LAN Technology

Virtual LAN Protocol

Arash Habibi Lashkari
PHD of Computer Science - Information Security
July 2010

Virtual LAN Protocol

Outlines:

VLAN: Virtual Local Area Network and the IEEE 802.1Q

IEEE 802.1P: LAN Layer 2 QoS/CoS protocol for Traffic Prioritization

PPTP: Point to Point Tunneling Protocol

L2TP: Level 2 Tunneling Protocol

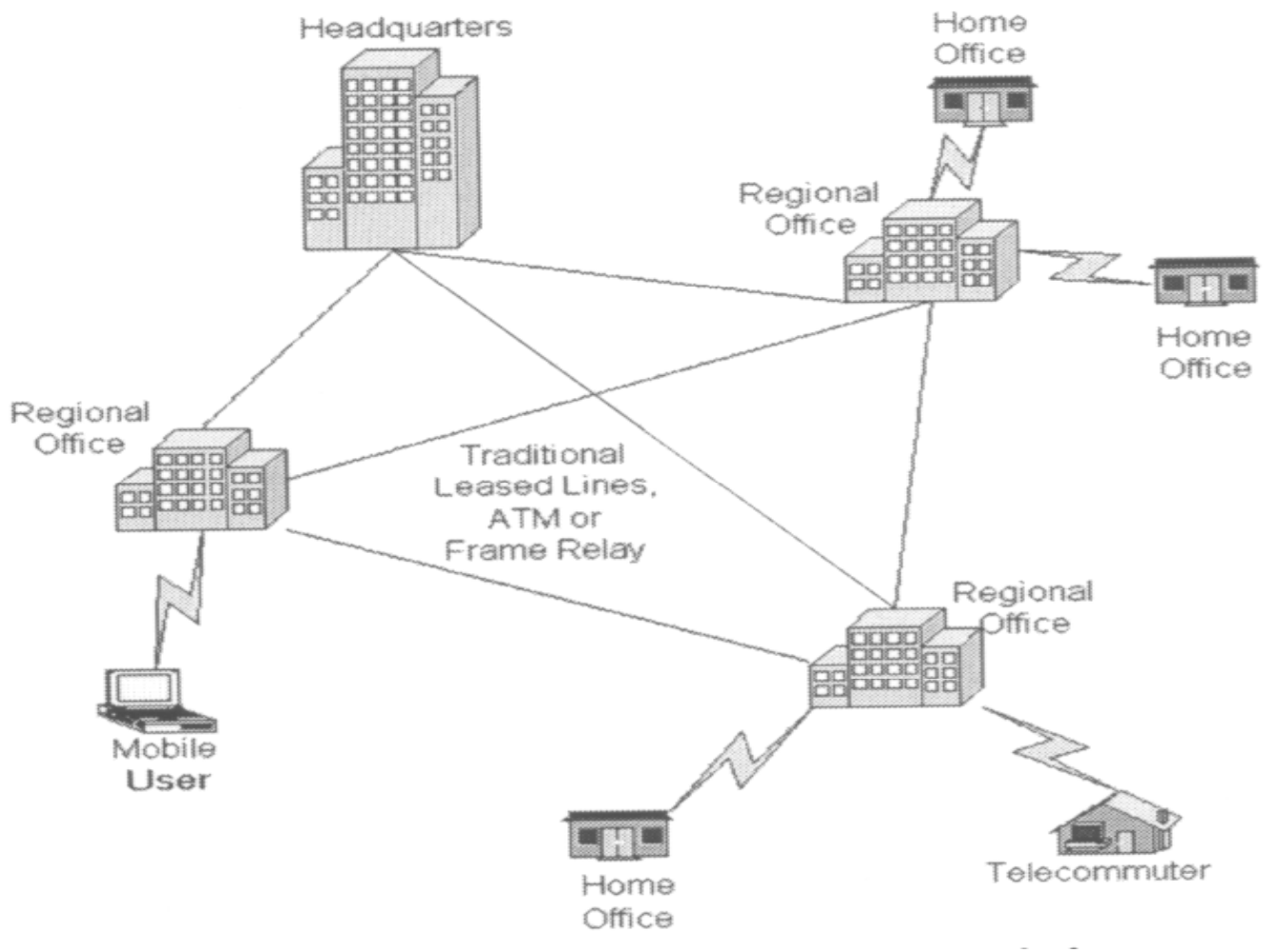
IPSec: IP Security

GMRP: GARP Multicast Registration Protocol

GARP: Generic Attribute Registration Protocol

GVRP: CARP VLAN Registration Protocol

Traditional Connectivity



[From Gartner Consulting]

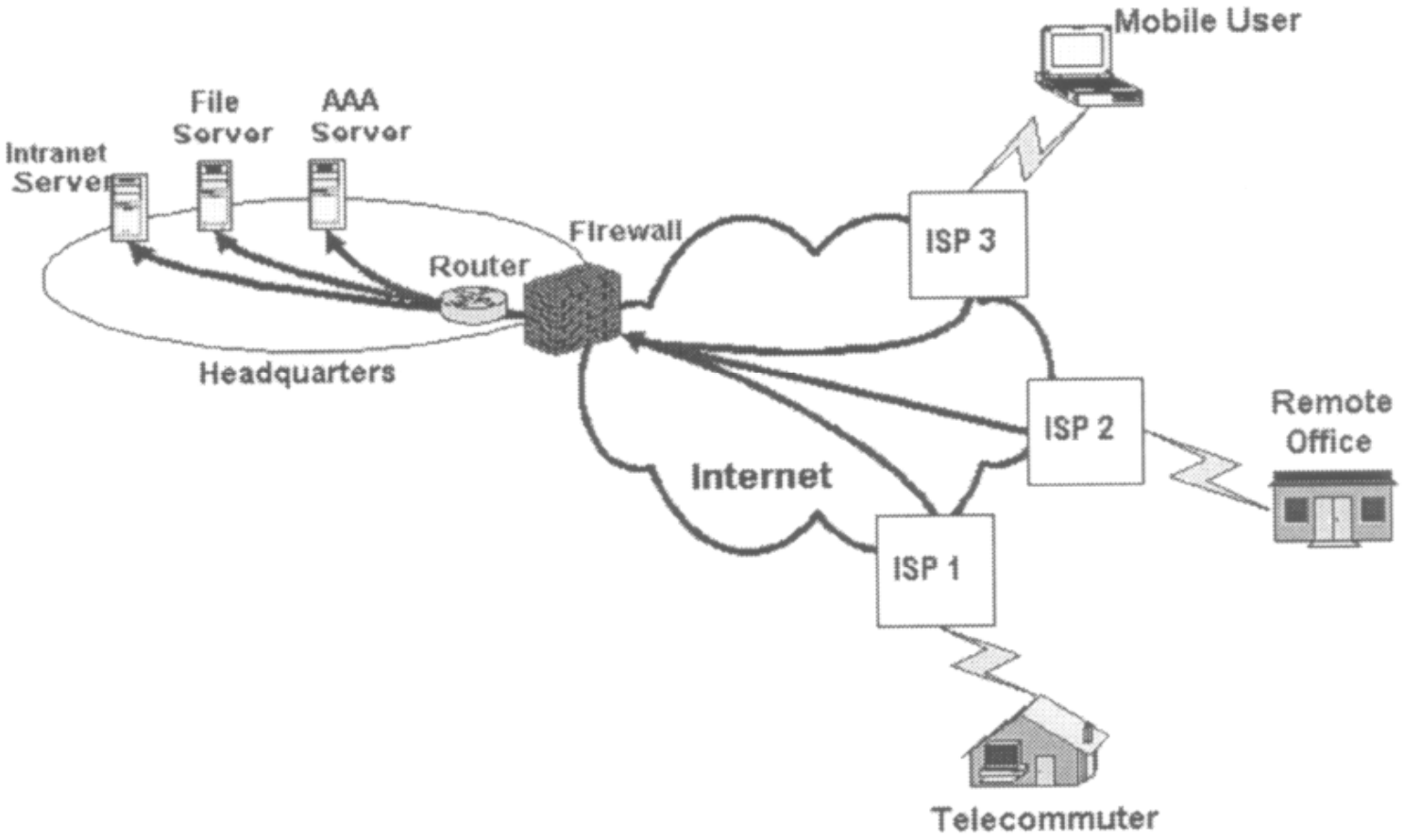
What is VPN?

- 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



(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.

Four Critical Functions

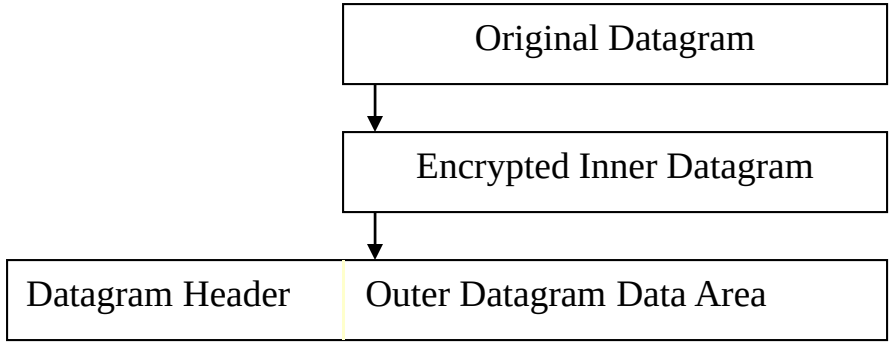
- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

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 [From Comer]

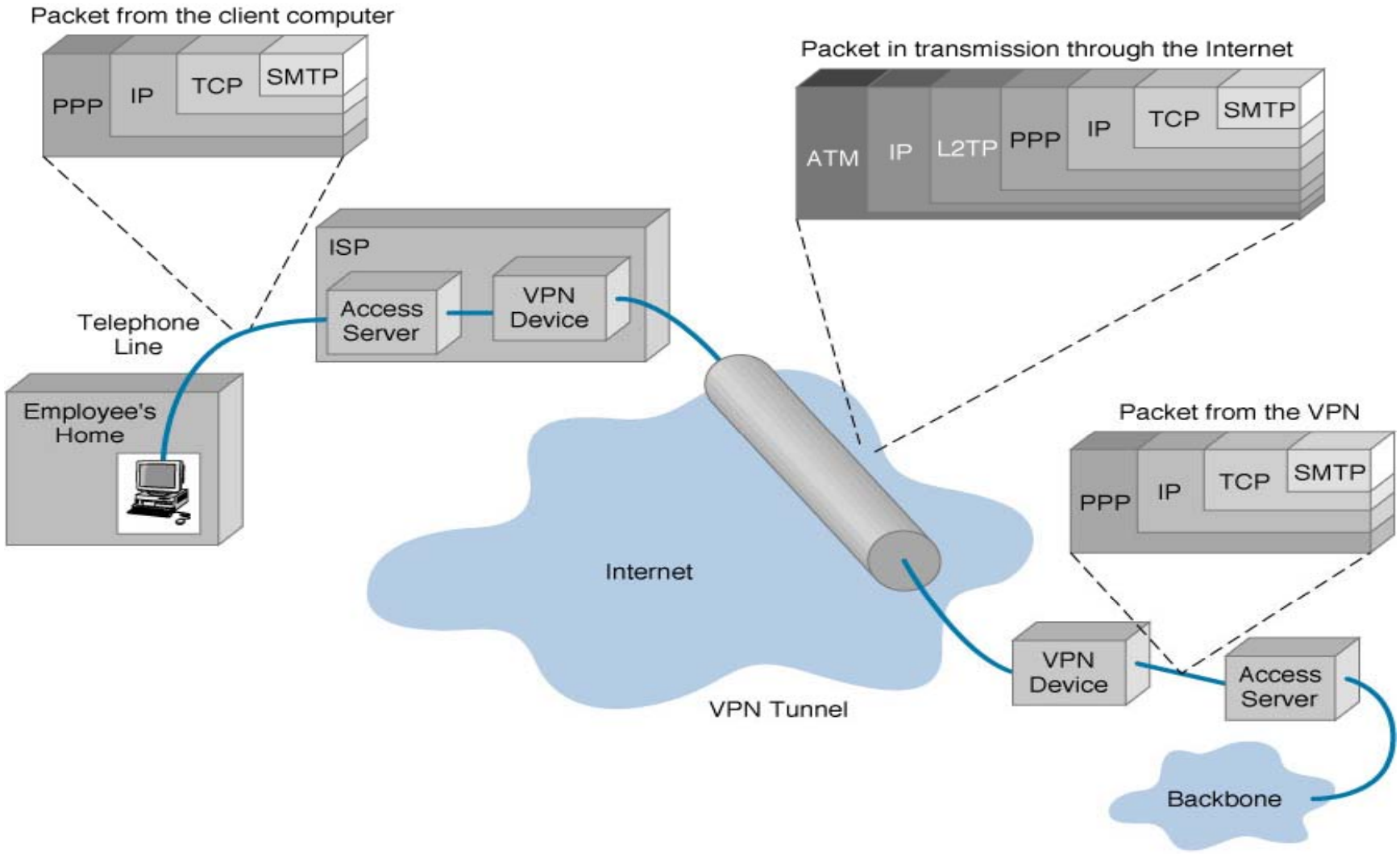
Two types of end points:

- 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

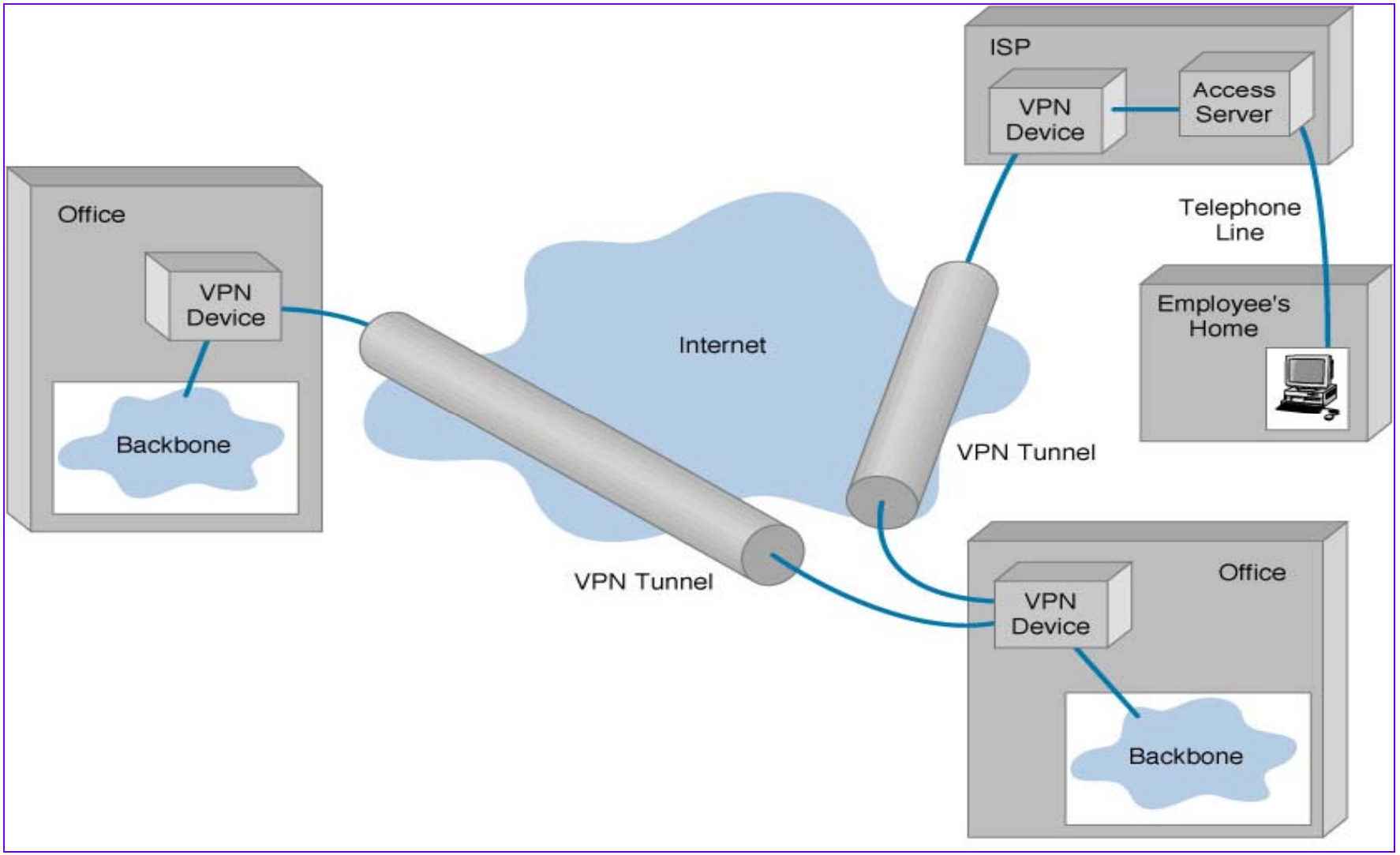
VPN Encapsulation of Packets



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

Advantages: Scalability

- Flexibility of growth
- Efficiency with broadband technology

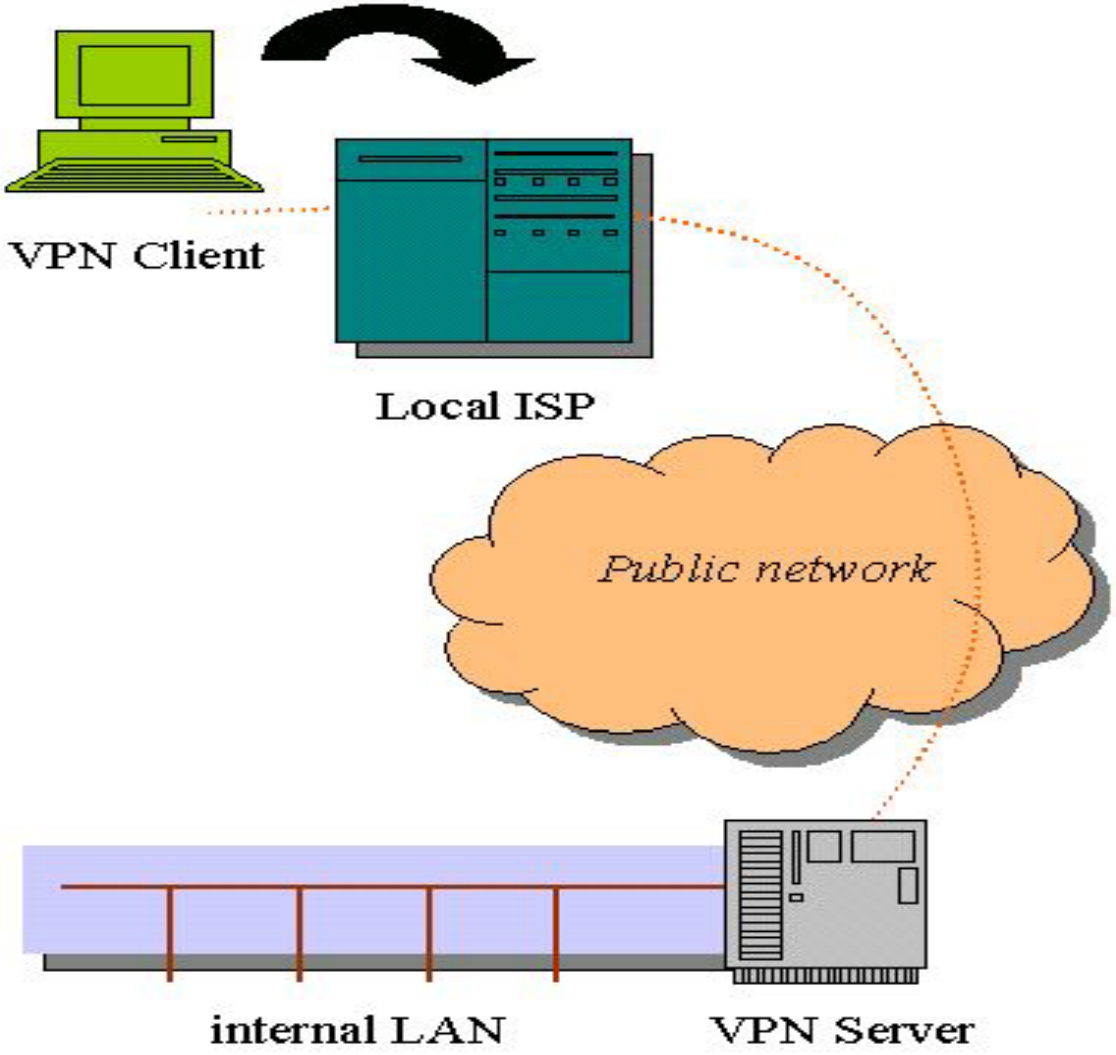
Disadvantages

- 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

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.

PPTP vs. L2TP

PPTP requires that the transit internetwork be an IP internetwork. L2TP requires only that the tunnel media provide packet-oriented point-to-point connectivity.

When header compression is enabled, L2TP operates with 4 bytes of overhead, compared to 6 bytes for PPTP.

L2TP provides tunnel authentication, while PPTP does not.

PPTP uses PPP encryption and L2TP does not.

LAB

Follow Lab 6 by Packet Tracer

Questions