VPN: Virtual Private Network

Name: Israa Hussain
ID: 15501045

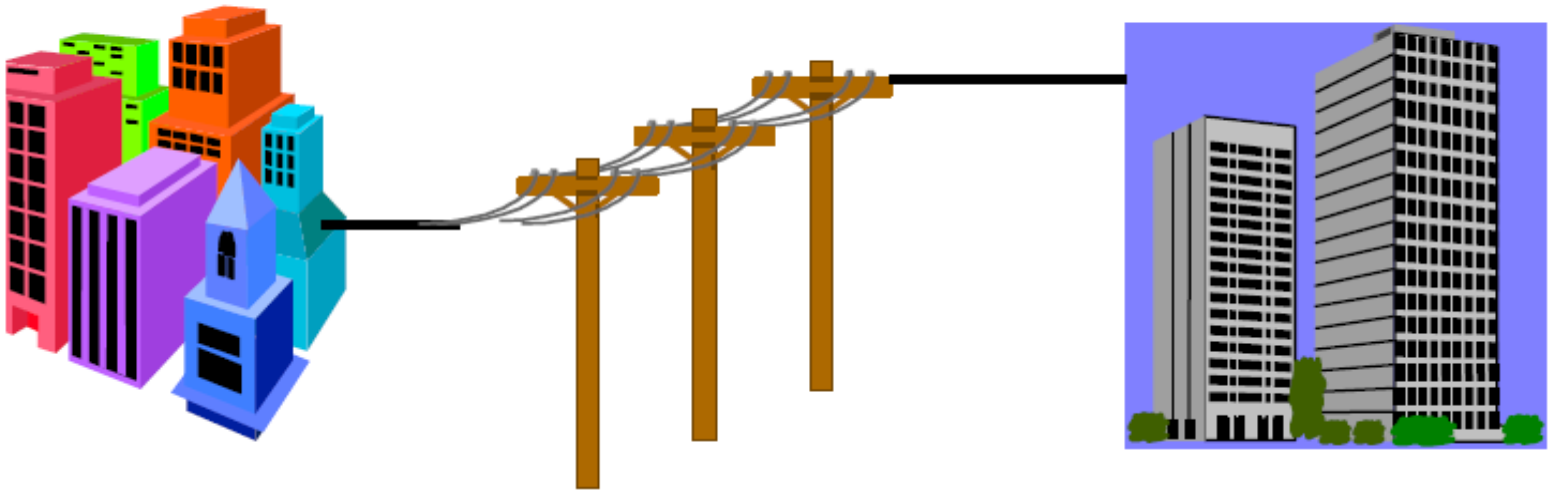
Introduction: What is a VPN?

- A VPN is a set of tools which allow networks at different locations to be securely connected, using a public network as the transport layer.
- A VPN is private network constructed within a public network infrastructure, such as the global Internet.
- VPNs use cryptography to provide protections against eavesdropping and active attacks.
- VPNs are most commonly used today for telecommuting and linking branch offices via secure WANs

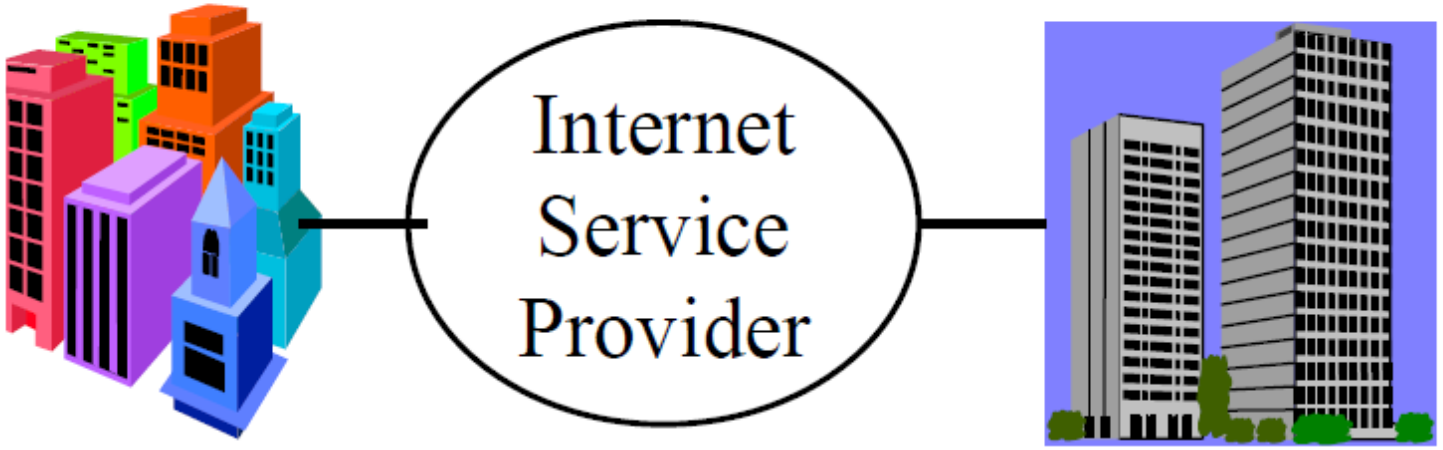
The Wide Area Network before VPNs

- Firms would spend thousands of dollars per month for private links to branch offices.
- The rise of the internet created cheap but insecure bandwidth.
- The VPN concept was to produce the virtual “dedicated circuit”, pump it over the internet, and use cryptography to make it secure.

Private Network: Uses leased lines



Virtual Private Network: Uses public Internet

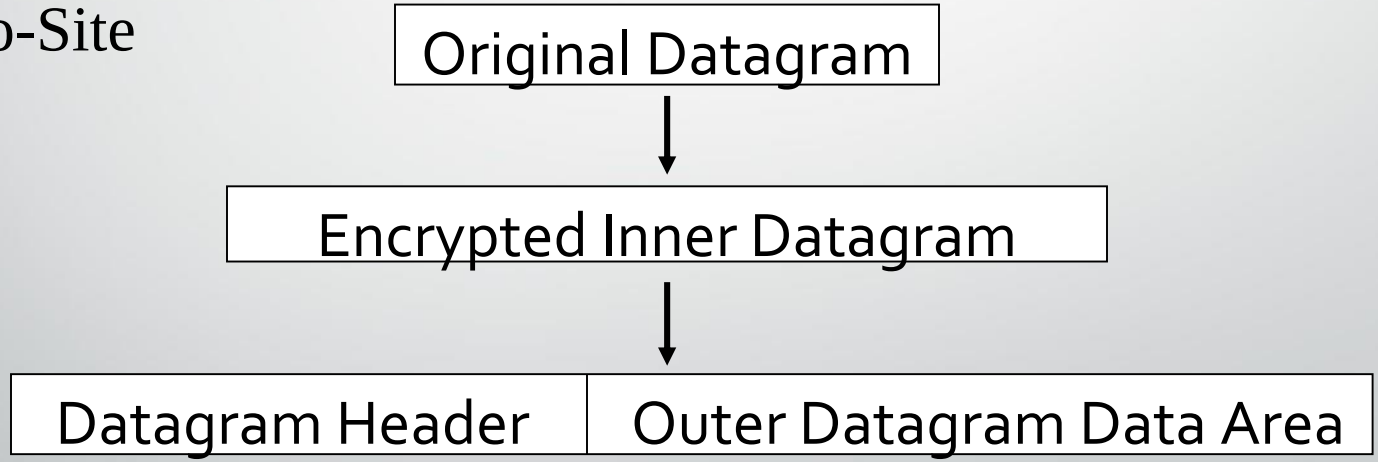


Tunneling

- A virtual point-to-point connection made through a public network. It transports encapsulated datagram's.

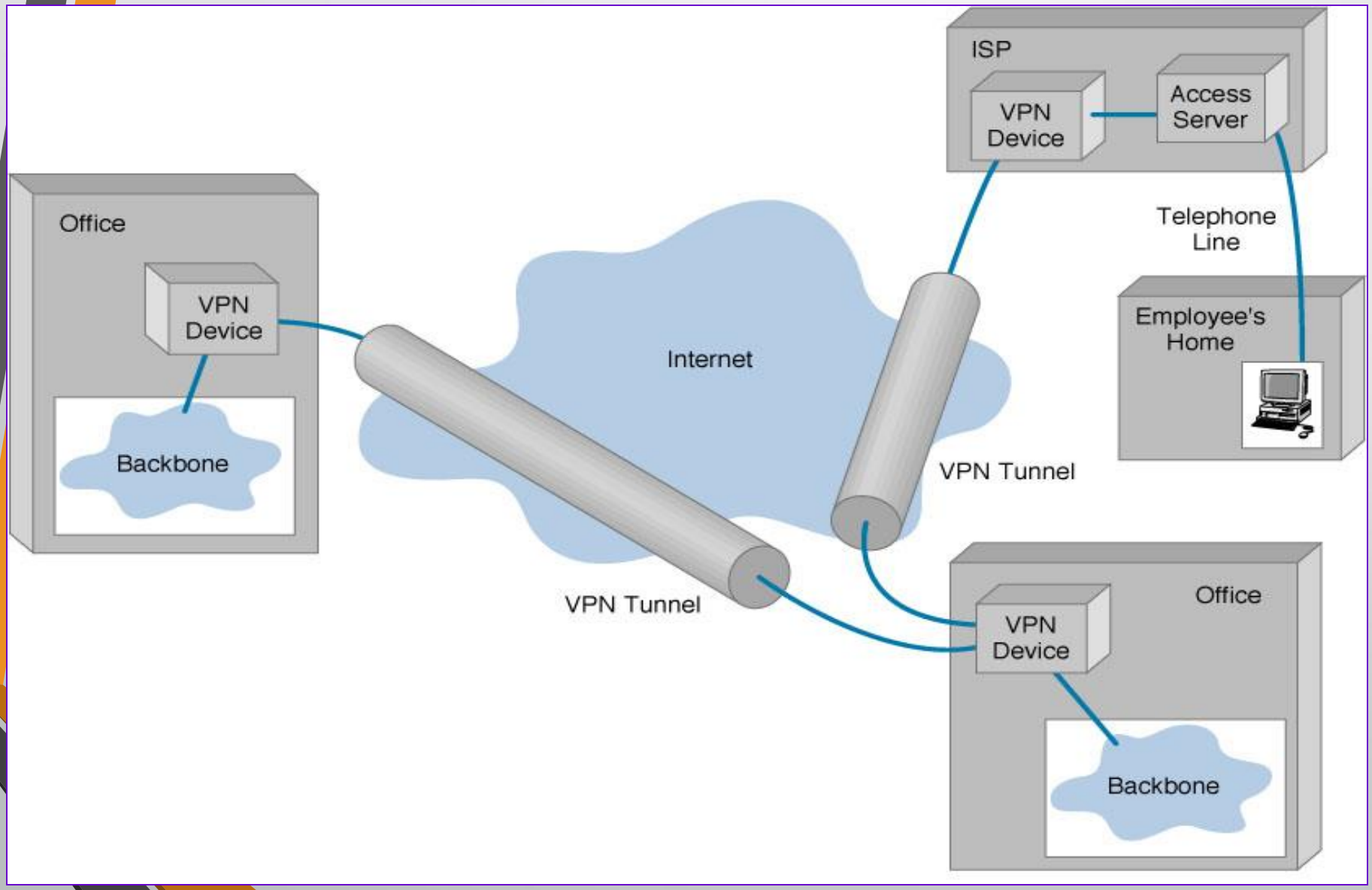
Two types of end points:

- ❑ Remote Access
- ❑ Site-to-Site



Data Encapsulation [From Comer]

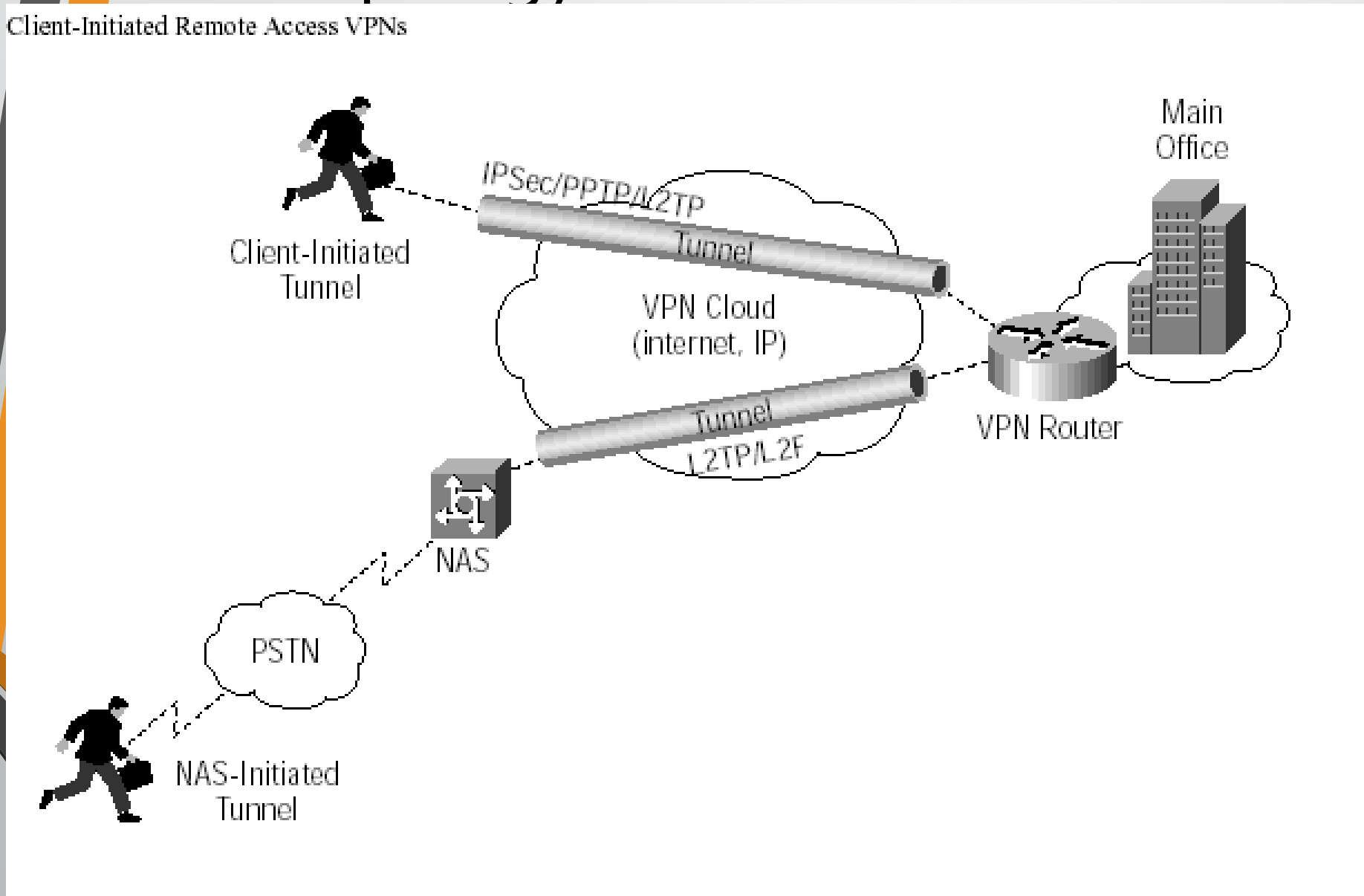
Basic Architecture



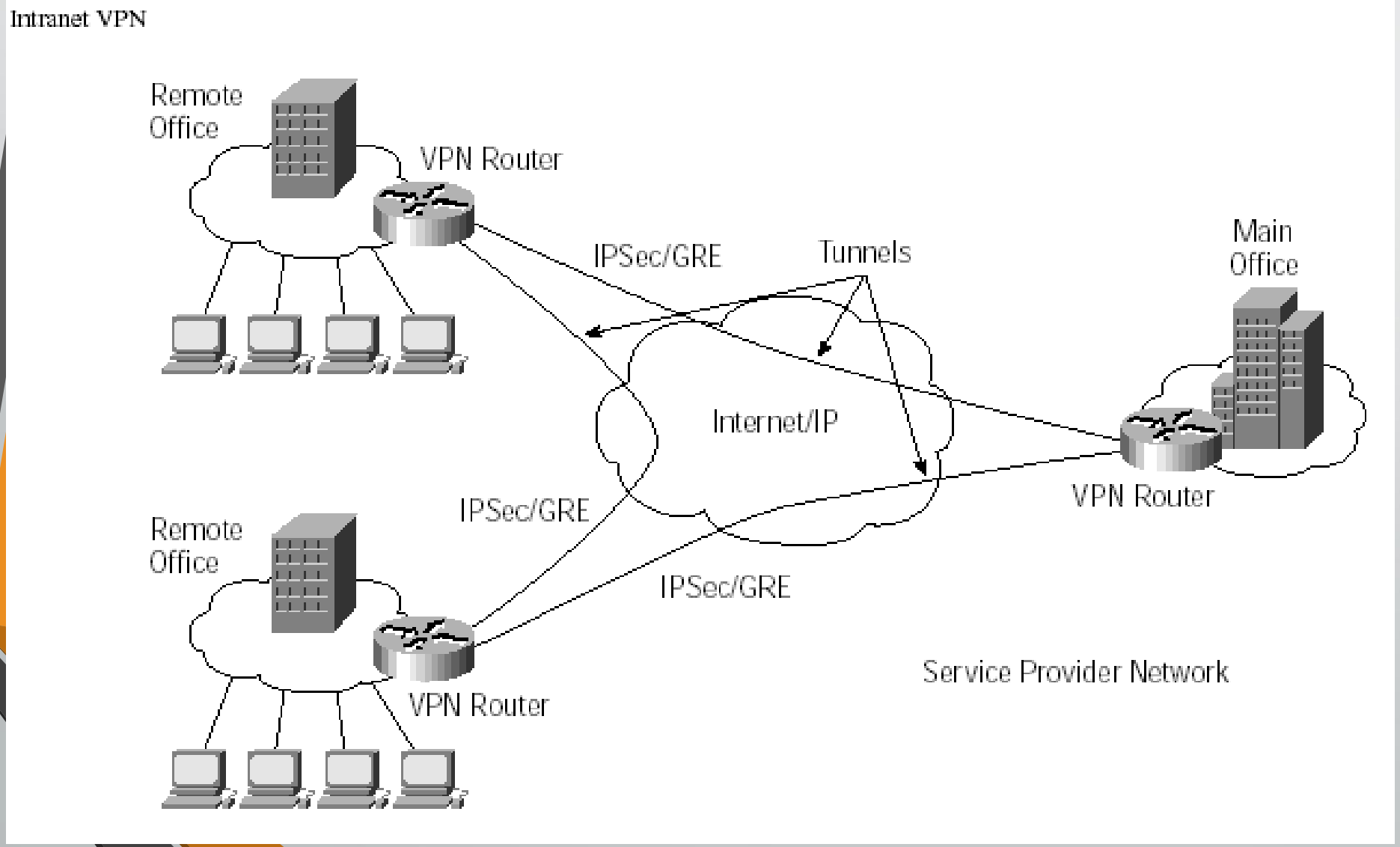
VPN Types

- Remote access VPN: Employee to Business
- Intranet VPN: Within an organization
- Extranet VPN: Outside an organization

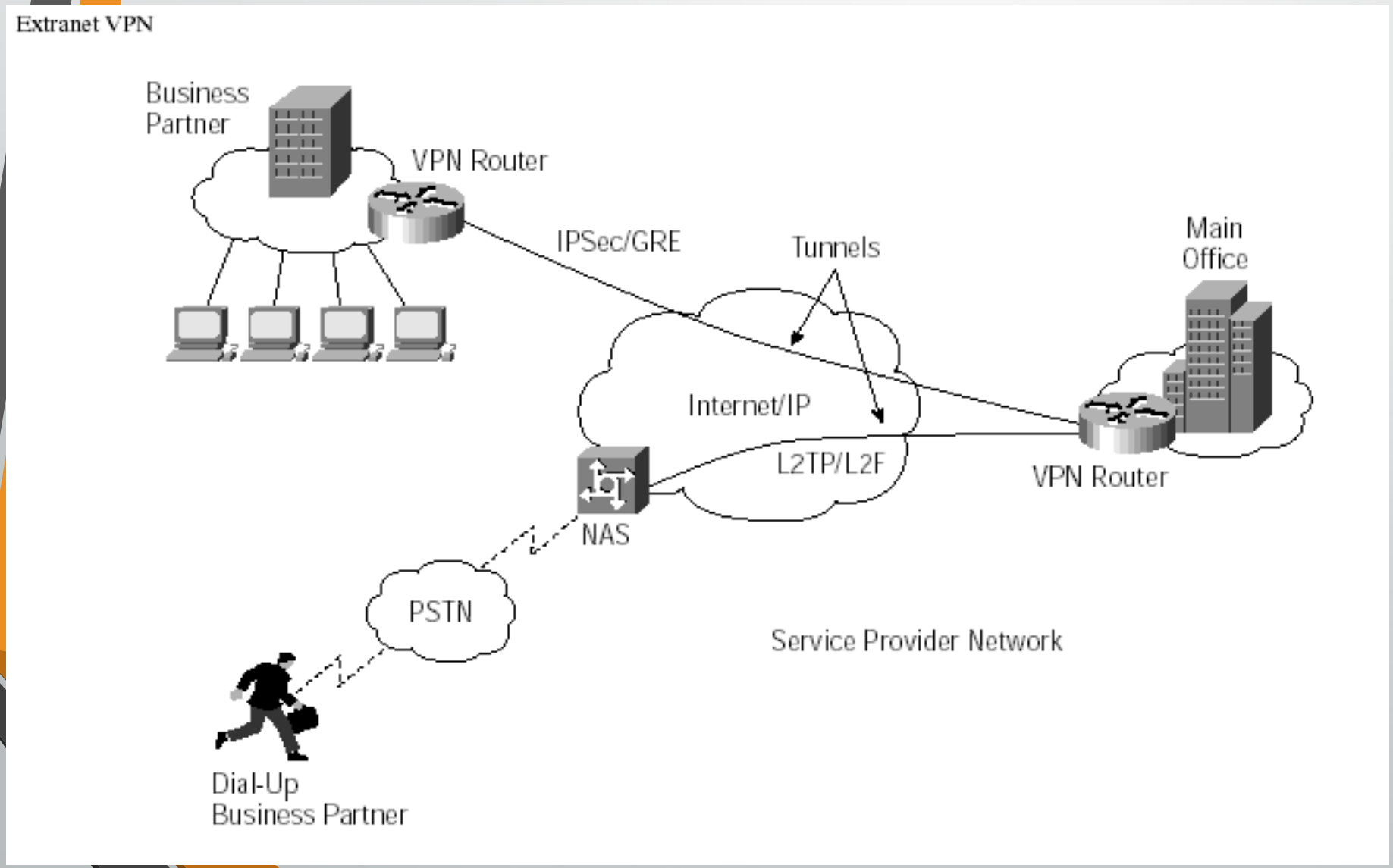
VPN Topology: Remote Access VPN



VPN Topology: Intranet VPN



VPN Topology: Extranet VPN



Advantages of VPN

1. Greater scalability.
2. Easy to add/remove users.
3. Reduced long-distance telecommunications costs.
4. Mobility.
5. Security.

Disadvantages of VPN

1. Lack of standards.
2. Understanding of security issues.
3. Unpredictable Internet traffic.
4. Difficult to accommodate products from different vendors.

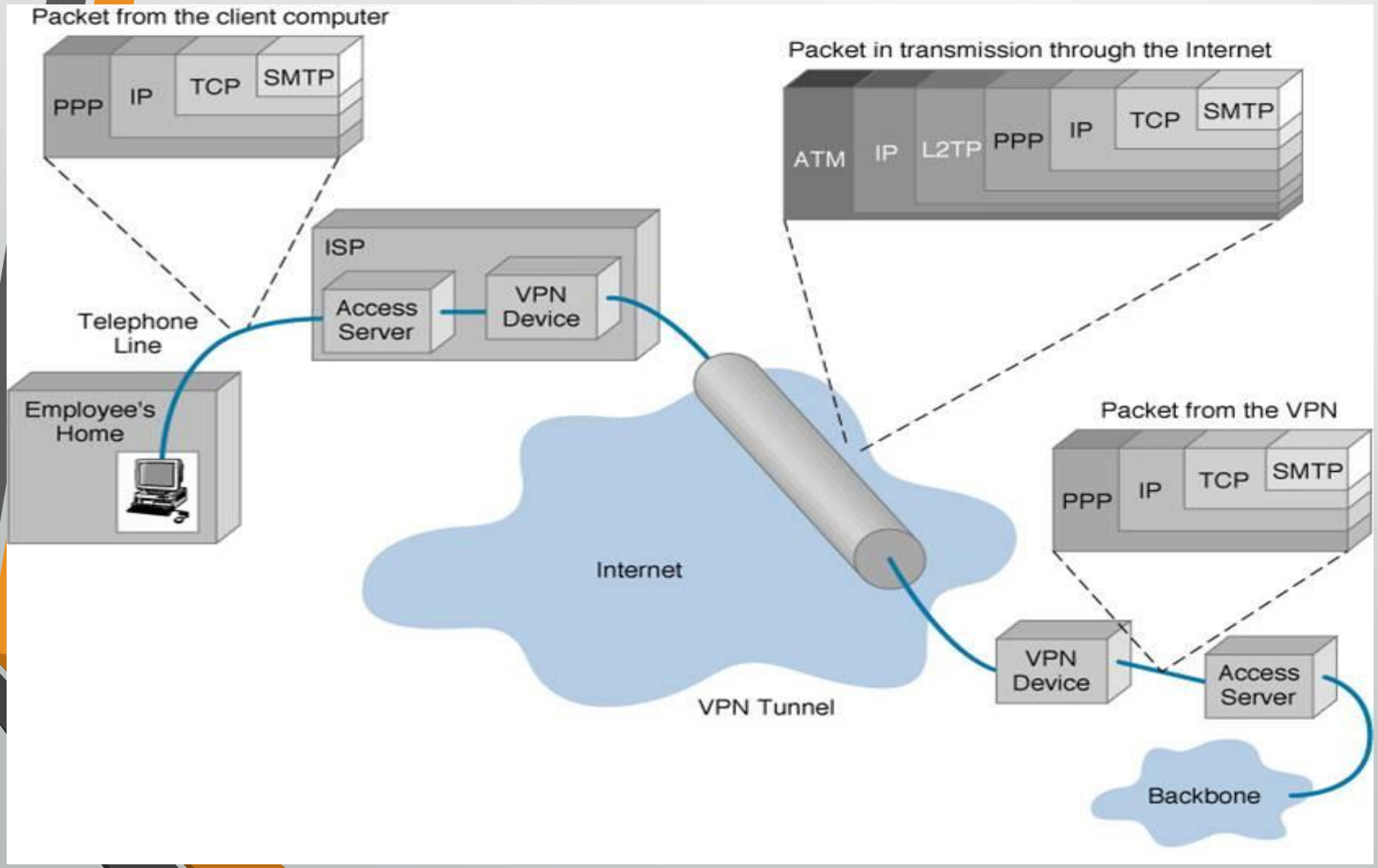
What is needed?

- Existing hardware (Servers, workstations,…)
- Internet connection
- VPN - Router/Switch
- Software to create and manage tunnels
- Security Device such as firewall

VPN Components: Protocols

- IP Security (IPSec)
  - Transport mode
  - Tunnel mode
- Point-to-Point Tunneling Protocol (PPTP)
  - Voluntary tunneling method
  - Uses PPP (Point-to-Point Protocol)

Example of packet encapsulation



VPN Security

Encryption

- Technique for scrambling and unscrambling information

  Unscramble – called plain-text

  Scrambled information – cipher-text

Keys

Secret code that the encryption algorithm uses to create a unique version of cipher-text

- 8-bits keys = 256 combinations or two to the eighth power
- 16-bits keys = 65,536 combinations or two to the 16^{th} power
- 168-bits keys …

VPN Components: Security

- Authentication
  - Determine if the sender is the authorized person and if the data has been redirect or corrupted
  - User/System Authentication
  - Data Authentication

VPN Components: Appliances

- Intrusion detection firewalls
  - Monitors traffic crossing network parameters and protects enterprises from unauthorized access
  - Packet-level firewall checks source and destination
  - Application-level firewall acts as a host computer between the organization’s network and the Internet

VPN Benefits

- Extends geographic connectivity
- Boosts employee productivity
- Improves Internet security
- Costs associated with implementing VPN
  - In House implementation
  - Outsourced implementation
  - Middle Ground implementation

References

- https://en.wikipedia.org/wiki/Virtual_private_network
- https://www.whatismyip.com/what-is-a-vpn/
- Design of a charging and accounting architecture for QoS-differentiated VPN services to mobile users.
- Multi-path routing versus tree routing for VPN bandwidth provisioning in the hose model.

ÖNEMLİ

Bu projeler lisansüstü öğrencilerinin hazırladığı çalışmalar olup tüm sorumluluk hazırlayan öğrencilere aittir. Öğrenciler hazırladığı projeye göre not almışlardır.