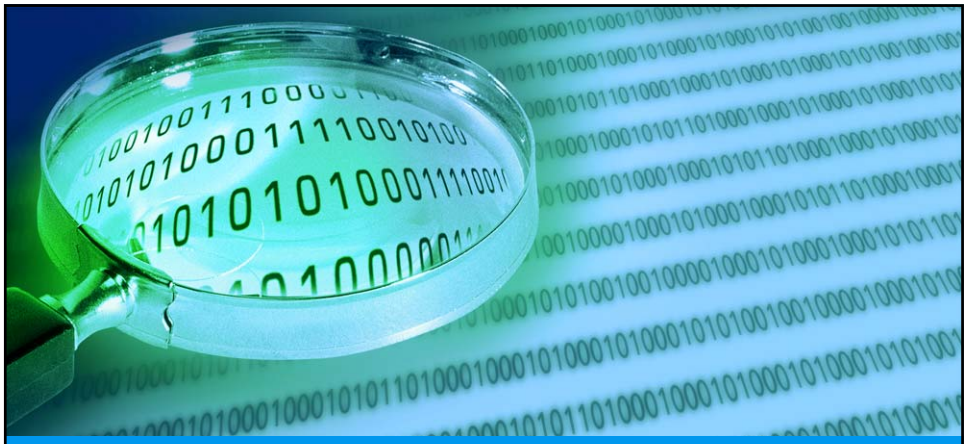


# Enterprise Guide to MPLS-VPN RFI

ERNST & YOUNG
*Quality In Everything We Do*

**Amr Ahmed**
**Senior Manager**
**Ernst & Young, Security & Technology Solutions**

Amr.ahmed@ey.com

MPLScon
MULTI PROTOCOL LABEL SWITCHING

0601-0702350

## Agenda

- RFI Perquisites
- Network Coverage
- Backbone Architecture
- Class of Service and QoS
- Unicast IP Routing
- High Availability
- Advanced Services
- Service Cost Model
- Security Consideration





MPLScon
MULTI PROTOCOL LABEL SWITCHING

## RFI Perquisites

**MUST have perquisites:**

- **Clear business objectives;** *Cost saving, service quality, TTM, etc.*
- **Fundamentals of MPLS VPN;** *Technology and business/technical benefits*
- **Network Strategy;** *LAN/WAN, voice, video, encryption, multicast, etc.*
- **Applications;** *Characteristics of applications traffic and flows*
- **Architecture;** *Reference architecture and technical position*
- **Vendor short list;** *Regional and global*





## Providers Network Coverage

**Understanding of Provider's Network Coverage.**

- MPLS reach-ability, point of presence geographical coverage; distinguish between:
  - o "active" and "non active/planned" POPs
  - o Strategic partners to deliver services
- Access connectivity types to client locations. Leased-line, Frame Relay, ATM, DSL, ISDN, Ethernet, etc.
- Identify where the provider's backhaul paths might impact availability and service quality.

## Backbone Architecture

**Review overall MPLS VPN backbone architecture**

- Provisioned VPNs (MPLS-based Layer 2 VPNs or BGP/MPLS VPNs "RFC2547bis" - Layer 3)
- Traffic engineering within the core (e.g. CR-LDP, RSVP-TE)
- Control, Data and Management Plane
- Provider (P), Provider Edge (PE), Customer Edge (CE) technology
- Provider CE offering ( Managed CE, non-managed CE or both)
- Routing protocols between PE and CE

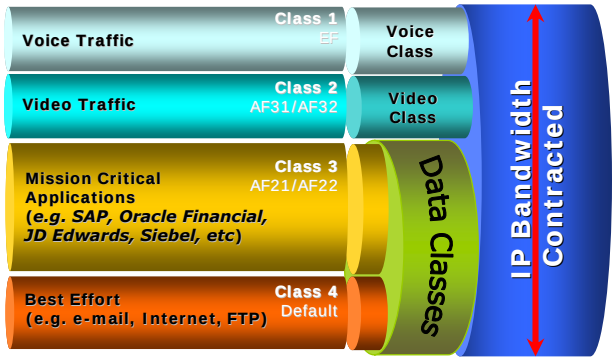




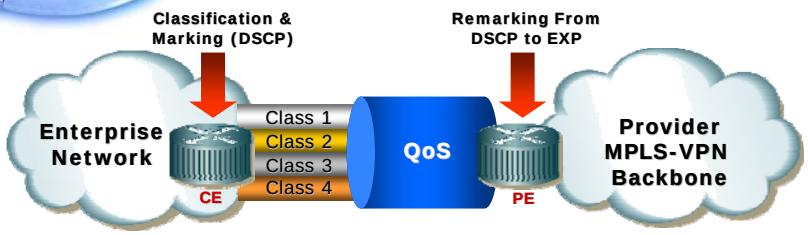
## Classes of Services and Traffic Classification

**Application and Bandwidth Allocation; *Provider Guidelines and Restrictions***

- Traffic Classification & marking techniques on the CE router *(example: marking by IP Address, TCP/UDP ports, URL, MIME, Citrix ICA, etc.)*
- Honoring of customer classification/marking (802.1Q/P, DSCP) to provide End-to-End QoS.
- Future plan for additional class of service.



## QoS in the MPLS VPN




- How the service provider implements QoS in their MPLS VPN backbone network
- How the service provider integrates their Diffserv domain (MPLS VPN backbone network) to the client Diffserv domain; *RFC 3270 (Uniform mode and Pipe mode)*.





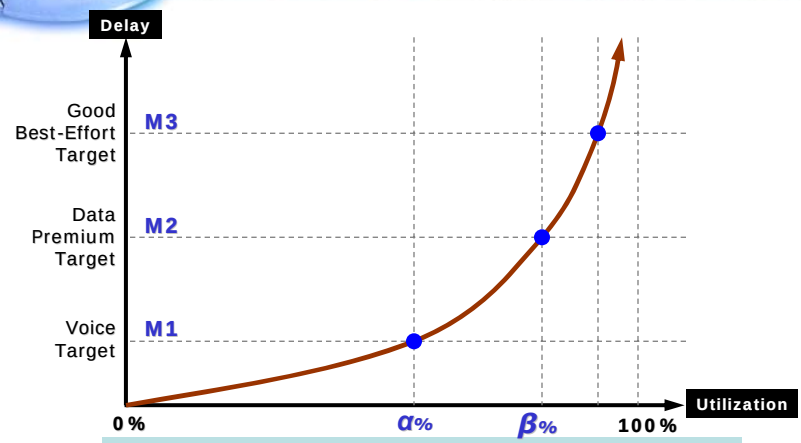
## Classes of Services
### *SLA and Reporting*

**Understanding of provider's service levels / guarantees offerings and reporting. Also, how client traffic / applications will map to the provider CoS levels.**

- Reporting CoS mapping, usage and SLA metrics (Online, periodic, etc.)
- Additional SLA for Voice traffic (Jitter, Delay, Packet Loss, *Bursts, Gaps, Average Call Setup/Teardown, Codec, MOS/R-Factor)*
- Providers internal management tools; *SLA metrics - identifies and isolates problems - capacity and resiliency for improved traffic engineering.*

| Class of Service | Availability | Delay | Packet Loss | Jitter |
|---|---|---|---|---|
| **Class 1** | ☑ | ☑ | ☑ | ☑ |
| **Class 2** | ☑ | ☑ | ☑ | |
| **Class 3** | ☑ | ☑ | | |
| **Class 4** | | | | |

## Classes of Services SLA
### *Delay/Load Trade-Off*




If I Can keep Traffic < α%, I will keep **EF** Delay Under **M1** ms

If I Can keep Traffic < β%, I will keep **AF1** Delay Under **M2** ms

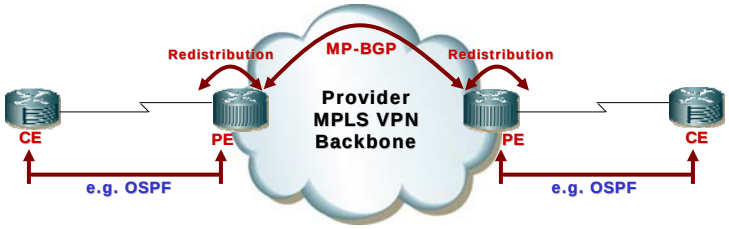
Reference Cisco Systems





## Unicast IP Routing via MPLS VPN

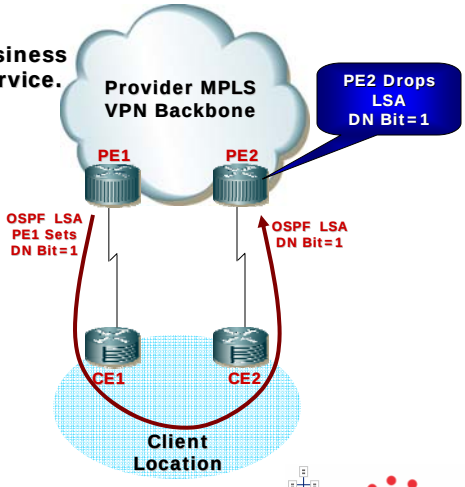
**Understanding of Provider's unicast routing provisioned between CE and PE;** *using either static routing or dynamic routing protocols (RIP, OSPF, IS-IS, EIGRP, eBGP).*



## High Availability

**Understanding of provider's MPLS contingency solution for client business continuity and high availability service.**

*The different high availability option should aid in determining a cost effective solution for service availability at different locations (e.g., Active/Active, Active Standby); also utilizing technologies such as ISDN, DSL, Ethernet services for backup links.*



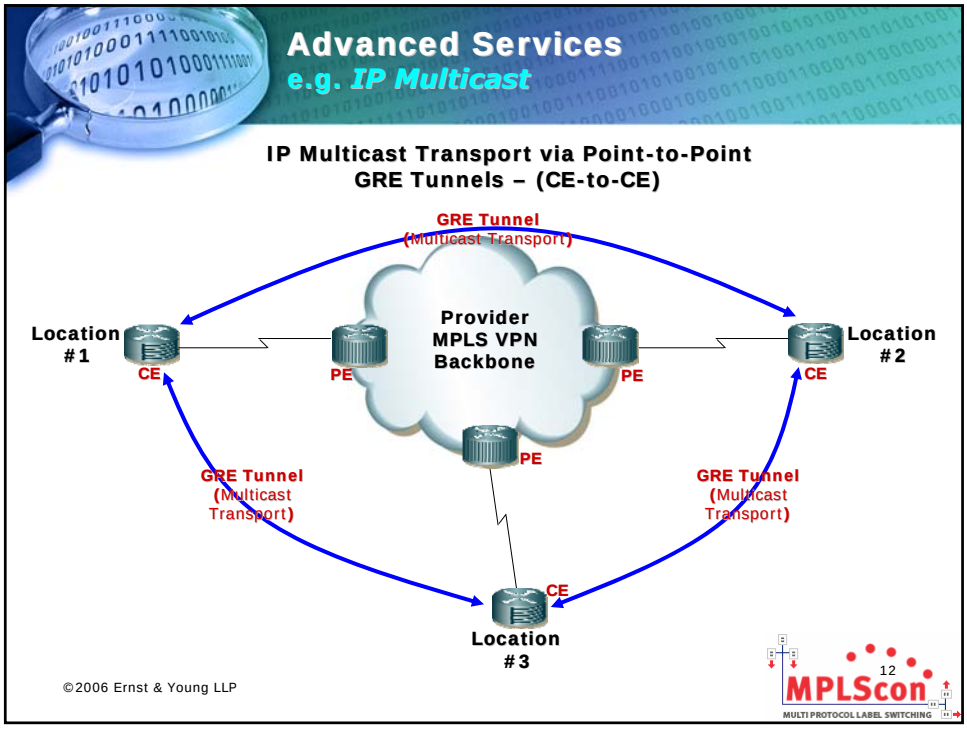


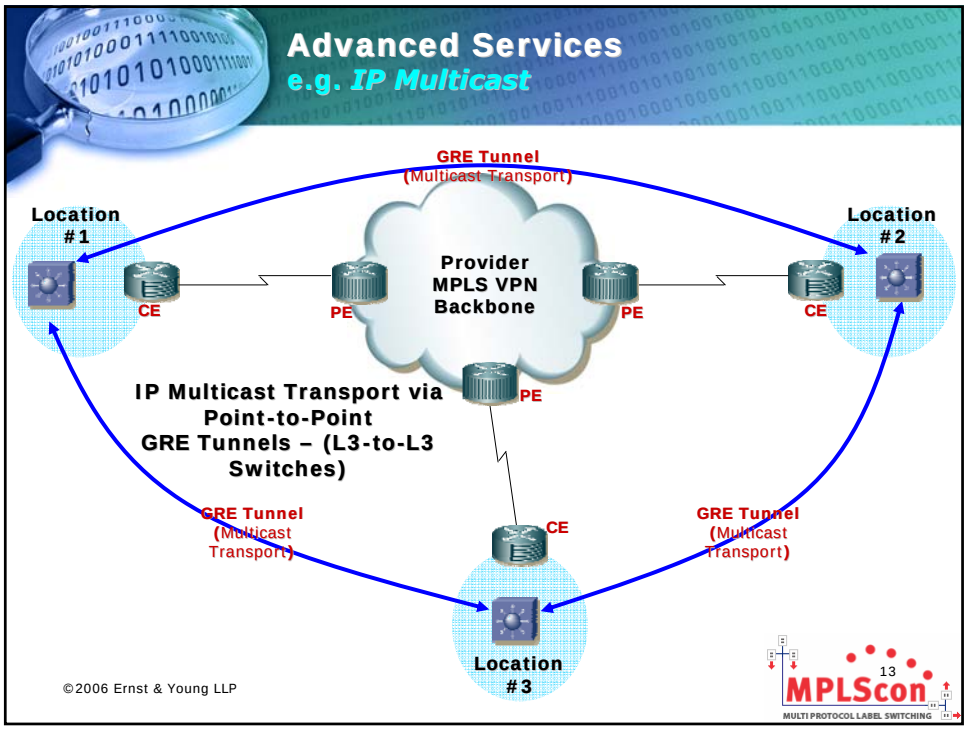



## Advanced Services

**Understanding of provider's MPLS advanced offerings to support services such as:**

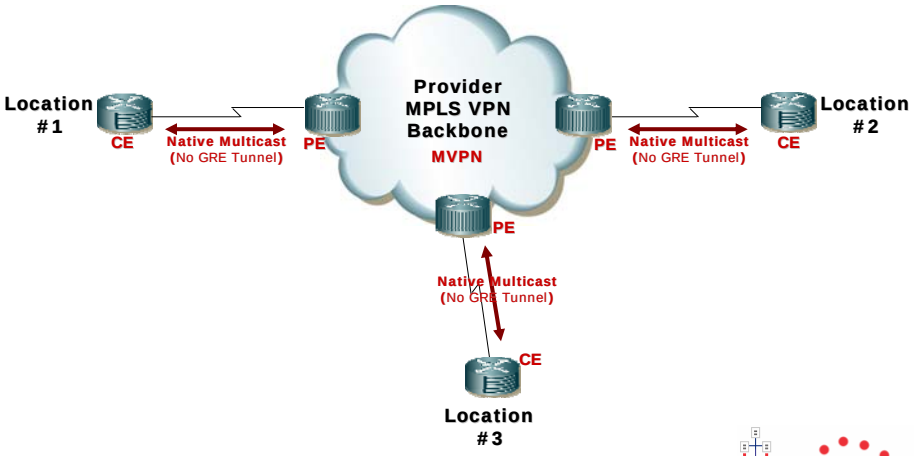
- IP Multicast (e.g., GRE tunnel, MVPN, etc.)
- Traffic encryption between all or selective locations
- IP Voice call processing functionality; *Voice over IP Gateway, IP Telephony call processing, on-net and off-net*
- IP Video bridging functionality; *point-to-point and point-to-multi-point*
- Internet Access Service
- Broadband Access Service (connectivity for small locations and Corp. Remote Access Users) to customer MPLS VPN


Advanced Services
e.g. IP Multicast
IP Multicast Transport via Point-to-Point GRE Tunnels – (CE-to-CE)
GRE Tunnel (Multicast Transport)
Location #1
CE
PE
Provider MPLS VPN Backbone
PE
PE
Location #2
CE
GRE Tunnel (Multicast Transport)
GRE Tunnel (Multicast Transport)
CE
Location #3
©2006 Ernst & Young LLP
12
MPLScon
MULTI PROTOCOL LABEL SWITCHING


Advanced Services
e.g. IP Multicast
GRE Tunnel (Multicast Transport)
Location #1
CE
PE
Provider MPLS VPN Backbone
PE
PE
Location #2
CE
IP Multicast Transport via Point-to-Point GRE Tunnels – (L3-to-L3 Switches)
GRE Tunnel (Multicast Transport)
GRE Tunnel (Multicast Transport)
CE
Location #3
©2006 Ernst & Young LLP
13
MPLScon
MULTI PROTOCOL LABEL SWITCHING

## Advanced Services
### e.g. *IP Multicast*

**Configuration of MVPN**



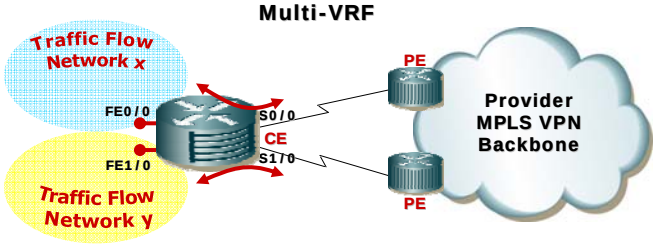





## Advanced Services
### *Traffic Separation*

**Understanding of Provider's virtual router capability with multiple routing tables (VRF tables);** *allows the logical association of those routing tables to separate logical or physical interfaces on CE device.*

**Multi-VRF**



## Security Consideration

**Understanding of provider's overall MPLS VPN Security features and controls; *Architecture, Implementation, Operation***

- Overall provider security reference model (VPN separation, Internet, Inter-providers)
- MPLS security implication over various tunnels (e.g. LSP, Native IP Core, etc.)
- Security issues not addressed by the MPLS Architecture
  - o Protection against mis-configuration in the core and attacks from within the core
  - o VPN data confidentiality, integrity, and origin authentication
  - o Attacks from the Internet through an MPLS backbone
  - o Customer Network Security





## Service Cost Model
### *Additional Service Cost*

**Understanding of cost component associated for additional MPLS service offerings;** *utilize the cost model as an initial guide to develop a cost/benefit analysis and determine the feasibility of converge services over MPLS (e.g. voice, video, etc.)*

- IP Multicast support
- IP Voice routing/processing functionality
- IP Video bridging functionality
- Internet access service
- Broadband access service
- Adding a new class of service
- Traffic Encryption
- Further, describe which services are within the standard price model or enhanced price model (requiring additional cost/customization).

## Service Cost Model
### *Deployment Time & Cost*

**Understanding of the provider approach to the MPLS deployment and associated cost.**

- Change Bandwidth (CDR) associated for specific Class of Service
- Change the status of classes of services (e.g., upgrade from one class to three classes)
- Change the status of an application in class of service; Add a new application to a class of service or remove it from particular class of service (e.g., in case of additional marking required on the CE device)
- Change the current status of CE from partial cloud to Any-to-Any connectivity or visa-versa
- Additional reporting requirements





## Questions