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:

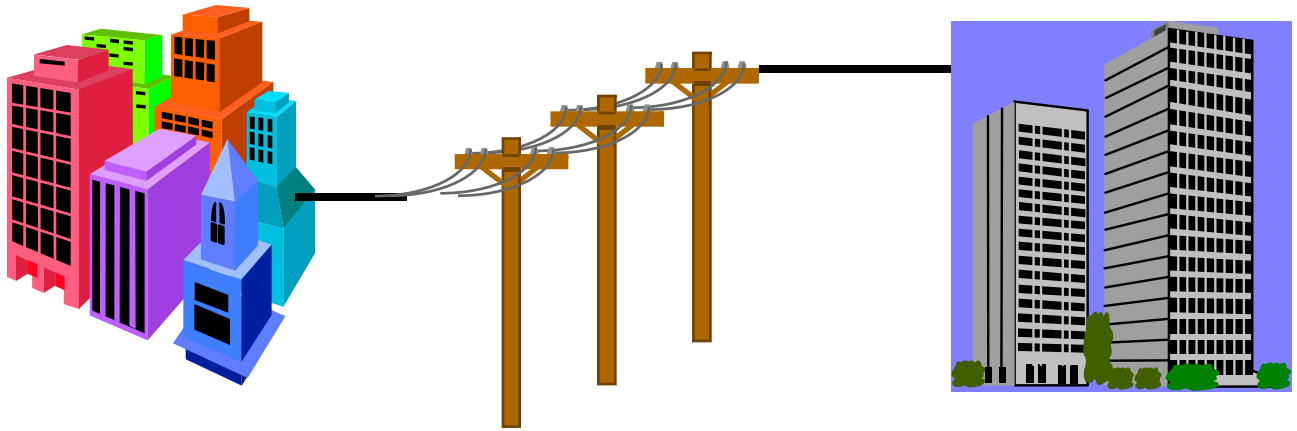
http://www.cse.wustl.edu/~jain/cse571-07/

Overview

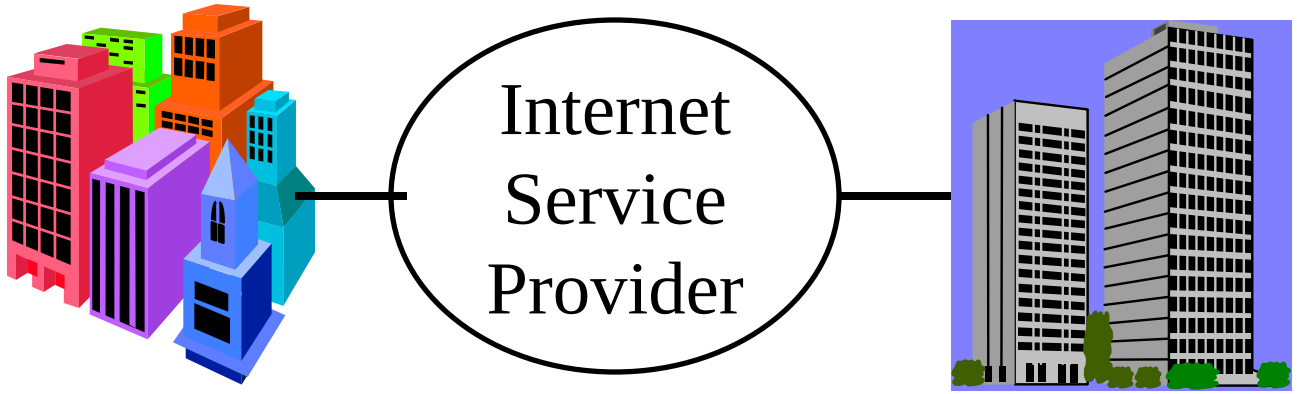
- Overview: What, When, Issues
- Types of VPNs: PE/CE based, L2 vs. L3
- PPP
- VPN Tunneling Protocols: GRE, PPTP, L2TPv3, MPLS

What is a VPN?

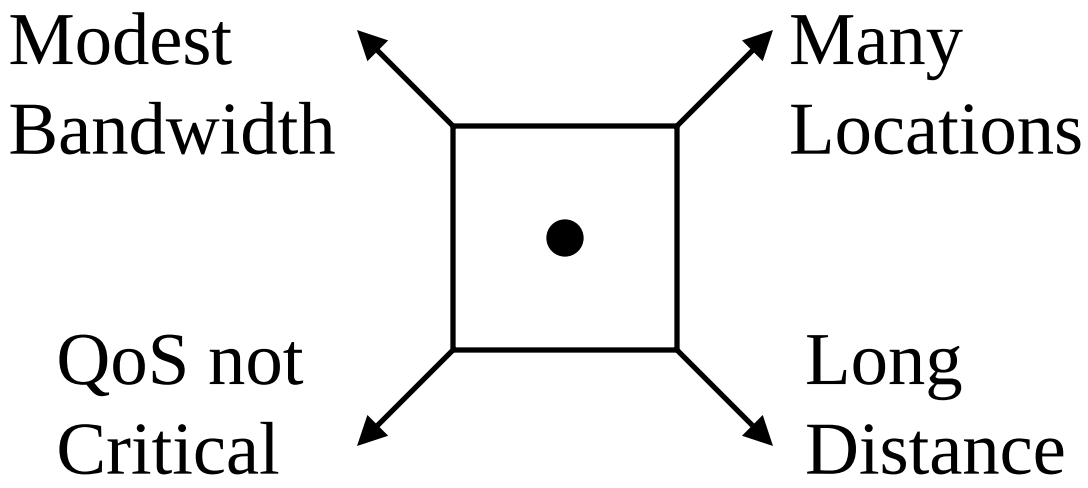
- Private Network: Uses leased lines



- *Virtual* Private Network: Uses public Internet



When to VPN?



- More Locations, Longer Distances, Less Bandwidth/site, QoS less critical
  ⇒ VPN more justifiable
- Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical
  ⇒ VPN less justifiable

VPN Design Issues

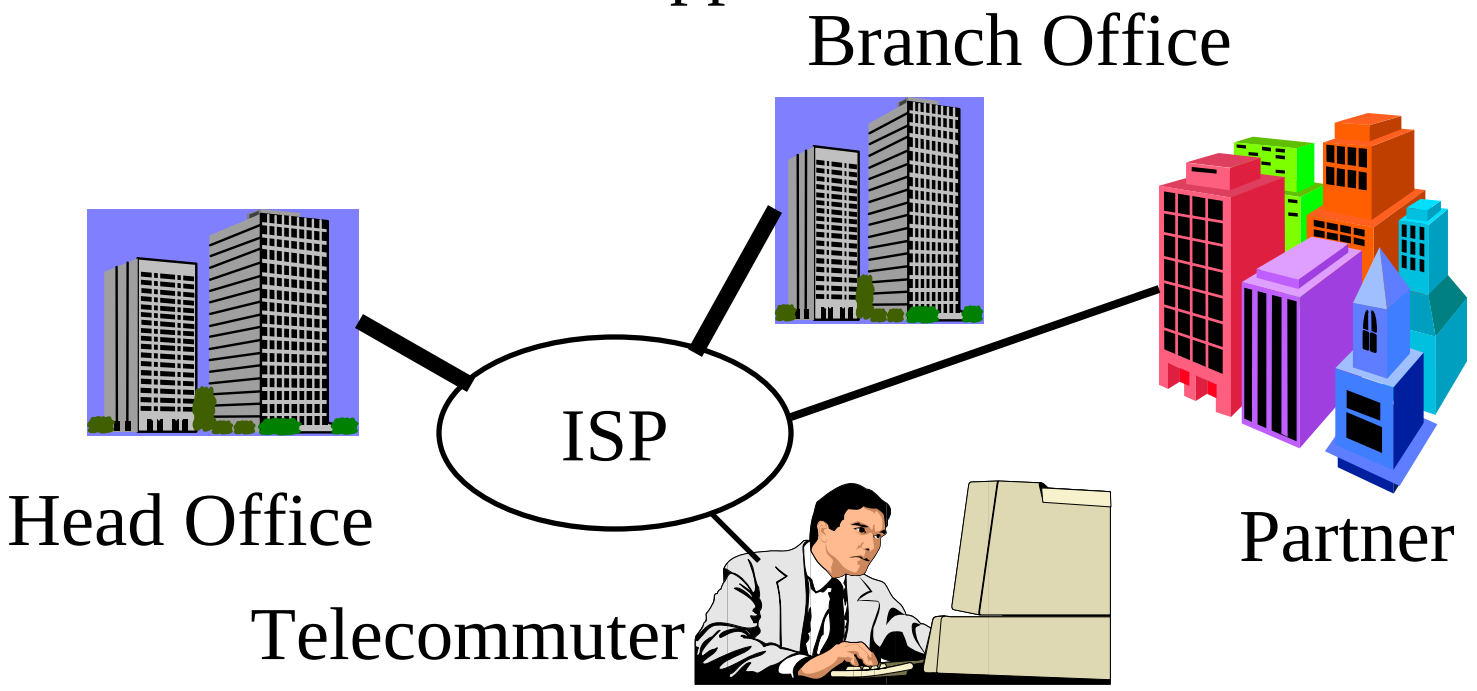
1. Security
2. Address Translation
3. Performance: Throughput, Load balancing (round-robin DNS), fragmentation
4. Bandwidth Management: RSVP
5. Availability: Good performance at all times
6. Scalability: Number of locations/Users
7. Interoperability: Among vendors, ISPs, customers (for extranets) $\Rightarrow$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

Design Issues (Cont)

8. Compression: Reduces bandwidth requirements
9. Manageability: SNMP, 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
    $\Rightarrow$ Need key recovery

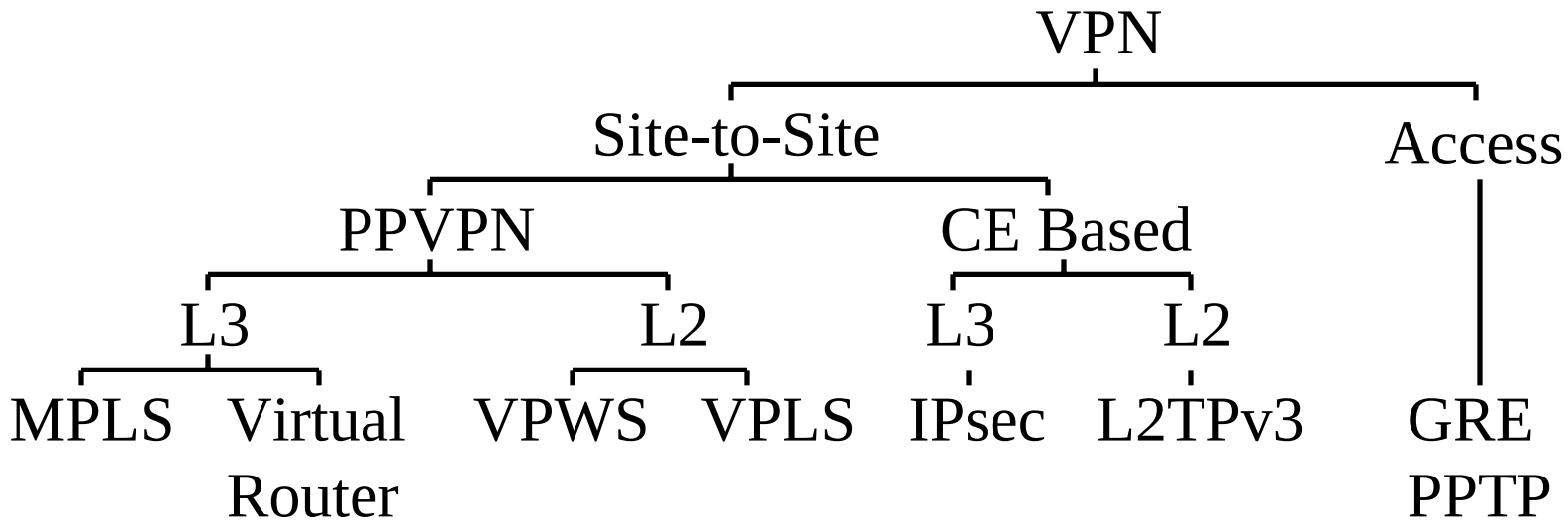
Types of VPNs

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



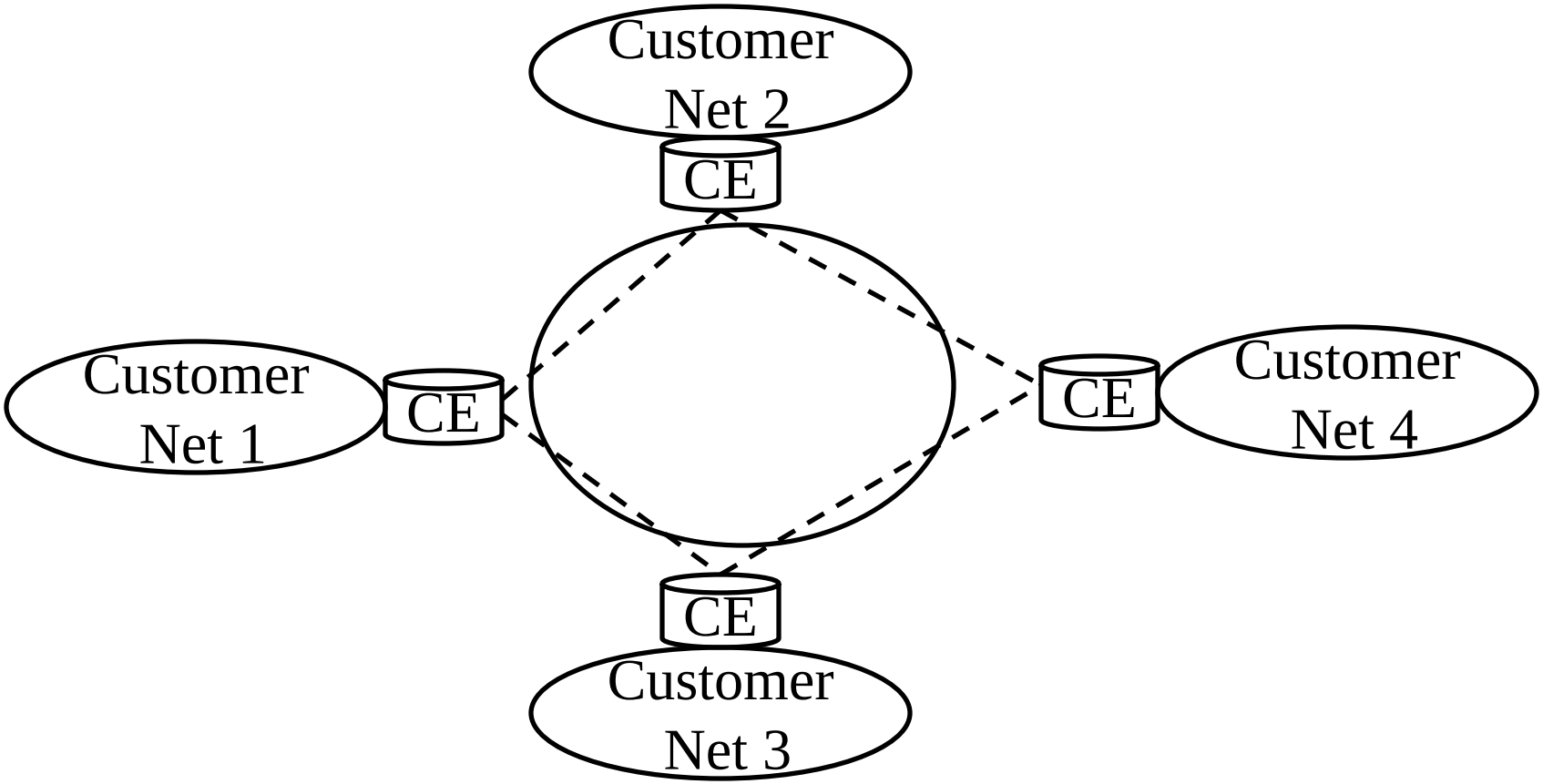
Types of VPNs (Cont)

- Payload Layer: L2 VPN (Ethernet), L3 VPN (IP)
- Tunneling Protocol: MPLS, L2TPv3, PPTP
- Who is in charge?: Provider Edge Device (PE Based) or Customer Edge Device (CE Based)



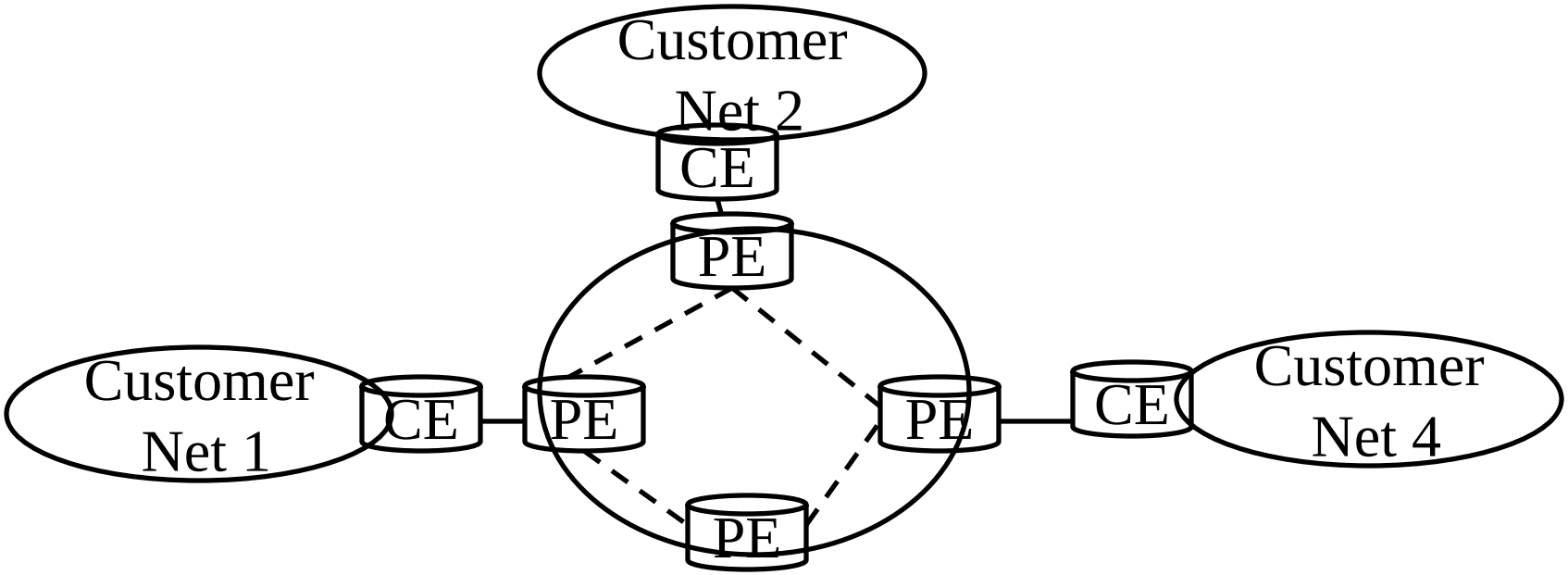
CE Based VPNs

- Customers Edge routers implement IPsec tunnels



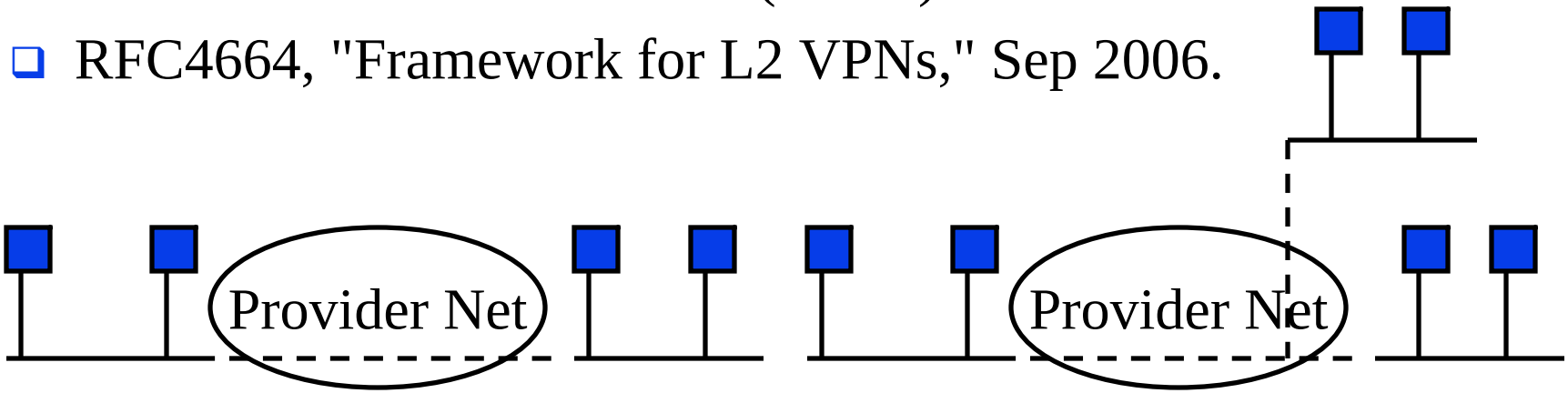
PE Based VPNs

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



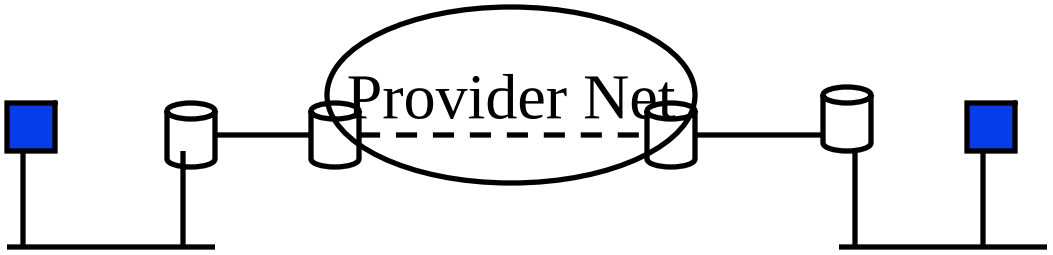
Layer 2 VPNs

- 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 ⇒ 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.



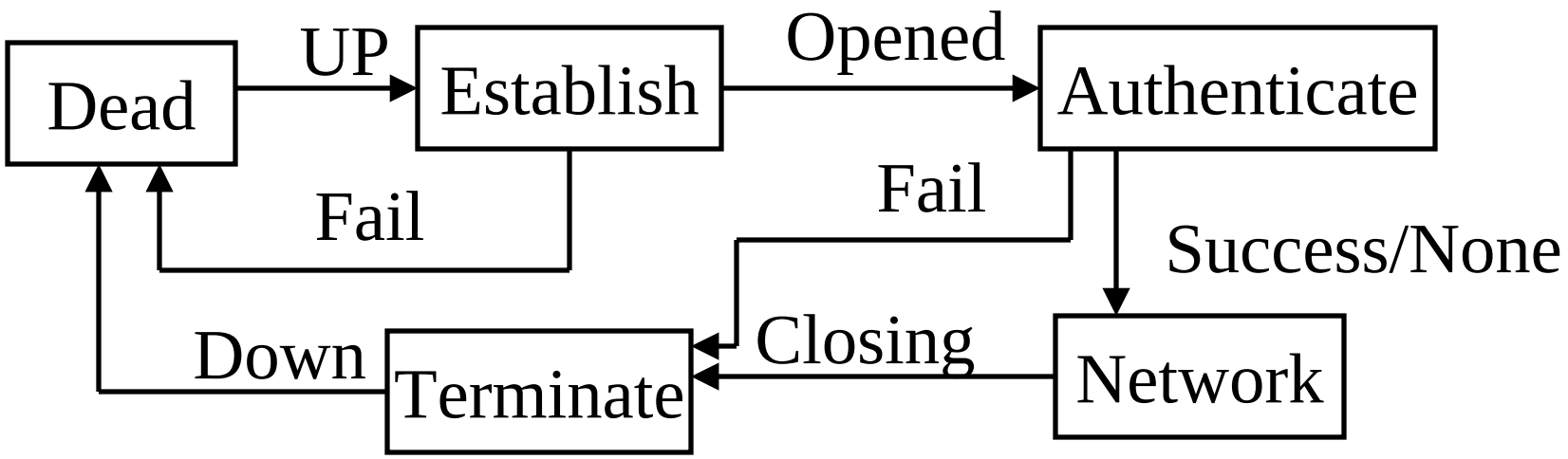
Layer 3 VPN

- 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 encaptulation, 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

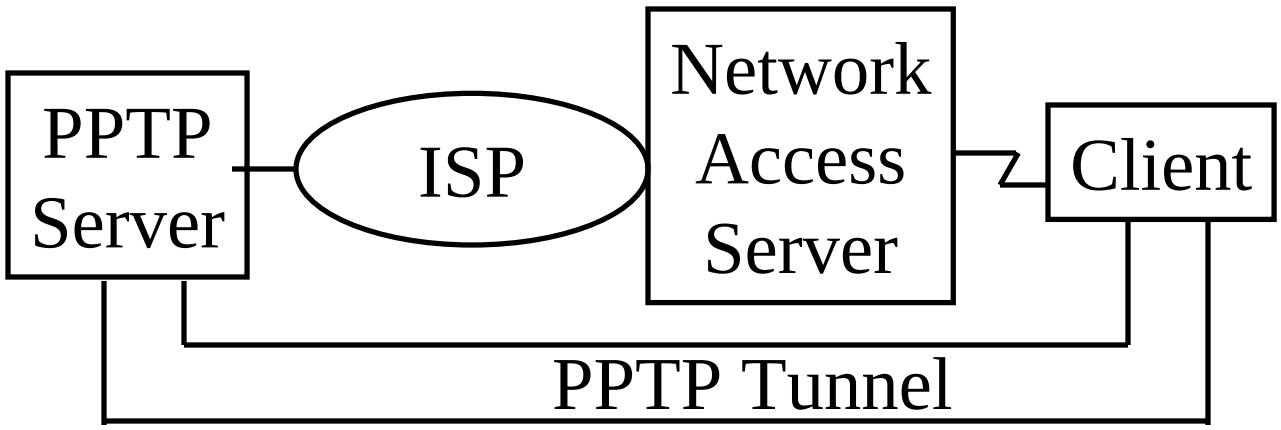
VPN Tunneling Protocols

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

GRE

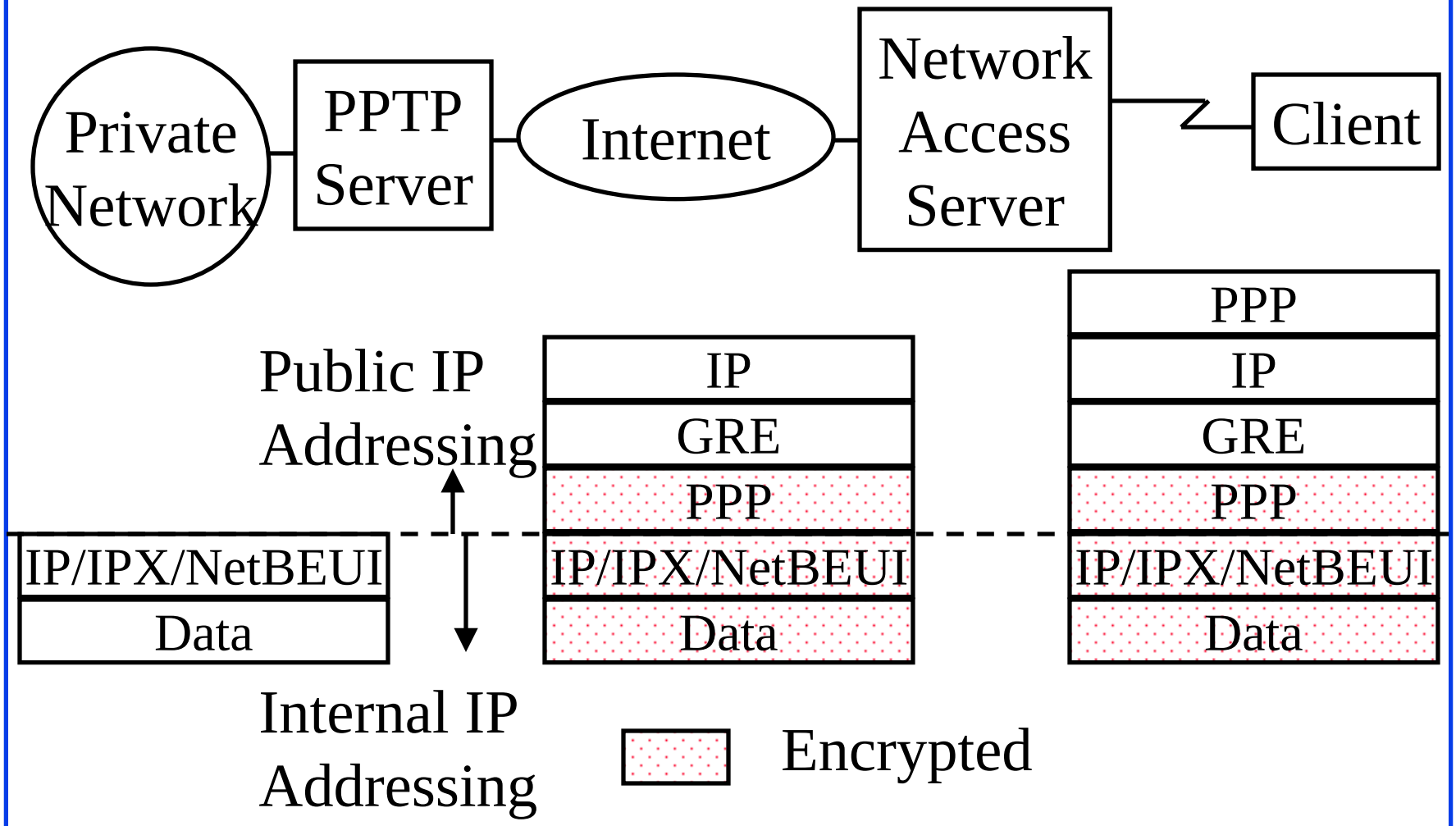
- Generic Routing Encaptulation (RFC 1701/1702)
- Generic ⇒ X over Y for any X or Y
- Optional Checksum, Loose/strict Source Routing, Key
- Key is used to authenticate the source
- Over IPv4, GRE packets use a protocol type of 47
- Allows router visibility into application-level header
- Restricted to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

PPTP



- 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

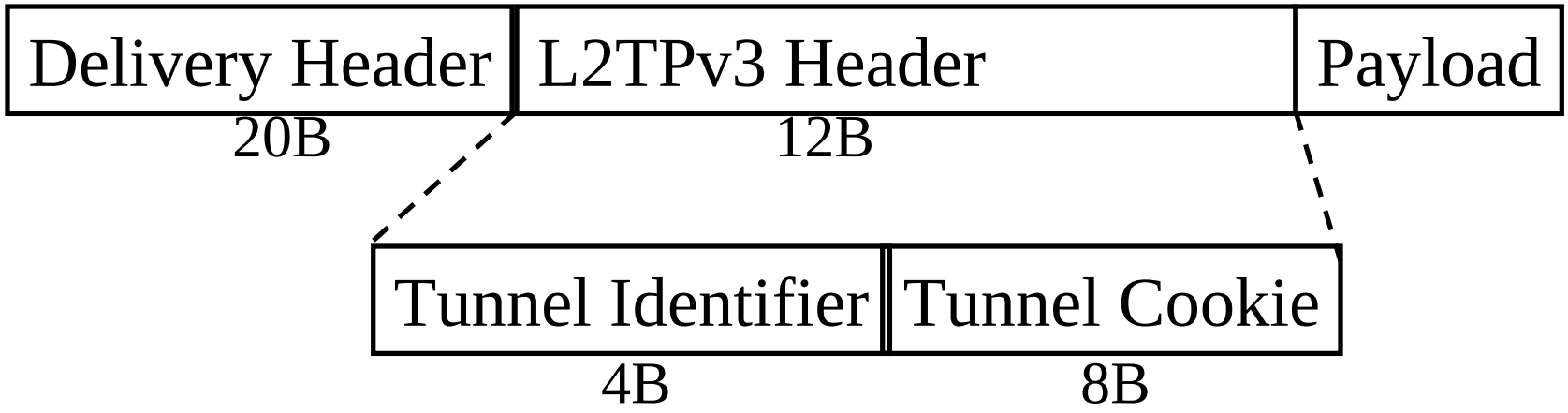
L2TPv3

- 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
  $\Rightarrow$ PPP specific header removed
- Can handle HDLC, Ethernet, 802.1Q VLANs, Frame relay, packet over SONET

L2TPv3 (Cont)

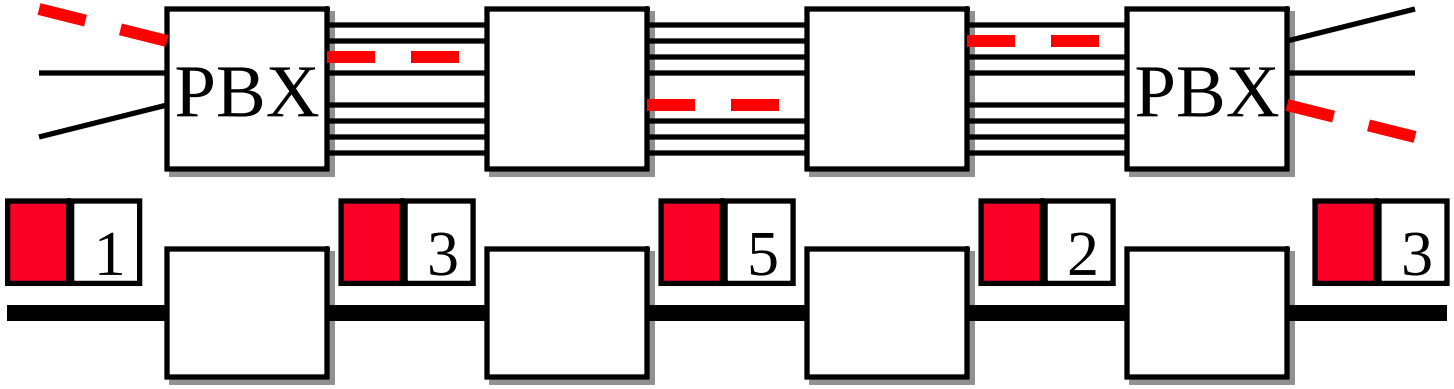
- Universal Transport Interface (UTI) is a pre-standard effort for transporting L2 frames.
- L2TPv3 extends UTI and includes it as one of many supported encapsulations.
- L2TPv3 has a control plane using reliable control connection for establishment, teardown and maintenance of individual sessions.
- 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

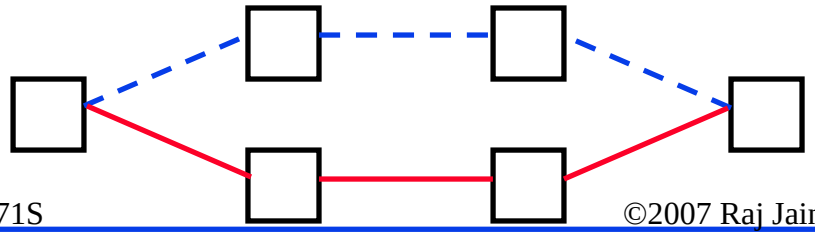


- Delivery Header: IPv4 header
- Payload: L2 or L3 packet

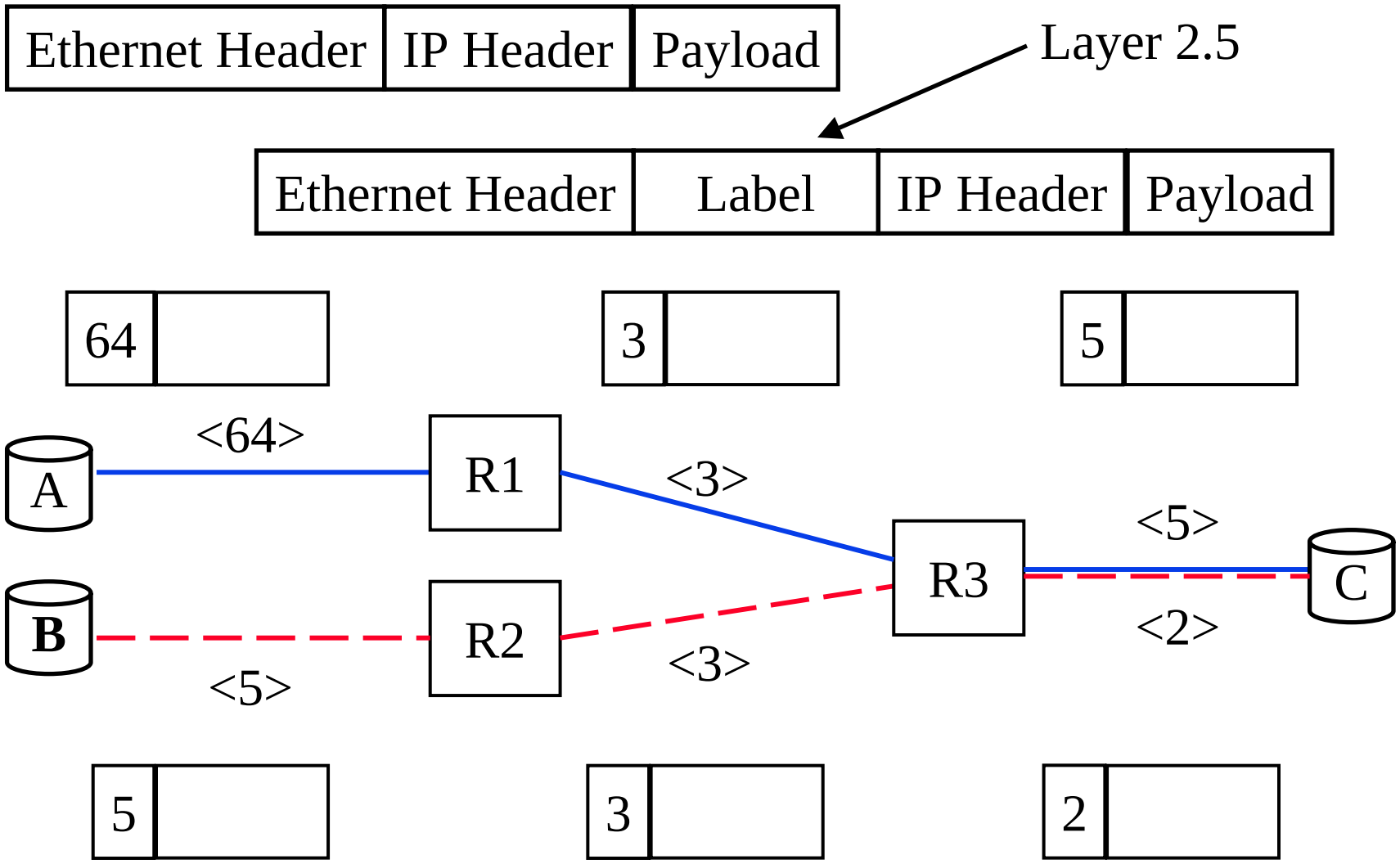
Multiprotocol Label Switching (MPLS)



- 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

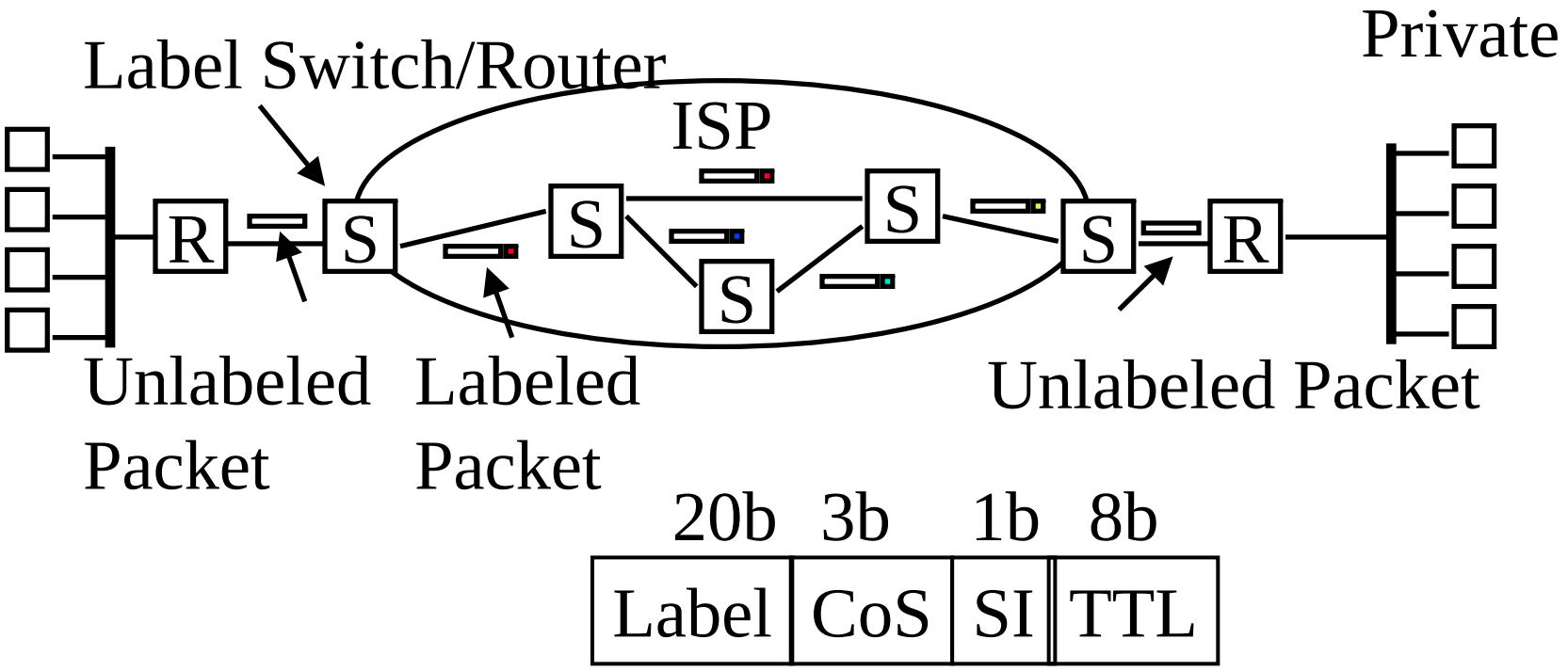


Label Assignment

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

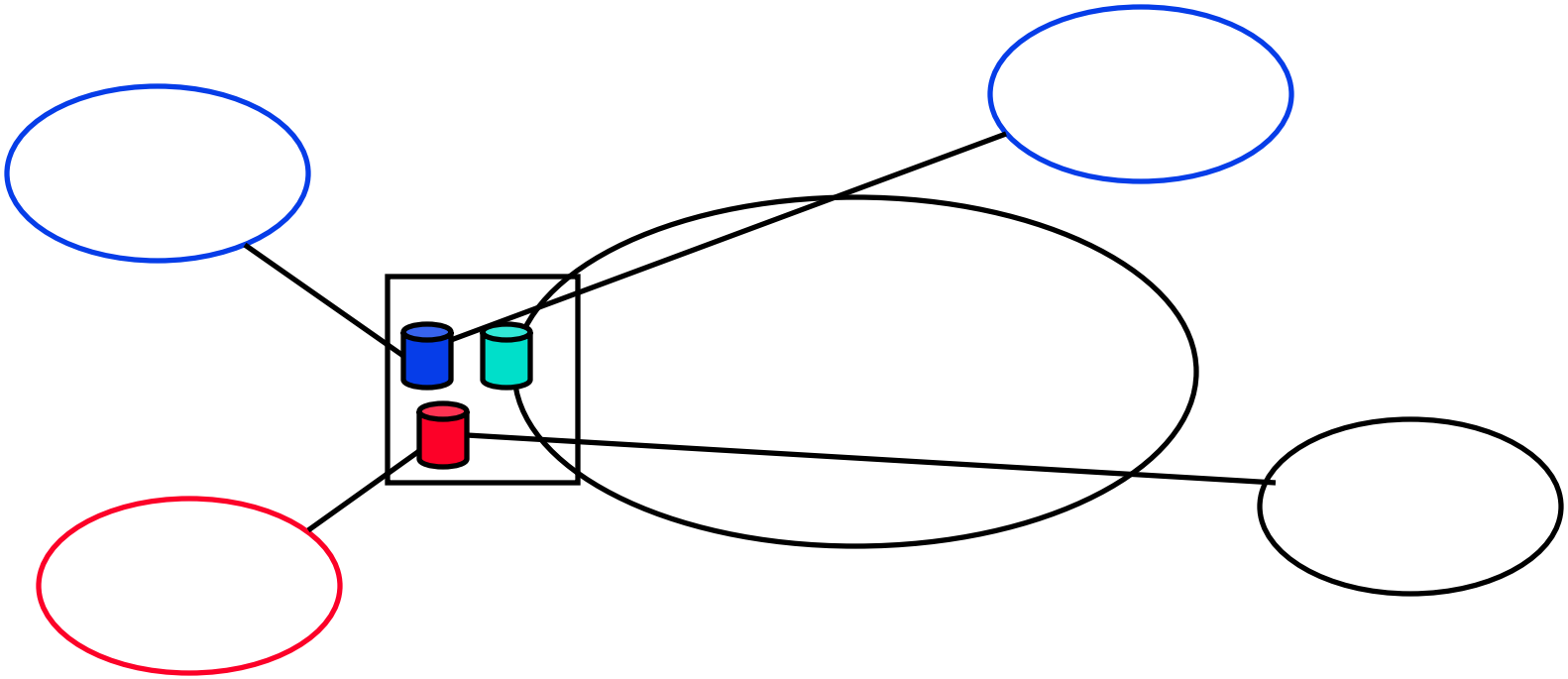
VPN Support with MPLS

- Labels contain Class of Service

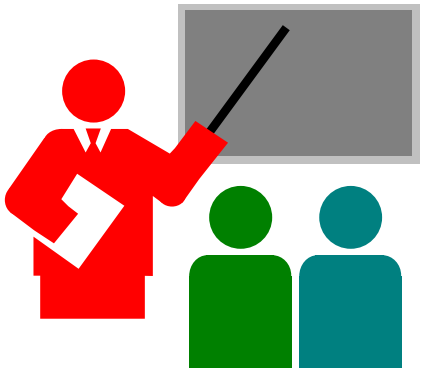


Virtual Router IP VPNS

- 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 ⇒ MPLS

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
- http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx?mfr=true
- RFC 2637 (PPTP), 3931 (L2TPv3), 4364 (BGP/MPLS VPNs)

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

VPN RFCs

- **RFC2637 PPTP, July 1999**
- 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.
- 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.

VPN RFCs (Cont)

- 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.
- 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.

VPN RFCs (Cont)

- 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.
- RFC4667 L2 VPN Extensions for L2TP. Sep 2006.
- RFC4684 Constrained Route Distribution for BGP/MPLS IP VPNs. Nov 2006.
- RFC4834 Requirements for Multicast in L3 PPVPNs. Apr 2007.