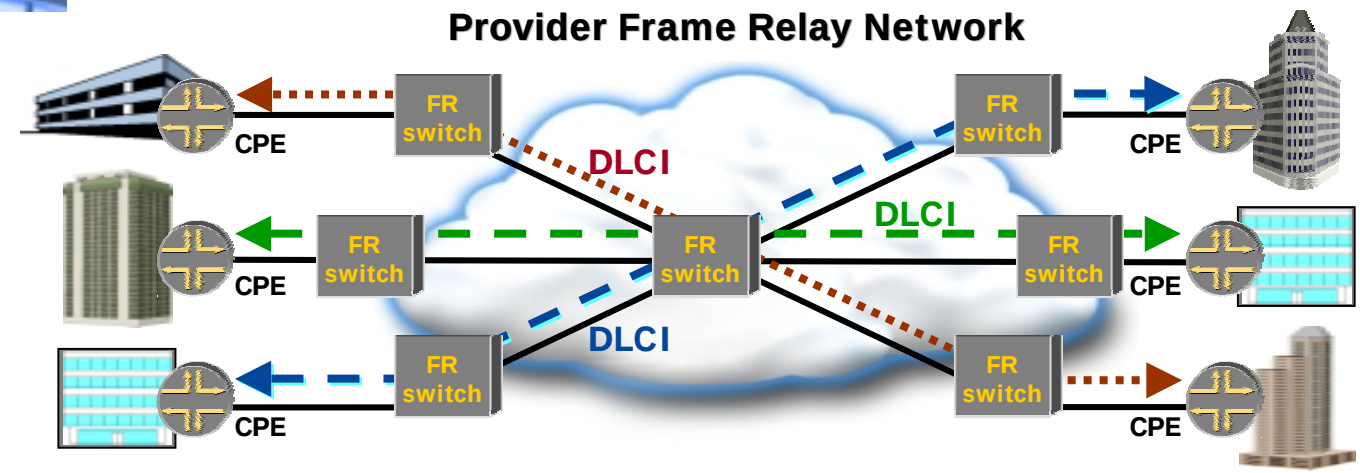
The MPLS Advantage

Part IV:
Virtual Private Networks (VPNs)

Agenda: Virtual Private Networks (VPNs)

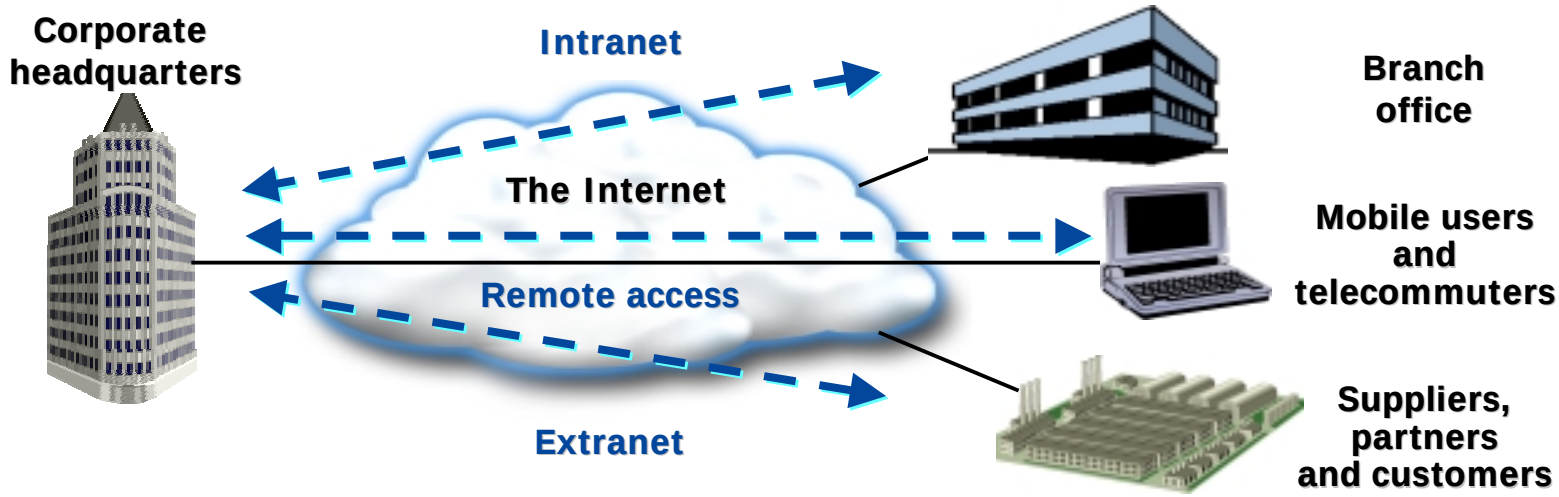
- Deploying VPNs in 1990s
- Deploying VPNs in the 21st century
- CPE-based VPNs (CPE-VPN)
  - L2: L2TP and PPTP
  - L3: IPSec
- Network-based VPNs (NB-VPN)
  - L3: RFC 2547bis
  - L3: Virtual Routers
- Hybrid CPE/NB-VPNs
  - Traditional Circuit Cross Connect
  - MPLS-based Layer 2 VPNs
- Conclusions

Deploying VPNs in the 1990s



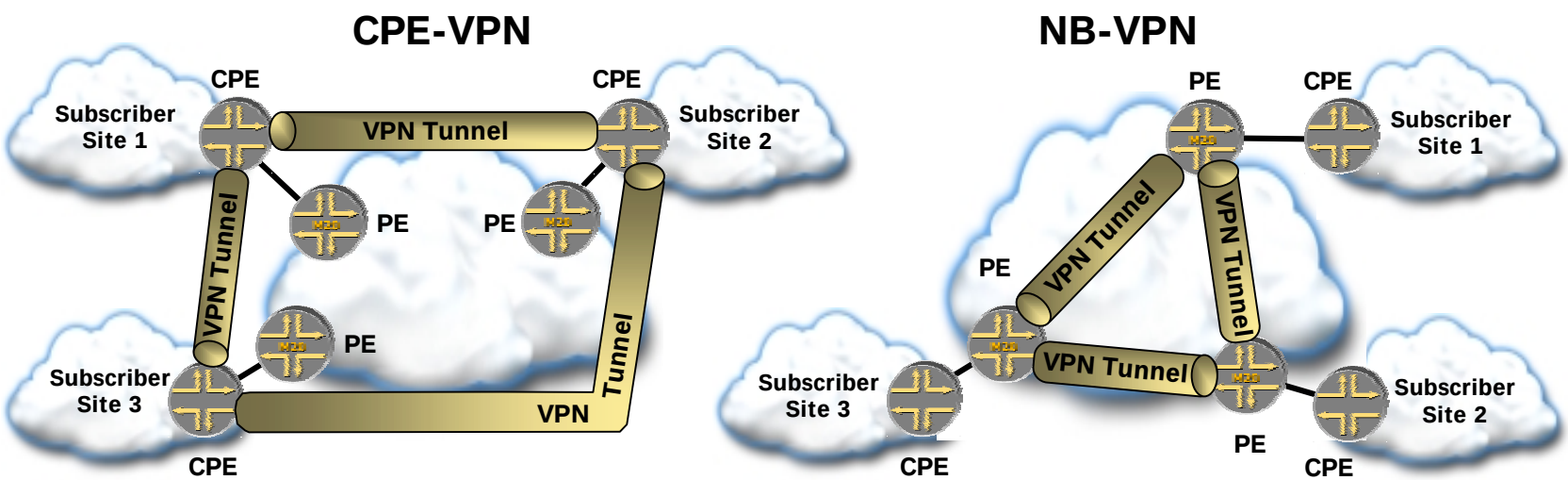
- **Operational model**
  - PVCs overlay the shared infrastructure (ATM/Frame Relay)
  - Routing occurs at CPE
- **Benefits**
  - Mature technologies
  - Inherently 'secure'
  - Service commitments (bandwidth, availability, etc.)
- **Limitations**
  - Scalability and management of the overlay model
  - Not a fully integrated IP solution

Deploying VPNs in the 21st Century



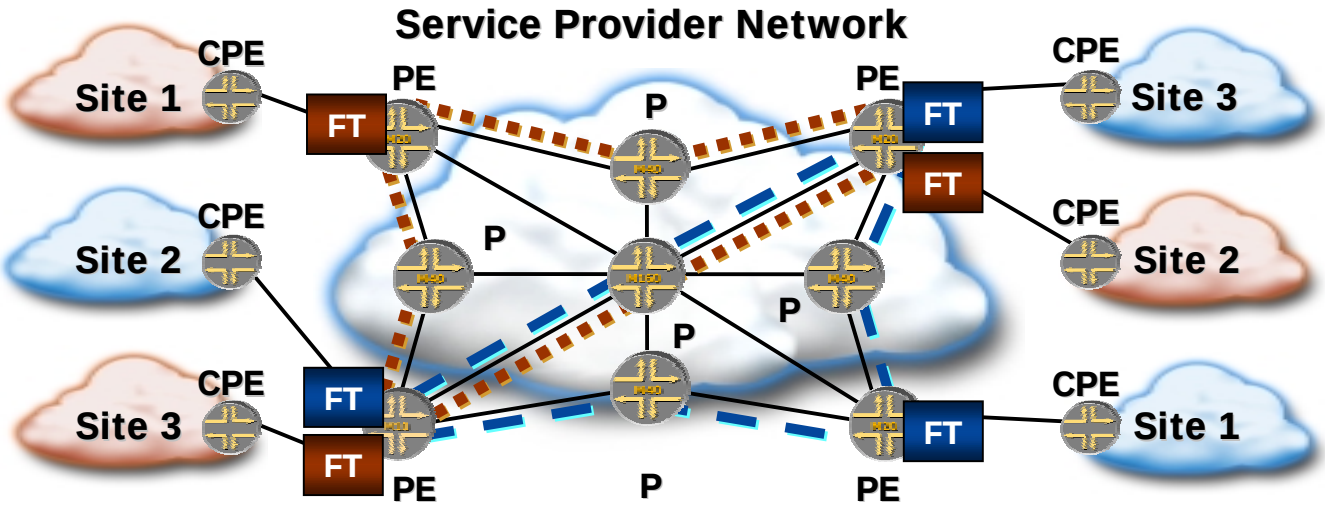
- The Internet is the shared infrastructure
- Increasing importance of IP/MPLS (not ATM/FR)
- Subscriber requirements
  - A single network connection for all services
  - Semi-public connectivity rather than private connectivity
- Provider requirements
  - Multiservice infrastructure that supports all services
  - Enhance the provider's role in VPN solutions

IETF VPN Classification Model



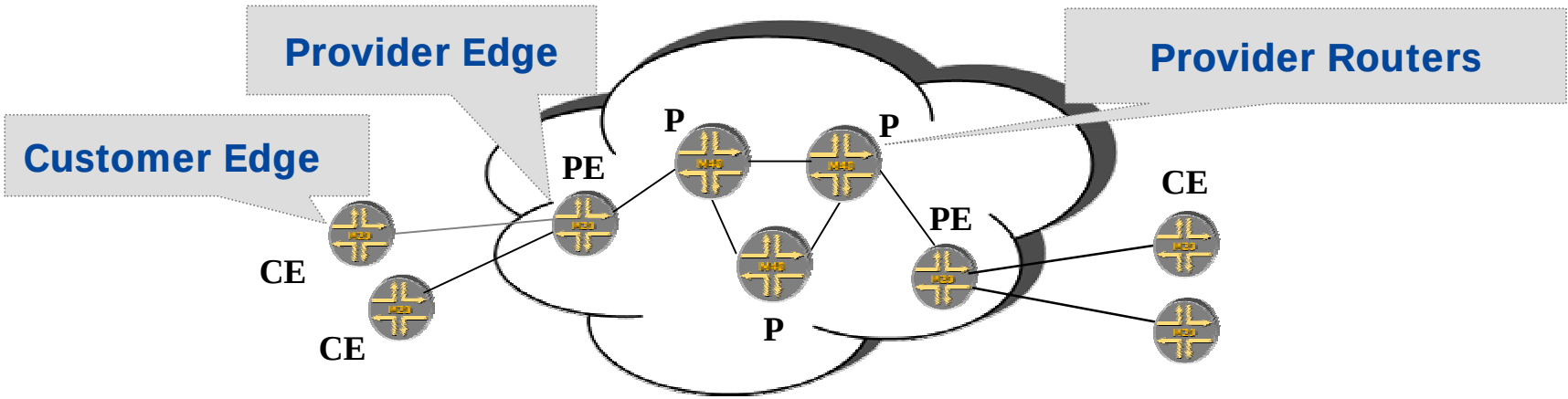
- **CPE-Based VPN Solutions (CPE-VPNs)**
  - **Layer 2: L2TP and PPTP**
  - **Layer 3: IPSec**
- **Network-Based VPN Solutions (NB-VPNs)**
  - **Layer 3: MPLS-Based VPNs (RFC 2547bis)**
  - **Layer 3: Non-MPLS-Based VPNs (Virtual Routers)**

Layer 3 Network Based (NB)-VPNs



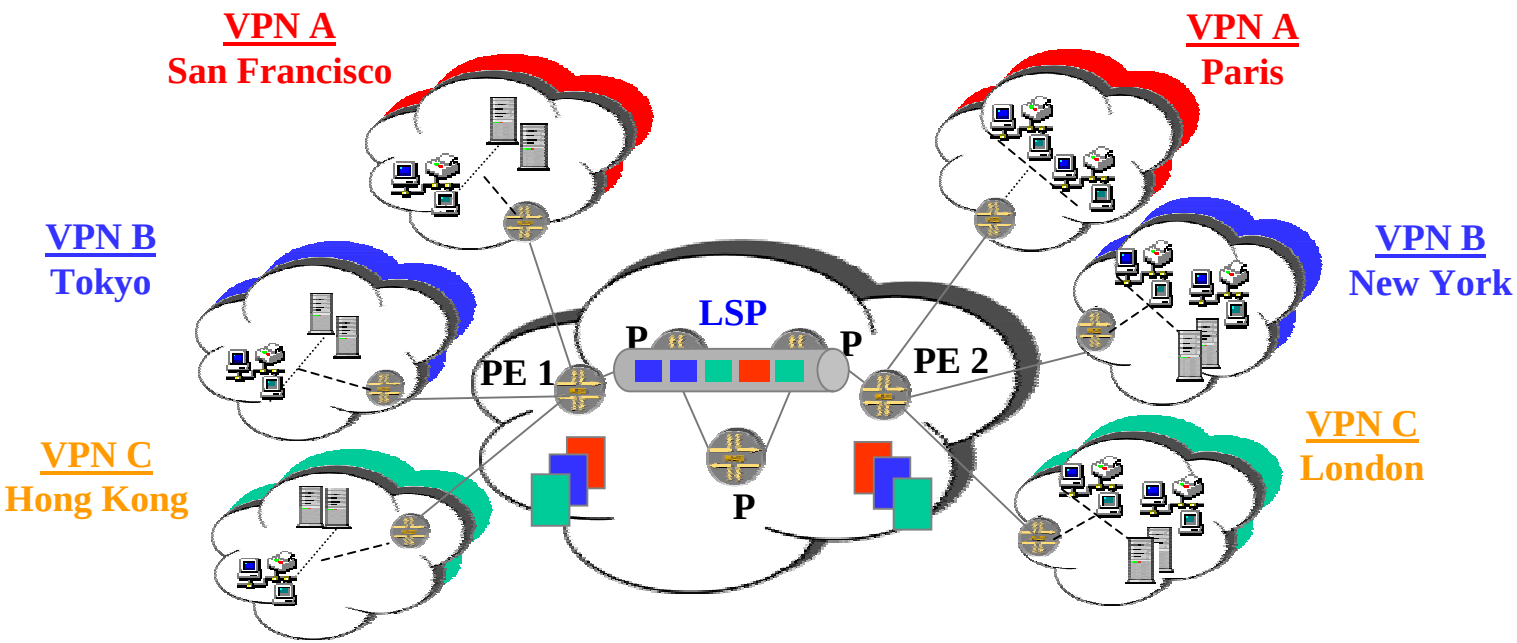
- Application: large or small enterprise VPNs
- Architecture
  - Conventional IP routing between CPE and PE
  - PE maintains site-specific forwarding tables for each of its directly connected VPN sites
- RFC 2547bis – Internet Draft (Juniper is a co-author)

RFC 2547bis Routers



- **P routers** – Provider Core routers that support MPLS LSR functionality. These routers are not VPN aware
- **PE routers** – Provider Edge routers that support MPLS LER functionality. These routers interface with customer sites and are VPN aware
- **CE routers** – Customer Edge routers located at customer premises. Provides access to the service provider network

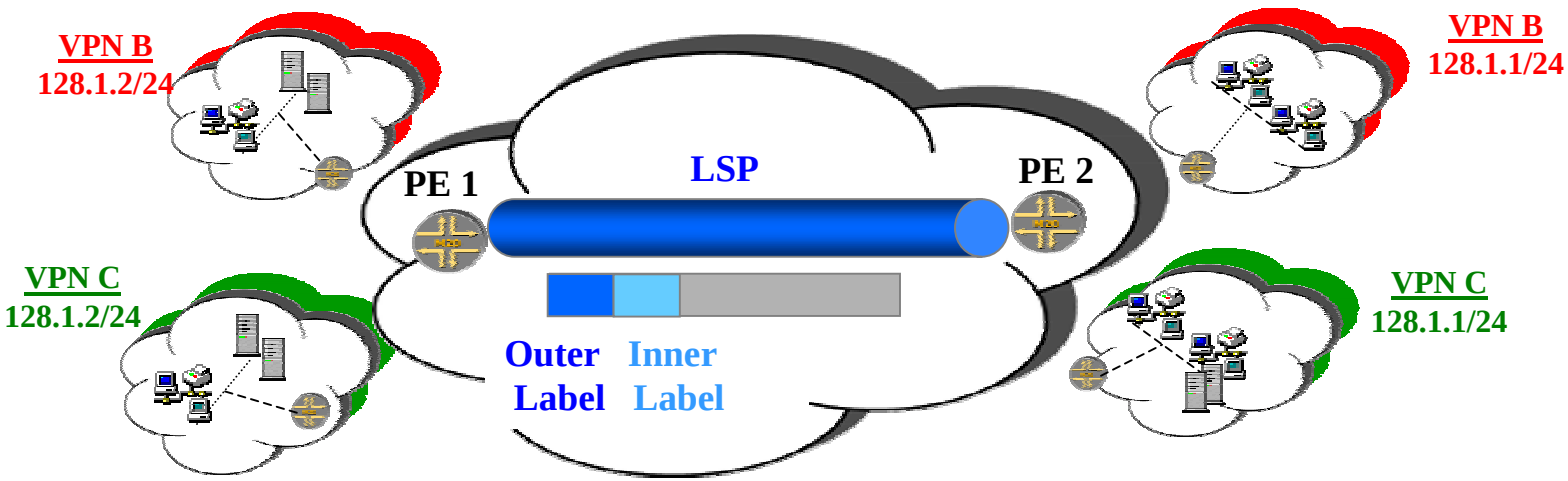
RFC 2547bis Model



- BGP is used to distribute routing information
- Each PE maintains a separate routing table for each site – VPN Routing and Forwarding or VRF tables
- Core MPLS LSP can be set up statically, or via LDP or RSVP and transports VPN traffic from ingress PE to egress PE

RFC 2547bis Forwarding Across the Backbone

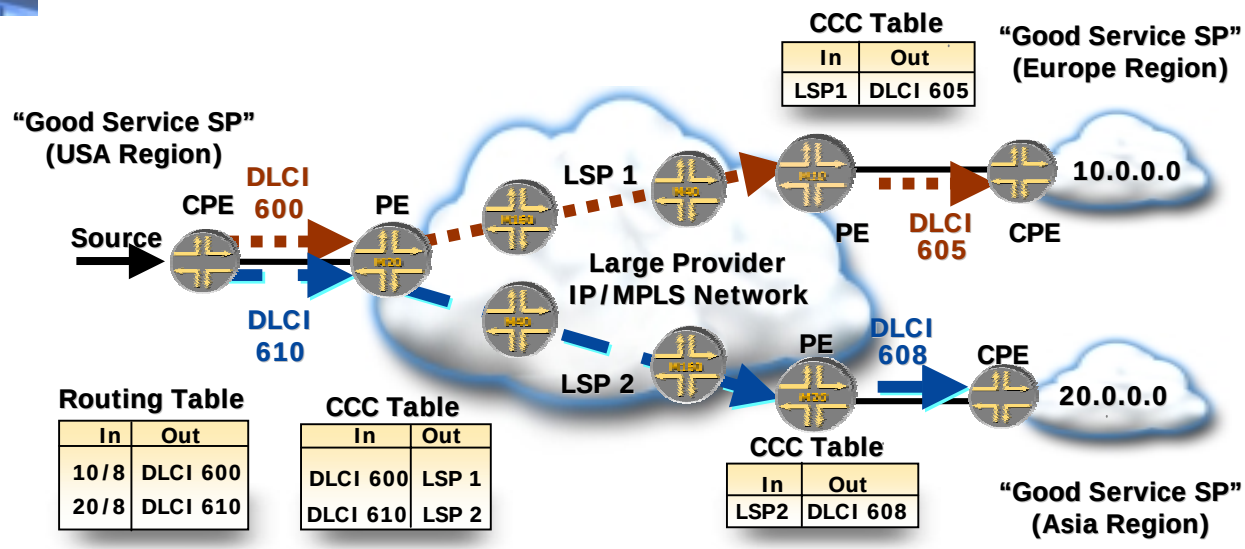
- P routers are not VPN aware
- PE to PE forwarding is tunneled through MPLS LSPs via two-level label stack
  - RFC 2547bis does not specify protocol for signaling backbone LSPs



BGP / MPLS VPNs (2547bis)

- LDP or RSVP sets up PE to PE tunnels
- BGP is used to distribute:
  - Information about the VPN (discovery)
  - Routing / reachability for the VPN
  - Labels for per-VPN LSPs
- Flexible control mechanism
  - “Route targets” control which routes are distributed to which PE routers
  - Supports intranets, extranets

Hybrid CPE/NB-VPN: Traditional Circuit Cross Connect

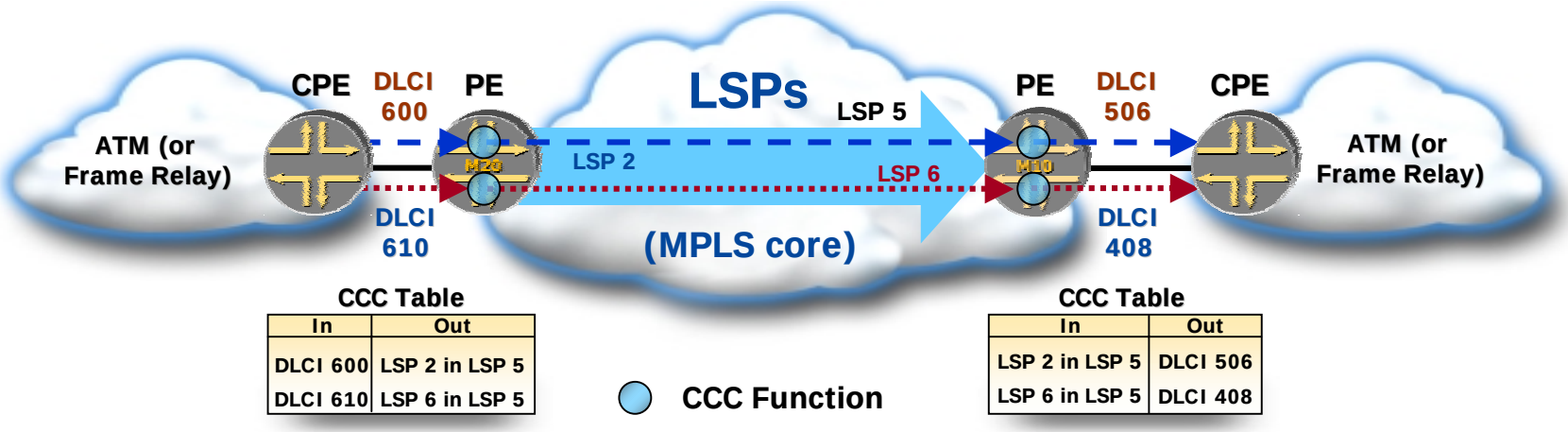


- Application: Carrier of carriers
- Operational model
  - FR/ATM interface between CPE and PE
  - SP maintains mesh of LSPs between PEs
  - CPE routes VPN traffic based on subnet/PVC mappings
  - Ingress PE maps each inbound PVC to a dedicated LSP
  - Egress PE maps incoming LSP to outbound PVC

Hybrid CPE/NB-VPN: Traditional Circuit-Cross-Connect

- Benefits
  - SP can collapse multiple networks (IP, FR, ATM) to a single network running IP/MPLS
  - VPN routing is performed by subscriber
    - Optionally, SP can offer routing as “managed CPE” service
  - Dynamic LSP establishment across core via LDP or RSVP
  - Security similar to traditional layer 2 VPNs
- Limitations
  - CPE and PE systems are statically configured
    - Complex initial configuration
    - Large configuration files
    - Tedious configuration for adds/moves/changes
  - Each DLCI/PVC requires a dedicated LSP
  - Practical only for a small number of very large subscribers

Hybrid CPE/NB-VPN: MPLS-Based Layer 2 VPNs (I-D)



CCC Table

In	Out
DLCI 600	LSP 2 in LSP 5
DLCI 610	LSP 6 in LSP 5

CCC Table

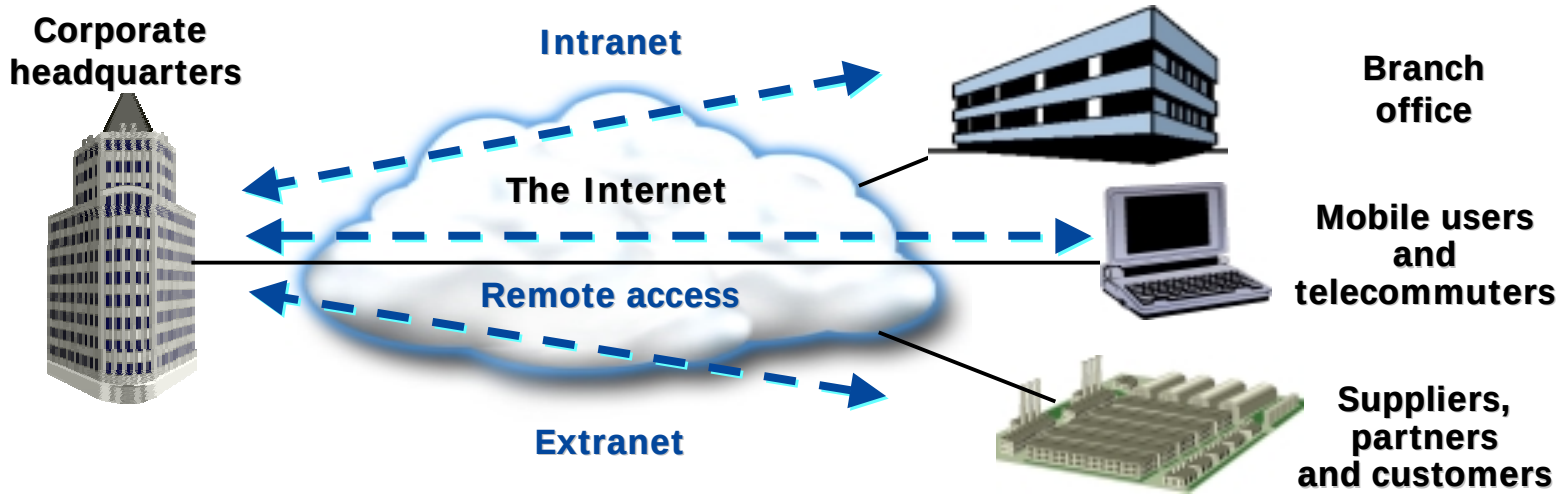
In	Out
LSP 2 in LSP 5	DLCI 506
LSP 6 in LSP 5	DLCI 408

- **Router requirements**
  - PEs support MPLS-based Layer 2 VPNs
  - Core routers support traditional MPLS
- **Label Functions**
  - Outer label: LSP tunnel to destination PE (5 above)
  - Inner label: Identifies DLCI/PVC to CPE (2 or 6 above)
- **Signaling Protocols on PEs**
  - LDP/RSVP: Establish LSP between PEs
  - LDP/BGP: Exchange local CPE VPN information

Hybrid CPE/NB-VPN: MPLS-Based Layer 2 VPNs (I-D)

- **Benefits**
  - Reduces provider configuration complexity
  - VPN routing performed at CPE
    - PE and core routers do not maintain VPN routes
    - Enhanced service scalability
  - Converged core supports IP, RFC 2547bis, and L2 VPNs
  - MPLS traffic engineered core
  - Label stacking reduces the number of LSPs
  - Eases subscriber migration
  - Subscriber can run any Layer 3 protocol
- **Limitations**
  - Circuit type (ATM/FR) to each VPN site must be uniform
  - Managed network service required for CPE revenue

Conclusions:
IP-Based VPN Core Requirements



- Accommodate a number of service-delivery models
  - Multiple approaches to deliver a service at edge
  - Solutions are constantly evolving
- IP and MPLS Infrastructure
  - Required for NB-VPN solutions

Summary: Virtual Private Networks

- Deploying VPNs in the 1990's
- Deploying VPNs in the 21st Century
- MPLS: A VPN enabling technology
- CPE-based VPNs (CPE-VPNs)
  - L2: L2TP and PPTP
  - L3: IPSec
- Network-based VPNs (NB-VPNs)
  - L3: RFC 2547bis
- Hybrid CPE/NB-VPNs
  - Traditional Circuit Cross Connect
  - MPLS-based Layer 2 VPNs
- Conclusions