

---

# Virtual Private Networks

Raj Jain

The Ohio State University

Columbus, OH 43210

Jain@CIS.Ohio-State.Edu

<http://www.cis.ohio-state.edu/~jain/>

Raj .



Types of VPNs

When and why VPN?

VPN Design Issues

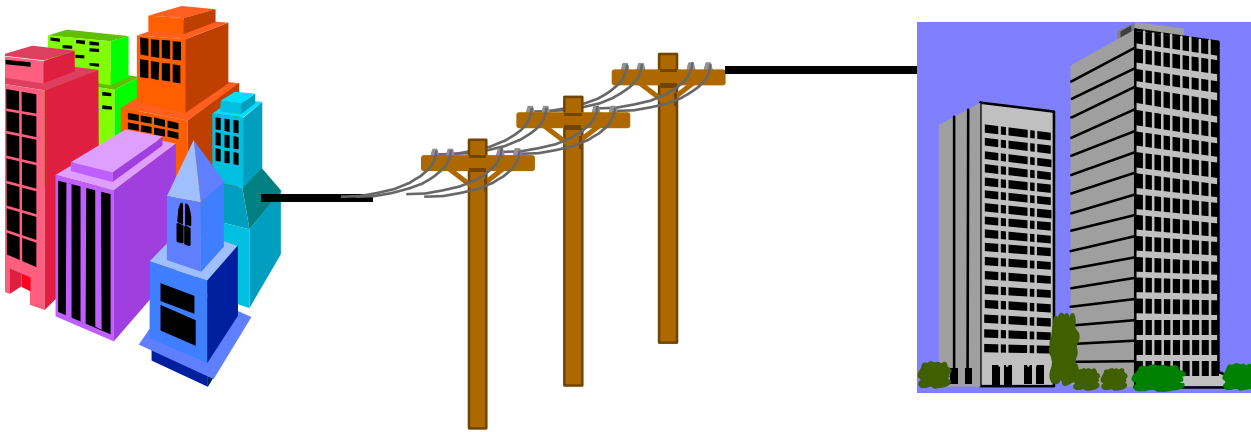
Security Issues

VPN Examples: PPTP, L2TP, IPSec

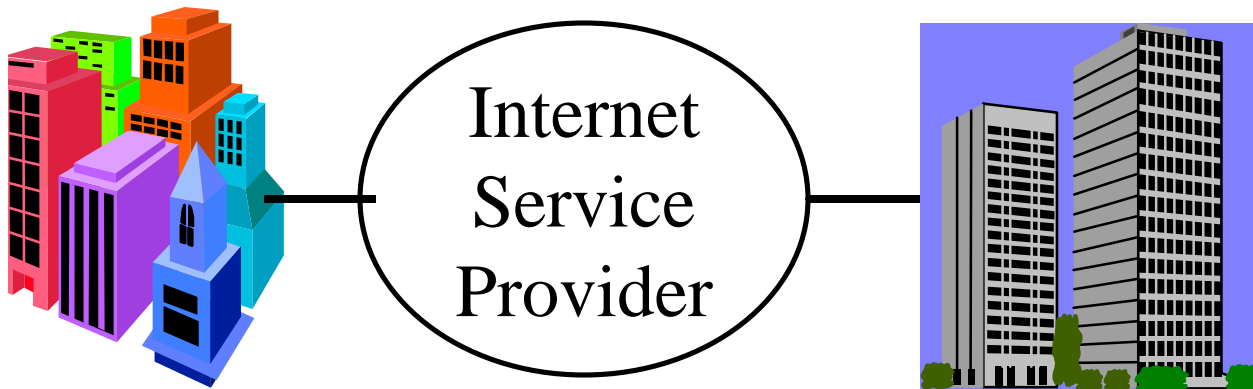
---

# What is a VPN?

Private Network: Uses leased lines



*Virtual* Private Network: Uses public Internet



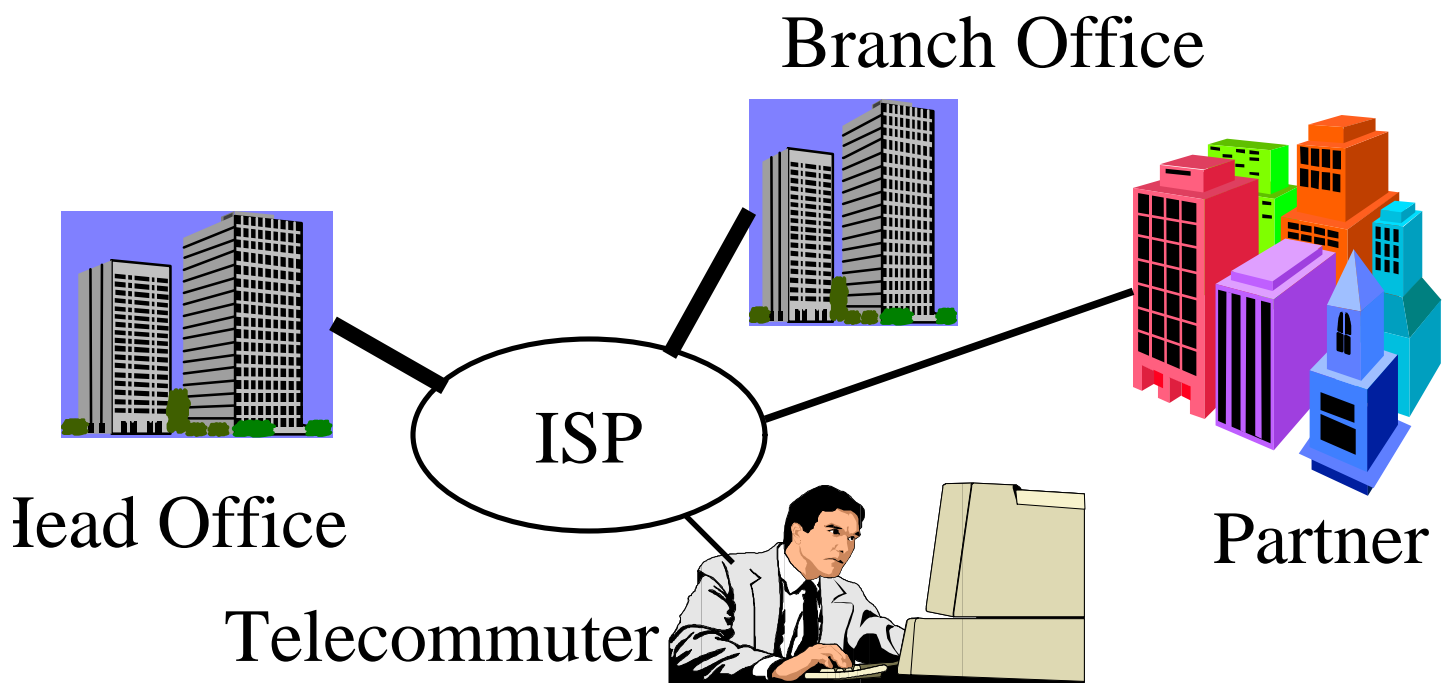
---

# Types of VPNs

WAN VPN: Branch offices

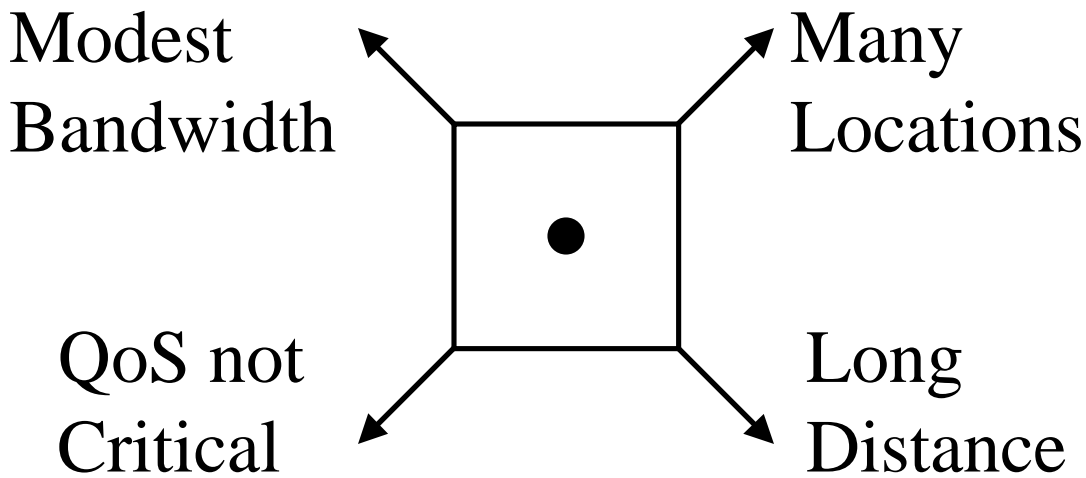
Access VPN: Roaming Users

Extranet VPNs: Suppliers and Customers



---

# 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

Security

Address Translation

Performance: Throughput, Load balancing (round-robin DNS), fragmentation

Bandwidth Management: RSVP

Availability: Good performance at all times

Scalability: Number of locations/Users

Interoperability: Among vendors, ISPs, customers (Intranets/extranets) ⇒ Standards Compatibility, With firewall

---

## Design Issues (Cont)

Compression: Reduces bandwidth requirements

Manageability: SNMP, Browser based, Java based, centralized/distributed

Accounting, Auditing, and Alarming

Protocol Support: IP, non-IP (IPX)

Platform and O/S support: Windows, UNIX, MacOS, HP/Sun/Intel

Installation: Changes to desktop or backbone only

Legal: Exportability, Foreign Govt Restrictions, Key Management Infrastructure (KMI) initiative  
⇒ Need key recovery

---

# Security 101

Integrity: Received = sent?

Availability: Legal users should be able to use.

Downing continuously  $\Rightarrow$  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 cancel the exam.

Authorization = Access Control

Only authorized users get to the data

---

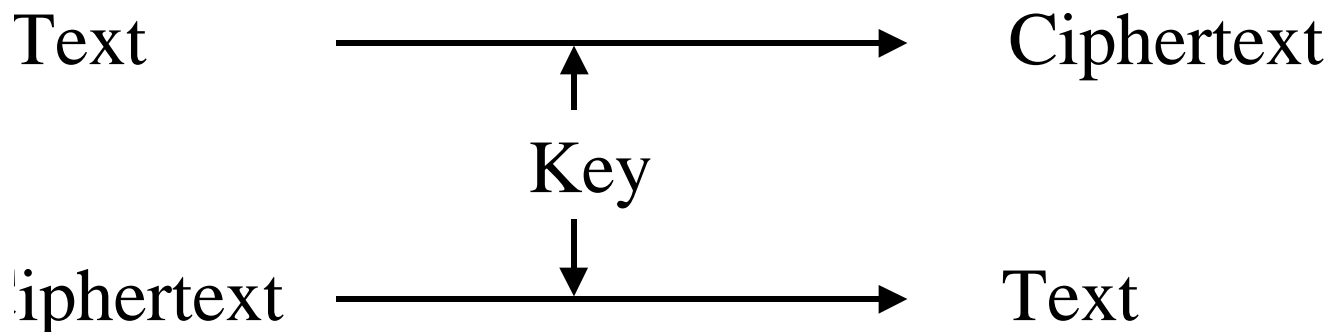
# Secret Key Encryption

Encrypted\_Message = Encrypt(Key, Message)

Message = Decrypt(Key, Encrypted\_Message)

Example: Encrypt = division

133 = 48 R 1 (using divisor of 9)



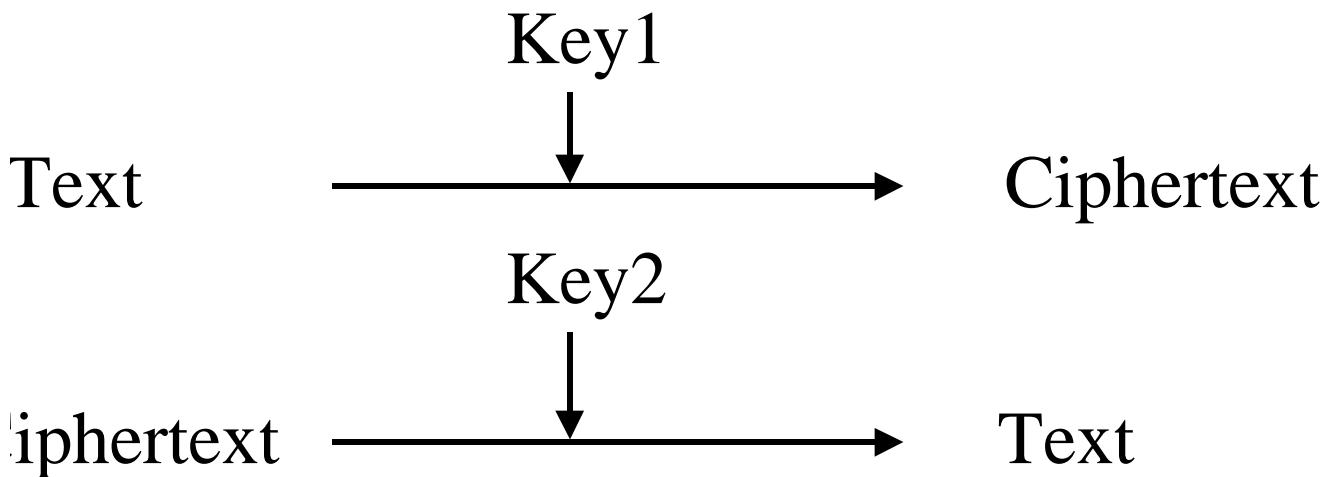
---

# Public Key Encryption

Invented in 1975 by Diffie and Hellman

$\text{Encrypted\_Message} = \text{Encrypt}(\text{Key1}, \text{Message})$

$\text{Message} = \text{Decrypt}(\text{Key2}, \text{Encrypted\_Message})$



---

# Public Key Encryption

RSA: Encrypted\_Message =  $m^3 \pmod{187}$

Message = Encrypted\_Message<sup>107</sup> mod 187

Key1 = <3,187>, Key2 = <107,187>

Message = 5

Encrypted Message =  $5^3 = 125$

Message =  $125^{107} \pmod{187}$

=  $125^{(64+32+8+2+1)} \pmod{187}$

=  $\{(125^{64} \pmod{187})(125^{32} \pmod{187})\dots$

$(125^2 \pmod{187})(125)\} \pmod{187} = 5$

$(125^4 \pmod{187} = (125^2 \pmod{187})^2 \pmod{187}$

---

## 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))

---

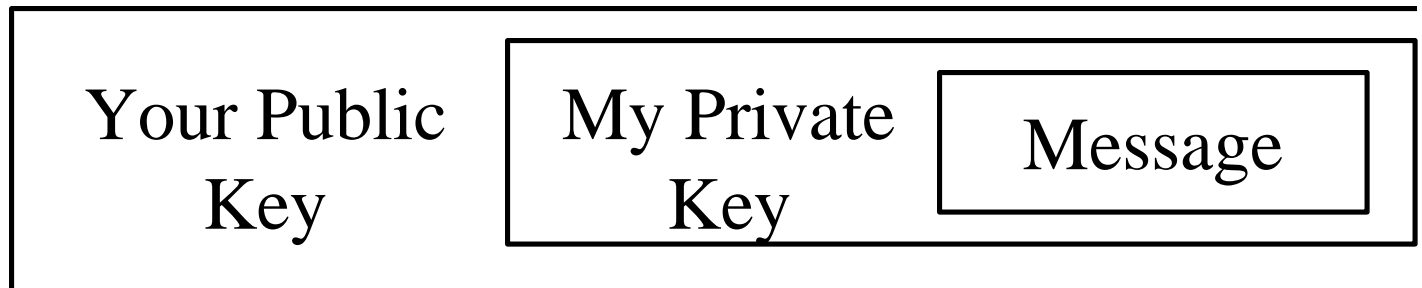
# Confidentiality

User 1 to User 2:

Encrypted\_Message = Encrypt(Public\_Key2,  
Encrypt(Private\_Key1, Message))

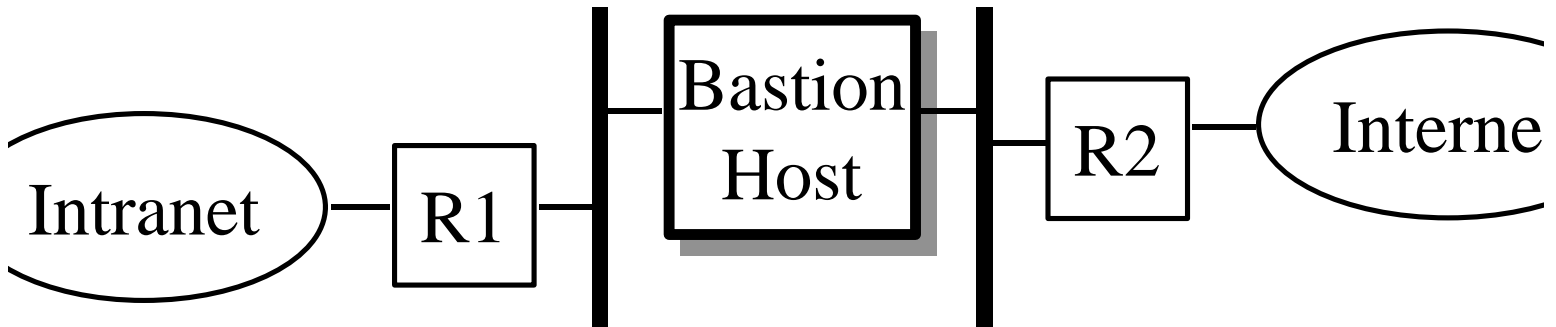
Message = Decrypt(Public\_Key1,  
Decrypt(Private\_Key2, Encrypted\_Message))

⇒ Authentic and Private



---

# Firewall: Bastion Host



Bastions overlook critical areas of defense, usually having stronger walls

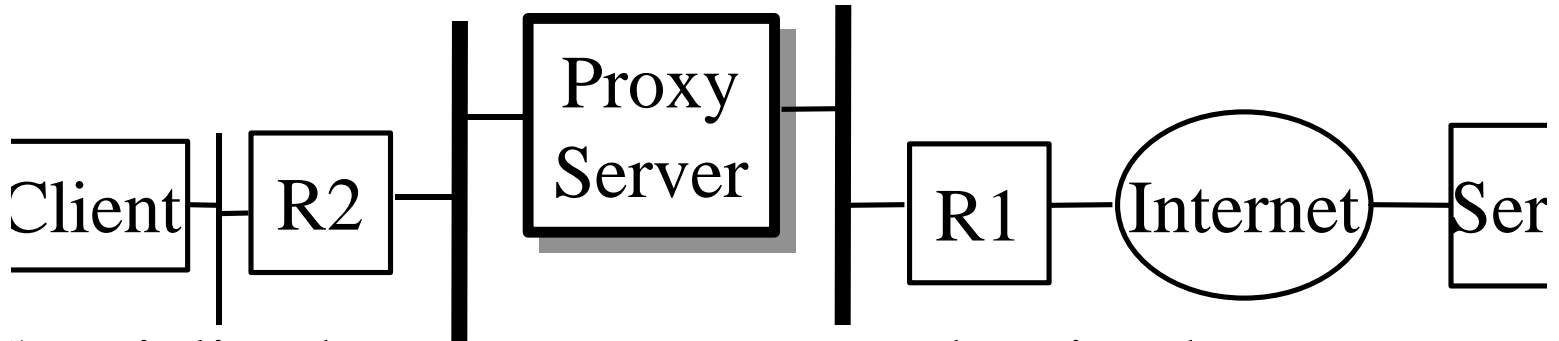
inside users log on the Bastion Host and use outside services.

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

⇒ 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  $\Rightarrow$  4 Billion addresses max

Subnetting  $\Rightarrow$  Limit is much lower

Shortage of IP address  $\Rightarrow$  Private addresses

Frequent ISP changes  $\Rightarrow$  Private address

Private  $\Rightarrow$  Not usable on public Internet

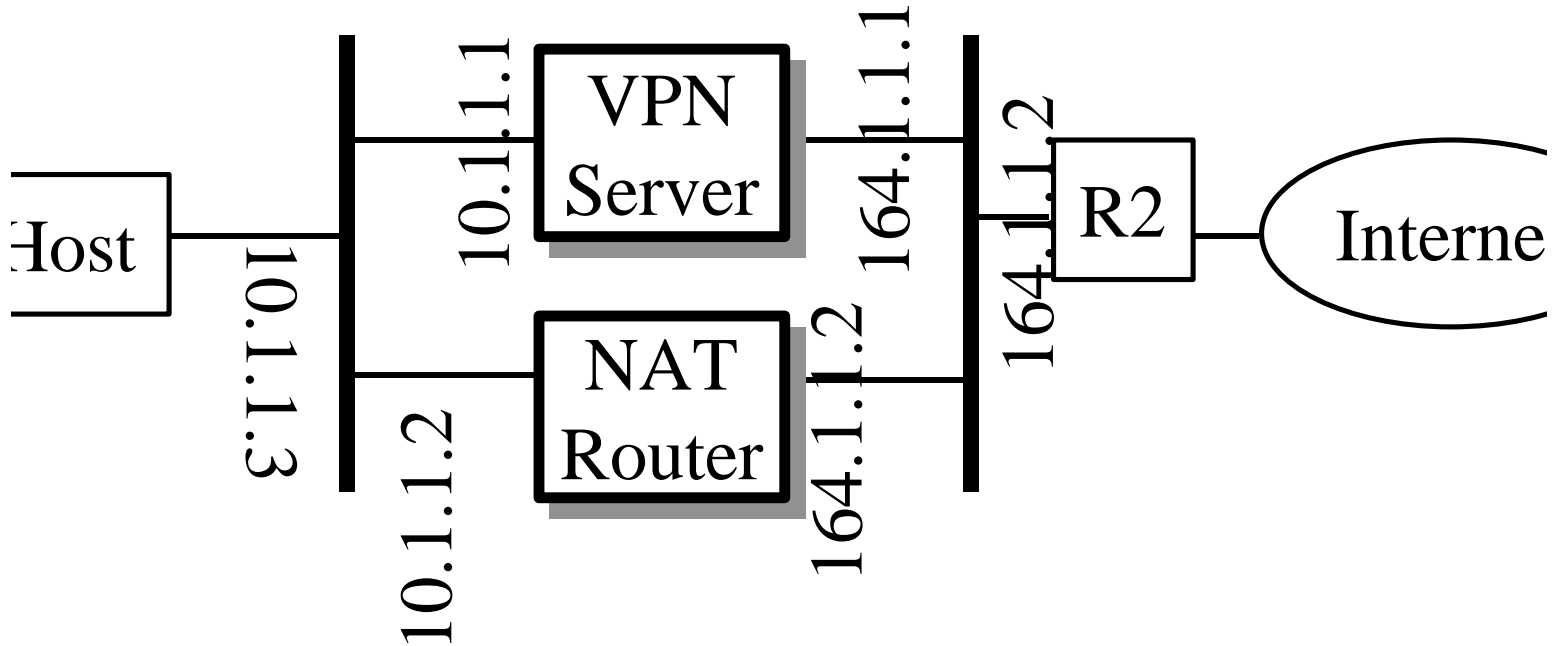
RFC 1918 lists such addresses for private use

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)

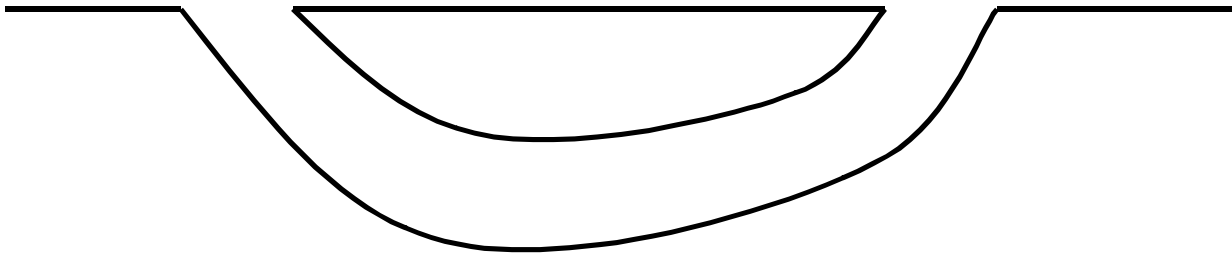
VPN Gateway: Like Firewall

Tunneling: Encapsulation

---

# Tunnel

P Land    IP Not Spoken Here    IP Land



Tunnel = Encapsulation

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

Raj .

---

# VPN Tunneling Protocols

GRE: Generic Routing Encapsulation (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

Delivery Header	GRE Header	Payload
-----------------	------------	---------

Generic Routing Encapsulation (RFC 1701/1702)

Generic  $\Rightarrow$  X over Y for any X or Y

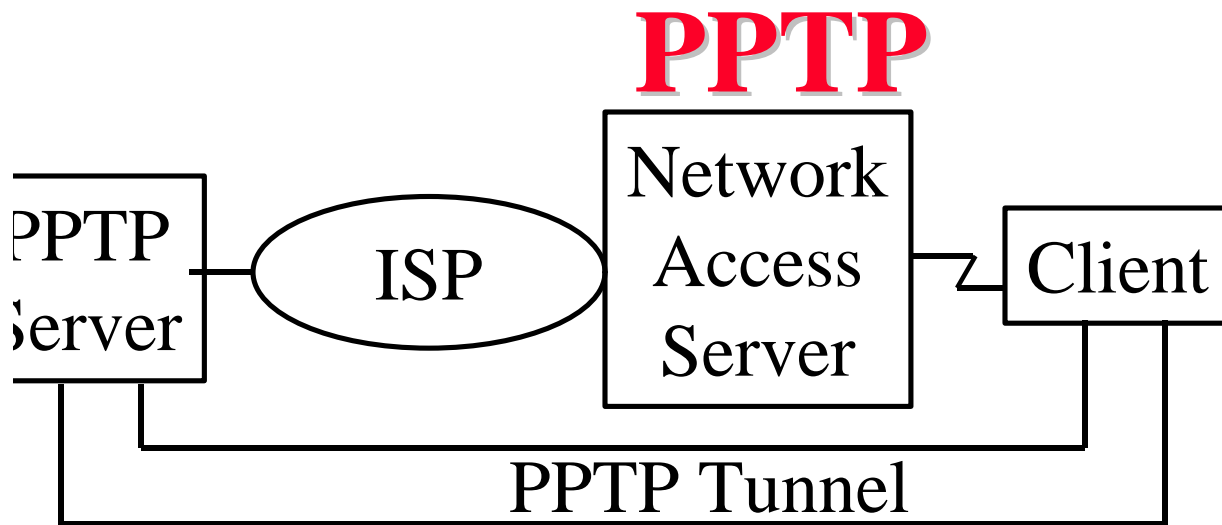
Optional Checksum, Loose/strict Source Routing, Key

Key is used to authenticate the source

Over IPv4, GRE packets use a protocol type of 47

Allows router visibility into application-level headers

Restricted to a single provider network  $\Rightarrow$  end-to-end



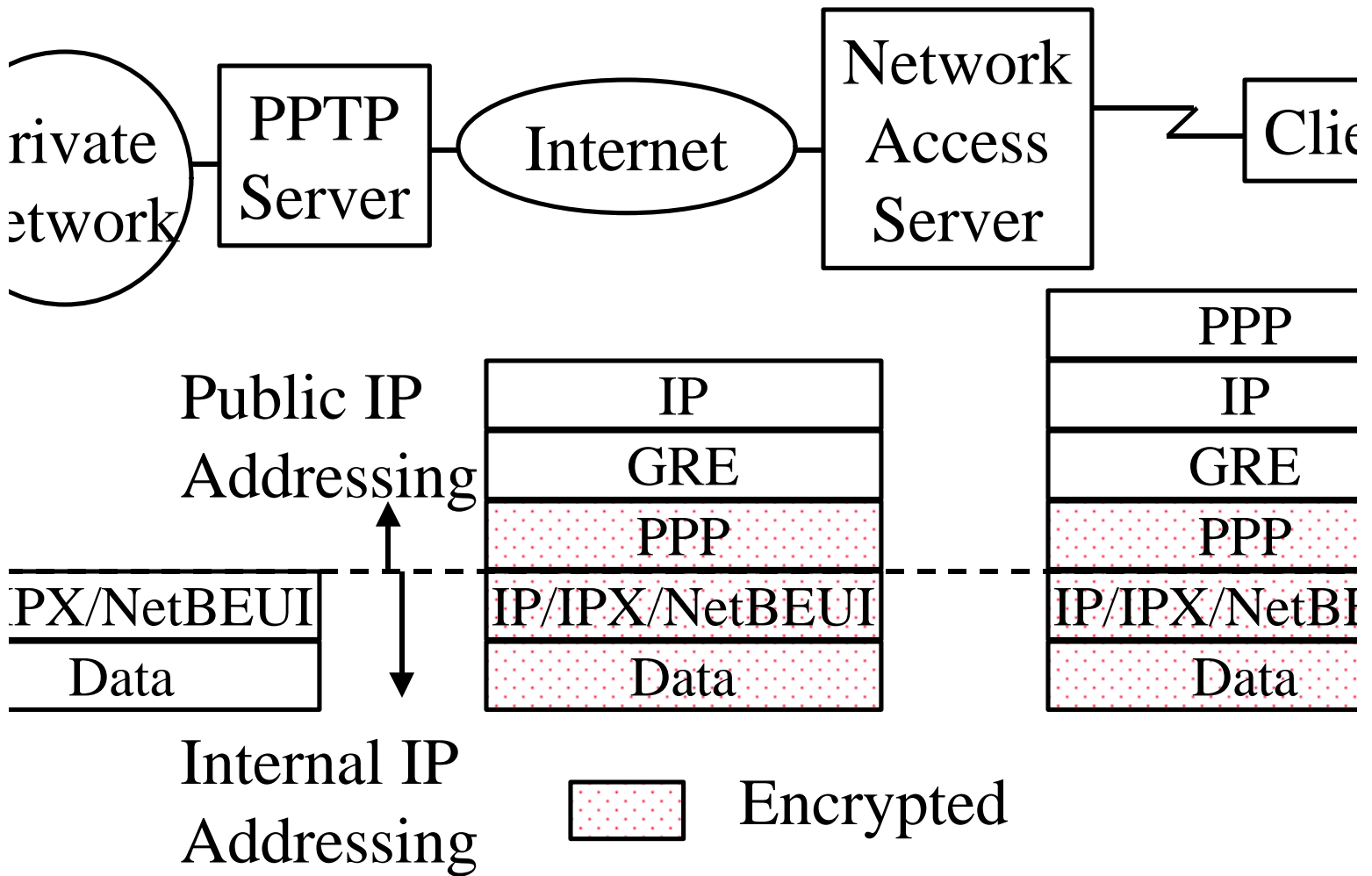
• PPTP = Point-to-point Tunneling Protocol

Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics

• PPTP server for NT4 and clients for NT/95/98

• MAC, WFW, Win 3.1 clients from Network Telesystems (nts.com)

# 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

---

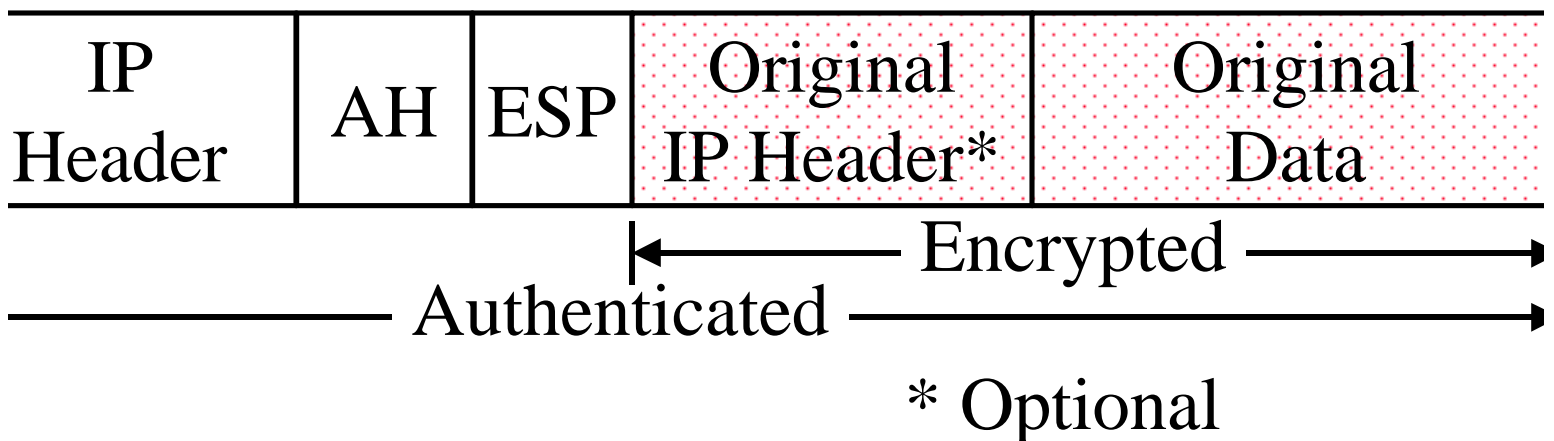
# IPSec

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



Raj .

---

## IPSec (Cont)

Two Modes: Tunnel mode, Transport mode

Tunnel Mode  $\Rightarrow$  Original IP header encrypted

Transport mode  $\Rightarrow$  Original IP header removed.

Only transport data encrypted.

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  $\Rightarrow$  Any user can use the tunnel

Needs more time for standardization than L2TP

---

# Application Level Security

Secure HTTP

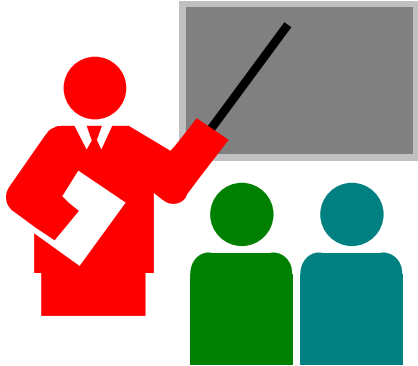
Secure MIME

Secure Electronic Transaction (SET)

Private Communications Technology (PCT)

---

# 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

QoS is still an issue  $\Rightarrow$  MPLS

---

# References

For a detailed list of references, see

[http://www.cis.ohio-state.edu/~jain/refs/refs\\_vpn.htm](http://www.cis.ohio-state.edu/~jain/refs/refs_vpn.htm)