Virtual Private Networks

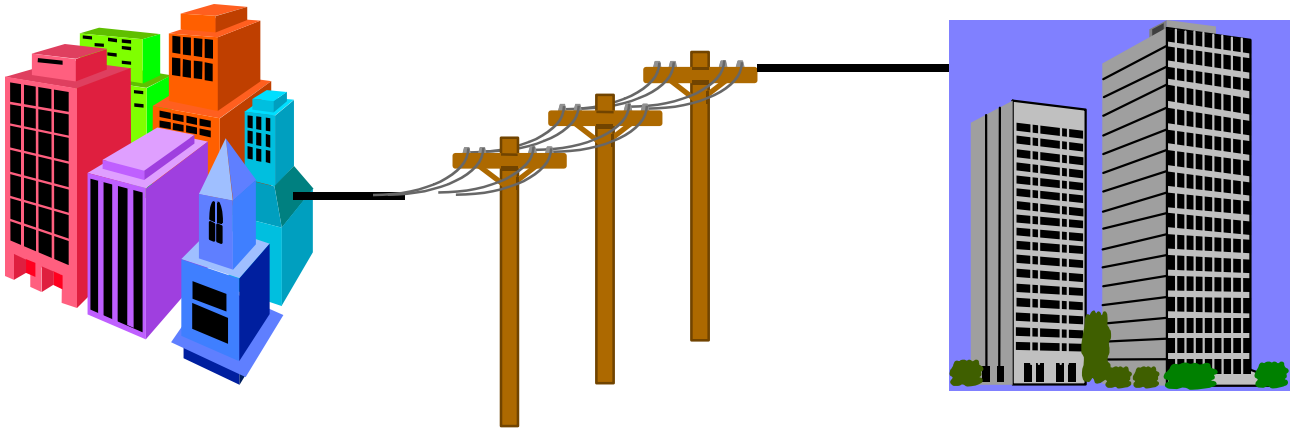
Raj Jain

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

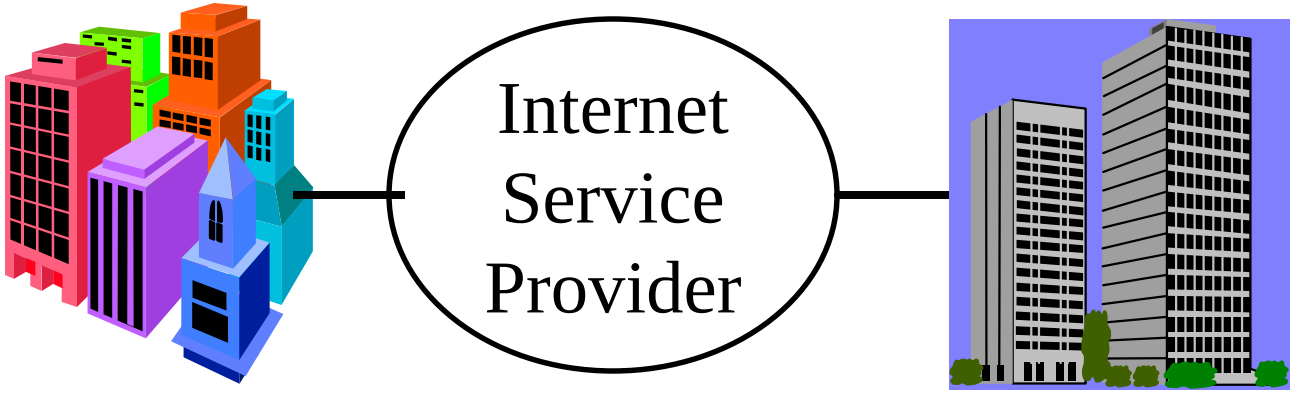
- Types of VPNs
- When and why VPN?
- VPN Design Issues
- Security Issues
- VPN Examples: PPTP, L2TP, IPSec
- Authentication Servers: RADIUS and DIAMETER
- VPNs using Multiprotocol Label Switching

What is a VPN?

- Private Network: Uses leased lines

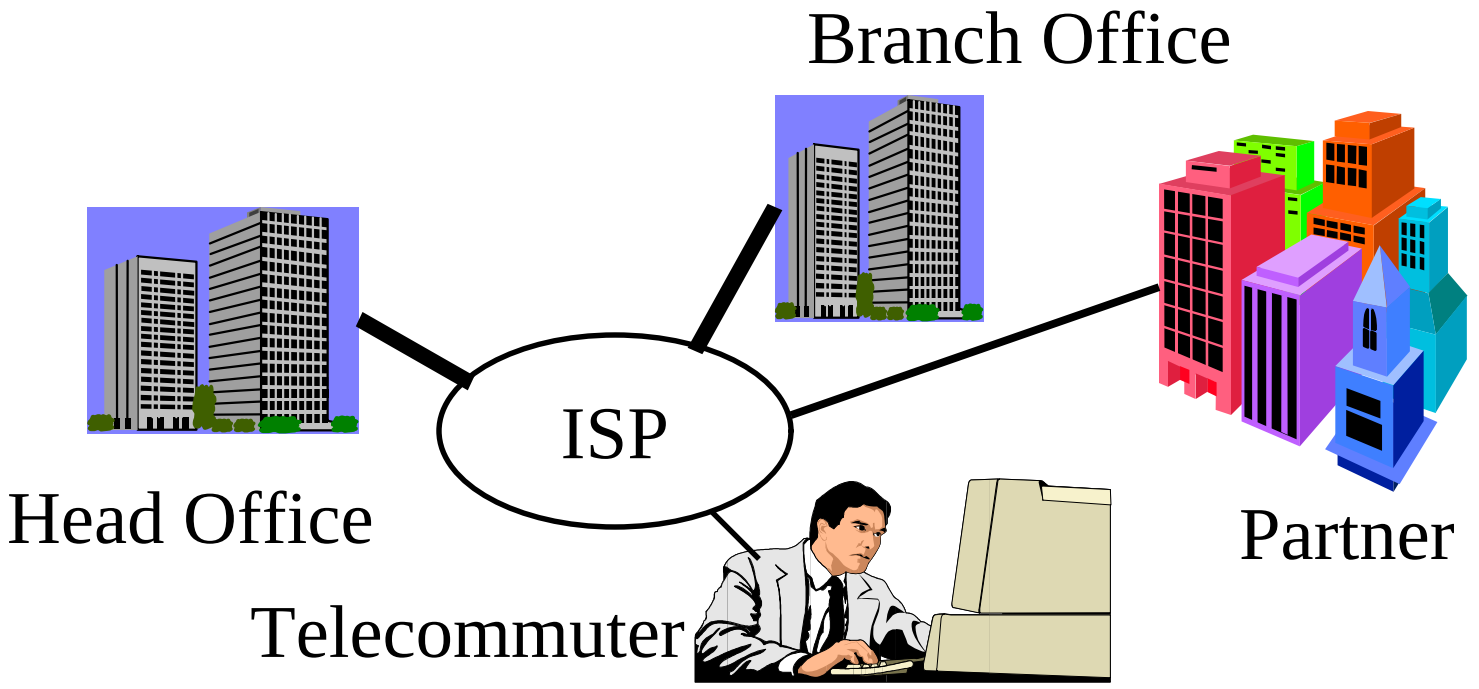


- *Virtual* Private Network: Uses public Internet



Types of VPNs

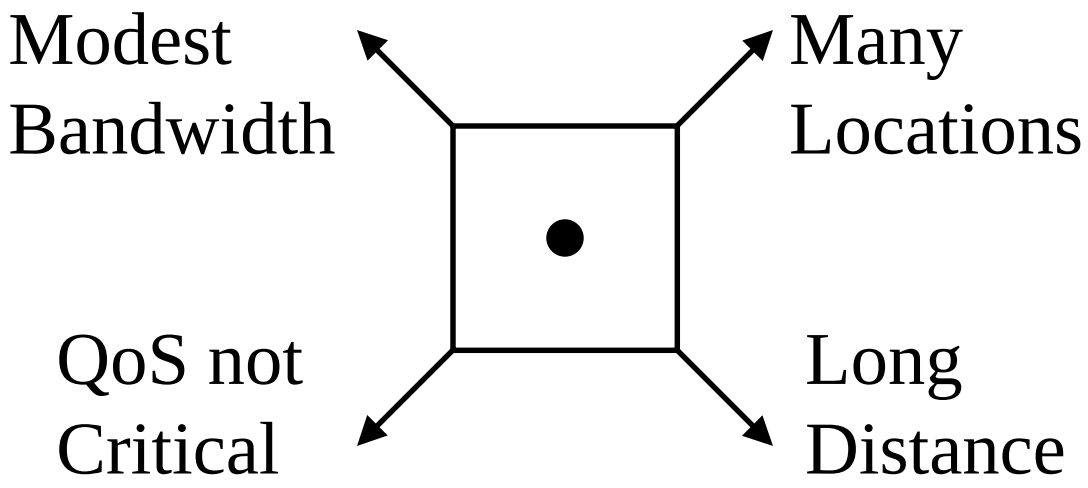
- WAN VPN: Branch offices
- Access VPN: Roaming Users
- Extranet VPNs: Suppliers and Customers



Why VPN?

- Reduced telecommunication costs
- Less administration ⇒ 60% savings (Forester Res.)
- Less expense for client and more income for ISPs
- Long distance calls replaced by local calls
- Increasing mobility ⇒ More remote access
- Increasing collaborations
  ⇒ Need networking links with partners

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)

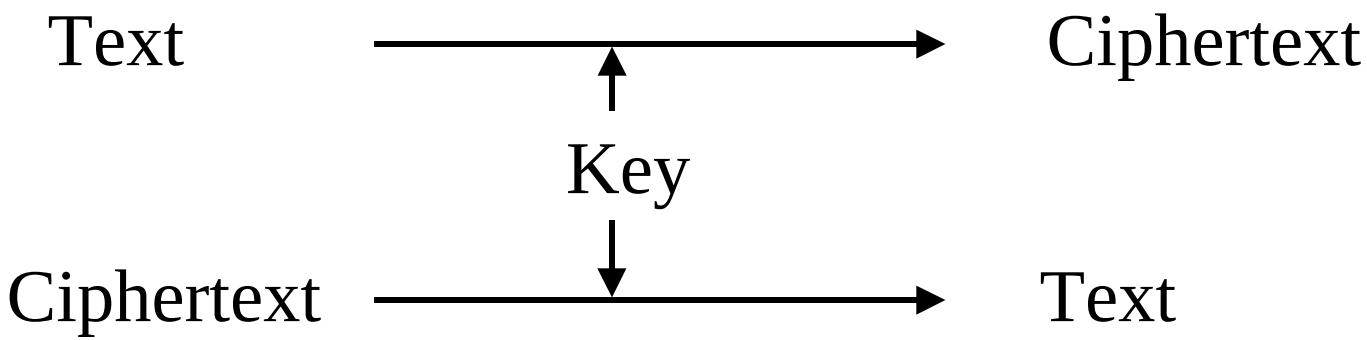
8. Compression: Reduces bandwidth requirements
9. Manageability: SNMP, Browser based, Java based, centralized/distributed
10. Accounting, Auditing, and Alarming
11. Protocol Support: IP, non-IP (IPX)
12. Platform and O/S support: Windows, UNIX, MacOS, HP/Sun/Intel
13. Installation: Changes to desktop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

Security 101

- Integrity: Received = sent?
- Availability: Legal users should be able to use.
  Ping continuously ⇒ No useful work gets done.
- Confidentiality and Privacy:
  No snooping or wiretapping
- Authentication: You are who you say you are.
  A student at Dartmouth posing as a professor canceled the exam.
- Authorization = Access Control
  Only authorized users get to the data

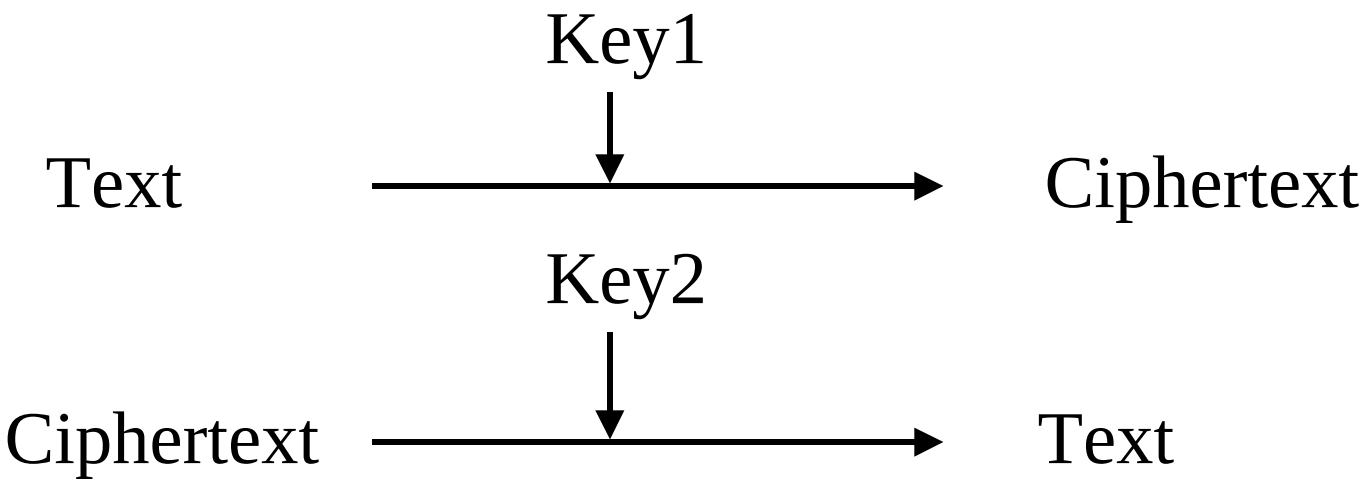
Secret Key Encryption

- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)



Public Key Encryption

- Invented in 1975 by Diffie and Hellman
- Encrypted_Message = Encrypt(Key1, Message)
- Message = Decrypt(Key2, Encrypted_Message)



Public Key Encryption

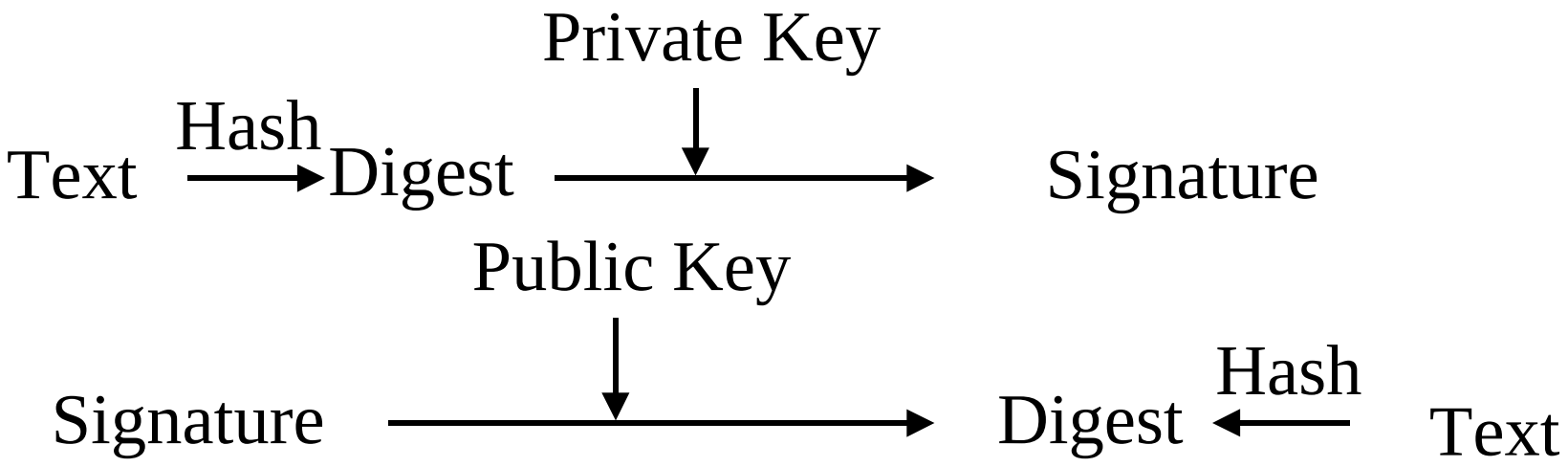
- RSA: Encrypted_Message = m^3 mod 187
- Message = Encrypted_Message^{107} mod 187
- Key1 = <3,187>, Key2 = <107,187>
- Message = 5
- Encrypted Message = $5^3 = 125$
- Message = 125^{107} mod 187
  $= 125^{(64+32+8+2+1)}$ mod 187
  $= \{(125^{64} \text{ mod } 187)(125^{32} \text{ mod } 187)...$
  $(125^2 \text{ mod } 187)(125)\} \text{ mod } 187 = 5$
- $125^4 \text{ mod } 187 = (125^2 \text{ mod } 187)^2 \text{ mod } 187$

Public Key (Cont)

- One key is private and the other is public
- Message = Decrypt(Public_Key, Encrypt(Private_Key, Message))
- Message = Decrypt(Private_Key, Encrypt(Public_Key, Message))

Digital Signature

- Message Digest = Hash(Message)
- Signature = Encrypt(Private_Key, Hash)
- Hash(Message) = Decrypt(Public_Key, Signature)
  ⇒ Authentic

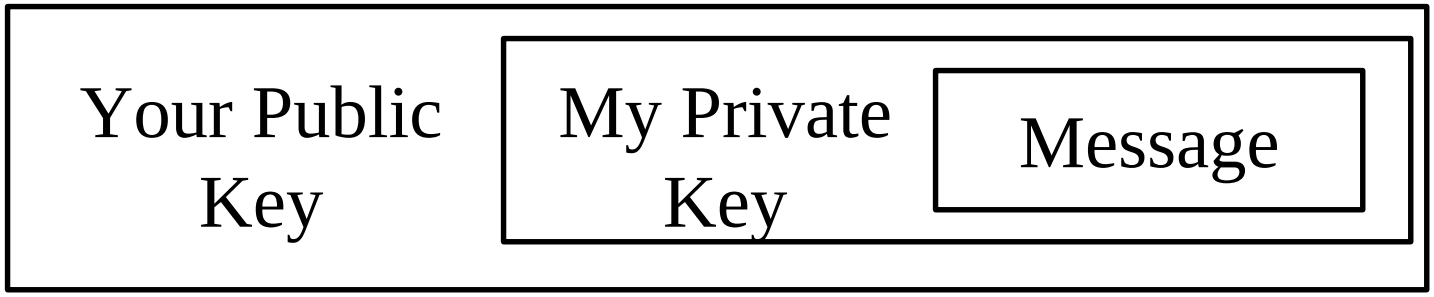


Certificate

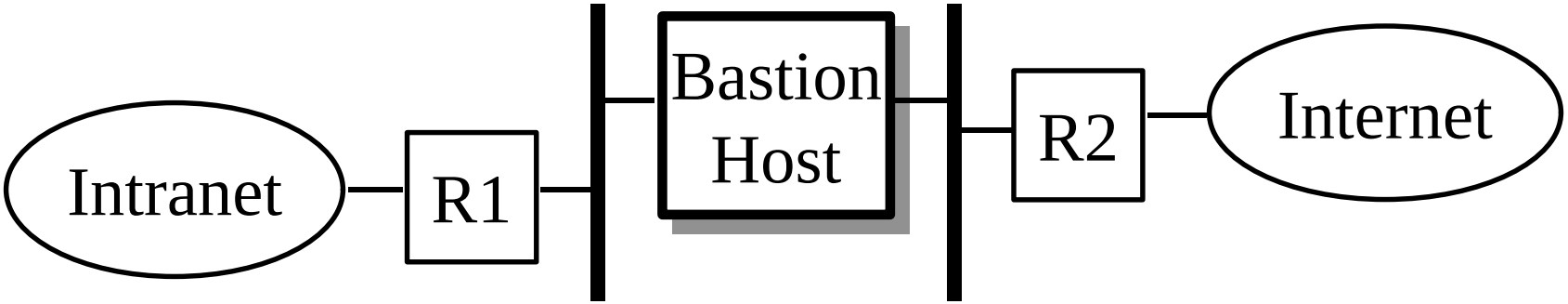
- Like driver license or passport
- Digitally signed by Certificate authority (CA) - a trusted organization
- Public keys are distributed with certificates
- CA uses its public key to sign the certificate
  $\Rightarrow$ Hierarchy of trusted authorities

Confidentiality

- User 1 to User 2:
- Encrypted_Message = Encrypt(Public_Key2, Encrypt(Private_Key1, Message))
- Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message)
  $\Rightarrow$ Authentic and Private

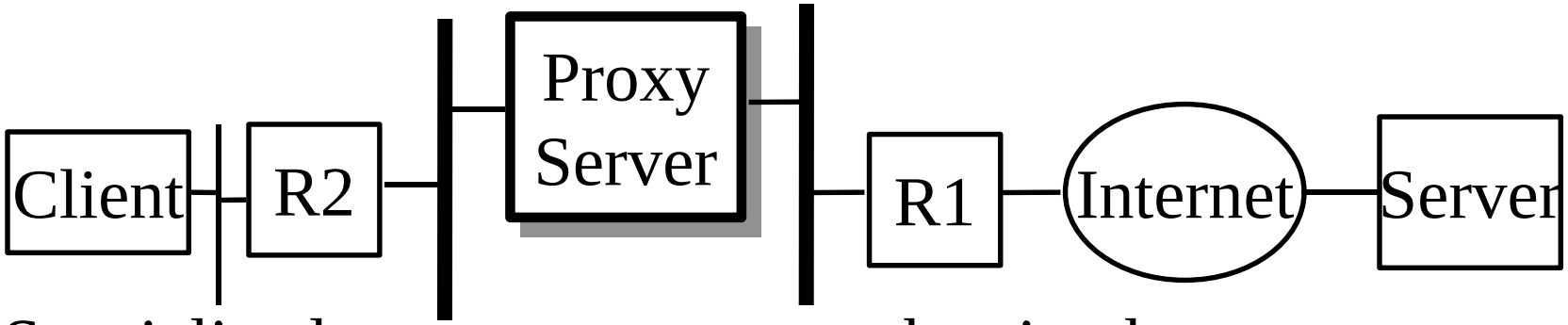


Firewall: Bastion Host



- Bastions overlook critical areas of defense, usually having stronger walls
- Inside users log on the Bastion Host and use outside services.
- Later they pull the results inside.
- One point of entry. Easier to manage security.

Proxy Servers



- Specialized server programs on bastion host
- Take user's request and forward them to real servers
- Take server's responses and forward them to users
- Enforce site security policy
  $\Rightarrow$ May refuse certain requests.
- Also known as application-level gateways
- With special "Proxy client" programs, proxy servers are almost transparent

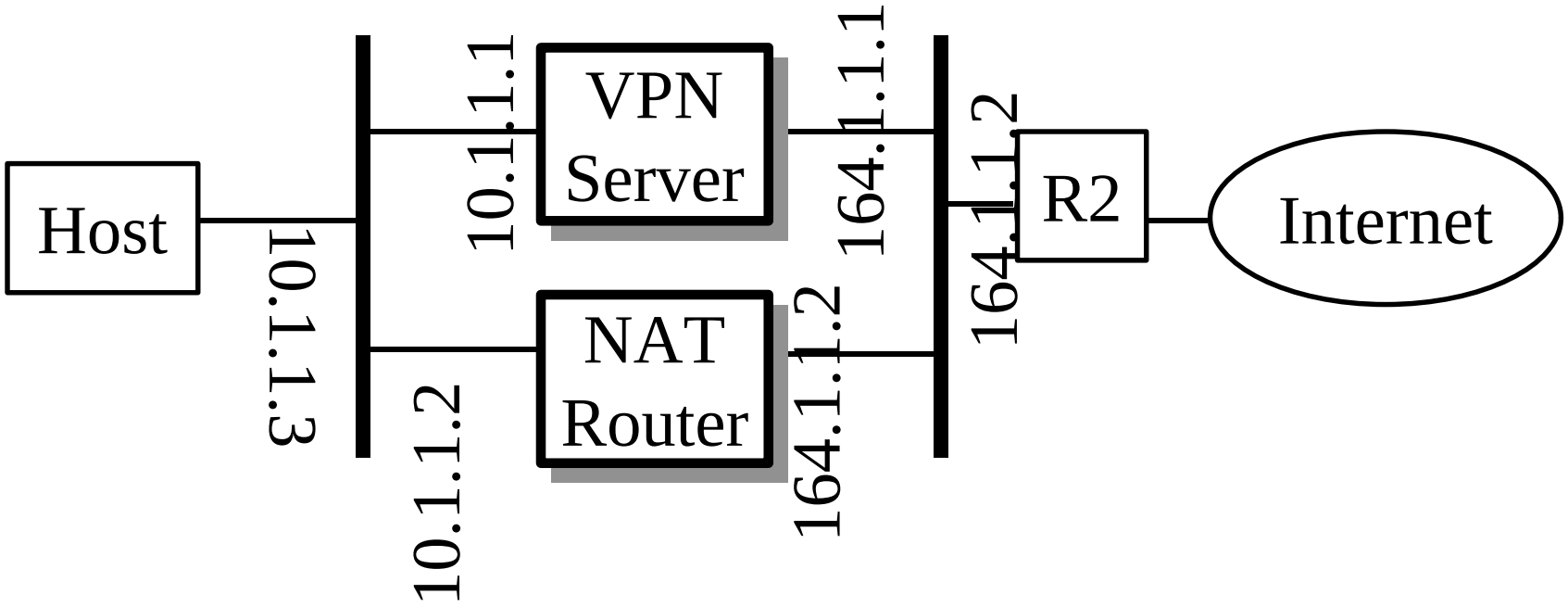
VPN Security Issues

- Authentication methods supported
- Encryption methods supported
- Key Management
- Data stream filtering for viruses, JAVA, active X
- Supported certificate authorities (X.509, Entrust, VeriSign)
- Encryption Layer: Datalink, network, session, application. Higher Layer $\Rightarrow$ More granular
- Granularity of Security: Departmental level, Application level, Role-based

Private Addresses

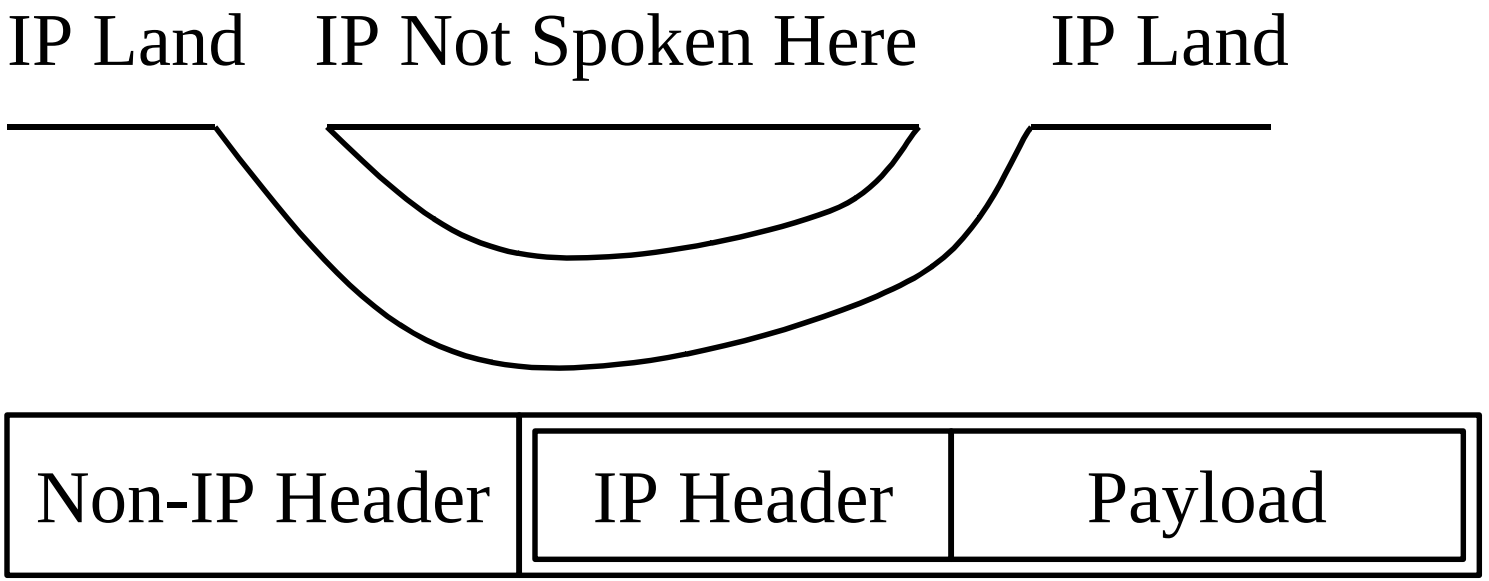
- 32-bit Address ⇒ 4 Billion addresses max
- Subnetting ⇒ Limit is much lower
- Shortage of IP address ⇒ Private addresses
- Frequent ISP changes ⇒ Private address
- Private ⇒ Not usable on public Internet
- RFC 1918 lists such addresses for private use
- Prefix = 10/8, 172.16/12, 192.168/16
- Example: 10.207.37.234

Address Translation



- NAT = Network Address Translation
  Like Dynamic Host Configuration Protocol (DHCP)
- IP Gateway: Like Firewall
- Tunneling: Encaptulation

Tunnel



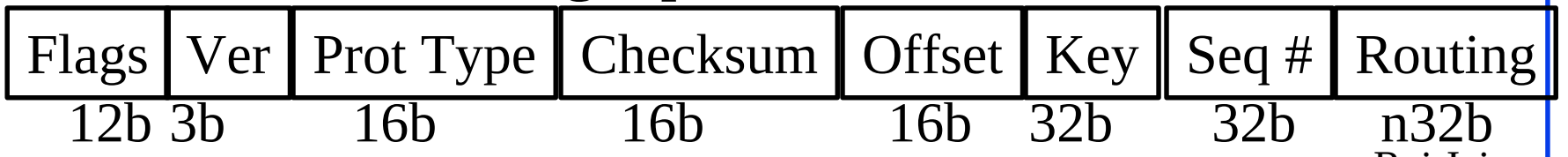
- Tunnel = Encaptulation
- Used whenever some feature is not supported in some part of the network, e.g., multicasting, mobile IP

VPN Tunneling Protocols

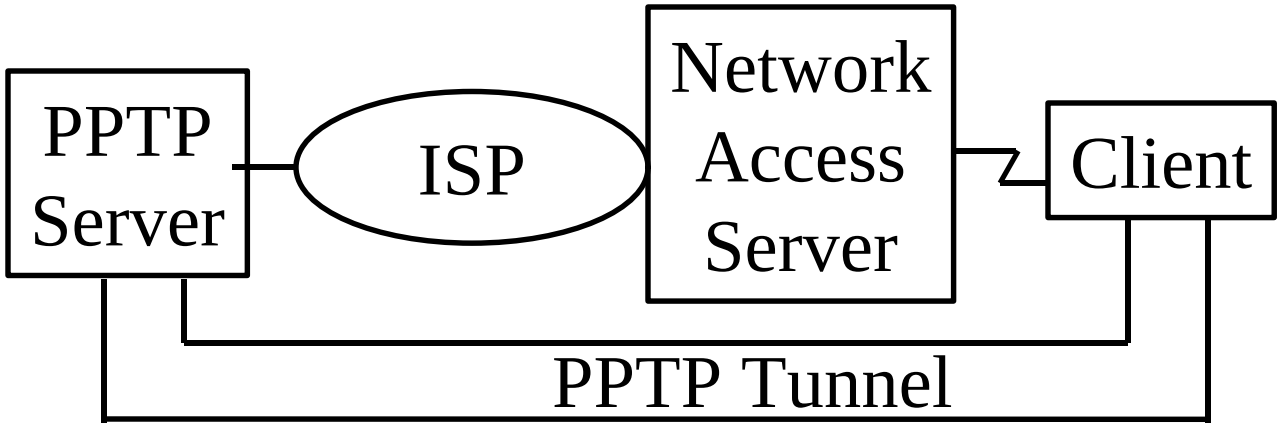
- GRE: Generic Routing Encaptulation (RFC 1701/2)
- PPTP: Point-to-point Tunneling Protocol
- L2F: Layer 2 forwarding
- L2TP: Layer 2 Tunneling protocol
- ATMP: Ascend Tunnel Management Protocol
- DLSW: Data Link Switching (SNA over IP)
- IPSec: Secure IP
- Mobile IP: For Mobile users

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

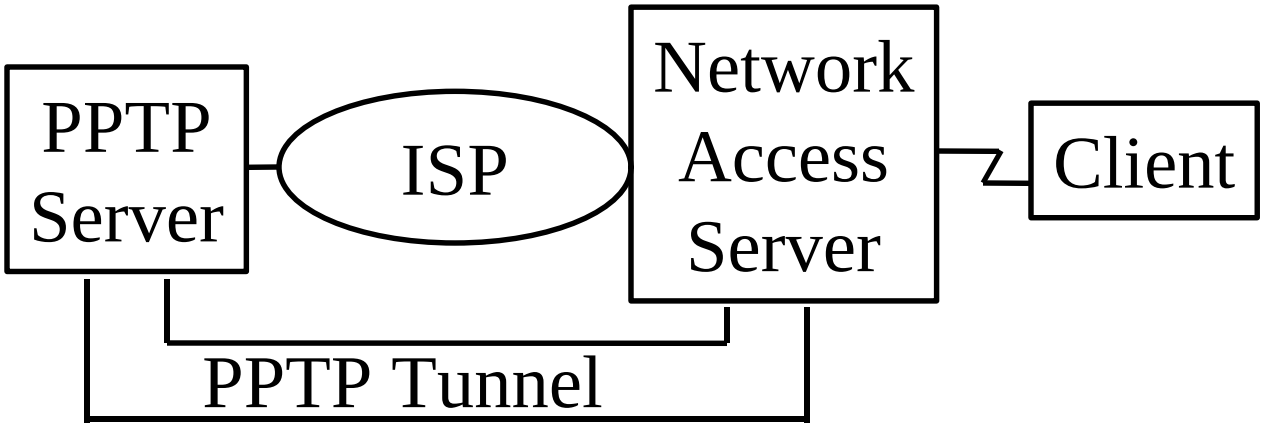


PPTP



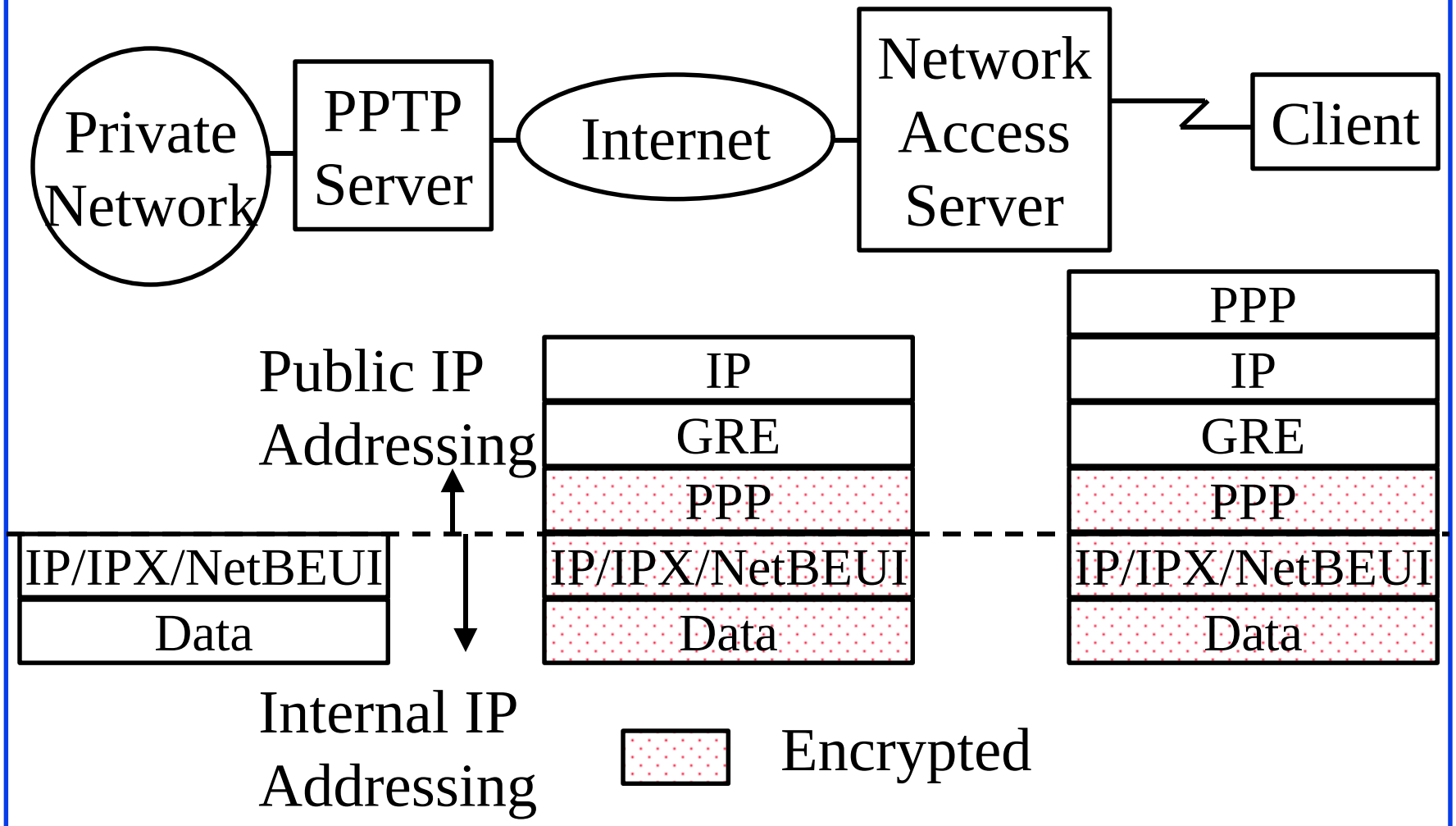
- PPTP = Point-to-point Tunneling Protocol
- Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics
- PPTP server for NT4 and clients for NT/95/98
- MAC, WFW, Win 3.1 clients from Network Telesystems (nts.com)

PPTP with ISP Support



- PPTP can be implemented at Client or at NAS
- With ISP Support: Also known as Compulsory Tunnel
- W/O ISP Support: Voluntary Tunnels

PPTP Packets

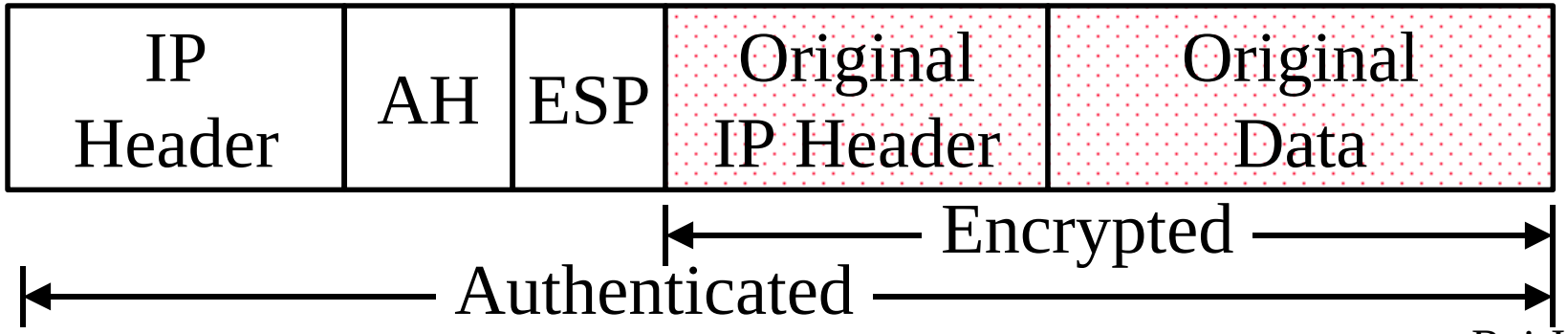


L2TP

- Layer 2 Tunneling Protocol
- L2F = Layer 2 Forwarding (From CISCO)
- L2TP = L2F + PPTP
  Combines the best features of L2F and PPTP
- Will be implemented in NT5
- 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

IPSec

- Secure IP: A series of proposals from IETF
- Separate Authentication and privacy
- Authentication Header (AH) ensures data integrity and authenticity
- Encapsulating Security Protocol (ESP) ensures privacy and integrity



IPSec (Cont)

- Two Modes: Tunnel mode, Transport mode
- Tunnel Mode ⇒ Encryption at IP level
- Supports a variety of encryption algorithms
- Better suited for WAN VPNs (vs Access VPNs)
- Little interest from Microsoft (vs L2TP)
- Most IPSec implementations support machine (vs user) certificates ⇒ Any user can use the tunnel
- Needs more time for standardization than L2TP

SOCKS

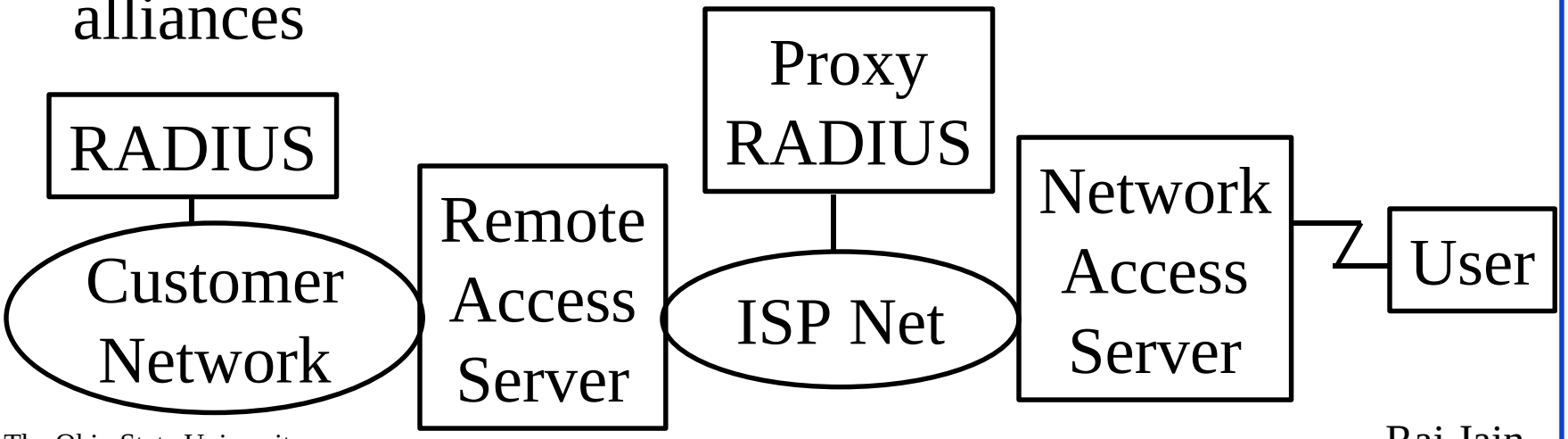
- Developed by David Koblas in 1990. Backed by NEC
- Made public and adopted by IETF Authenticated Firewall Traversal (AFT) working group
- Current version v5 in RFC 1928
- Session layer proxy
- Can be configured to proxy any number of TCP or UDP ports
- Provides authentication, integrity, privacy
- Can provide address translation
- Proxy $\Rightarrow$ Slower performance
- Desktop-to-Server $\Rightarrow$ Not suitable for extranets

Application Level Security

- Secure HTTP
- Secure MIME
- Secure Electronic Transaction (SET)
- Private Communications Technology (PCT)

RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ AAA server
- Network Access servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances



DIAMETER

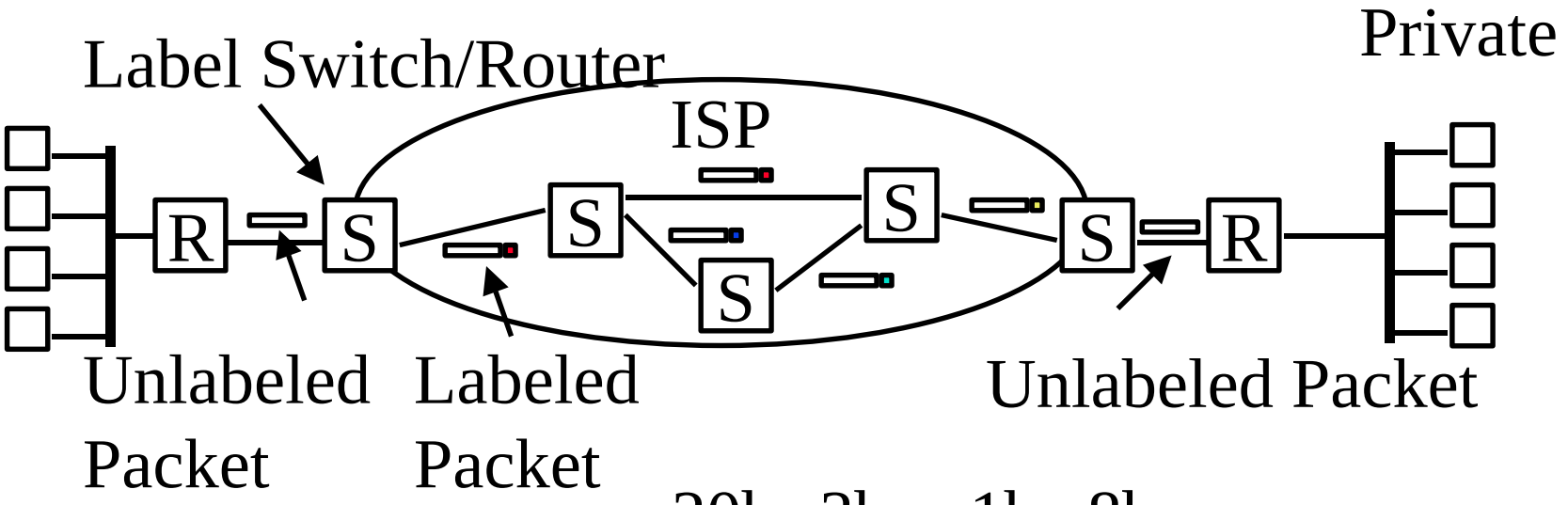
- Enhanced RADIUS
- Light weight
- Can use both UDP and TCP
- Servers can send unsolicited messages to Clients
  $\Rightarrow$ Increases the set of applications
- Support for vendor specific Attribute-Value-Pairs (AVPs) and commands
- Authentication and privacy for policy messages

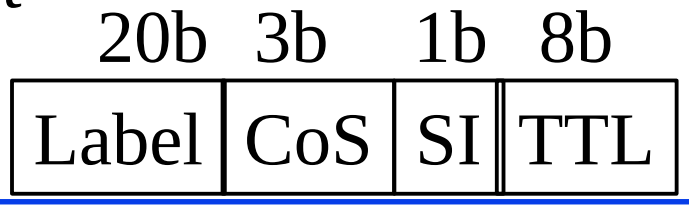
Quality of Service (QoS)

- Resource Reservation Protocol (RSVP) allows clients to reserve bandwidth
- Need routers with proper scheduling: IP Precedence, priority queueing, Weighted Fair Queueing (WFQ)
- All routers may not support RSVP
- Even more difficult if multiple ISPs

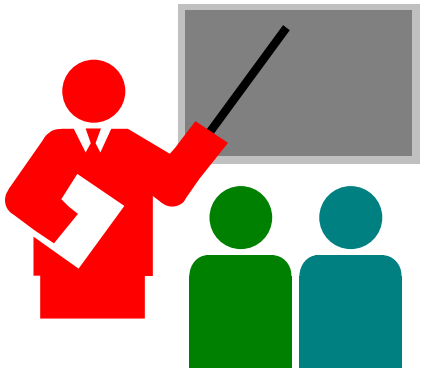
VPN Support with MPLS

- Multiprotocol Label Switching
- Allows packets to be switched using labels (tags)
  ⇒ Creates connections across a network
- Labels contain Class of Service





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), Layer 5 (SOCKS), Layer 7 (Application level) VPNs
- RADIUS allows centralized authentication server
- QoS is still an issue ⇒ MPLS

References

- For a detailed list of references, see http://www.cis.ohio-state.edu/~jain/refs/refs_vpn.htm

Acronyms

- AAA Authorization, Accounting, and Auditing
- AFT Automatic Firewall Traversal
- AH Authentication Header
- ATMP Ascend Tunnel Management Protocol
- AVP Attribute-Value-Pair
- CA Certification Authority
- CAST Carlisle Adams and Stafford Tavares
- CBC Cipher Block Chaining
- CERT Computer Emergency Response Team
- CFB Cipher feedback

- CHAP Challenge Handshake Authentication Protocol
- CRC Cyclic Redundancy Check
- DES Data Encryption Standard
- DHCP Dynamic Host Configuration Protocol
- DLSW Data Link Switching (SNA over IP)
- DMZ Demilitarized Zone
- DNS Domain Name Service
- DSA Digital Signature Authorization
- DTS Digital Timestamp Service
- EAP Extensible Authentication Protocol

- ECB Electronic code blocks
- ESP Encapsulating Security Protocol
- GRE Generic Routing Encaptulation
- HTTP Hypertext Transfer Protocol
- IDEA International Data Encryption Standard
- IETF Internet Engineering Task Force
- IKE Internet Key Exchange
- IMPs Interface Message Processor
- IPSec Internet Protocol Security
- IPX Netware IP

- IPv4 IP version 4
- ISAKMP Association Key Management Protocol
- ISP Internet Service Provider
- IVPN IP VPN
- JAVA Just Another Vague Acronym
- KMI Key Management Infrastructure
- L2F Layer 2 Forwarding Protocol
- L2TP Layer 2 Tunneling protocol
- LDAP Lightweight Directory Protocol
- MAC Message Authentication Code

- MD2 Message Digest 2
- MD4 Message Digest 4
- MD5 Message Digest 5
- MPLS Multiprotocol Label Switching
- MPPE Microsoft Point to Point Encryption
- MS-CHAP Microsoft CHAP
- NAS Network Access Server
- NAT Network Address Translation
- NBS National Bureau of Standards
- NDS Netware Directory Service

- NIST National Institute of Science and Technology
- NSA National Security Agency
- NT5 Windows NT 5.0
- OFB Output feedback
- OTP One-Time Password
- PAP Password Authentication Protocol
- PIX Private Internet Exchange
- PKI Public key infrastructure
- PPP Point-to-Point protocol
- PPTP Point-to-point Tunneling Protocol

- RADIUS Remote Authentication Dial-in User Service
- RAS Remote Access Services
- RC2 Ron's Code 2
- RC4 Ron's Code 4
- RC5 Ron's Code 5
- RFC Request for Comment
- RSVP Resource Reservation Protocol
- S/WAN Secure Wide Area Network
- SHA Secure Hash Algorithm
- SKIP Simple Key Exchange Internet Protocol

- SNA System Network Architecture
- SNMP Simple Network Management Protocol
- TACACS Terminal Access Controller Access System
- TCP Transport Control Protocol
- TLS Transport Level Security
- UDP User Datagram Protocol
- VPDN Virtual Private Data Network
- VPN Virtual Private Networks
- WAN Wide Area Network
- WFQ Weighted Fair Queueing

- WFW Windows for Workgroup
- WRED Weighted Random Early Drop
- XTACACS Extended TACACS