IP VPN Management

Samsung Electronics
Telecom R&D Center
Yongseok Park

Taxonomy

- Data Service
  - Private Line
  - Frame Relay
  - ATM
  - Internet Access
    - Dial-up, Broadband, Private line, ATM, Frame relay, Ethernet
    - Managed or Do-it-yourself
  - IP VPN
    - Network based
    - Premise based
      - IPSec based
        - Remote Access
        - Site to Site
      - SSL based

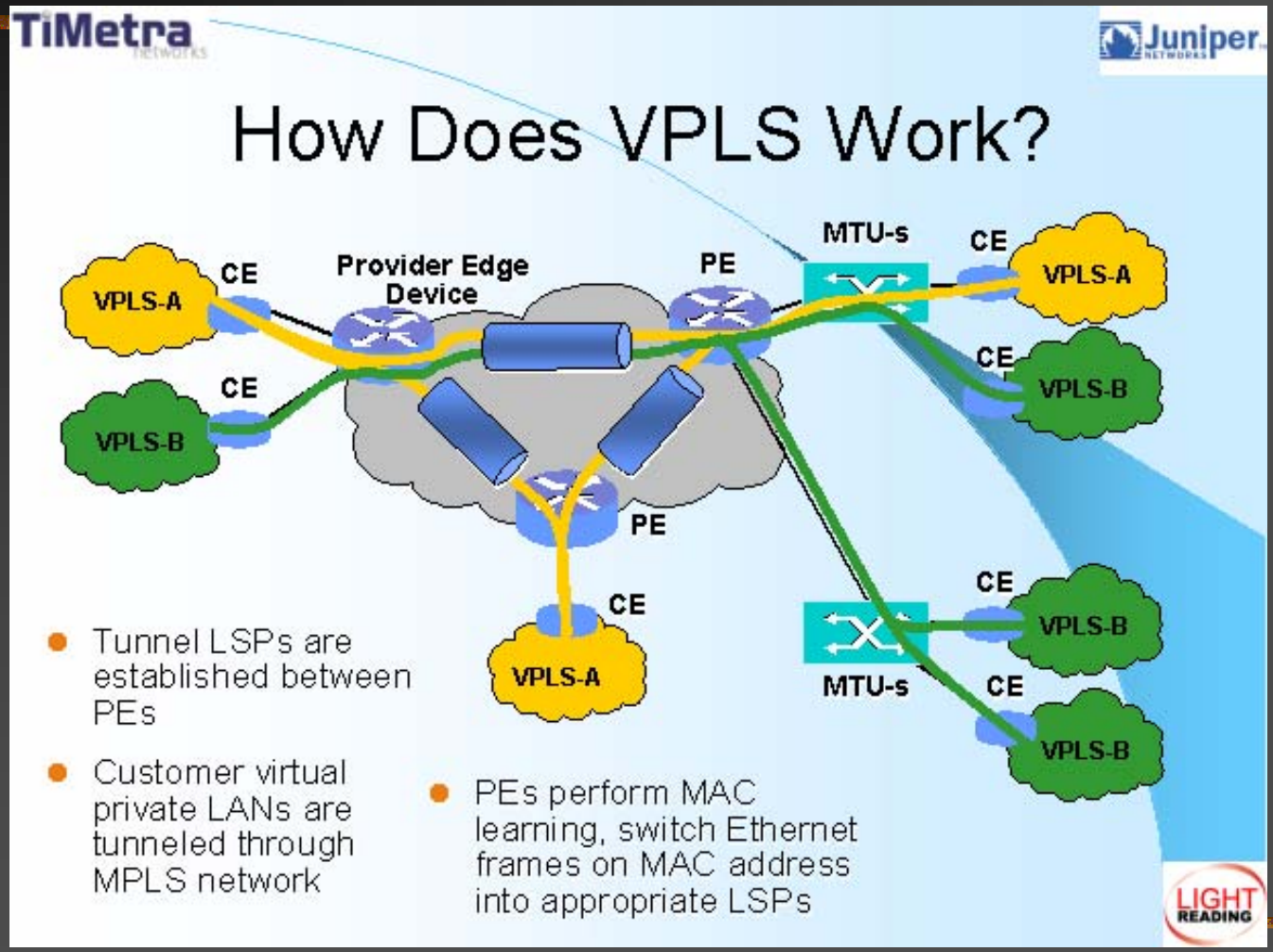
Network based IP VPN

- Layer 3 VPN
  - BGP/MPLS based (rfc2547)
  - Virtual Router based
  - IPSec VPN
- Layer 2 VPN
  - VPLS (Virtual Private LAN Service)
  - VPWS (Virtual Private Wire Service)
  - IPLS (IP-only LAN-like Service)
    - Functional subset of VPLS

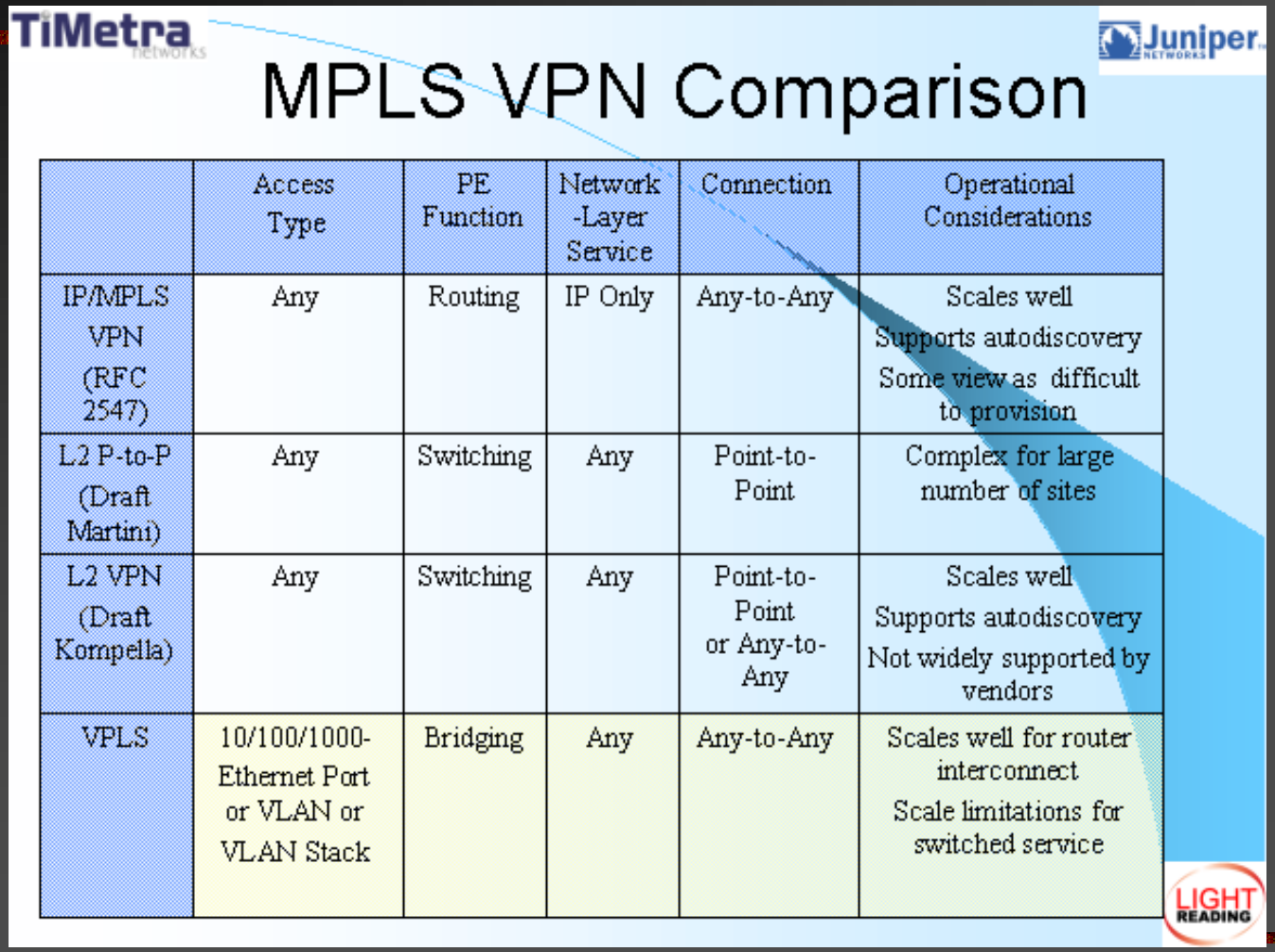
BGP/MPLS VPN

- RFC2547 based
- Two-level Label Stacking
  - Outer label for tunneling
    - Signaled by LDP or RSVP-TE
  - Inner label for VPN identification
    - MP-iBGP (PE to PE)
- CE (Customer Edge) router to PE (provider Edge) router
  - Static, rip, ospf, isis, eBGP
- PE router
  - VRF (VPN Routing and Forwarding) table per VPN

VPLS


TiMetra Networks
Juniper Networks
How Does VPLS Work?
VPLS-A
CE
Provider Edge Device
PE
MTU-s
CE
VPLS-A
CE
VPLS-B
CE
VPLS-B
PE
CE
VPLS-A
CE
VPLS-B
MTU-s
CE
VPLS-B
Tunnel LSPs are established between PEs
Customer virtual private LANs are tunneled through MPLS network
PEs perform MAC learning, switch Ethernet frames on MAC address into appropriate LSPs
LIGHT READING

MPLS VPN Comparison



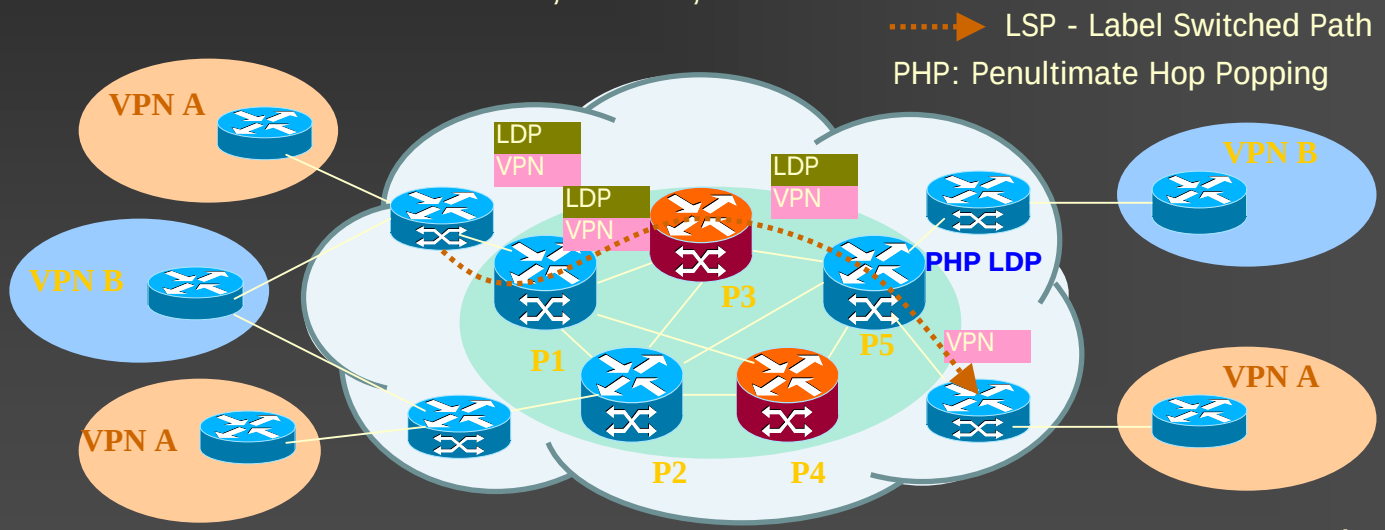
	Access Type	PE Function	Network -Layer Service	Connection	Operational Considerations
IP/MPLS VPN (RFC 2547)	Any	Routing	IP Only	Any-to-Any	Scales well Supports autodiscovery Some view as difficult to provision
L2 P-to-P (Draft Martini)	Any	Switching	Any	Point-to-Point	Complex for large number of sites
L2 VPN (Draft Kompella)	Any	Switching	Any	Point-to-Point or Any-to-Any	Scales well Supports autodiscovery Not widely supported by vendors
VPLS	10/100/1000-Ethernet Port or VLAN or VLAN Stack	Bridging	Any	Any-to-Any	Scales well for router interconnect Scale limitations for switched service

Deployment Scenarios – AT&T case

Case Study 1: VPN (PE) + LDP (P,PE)

Configuration:

- IGP (e.g. OSPF, or IS-IS) routing in the core
- MPLS (e.g. LDP) enabled for all P and PE routers
- MP-iBGP fully meshed between PE's
- VPN configured on VPN PE's
- PE-CE can be e-BGP, OSPF, RIP or Static



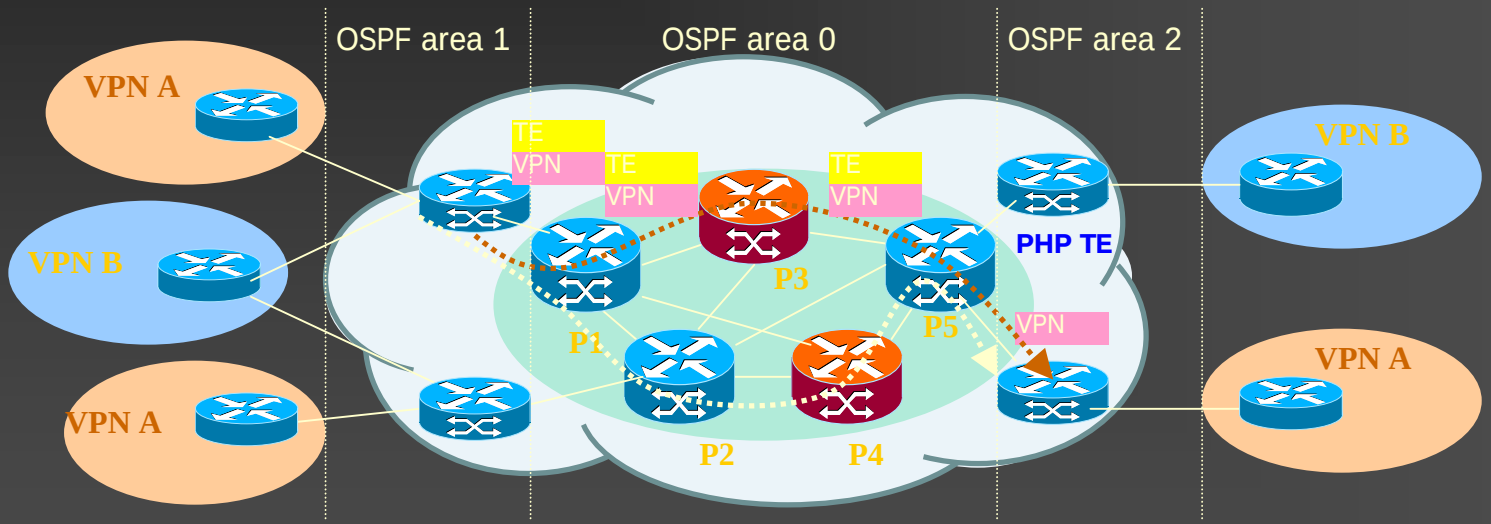
<L. Fang, AT&T>

- Setting up LSP through LDP, LSP path = IGP path - Simplicity
- Requires LDP interoperability; VPN/LDP inter-working
- No control on LSP, label failure on IGP path can cause VPN failure

Case Study 2: VPN (PE) + RSVP TE (PE-PE)

Configuration:

- Using RSVP TE Tunnel (PE-PE) to set up the LSP
- Set up back-up tunnel for failure protection
- IGP, BGP, VPN, and PE-CE link configuration as in Case 1



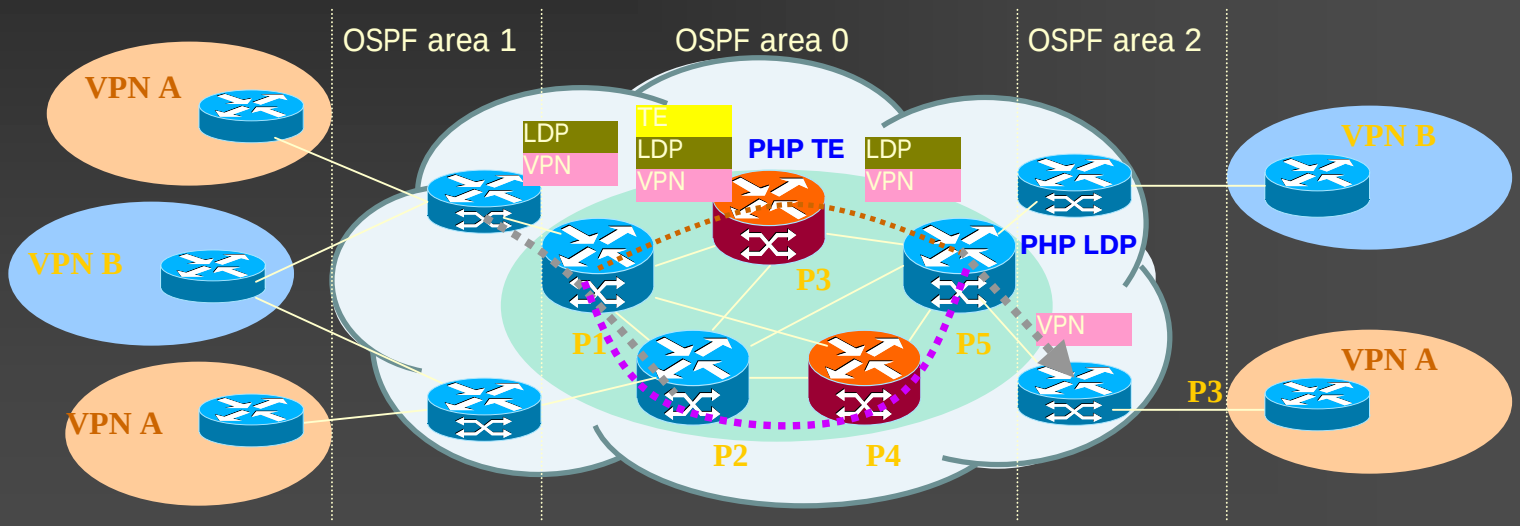
<L. Fang, AT&T>

- Requires RSVP TE tunnel, potentially across multi-OSPF areas
- Requires RSVP TE interoperability; VPN / TE inter-working
- End-to-end LSP control - better failure protection, fast re-route may be used

Case Study 3: VPN + LDP + RSVP TE Tunnel

Configuration:

- LDP enabled on all routers, *except P4 and P5*
- RSVP TE Tunnels used only in OSPF area 0 (P1-P3-P5), with back-up tunnel (P1-P2-P4-P5)



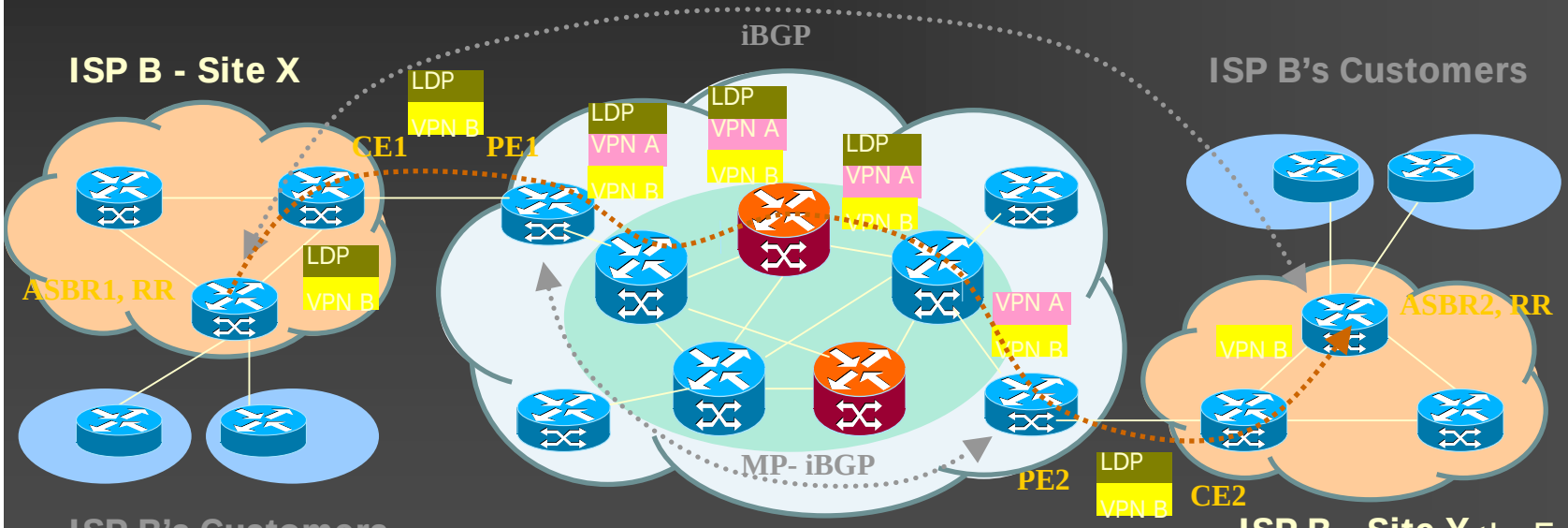
<L. Fang, AT&T>

- Requires RSVP TE interoperability
- Requires VPN/LDP inter-working, LDP/TE inter-working
- Provides feasible solutions when cases 1 and 2 cannot be realized

Carrier's Carrier VPN

ISP A backbone provides VPN services to ISP B

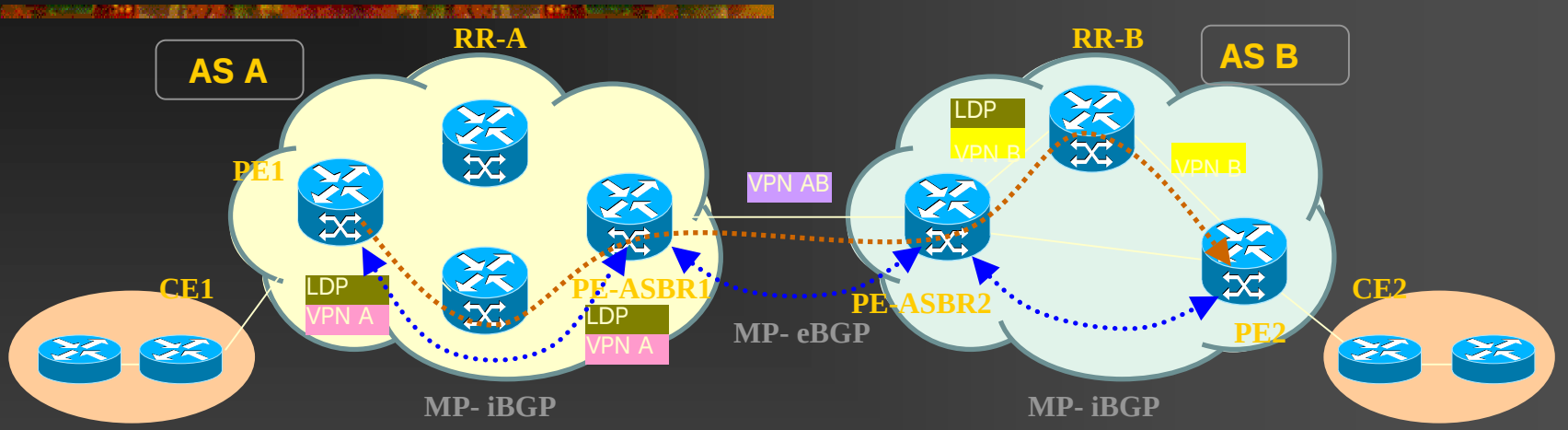
- Case 1. ISP B may not run MPLS in its network
- Case 2. ISP B may run MPLS (LDP) in its network
- Case 3. ISP B may run MPLS VPN in its network - Hierarchical VPN's



<L. Fang, AT&T>

Carrier's Carrier VPN Case 3

Inter-Providers Backbone VPN

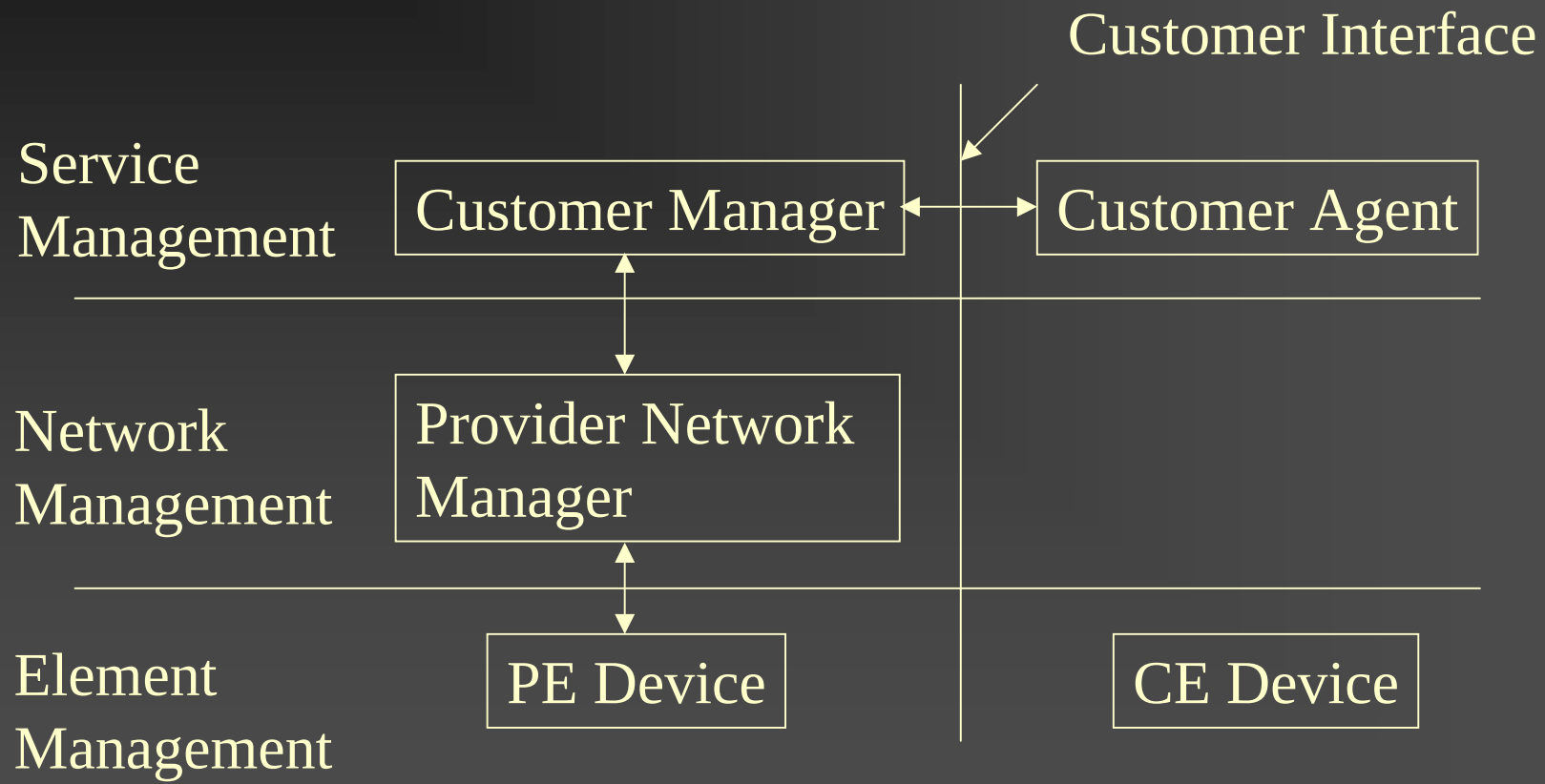


- Customers have sites connected to different AS's or ISP's
- PE-ASBR's connect the two AS's
  - E-BGP sessions for VPN-IPv4
  - single VPN label, no LDP label
  - no VRF assigned, based on policy agreed by the two ISP's (AS's)
- Route reflectors reflect VPN-IPv4 internal routes within its AS
- Security, scalability, policies between ISP's

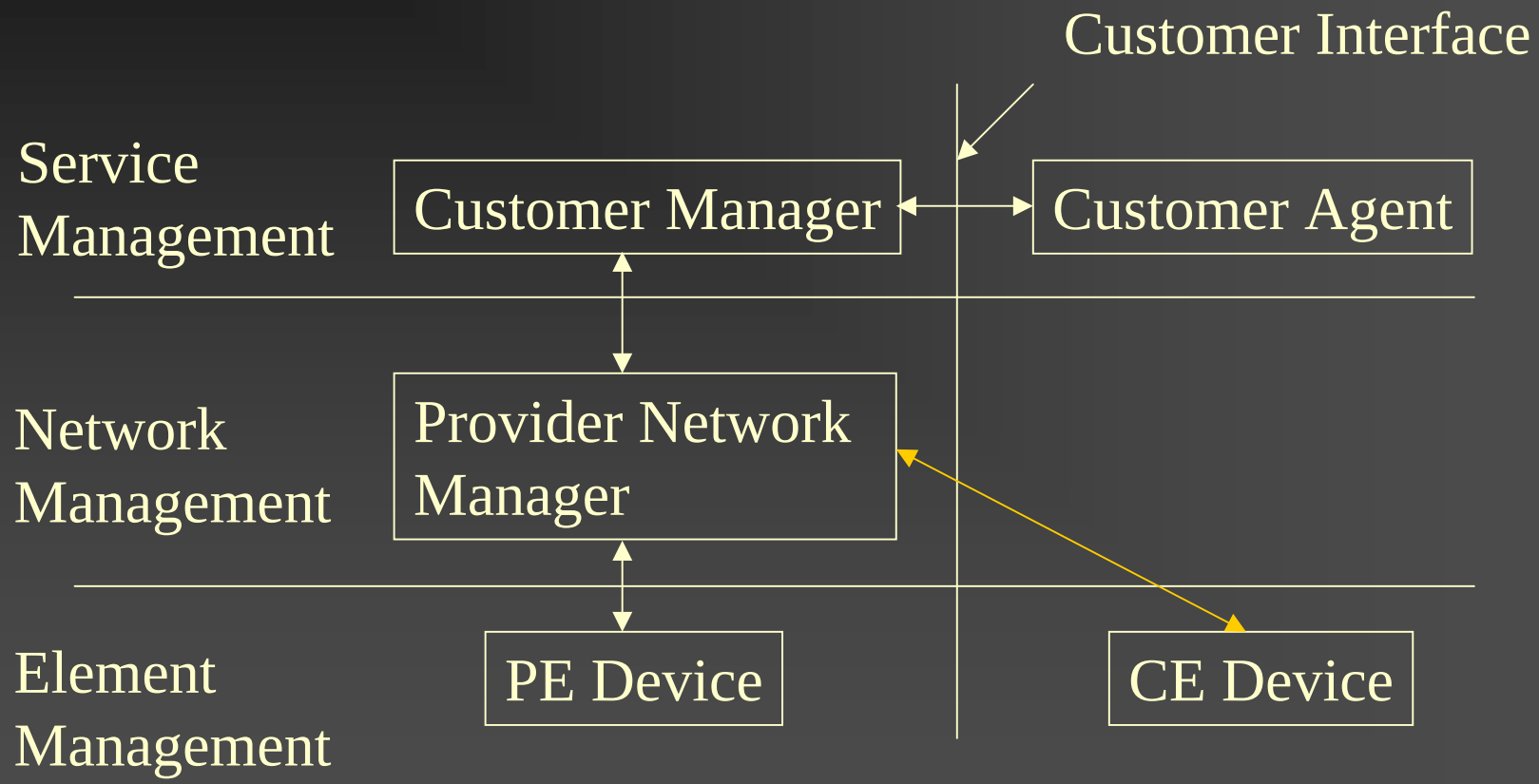
<L. Fang, AT&T>

Framework for PPVPN Operations and Management

PE-based Management



CE-based Management



Customer Manager/Agent

- Definition
  - Provides customer-specific topology, operational state, order status, etc.
- Customer Agent
  - Make dynamic requests for changes to service parameters

Customer management information model

- SLA/SLS content
  - Per access connection, VPN, site, etc
  - Service Level Objects
    - QoS and traffic parameters
    - Availability for the site, VPN, and access connection
    - Duration of outage per site, route, or VPN
    - Trouble report response time
    - Time to repair
    - Total traffic offered to the site, route, or VPN
    - Measure of non-conforming traffic for the site, route, or VPN

Customer Management Functions

- Fault management
  - Indication of customer's service impacted by failure
  - Incident recording or logs
- Configuration Management
  - Service templates for customer's configuration
    - Examples
      - IPSec tunnel setup
        - Tunnel end points, authentication modes, encryption and authentication algorithms, pre-shared keys, traffic filters
      - BGP/MPLS VPN service: sites
      - QoS agreement
        - Throughput, delay, jitter, packet loss

Customer Management Functions

- Accounting
  - Retrieval of accounting information from Provider Network Manager
  - Analysis, storage, and administration of measurements
- Performance management
  - Provide measurements w.r.t. SLS
  - Support analysis of measurements
  - Capacity Planning for Customer VPN

Customer Management Functions

- Security management
  - Management access control
  - Authentication
    - PE to PE
    - CE to PE

Provider Network Manager

- Definition
  - Provides customer-specific topology, operational state, order status, etc.
  - Provides underlying logical and physical topology, operational state, provisioning ststus, etc associated with network

Network Management Functions

- Fault Management
  - Fault detection (reports, alarms, failure visualization)
  - Fault localization (analysis of alarms, diagnostics)
  - Corrective actions (traffic, routing, resource allocation)

Network Management Functions

- Configuration management
  - PE-based VPN
    - Intranet/extranet membership, CE routing
    - Tunnels between PE and P devices
    - Routing protocols running between PE routers, and between PE and P routers
    - Configuration of Layer 1 and 2 networks
  - CE-based VPN
    - Tunnels between CE devices
    - Routing protocols between PE and CE devices
  - Routing
  - Network access
  - Security service
  - VPN resource parameters
  - Value-added service access
  - Hybrid VPN services

Network Management Functions

- Accounting Management
  - Measurement of resource utilization
- Performance Management
  - Monitoring and collecting performance data regarding devices, facilities, and services
  - Threshold crossing alerts (TCA)
  - Capacity Planning for Service Provider
- Security Management
  - Management features to guarantee security of customer data and control

Standard MIBs/PIBs

- Standard MIBs for routing protocols
  - [IPSEC-PIB] draft-ietf-ipsp-ipsecpib-04
  - [Diffsev MIB] RFC3289
  - [Diffserv QoS PIB] RFC3317
  - [MIB-2547] draft-ietf-ppvpn-mpls-vpn-mib-04
  - [PIB-2547] draft-yacine-ppvpn-2547bis-pib-02

MPLS-VPN-MIB

- mplsVpnVrfTable
- mplsVPNInterfaceConfTable
- mplsVPNPerfTable
- mplsVpnVrfRouteTable
- MplsVpnRouteTargetTable

Communication Protocols

- SNMP
- COPS-PR
- LDAP
- Netconf XML

Tools

- Cisco
  - IP Solution Center MPLS VPN module
    - VRF
    - PE-CE routing
    - Multicast VPN
    - Auto-discovery of MPLS VPN service
    - Role-based access control
    - Automatic Resource allocation
    - Inter-AS support
    - L2 access to MPLS VPN
    - CORBA and XML interface

Tools

- Metasolv
  - Orchestream Service Activator
    - BGP/MPLS VPN
      - Cisco, Juniper, Alcatel
      - Automated VRF table
      - iBGP peering iBGP PE’s
      - Static, rip, ospf, eBGP peering between PE and CE
    - VPLS
      - Riverstone

Tools

- Trendium
  - ServicePATH
    - Management of Application Service (VoIP)
    - Management of CE-CE Service
    - Management of MPLS tunnels
    - Interface and device statistics
    - Probes
    - QoS policies

Tools

- HP OpenView
  - NNM smart plug-in for MPLS VPN
    - PE interface impact on VPN information
    - PE-CE link management
    - Discovery of interface to VRF and VPN relationships
    - Core MPLS VPN network availability
    - Cisco SAA test configuration utility

Conclusions

- BGP/MPLS Service has many components to manage
- Efficient Operations Architecture is key to rapid deployment of profit generation
- Highly integrated solution is wanted
  - OSS
  - NMS
  - Device