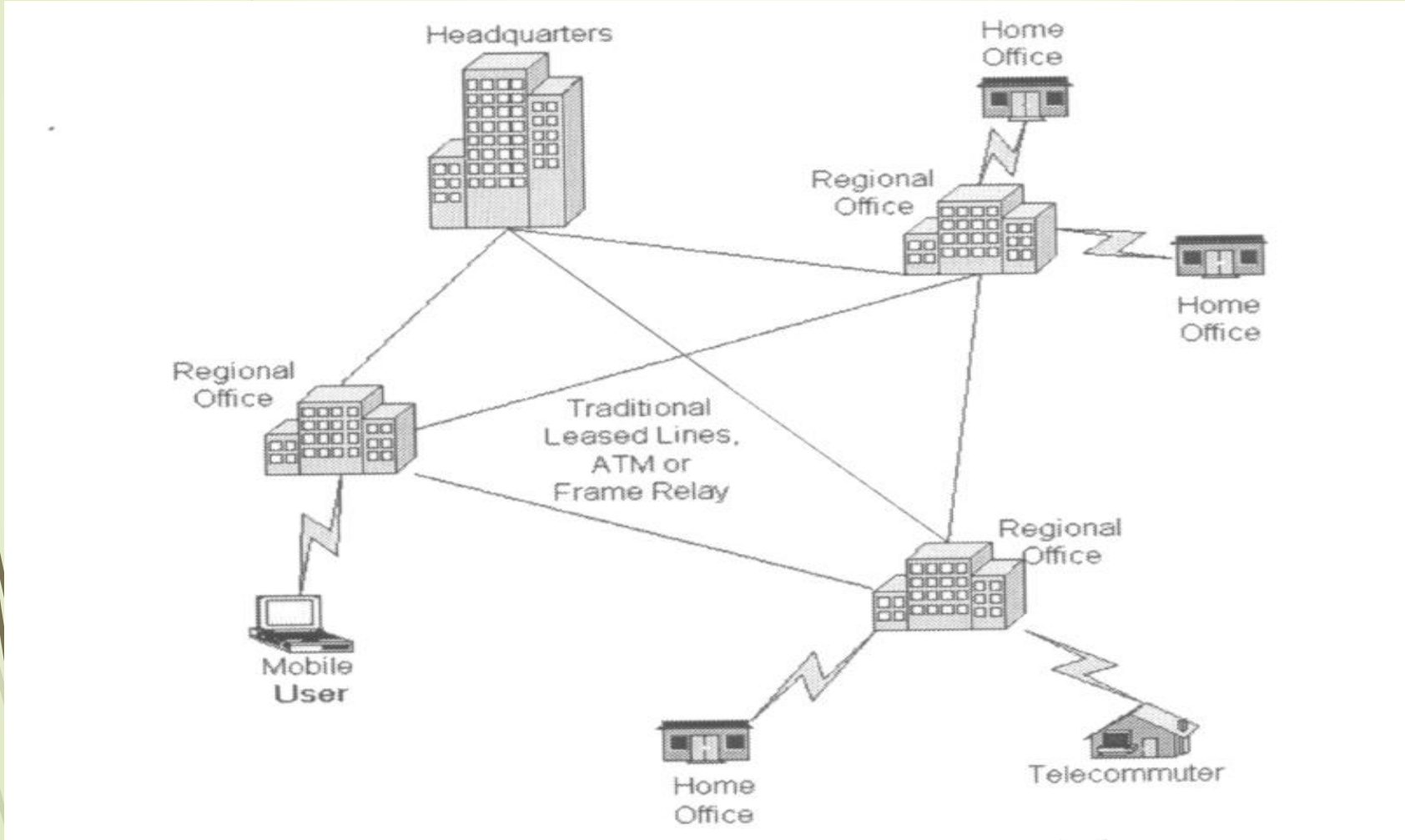
VIRTUAL PRIVATE NETWORKS (VPN)

Traditional Connectivity



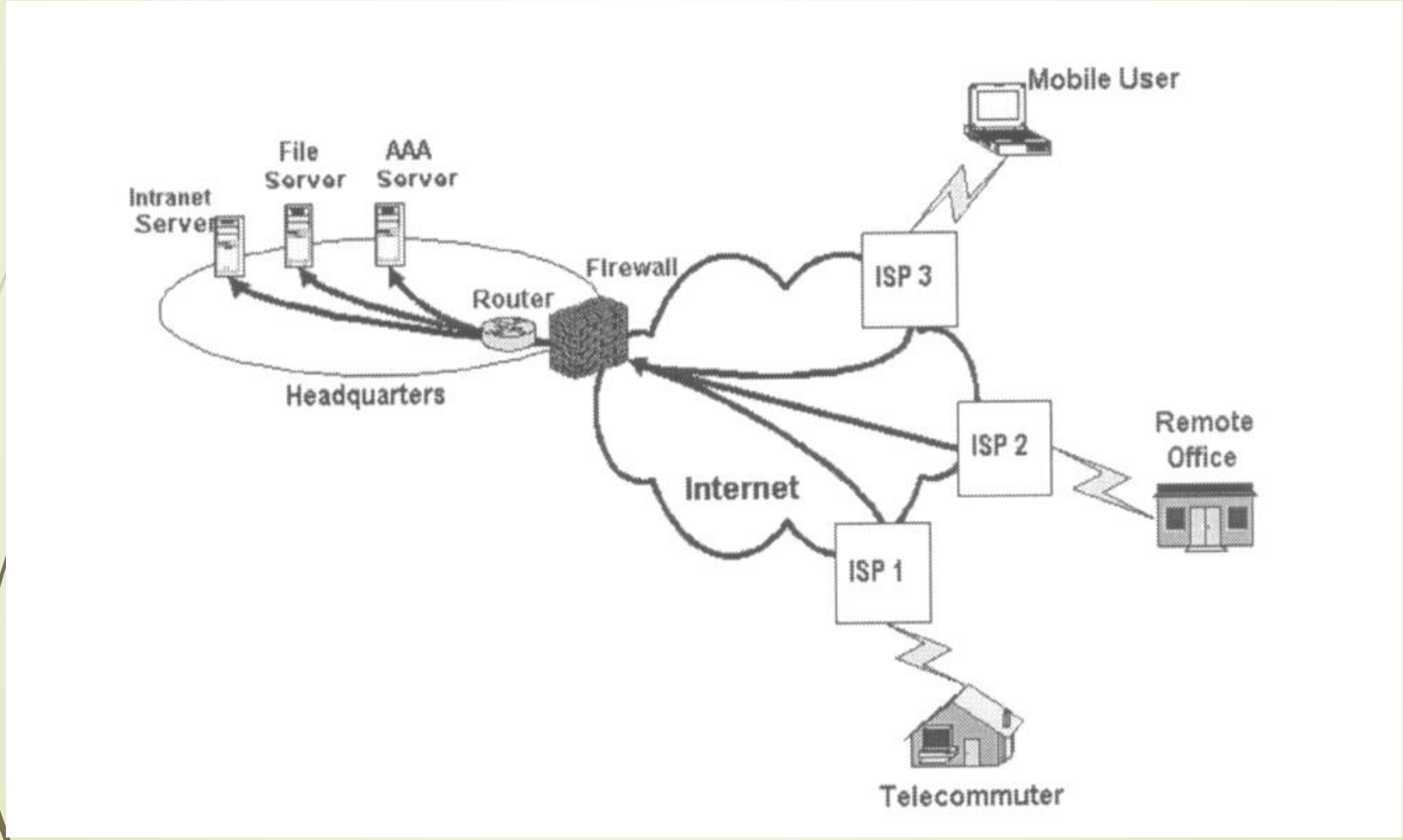
What is VPN?

- 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

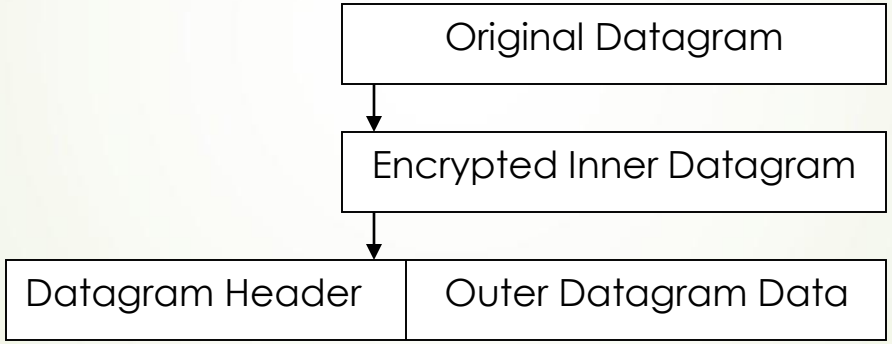
- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

Encryption

- Encryption -- is a method of "*hashing*" 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.



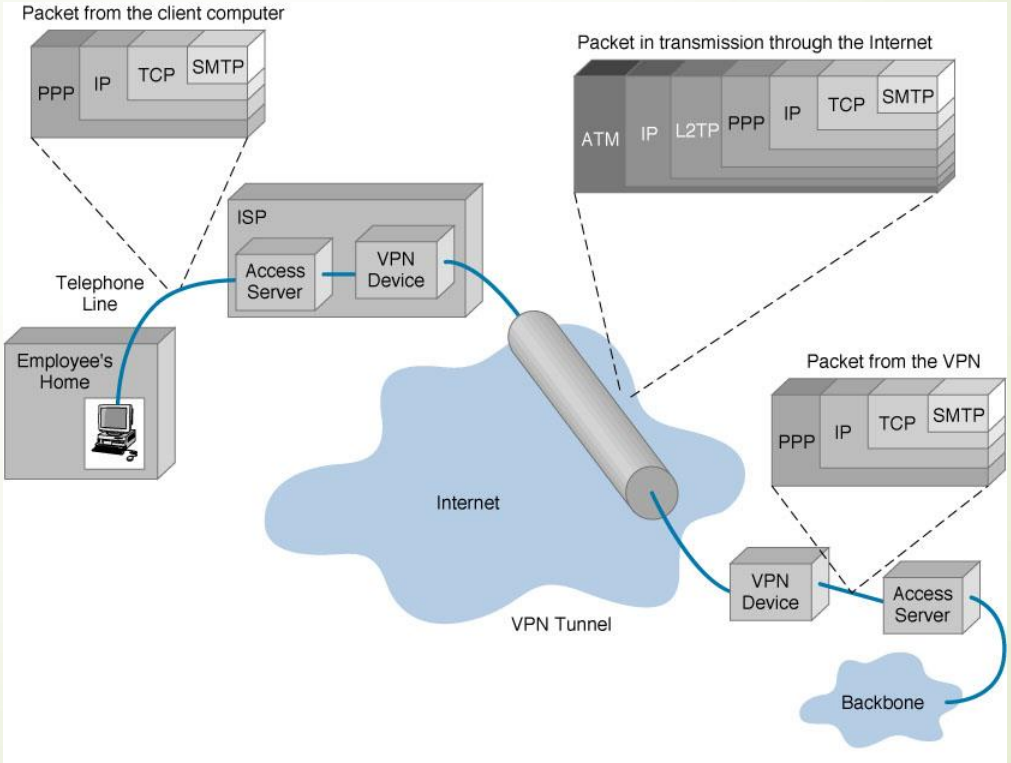
Two types of end points:

- 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

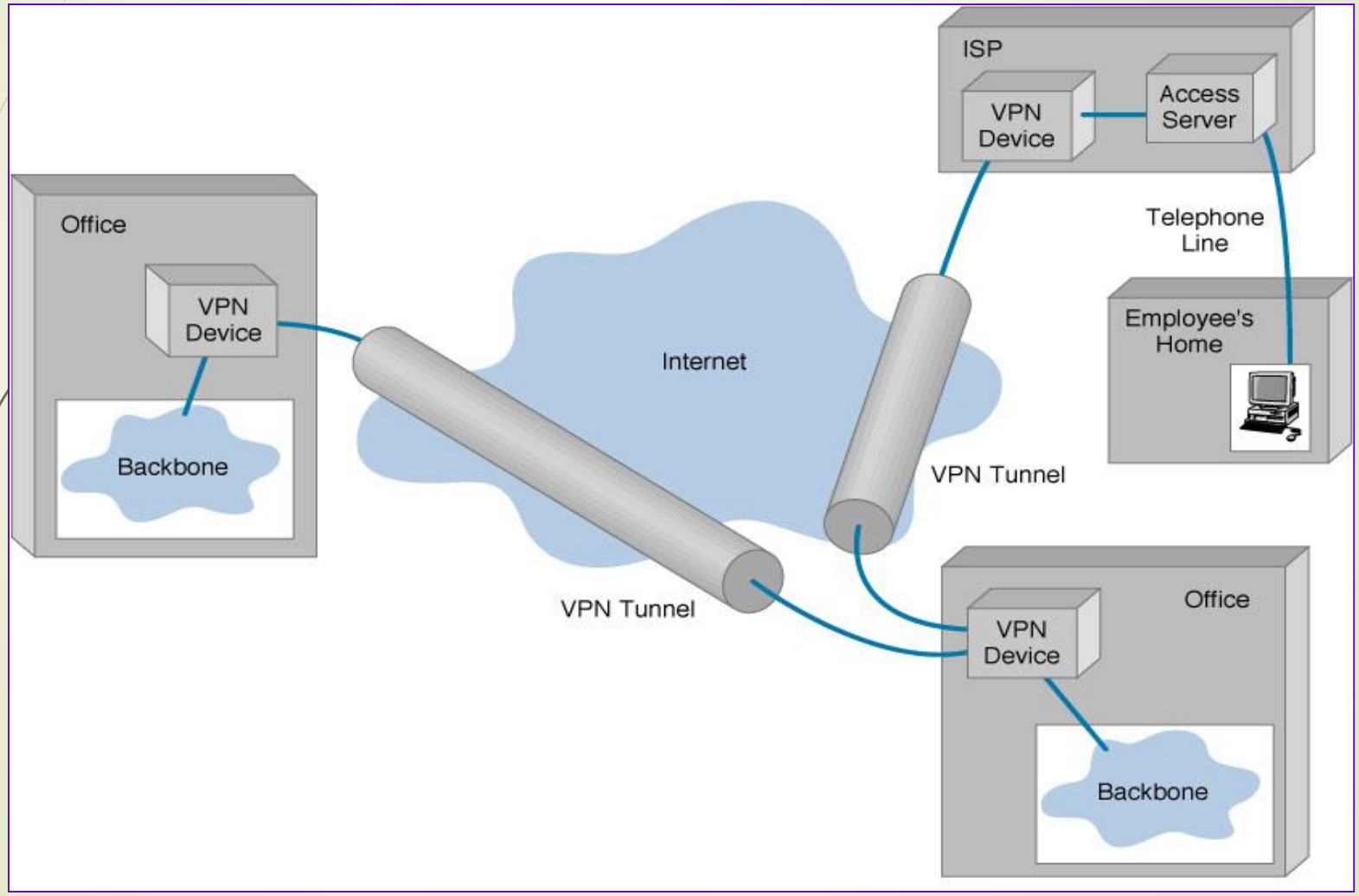


Types of Implementations

- 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 charges for remote access.
- Transferring the support to the service providers
- Operational costs

Advantages: Scalability

- Flexibility of growth
- Efficiency with broadband technology

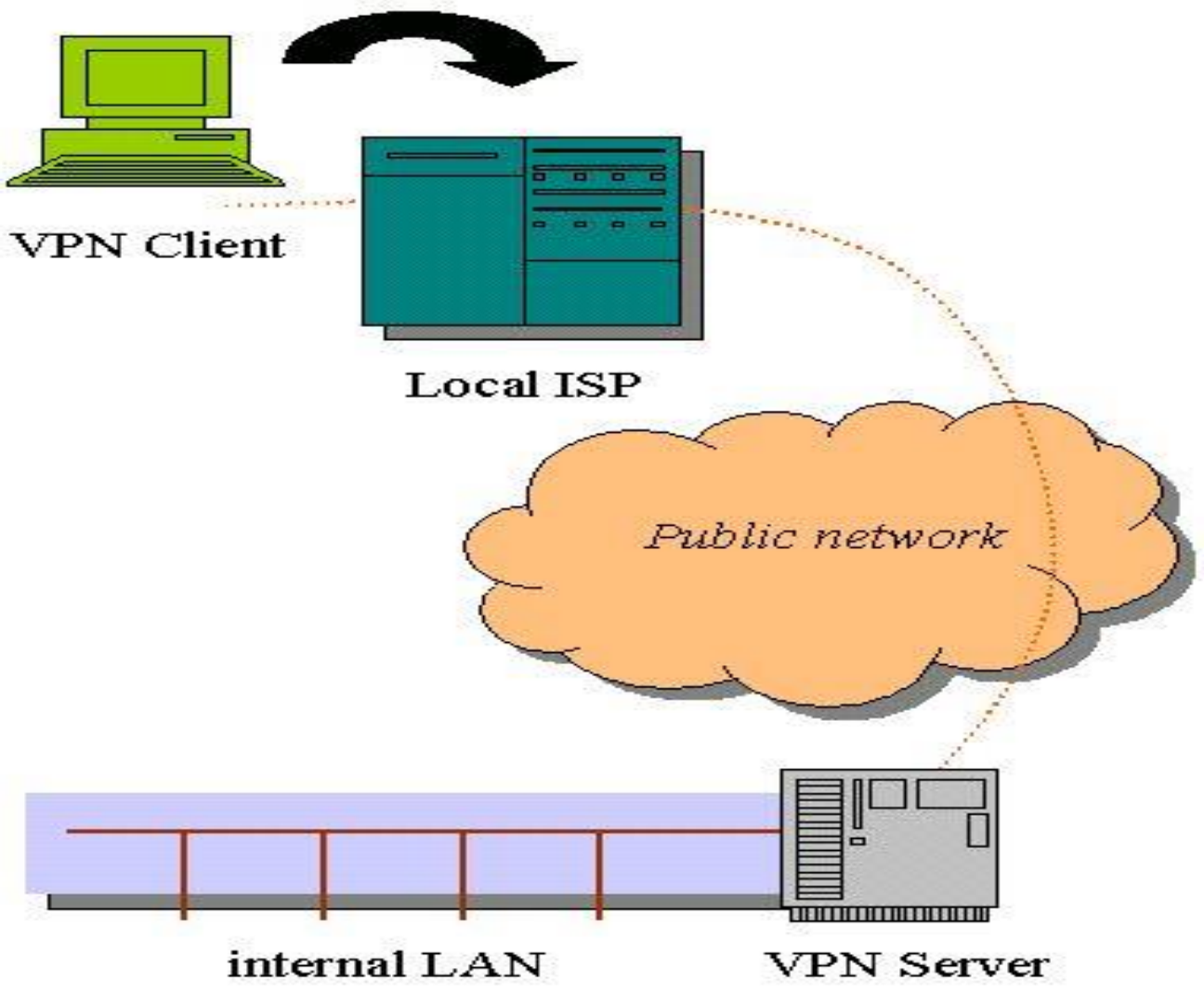
Disadvantages

- 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



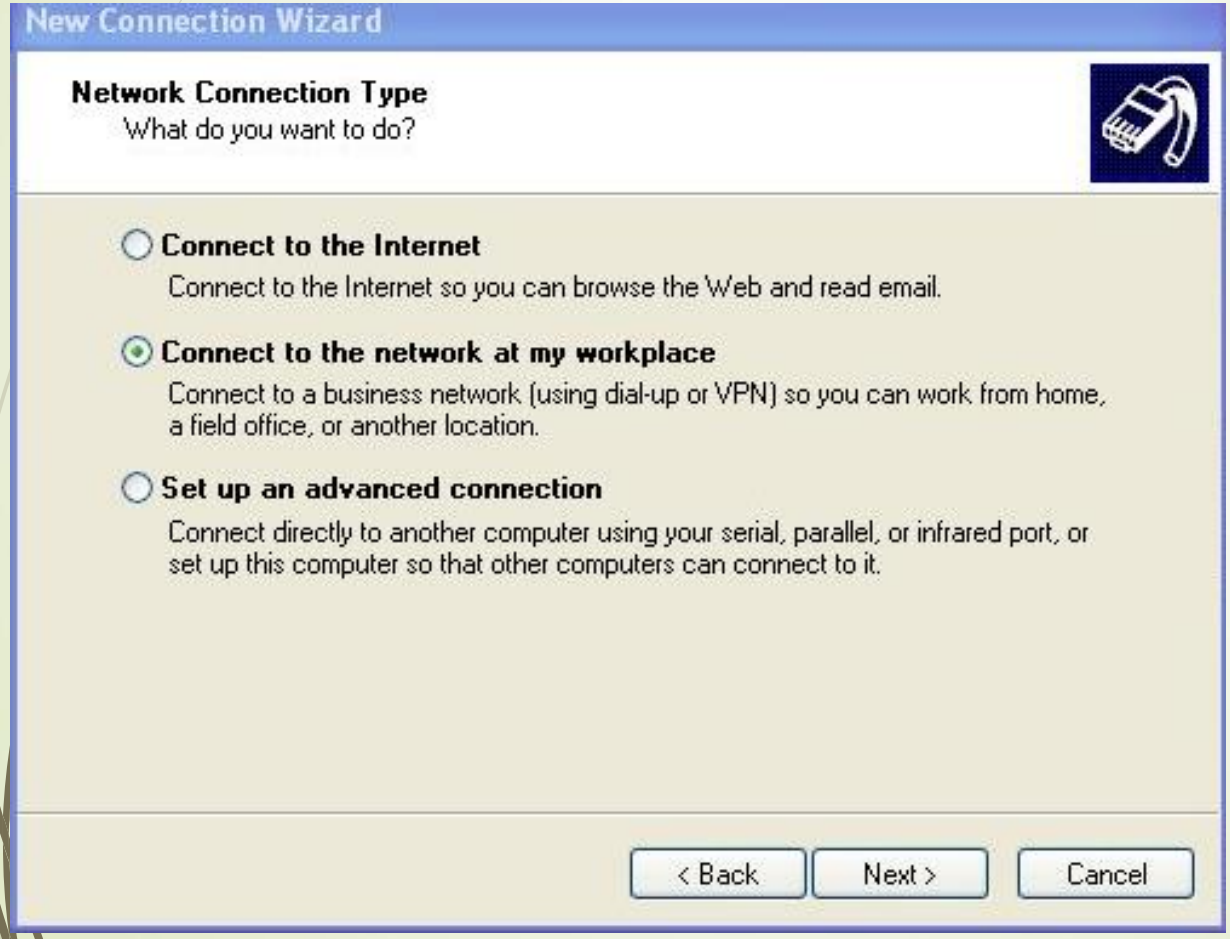
VPN Demonstration

Click on Start – select Network Connections

VPN Demonstration

In Network Connections on the left hand side there is a link to “Create New Connection” – click on this and a wizard will pop up assisting the user

VPN Demonstration

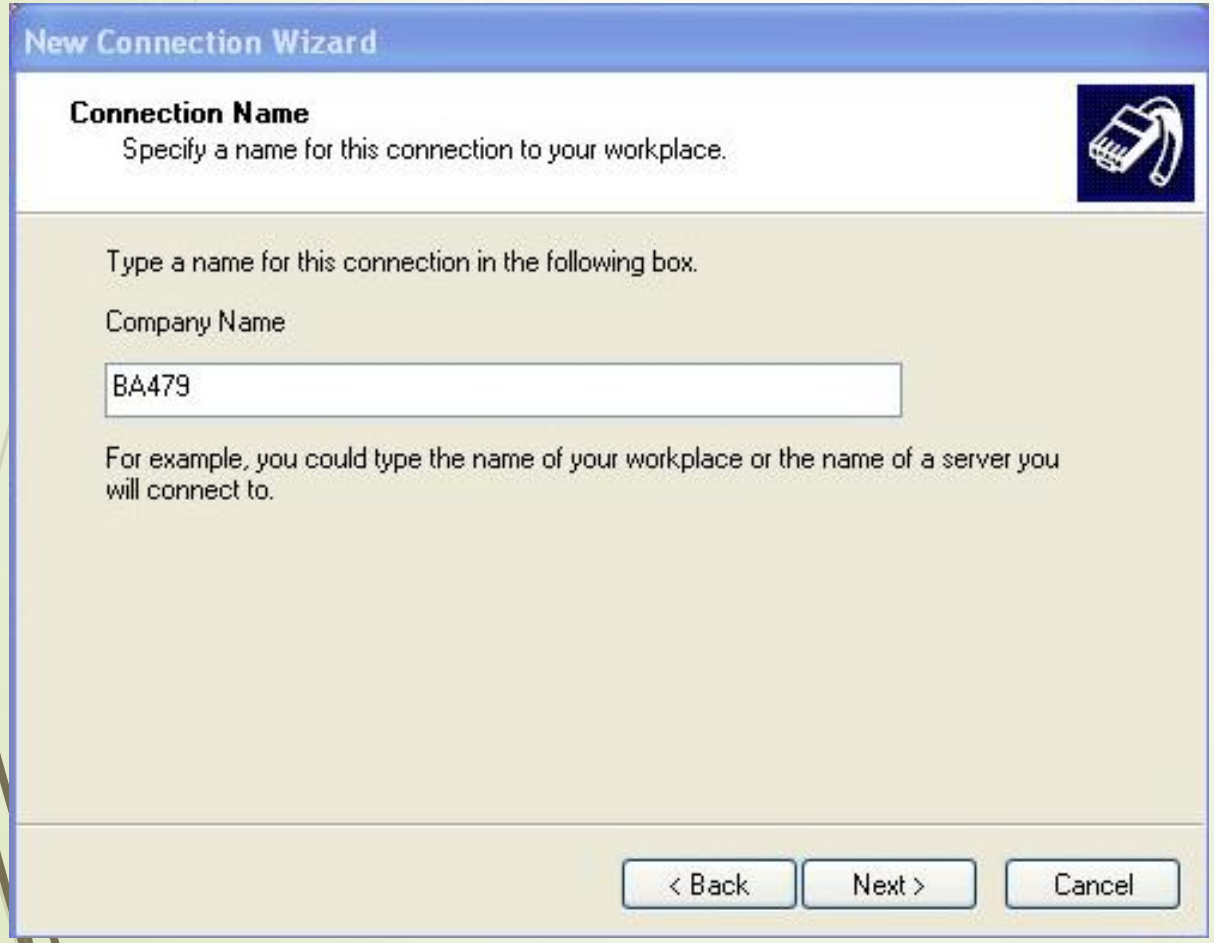


Select "Connect to the Network at my Workplace"

VPN Demonstration

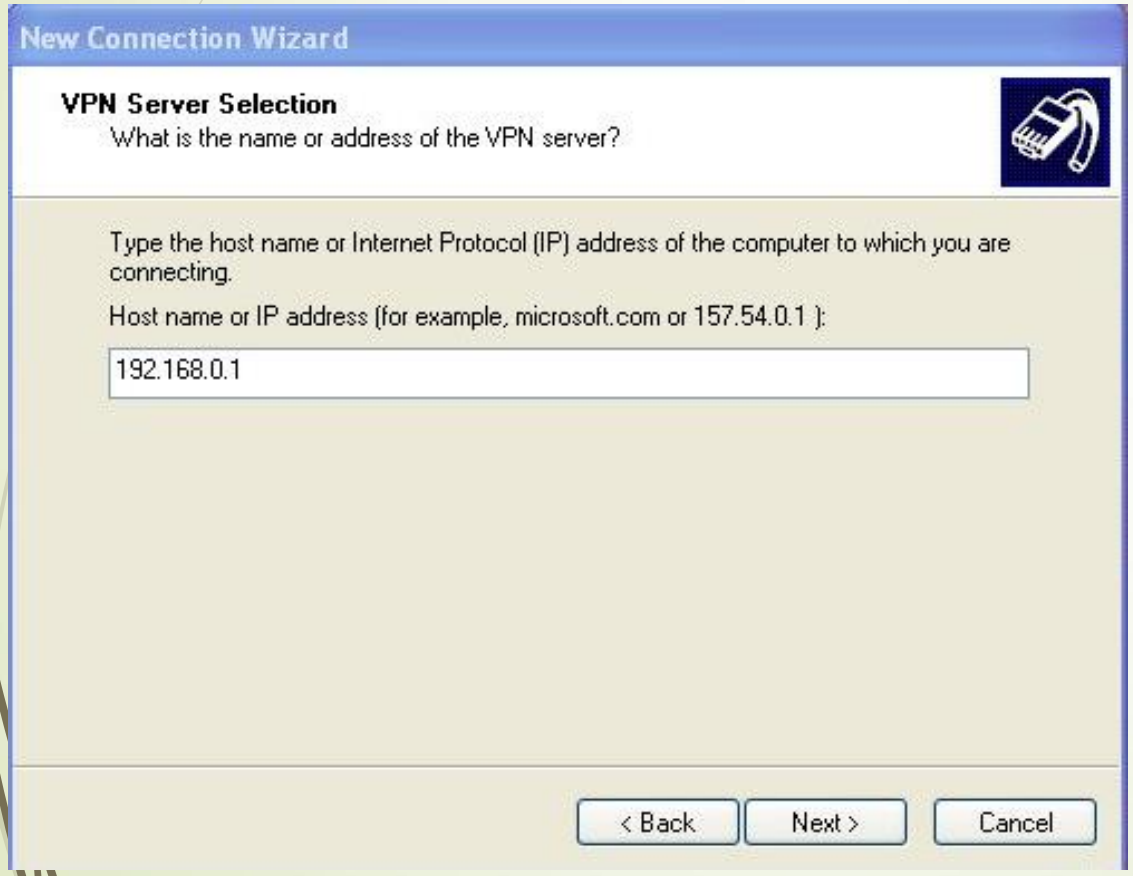
Select “Virtual Private Network Connection”

VPN Demonstration



Make a name for this connection that you are establishing – to distinguish this connection from other VPN connections that might already be established

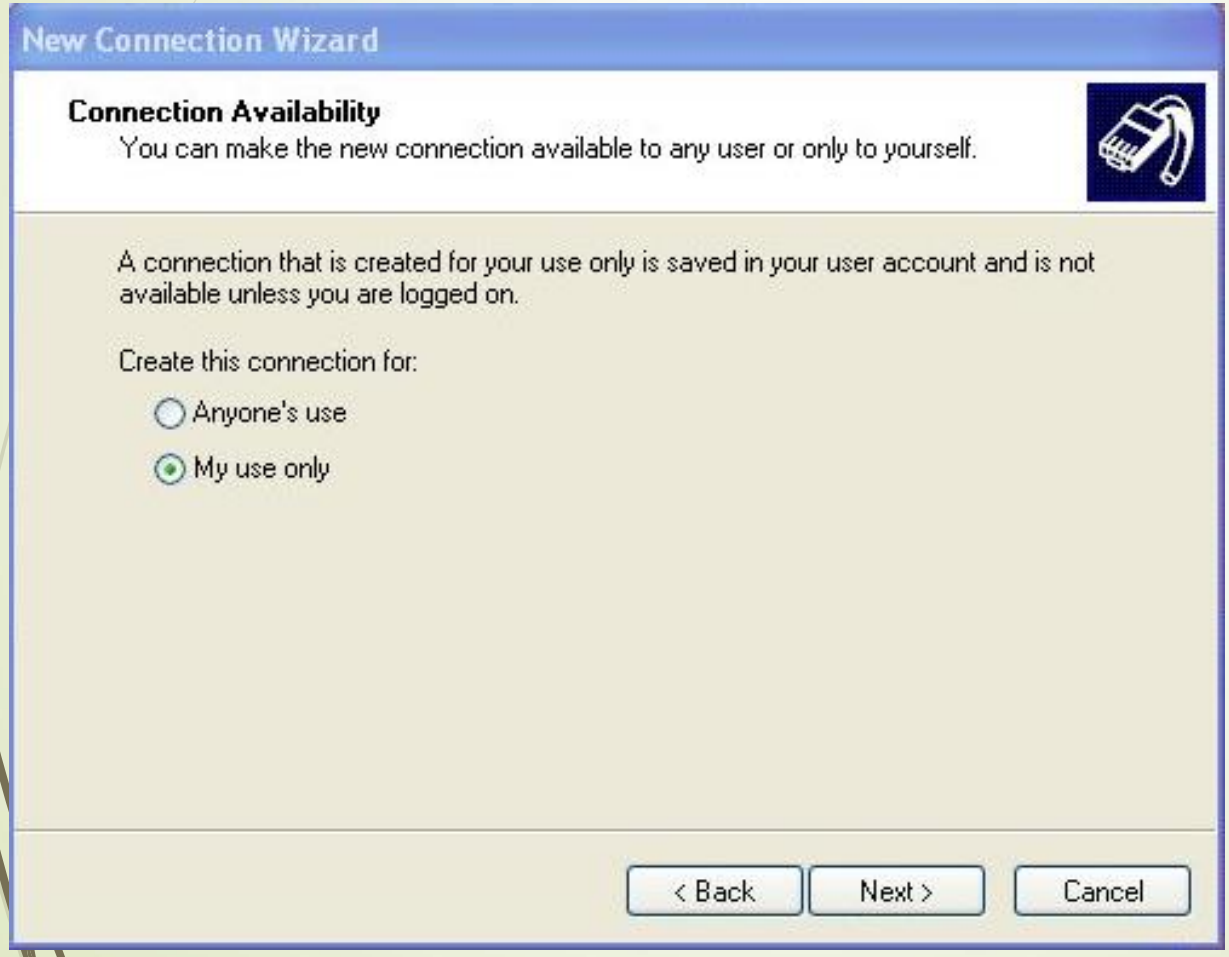
VPN Demonstration



For this demonstration I am trying to connect to my wireless router off campus therefore the IP address that I insert is the IP address for my router which I can find out by running an ipconfig and it is the IP address for your default gateway

NOTE: Not all routers will allow users to VPN into it

VPN Demonstration



Personal preference as to whether or not you want other users to be able to use this VPN connection on this computer

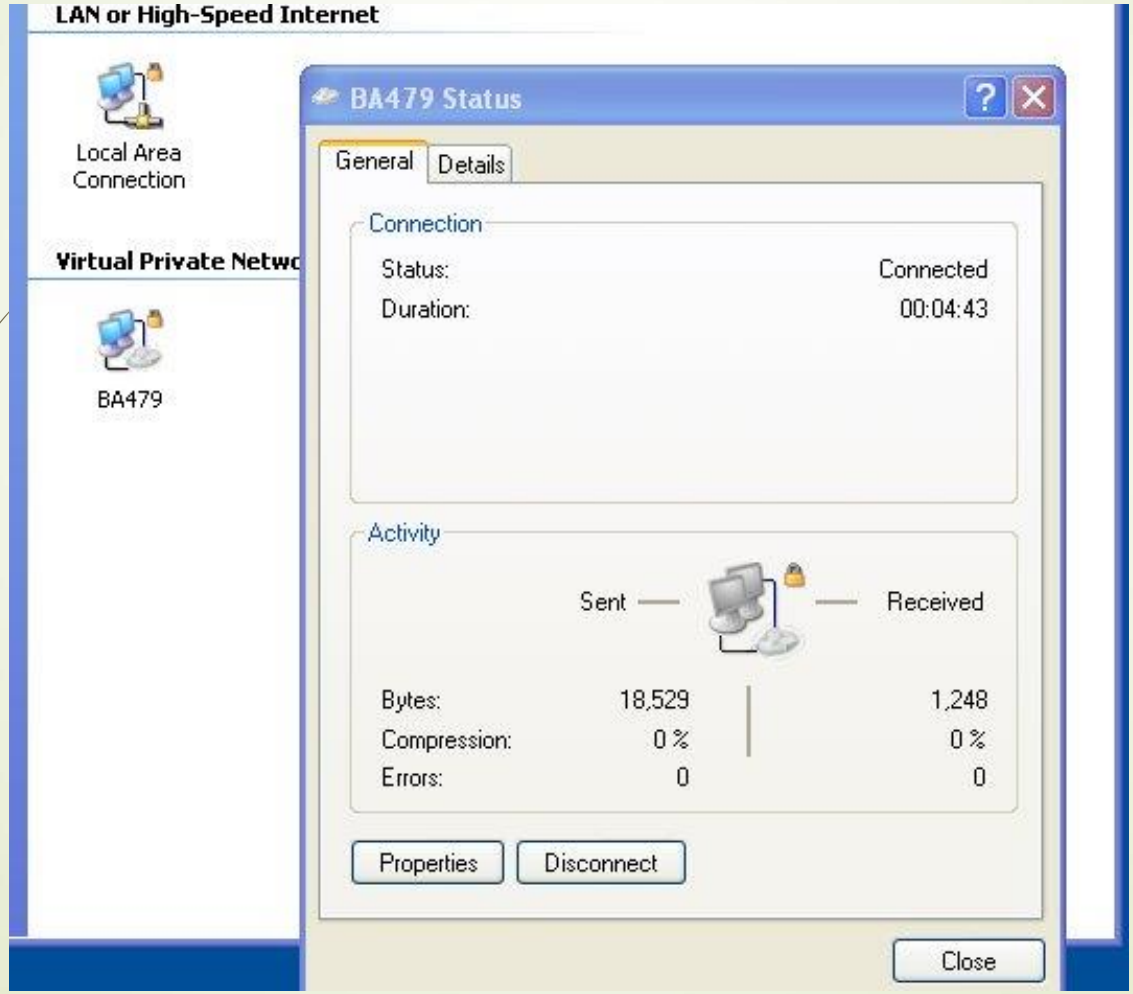
VPN Demonstration

VPN Demonstration

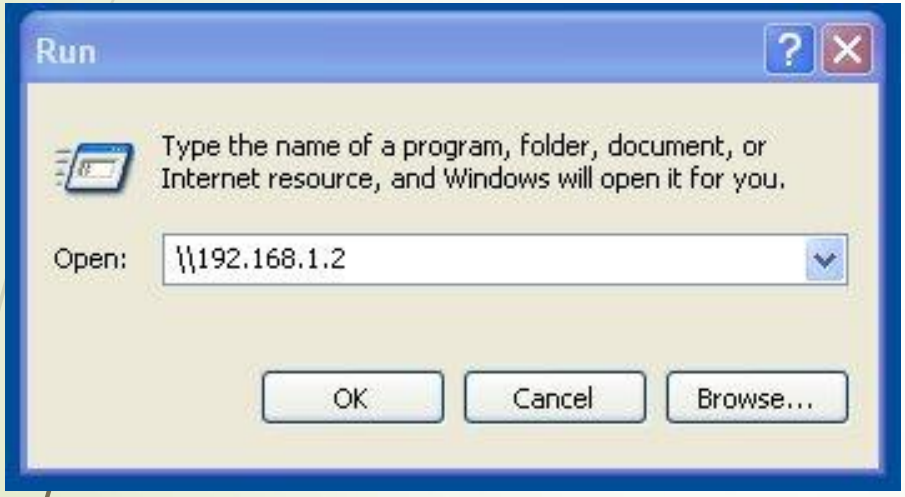
VPN Demonstration

This is a profile (username and password) that has already been created on your router – which can be created by typing in the IP address of your router in a web browser

VPN Demonstration



VPN Demonstration

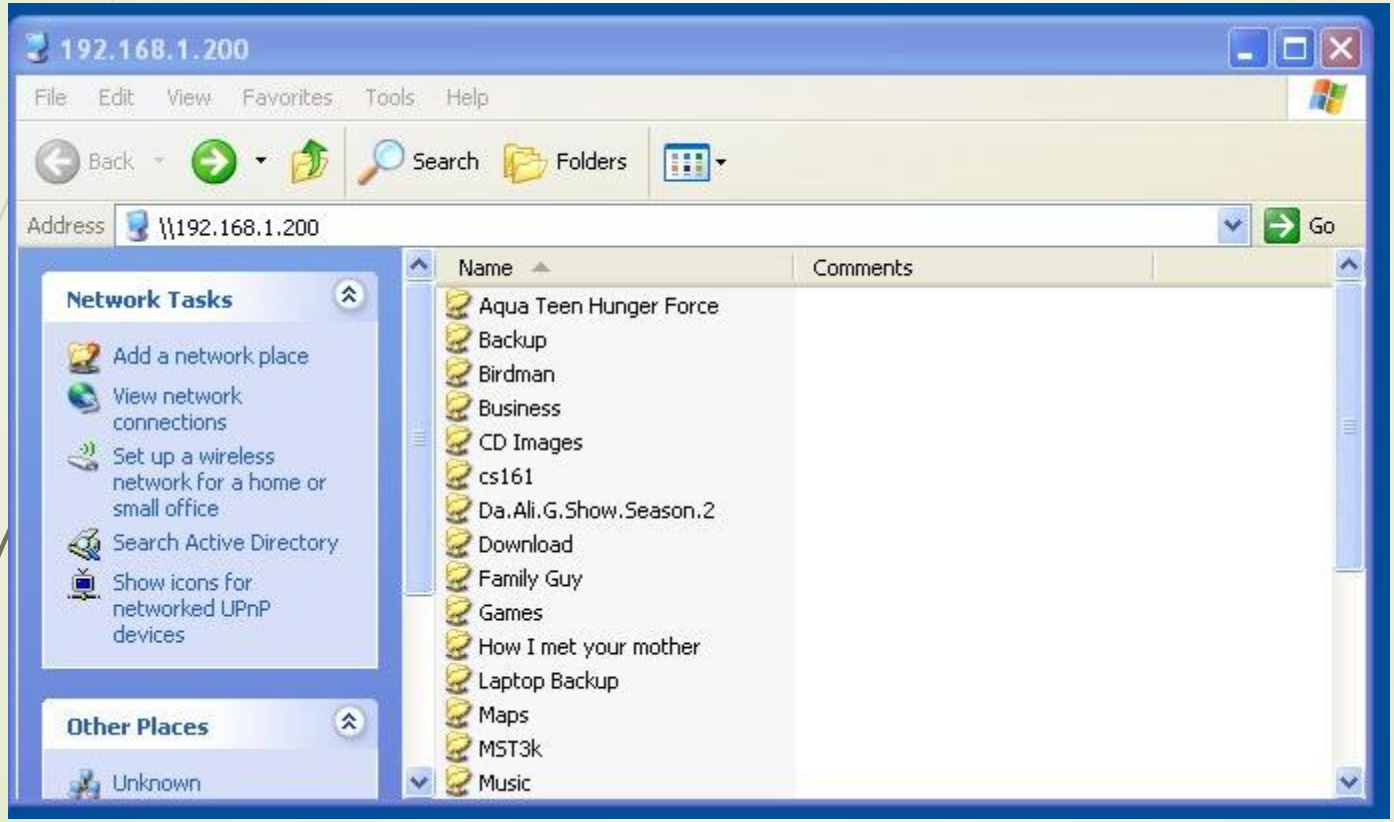


In Start – Run insert the IP address of the computer that you want to access that is connected to the router

VPN Demonstration

Using the same username and password already established for the router you can connect to this specific computer

VPN Demonstration



These are only the files that are “shared” on this computer

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.

VPN Best Practices

- Use a real firewall
- Secure the base operating system
- Use a single ISP (minimize routing hops and insure cooperation)
- Use packet filtering to reject unknown hosts
- Use public-key encryption and secure Authentication
- Compress before you encrypt (stream compression will help overall performance)
- Secure remote hosts

SSL Based VPNs

- Browser based
  - PositivePRO – Positive Networks ; Connectra – Checkpoint Software
    - No special client needed
      - can be used on any device that is web enabled that supports SSL (PDA, Cell phones...)
      - OS independent
    - Can't access desktop applications
  - Netifice
    - Browser based
    - Java Agent Based
    - SSL Windows client for desktop access
  - SSL-Explorer – Open Source

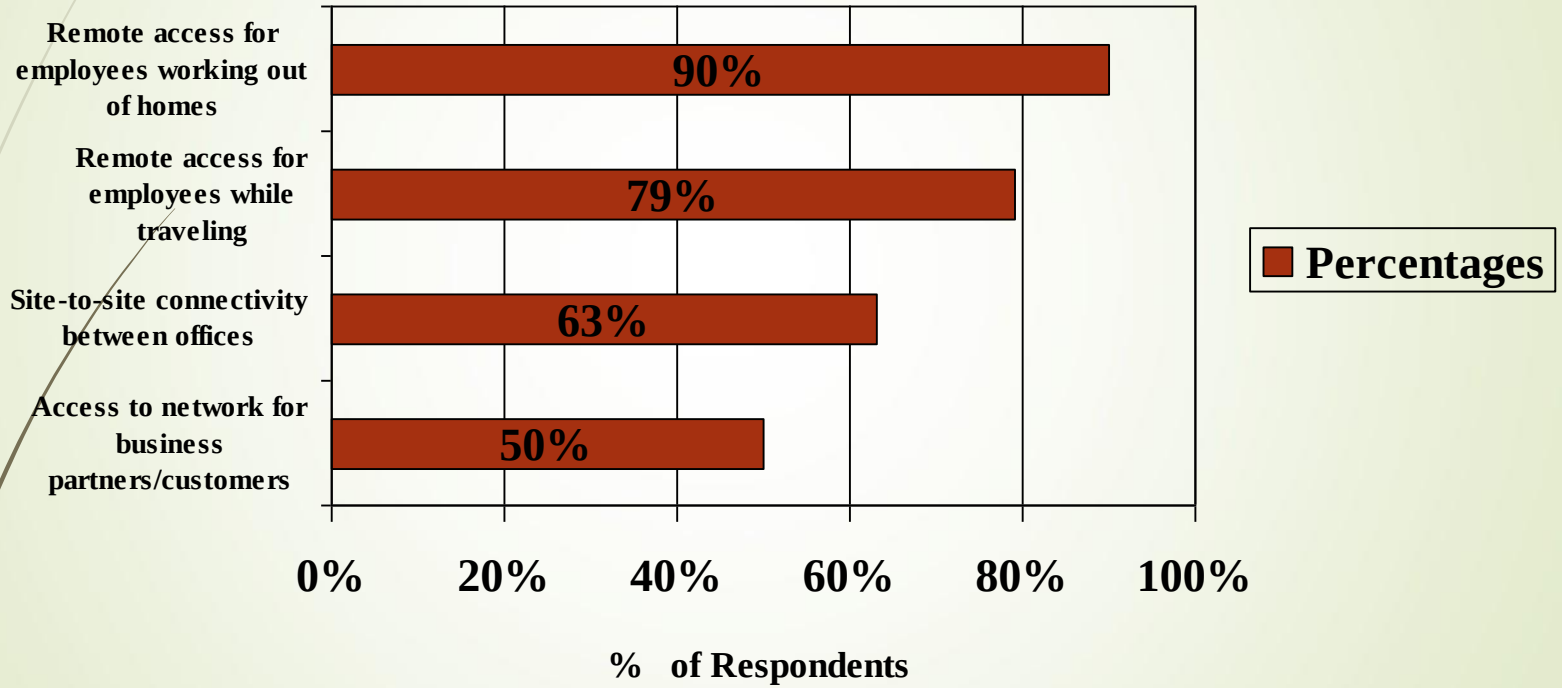
SSL Based VPNs

- Non-browser based
  - OpenVPN
    - requires client software be installed for each user
    - Open Source (free)
    - Runs on most OSs
    - compatible with with:
      - SSL/TLS
      - RSA Certificates
      - X509 PKI
      - NAT
      - DHCP
- https://github.com/hwdsl2/setup-ipsec-vpn
- https://kifarunix.com/how-to-configure-ipsec-vpn-using-strongswan-on-ubuntu-18-04/

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

Statistics From Gartner-Consulting*



*Source: www.cisco.com

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.