VPN
Virtual Private Network

Mario Baldi

Synchrodyne Networks, Inc.

http://www.synchrodyne.com/baldi

Nota di Copyright

A Definition

Virtual Private Network

Customer connectivity deployed on a shared infrastructure such that policies can be enforced as in a private network

- Shared infrastructure:
  - Private/public network
    - e.g., the one of an Internet Service Provider
    - IP
    - Frame Relay
    - ATM
  - The Internet
- Policies
  - Security, Quality of Service (QoS), reliability, etc.

Why VPN?

VPNs enable cutting costs with respect to expensive connectivity solutions

Private Networks are based on

- **Private leased lines**
- **Long distance dial-up solutions**

Why VPN?

VPN enable selective and flexible access to corporate network

- Limited services available to external users
  - High security
  - Few services allowed through firewall
- All intranet functionalities available to corporate users accessing from the Internet
  - VPN connection allowed through firewall
  - Services available as on the corporate network

VPN Flavors

- Access VPN or remote VPN or virtual dial in
  - Connect terminal to remote network
  - Virtualizes (dial-u p) access connection
    - e.g., ISDN, PSTN, cable, DSL
  - PPTP, L2TP
- Site-to-site VPN
  - Connect remote networks
  - Virtualizes leased line
  - IPsec, GRE, MPLS

VPN Deployment Scenarios

- Intranet VPN
  - Interconnection of corporate headquarters, remote offices, branch offices
- Extranet VPN
  - Interconnection of customers, suppliers, partners, or communities of interest to a corporate intranet
- Remote user access
  - Telecommuter
  - Traveling employee
  - Customer/partner/provider

Intranet VPN and Extranet VPN

- Site-to-site VPN
- Shared infrastructure
  - Nework of a service provider
  - Two or more service provider networks
  - The Internet
- Access to shared infrastructure
  - aDSL
  - Leased line
  - Fiber
  - Ethernet
- Technologies
  - IPsec
  - GRE
  - MPLS

Extranet VPN

- Restricted access to network resources from interconnected networks
  - Firewall at the VPN
- Address clash
  - Network address translation

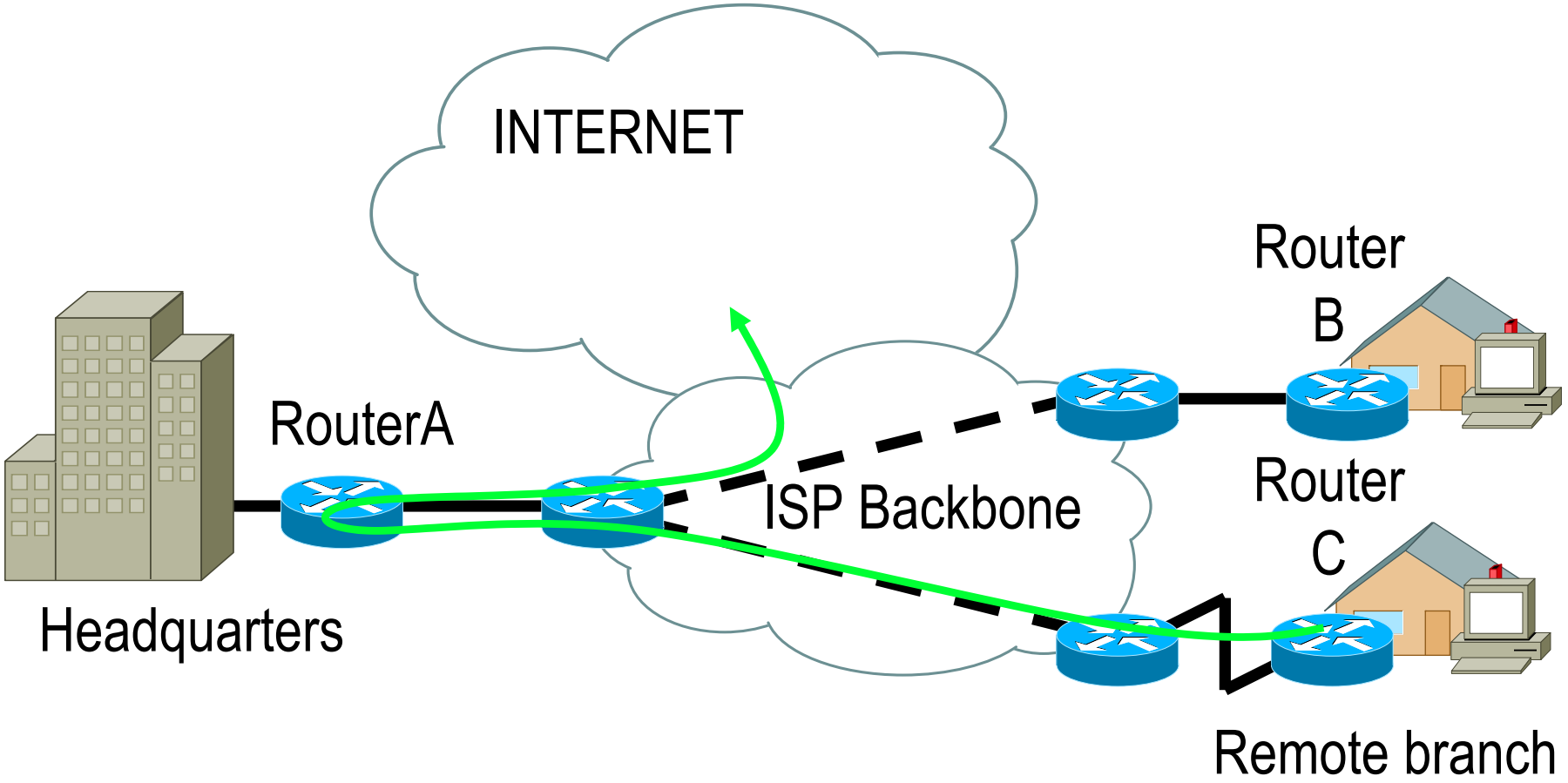
Remote User Access

- Shared infrastructure
  - Nework of a service provider
  - The Internet
- Access to the shared infrastructure
  - ISDN, PSTN
  - Cable modem, DSL
  - Wireless LAN (host spot)
- Technologies
  - PPTP
  - L2TP
  - IPsec
    - Implemented by user's access device

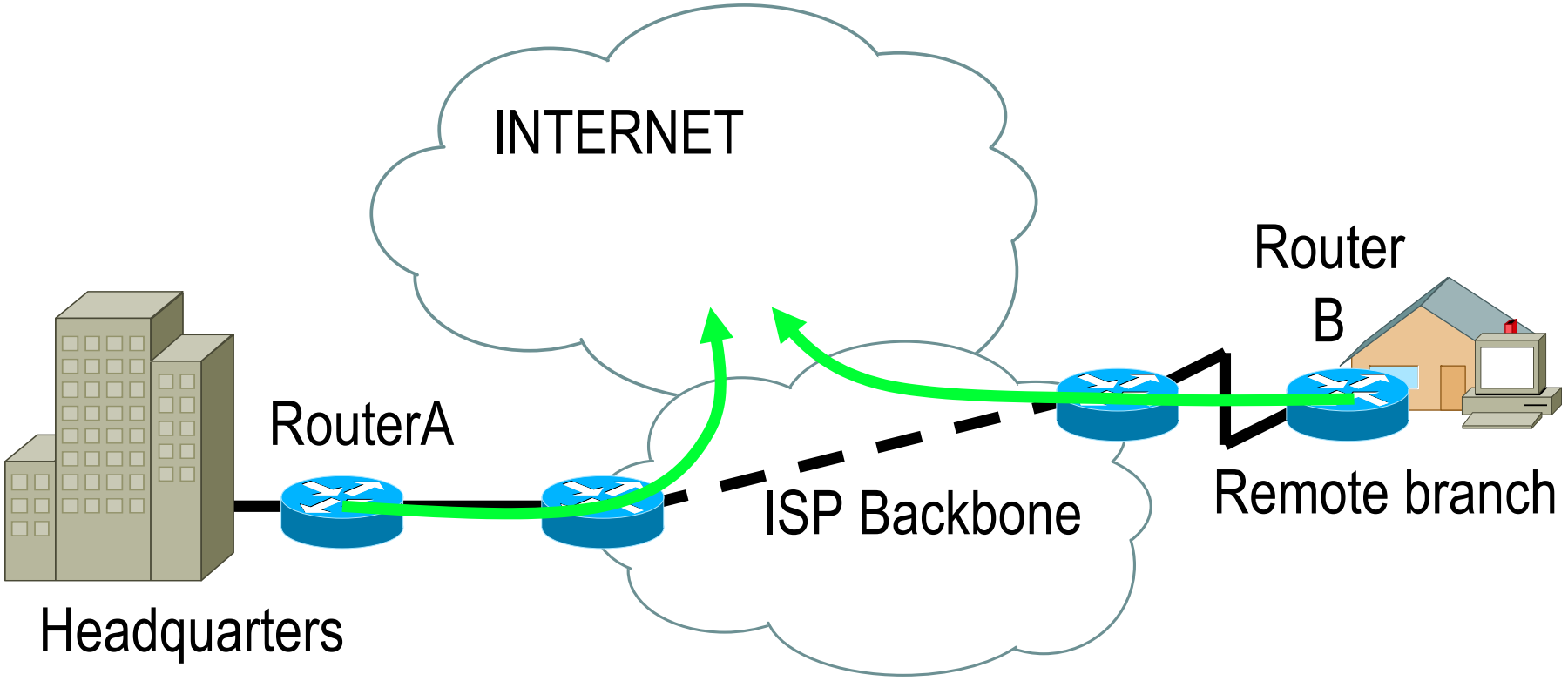
Internet Access

- Centralized
  - Remote branches use IP network only to reach headquartes
  - Internet access only from headquarters
  - VPN carries also traffic to and from the Internet
  - Centralized access control
    - Firewall
- Distributed
  - Any branch accesses Internet through the IP network
  - VPN is deployed only for corporate traffic

Centralized Internet Access



Distributed Internet Access

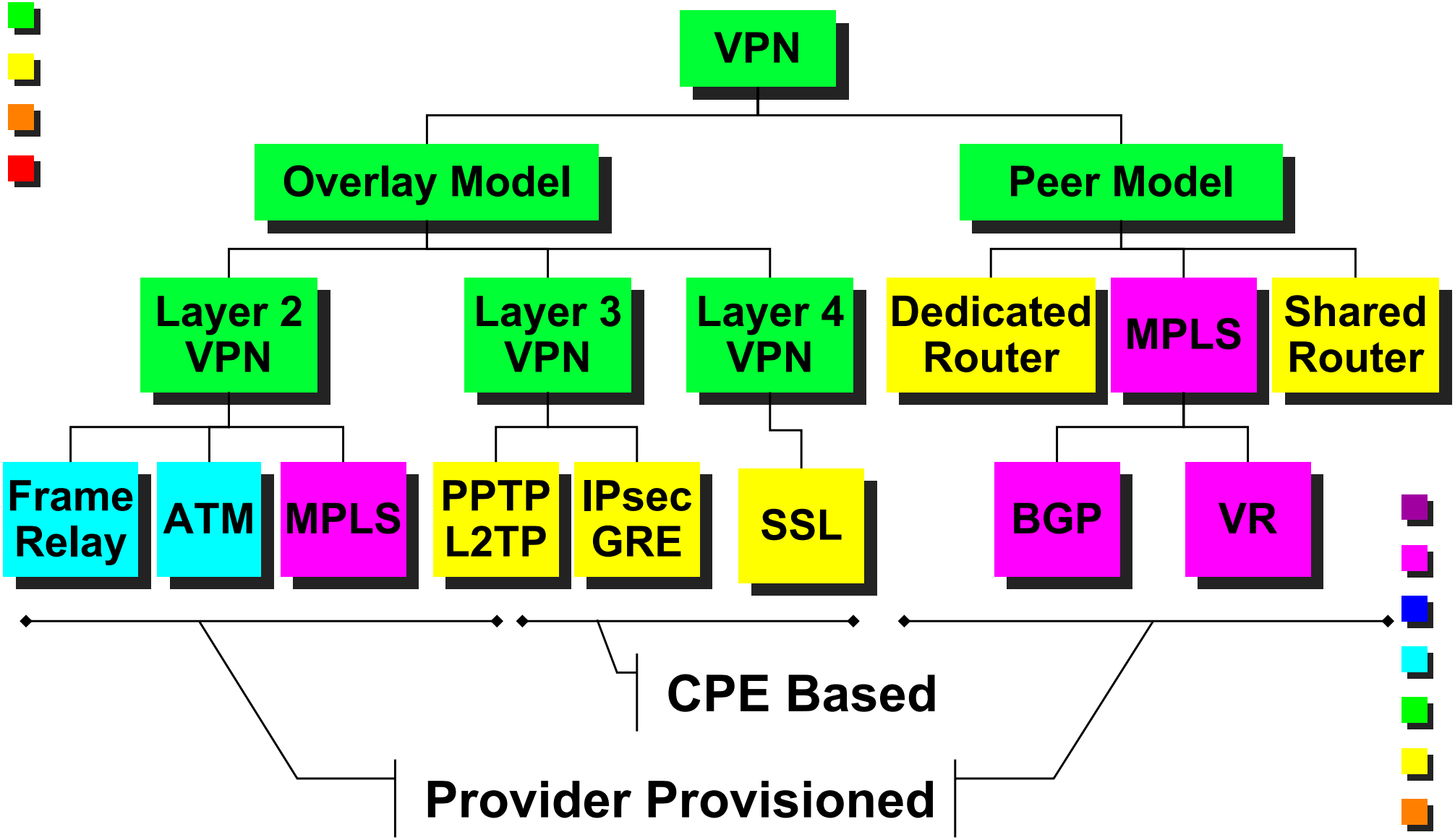


VPN Models

- Overlay Model
  - IPSec-based (managed) service
  - Many separate highly meshed tunnels
    - Each VPN gateway must know every other VPN gateway
- Peer Model
  - MPLS network
  - Each VPN gateway knows only its peer public router
    - Exchange of routing information
    - Service provider network disseminates routing information
  - Public network routes traffic between gateways of the same VPN

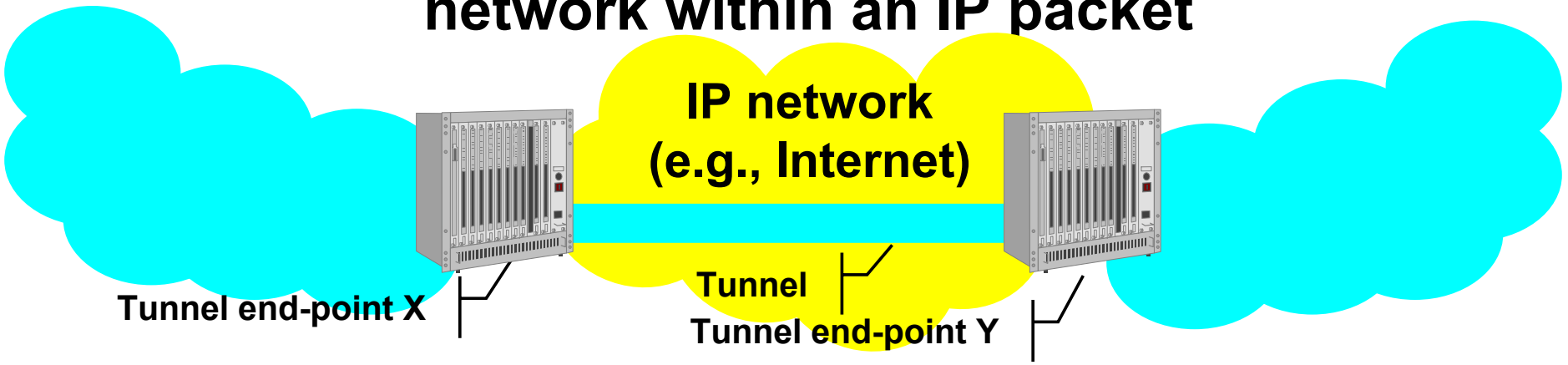
Model	Overlay	Peer
Access	L2TP, PPTP	
Site-to-site	IPSec, GRE	MPLS

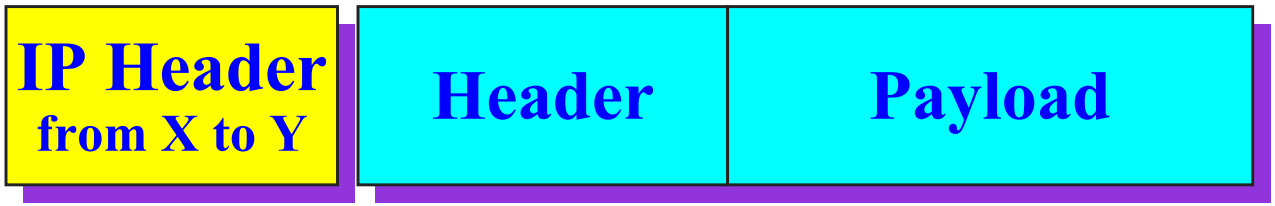
A Tassonomy of VPN Technologies



Tunneling

A packet (or frame) is carried through an IP network within an IP packet

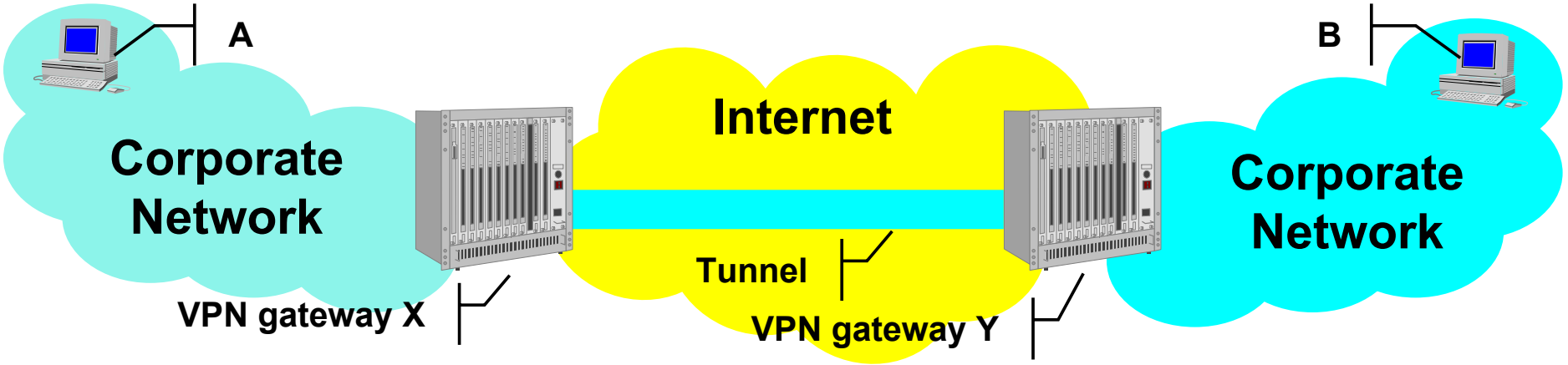


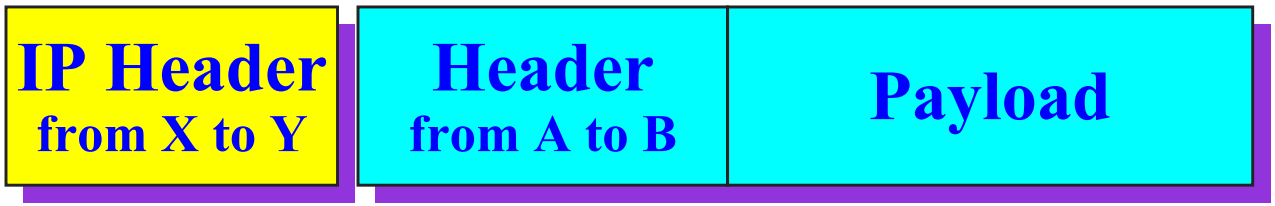


- An IP packet within an IP packet
  - GRE, IPsec
- A layer 2 frame, within an IP packet
  - PPTP, L2TP

Tunneling

- A and B are enterprise addresses
  - Not necessarily public
- Tunneling enables operation
- Tunneling by itself does not ensure security

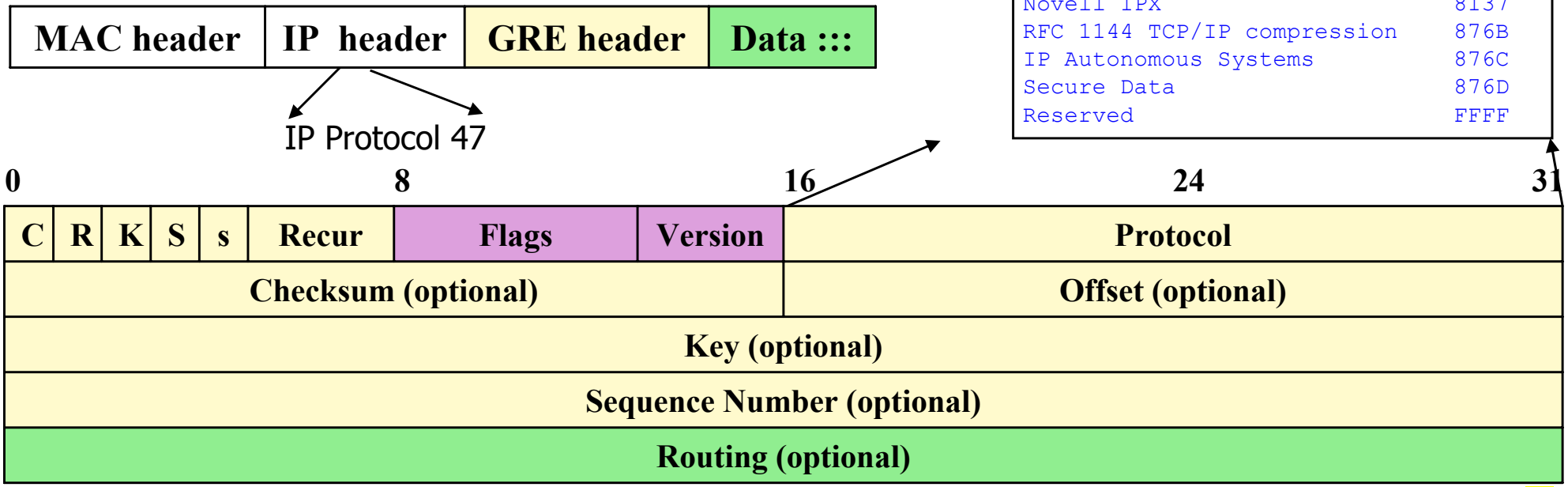




GRE

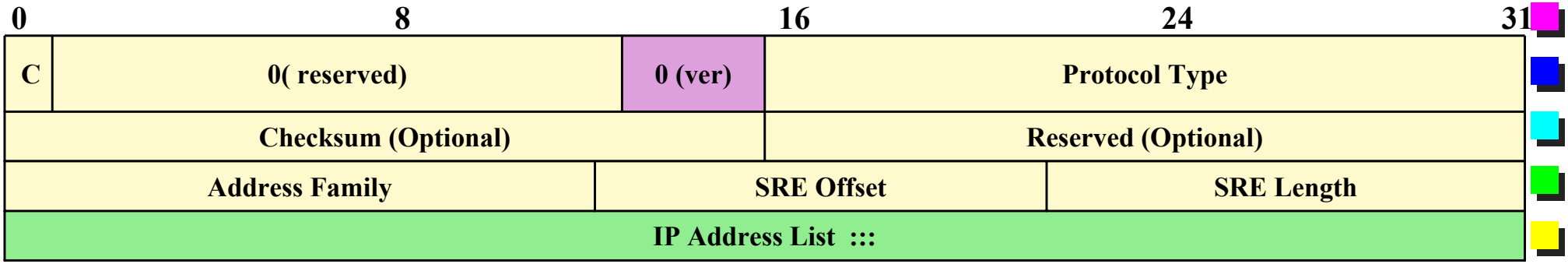
- Generic Routing Encapsulation
- Encapsulation (tunneling) of any protocol (including IP) into IP
- Header version 0

Protocol Family	PTYPE
Reserved	0000
SNA	0004
OSI network layer	00FE
PUP	0200
XNS	0600
IP	**0800**
Chaos	0804
RFC 826 ARP	0806
Frame Relay ARP	0808
VINES	0BAD
VINES Echo	0BAE
VINES Loopback	0BAF
DECnet (Phase IV)	6003
Transparent Ethernet Bridging	6558
Raw Frame Relay	6559
Apollo Domain	8019
Ethertalk (Appletalk)	809B
Novell IPX	8137
RFC 1144 TCP/IP compression	876B
IP Autonomous Systems	876C
Secure Data	876D
Reserved	FFFF



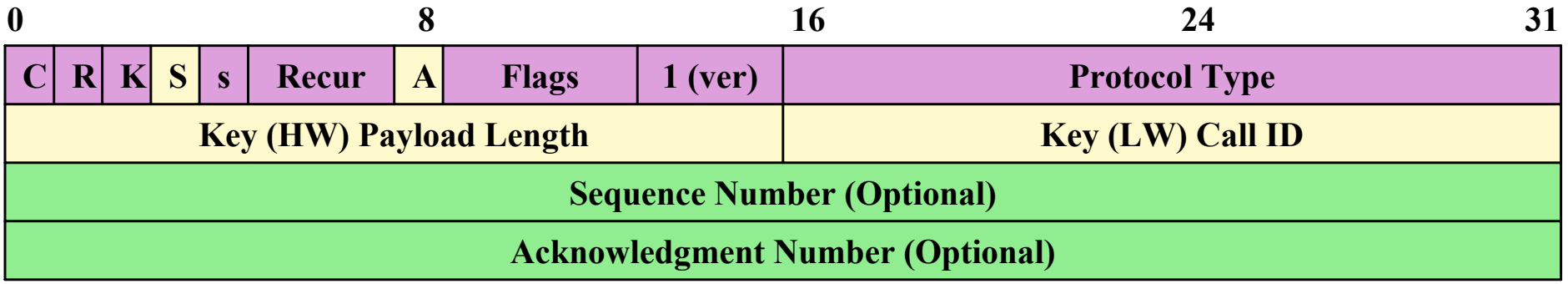
IPv4 Encapsulation and Routing Information

- `IP Address List`: source routing information
  - List of routers to traverse
- `SRE Offset`: byte of IP address of current next hop
  - Updated at each source route hop
- `SRE Length`: total address list length (in bytes)



Enhanced GRE (version 1)

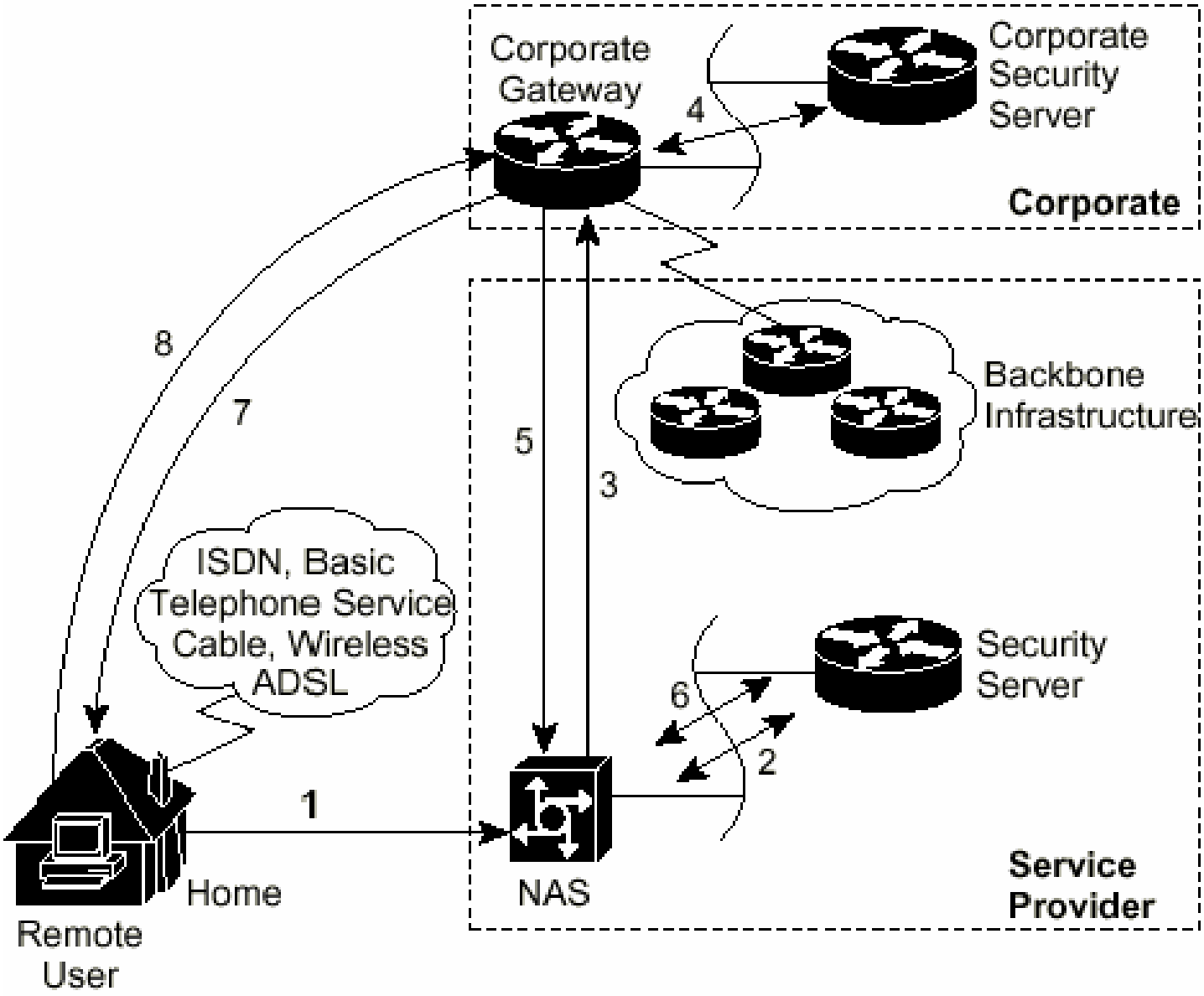
- Deployed by PPTP
- `Acknowledgment Number`
  - Delivery of packets by remote end-point can be notified



(Virtual) VPN Topologies

- Hub and spoke
  - Each branch communicates directly with headquarters
  - Fits to data flow of many corporations
    - Mainframe or data-center centered
  - Routing is sub-optimal
  - Small number of tunnels
    - Hard to manually configure
  - Hub could become bottleneck
- Mesh
  - Larger number of tunnels
    - Easier to manually configure
  - Optimized routing

Access VPN: Two Deployment Modes



Provider Provisioned Deployment Mode

1. Remote user initiates PPP connection with NAS that accepts the call
2. NAS identifies remote user
3. NAS initiates L2TP or PPTP tunnel to desired corporate gateway (access server)
4. Corporare gateway authenticates remote user according to corporate security policy
5. Corporate gateway confirms acceptance of tunnel
6. NAS logs acceptance and/or traffic (optional)
7. Corporate gateway performs PPP negotiations with remote users (e.g., IPaddress assignment)
8. End-to-end data tunneled between user and corporate gateway

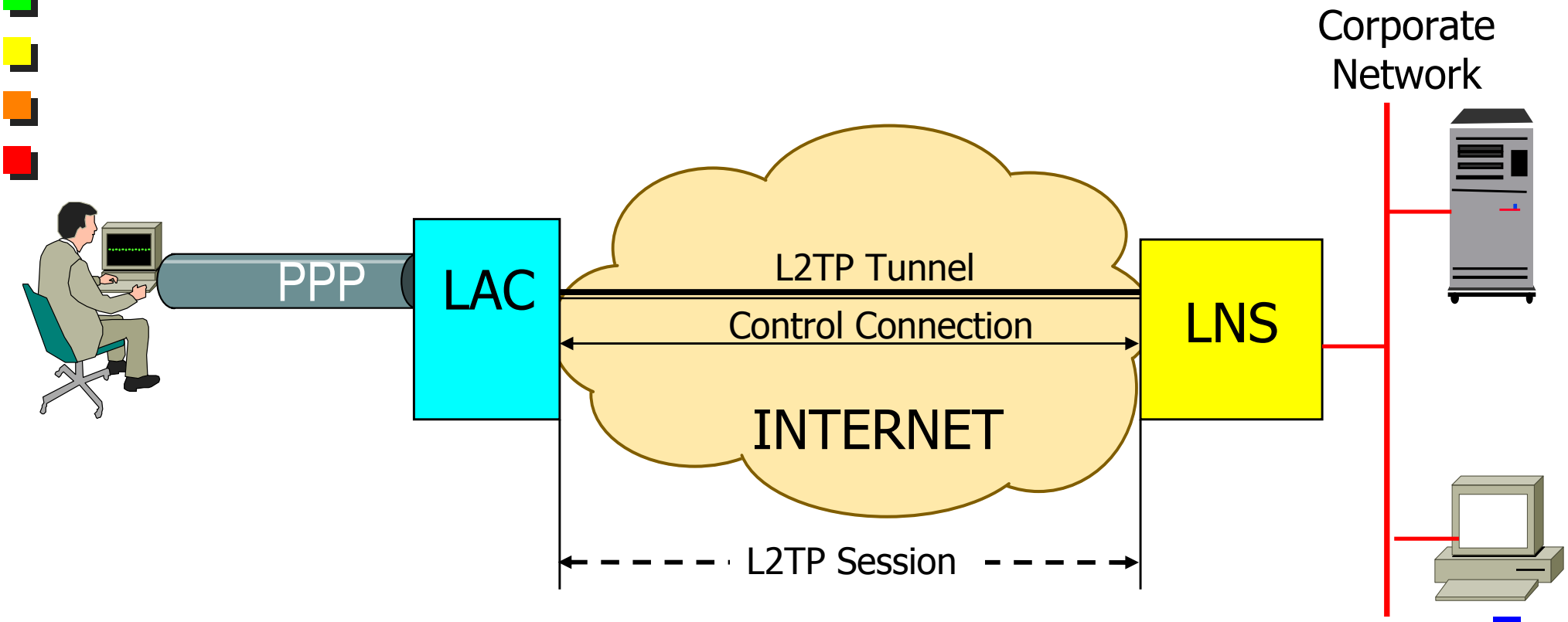
Highlights of Virtual Dial-Up

- Authentication/Security
  - Performed by VPN Gateway
  - Policies and information of the corporate network
- Authorization
  - Performed by the VPN Gateway
  - Policies and information of the corporate network
- Address allocation
  - Corporate addresses are dynamically allocated
  - Same access as when directly connected

Access VPN: Two Protocols

- L2TP (Layer 2 Tunneling Protocol)
  - Not widely implemented in terminals
  - Idependent of layer 2 protocol
  - Security through IPsec
    - Strong
    - But complicated
- PPTP (Point-to-Point Tunneling Protocol)
  - Originally proposed by Microsoft, Apple, …
    - Integrato nel dial-up networking
  - Multiprotocol
  - Weak encryption and authentication
  - Proprietary key management

Layer 2 Tunneling Protocol
Original Reference Scenario



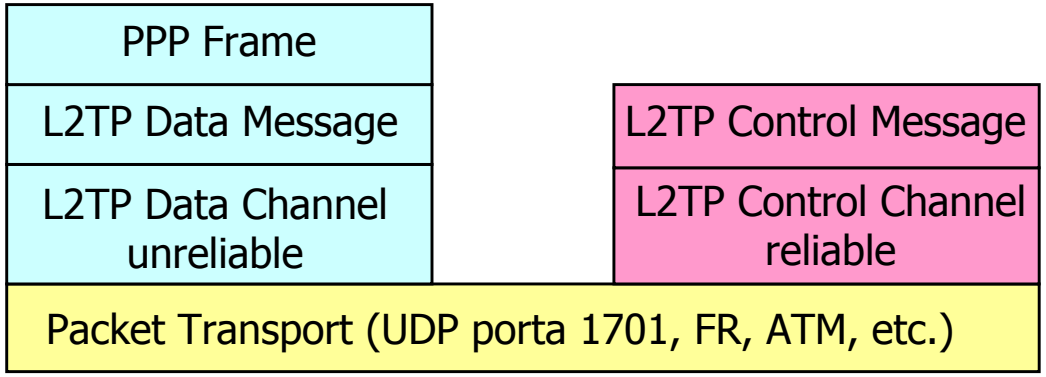
Provider provisioned deployment mode

Layer 2 Tunneling Protocol

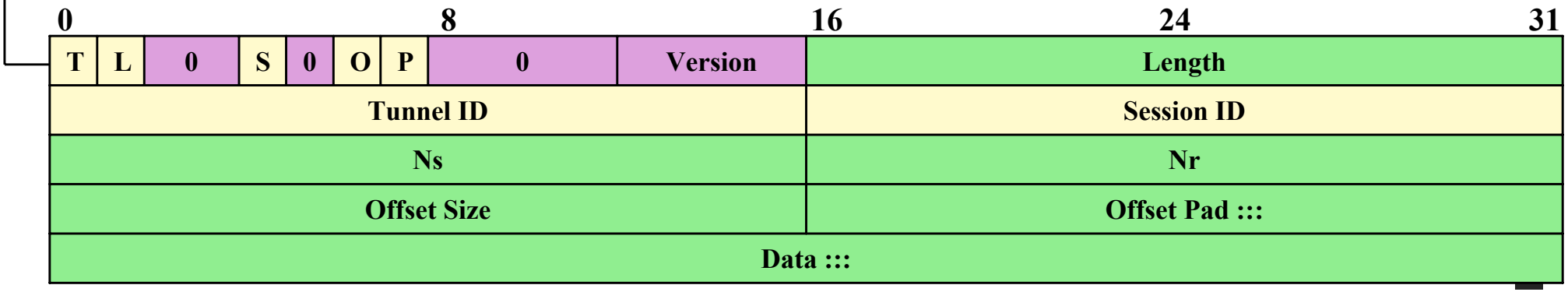
- Tunneling between public network access point and corporate network
  - Also wholesale dial-up services
    - Between access provider and Internet Service Provider
- L2TP Access Concentrator (LAC)
  - Network access device supporting L2TP
  - NAS (Network Access Server)
- L2TP Network Server (LNS)
  - Corporate (VPN) Gateway
- CPE based deployment mode by including LAC functionalities within user terminal

L2TP Header

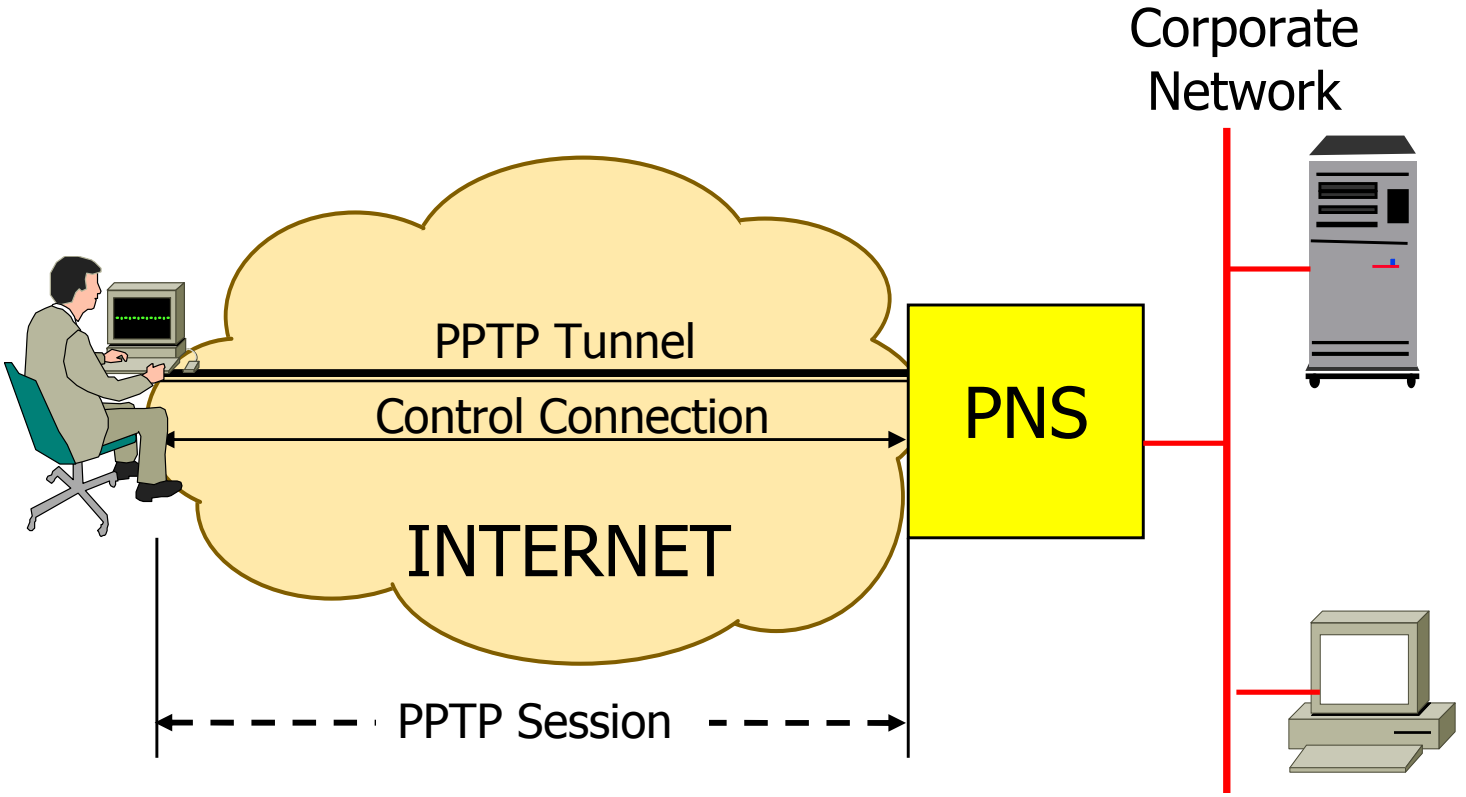
- Control Message
- Data Message



T	Description
0	**Data message.**
1	**Control message.**



Point-to-Point Tunneling Protocol
Original Reference Scenario



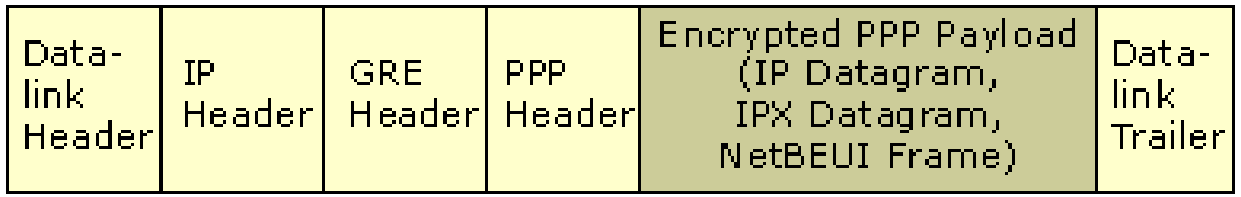
CPE based deployment mode

Point-to-Point Tunneling Protocol (PPTP)

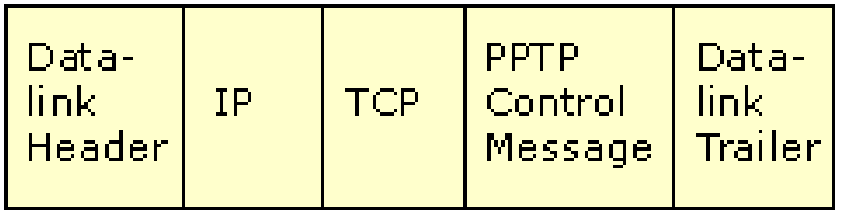
- Adopted by IETF (RFC 2637)
- Microsoft Encryption: MPPE
- Microsoft Authentication: MS CHAP
- PPTP Network Server (PNS)
  - Corporate (VPN) gateway
- PPTP Access Concentrator (PAC)
  - For provider provisioned deployment mode

PPTP Connections

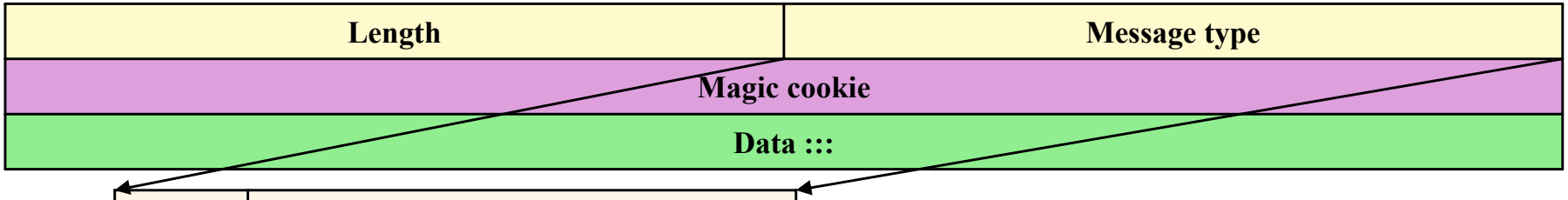
- PPTP Data Tunneling
  - Data transport
  - PPP tunneling
  - GRE (of PPP over IP)



- Control Connection
  - Tunnel data session setup, management, and tear-down
  - TCP encapsulaton
    - PNS port 1723



PPTP Header

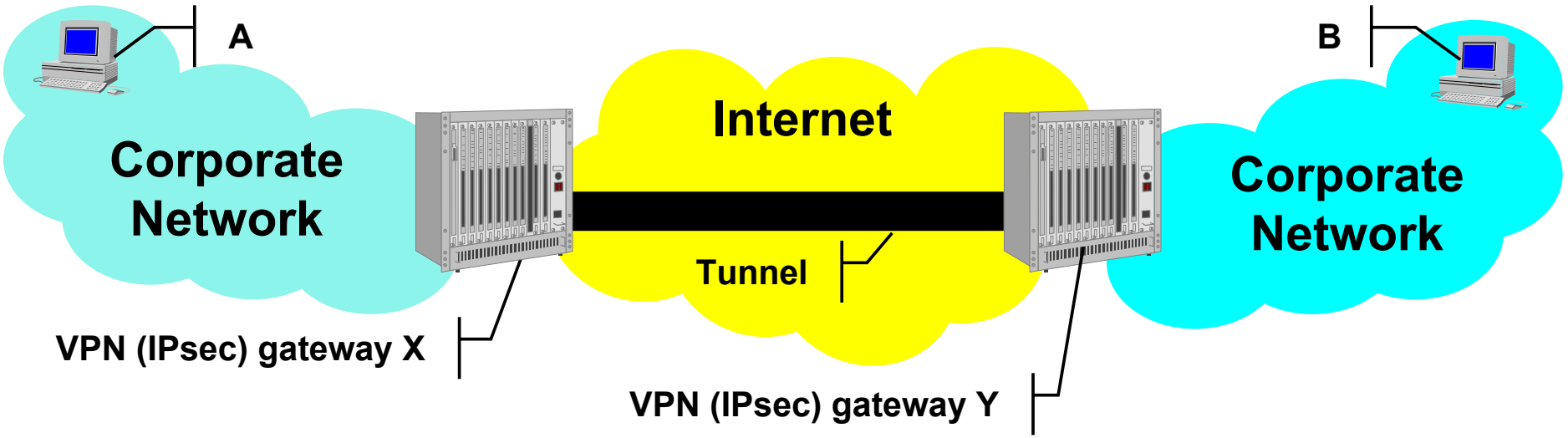


Value	Control Message
1	**Start-Control-Connection-Request.**
2	**Start-Control-Connection-Reply.**
3	**Stop-Control-Connection-Request.**
4	**Stop-Control-Connection-Reply.**
5	**Echo-Request.**
6	**Echo-Reply.**
7	**Outgoing-Call-Request.**
8	**Outgoing-Call-Reply.**
9	**Incoming-Call-Request.**
10	**Incoming-Call-Reply.**
11	**Incoming-Call-Connected.**
12	**Call-Clear-Request.**
13	**Call-Disconnect-Notify.**
14	**WAN-Error-Notify.**
15	**Set-Link-Info.**

IPsec VPNs

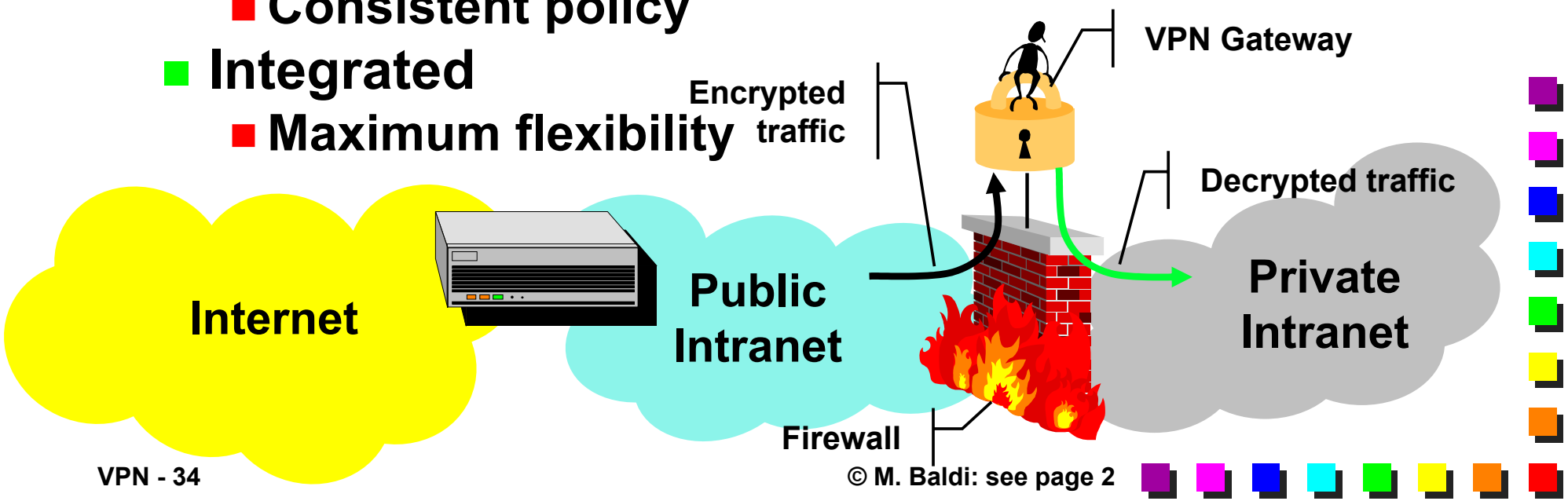
IPsec tunnel between VPN gateways

- Encryption
- Authentication
- Encapsulation



VPN Gateway and Firewall

- Inside
  - No inspection of VPN traffic
  - VPN gateway protected by firewall
- Parallel
  - Potential uncontrolled access
- Outside
  - VPN gateway protected by access router
  - Consistent policy
- Integrated
  - Maximum flexibility

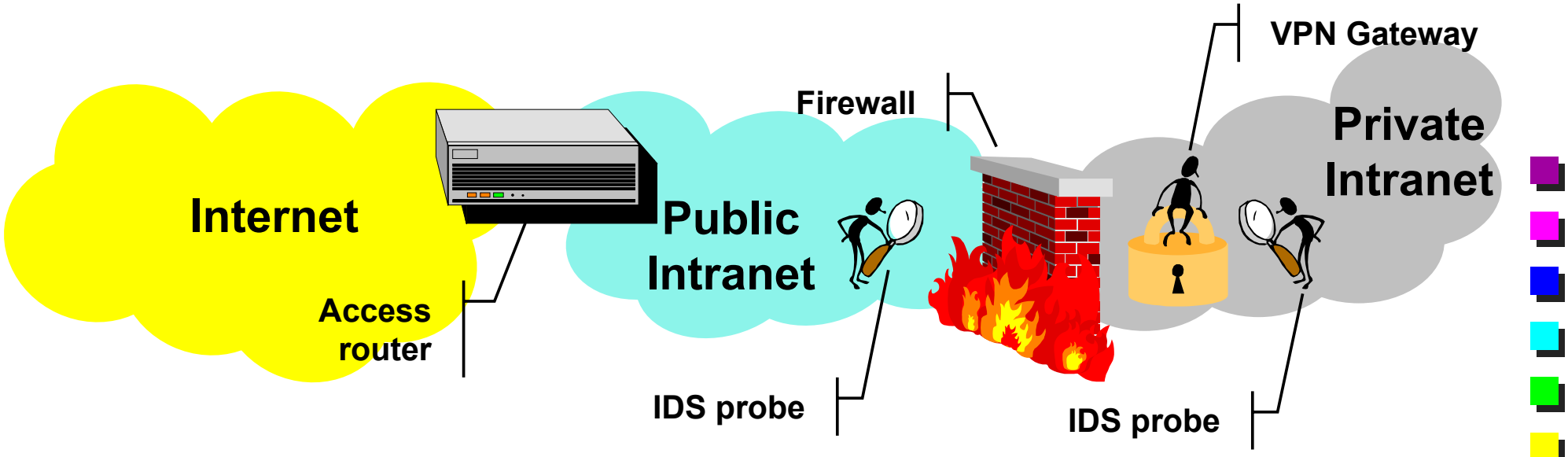


VPN Gateway and NAT

- Authentication Header (AH)
  - IP addresses are part of AH checksum calculation → packets discarded
- Transport mode
  - IP address of IPSec tunnel peer is not what expected → packets discarded
- No PAT (Protocol Address Translation)
- Tunnel mode
  - IP address within secure packet can be changed before entering the gateway
    - E.g., same addresses in two different VPN sites
  - Most often NAT is not needed on external packet

VPN Gateway and IDS

- IDS is usually outside the firewall
- No control on VPN traffic
- Multiple IDS probes
  - Outside firewall
  - Inside VPN gateway



IP-based peer VPNs

- Dedicated router
  - Service provider operates a network of routers dedicated to the customer
  - Viable only for major clients
- Shared/virtual router
  - Service provider creats dedicated router instances within his physical routers
  - High-end routers enable hundreds of virtual routers
    - Instance-specific routing table and routing protocol
    - ASIC and operating system support
  - Packet exchange through IPsec or GRE tunnels

MPLS-based Layer 2 VPNs: PWE3

- Pseudo Wire Emulation End-to-End
- Several services on the same network:
  - IP, but also leased lines, frame relay, ATM, Ethernet
- Customer edge (CE) device features native service interface
- Traffic is carried through an LSP between Ces
- Two labels
  - External – for routing within the network
    - Identifies access point to the network
  - Internal - multiplexing of several users/services at the same access point

MPLS-based Layer 2 VPNs: PWE3

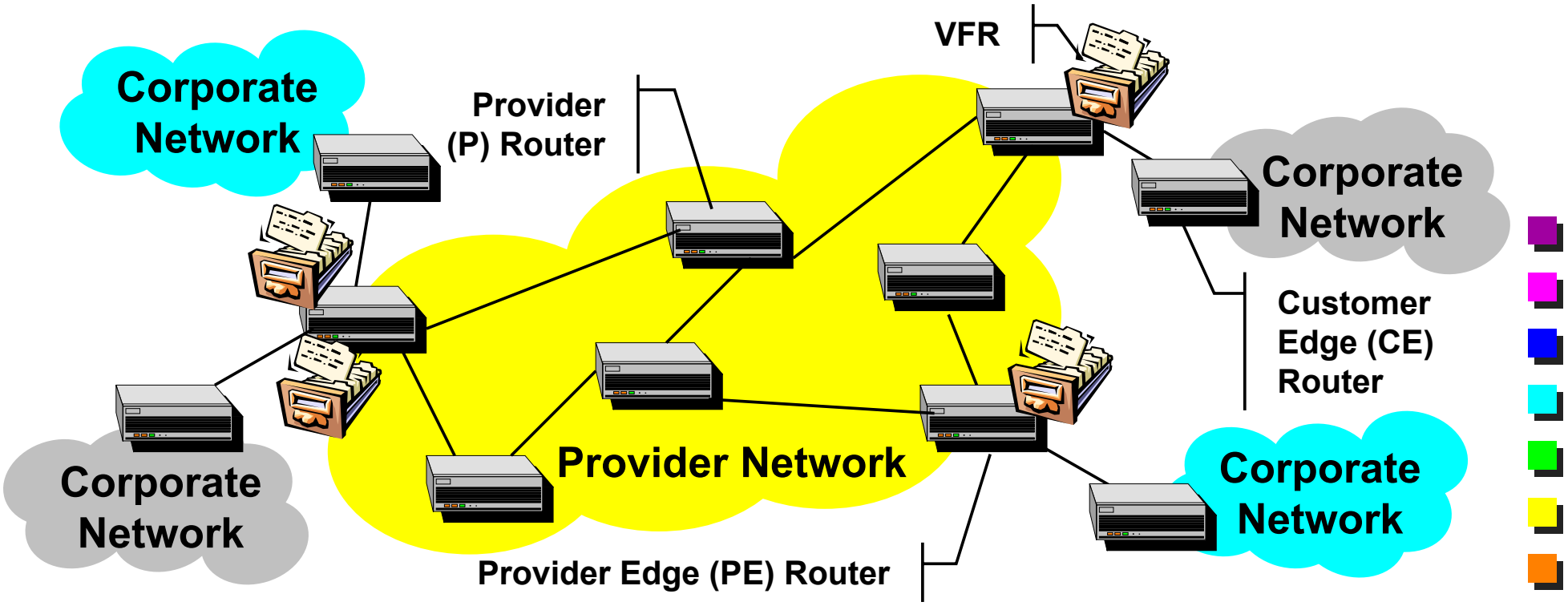
- There may be aggregation devices inside the network
  - E.g., an ATM switch inside the service provider network switching traffic between users
    - LSP ended on the device
- Mainly manual LSP setup
- Proposals exist for deployment of LDP and BGP

MPLS-based Layer 3 VPNs

- Provider provisioned solutions
  - VPN policies implemented by Service Provider
  - No experience needed on the Customer side
- Scalability
  - Large scale deployments
- Two alternative solutions
  - RFC2547bis (BGP)
    - Initially supported by Cisco Systems
    - Currently most widely deployed approach
  - Virtual router
    - Initially supported by Nortel and Lucent

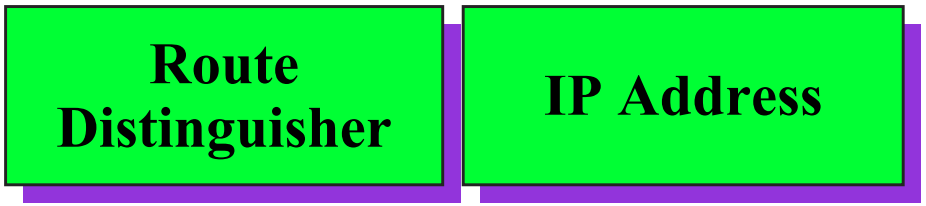
MPLS/BGP VPN Components

- VRF (VPN Routing and Forwarding) table
  - Associated to one or more ports
  - Forwarding information to be used for traffic received through the port



Control Plane

- Routing exchange at edges based on MP-BGP (Multi-protocol BGP)
- Route filtering
  - PE routers determine which routes to install in VRF
- Support for overlapping address spaces
  - VPN-IPv4 Address family
    - Route Distinguisher + IPv4 address

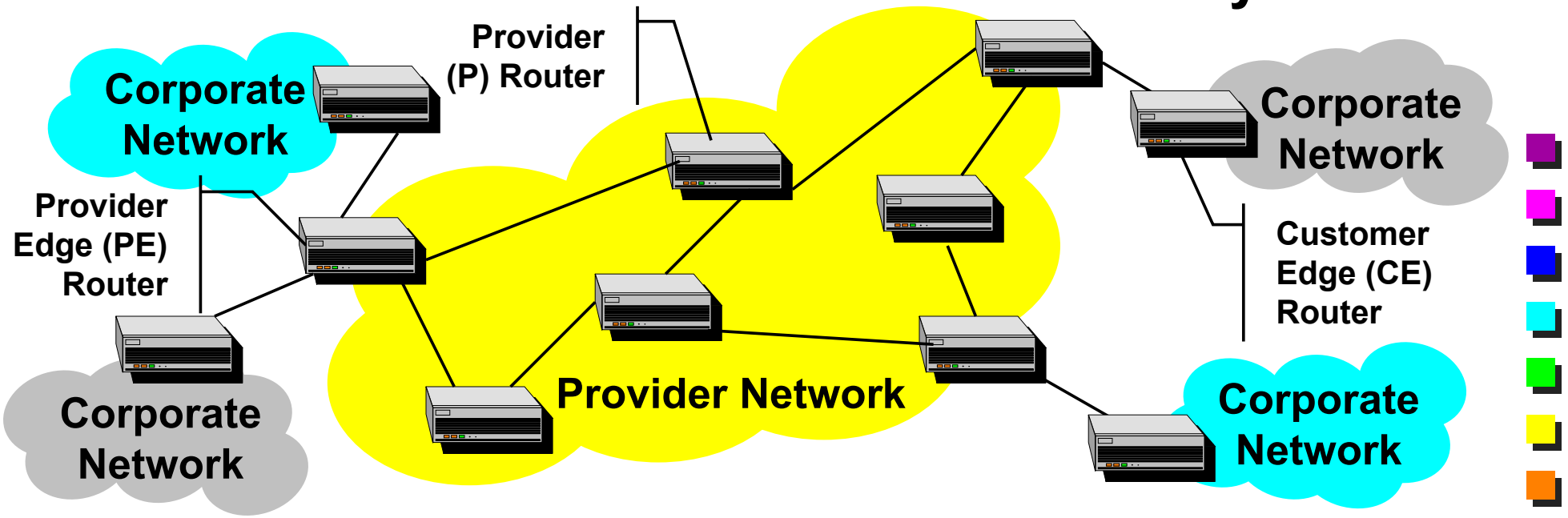


MPLS VPN Components

- CE router creates adjacency with PE router
  - It advertises its destinations
  - It receives advertisements of other VPN destinations
  - Static routing, or
  - IGP (Interior Gateway Protocol)
    - (e.g., OSPF, RIP)
  - E-BGP (Exterior-Border Gateway Protocol)
  - PE router does not keep routes for all VPNs

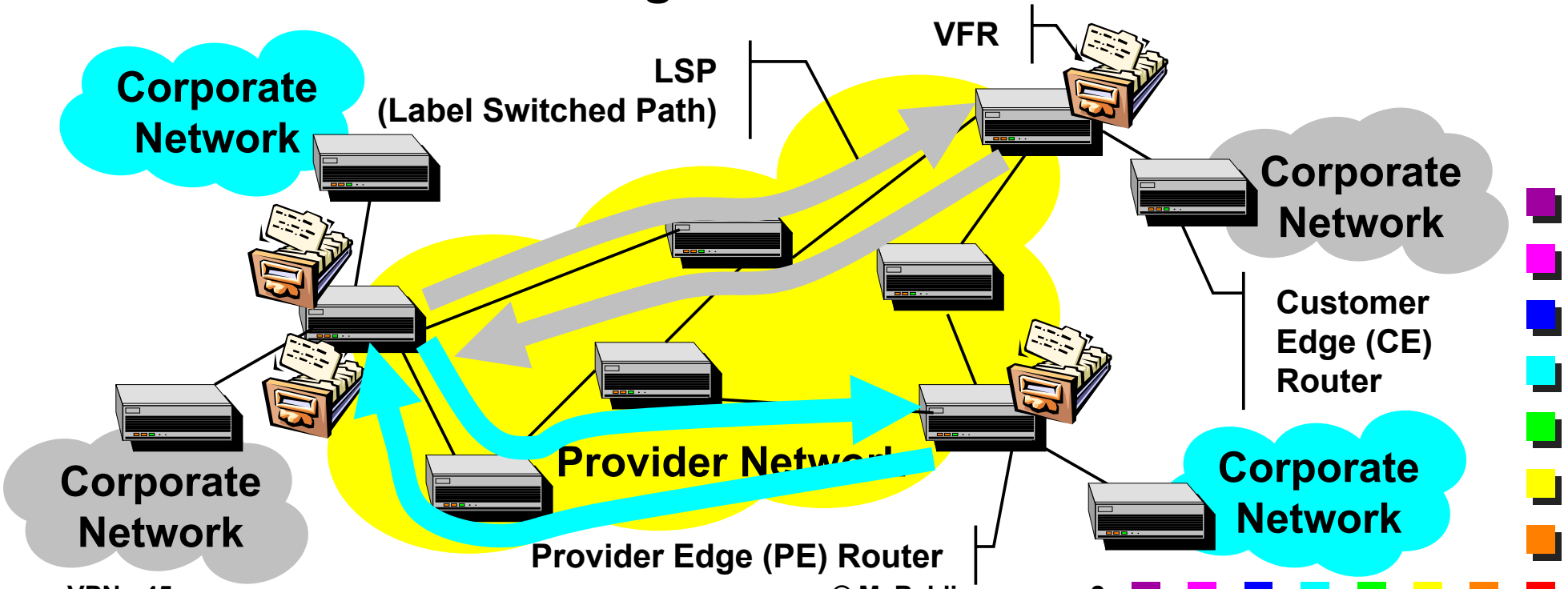
MPLS/BGP VPN Components

- PE routers
  - Exchange routing information
    - I-BGP (Interior-Border Gateway Protocol)
  - Are ingress and egress LSR (Label Switch Router) for the backbone
- P routers have routes to PE routers only



Control Plane

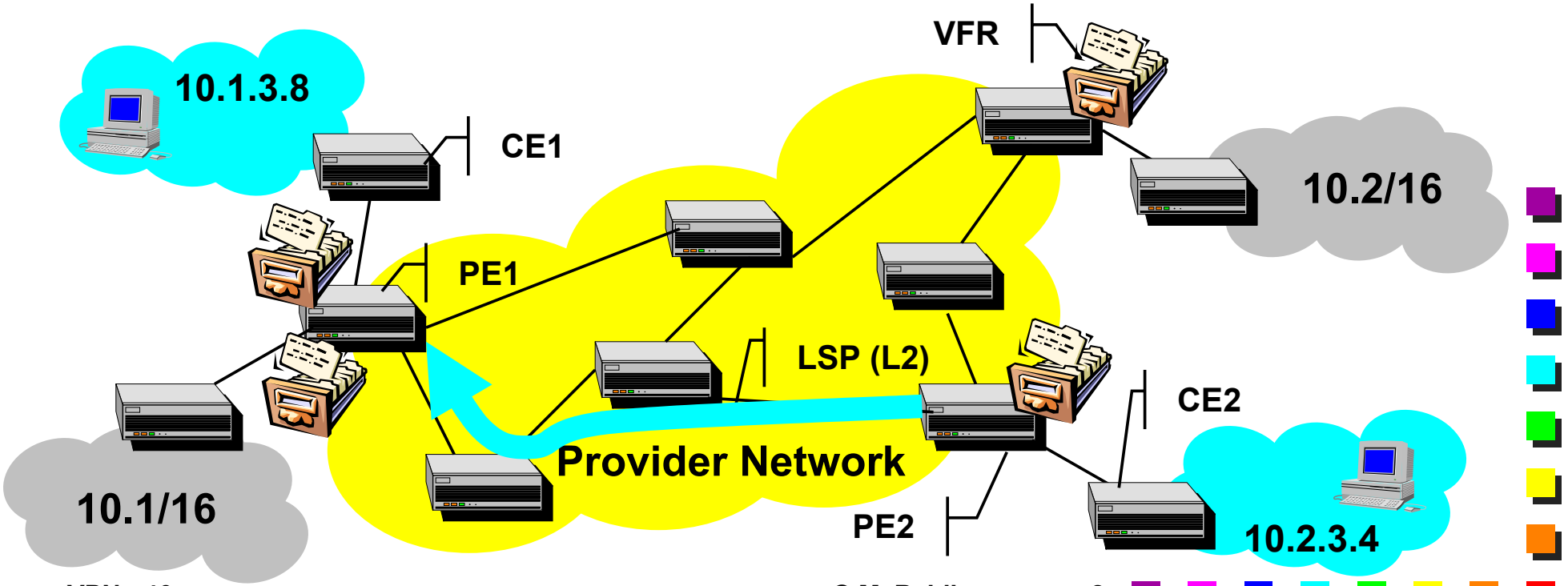
- Establishment of LSPs across the backbone
  - I-BGP carrying label information
  - LDP (Label Distribution Protocol) and/or
  - RSVP (Resource reSerVation Protocol)
  - LSP mesh among PE routers with same VPN



Packet Routing

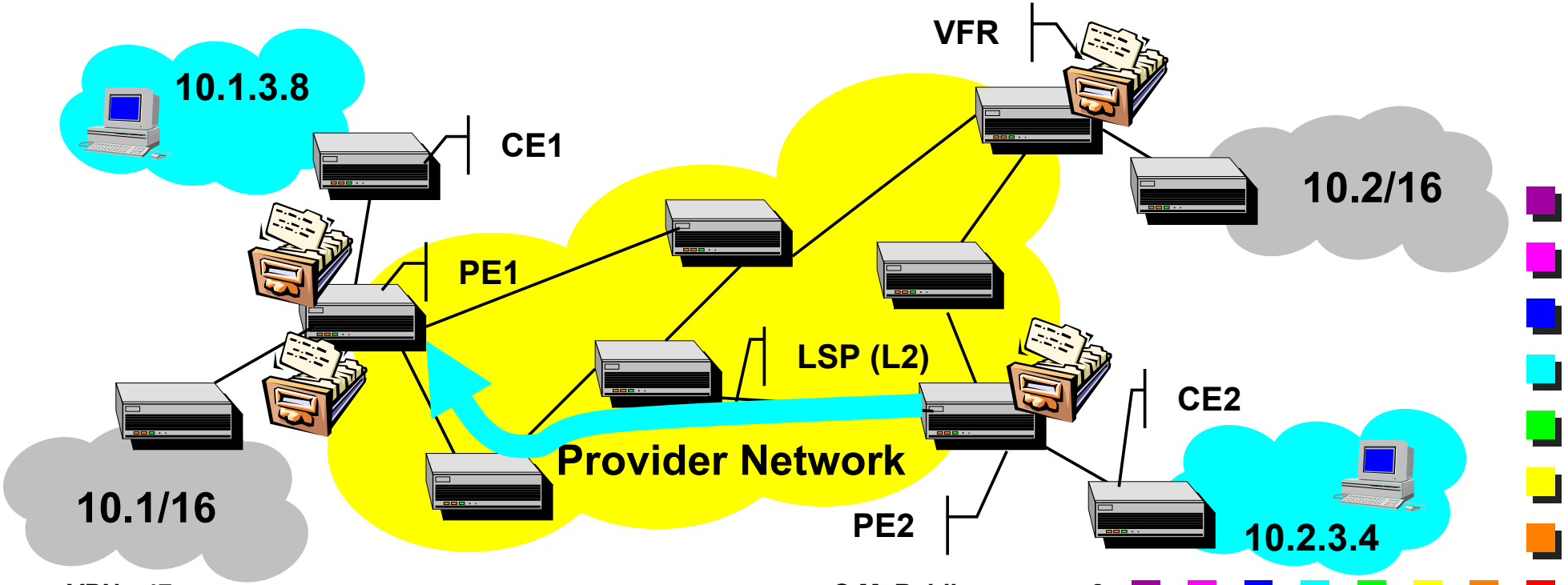
Packet from 10.2.3.4 to 10.1.3.8

- **Default gateway → PE2 router**



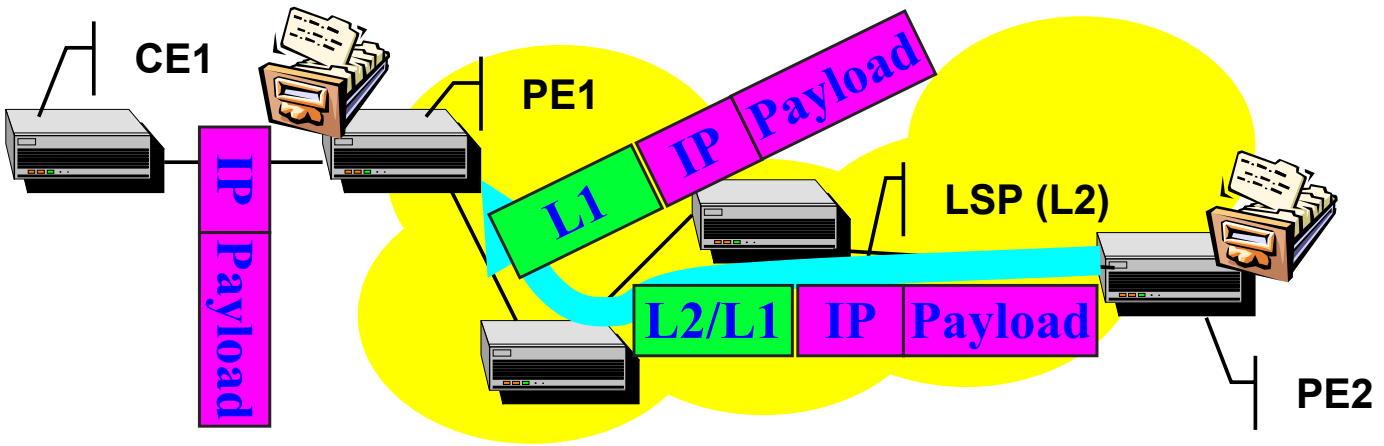
Packet Routing

- PE2 looks-up VRF
  - MPLS label advertised by PE1 for 10.1.3/24: L1
  - BGP next hop (PE1)
  - Outgoing interface for LSP to PE1
  - Initial label for LSP from PE2 to PE1: L2



Packet Routing

- PE2 pushes L1 and L2 on label stack
- P routers forward packet to PE1 using L2
- Last hop before PE1 pops L2
- PE1 receives packet with L1
  - PE1 pops L1: plain IP packet
  - PE1 uses L1 to route packet to proper output interface

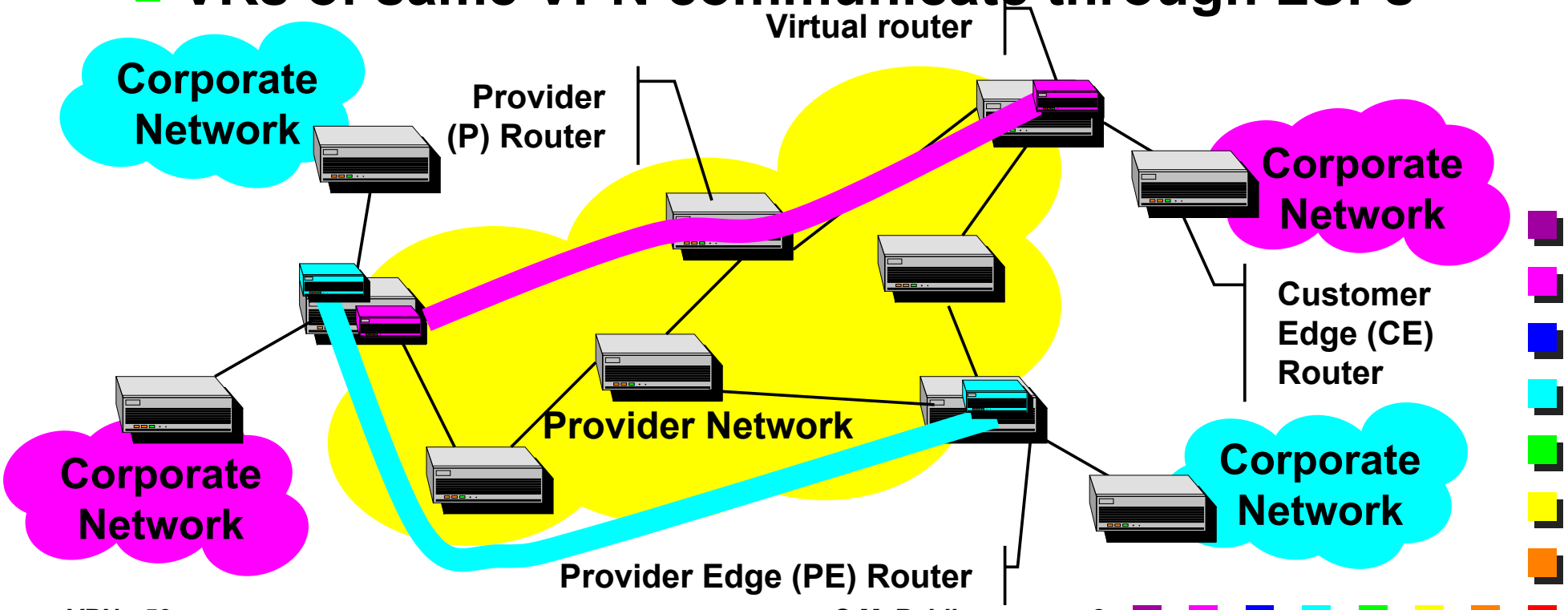


Benefits

- No constraints on addressing plan
  - Address uniqueness only within VPN
- CE routers do not exchange information
- Customer does not manage backbone
- Providers do not have one virtual backbone per customer
- VPN can span multiple providers
- Security equivalent to Frame relay or ATM
  - Traffic isolation
  - No cryptography (confidentiality)
- QoS supported through experimental bits in MPLS header

MPLS/Virtual Router VPNs

- PEs execute a (virtual) router instance for each VPN
- Each VR instance has separate data structures
- VRs of same VPN communicate through LSPs



Multi-Protocol Support

- Access VPN
  - Transparent
    - L2TP and PPTP
- Overlay (IPsec based)
  - Generic Routing Encapsulation (GRE)
    - Transport any layer 3 protocol within IP
- Peer (MPLS based)
  - Built in MPLS (*Multi-Protocol* Label Switching)

References

- E. Rosen and Y. Rekhter, “BGP/MPLS VPNs,” RFC 2547, March 1999.
- E. Rosen et al., “BGP/MPLS VPNs,” <draft-rosen-rfc2547bis-02.txt>, July 2000.
- C. Semeria, “RFC 2547bis: BGP/MPLS VPN Fundamentals,” Juniper Networks, White paper 200012-001, March 2001.
- IETF MPLS Working Group, http://www.ietf.org/html.charters/mpls-charter.html

References

- Hanks, S., Editor, "Generic Routing Encapsulation over IPv4", RFC 1702, October 1994.
- Brian Browne, “Best Practices For VPN Implementation,”Business Communication Review, March 2001.
- http://www.ietf.org/html.charters/l2vpn-charter.html
- http://www.ietf.org/html.charters/l3vpn-charter.html