

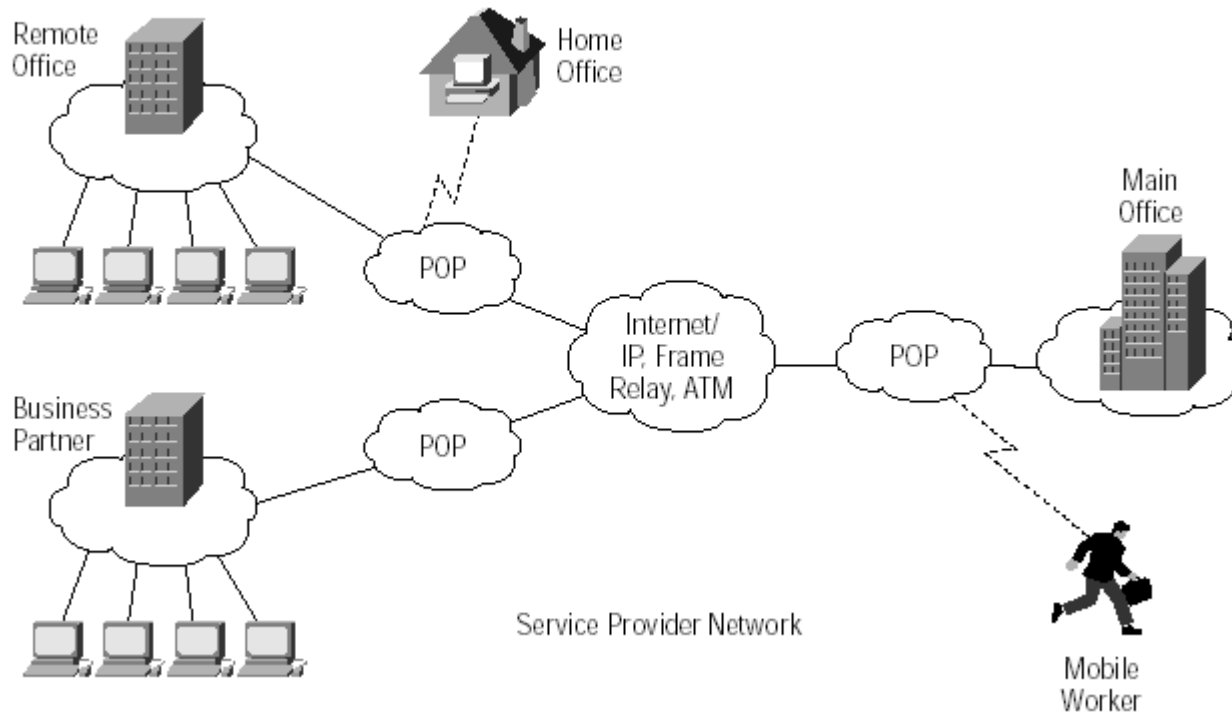
# **COSC 301**

## **Network Management and Security**

### Lecture 20: Virtual Private Network

# Today's Focus

VPN Defined



- What is VPN?
- How VPN works?

# Types of VPN

---

- Remote access VPN
  - Allows individual users to set up secure connections with a remote network through a VPN router (network access server)
- Intranet VPN
  - Allows offices of the same company in different locations to set up secure connections with public networks like the Internet.
- Extranet VPN
  - Allows offices of different companies in different locations to set up secure connections with public networks like the Internet.

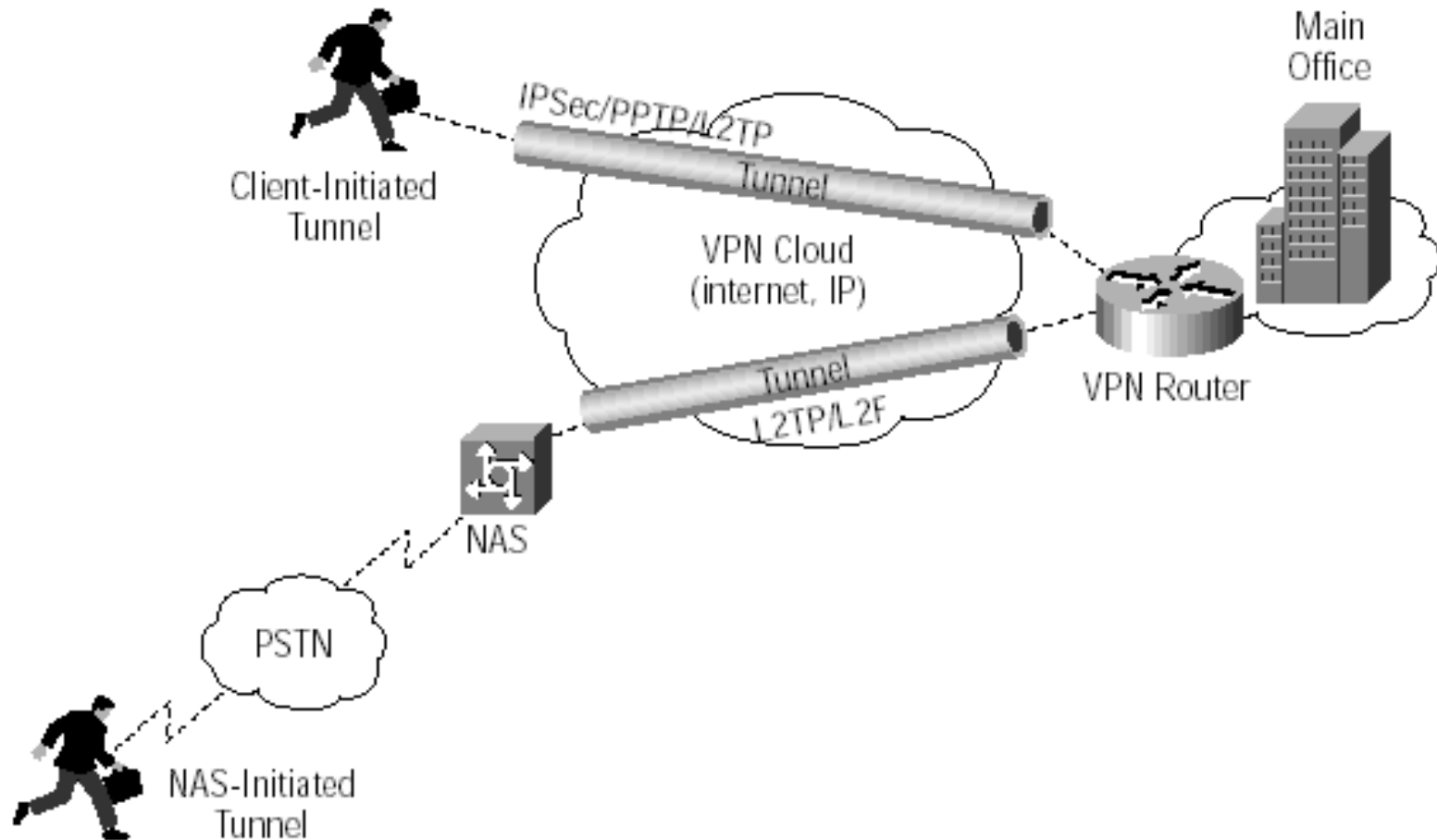
# Concepts

---

- Point Of Presence (POP)
  - An artificial demarcation point or interface between networking entities
- Network Access Server (NAS)
  - A computer server that enables an independent service provider (ISP) to provide customers with internet access. NAS provides interface between telecommunication network and the internet backbone.

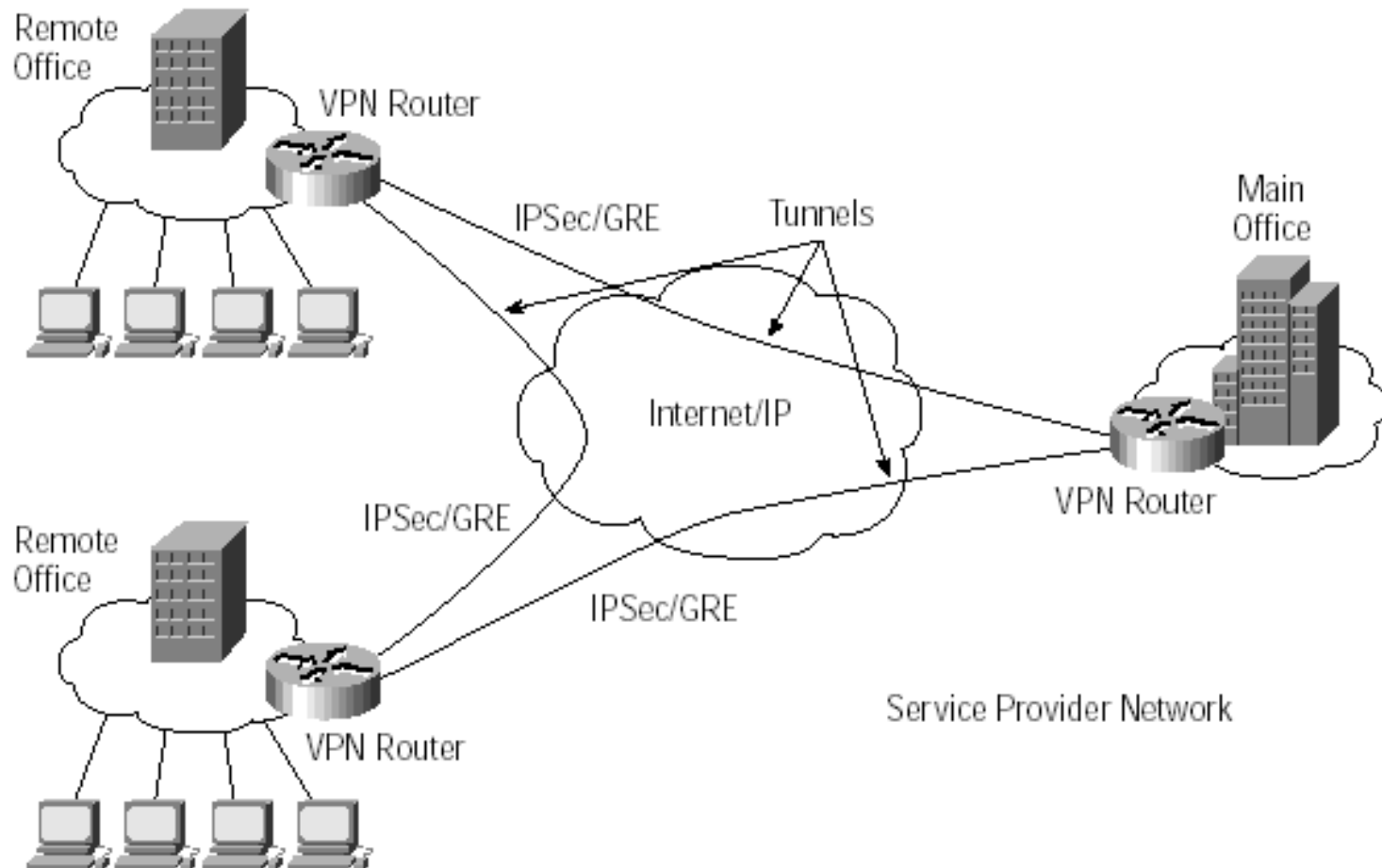
# Remote Access VPN

## Client-Initiated Remote Access VPNs



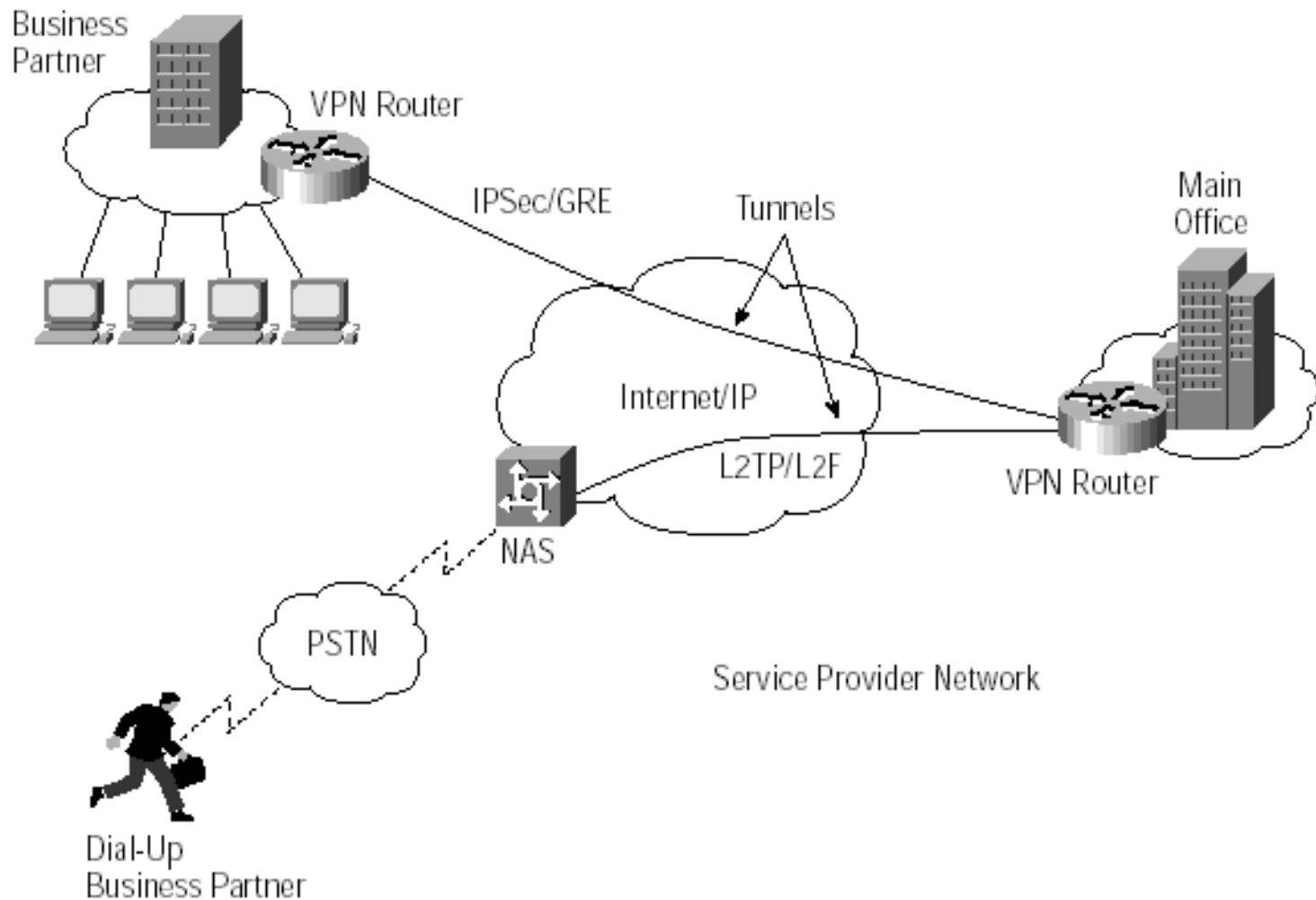
# Intranet VPN

Intranet VPN



# Extranet VPN

Extranet VPN



# Pros and Cons of VPN

---

- Pros

- Easy to install
- Reduced cost compared with dedicated private network
- Flexibility, scalability and mobility
- Security

- Cons

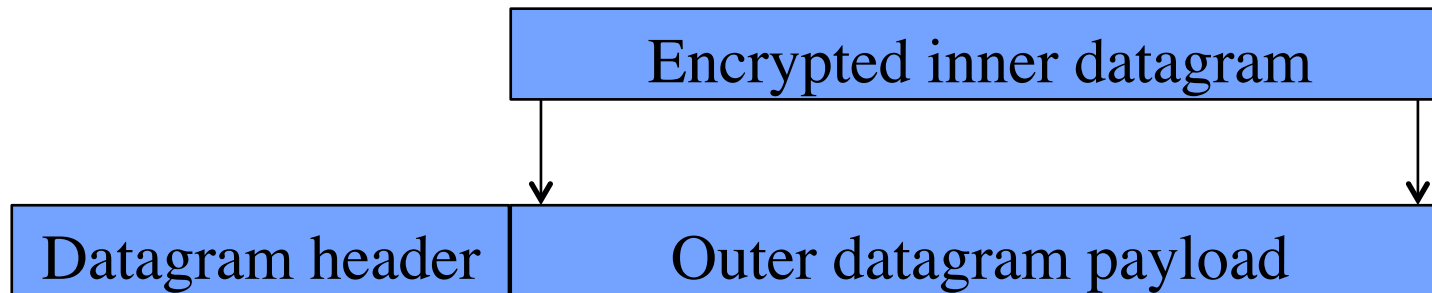
- Overhead and loss of bandwidth
- Unpredictable Internet traffic
- Compatibility issues due to various standards and vendors
- Understanding of security is harder due to complex protocol



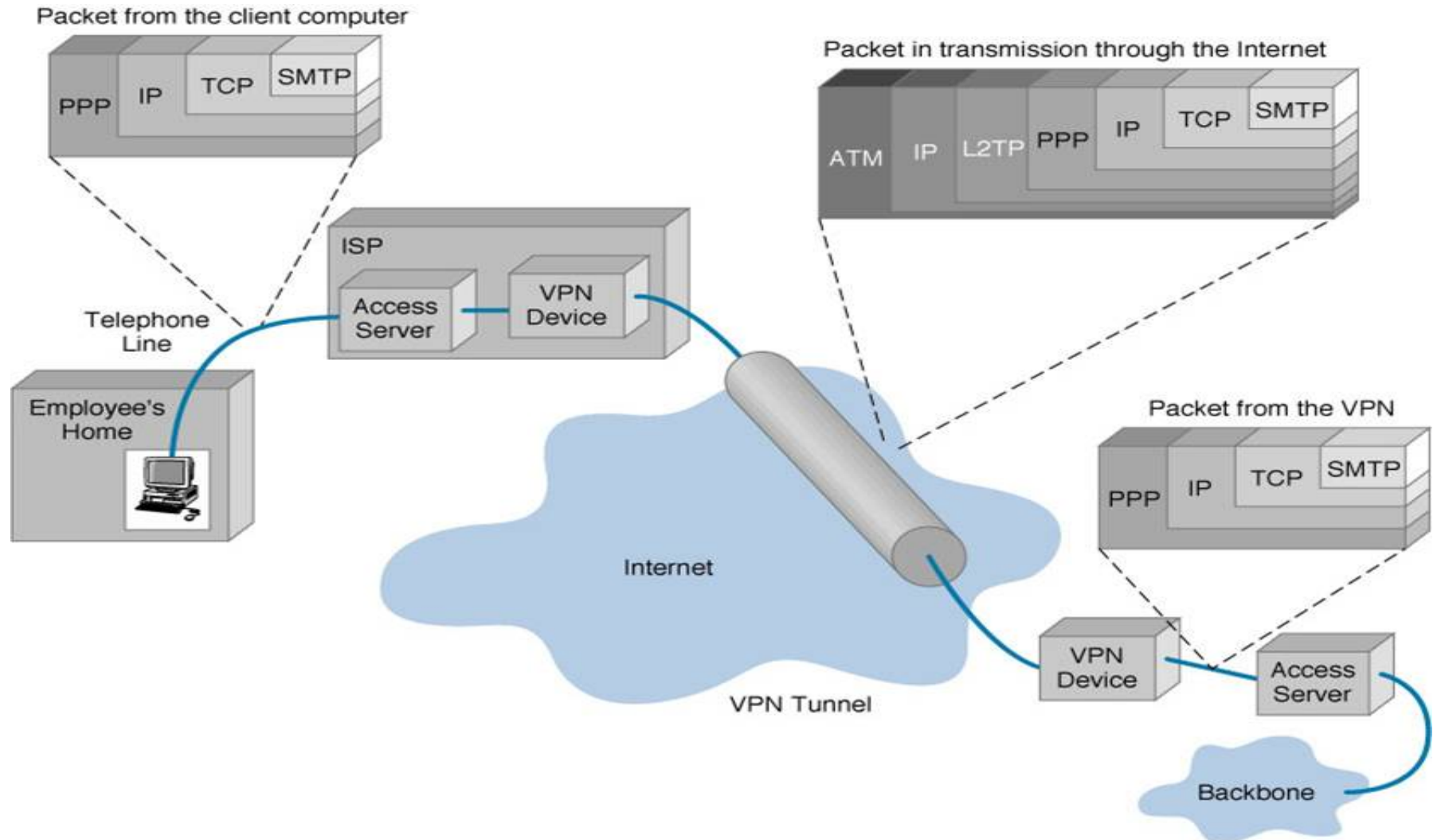
# How VPN works?

---

- Operates at layer 2 or layer 3 of OSI model
  - Layer 2 frame – Bridged VPN, virtual devices called TAP
  - Layer 3 packet – Routed VPN, virtual devices called TUN
- Tunneling
  - Encapsulate data in IP packets that encrypt their payload
  - Two VPN routers/switches exchange such IP packets directly but encode/decode before sending or after receiving the IP packets.



# Tunneling



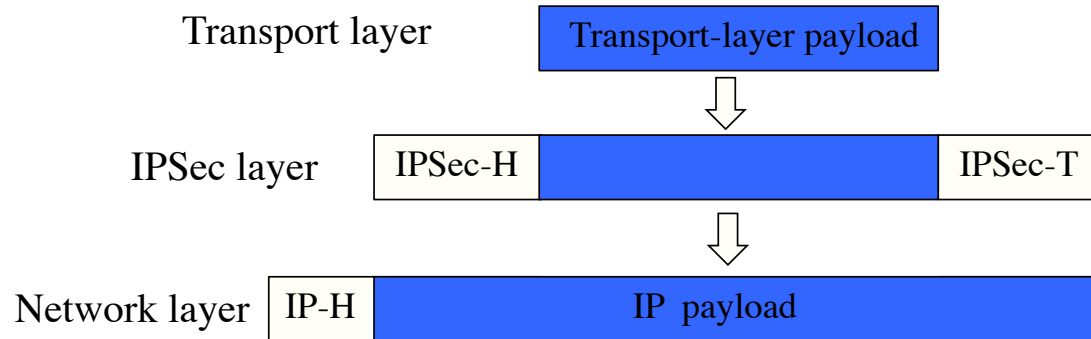
# Layer 3 VPN Protocols - IPSec

---

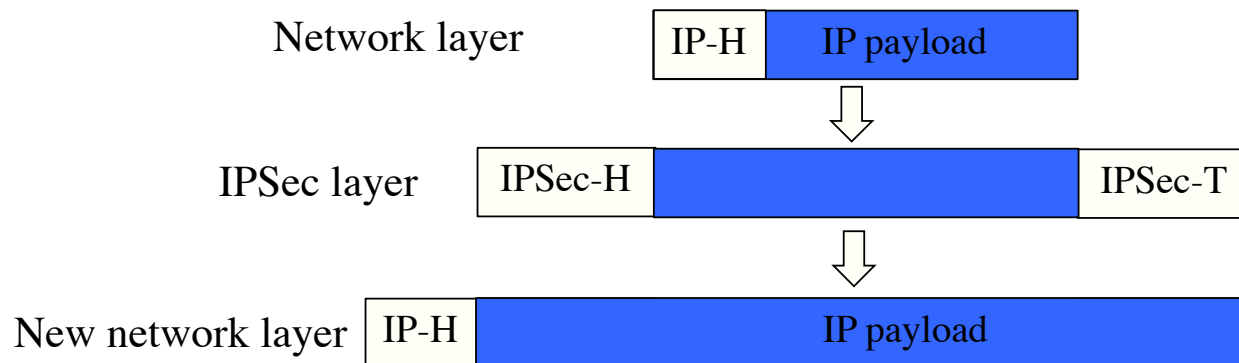
- IPSec
  - A widely used protocol for securing traffic on IP networks. It can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server.
  - It has two sub-protocols:
    - Encapsulated Security Payload (ESP) encrypts the payload with a symmetric key
    - Authentication Header (AH) ensures data integrity by using a hash function and a shared secret key.

# IPSec details

- Provides two modes



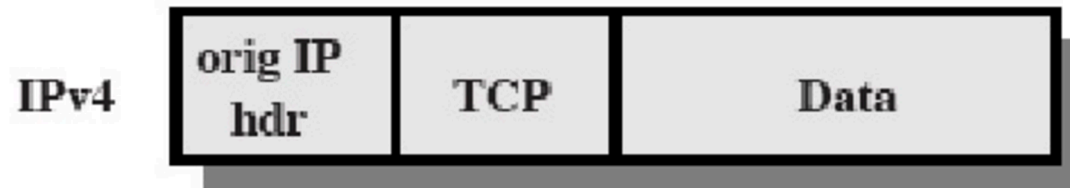
Transport mode



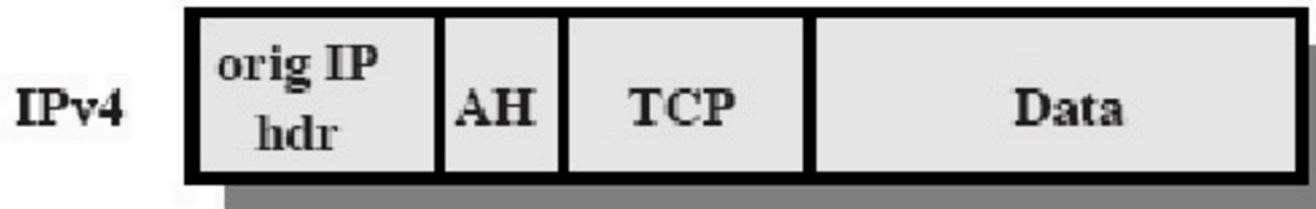
Tunnel mode

# IPSec details (cont.)

- Authentication Header in two modes



← authenticated except for mutable fields →

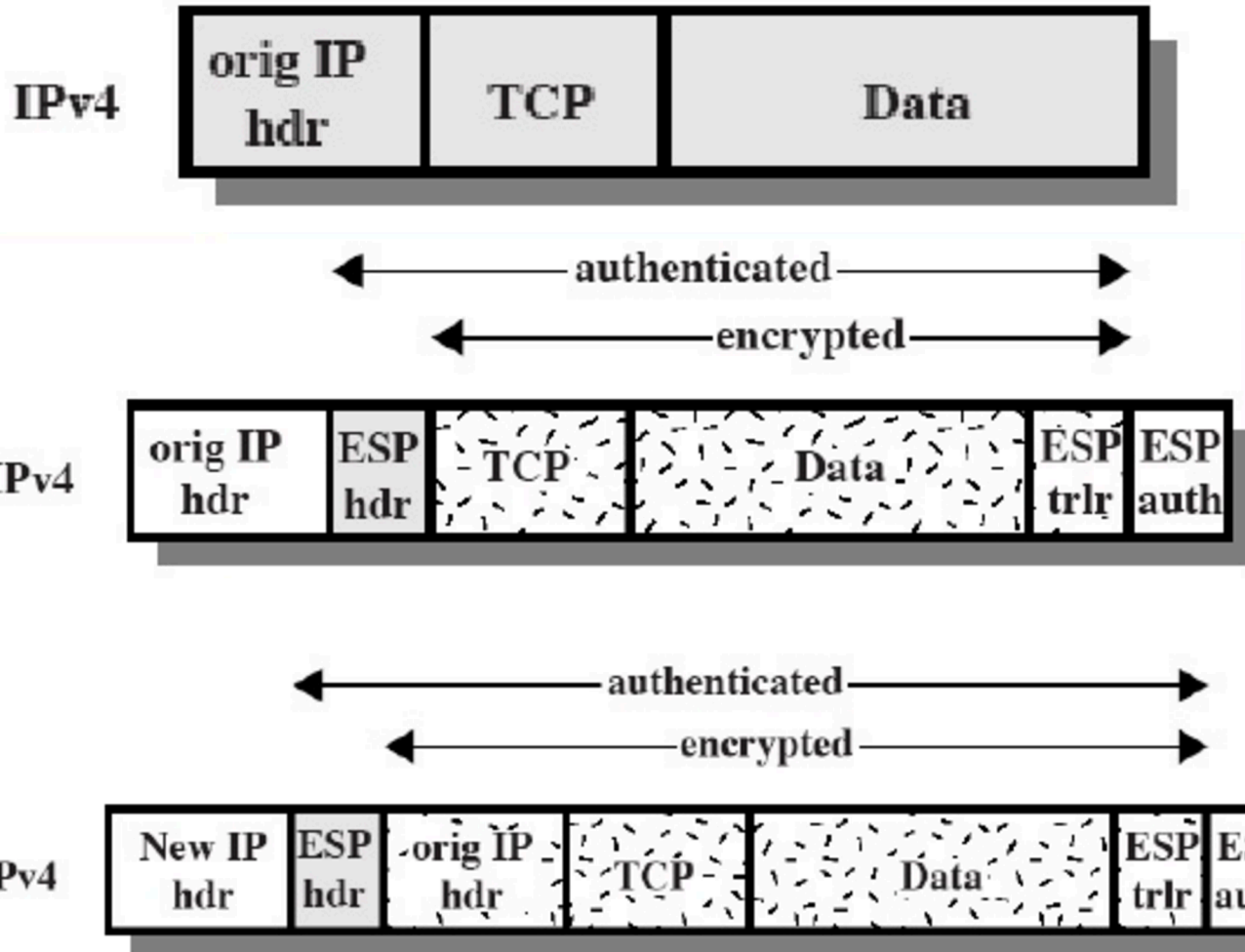


← authenticated except for mutable fields in the new IP header →



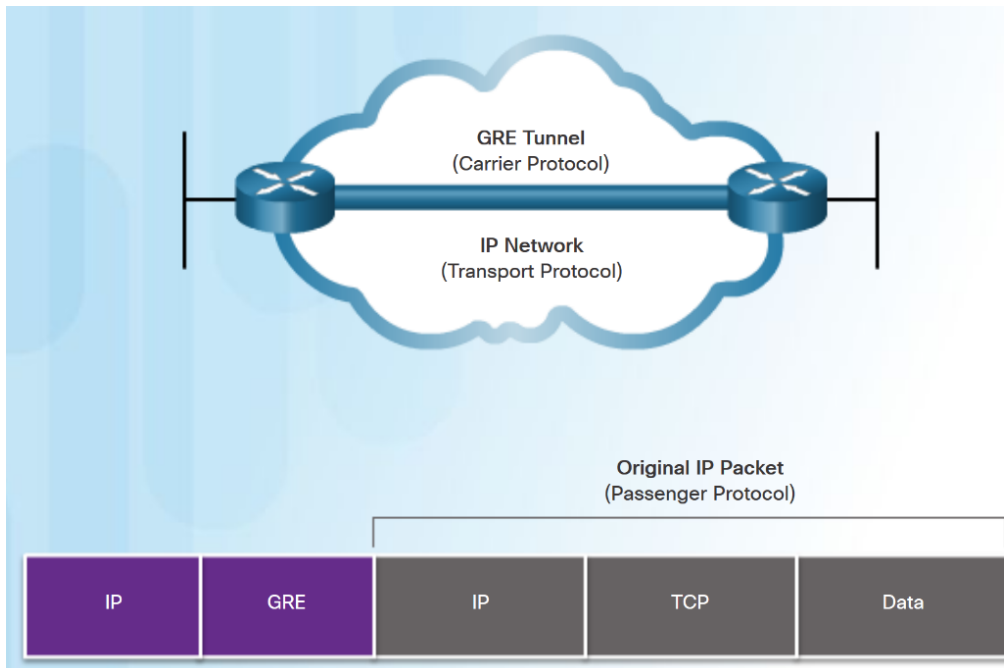
# IPSec details (cont.)

- ESP header in two modes



# Layer 3 VPN Protocols - GRE

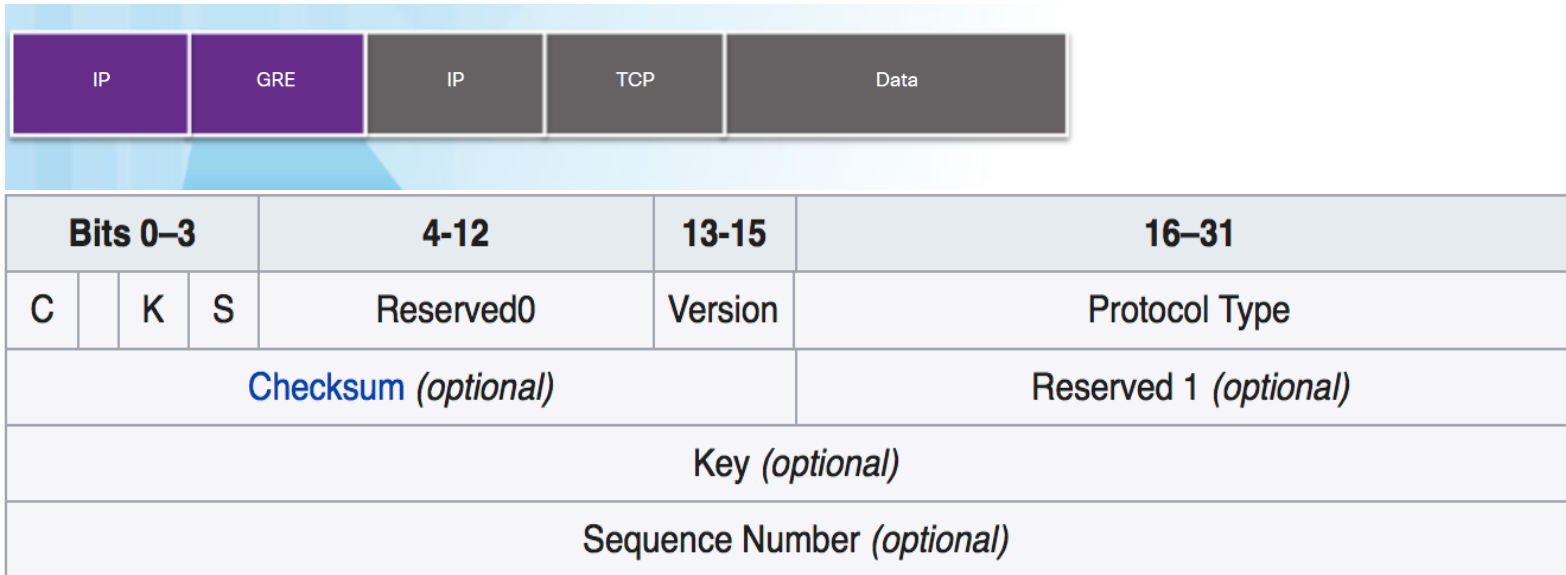
- GRE (Generic Routing Encapsulation)
  - a non-secure site-to-site VPN tunneling protocol developed by Cisco.
  - defined as an IETF standard (RFC 2784).



A tunnel interface supports a header for each of the following:

- An encapsulated protocol or passenger protocol such as IPv4, IPv6.
- An encapsulation protocol or carrier protocol, such as GRE.
- A transport delivery protocol, such as IP.

# Layer 3 VPN Protocols - GRE



- In the outer IP header, 47 is used in the protocol field.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE does not include any strong security mechanisms.
- GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

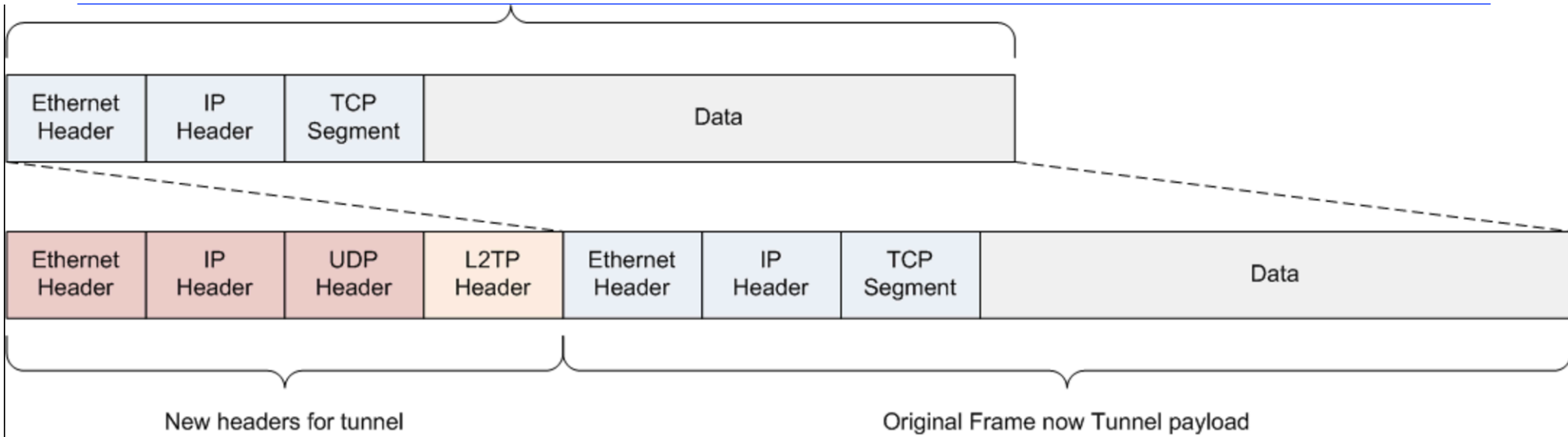


# Layer 2 VPN Protocols

---

- In remote access VPN, tunneling relies on Point-to-Point Protocol (PPP), on which the following three protocols are based.
- L2F (Layer 2 Forwarding)
  - Developed by Cisco; uses any authentication scheme supported by PPP
- PPTP (Point-to-Point Tunneling Protocol)
  - Supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP.
- L2TP (Layer 2 Tunneling Protocol)
  - Combines features of PPTP and L2F and fully supports IPSec.

# L2TP details



00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<u>T</u>	<u>L</u>	0	<u>S</u>	0	<u>O</u>	<u>P</u>	0				<u>Version</u>				<u>Length</u>																
<u>Tunnel ID</u>															<u>Session ID</u>																
<u>Ns</u>															<u>Nr</u>																
<u>Offset Size</u>															<u>Offset Pad</u> :::																
Data :::																															

# VPN vs SSH

---

- VPN
  - the network/data link layer
  - encrypt data packets/frames
  - require routers and software to run which makes it a more costly solution
- SSH
  - the application layer
  - encrypt the application data
  - require each service to be configured and maintained separately, a lot of effort to set up and maintain.

# Summary

---

- Types of VPN
- VPN protocols
  - IPsec
  - L2TP/IPsec