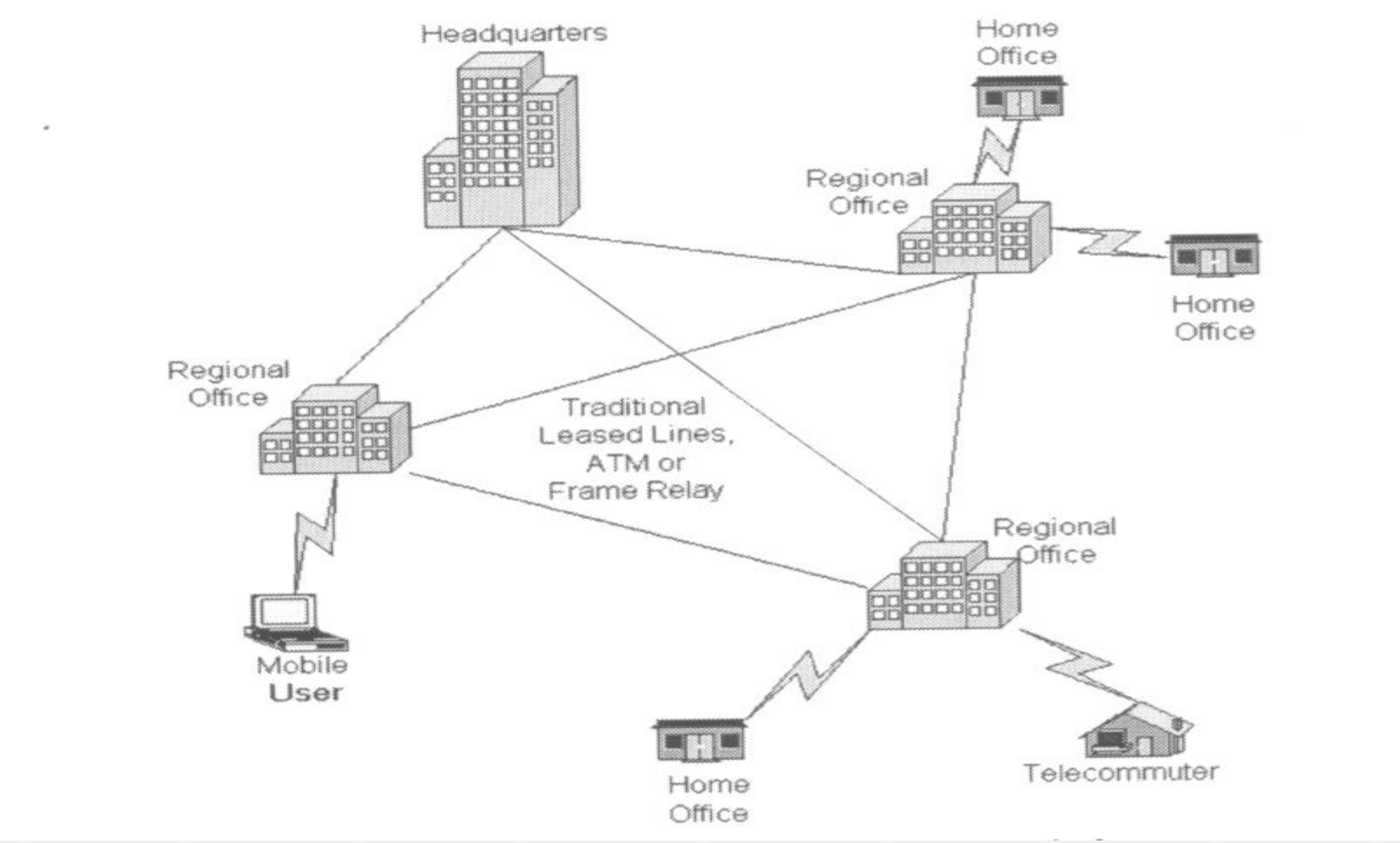
VIRTUAL PRIVATE NETWORKS (VPN)

Traditional Connectivity



What is VPN?

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.

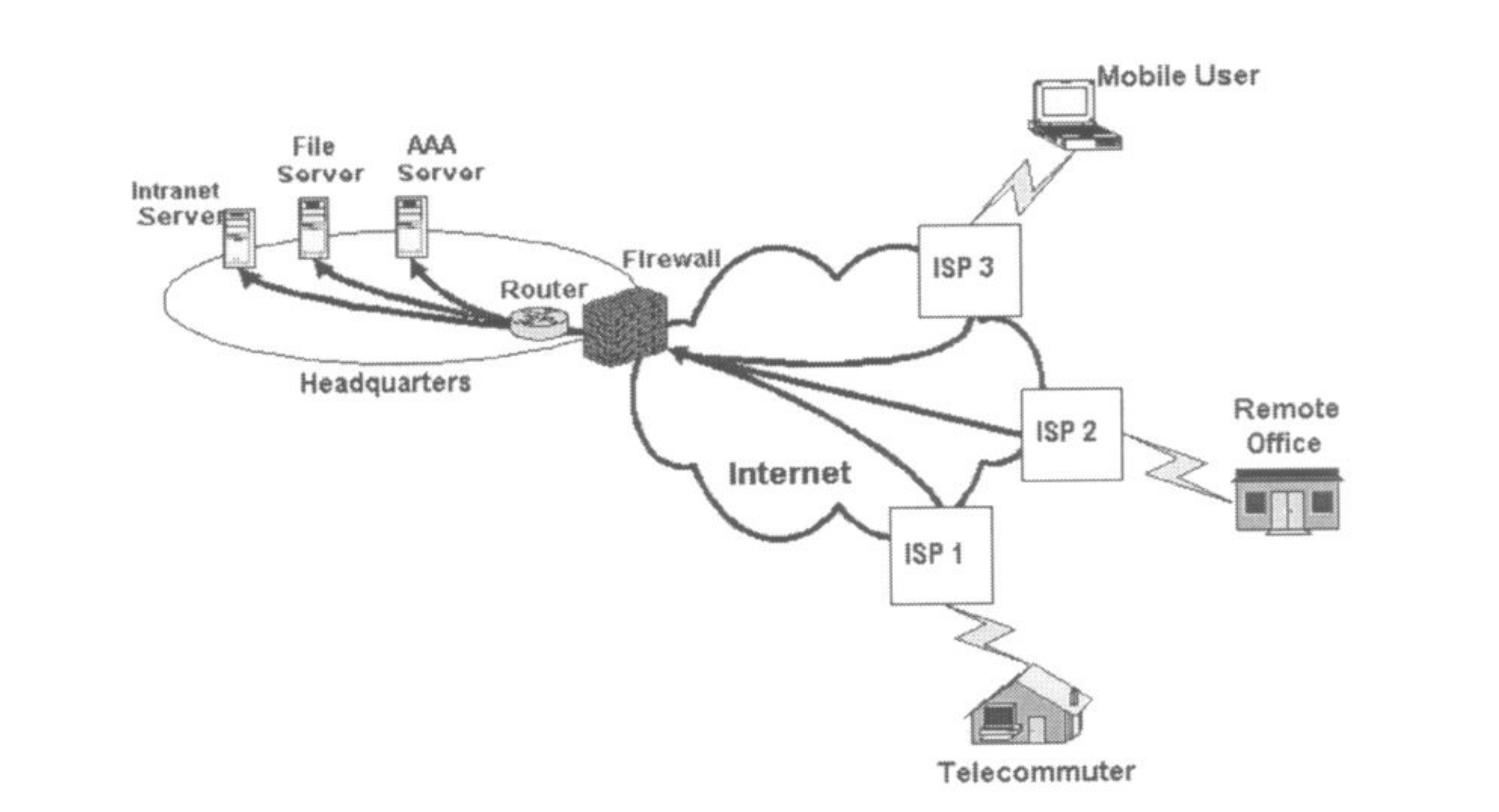
- Became popular as more employees worked in remote locations.

- Terminologies to understand how VPNs work.

Private Networks
vs.
Virtual Private Networks

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability

Remote Access Virtual Private Network



Brief Overview of How it Works

- ✔ Two connections – one is made to the Internet and the second is made to the VPN.
- ✔ Datagrams – contains data, destination and source information.
- ✔ Firewalls – VPNs allow authorized users to pass through the firewalls.
- ✔ Protocols – protocols create the VPN tunnels.

Four Critical Functions

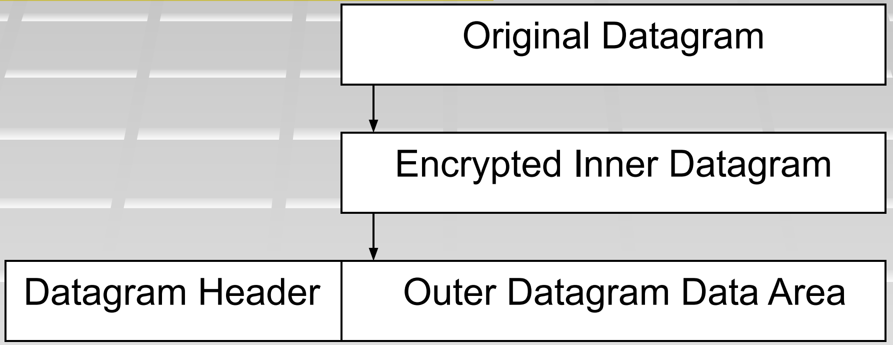
- ❑ Authentication – validates that the data was sent from the sender.
- ❑ Access control – limiting unauthorized users from accessing the network.
- ❑ Confidentiality – preventing the data to be read or copied as the data is being transported.
- ❑ Data Integrity – ensuring that the data has not been altered

Encryption

- Encryption -- is a method of “scrambling” data before transmitting it onto the Internet.
- Public Key Encryption Technique
- Digital signature – for authentication

Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated datagrams.



Data Encapsulation

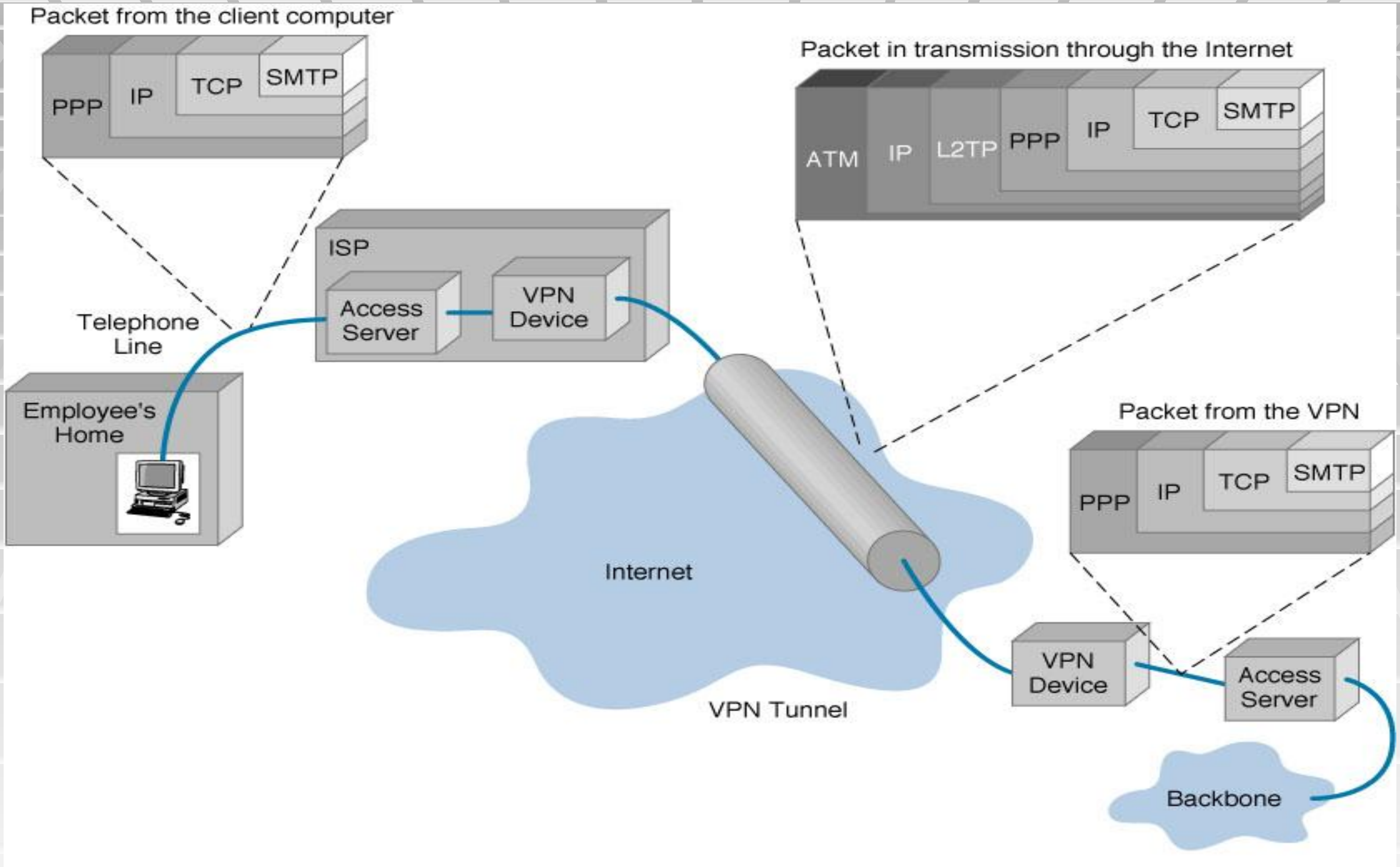
Two types of end points:

- ❑ Remote Access
- ❑ Site-to-Site

Four Protocols used in VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security
- SOCKS – is not used as much as the ones above

VPN Encapsulation of Packets



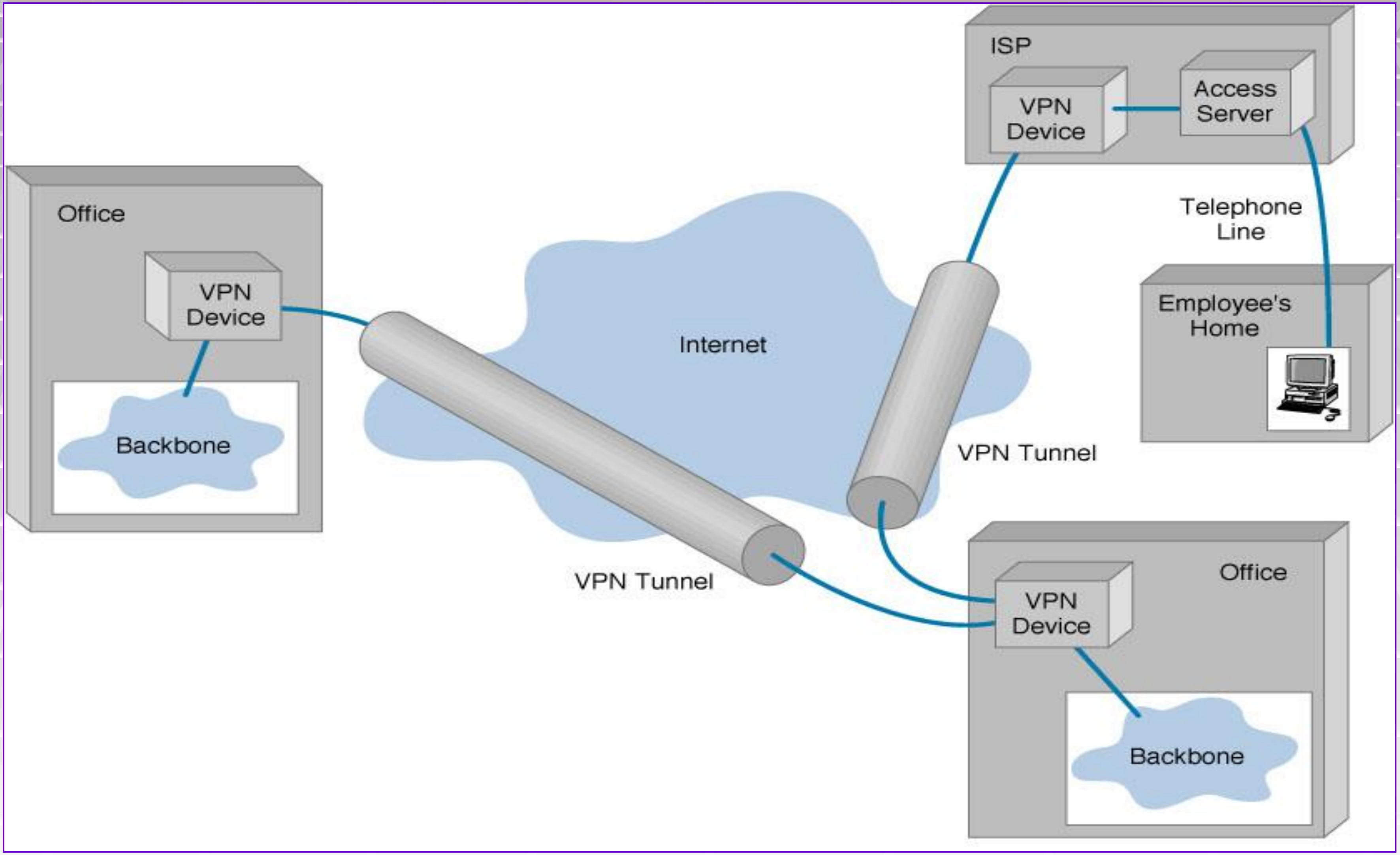
Types of Implementations

- What does "implementation" mean in VPNs?

- 3 types
  - Intranet – Within an organization
  - Extranet – Outside an organization
  - Remote Access – Employee to Business

Virtual Private Networks (VPN)

Basic Architecture



Device Types

- What it means

- 3 types
  - Hardware
  - Firewall
  - Software

Device Types: Hardware

- Usually a VPN type of router

Pros

- Highest network throughput
- Plug and Play
- Dual-purpose

Cons

- Cost
- Lack of flexibility

Device Types: Firewall

- More security?

Pros

- “Harden” Operating System
- Tri-purpose
- Cost-effective

Cons

- Still relatively costly

Device Types: Software

- Ideal for 2 end points not in same org.
- Great when different firewalls implemented

Pros

- Flexible
- Low relative cost

Cons

- Lack of efficiency
- More labor training required
- Lower productivity; higher labor costs

Advantages
VS.
Disadvantages

Advantages: Cost Savings

- Eliminating the need for expensive long-distance leased lines
- Reducing the long-distance telephone charges for remote access.
- Transferring the support burden to the service providers
- Operational costs

- **Cisco VPN Savings Calculator**

Advantages: Scalability

- Flexibility of growth
- Efficiency with broadband technology

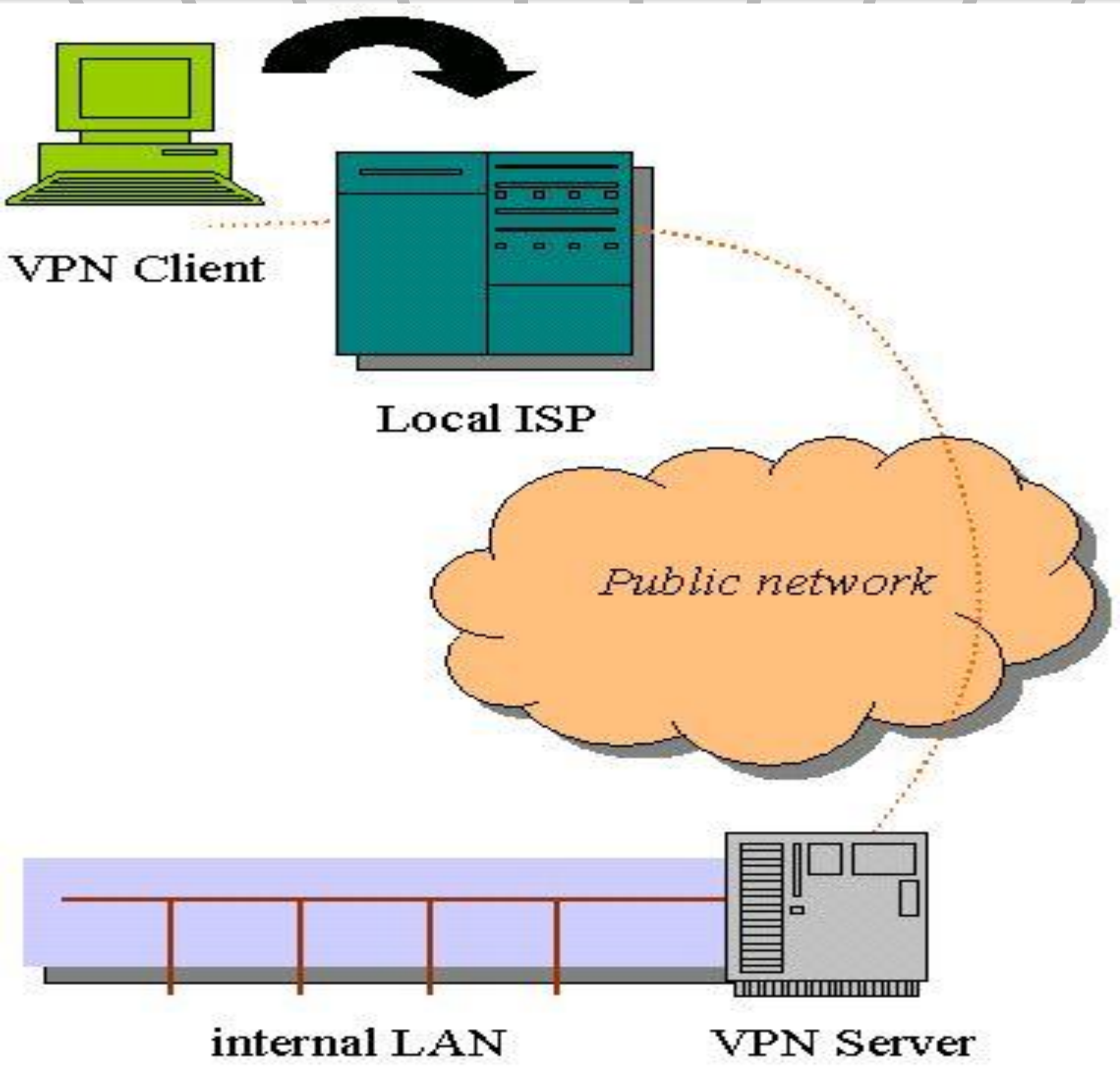
Disadvantages

- VPNs require an in-depth understanding of public network security issues and proper deployment of precautions
- Availability and performance depends on factors largely outside of their control
- Immature standards
- VPNs need to accommodate protocols other than IP and existing internal network technology

Applications: Site-to-Site VPNs

- Large-scale encryption between multiple fixed sites such as remote offices and central offices
- Network traffic is sent over the branch office Internet connection
- This saves the company hardware and management expenses

Site-to-Site VPNs



Applications: Remote Access

- Encrypted connections between mobile or remote users and their corporate networks
- Remote user can make a local call to an ISP, as opposed to a long distance call to the corporate remote access server.
- Ideal for a telecommuter or mobile sales people.
- VPN allows mobile workers & telecommuters to take advantage of broadband connectivity.
  i.e. DSL, Cable

Industries That May Use a VPN

- **Healthcare:** enables the transferring of confidential patient information within the medical facilities & health care provider

- **Manufacturing**: allow suppliers to view inventory & allow clients to purchase online safely

- **Retail:** able to securely transfer sales data or customer info between stores & the headquarters

- **Banking/Financial:** enables account information to be transferred safely within departments & branches

- **General Business:** communication between remote employees can be securely exchanged

Some Businesses using a VPN

- CVS Pharmaceutical Corporation upgraded their frame relay network to an IP VPN

- ITW Foilmark secured remote location orders, running reports, & internet/intranet communications w/ a 168-bit encryption by switching to OpenReach VPN

- Bacardi & Co. Implemented a 21-country, 44-location VPN

Where Do We See VPNs Going in the Future?

- VPNs are continually being enhanced.

  Example: Equant NV

- As the VPN market becomes larger, more applications will be created along with more VPN providers and new VPN types.
- Networks are expected to converge to create an integrated VPN
- Improved protocols are expected, which will also improve VPNs.

Pop Quiz!

Q.1

VPN stands for…

a) Virtual Public Network

[✓ b) Virtual Private Network]

c) Virtual Protocol Network

d) Virtual Perimeter Network

Pop Quiz!

A.1

VPN stands for…

b) Virtual Private Network

VPN stands for "Virtual Private Network" or "Virtual Private Networking." A VPN is a private network in the sense that it carries controlled information, protected by various security mechanisms, between known parties. VPNs are only "virtually" private, however, because this data actually travels over shared public networks instead of fully dedicated private connections.

Pop Quiz!

Q.2

What are the acronyms for the 3 most common VPN protocols?

Pop Quiz!

A.2

3 most common VPN protocols are…

- **PPTP**
- **L2TP**
- **IPsec**

PPTP, IPsec, and L2TP are three of today's most popular VPN tunneling protocols. Each one of these is capable of supporting a secure VPN connection.

Pop Quiz!

Q
.3

What does PPTP stand for?

Pop Quiz!

A.3

PPTP = Point-to-Point Tunneling Protocol !

Pop Quiz!

Q.4

What is the main benefit of VPNs compared to dedicated networks utilizing frame relay, leased lines, and traditional dial-up?

a) better network performance

b) less downtime on average

c) reduced cost

d) improved security

Pop Quiz!

A.4

The main benefit of VPNs is…

c) <u>reduced cost</u>

The main benefit of a VPN is the potential for significant cost savings compared to traditional leased lines or dial up networking. These savings come with a certain amount of risk, however, particularly when using the public Internet as the delivery mechanism for VPN data.

Pop Quiz!

Q
.5

In VPNs, the term "tunneling" refers to

a) an optional feature that increases network performance if it is turned on

b) the encapsulation of packets inside packets of a different protocol to create and maintain the virtual circuit

c) the method a system administrator uses to detect hackers on the network

d) a marketing strategy that involves selling VPN products for very low prices in return for expensive service contracts

Pop Quiz!

A.5

In VPNs, the term "tunneling" refers to...

b) the encapsulation of packets inside packets of a different protocol to create and maintain the virtual circuit