocols
Data Integrity & Privacy	• PE-PE packet/path integrity	• VRF-aware control plane msg validation/auth (e.g., TTL) • VPN (max) route/prefix filtering
MPLS Network Inter-Connect		
Access Control	• Ingress MPLS packet validation (top label validation check)	• Session authentication for inter-AS signaling protocols
Data Integrity & Privacy	• End-to-end cross-AS MPLS packet/path integrity validation	• VPN route/prefix (RD/RT) filtering

Relevant Standardization

IETF L3VPN WG:

Working on Layer 3 VPN architectures, such as MPLS IP VPNs, IP VPNs using virtual routers, and IPsec VPNs.

http://www.ietf.org/html.charters/l3vpn-charter.html

IETF L2VPN WG:

Working on Layer 2 VPN architectures, such as VPLS and VPWS

http://www.ietf.org/html.charters/l2vpn-charter.html

Conclusions

- MPLS security covers protection mechanisms for MPLS forwarding and signaling
- MPLS security requires holistic approach including network design, implementation, and operation
- Level of MPLS network deployment complexity determines perceived network security risks
- Growing importance of MPLS security as a result of network and service convergence

References

- MPLS VPN Security – ISBN 1587051834
- RFC4381 – Analysis of MPLS VPN Security
- RFC2082 – RIP-2 MD5 Authentication
- RFC2154 – OSPF with Digital Signatures
- RFC2385 – Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC3013 – Recommended Internet Service Provider Security Services and Procedures
- RFC2196 – Site Security Handbook
- Gartner research note M-17-1953: "MPLS Networks: Drivers Beat Inhibitors in 2003"; 10 Feb 2003
- MPLS and VPN Architectures – ISBN 1587050021

Q and A

CISCO SYSTEMS