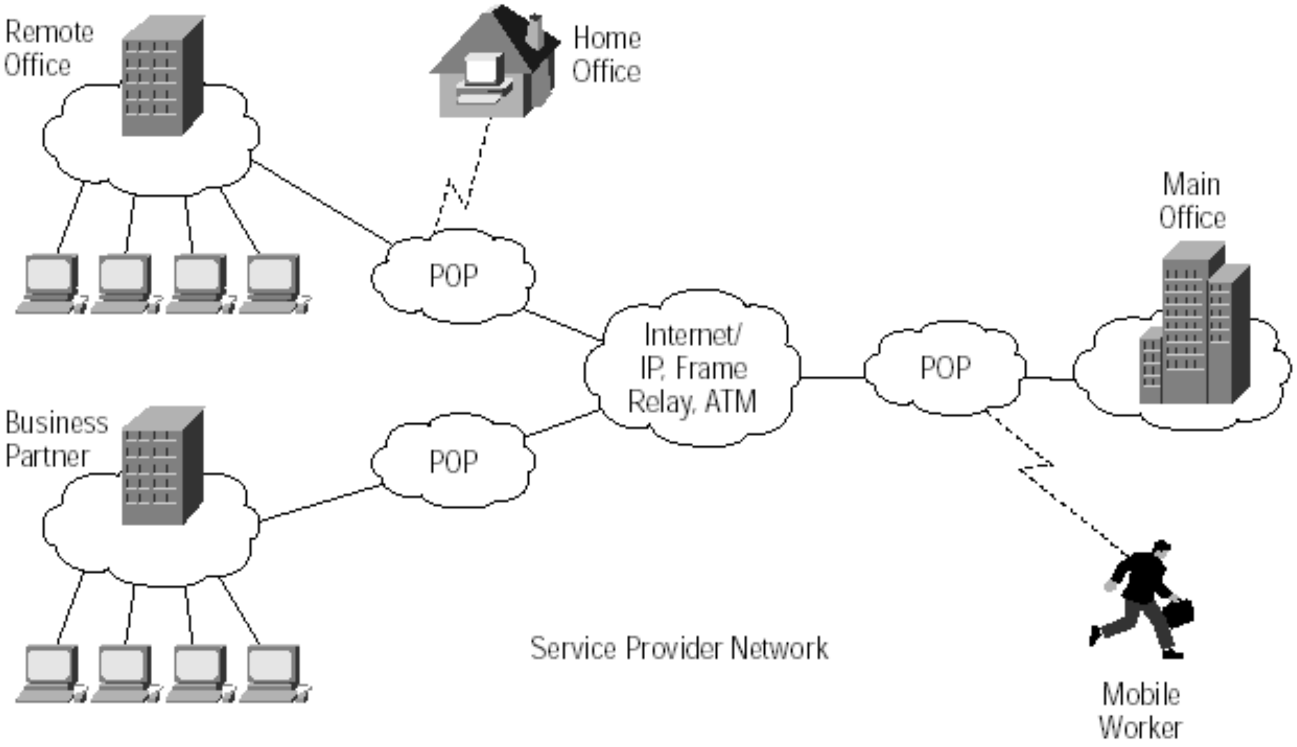
# COSC 301
# Network Management and Security

## Lecture 20: Virtual Private Network

# Today's Focus

VPN Defined



-- What is VPN?

-- How VPN works?

# Types of VPN

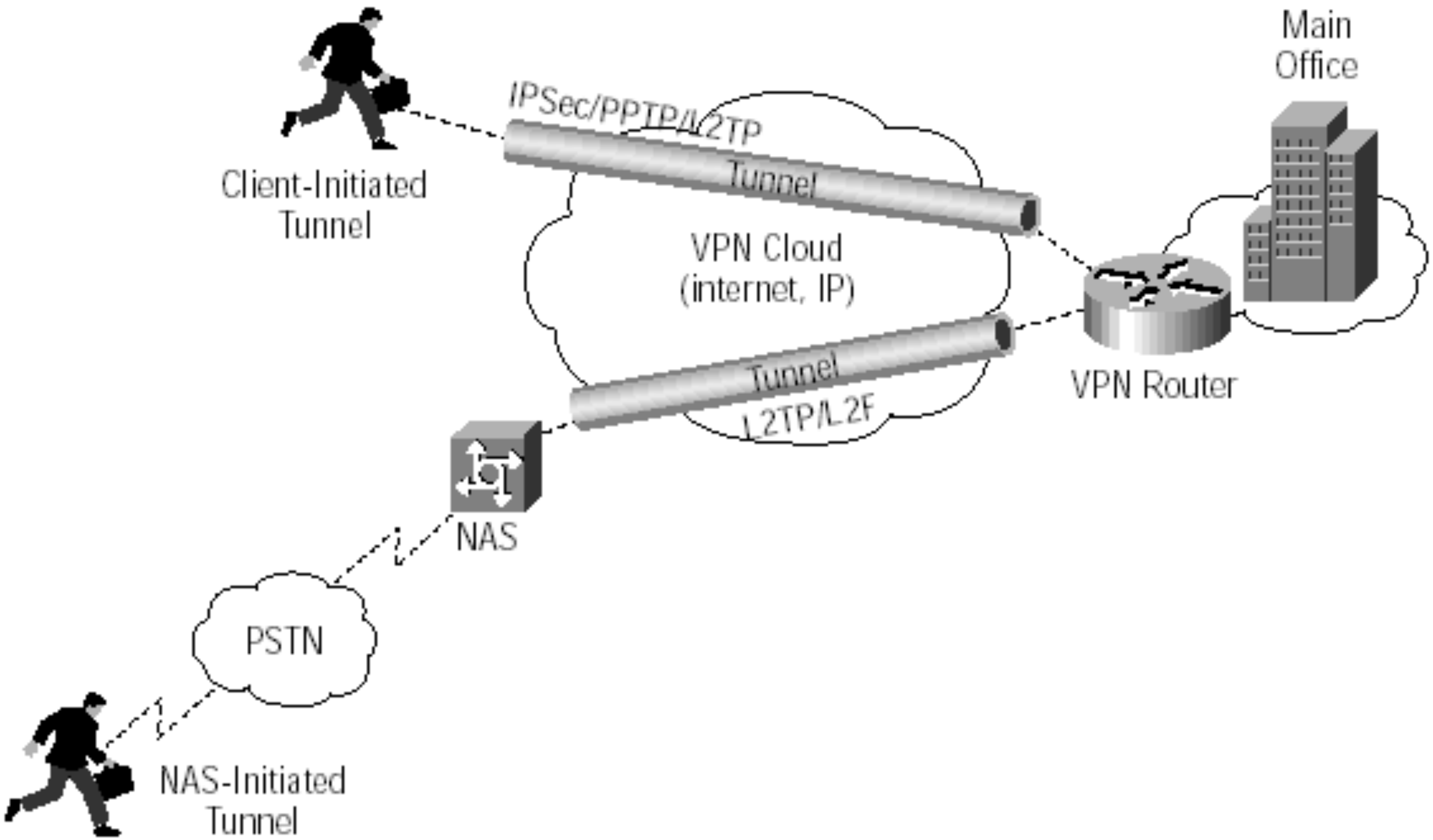
- Remote access VPN
  - Allows individual users to set up secure connections with a remote network through a VPN router (network access server)
- Intranet VPN
  - Allows offices of the same company in different locations to set up secure connections with public networks like the Internet.
- Extranet 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 Internet service provider (ISP) to provide customers with internet access. NAS provides interface between telecommunication network and the Internet backbone.

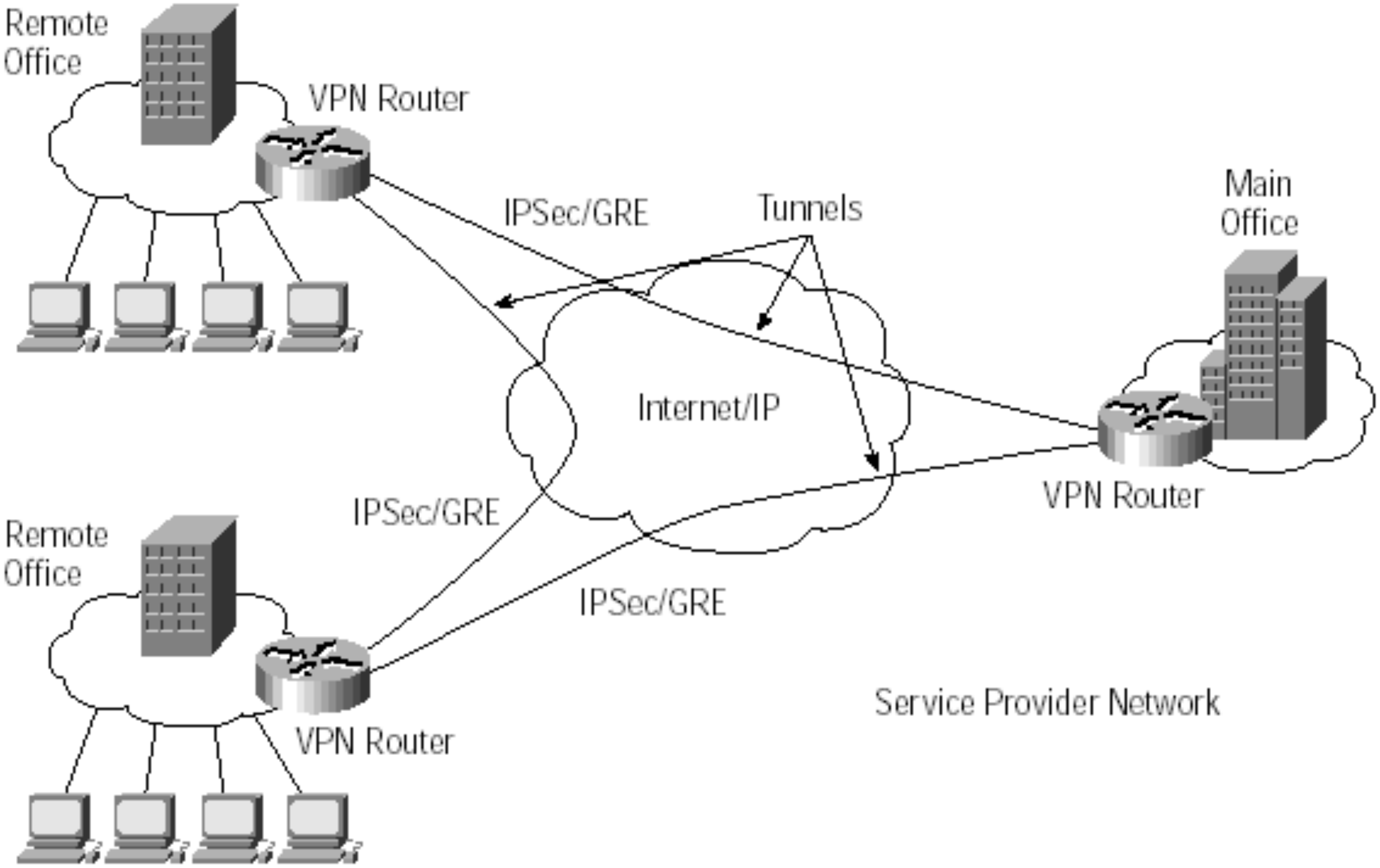
# Remote Access VPN

Client-Initiated Remote Access VPNs



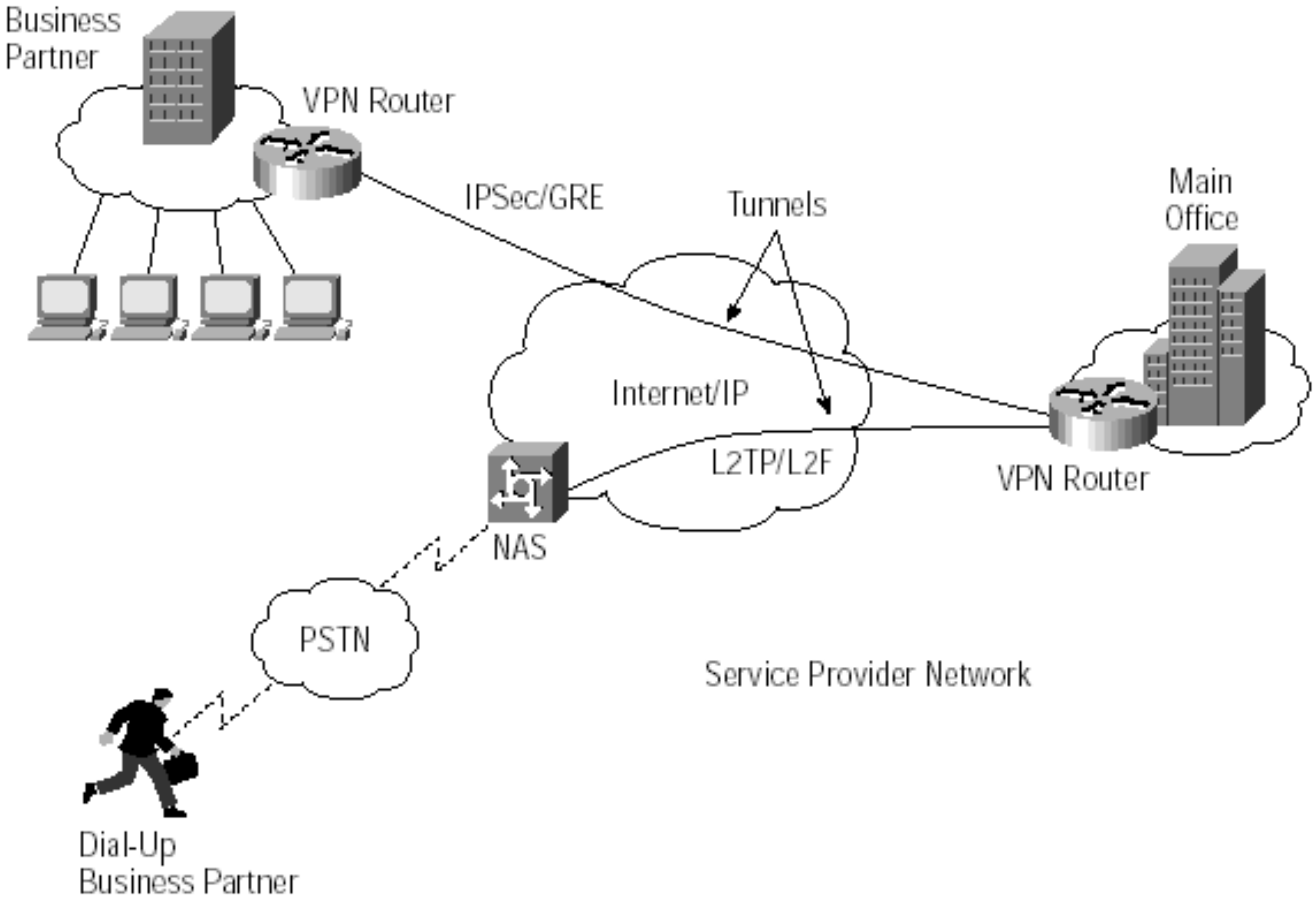
# Intranet VPN

Intranet VPN



# Extranet VPN

Extranet VPN

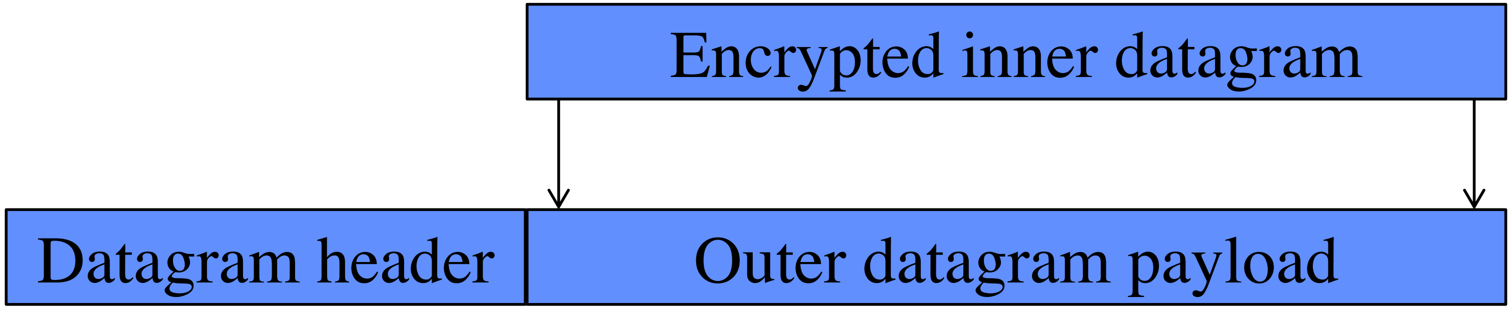


# Pros and Cons of VPN

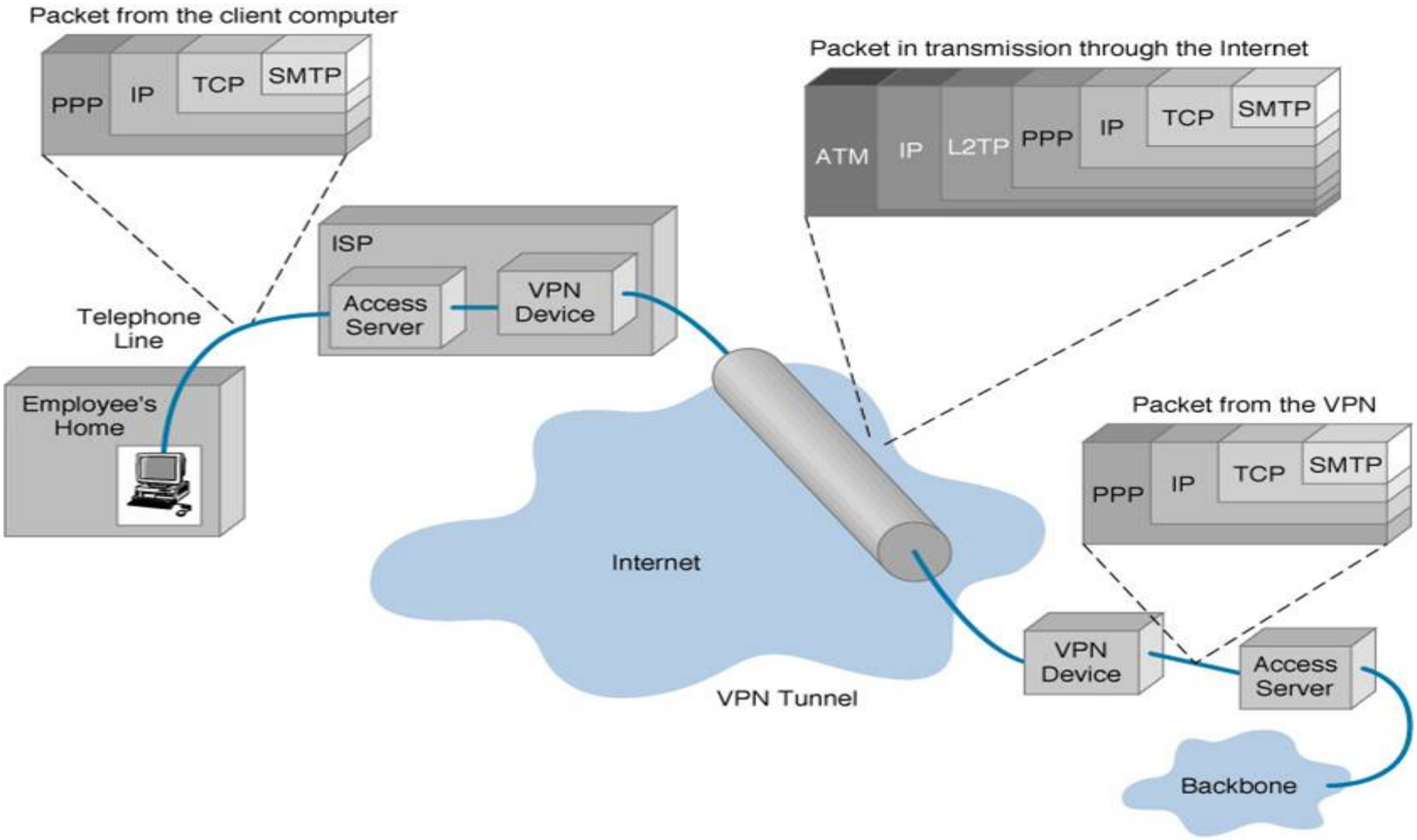
- Pros
  - Easy to install
  - Reduced cost compared with dedicated private network
  - Flexibility, scalability and mobility
  - Security
- Cons
  - Overhead and loss of bandwidth
  - Unpredictable Internet traffic
  - Compatibility issues due to various standards and vendors
  - Understanding of security is harder due to complex protocol
  - If not configured and managed correctly, serious security issues can arise

# 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

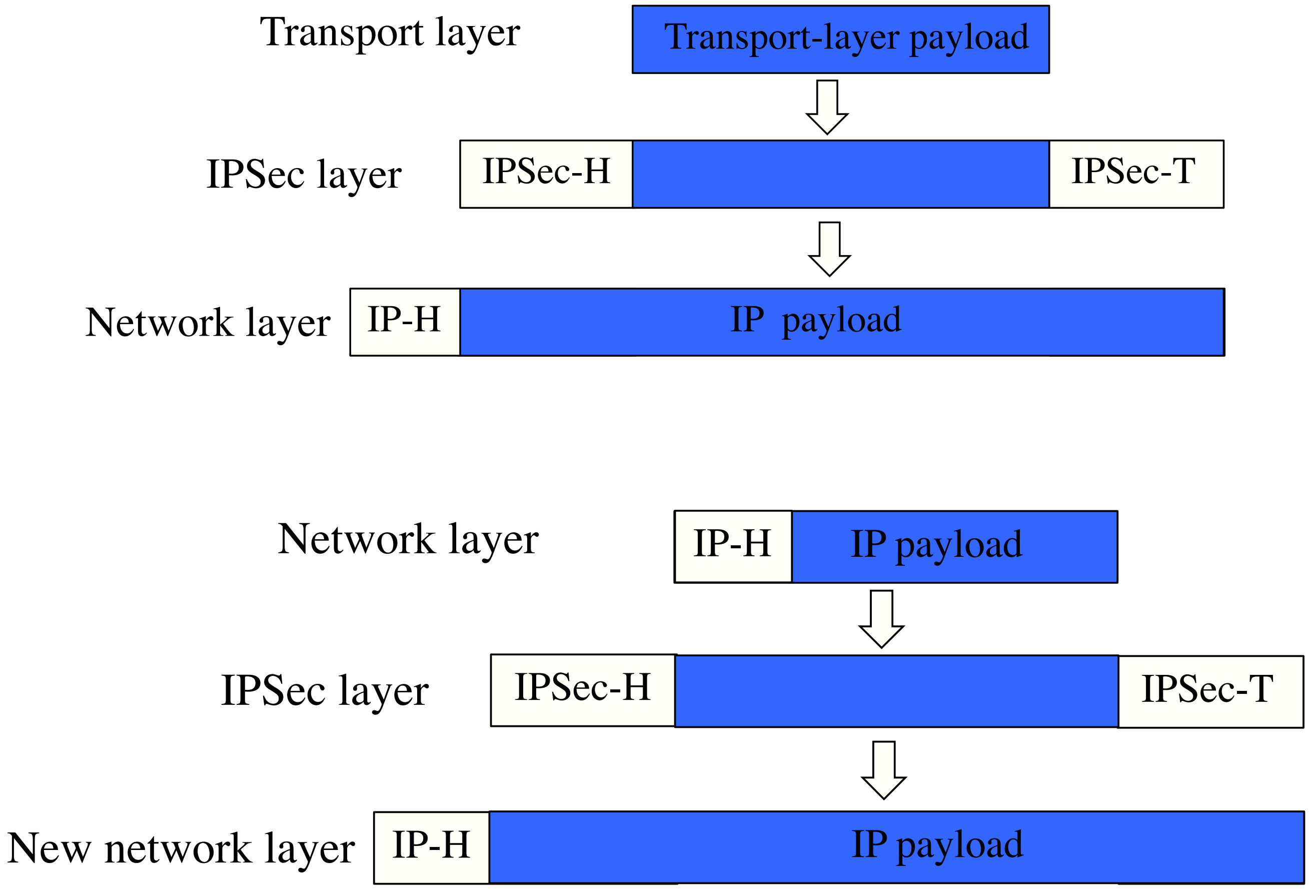

Packet from the client computer
PPP
IP
TCP
SMTP
Packet in transmission through the Internet
ATM
IP
L2TP
PPP
IP
TCP
SMTP
ISP
Access Server
VPN Device
Telephone Line
Employee's Home
Packet from the VPN
PPP
IP
TCP
SMTP
Internet
VPN Tunnel
VPN Device
Access Server
Backbone

# 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

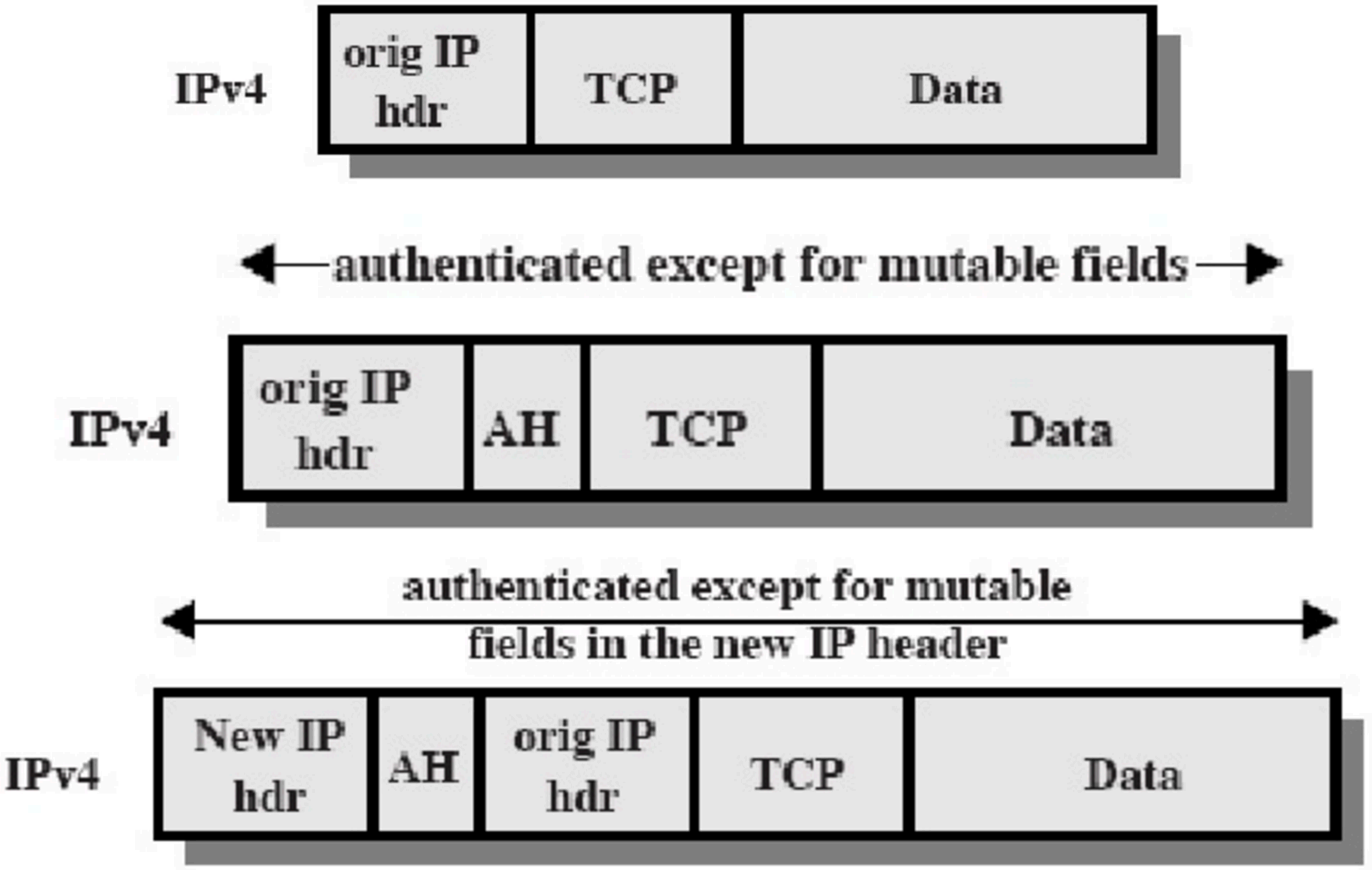


Transport mode

Tunnel mode

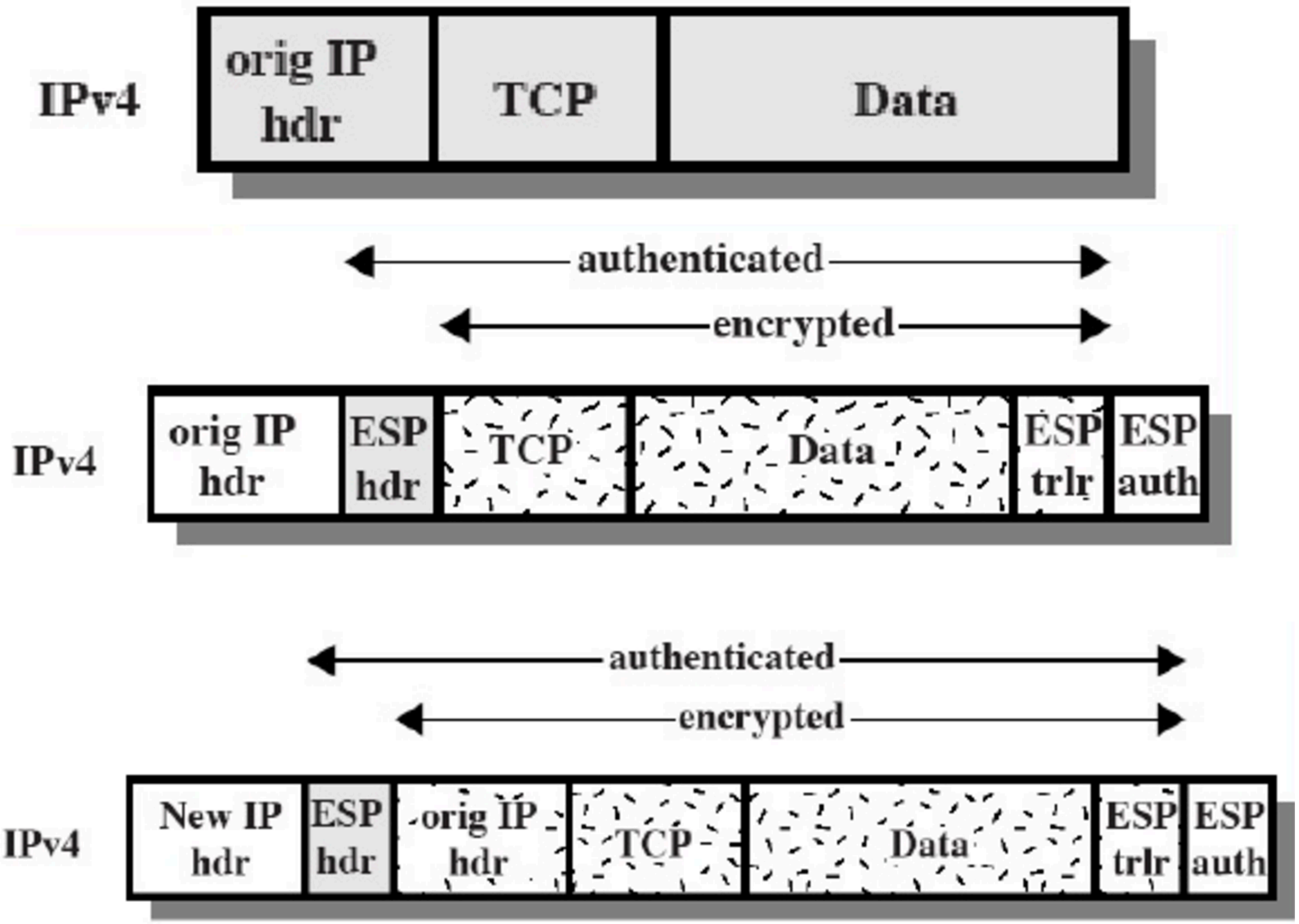
# IPSec details (cont.)

- Authentication Header in two modes


IPv4
orig IP hdr
TCP
Data
authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data

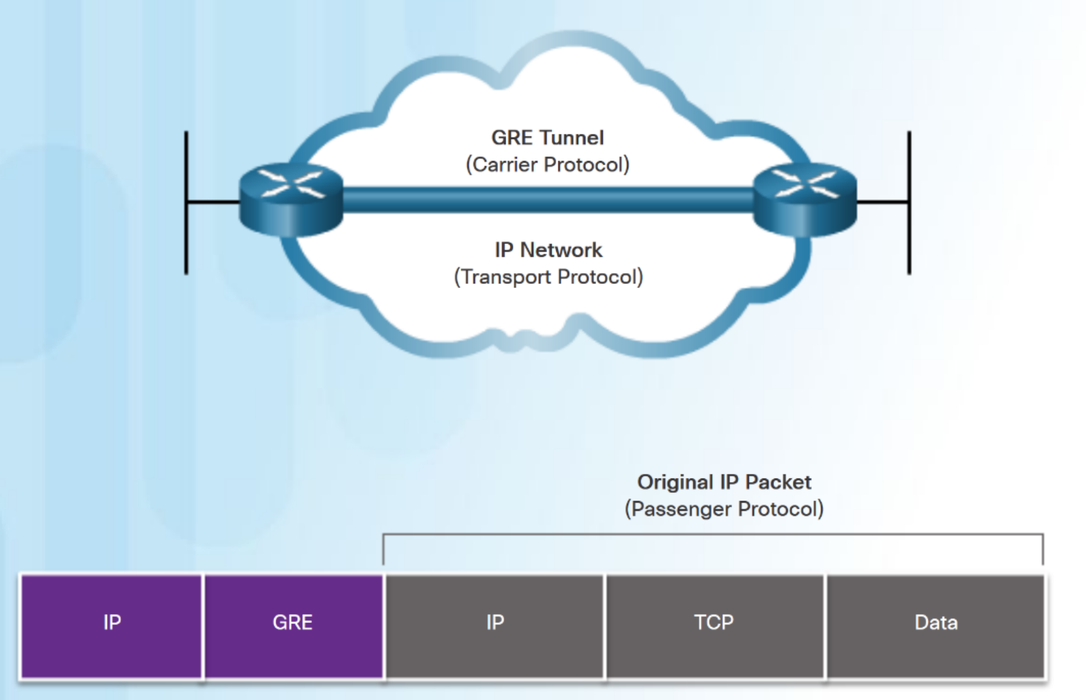
# IPSec details (cont.)

- ESP header in two modes



# Layer 3 VPN Protocols - GRE

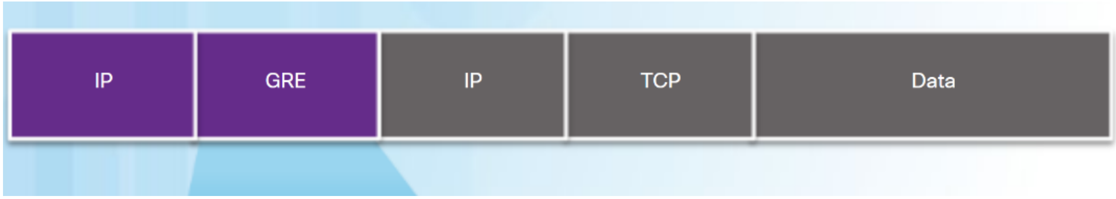
- GRE (Generic Routing Encapsulation)
  - a non-secure site-to-site VPN tunneling protocol developed by Cisco.
  - defined as an IETF standard (RFC 2784).

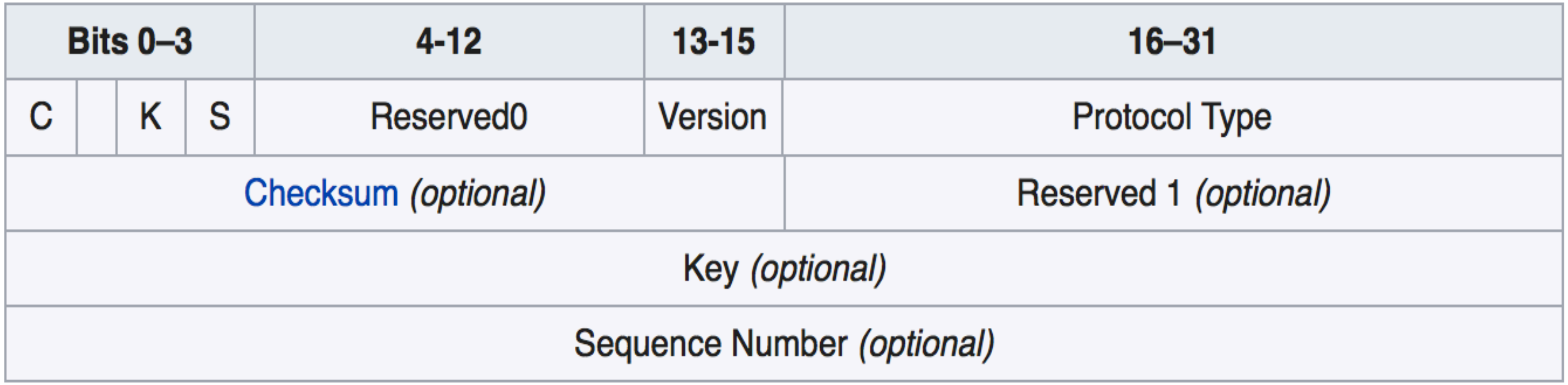


A tunnel interface supports a header for each of the following:

- 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





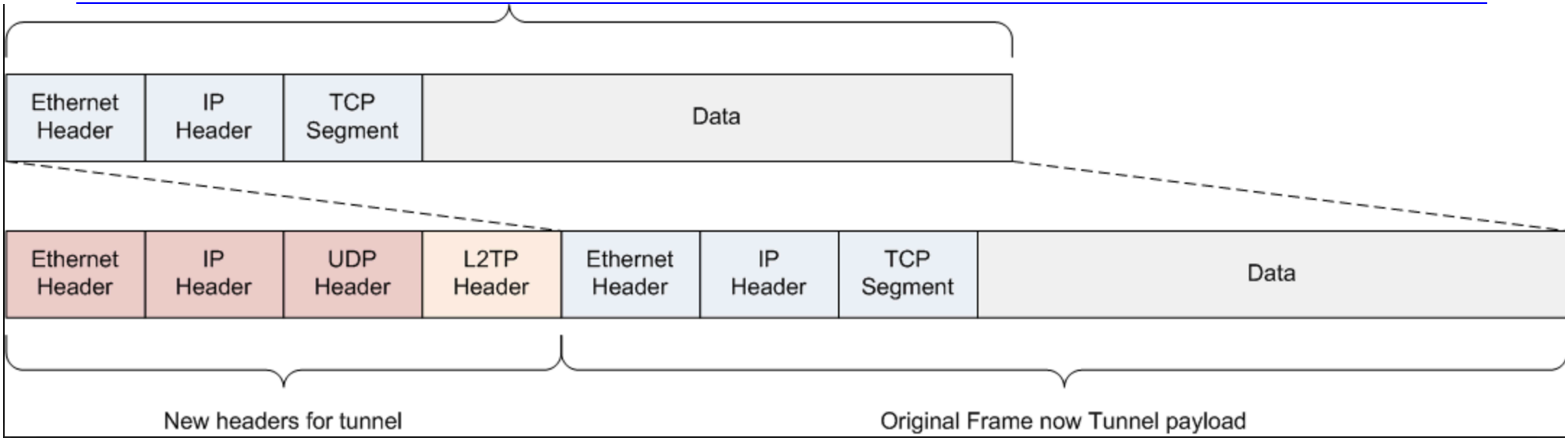
| Bits 0–3 | | | | 4-12 | 13-15 | 16–31 |
|---|---|---|---|---|---|---|
| C | | K | S | Reserved0 | Version | Protocol Type |
| Checksum *(optional)* | | | | | | Reserved 1 *(optional)* |
| Key *(optional)* | | | | | | |
| Sequence Number *(optional)* | | | | | | |

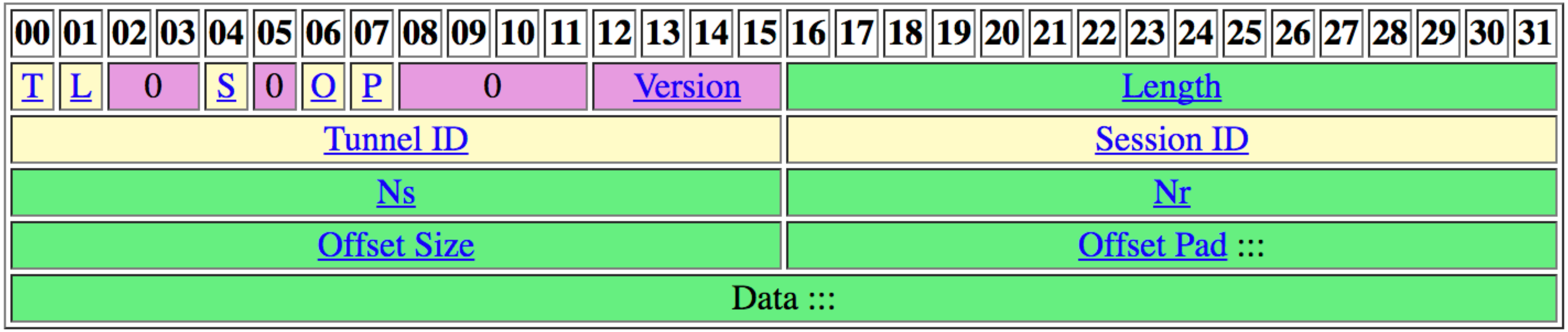
- In the outer IP header, 47 is used in the protocol field.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE does not include any strong security mechanisms.
- GRE header, together with the tunneling IP header, creates at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





<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>T</td><td>L</td><td colspan="2">0</td><td>S</td><td>0</td><td>O</td><td>P</td><td colspan="4">0</td><td colspan="4">Version</td><td colspan="16">Length</td></tr>
<tr><td colspan="16">Tunnel ID</td><td colspan="16">Session ID</td></tr>
<tr><td colspan="16">Ns</td><td colspan="16">Nr</td></tr>
<tr><td colspan="16">Offset Size</td><td colspan="16">Offset Pad :::</td></tr>
<tr><td colspan="32">Data :::</td></tr>
</table>

# 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 with port forwarding
  - 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
  - GRE