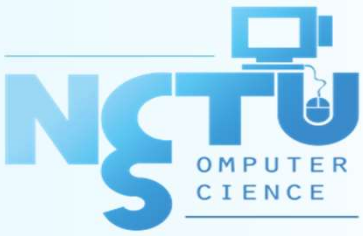


Virtual Private Network (VPN)

Prof. Chien-Chao Tseng

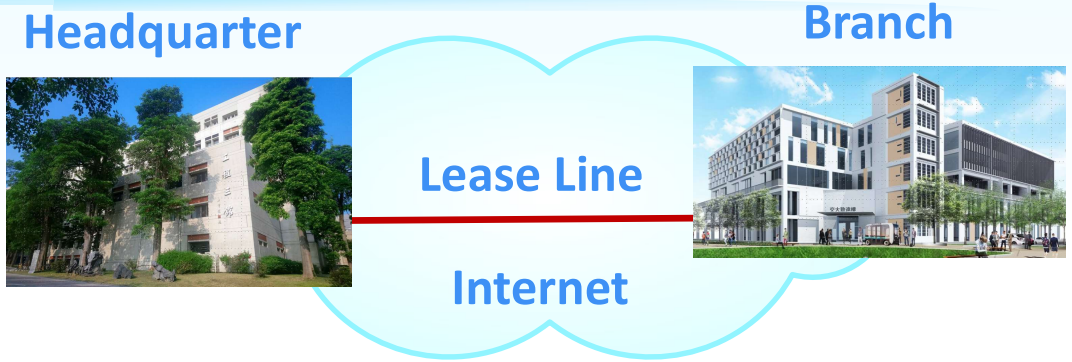
曾 建 超 教授

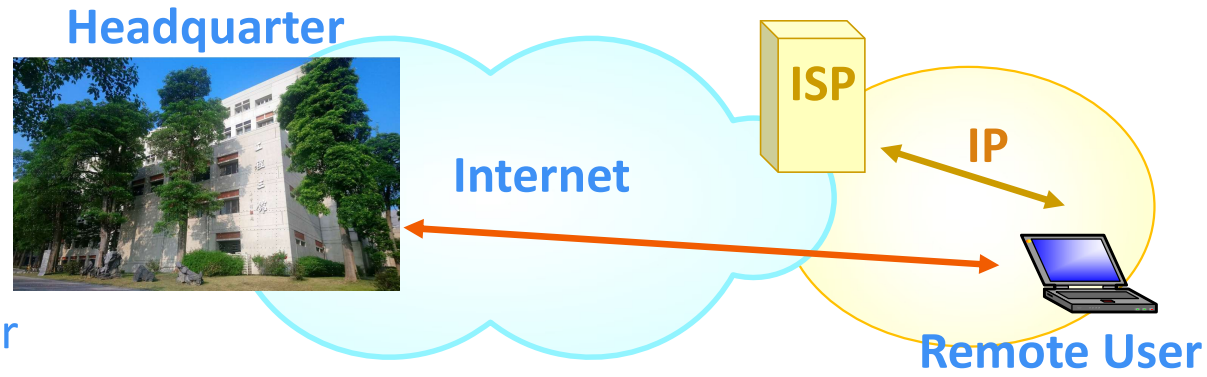
Department of Computer Science
National Yang Ming Chiao Tung University
cctseng@cs.nctu.edu.tw

References: https://www.comparitech.com/blog/vpn-privacy/ipsec-vs-ssl-vpn/

Remote Accessing a Private Network

- Legacy approaches:
  - **Site to site:**
    - Leased line networks
    - Expensive
  - Remote access (for roaming user):
    - Use ISP allocated IP
    - Untrusted

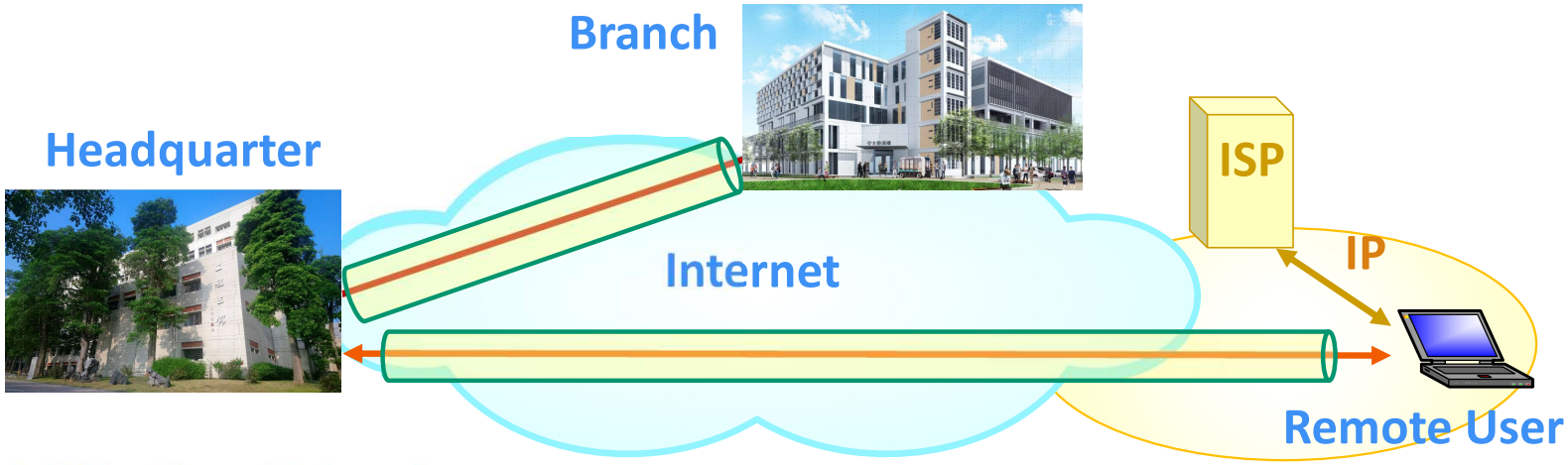




- ISP: Internet Service Provider

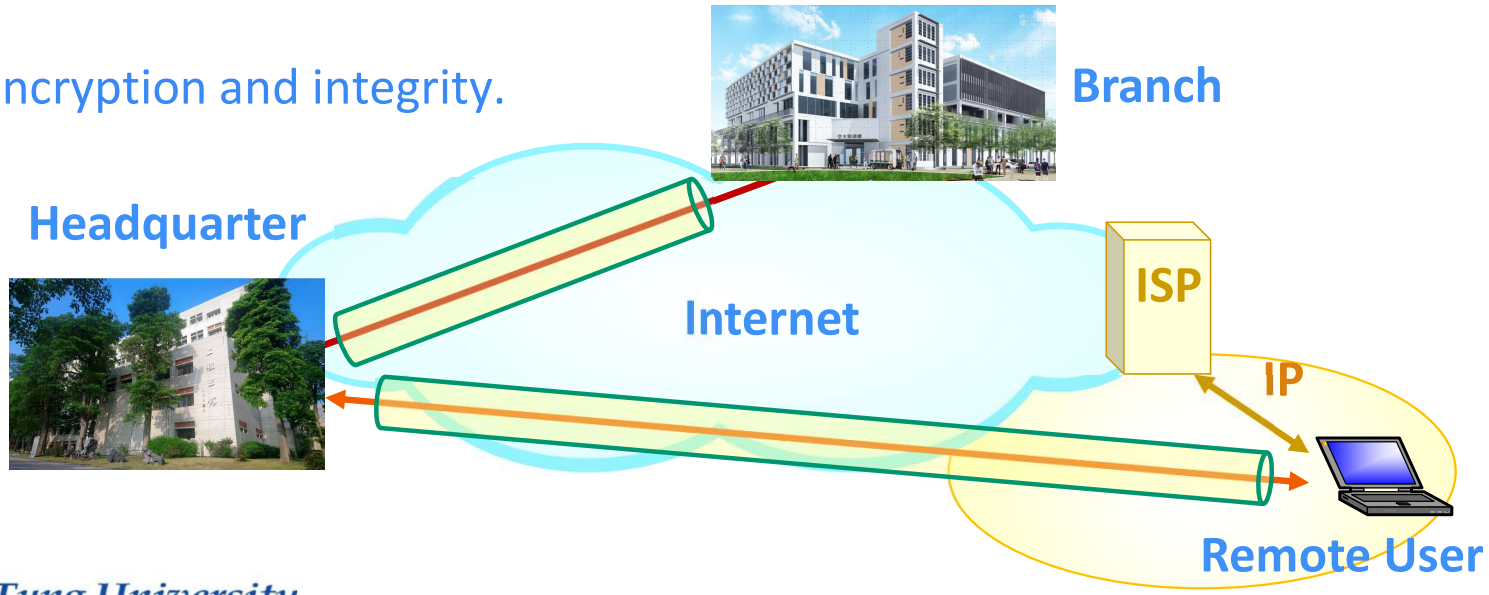
Virtual Private Network

- Extension of a private network that **encompasses** links across shared or public networks
  - **emulates** the properties of **a point-to-point private link**
  - Provide an **encrypted connection**
- Enables two hosts to send and receive data across shared or public networks
  - as if the two hosts **were directly connected** to each another



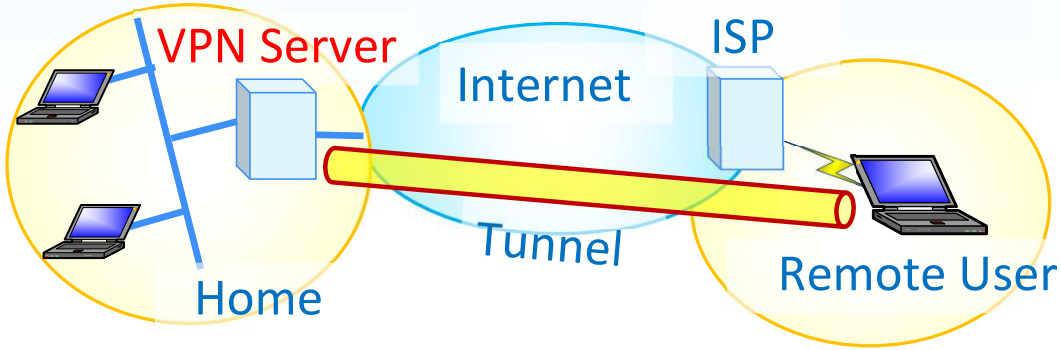
Advantages of VPN

- Advantages of VPN
  - Low cost
  - Scalable
    - Easy to scale and administer.
      - Extending a leased line connection is much more complex
  - Secured
    - With encryption and integrity.

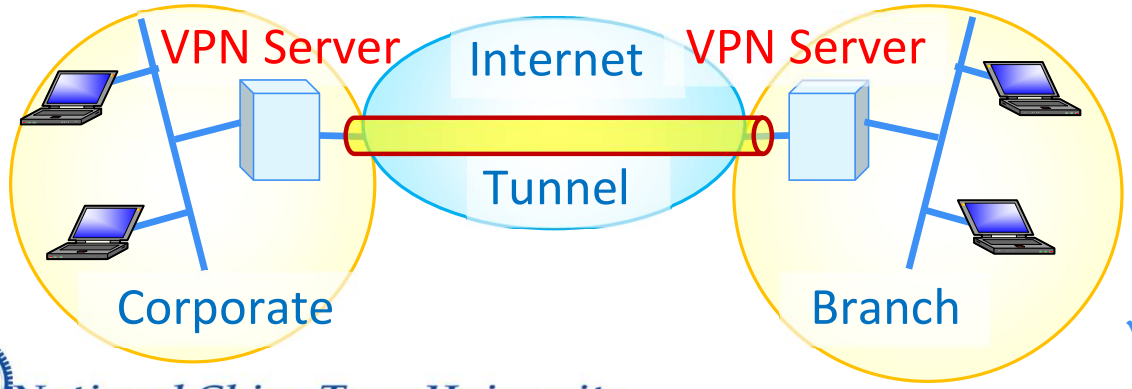


Common Use Cases of VPN

- Remote Access

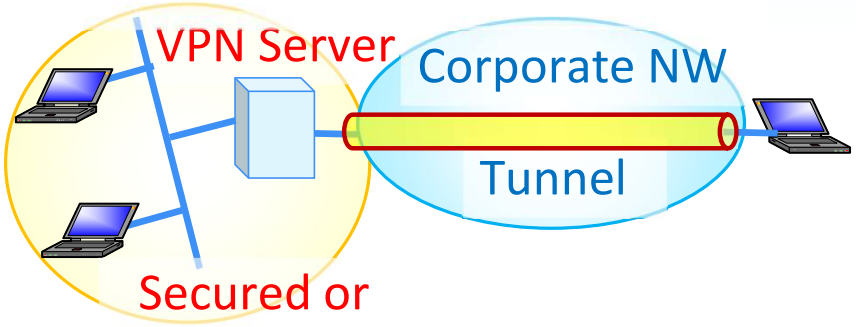


- Site to Site Connection



3. **Intranet Secured Network Access**

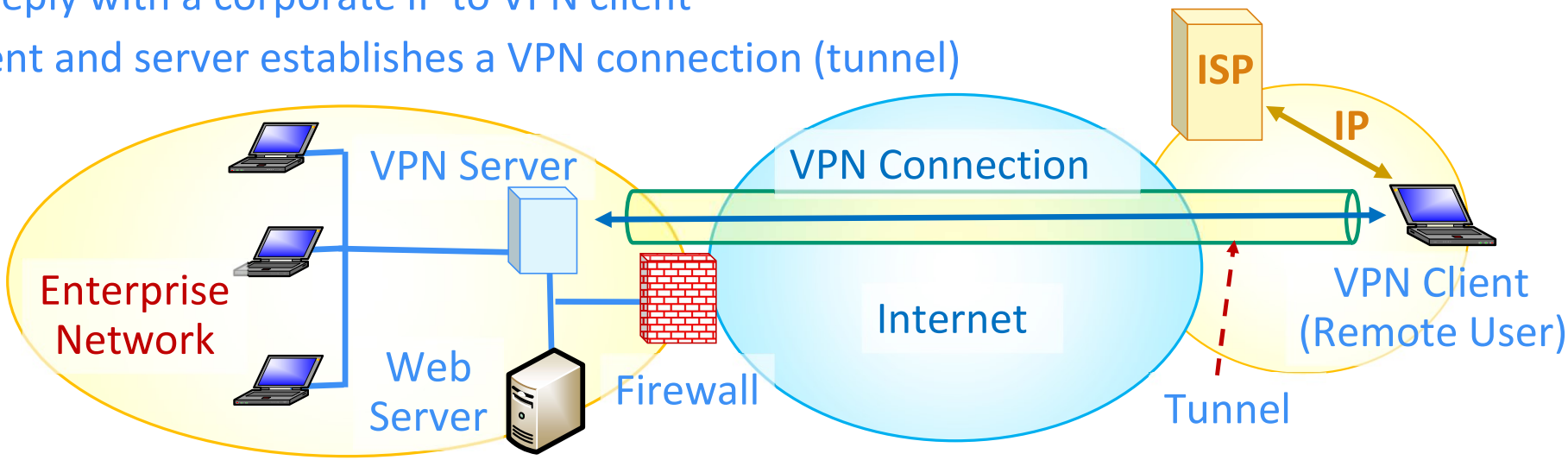
- Network Isolation



✓ Different from Virtual LAN (VLAN)

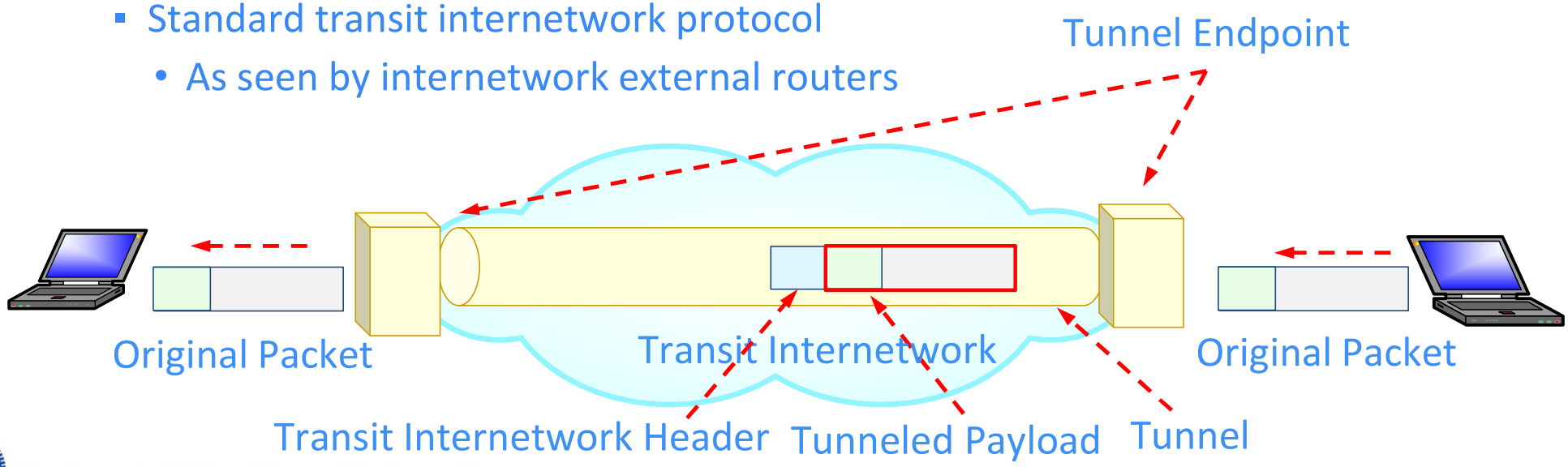
Operation Scenario with VPN

1. VPN Client (Remote user)
   - Acquires an IP from ISP and
   - Sends request to VPN server
2. VPN server
   - Authenticates VPN client (remote user)
   - Reply with a corporate IP to VPN client
3. Client and server establishes a VPN connection (tunnel)



VPN Key Concept - Tunneling

- VPN consists of a set of point-to-point connections **tunneled over the Internet.**
- **VPN Packet:**
  - Payload:
    - Original packets are encapsulated as payload of VPN tunnel packets.
  - Header:
    - Standard transit internetwork protocol
      - As seen by internetwork external routers

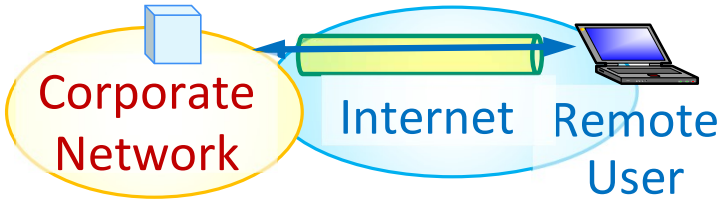


Tunneling vs. Encapsulation

- Tunneling
  encapsulates and transport PDU from one protocol **within another protocol**.
  - Unlike encapsulation, tunneling can carry **a lower-layer protocol** or a **same-layer protocol** PDU.

- IP-in-IP Tunnel

Ethernet Header	Outer IP Header	Inner IP Header	Inner IP Payload



- Generic Route Encapsulation (GRE) Tunnel [RFC 2890]

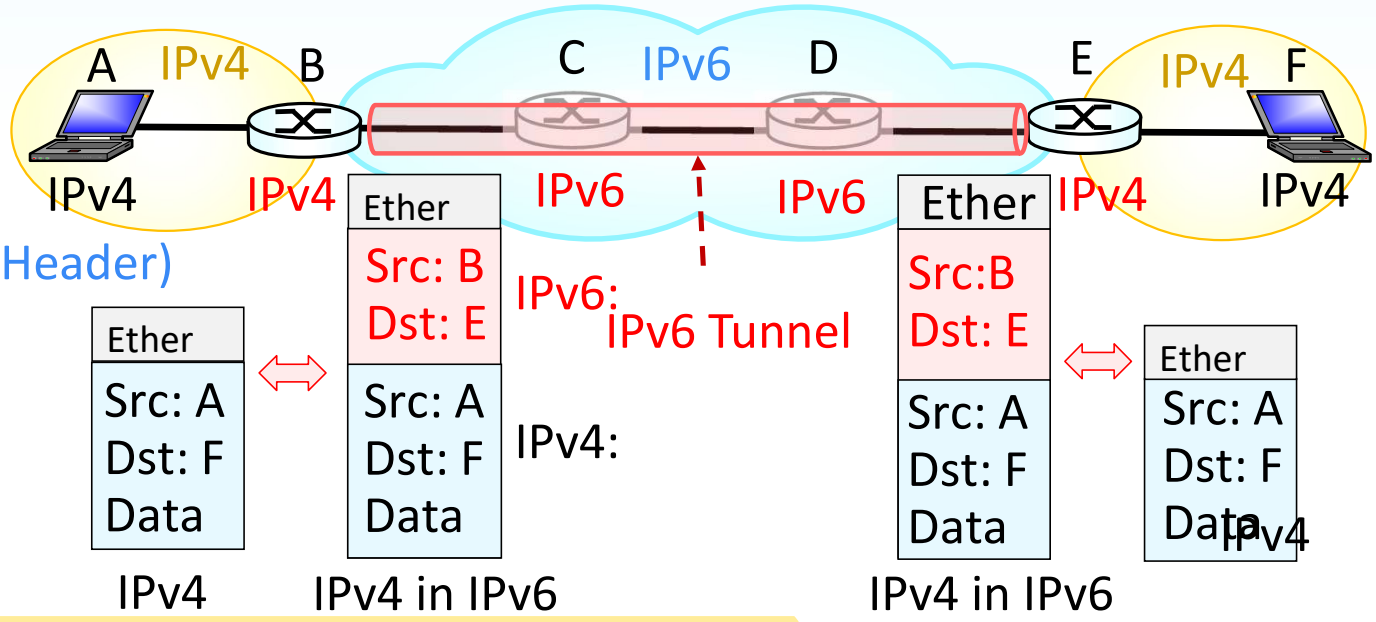
Ethernet Header	Outer IP Header	GRE Header	Inner IP Header	Inner IP Payload

- Virtual Extensible LAN (VXLAN) Tunnel

Ethernet Header	Outer IP Header	UDP Header	VXLAN Header	Ethernet Header	Inner IP Header	Inner IP Payload

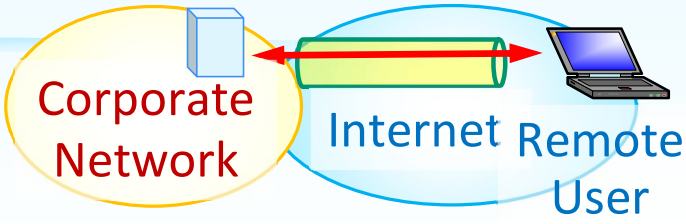
Tunneling – Use Case 1

- Provides a network service that the underlying network does not support or provide directly
- E.g., IPv6 Tunnel for IPv4 Networking
  - Protocol Value (Next Header) in IPv6 header:
    - IPv4: 0x04
    - TCP: 0x06
    - IPv6: 0x41



- IPv4 carried as payload in IPv6 datagram among IPv6 routers
  - Logical view: B ↔ E
  - Physically: B ↔ C ↔ D ↔ E

Tunneling – Use Case 2



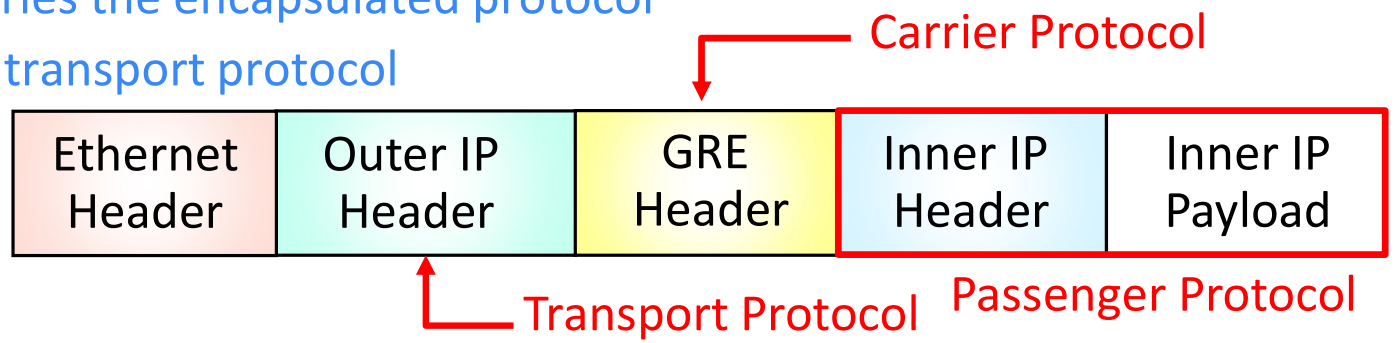
- When providing services that are impractical or unsafe using only the underlying network services,
  - E.g., Remote access to corporate network services
    - Remote user uses a network address is not part of corporate network.
    - ➢ Use GRE to establish a virtual point-to-point connection between two NWs.
- **Generic Routing Encapsulation** (GRE): RFC 2784 and updated by RFC 2890
  - A **GRE header** between the **inner** and **outer** IP headers

Ethernet Header	Outer IP Header	GRE Header	Inner IP Header	Inner IP Payload

  - IP as a transport protocol
  - **Virtual Tunnel**: **Tunnel IP Header + GRE Packet Header**
  - Encapsulation, *not* encryption

Main Components of Tunneling

- Three Main Components of Tunneling:
  - Passenger protocol
    Protocol that the tunnel encapsulates
    - e.g., IPv4, Ethernet,
  - Carrier protocol
    Protocol the tunnel uses to encapsulates passenger protocol
    - GRE, IP-in-IP, Multiprotocol Label Switching (MPLS).
  - Transport protocol
    Protocol that carries the encapsulated protocol
    - IP is the main transport protocol
- E.g., GRE Tunnel



- Reference: Cisco

VPN Requirements

- User Authentication
- Address Management
- Key Management
- Security
  - Confidentiality

    Preventing anyone from reading or copying data as it travels across the Internet.
  - Data Integrity

    Ensuring that no one tampers with data as it travels across the Internet.

Common Implementations

- Based on **Point-to-Point Protocol (PPP)**
  - Point-to-Point Tunneling Protocol (PPTP) (PPP + encryption + GRE) [2637]
  - Layer Two Tunneling Protocol (L2TP) (Origin from (Cisco L2F + MS PPTP))
- Based on **TCP/IP**
  - L2TP/IPsec
  - IPsec Tunnel Mode [RFC 4301]
  - BGP/MPLS IP VPN [RFC 4364]
- Based on **Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)**
  - Secure Socket Tunneling Protocol (SSTP) (PPTP + SSL)
  - SSL VPN
  - **OpenVPN**

✓ **Note: TLS**, and its deprecated **SSL**, are cryptographic protocols

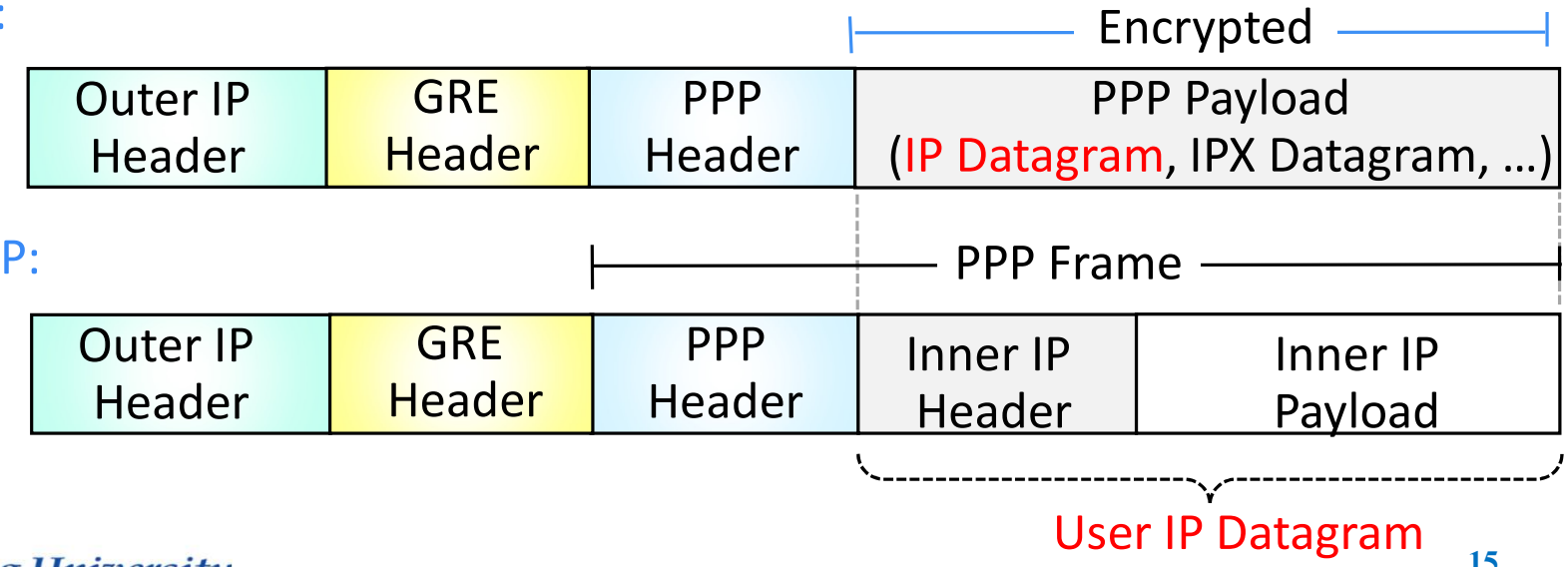
Point-to-Point Protocol (PPP) [RFC 1661]

- PPP is a Data link layer (layer 2) protocol
  - A standard method for transporting **multi-protocol datagrams** over point-to-point (direct) links.
- **Three components**
  - **Encapsulation** (for transporting purpose)
  - **Link Control Protocol** (for data-link connectivity)
  - **Network Control Protocols** (NCP) family (for L3 management support)
- Extra Options
  - Authentication: PAP, CHAP, EAP, MS-CHAP, MS-CHAPv2, etc.
  - Link Quality and error detection
  - Compression
  - Encryption: MPPC + MPPE, etc.
  - Multilink (MP, PPP Multilink Protocol)

Point-to-Point Tunneling Protocol (PPTP)

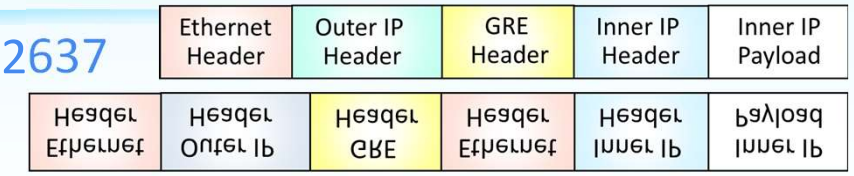
- PPTP [RFC 2637]
  - Use **PPP** to carries user data packets
  - Use an **enhanced GRE** mechanism to encapsulate PPP packets
  - Use **TCP control channel** to provide a flow and congestion control.

- Packet Format:



- E.g., IP over PPP:

Generic Routing Encapsulation (GRE) [RFC 2890]



- Enhanced GRE Header (for PPTP): defined in RFC 2637
  - A new Acknowledgment Number field,
    - Indicating GRE packets have arrived at the remote end.
      - to determine transmission rate

0						8			16	24	31
C	R	K	S	s	Recur	A	Flags		Ver	Protocol	
Checksum										Reserved	
Key Payload Length										Key Call ID	
Sequence Number (Optional)											
Acknowledgement Number (Optional)											

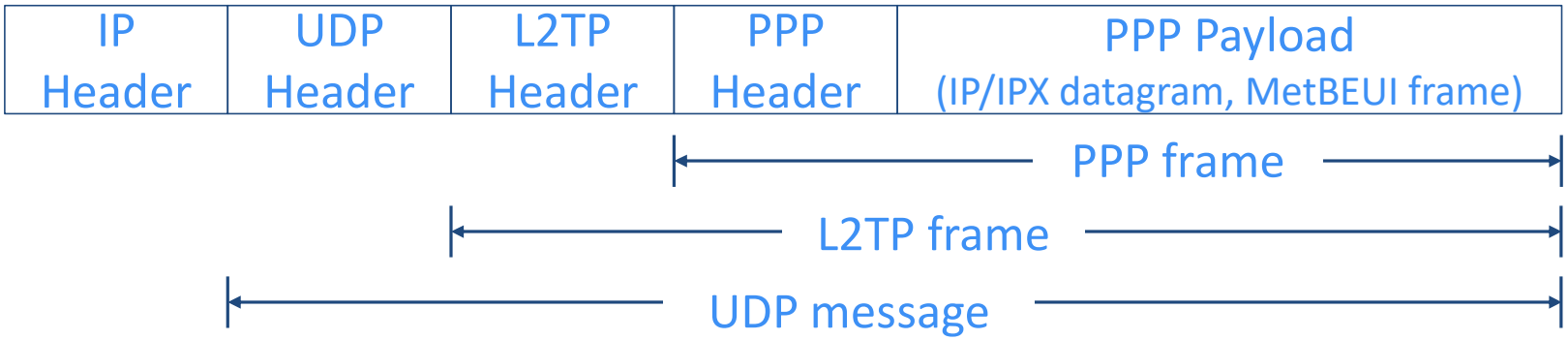
- **Protocol: Ethertype** of encapsulated protocol (IP: 0x0800, PPP: 0x880B, …)
- (Optional) **Checksum, Key, Sequence Number**

Security of PPTP

- PPTP has been the subject of many security analyses
- Serious security vulnerabilities have been found
  - MS-CHAP is fundamentally insecure.
  - MS-CHAPv2 is vulnerable to dictionary attack on the captured challenge response packets.
- PPP payload can be encrypted by using Microsoft Point to Point Encryption (MPPE) when using MS-CHAPv1/v2
- Extensible Authentication Protocol – TLS (EAP-TLS) is a superior authentication choice for PPTP.

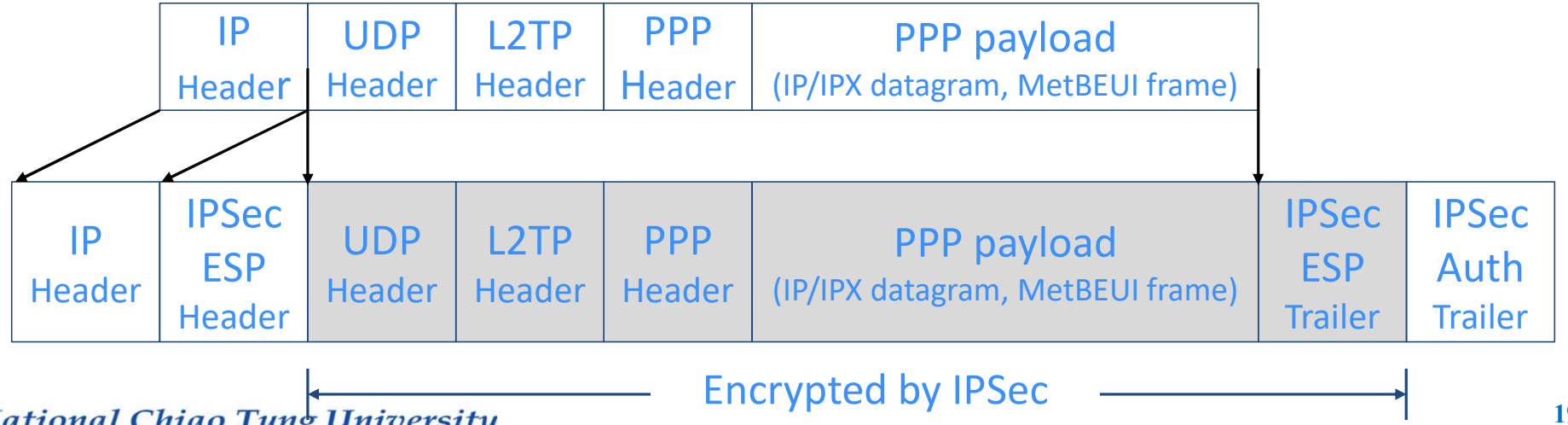
L2TP – Layer Two Tunneling Protocol

- L2TP [RFC 2661]: PPTP + L2F (Layer Two Forwarding)
- High level protocols (e.g., PPP) establish L2TP session ("call") within the L2TP tunnel, and traffic for each session is isolated.
- A tunnel can contains multiple connections at once.
- L2TP over IP internetworks uses UDP and a series of L2TP messages for tunnel maintenance.
- L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network. (Wikipedia)



L2TP/IPsec

- L2TP does not provide confidentiality or strong authentication.
- Commonly use IPsec ESP to encrypt L2TP packets.
  - IPsec: Internet Protocol Security,
  - ESP: Encapsulating Security Payload
  - Data encryption begins before PPP connection process by negotiating an IPsec security association.
  - Require computer-level authentication using computer certificates.



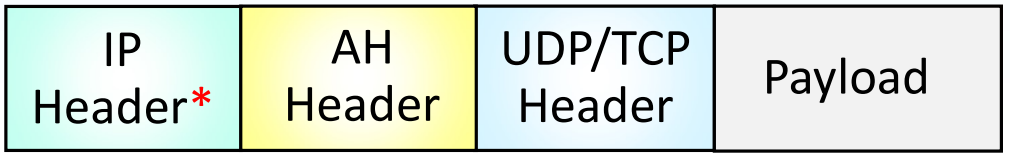
IPsec VPN – Layer 3 VPN

- IPSec [RFC 4301] is a suite of protocols designed to provide
  - authentication, confidentiality, and integrity for a VPN.
- Overview of IPSec
  - Uses **Internet Key Exchange** (IKE) to manage the connection to a peer,
  - Defines **Security Associations** used to secure and validate data exchanges, and
  - Defines two **Security Protocols** used to **carry IP traffic over the VPN**.
- ✓ **Security Protocols** determine how data plane traffic is sent through the VPN tunnel.
- **Two Distinct Protocols**
  - Authentication Header (AH): Authentication, Data integrity, and Anti-replay
  - Encapsulating Security Payload (ESP): Both Authentication and Confidentiality
- Two modes of operations:
  - Transport: IPsec header between IP and TCP header, modify original IP header.
  - Tunnel: Encapsulate original packet and prepend new IP and IPsec header.

AH and ESP

- Authentication Header: authenticates entire IP packet (IP headers and payloads)
  - Transport Mode

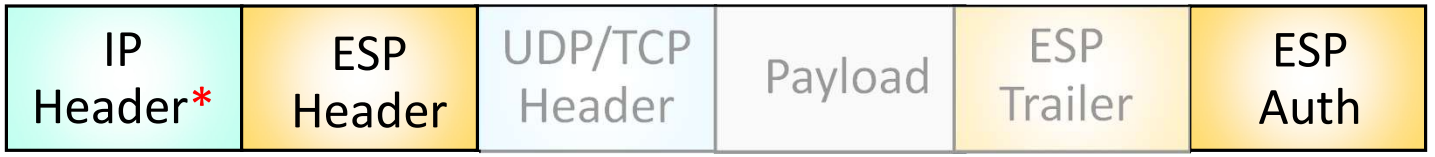
    *: Modified



  - Tunnel Mode:

- Encapsulating Security Payload (ESP): authenticates only IP datagram portion
  - Transport Mode

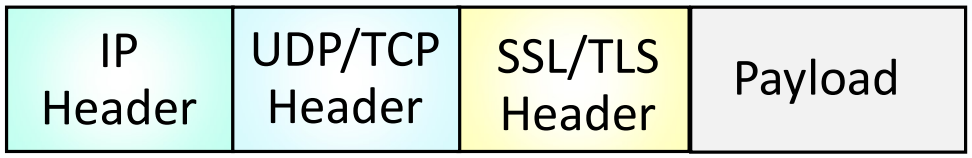
    *: Modified

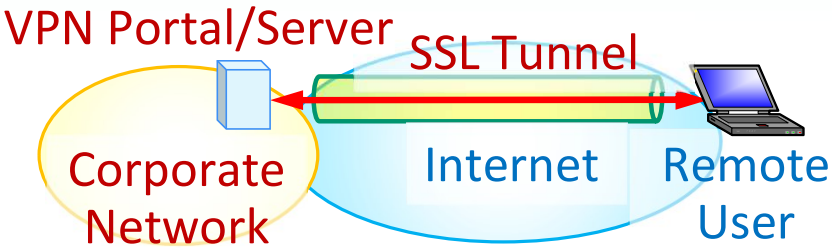


  - Tunnel Mode:

SSL VPN – Layer 4 VPN

- Uses Secure Sockets Layer (SSL) protocol or Transport Layer Security (TLS) protocol to provide secure, remote-access VPN capability





- **Two primary types:**

1. **SSL Portal VPN**:
   a **webpage** that acts as **a portal to other services**
2. **SSL Tunnel VPN**
   A circuit established between **remote user** and **VPN server**;
   - enables users to securely **access multiple network services** via
     - standard web browsers, or
     - other protocols and applications that are not web-based.

Comparison of VPNs

- PPTP at Layer 2
  - Has a pre-installed client on Windows, but suffer security vulnerabilities
  - Payload can be encrypted by using Microsoft Point to Point Encryption (MPPE)
- IPsec VPN at Layer 3
  - Requires **IPsec client software** on a client machine
  - Different vendors may have different implementations and configurations.
- SSL VPNs at Layer 4
  - More precise access control (**fine-grain** control)
  - "**Clientless VPN**" or "Web VPN": **not necessary to install a VPN client**
    - SSL/TLS function exists ubiquitously in modern web browsers.
  - Firewall and NAT-friendly (SSL is carried over TCP)
  - Ease of configuration

  ✓E.g., OpenVPN (https://openvpn.net/faq/why-ssl-vpn/)