RA-MPLS
VPN Services

Kapil Kumar

Network Planning & Engineering – Data

E-mail: Kapil.Kumar@relianceinfo.com

Reliance
Infocomm

Agenda

- Introduction
- Why RA MPLS VPNs?
- Overview of RA MPLS VPNs
- Architecture for RA MPLS VPNs
- Typical Call Flow for RA MPLS VPN Customers
- Advantages

Reliance
Infocomm

Introduction

- Highly scalable and effective technology for deployment of IP VPN services

- Supports a wide range of services, including extranets, application hosting and e-commerce.

- Potential for additional revenue streams and increased ROI

Why RA-MPLS VPNs?

- Enabled by MPLS' technique for designating packets for transmission over explicit routes

- Does not rely on encapsulation and encryption to maintain a high level of security giving optimal performance.

- Extremely scalable and provides the ability for very large, fully meshed networks

- Metro Ethernet emerging as the next-generation access technology for service providers. But still far away to reach all customers because of cost and many other factors.

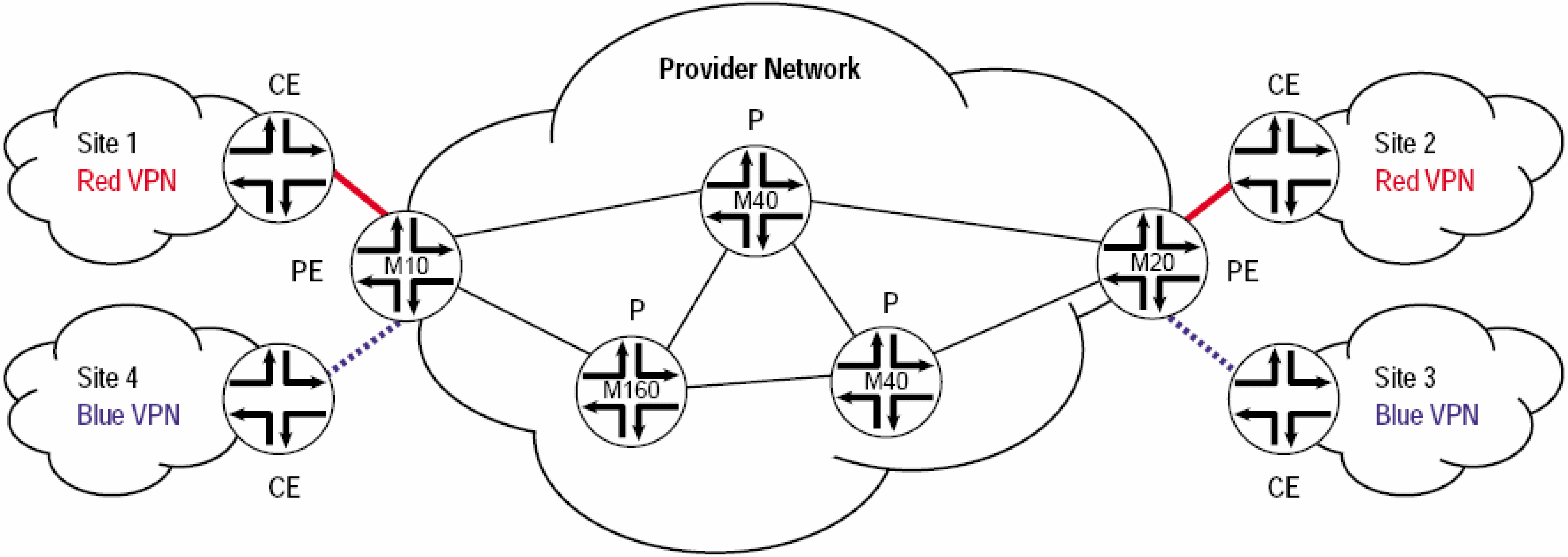
Why RA-MPLS VPNs? (...contd)

- Scalability —MPLS-based VPN deployment is capable of supporting tens of thousands of VPNs over the same network.

- Security—MPLS provides traffic separation between VPNs by using unique route distinguishers.

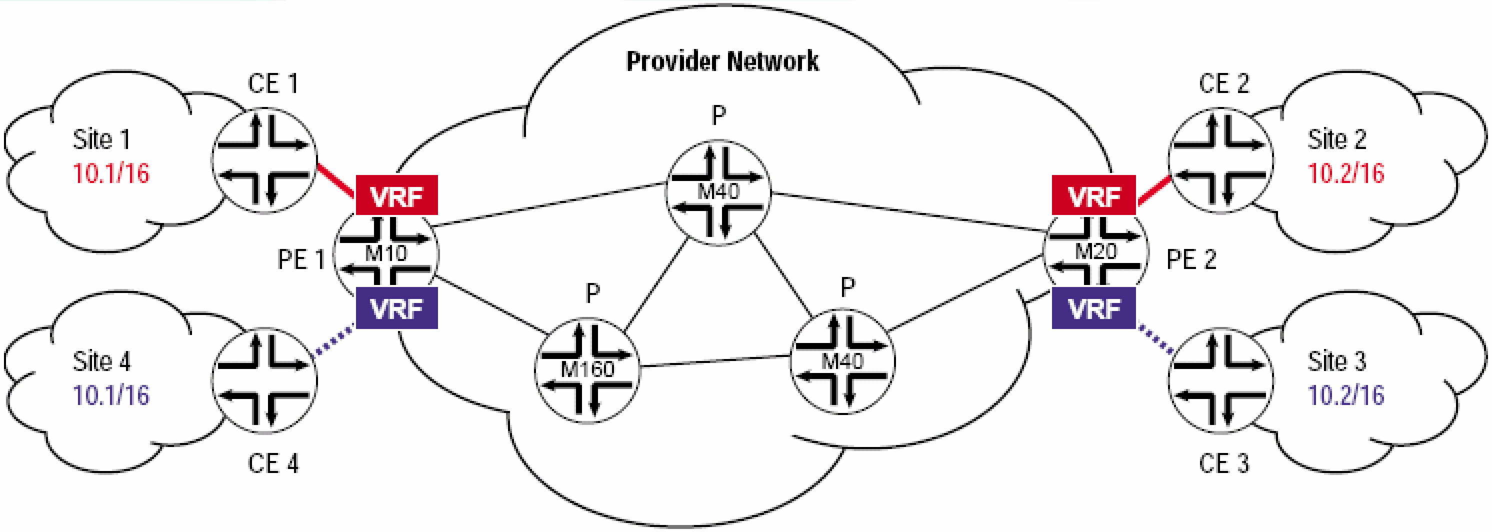
- Support for SLAs—A well-executed MPLS-based VPN implementation supports SLAs and service-level guarantees (SLGs) by providing scalable, robust QoS mechanisms, guaranteed bandwidth, and traffic engineering capabilities.

Overview of MPLS VPNs



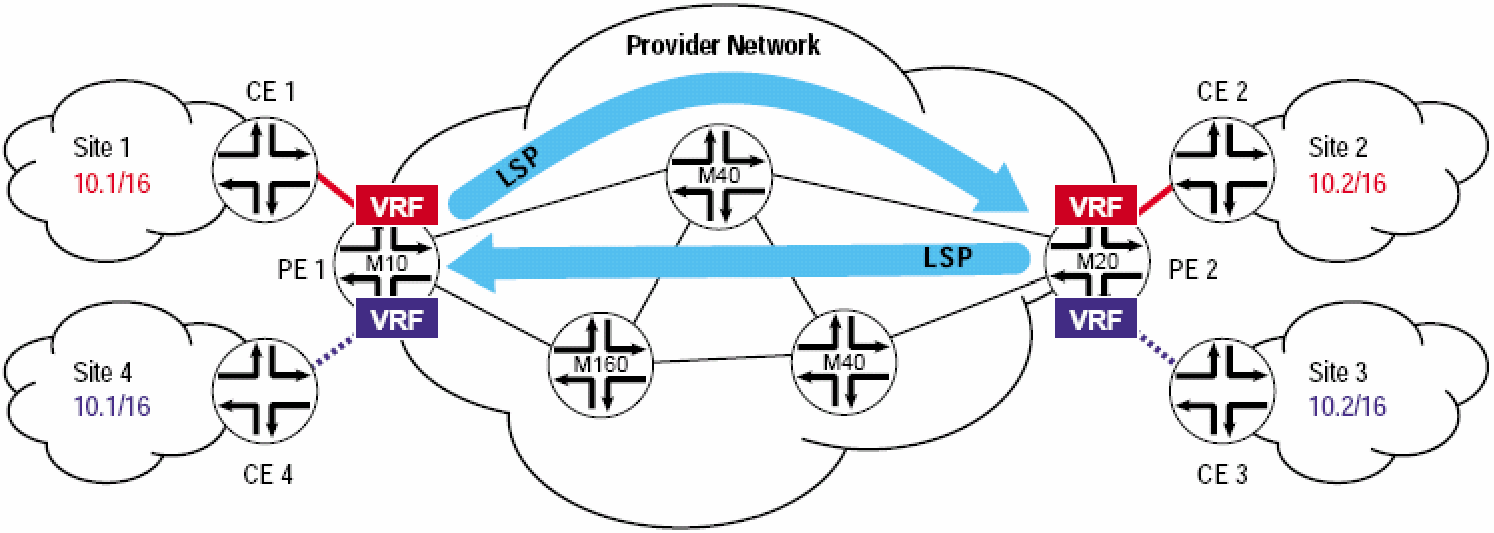
CE	=	Customer Edge
P	=	Provider Routers
PE	=	Provider Edge

Overview of MPLS VPNs (…contd)



CE = Customer Edge
P = Provider Routers
PE = Provider Edge
VRF = VPN Routing and Forwarding Table

Overview of MPLS VPNs *(...contd)*



Reliance Infocomm

Overview of MPLS VPNs (...contd)

- Routing protocol used to distribute VPN routing information across the provider's backbone and MPLS is used to forward VPN traffic from one VPN site to another.

- Edge routers have multiple routing and forwarding tables called VRF and routing information of a VPN remains inside a VRF.

- Labels are assigned based on VPN information received by routing protocols, thus isolating traffic to that VPN. The routing protocols create and store routing tables for each VPN on routers and switches throughout the carrier's backbone.

Overview of MPLS VPNs *(...contd)*

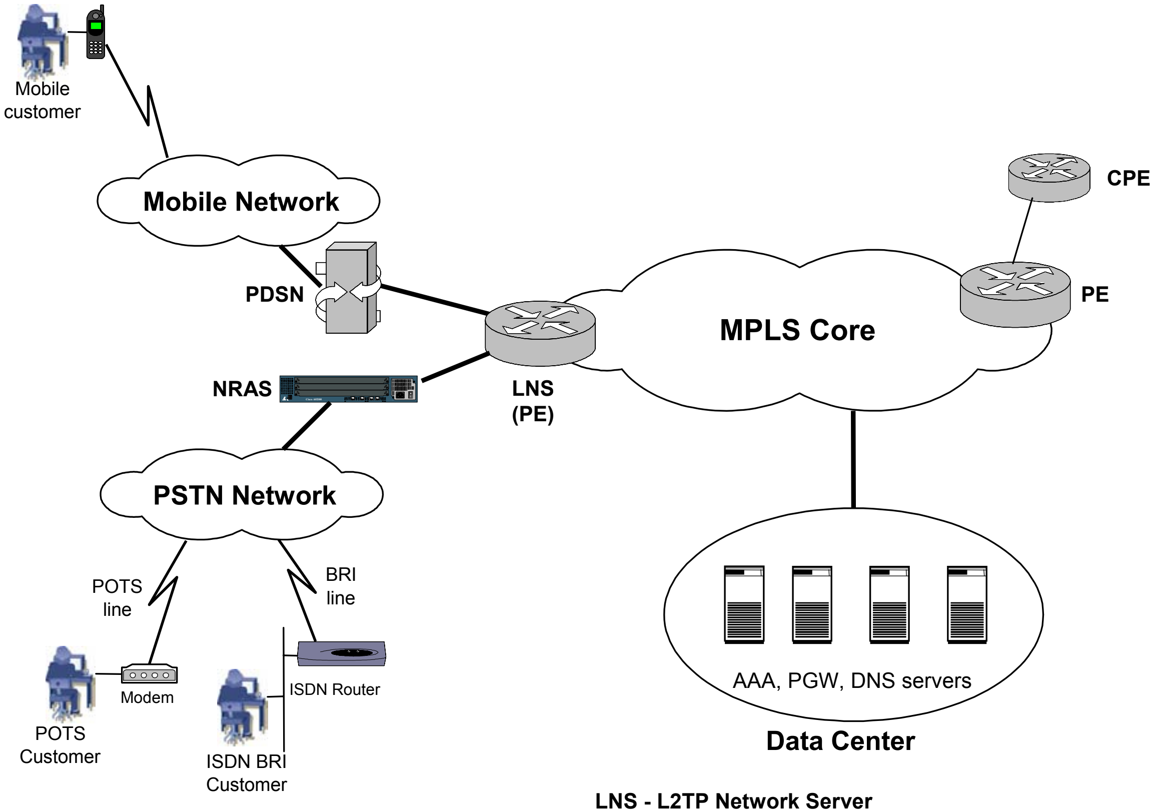
- Packet forwarding is performed using labels, or label values, instead of IP header information.

- Labels indicate routes as well as service (VPN) attributes.

- At the ingress edge, incoming packets are processed and labels are selected and applied. First a label indicating the VPN is applied, and on top of that a label identifying the route is applied.

- MPLS core reads only the upper label, and forwards packets based on the label. When the packets reach the egress edge, labels are removed and based on the inner label packets are forwarded to their final VPN destinations.

Architecture for RA MPLS VPNs



LNS - L2TP Network Server
PDSN - Packet Data Serving Node
PGW - Packet Gateway (used with SS7 signalling)

Reliance Infocomm

Architecture for RA MPLS VPNs (...contd)

- ***Customer Premises Equipments (CPE)***

Provides customer access to the service provider network over a data link to one or more provider edge (PE) routers.

- ***Narrowband Remote Access Server (NRAS)***

Customers having a PSTN connection or BRI connection dial up the number dedicated for VPN services.

The customer call is routed to the NRAS. The NRAS terminates the customer call and forwards the ppp session of the customer to the LNS by building an L2TP tunnel.

- ***Packet Data Serving Node (PDSN)***

PDSN works as a gateway for the wireless customers. It terminates connections from the wireless customers and forwards the ppp session to the LNS.

Architecture for RA MPLS VPNs (…contd)

➢ ***Provider Edge (PE) Routers***

- It exchanges routing information with CPE routers using static routing, RIPv2, OSPF, or EBGP.

- Maintains VPN routing information for those VPNs to which it is directly attached. This design enhances the scalability because it eliminates the need for PE routers to maintain all of the service provider's VPN routes.

- Each PE router maintains a VRF for each of its directly connected sites. Each customer connection is mapped to a specific VRF.

- Ability of PE routers to maintain multiple forwarding tables that supports the per-VPN segregation of routing information.

- After learning local VPN routes from CPE routers, a PE router exchanges VPN routing information with other PE routers using IBGP.

Architecture for RA MPLS VPNs (…contd)

- PE routers can maintain IBGP sessions to route reflectors as an alternative to a full mesh of IBGP sessions.

- When using MPLS to forward VPN data traffic across the provider’s backbone, the ingress PE router functions as the ingress LSR and the egress PE router functions as the egress LSR.

Architecture for RA MPLS VPNs (…contd)

➢ ***Provider (P) Routers***

• It is a router in the provider's MPLS core that does not attach to CPE devices.

• It functions as MPLS transit LSRs when forwarding VPN data traffic between PE routers.

• Since traffic is forwarded across the MPLS backbone using a two layer label stack, P routers are only required to maintain routes to the provider’s PE routers; they are not required to maintain specific VPN routing information for each customer site.

Architecture for RA MPLS VPNs (…contd)

➢ ***L2TP Network Server (LNS)***

- Terminates the ppp session of the customer forwarded by NRAS in L2TP tunnel.

- Single shared LNS can be used for terminating both wire line as well as wireless customers.

- Before terminating the ppp session, the customer is authenticated with use of an AAA server. Then the customer is put into his associated VPN.

- LNS works as a PE router for dial-up customers.

- It maintains VPN routing information of all customers connecting it, and advertises the routing information of customers dynamically whenever they connect or disconnect.

Architecture for RA MPLS VPNs (…contd)

➢ ***Packet Gateway (PGW) and Signalling Link Terminator (SLT)***

- It is deployed when out-of-band signalling is used.

- Out-of-band signalling does not consume bandwidth on the bearer channel and effectively increases the number of customers that can be supported.

- It works in conjunction with STP (Signal Terminating Point) for routing of the signalling information between PSTN Switch and NRAS.

Architecture for RA MPLS VPNs (…contd)

- ***AAA Server***

- The AAA server is used to authenticate, authorize and account the customers.

- NRAS and LNS sends the request to AAA for tunnel and user authentication and authorization

- AAA server authenticates the customer and returns authorization attributes if the authentication is successful. AAA server also stores accounting records which are used for billing.

Typical Call flow for RA-MPLS VPN customers

- Wireline customer dials the RA-MPLS VPN services number with his username and password, which lands on the NRAS device. If the customer is wireless, his call lands on PDSN.

- The NRAS or the PDSN builds an L2TP tunnel to the LNS and tunnels the ppp session of the customer inside it after the successful authentication

- LNS terminates the ppp session of the customers, and passes the authentication information i.e. “username and password” obtained during ppp negotiations to the AAA server in an access-request packet.

- AAA server issues an accept response to the LNS along with the customer profile information. The LNS requires the profile to set up the connection. If the RADIUS server is unable to authenticate the customer, it issues access-reject response to the LNS along with a text string indicating the reason.

Typical Call flow for RA-MPLS VPN (...contd)

- Customer is assigned an IP address and put into his VRF according to the AAA response after the customer is authenticated. The customer will then be part of his Enterprise network.

- AAA server generates billing logs as soon as the dial-up session is established and also when the session is terminated. This billing information is then exported to the billing servers for billing purposes.

Advantages

- No constraints on the address plan used by each VPN customer. The customer can use either globally unique or private IP address spaces.

- CPE router at each customer site does not directly exchange routing information with other CPE routers.

- Providers do not have a separate backbone or virtual backbone to administer for each customer VPN. Thus, providers do not require management access to CPE routers.

- By using the PSTN network, anytime-anywhere connectivity is possible thus enabling customers to work from home, hotel or anywhere

Advantages (…contd)

- Allows low-speed network access using a dial-up connection
- With ISDN technology, speed as much as 2 Mbps can be delivered
- With growing base of mobile customers, the service providers can offer value add to their customers by offering VPN services through mobile networks.

Thank you

Reliance
Infocomm