

Virtual Private Networks

Raj Jain

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

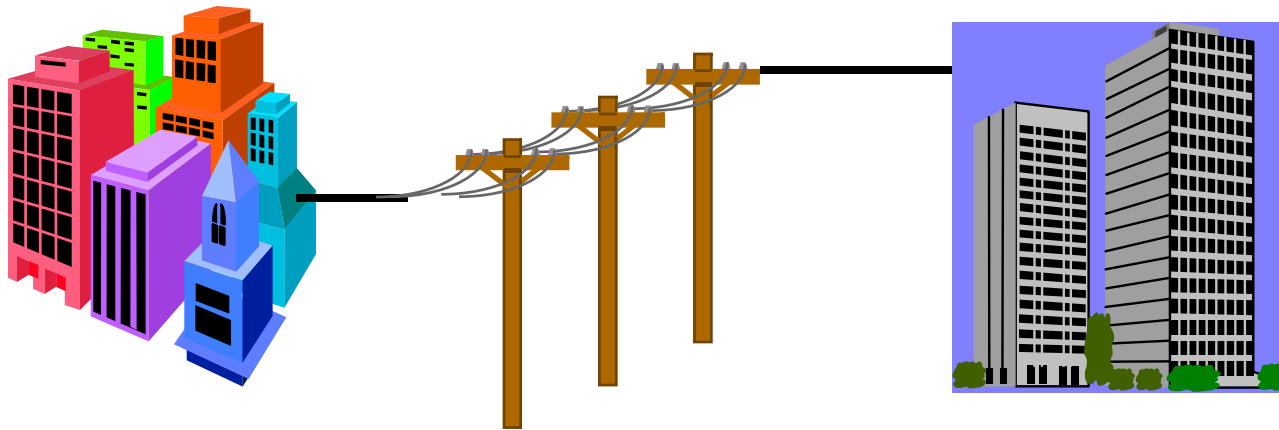
<http://www.cse.wustl.edu/~jain/cse571-09/>



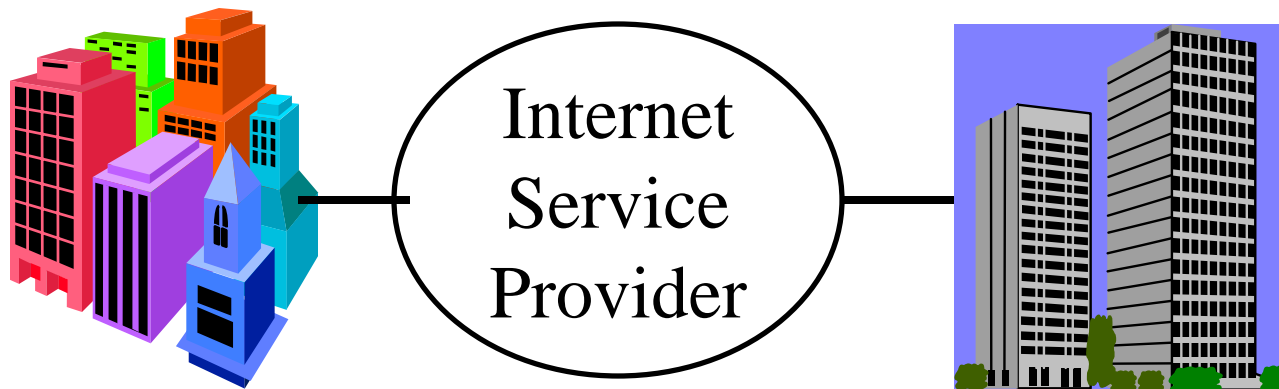
- ❑ Overview: What, When, Issues
- ❑ Types of VPNs: PE/CE based, L2 vs. L3
- ❑ Point-to-Point Protocol (PPP)
- ❑ VPN Tunneling Protocols: GRE, PPTP, L2TPv3, MPLS

What is a VPN?

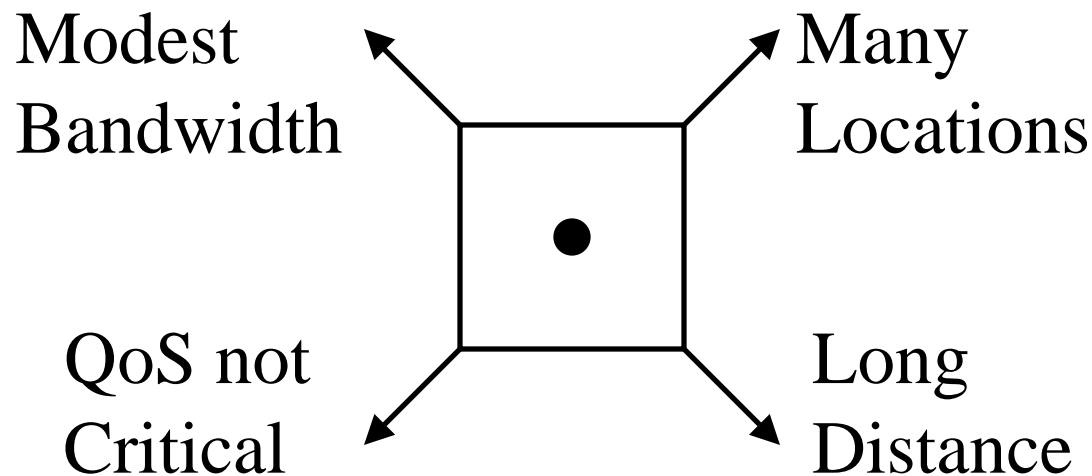
- ❑ Private Network: Uses leased lines



- ❑ *Virtual* Private Network: Uses public Internet



When to VPN?



- ❑ More Locations, Longer Distances, Less Bandwidth/site, QoS (Quality of Service) less critical \Rightarrow VPN more justifiable
- ❑ Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical \Rightarrow VPN less justifiable

VPN Design Issues

1. Security
2. Address Translation
3. Performance: Throughput, Load balancing (round-robin DNS), fragmentation
4. Bandwidth Management: RSVP (Resource Reservation Protocol)
5. Availability: Good performance at all times
6. Scalability: Number of locations/Users
7. Interoperability: Among vendors, Internet Service Providers (ISPs), customers (for extranets) \Rightarrow Standards Compatibility, With firewall

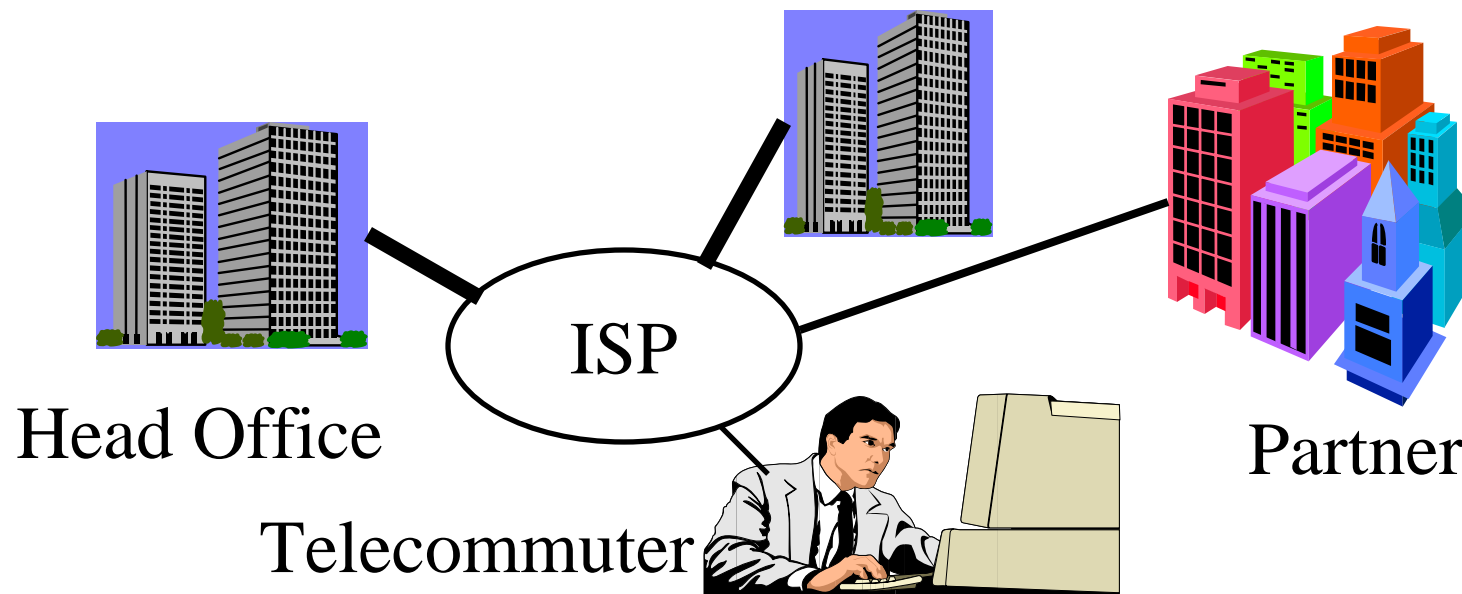
Design Issues (Cont)

8. Compression: Reduces bandwidth requirements
9. Manageability: SNMP (Simple Network Management Protocol), Browser based, Java based, centralized/distributed
10. Accounting, Auditing, and Alarming
11. Protocol Support: IP, non-IP (IPX)
12. Platform and O/S support: Windows, UNIX, MacOS, HP/Sun/Intel
13. Installation: Changes to desktop or backbone only
14. Legal: Exportability, Foreign Govt Restrictions, Key Management Infrastructure (KMI) initiative
⇒ Need key recovery

Types of VPNs

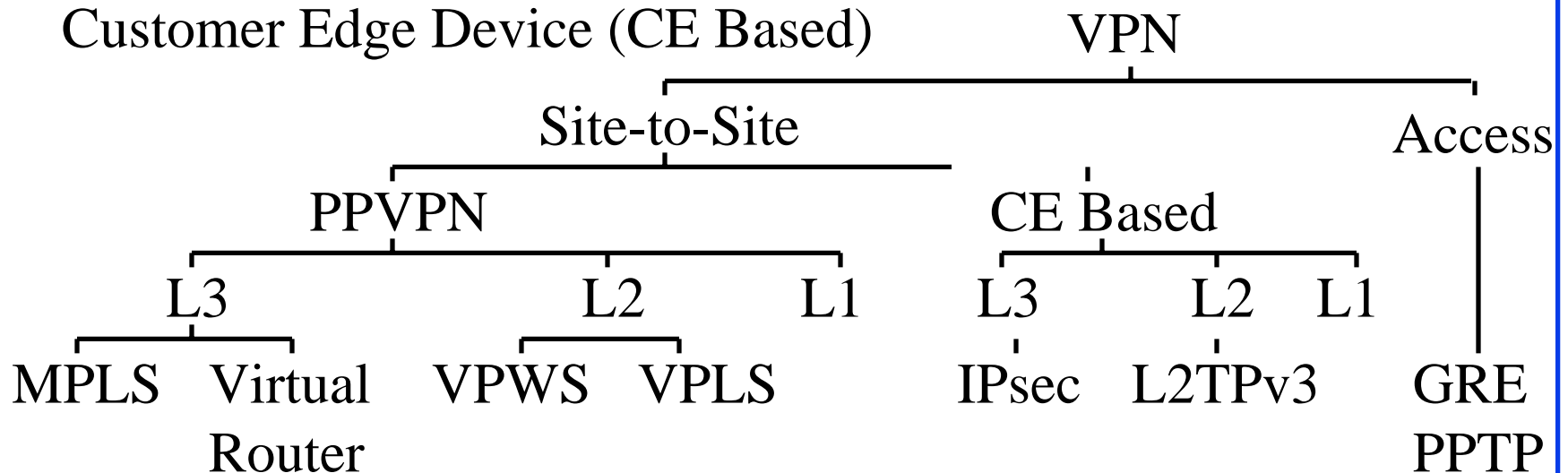
□ Ends:

- WAN VPN: Branch offices
- Access VPN: Roaming Users
- Extranet VPNs: Suppliers and Customers
Branch Office



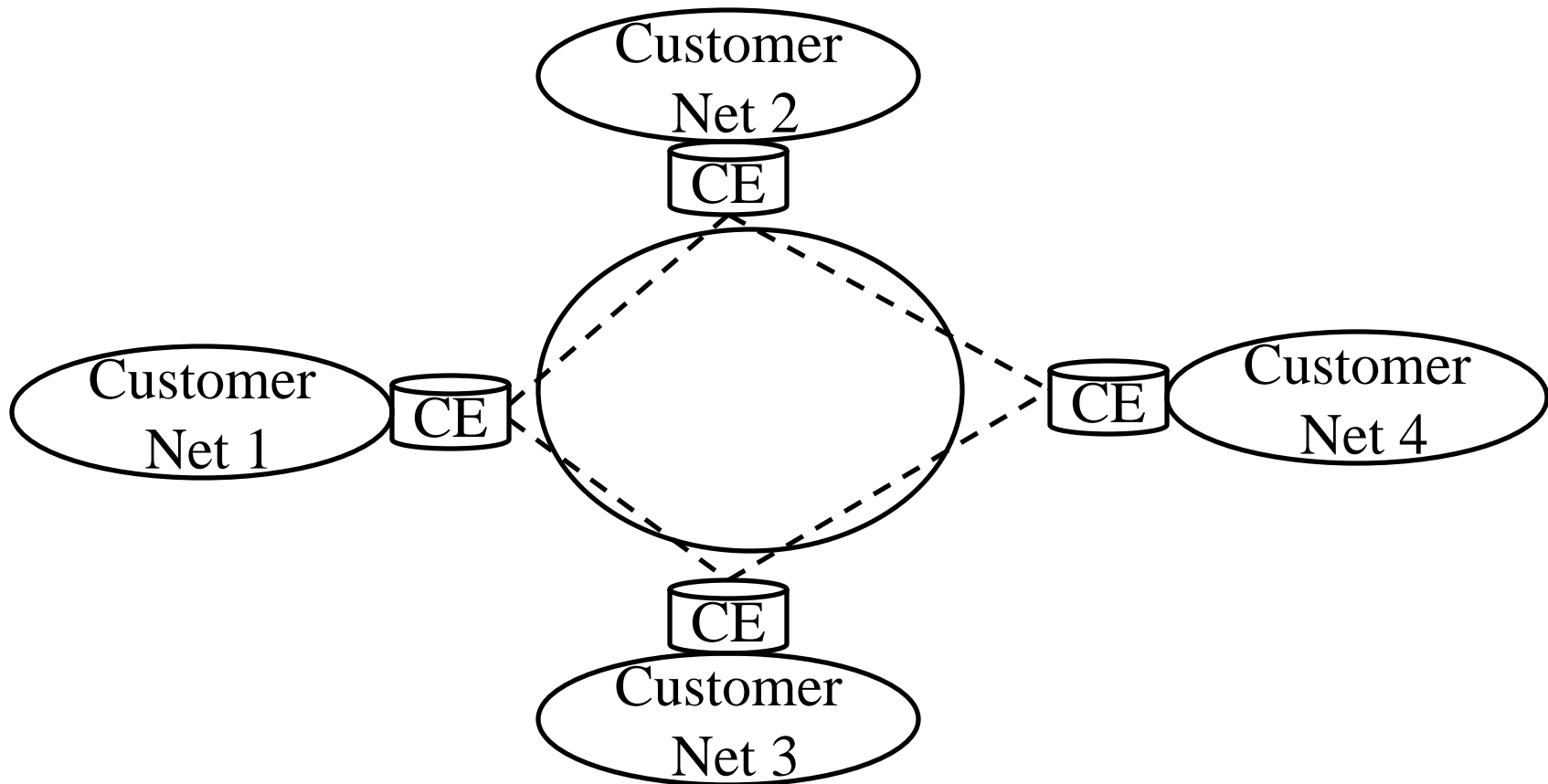
Types of VPNs (Cont)

- ❑ Payload Layer: Layer 1 (L1), Layer 2 (L2) VPN (Ethernet), L3 VPN (IP)
- ❑ Tunneling Protocol: MPLS (Multiprotocol Label Switching), GMPLS (Generalized MPLS), L2TPv3 (Layer 2 Tunneling Protocol version 3), PPTP (Point to Point Tunneling Protocol)
- ❑ Who is in charge?: Provider Edge Device (PE Based) or Customer Edge Device (CE Based)



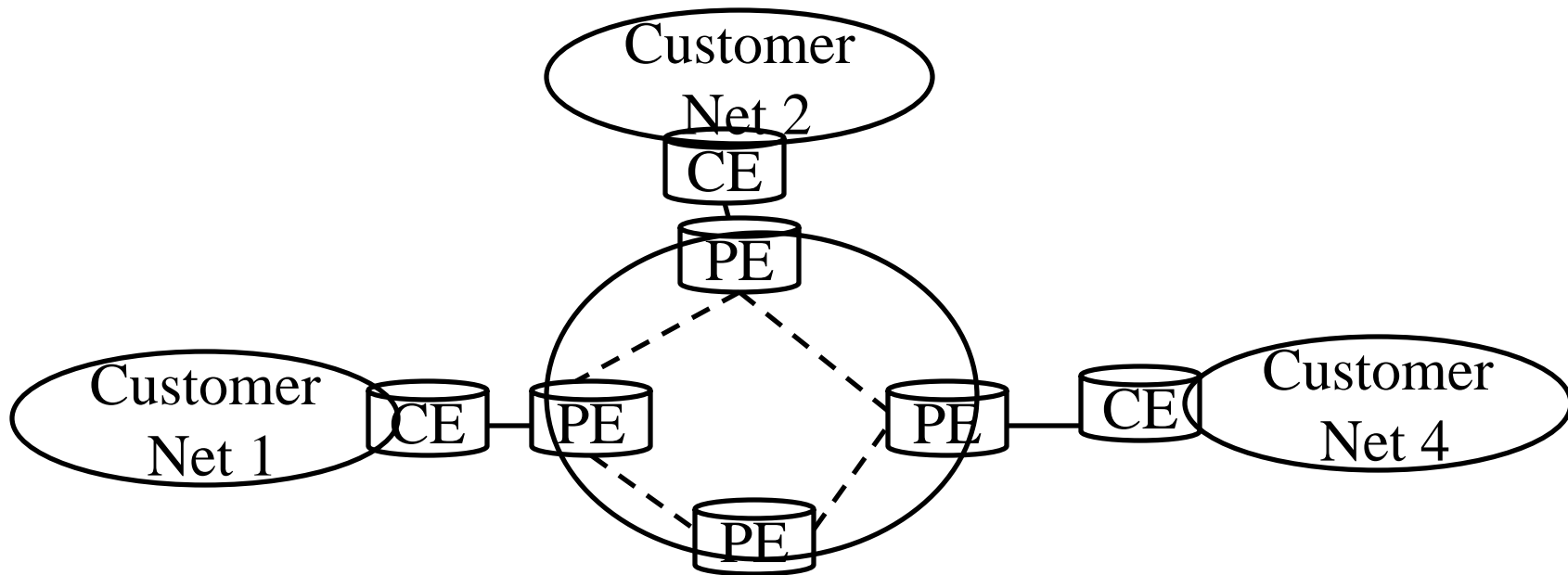
CE Based VPNs

- Customer's Edge routers implement IPsec tunnels



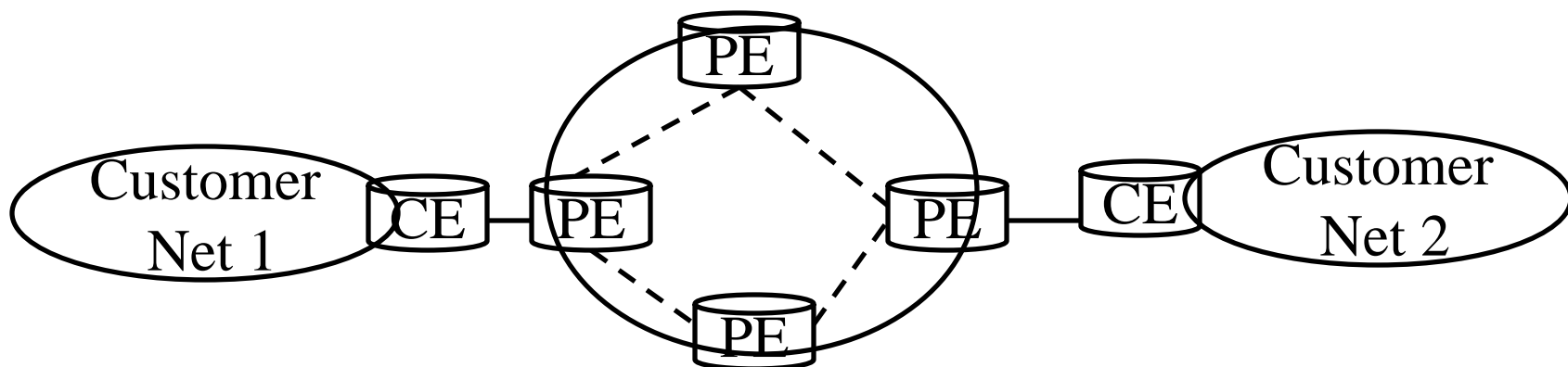
PE Based VPNs

- ❑ Service providers offers privacy, QoS, and Routing
- ❑ Customer uses standard routers



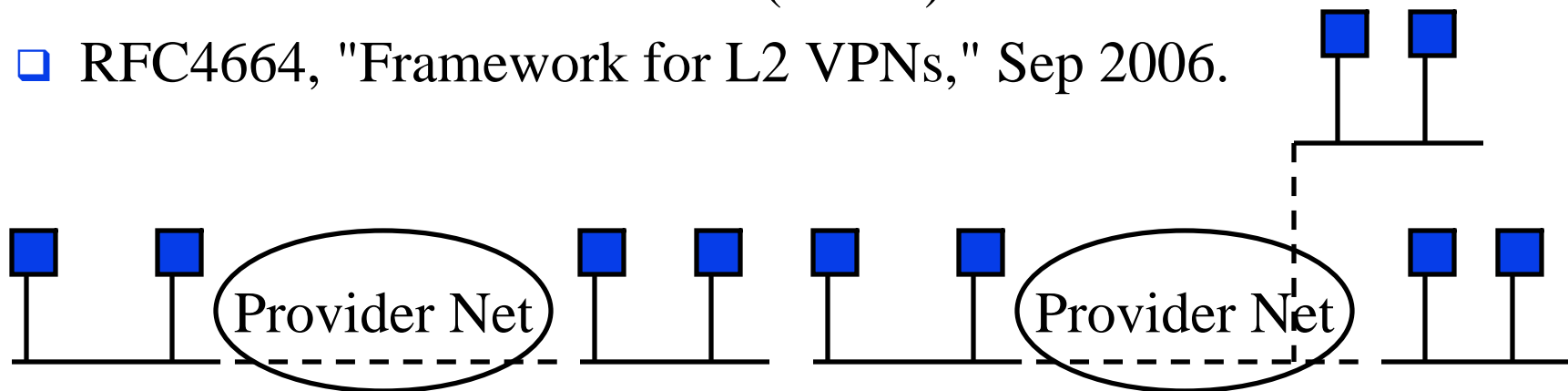
Layer 1 VPNs

- ❑ A single fiber can carry multiple wavelengths, which can be rearranged dynamically to provide a VPN for customers.
- ❑ Similarly, a single SONET (Synchronous optical network) stream can be shared by multiple customers.
- ❑ Connectivity is at layer 1. Any layer 2 signal (Ethernet, ATM, etc) or multiple L2 signals can be carried. [RFC 4847]
- ❑ Can be used by carrier's carriers



Layer 2 VPNs

- ❑ Customers' Layer 2 packets are encapsulated and delivered at the other end
- ❑ Looks like the two ends are on the same LAN or same wire \Rightarrow Provides Ethernet connectivity
- ❑ Works for all Layer 3 protocols
- ❑ Virtual Private Wire Service (VPWS)
- ❑ Virtual Private LAN Service (VPLS)
- ❑ RFC4664, "Framework for L2 VPNs," Sep 2006.



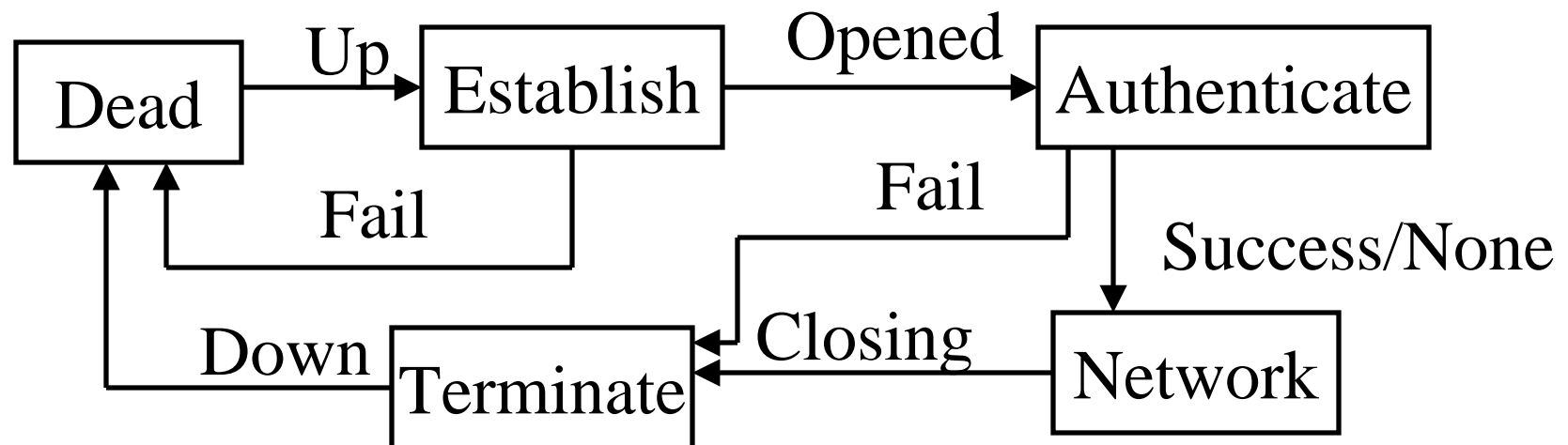
Layer 3 VPN

- ❑ Provides Layer 3 connectivity
- ❑ Looks like the two customer routers are connected
- ❑ Usually designed for IP packets



PPP: Introduction

- ❑ Point-to-point Protocol
- ❑ Originally for User-network connection
- ❑ Now being used for router-router connection
- ❑ Three Components: Data encapsulation, Link Control Protocol (LCP), Network Control Protocols (NCP)



PPP Procedures

- ❑ Typical connection setup:
 - Home PC Modem calls Internet Provider's router: sets up physical link
 - PC sends series of LCP packets
 - ❑ Select PPP (data link) parameters
 - ❑ Authenticate
 - PC sends series of NCP packets
 - ❑ Select network parameters
E.g., Get dynamic IP address
- ❑ Transfer IP packets

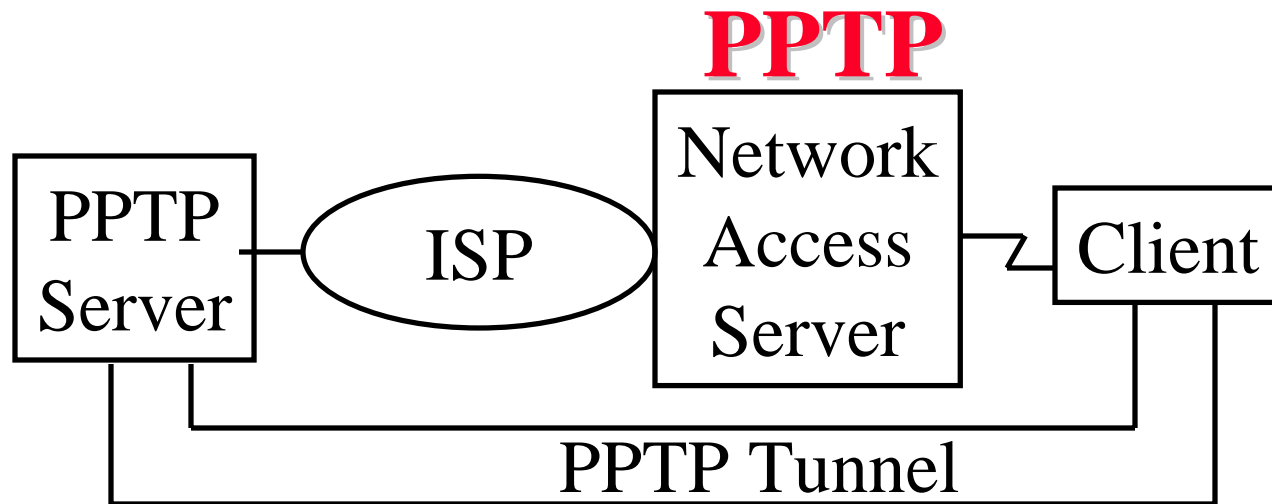
VPN Tunneling Protocols

- ❑ GRE: Generic Routing Encapsulation (RFC 1701/2)
- ❑ PPTP: Point-to-point Tunneling Protocol
- ❑ L2TP: Layer 2 Tunneling protocol
- ❑ IPsec: Secure IP
- ❑ MPLS: Multiprotocol Label Switching

GRE

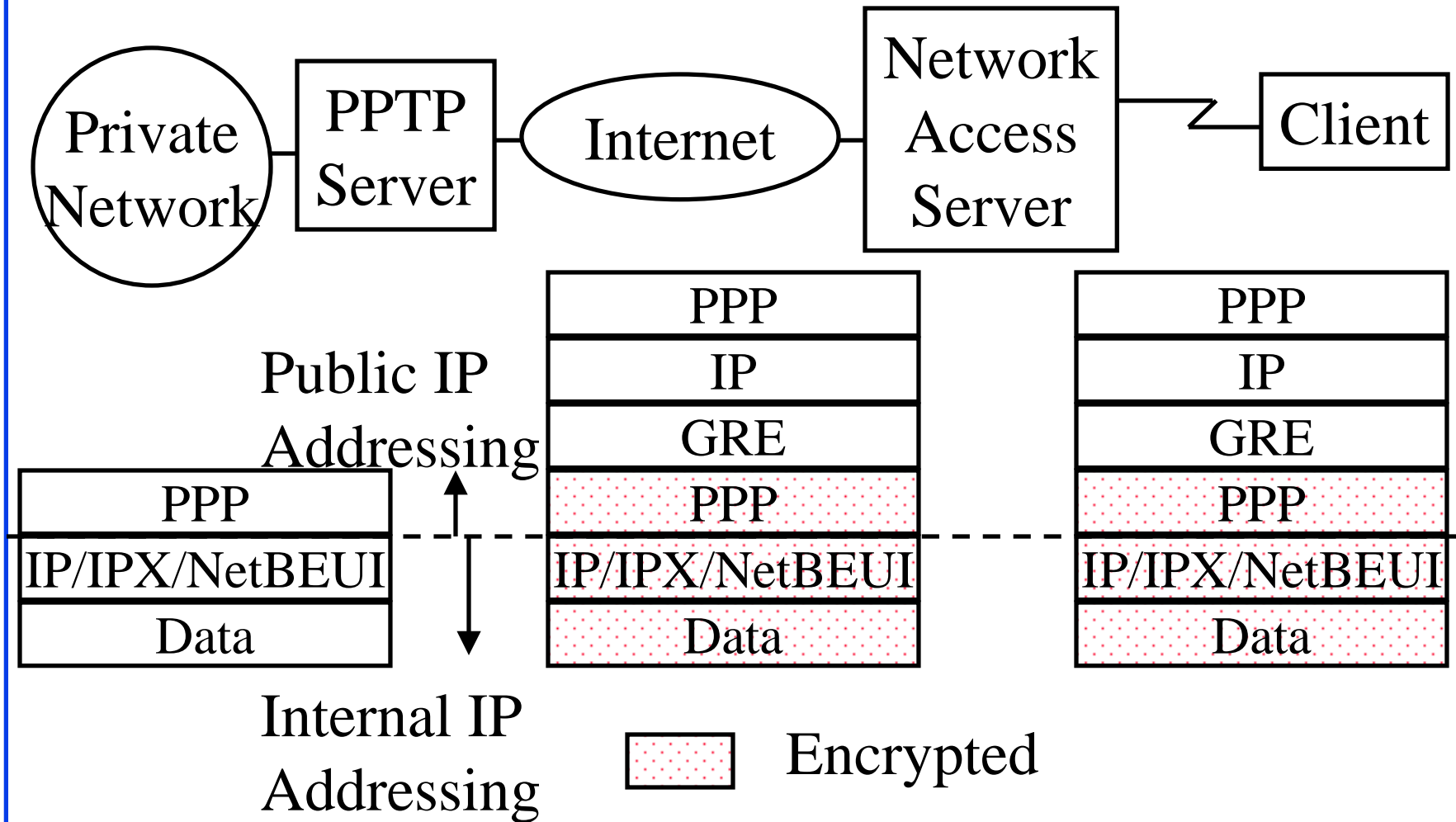


- ❑ Generic Routing Encapsulation (RFC 1701/1702)
- ❑ Generic \Rightarrow X over Y for any X or Y
- ❑ Optional Checksum, Loose/strict Source Routing, Key
- ❑ Key is used to authenticate the source
- ❑ Over IPv4, GRE packets use a protocol type of 47
- ❑ Allows router visibility into application-level header
- ❑ Restricted to a single provider network \Rightarrow end-to-end



- ❑ PPTP = Point-to-point Tunneling Protocol
- ❑ Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics
- ❑ PPTP server for NT4 and clients for NT/95/98

PPTP Packets



L2TP

- ❑ Layer 2 Tunneling Protocol
- ❑ L2F = Layer 2 Forwarding (From CISCO)
- ❑ L2TP = L2F + PPTP
Combines the best features of L2F and PPTP
- ❑ Easy upgrade from L2F or PPTP
- ❑ Allows PPP frames to be sent over non-IP (Frame relay, ATM) networks also (PPTP works on IP only)
- ❑ Allows multiple (different QoS) tunnels between the same end-points. Better header compression.
Supports flow control

L2TPv3

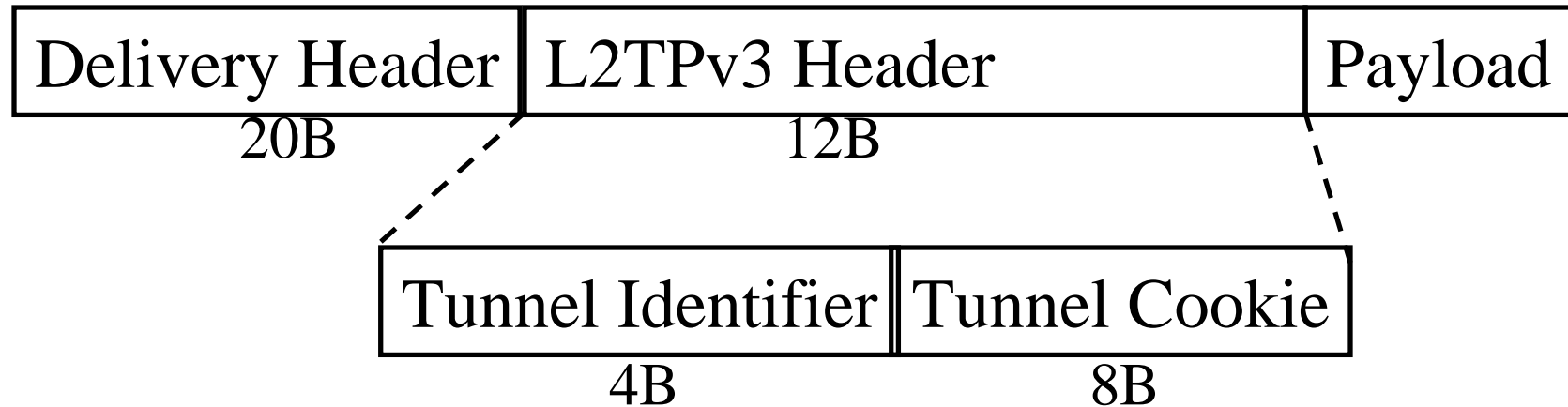


- ❑ Allows service providers to offer L2 VPN over IP network.
- ❑ L2TPv2 was for tunneling PPP over packet switched data networks (PSDN)
- ❑ V3 generalizes it for other protocols over PSDN
⇒ PPP specific header removed
- ❑ Can handle HDLC (High-Level Data Link Control), Ethernet, 802.1Q VLANs, Frame relay, packet over SONET (Synchronous Optical Network)

L2TPv3 (Cont)

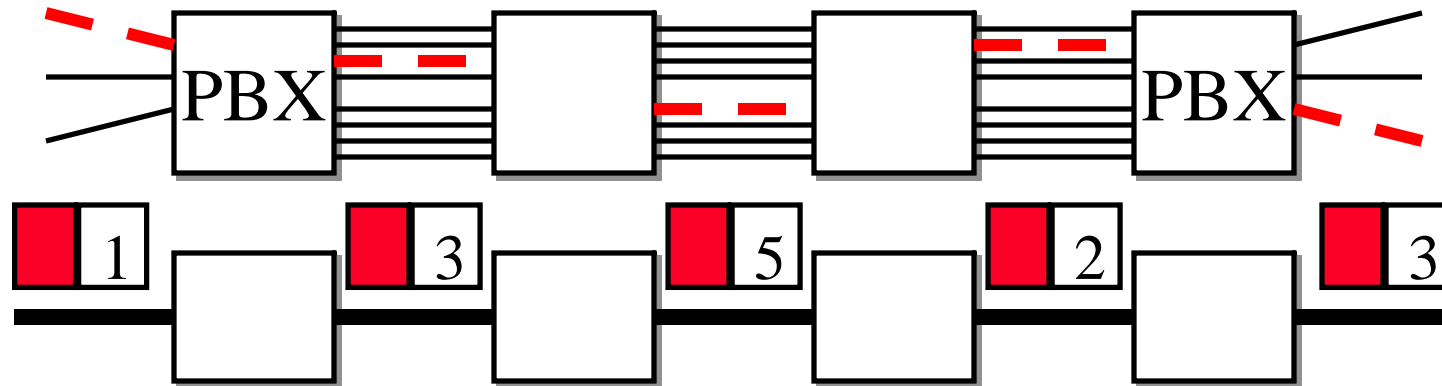
- ❑ Universal Transport Interface (UTI) is a pre-standard effort for transporting L2 frames.
- ❑ L2TPv3 extends UTI and includes it as one of many supported encapsulations.
- ❑ L2TPv3 has a control plane using reliable control connection for establishment, teardown and maintenance of individual sessions.
- ❑ RFC4667, "L2 VPN extensions for L2TP," Sept 2006
- ❑ Ref: L2TPv3 FAQ,
www.cisco.com/warp/public/cc/so/neso/vpn/unvpnst/2tpv3_qp.pdf

L2TPv3 Frame Format

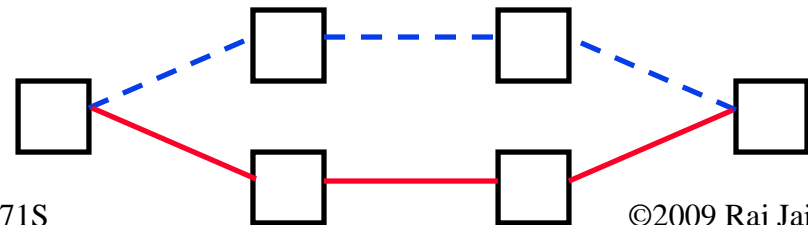


- ❑ Delivery Header: IPv4 header
- ❑ Payload: L2 or L3 packet

Multiprotocol Label Switching (MPLS)



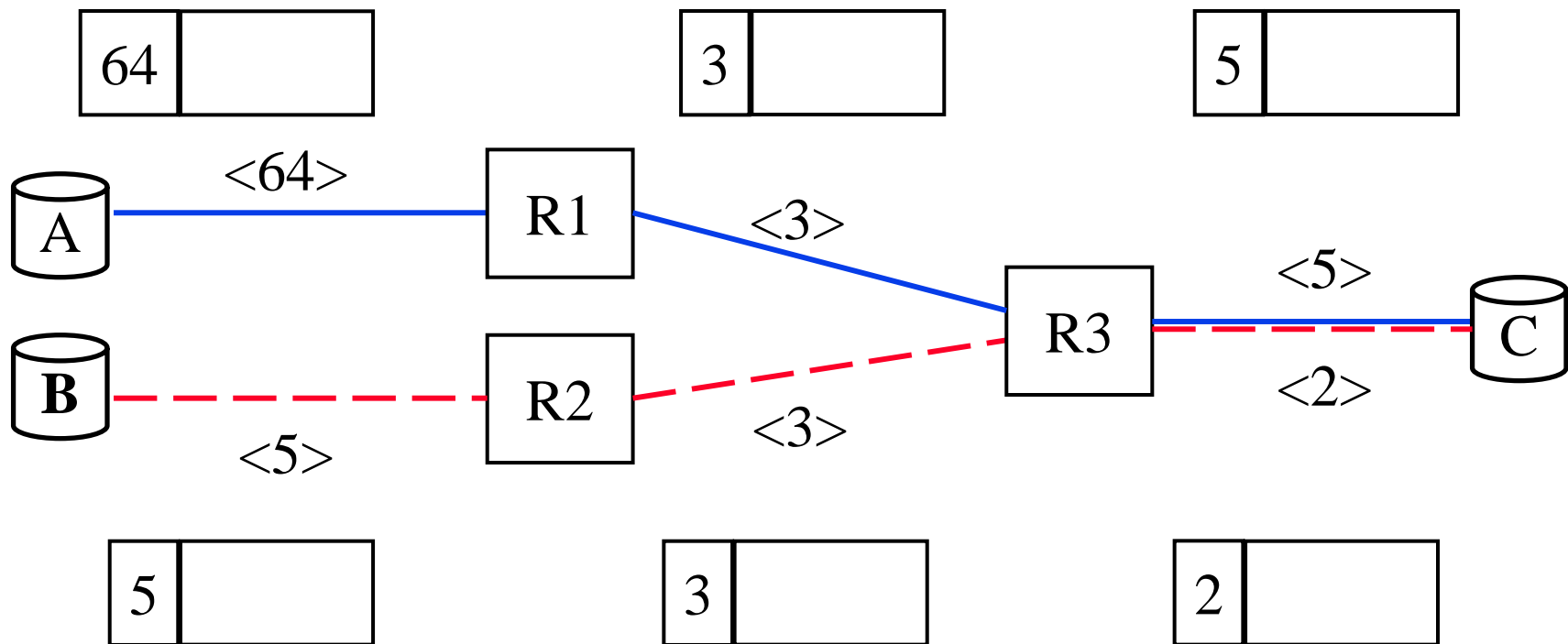
- ❑ Allows virtual circuits in IP Networks (May 1996)
- ❑ Each packet has a virtual circuit number called 'label'
- ❑ Label determines the packet's queuing and forwarding
- ❑ Circuits are called Label Switched Paths (LSPs)
- ❑ LSP's have to be set up before use
- ❑ Allows traffic engineering



Label Switching Example



Layer 2.5

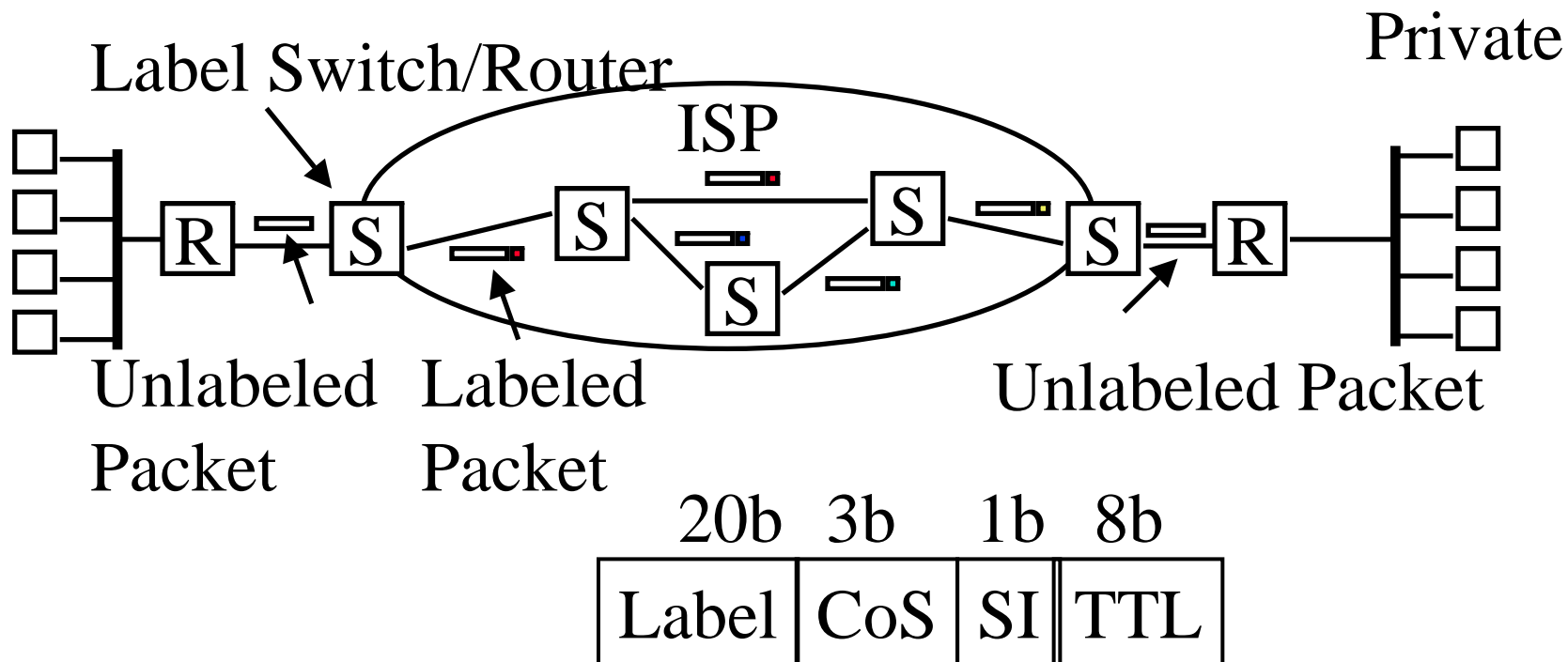


Label Assignment

- ❑ Unsolicited: Topology driven \Rightarrow Routing protocols exchange labels with routing information.
Many existing routing protocols are being extended:
BGP, OSPF
- ❑ On-Demand:
 \Rightarrow Label assigned when requested,
e.g., when a packet arrives \Rightarrow latency
- ❑ Label Distribution Protocol called **LDP**
- ❑ **RSVP** has been extended to allow label request and response

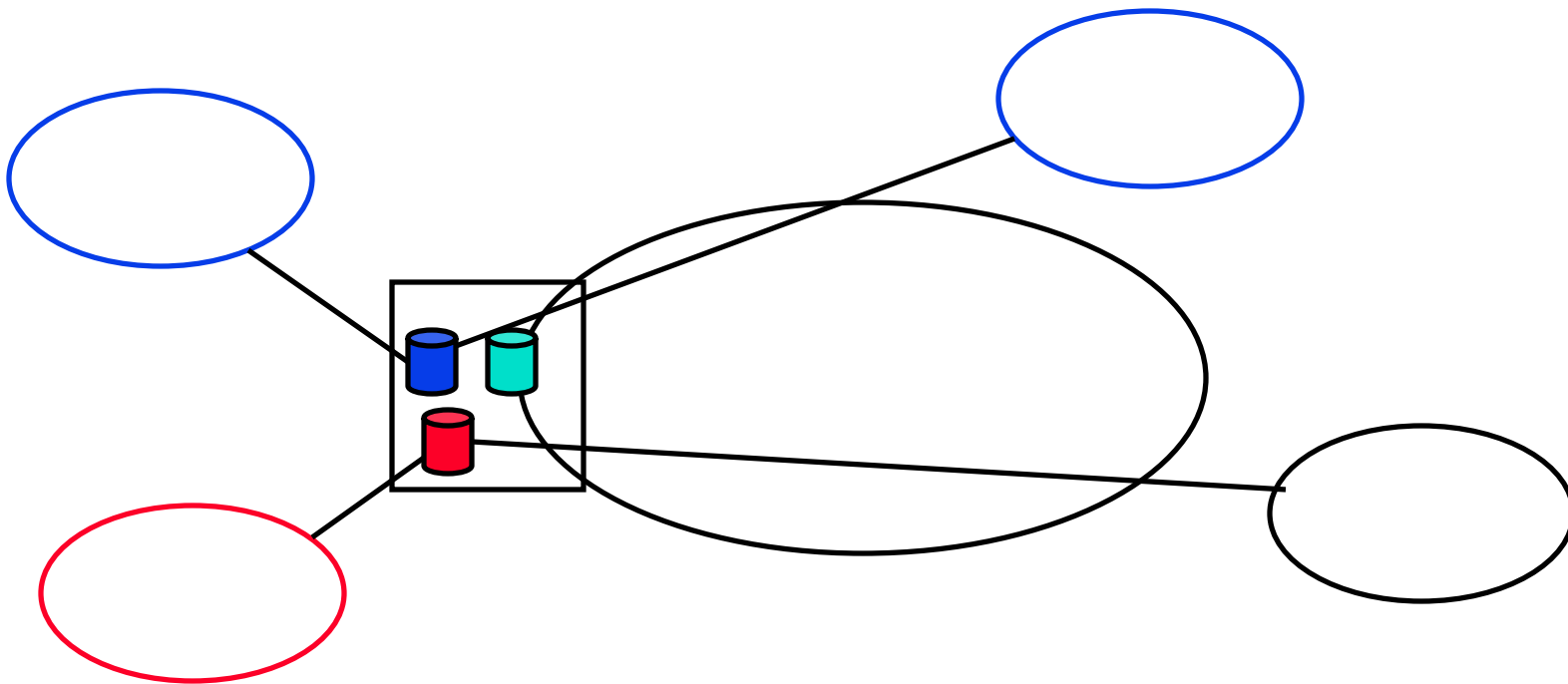
VPN Support with MPLS

- Labels contain Class of Service (CoS), Stack Indicator (SI), and Time to Live (TTL)

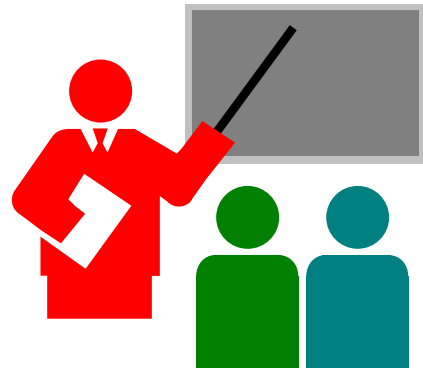


Virtual Router IP VPNS

- ❑ PE router emulates many virtual routers
- ❑ Each virtual router belongs to only one VPN



Summary



- ❑ VPN allows secure communication on the Internet
- ❑ Three types: WAN, Access, Extranet
- ❑ Key issues: address translation, security, performance
- ❑ Layer 2 (PPTP, L2TP), Layer 3 (IPSec)
- ❑ QoS is still an issue \Rightarrow MPLS

Lab Homework 17

- ❑ Install CSE VPN or CEC VPN. See instructions at <http://www.cts.wustl.edu/cts/help/vpn/cse-vpnconfig.htm> or <https://www.cec.wustl.edu/help.aspx?page=20&treepath=0.5>
- ❑ Connect to VPN from outside the campus using your computer. Right click on the VPN icon and submit a screen capture of the statistics or note down the following:
 - Encryption algorithm
 - Authentication algorithm
 - Client Address
 - Server Address

Acronyms

- ❑ BGP Border Gateway Protocol
- ❑ CE Customer Edge
- ❑ DNS Domain Name System
- ❑ GRE Generic Routing Encapsulation
- ❑ IPsec IP Security
- ❑ IPv4 IP Version 4
- ❑ IPv6 IP Version 6
- ❑ ISP Internet Service Provider
- ❑ KMI Key Management Infrastructure
- ❑ L2 Layer 2
- ❑ L2F Layer 2 Forwarding
- ❑ L2TP Layer 2 Tunneling Protocol

Acronyms (Cont)

- ❑ L2TPv3 Layer 2 Tunnelling Protocol Version 3
- ❑ L3 Layer 3
- ❑ LAN Local Area Network
- ❑ LCP Link Control Protocol
- ❑ LDP Label Distribution Protocol
- ❑ LSP Label Switched Path
- ❑ MIB Management Information Base
- ❑ MPLS Multiprotocol Label Switching
- ❑ OSPF Open Shortest Path
- ❑ PE Provider Edge
- ❑ PPP Point-to-point Protocol
- ❑ PPTP Point-to-point Tunneling Protocol

Acronyms (Cont)

- ❑ PPVPN Provider Provisioned VPN
- ❑ RFC Request for Comment
- ❑ SNMP Simple Network Management Protocol
- ❑ TP Tunneling protocol
- ❑ USR US Robotics
- ❑ UTI Universal Transport Interface
- ❑ VPN Virtual Private Network
- ❑ VPWS Virtual Private Wire Service
- ❑ WAN Wide Area Network

Reading List

- ❑ <http://en.wikipedia.org/wiki/Vpn>
- ❑ http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol
- ❑ <http://en.wikipedia.org/wiki/L2TPv3>
- ❑ <http://www.ripe.net/ripe/meetings/ripe-42/presentations/ripe42-eof-pseudowires2/sld001.html>
- ❑ http://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
- ❑ <http://www.netcraftsmen.net/welcher/papers/mplsvpn.html>
- ❑ <http://en.wikipedia.org/wiki/Pptp>
- ❑ Understanding PPTP, <http://technet.microsoft.com/en-us/library/cc768084.aspx>
- ❑ RFC 2637 (PPTP), 3931 (L2TPv3), 4364 (BGP/MPLS VPNs)

VPN RFCs

- ❑ **RFC2637, PPTP, July 1999**
- ❑ RFC 2685, Virtual Private Networks Identifier, September 1999.
- ❑ RFC 2735, NHRP Support for VPNs, December 1999.
- ❑ RFC 2764, A Framework for IP Based VPNs, February 2000.
- ❑ RFC2917, A Core MPLS IP VPN Architecture. Sep 2000.
- ❑ RFC3809, Generic Requirements for PPVPN. Jun 2004.
- ❑ **RFC3931, L2TPv3, Mar 2005.**
- ❑ RFC4026, PPVPN Terminology. Mar 2005.
- ❑ RFC4031, Service Requirements for Layer 3 PPVPNs. Apr 2005.

VPN RFCs (Cont)

- ❑ RFC4093, Problem Statement: Mobile IPv4 Traversal of VPN Gateways. Aug 2005.
- ❑ RFC4110, A Framework for Layer 3 PPVPNs. Jul 2005.
- ❑ RFC4111, Security Framework for PPVPNs. Jul 2005.
- ❑ RFC4176, Framework for L3 VPN Operations and Management. Oct 2005.
- ❑ RFC4265, Definition of Textual Conventions for VPN Management. Nov 2005.
- ❑ **RFC4364, BGP/MPLS IP VPNs. Feb 2006.**
- ❑ RFC4365, Applicability Statement for BGP/MPLS IP VPNs. Feb 2006.
- ❑ RFC4381, Analysis of the Security of BGP/MPLS IP VPNs. Feb 2006.

VPN RFCs (Cont)

- ❑ RFC4382, MPLS/BGP Layer 3 VPN MIB. Feb 2006.
- ❑ RFC4576, Using a LSA Options Bit to Prevent Looping in BGP/MPLS IP VPNs. Jun 2006.
- ❑ RFC4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP VPNs. Jun 2006.
- ❑ RFC4659, BGP-MPLS IP VPN Extension for IPv6 VPN. Sep 2006.
- ❑ RFC4664, Framework for L2 VPNs. Sep 2006.
- ❑ RFC 4665, Service Requirements for Layer 2 PPVPNs, September 2006.
- ❑ RFC4667, L2 VPN Extensions for L2TP. Sep 2006.
- ❑ RFC4684, Constrained Route Distribution for BGP/MPLS IP VPNs. Nov 2006.

VPN RFCs (Cont)

- ❑ RFC 4797, Use of PE-PE GRE or IP in BGP/MPLS IP VPNs, January 2007.
- ❑ RFC4834, Requirements for Multicast in L3 PPVPNs. Apr 2007.
- ❑ RFC 4847, Framework and Requirements for Layer 1 VPNs, April 2007.
- ❑ RFC 4923 QoS Signaling in a Nested VPN, August 2007.
- ❑ RFC 5195, BGP-Based Auto-Discovery for Layer-1 VPNs, June 2008.
- ❑ RFC 5251, Layer 1 VPN Basic Mode, July 2008.
- ❑ RFC 5252, OSPF-Based Layer 1 VPN Auto-Discovery, July 2008.
- ❑ RFC 5253, Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Basic Mode, July 2008.
- ❑ RFC 5265, Mobile IPv4 Traversal across IPsec-Based VPN Gateways, June 2008.