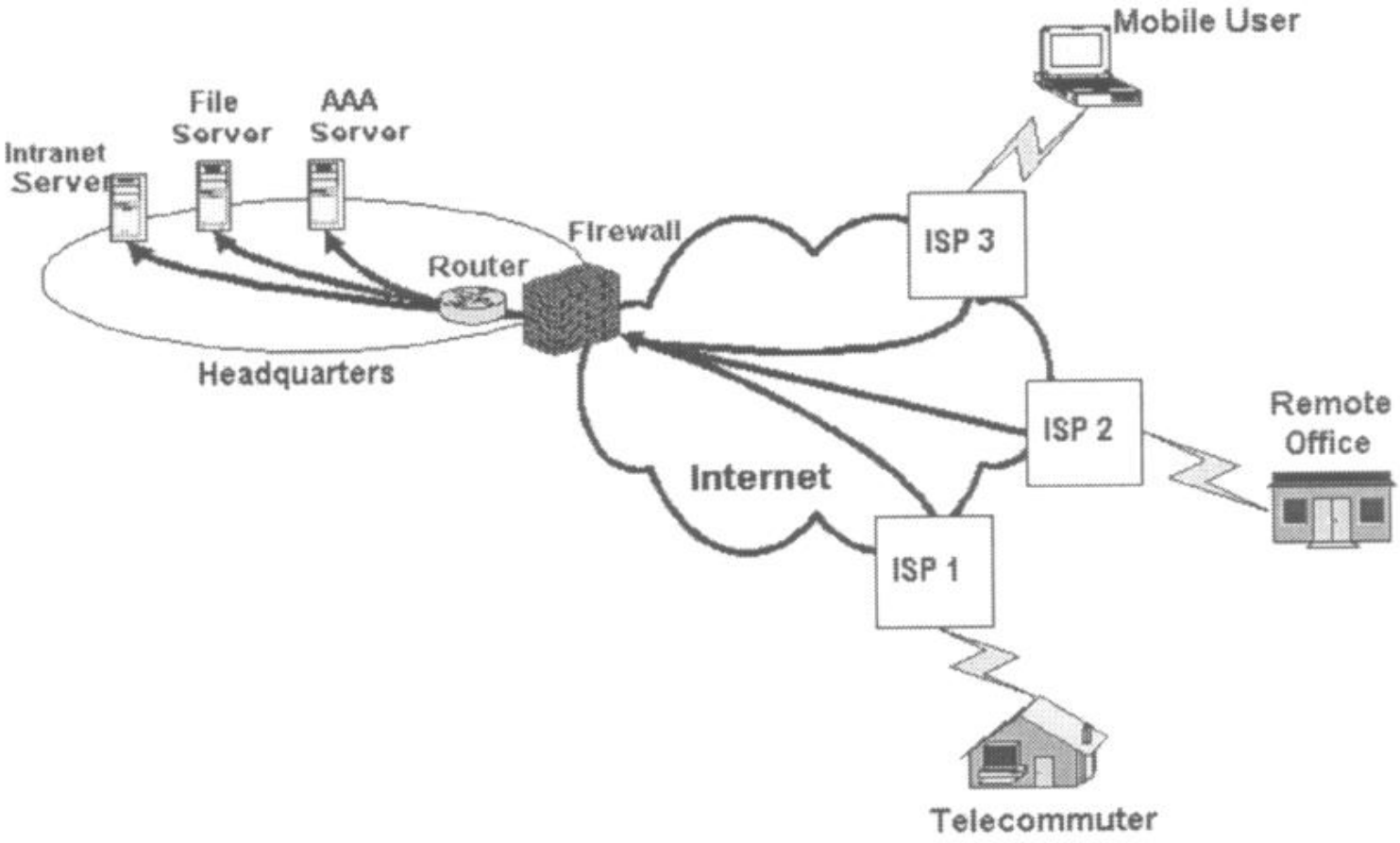
VIRTUAL PRIVATE NETWORKS (VPN)

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.

Remote Access Virtual Private Network



(From Gartner Consulting)

Brief Overview of How it Works

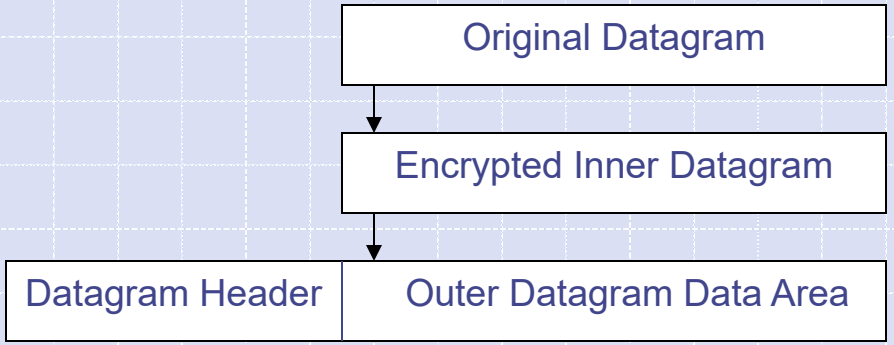
- Two connections – one is made to the Internet and the second is made to the VPN.
- Datagrams – contains data, destination and source information.
- Firewalls – VPNs allow authorized users to pass through the firewalls.
- Protocols – protocols create the VPN tunnels.

Tunneling

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

Two types of end points:

- Remote Access
- Site-to-Site

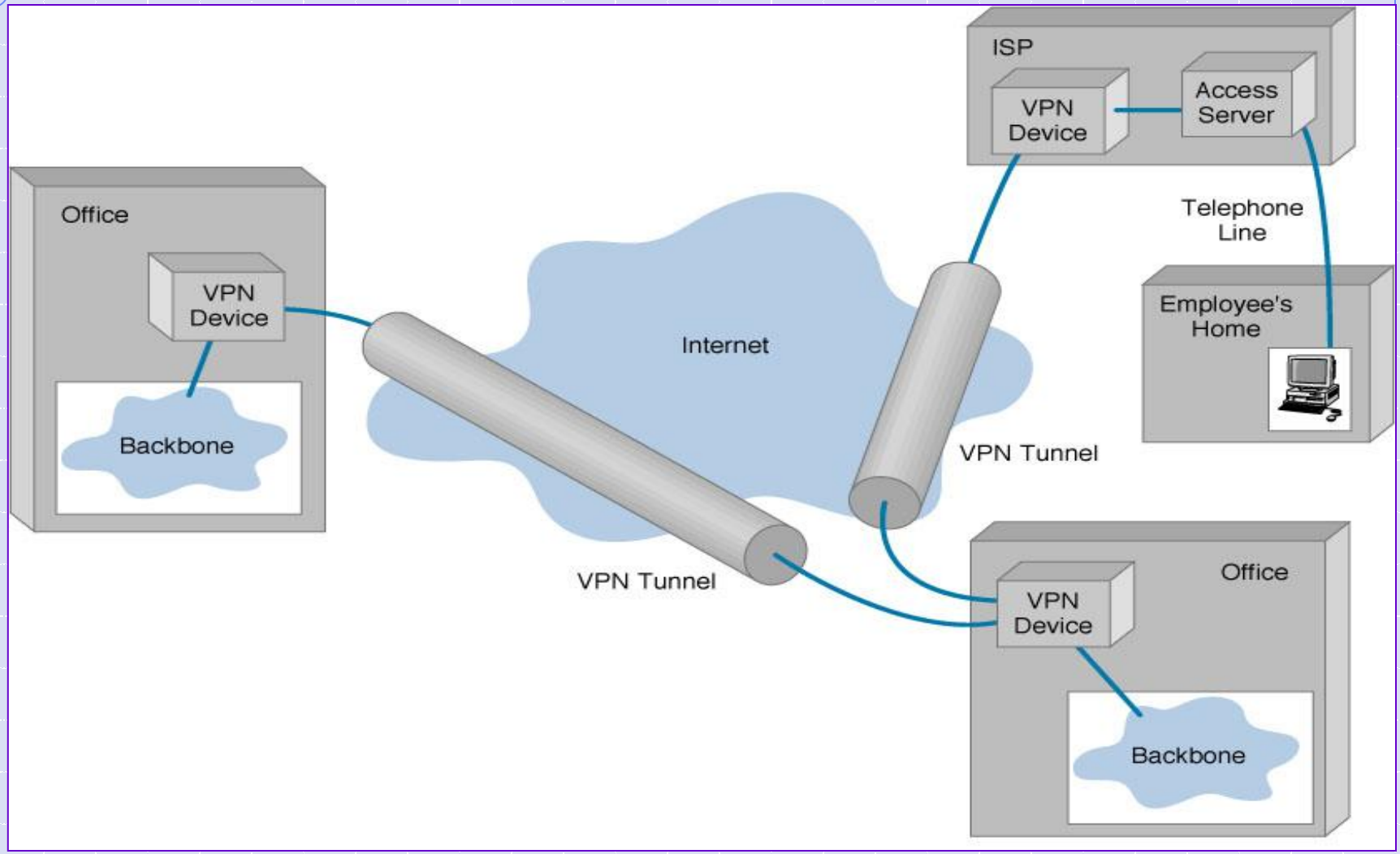


Data Encapsulation [From Comer]

Protocols used in VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security

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

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

Advantages: Scalability

- Flexibility of growth
- Efficiency with broadband technology

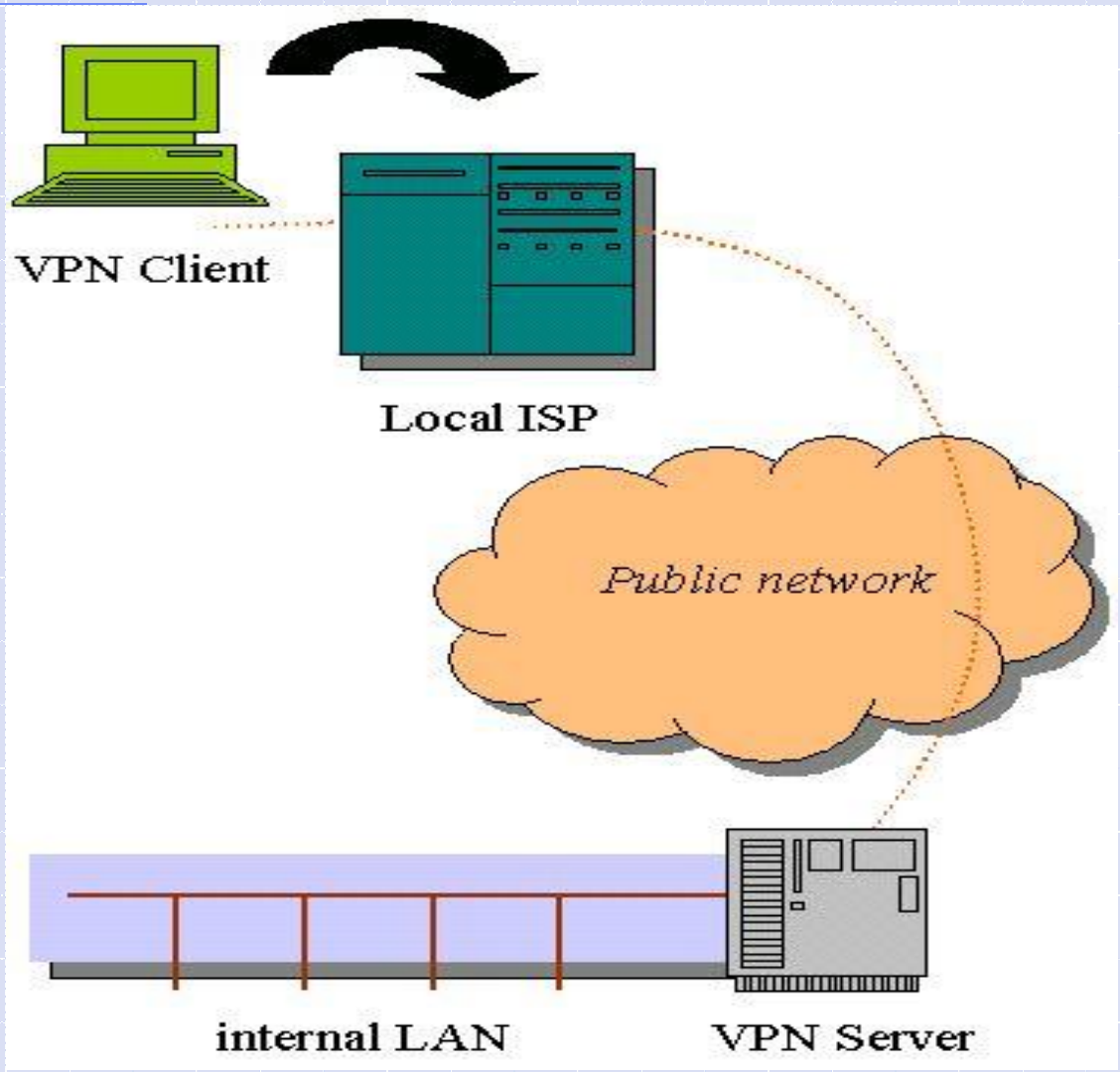
Disadvantages

- 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

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

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.
- Managed Security Service providers