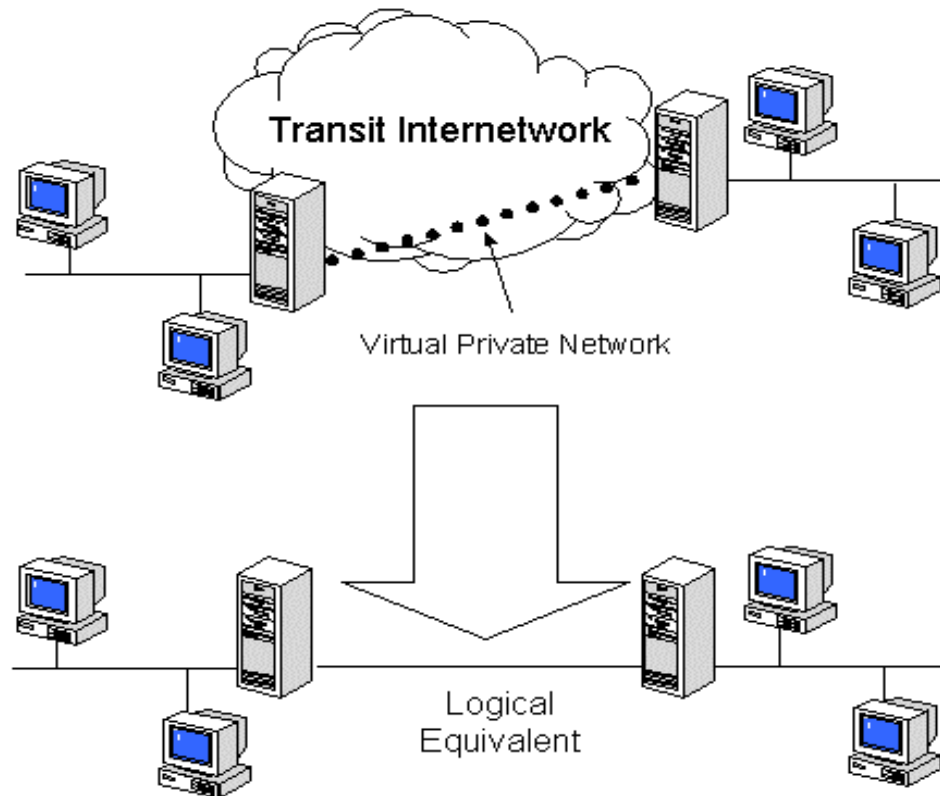


Virtual Private Networks



Public and Private Networks

- What is a Public Network?

- Examples:

- ⊗ Internet

- ⊗ PSTN

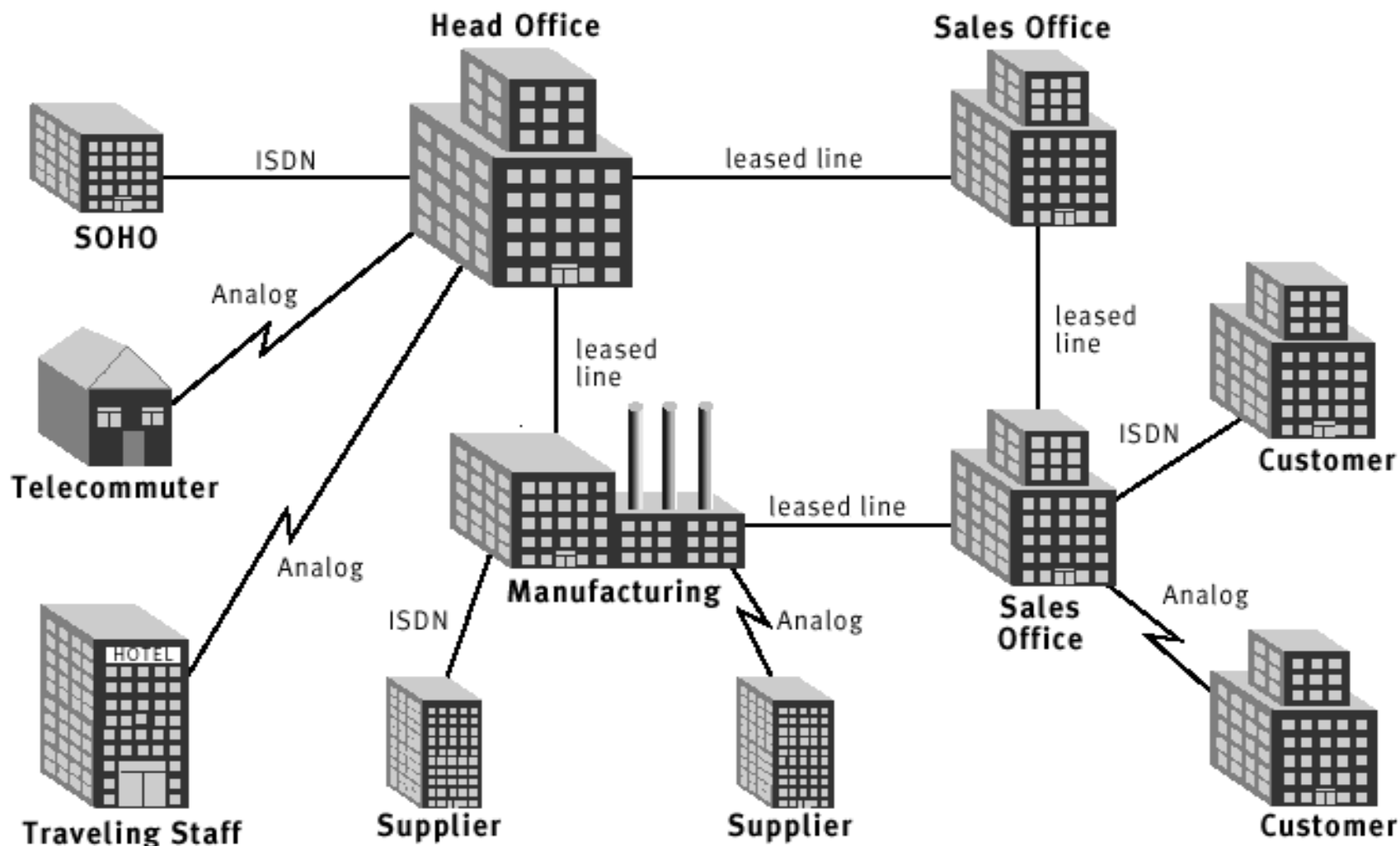
- What is a Private Network?

- Examples:

- ⊗ LANs

- ⊗ Intranet

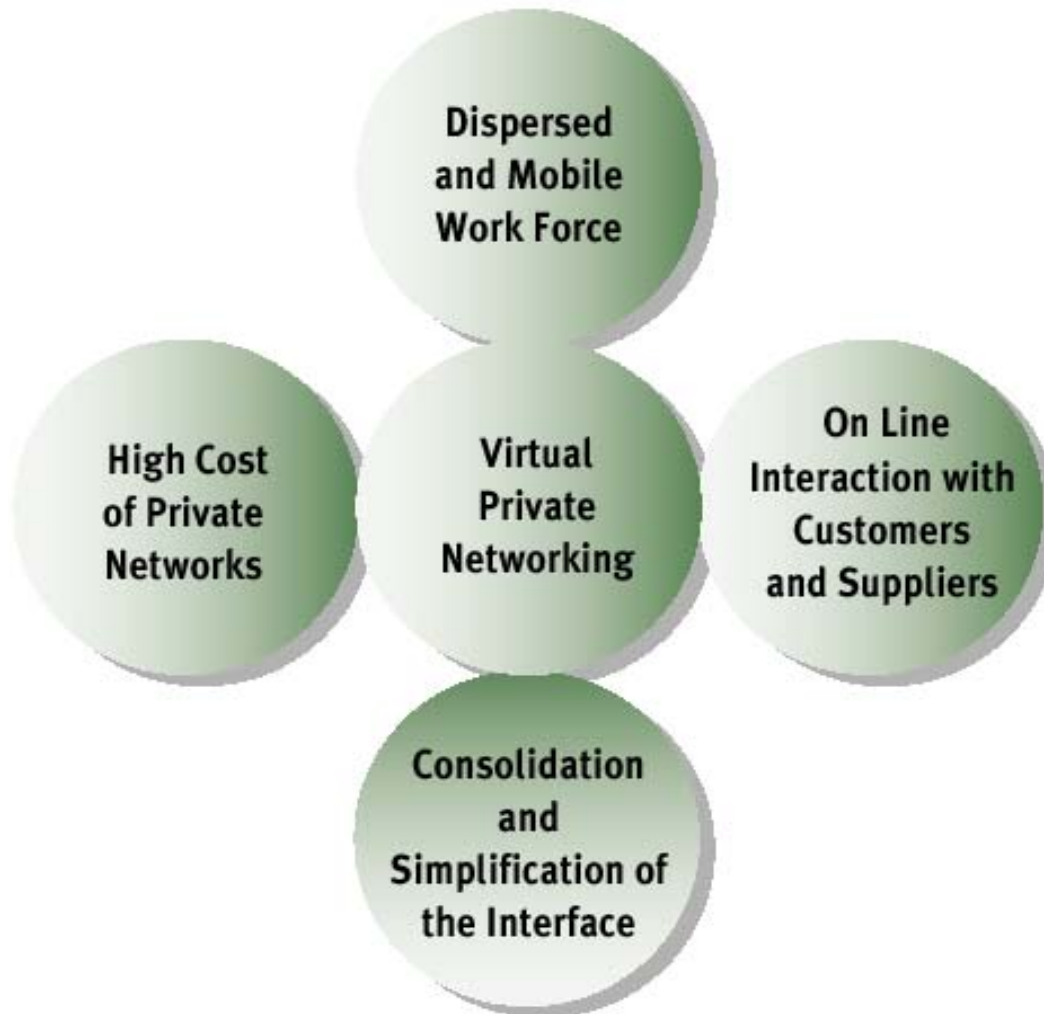
Dedicated Connectivity Solutions Now



The Realities

- 1. Cost of dedicated private WAN connectivity is very high
 - ⊗ Multitude of connectivity options
 - ⊗ Disparate hardware/software
- 2. Internet is the ubiquitous network
 - ⊗ Internet connectivity is cheap
 - ⊗ But Internet is a Public network

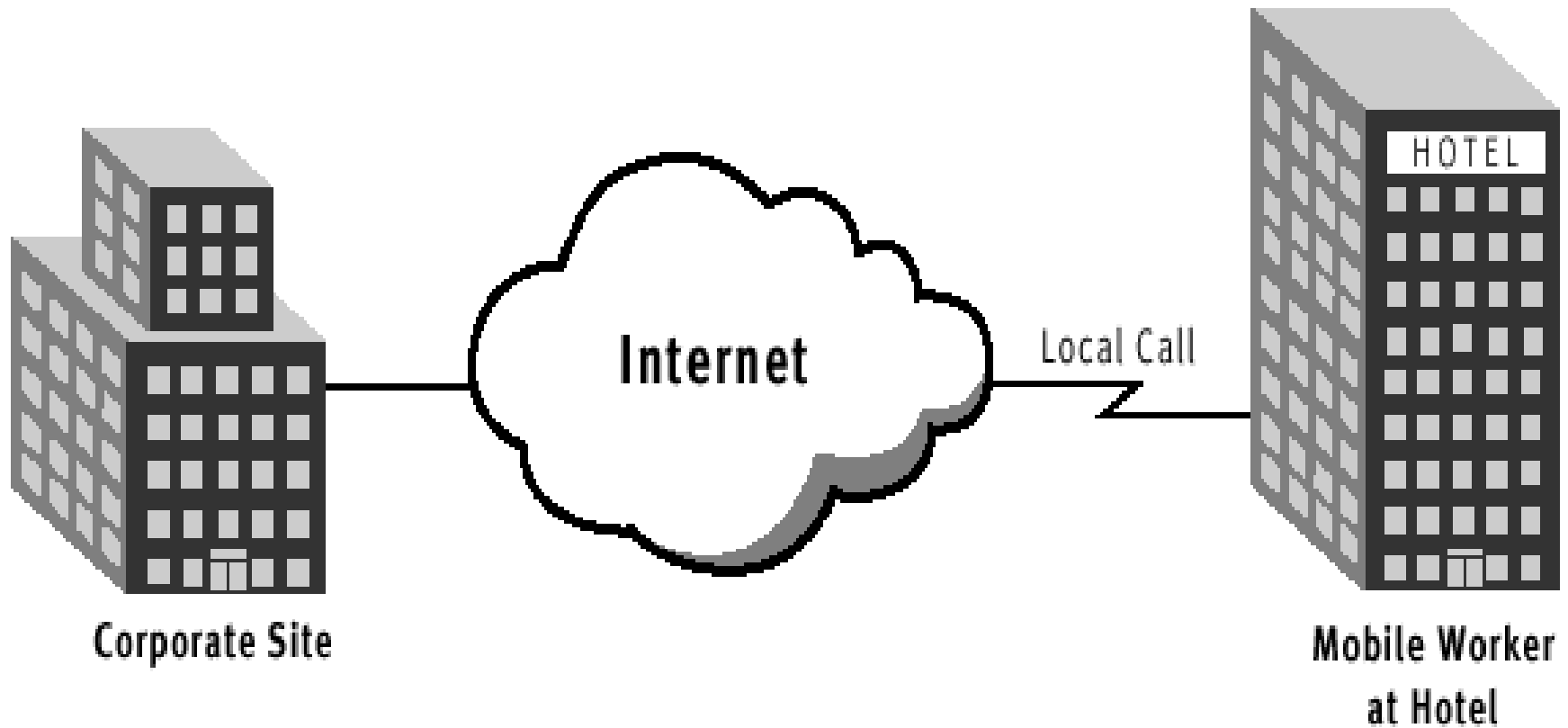
Virtual Private Network Driving Forces



Why VPNs?

- Today's workforce is increasingly mobile
 - ⊗ Telecommuting increasing
 - ⊗ Increasing focus on global operations
 - ⊗ Beyond “work from home”
- Firms need to provide employees with secure access to corporate information, wherever they may be
- Need scalable remote access solution
 - ⊗ Can't keep up with modem pool demand
 - ⊗ Maintaining dedicated corporate modem pools not economical
 - ⊗ Growing trend to outsourcing of dialin infrastructure
 - ⊗ Replacing WANs, dedicated corporate networks with less expensive solutions based on Internet technology
- Result: VPNs are a critical part of every firm's Intranet strategy

Internet is the Ubiquitous Network

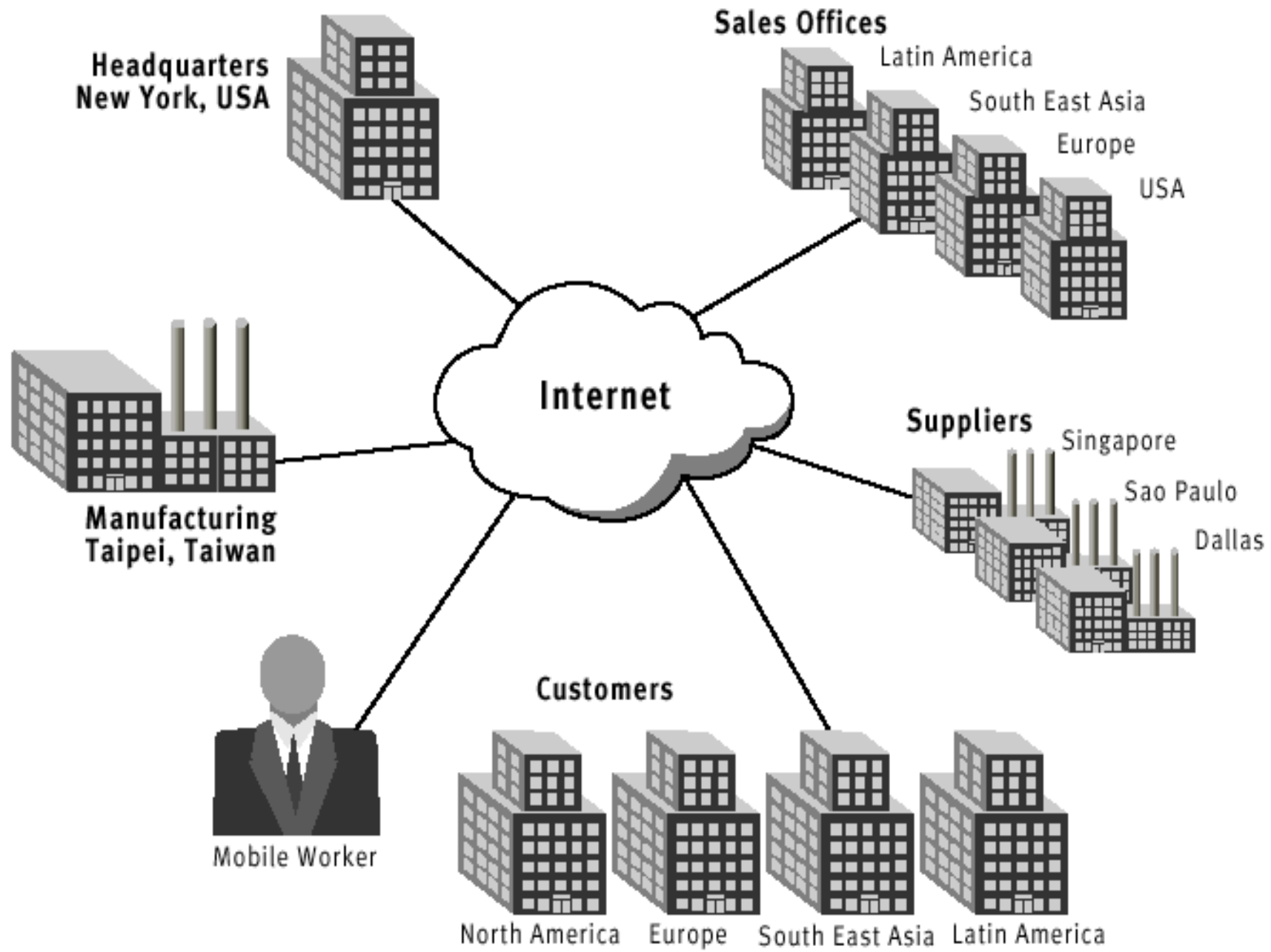


What are VPNs used for?

- The answer: VPNs reduce communications costs.
- The general idea behind using a VPN is that a company reduces the **recurring telecommunications charges** that are incurred when connecting remote users and branch offices to resources in corporate headquarters.

Use of the Internet a Corporate WAN

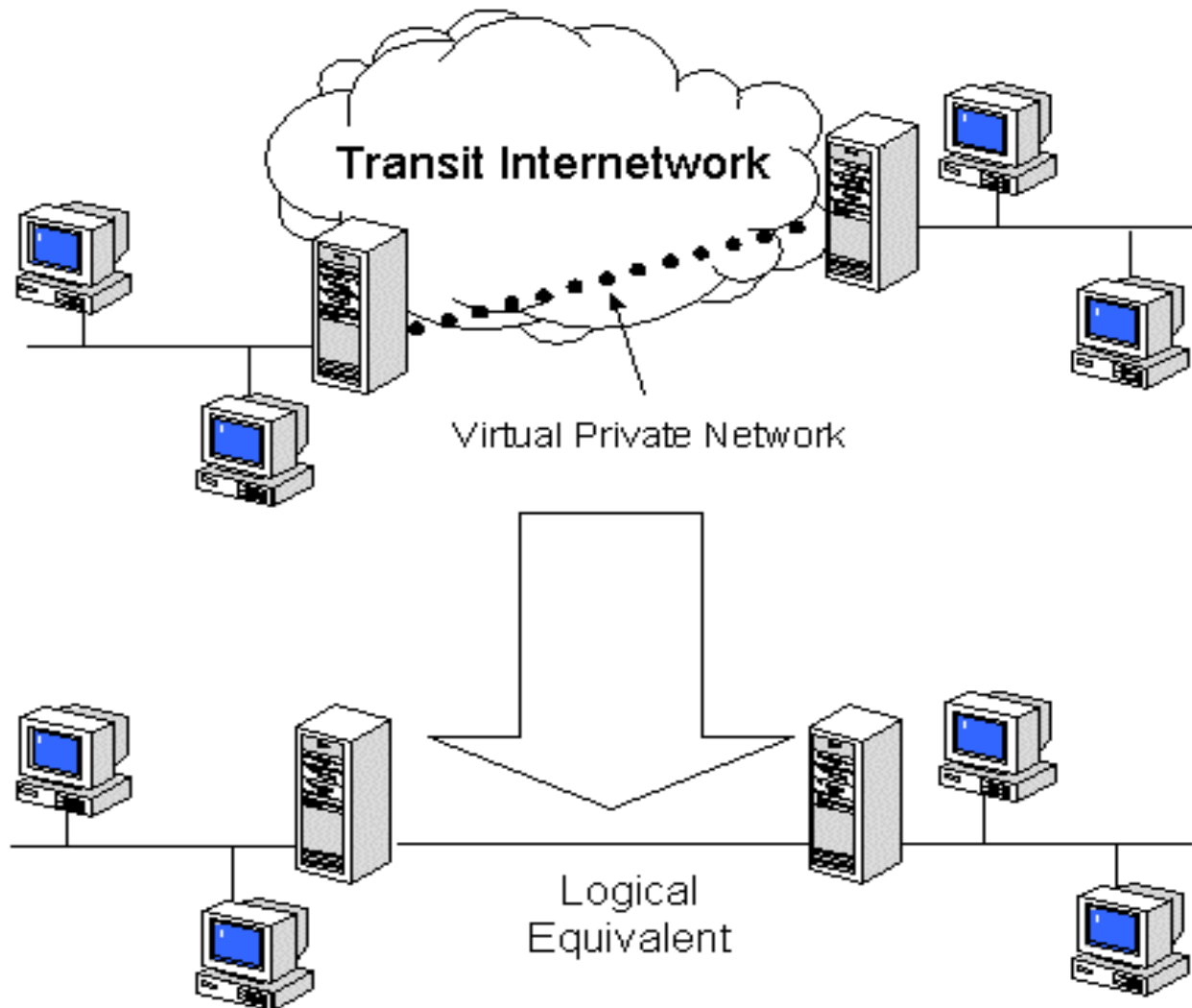
- Internet can be used as an economical corporate WAN connection
- Security concerns must be addressed
- Quality of service will remain a problem for some time



What is a VPN?

- VPN is a combination of tunneling, encryption, authentication, and access control technologies and services used to carry traffic over the Internet, a managed IP network or a provider's backbone.

Virtual Private Network



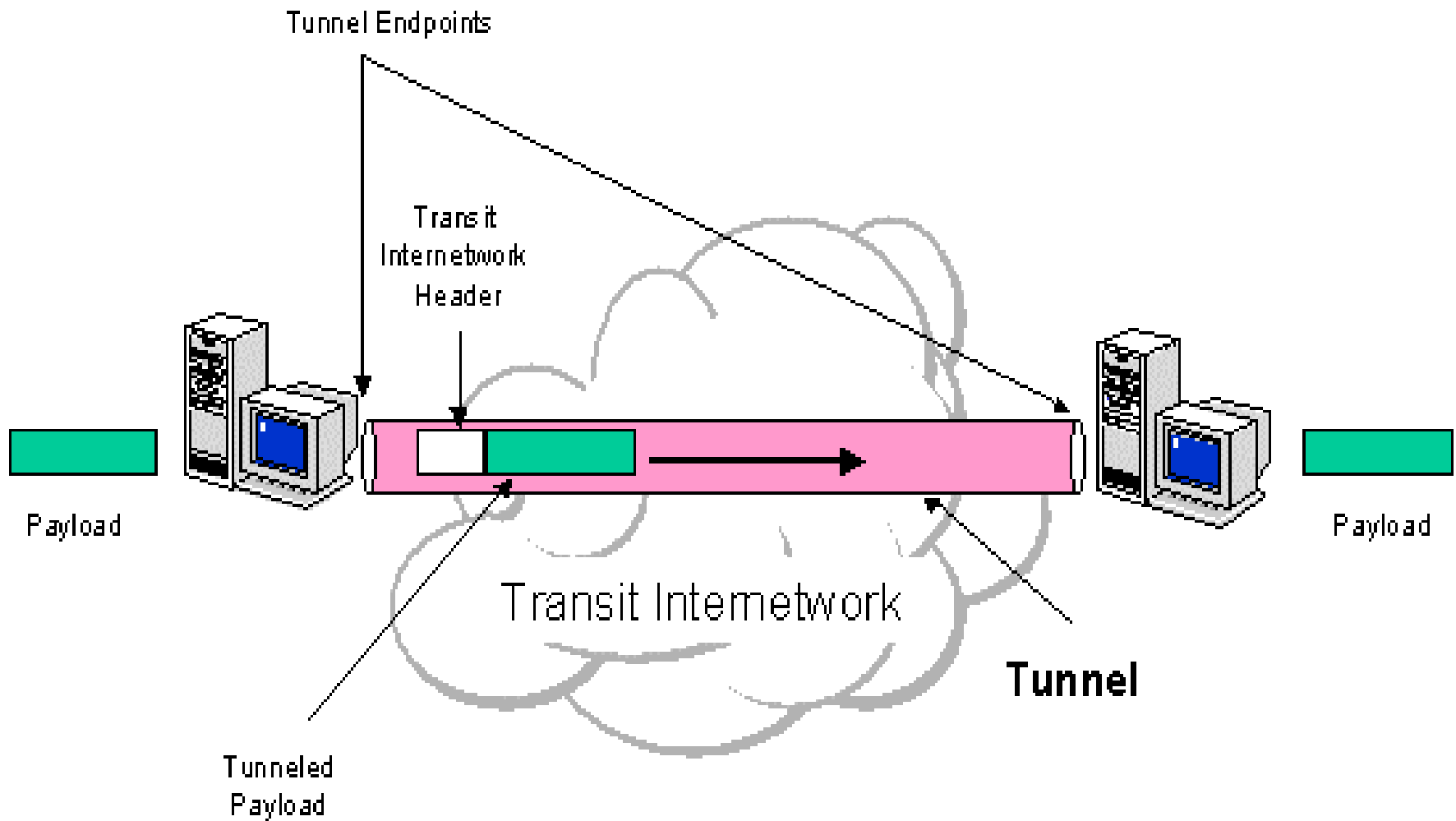
networks one for all practical purposes

- The secure connection across the internet network appears to the user as a private network communication-despite the fact that this communication occurs over a public internet network - hence the name Virtual Private Network.

VPNs use Tunneling

- A Virtual Private Network (VPN) connects the components and resources of one network over another network.
- VPNs accomplish this by allowing the user to tunnel through the Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only in private networks.

Tunneling



Tunneling Basics

- Tunneling is a method of using an internetwork infrastructure to transfer data from one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork.
- The encapsulated packets are then routed between tunnel endpoints over the internetwork. The logical path through which the encapsulated packets travel through the internetwork is called a tunnel. Once the encapsulated frames reach their destination on the internetwork, the frame is unencapsulated and forwarded to its final destination. Note that tunneling includes this entire process (encapsulation, transmission, and unencapsulation of packets).

A VPN solution should provide all of the following:

- **User Authentication** - The solution must verify a user's identity and restrict VPN access to authorized users. In addition, the solution must provide audit and accounting records to show who accessed what information and when.
- **Address Management** - The solution must assign a client's address on the private net, and must ensure that private addresses are kept private.
- **Data Encryption** - Data carried on the public network must be rendered unreadable to unauthorized clients on the network.
- **Key Management** - The solution must generate and refresh encryption keys for the client and server.
- **Multiprotocol Support** - The solution must be able to handle common protocols used in the public network. These include Internet Protocol (IP), Internet Packet Exchange (IPX), and so on.

VPN Architecture Solutions

- PPTP
- L2TP
- IPSec

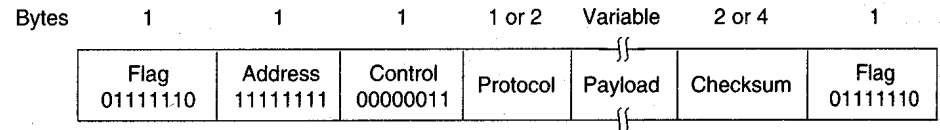
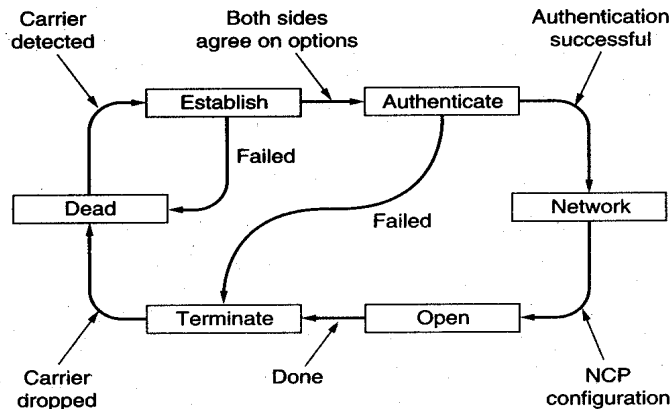
PPTP

- Internet RFC-based - From Microsoft and USR
- Widely supported standard
- Follows Client Server model
- Based on PPP

What is PPTP?

- Simply: PPP in IP
 - ⊗ Traditional PPP dial up frames are encapsulated in IP
 - ⊗ PPP is ubiquitous dial up standard
 - ⊗ PPP is multi-protocol, extensible, and authenticated
- Enables Internet to be used as a WAN
 - ⊗ Clients
 - ⊗ Networks

Review of PPP

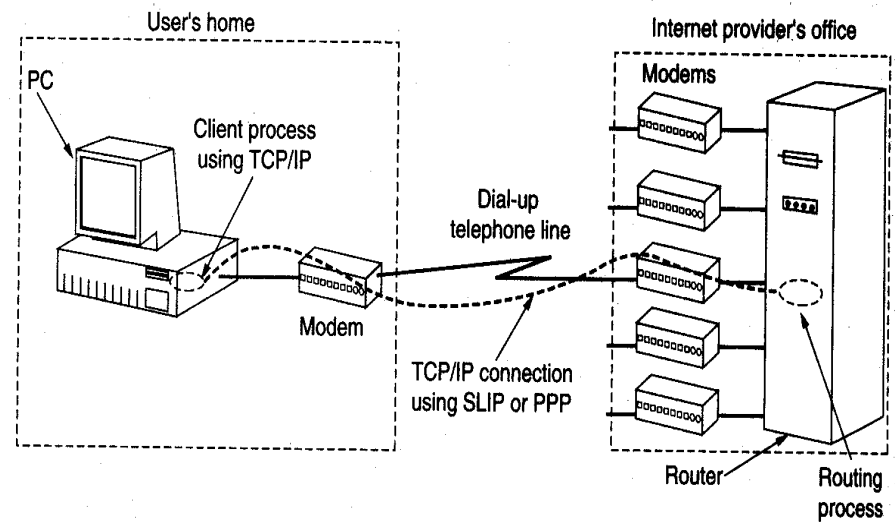


■ PPP provides three things:

- ⊗ A framing method that unambiguously delineates the end of one frame and the start of the next one. The frame format also handles error detection.
- ⊗ A link control protocol for bringing up lines, testing them, negotiating options, and bringing them down gracefully when no longer needed. This protocol is called Link Control Protocol (LCP).
- ⊗ A way to negotiate network layer options in a way that is independent of the network layer protocol to be used. The method chosen is to have a different Network Control Protocol (NCP) for each network layer supported.

Review of PPP

- PPP handles error detection, supports multiple protocols, allows IP addresses to be negotiated at connection time, permits authentication. It is used on both dial-up lines and router to router leased lines

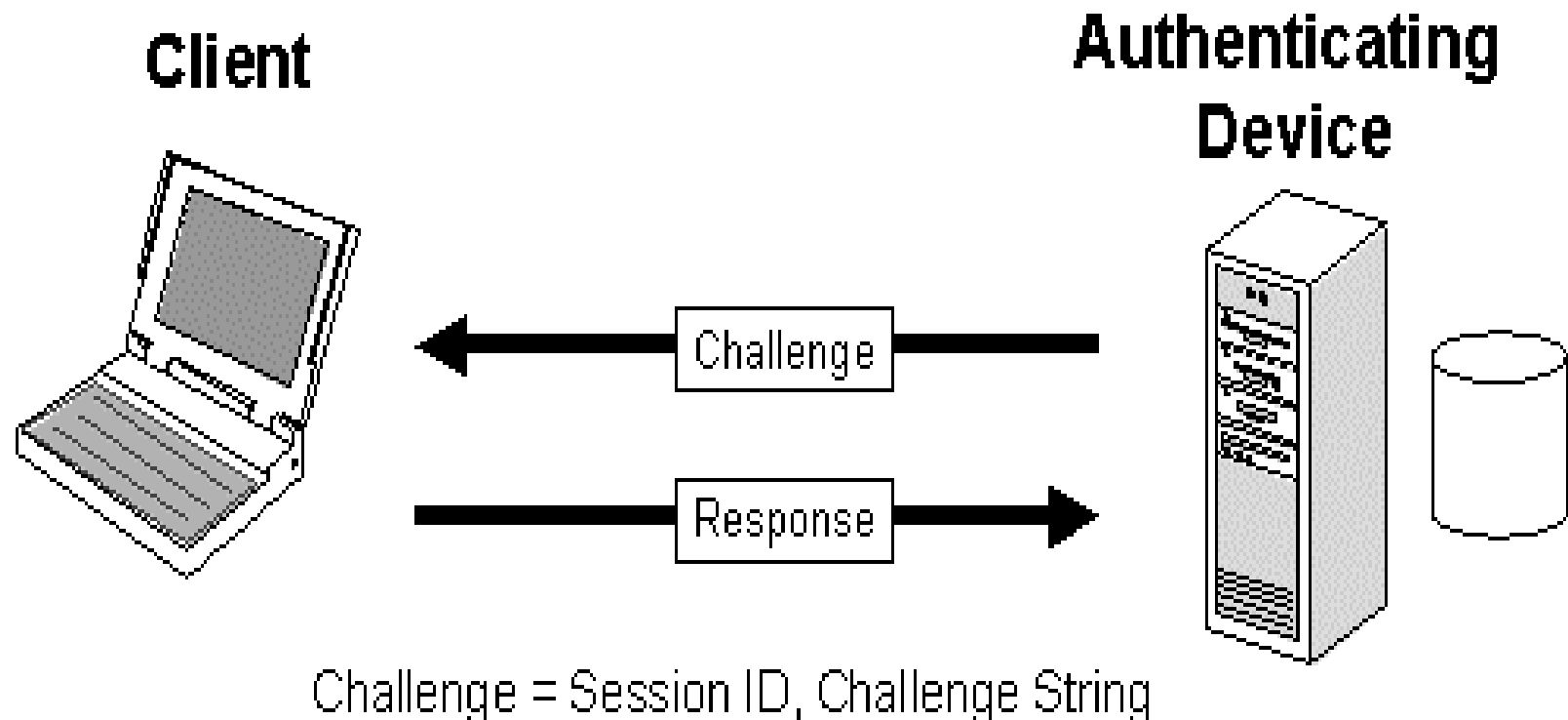


Review of PPP

- PPP Suite:
- LCP
- NCPs - IPCP, IPXCP, ATCP, etc.
- CCP
- ECP
- CHAP
- PAP

Name	Direction	Description
Configure-request	I → R	List of proposed options and values
Configure-ack	I ← R	All options are accepted
Configure-nak	I ← R	Some options are not accepted
Configure-reject	I ← R	Some options are not negotiable
Terminate-request	I → R	Request to shut the line down
Terminate-ack	I ← R	OK, line shut down
Code-reject	I ← R	Unknown request received
Protocol-reject	I ← R	Unknown protocol requested
Echo-request	I → R	Please send this frame back
Echo-reply	I ← R	Here is the frame back
Discard-request	I → R	Just discard this frame (for testing)

The CHAP Process

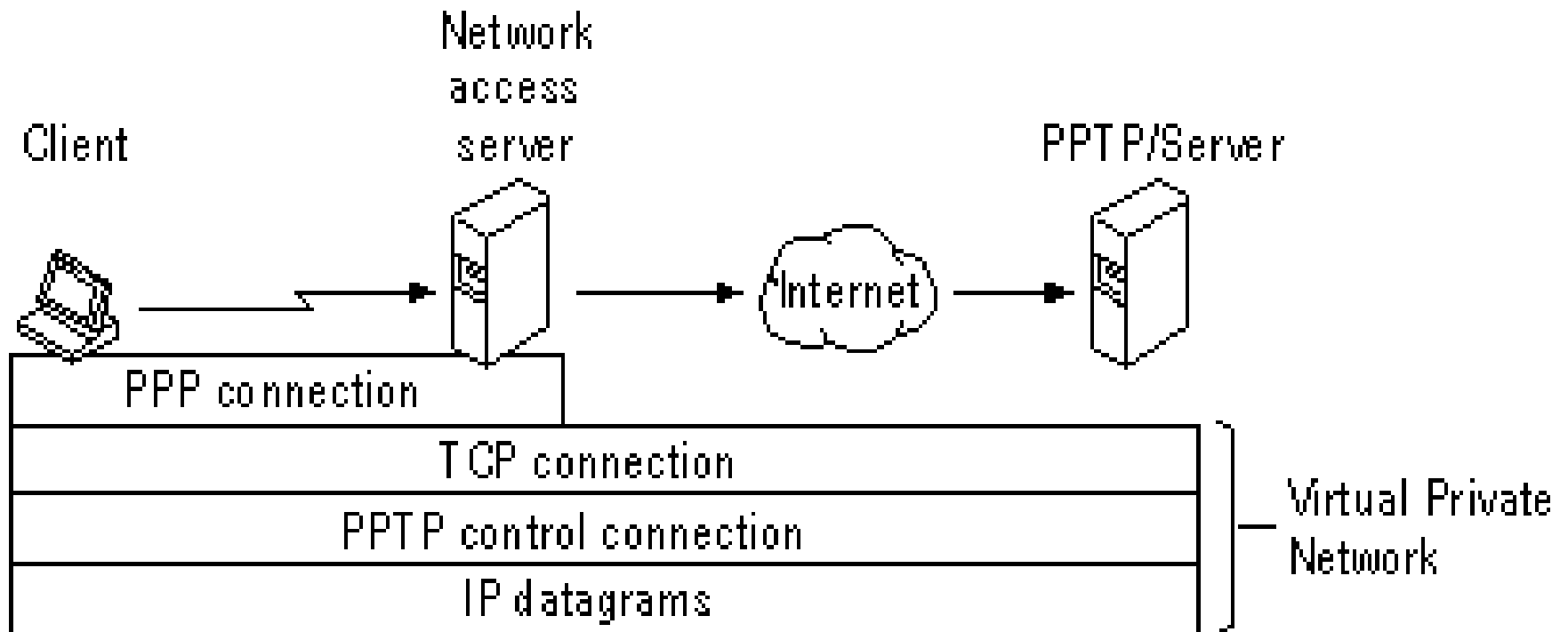


Response = MD5 Hash(Session ID, Challenge String, User Password), User Name

PPTP Details

- Tunnel
 - ⊗ Between PPTP FEP or Client, and PPTP server
 - ⊗ Control and Data Channel
 - ⊗ Many PPP sessions carried
- Control Channel
 - ⊗ TCP based (IANA port 1723)
 - ⊗ Session establishment, tear down, and management
- Data Channel
 - ⊗ Enhanced GRE encapsulation (Ethertype 0x880B, IP Protocol ID 47)
 - ⊗ Flow control for congestion and link feedback

The PPTP Tunnel



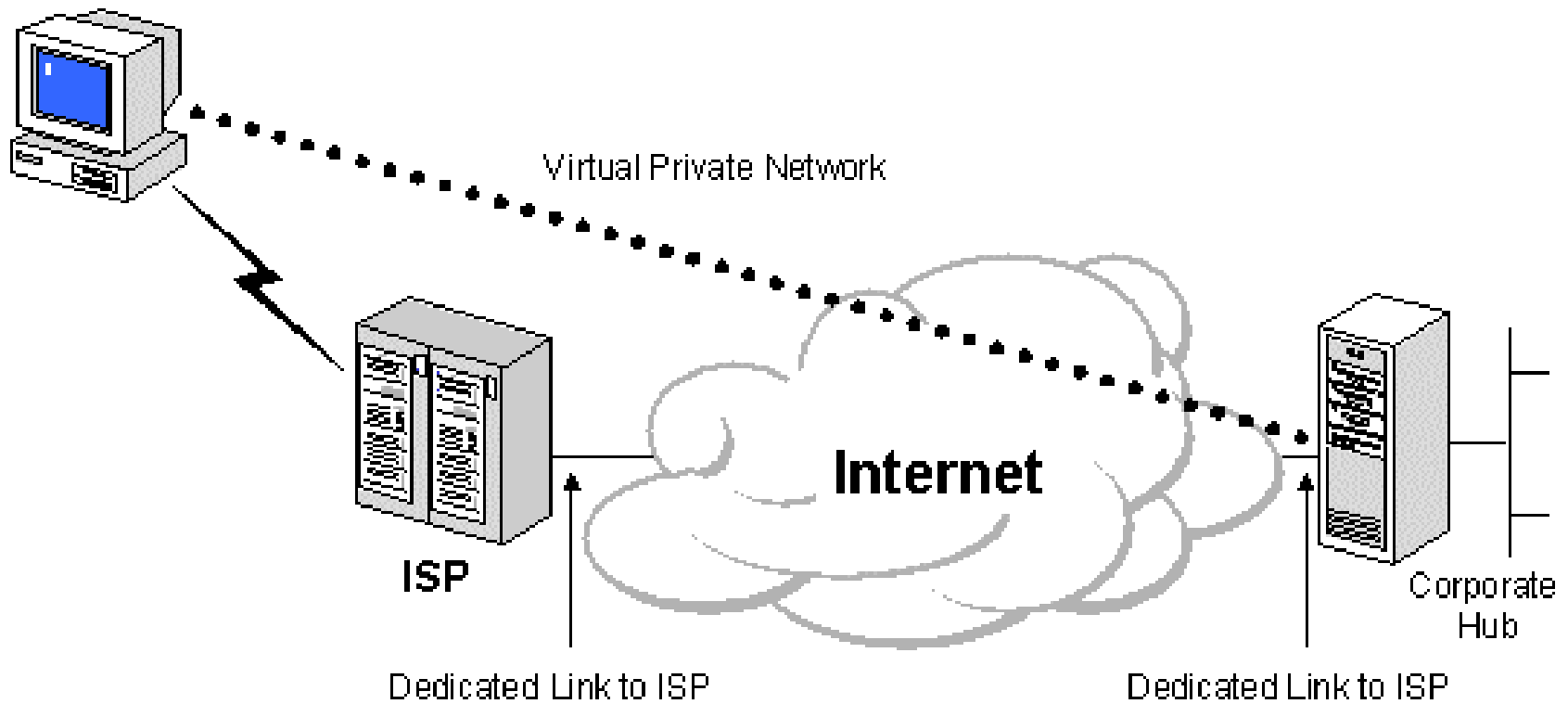
A Typical PPTP Data Packet

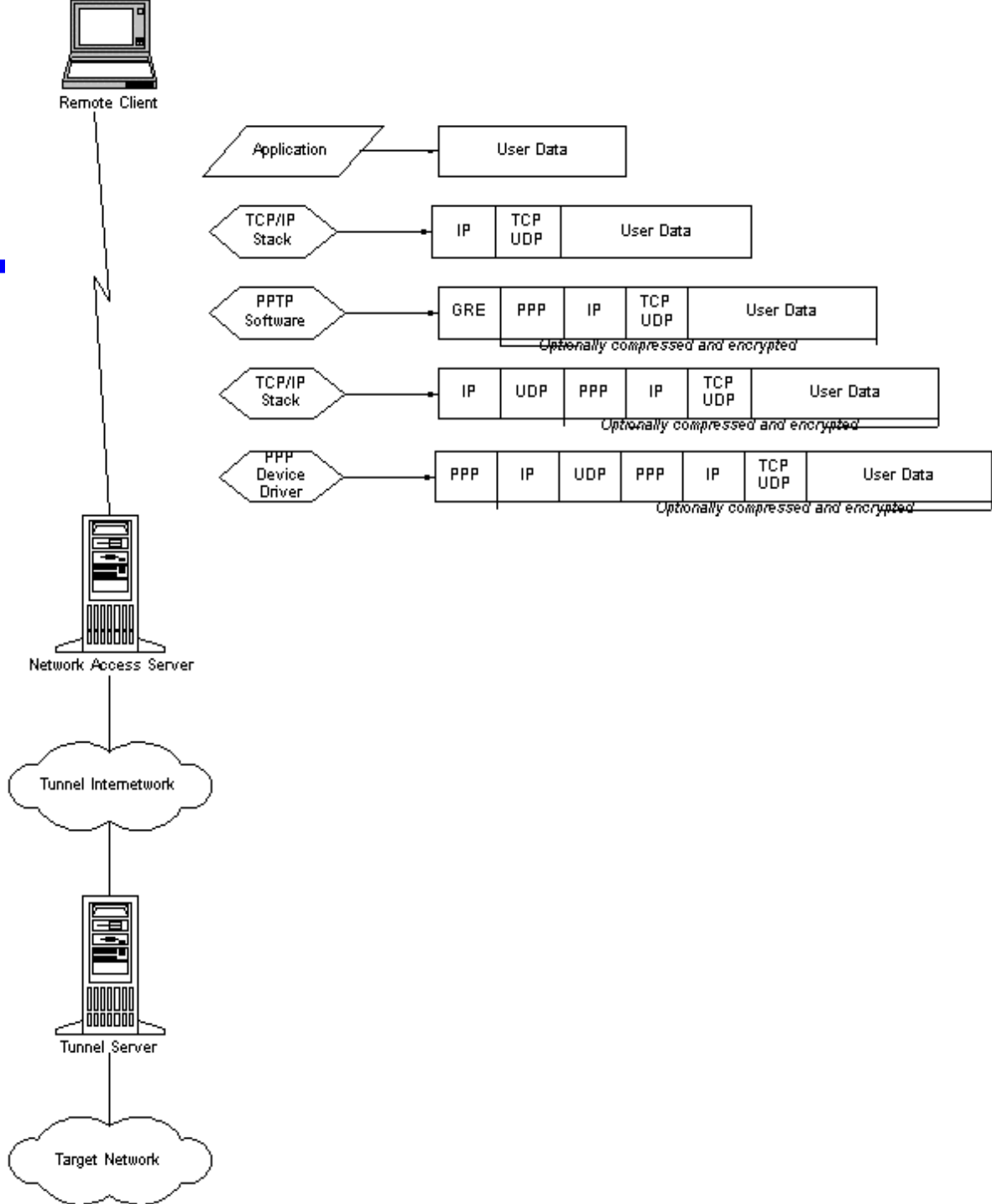


Remote User Access Over the Internet

- VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.
- Rather than making a leased line, long distance (or 1-800) call to a corporate or outsourced Network Access Server (NAS), the user first calls a local ISP NAS phone number.
- Using the local connection to the ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

remote client to a private LAN





GRE

Standard IP Header

(Using Home and Foreign Agents' IP Address for Source/Destination)

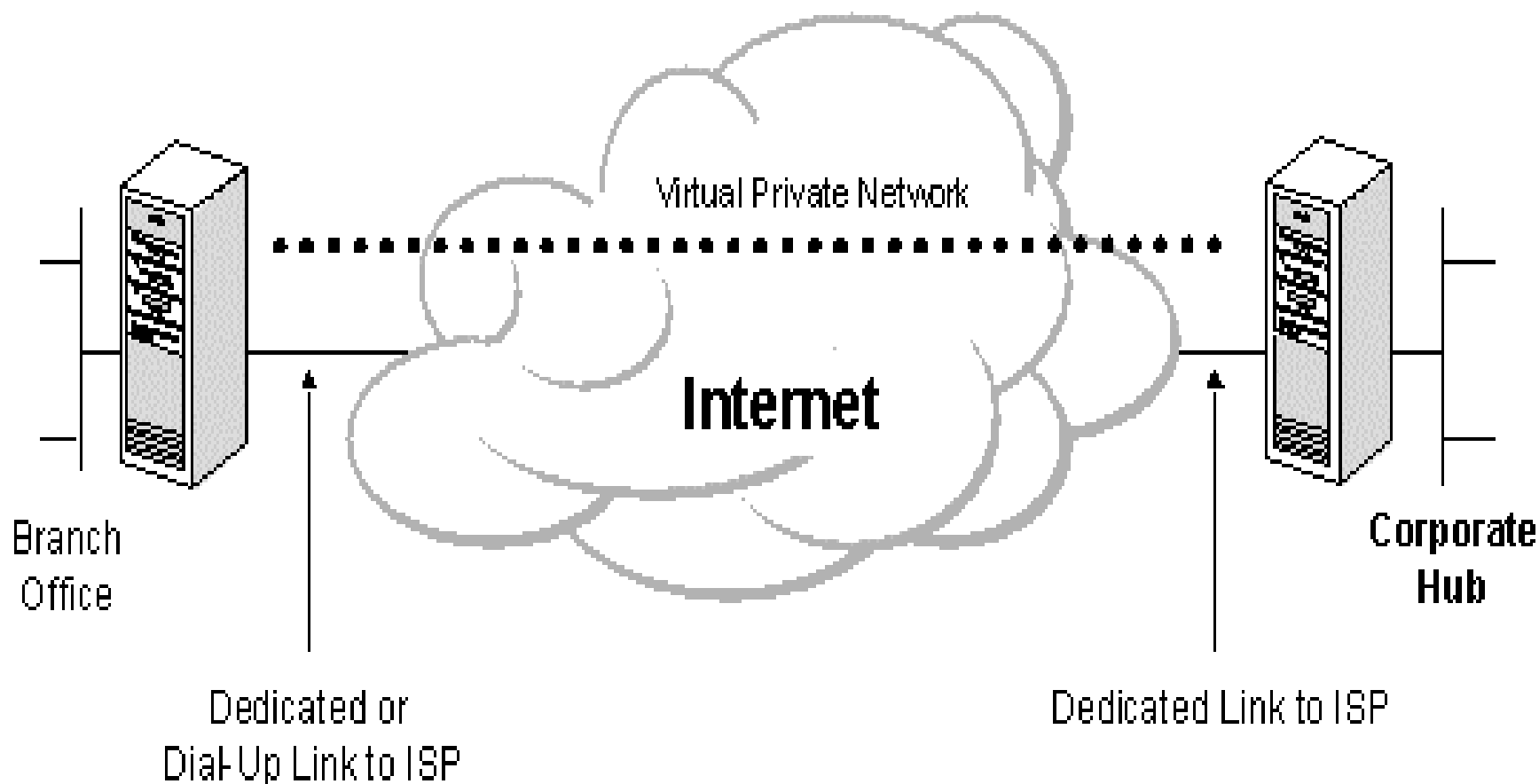
GRE Header

- **Protocol Type** of Payload Packet
- **Checksum** (optional)
- **Key** to Identify/Authenticate Actual Source
- **Sequence Number** of Packet in Series Transmitted
- **Source Routing** (optional)

Payload

(Original Packet, Complete with Original Header)

Using a VPN to connect two remote sites



a branch office to a corporate LAN

- Rather than using an expensive long-haul dedicated circuit between the branch office and the corporate hub, both the branch office and the corporate hub routers can use a local dedicated circuit and local ISP to connect to the Internet.
- The VPN software uses the local ISP connections and the public Internet to create a virtual private network between the branch office router and corporate hub router.

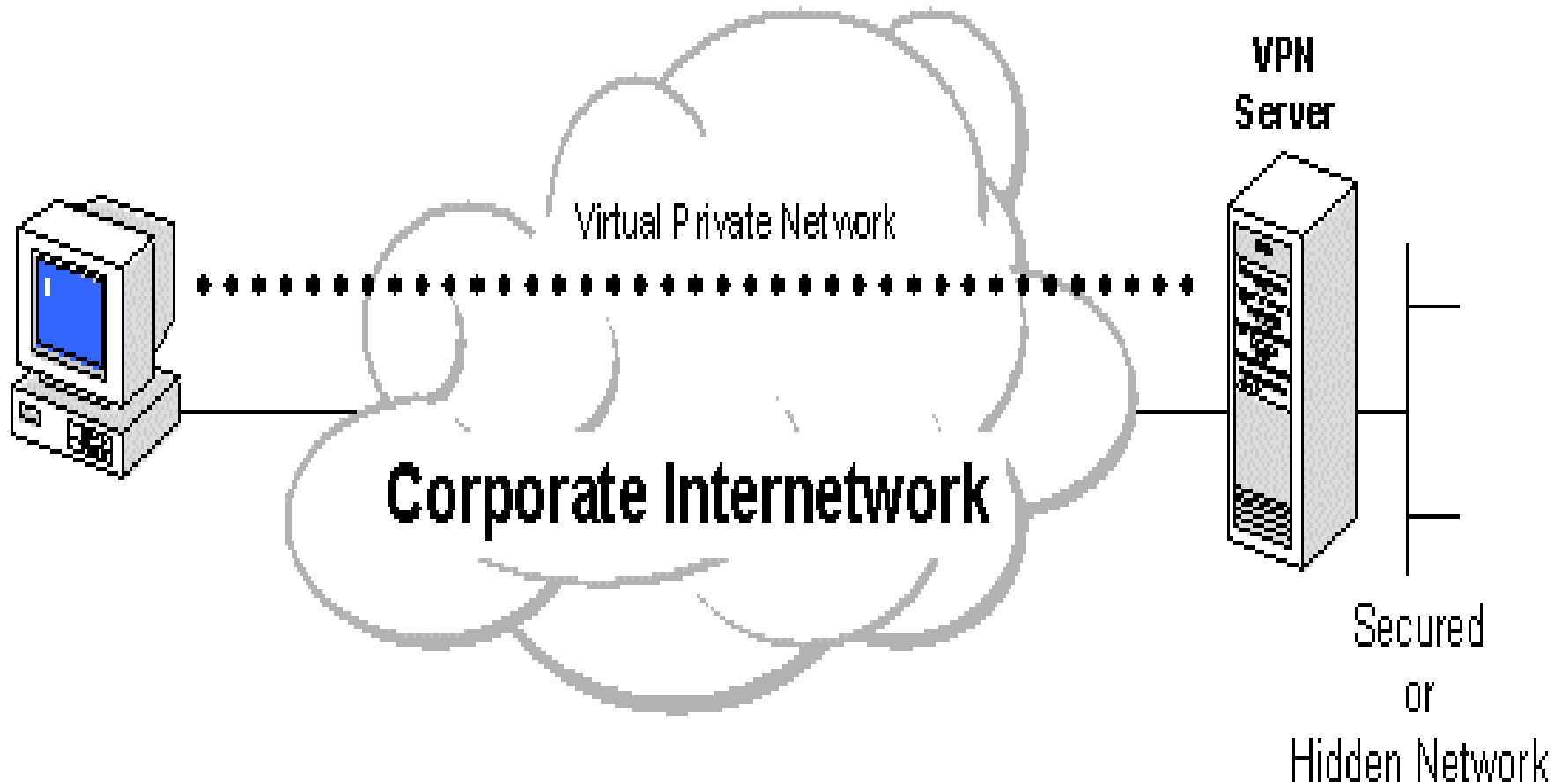
branch office to a corporate LAN

- Using a dial-up line to connect a branch office to a corporate LAN. Rather than having a router at the branch office make a leased line, long distance or (1-800) call to a corporate or outsourced NAS, the router at the branch office can call the local ISP. The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.

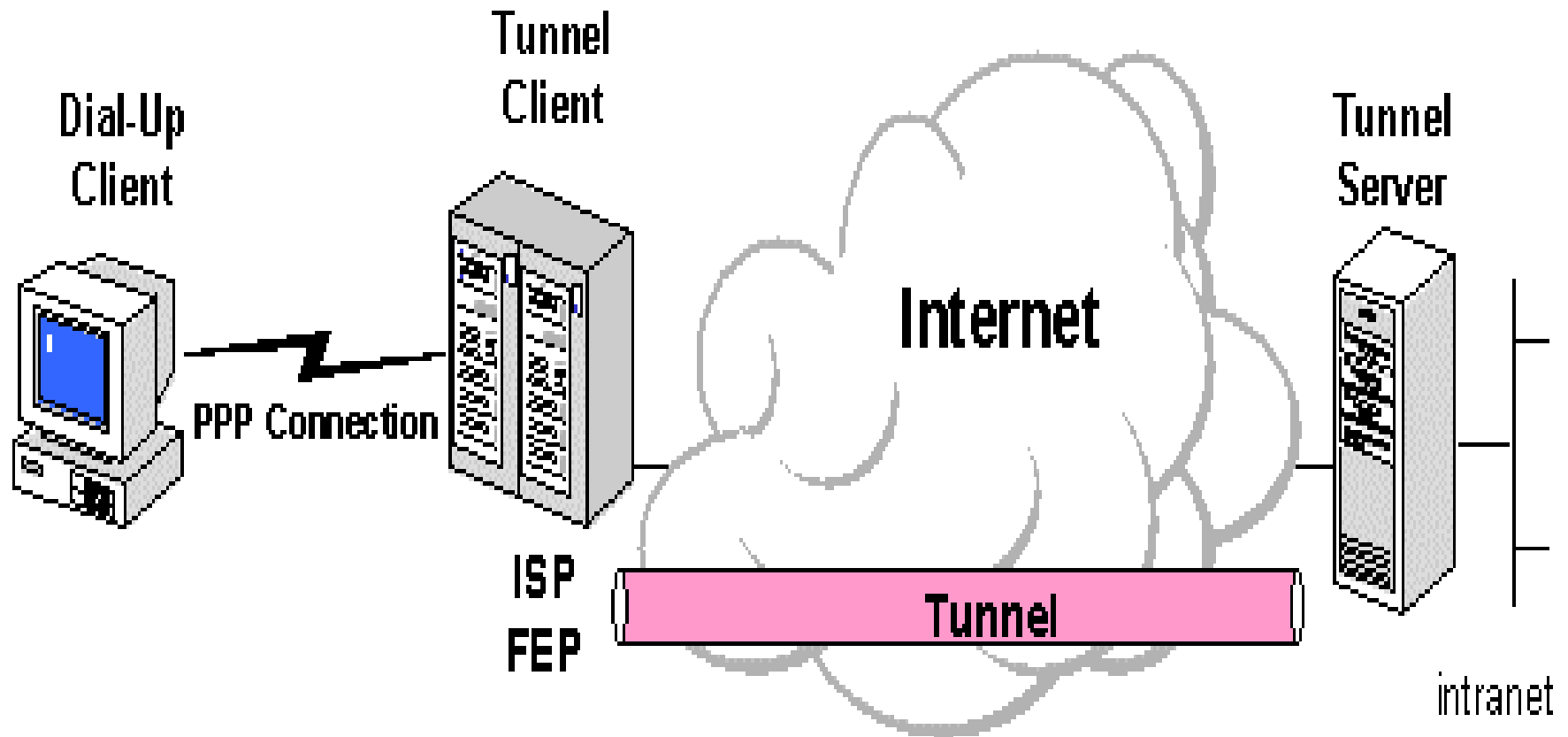
Connecting Computers Over an Intranet

- In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork.
- While this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.

Using a VPN to connect to a two computers on the same LAN



Compulsory Tunneling



L2TP

■ Advantages

- ⊗ On IETF standards track
 - combines L2F and PPTP plus new features
- ⊗ Support for authenticated tunnels
- ⊗ Ability to run directly over multiple media: ATM, Frame Relay, X.25
- ⊗ Ability to bundle multiple tunnels
- ⊗ Firewall and NAT friendly (runs over UDP)

■ Disadvantages

- ⊗ Increased Payload overhead

■ Specification stabilizing

- ⊗ Proposed standard likely by December '97

■ IETF draft available

IPSEC Tunnel Mode

■ Advantages

- ⊗ Universal IP-level security
 - Authentication and encryption
 - End-to-end security: A step beyond the “firewall” model

■ Largely complementary to PPTP/L2TP

- ⊗ IPSEC tunnel mode not yet a complete solution
- ⊗ IPSEC security + PPTP/L2TP tunneling: a marriage made in heaven?

■ Interoperability testing proceeding

- ⊗ First bake-off completed, manual keying tested

Tunneling Protocol Comparison

PPTP

L2TP

IPSEC

Authenticated Tunnels	X	X	X
Compression	X	X	X
Cert-based Smart Cards	X	X	X
Crypto calculators	X	X	
Address Allocation	X	X	
Multiprotocol	X	X	
Encryption	X	X	X
Flow control	X	X	