COMP 3355 Communication Network Security

K.P. Chow

University of Hong Kong

Communication Network Security

- Introduction
- The OSI Reference Model
- The Internet Model (TCP/IP Model)
- Security at Different Layers
- Communication Security Issues

Introduction

- Communication network: an infrastructure for exchanging information in electronic form
  - a physical infrastructure: communication links (wires and cables), routers, repeaters, and other devices
  - a logical infrastructure, which includes communication protocols that give “meaning” to the electronic impulses or binary information exchanged over the network

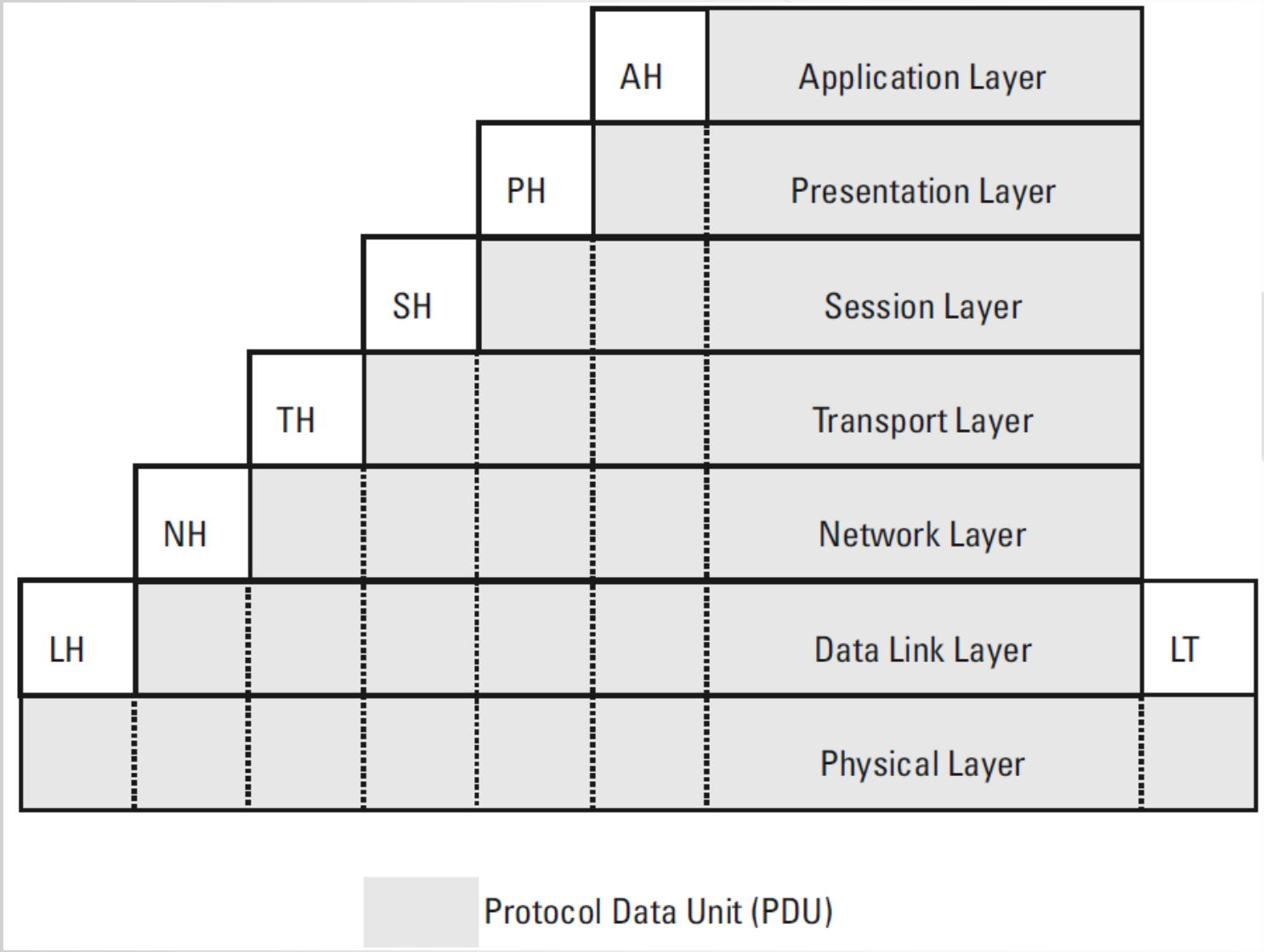
Communication Network

- Types of information: voice, documents, photos, or video
- Types of communication network
  - a public switched telephone network
  - a mobile telephone network
  - the Internet
  - a common infrastructure (i.e., a common communication network), for exchanging various types of information.

The OSI Reference Model

- The 7-layer OSI (Open Systems Interconnection): one of the frequently used models for explaining the logical structure of a communication network
- Function of each layer: provides a subset of communication services in such a way that it uses the services from the next lower layer and provides services to the next higher layer

The 7-layer OSI reference model.



The OSI Reference Model

- Encapsulation: each layer receives a protocol data unit (PDU, i.e., the data to be transmitted) from the next higher level and appends its layer-specific control information in the form of a header (e.g., AH, PH, SH). The data link layer additionally appends a trailer (LT)

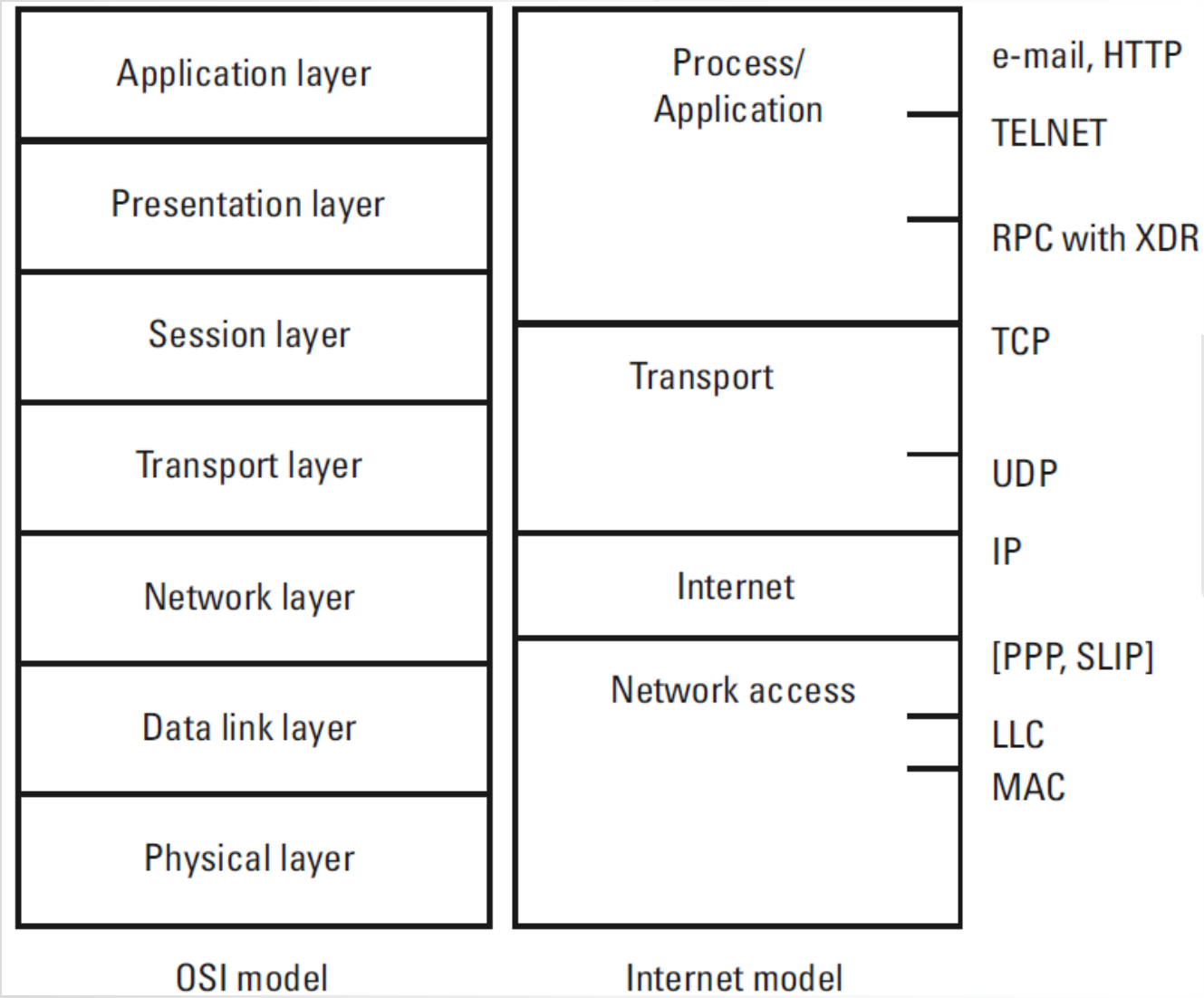
Seven Layers of OSI

1. The **physical layer** provides the point-to-point connection managed by the data link layer
2. The **data link layer** establishes the "point-to-point" connection
3. The **network layer** provides the "end-to-end" connection between two systems
4. The **transport layer** is to provide a reliable data exchange mechanism between processes running on different end systems
5. The **session layer** is necessary for applications that need a mechanism for establishing, managing, and terminating a session (i.e., a dialogue) between them
6. The **presentation layer** translates between the local data representation & the representation used for infomation exchange
7. The **application layer** provides an access point to the OSI environment as well as certain distributed infomation services

The Internet Model (TCP/IP Model)

- The Internet model is based on the TCP/IP protocol suite: a protocol suite is a set of ***cooperating*** communication protocols
- The name “Internet” is used to refer to a network using the internetworking technology based on that protocol suite

The OSI reference model and the Internet model.

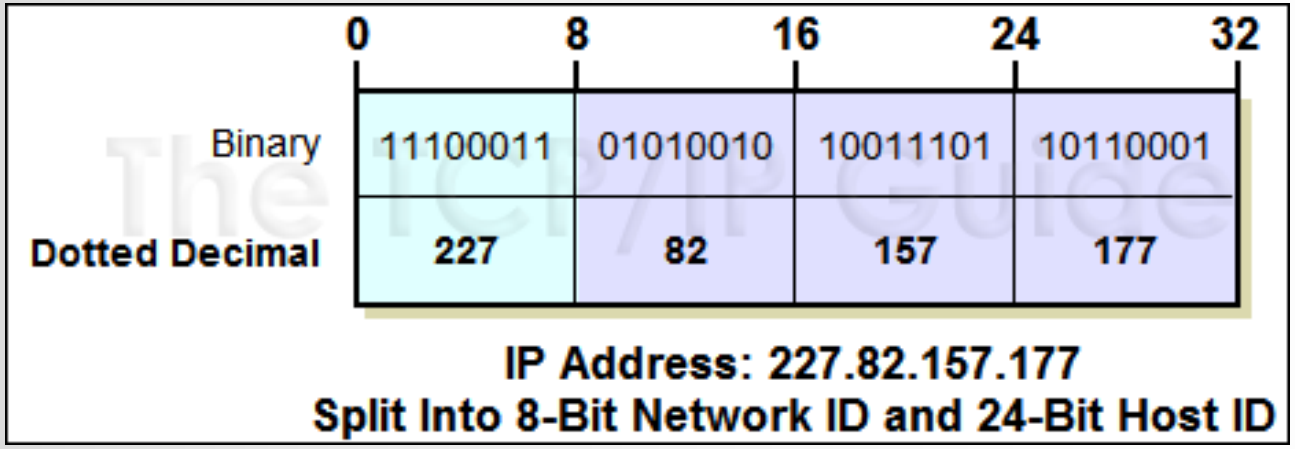


Four layers in TCP/IP – Network Access Layer

- The **network access layer** roughly corresponds to that of the OSI data link and physical layer: makes communication possible between a host and the transmission medium
  - The **Logical Link Control** (LLC, IEEE 802.2 standard) sublayer: addressing hosts across the transmission medium and for controlling the data link, routing data between hosts attached to the same local area network (LAN).
  - The **Medium Access Control** (MAC) sublayer: "hides" the specifics of the underlying physical transmission medium (e.g., optical fiber or twisted pair), the network topology, and the medium control technique employed (e.g., Ethernet based on the IEEE 802.3 standard, or token ring from IEEE 802.5).

Four layers in TCP/IP – Internet Layer

- The **Internet layer** (the core part of the Internet): makes internetworking possible since it allows data to be sent between two hosts even if they are not attached to the same LAN. Its most important task is ***routing***, that is, deciding to which host to send a piece of data even if the routing host has no idea how the actual path to the destination host will look
  - The routing is based on the 4-byte IP addresses (IPv4)



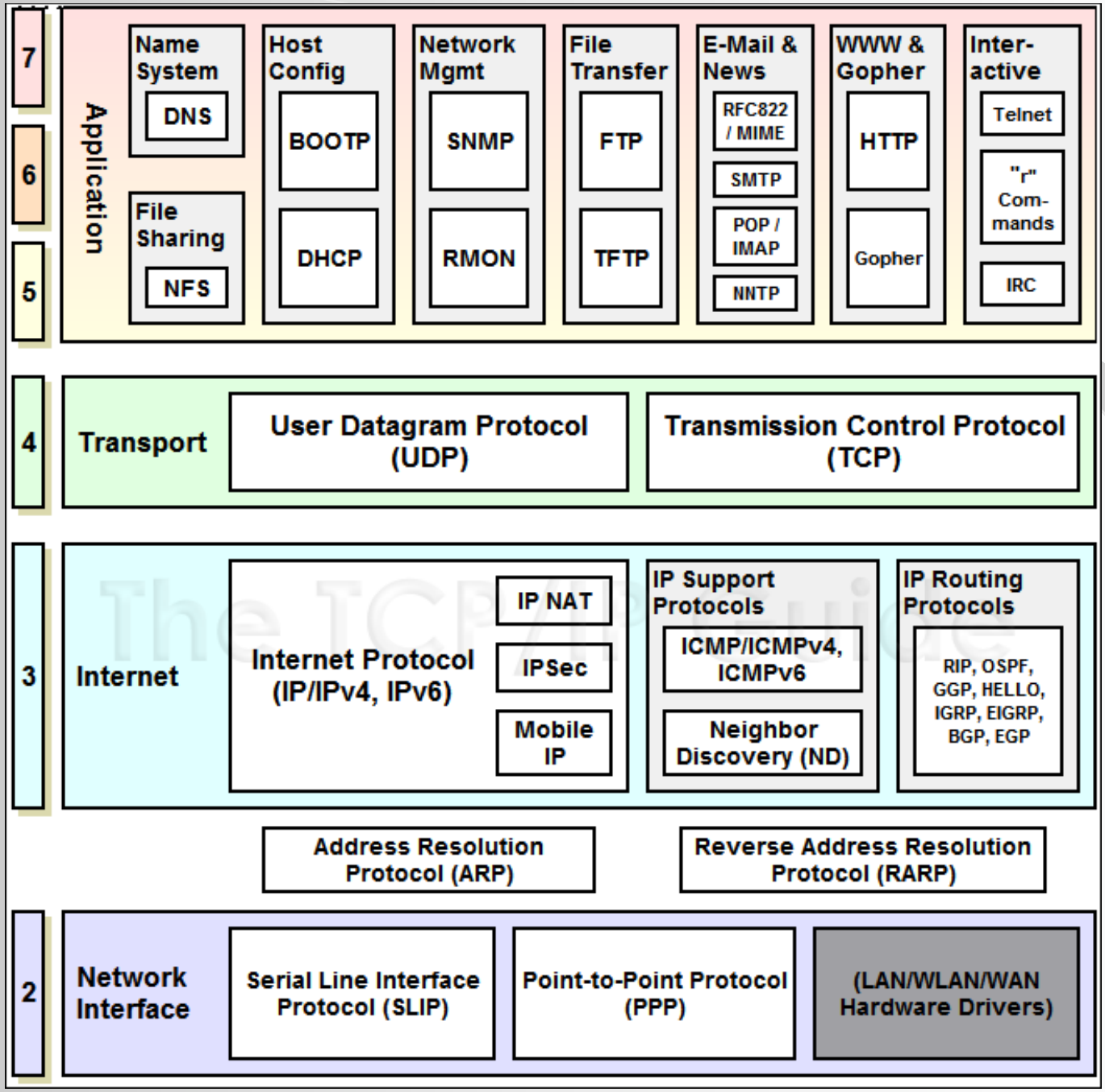
Four layers in TCP/IP – Transport Layer

3. The **transport layer** (the host-host layer): supports the exchange of data between processes running on different hosts. It is in charge of allowing logical connections to be made between devices to allow data to be sent either unreliably or reliably
   - Transmission Control Protocol (TCP)
   - User Datagram Protocol (UDP)

Four layers in TCP/IP – Application Layer

4. The **process/application layer**
   - Encompass layers five through seven in the OSI model

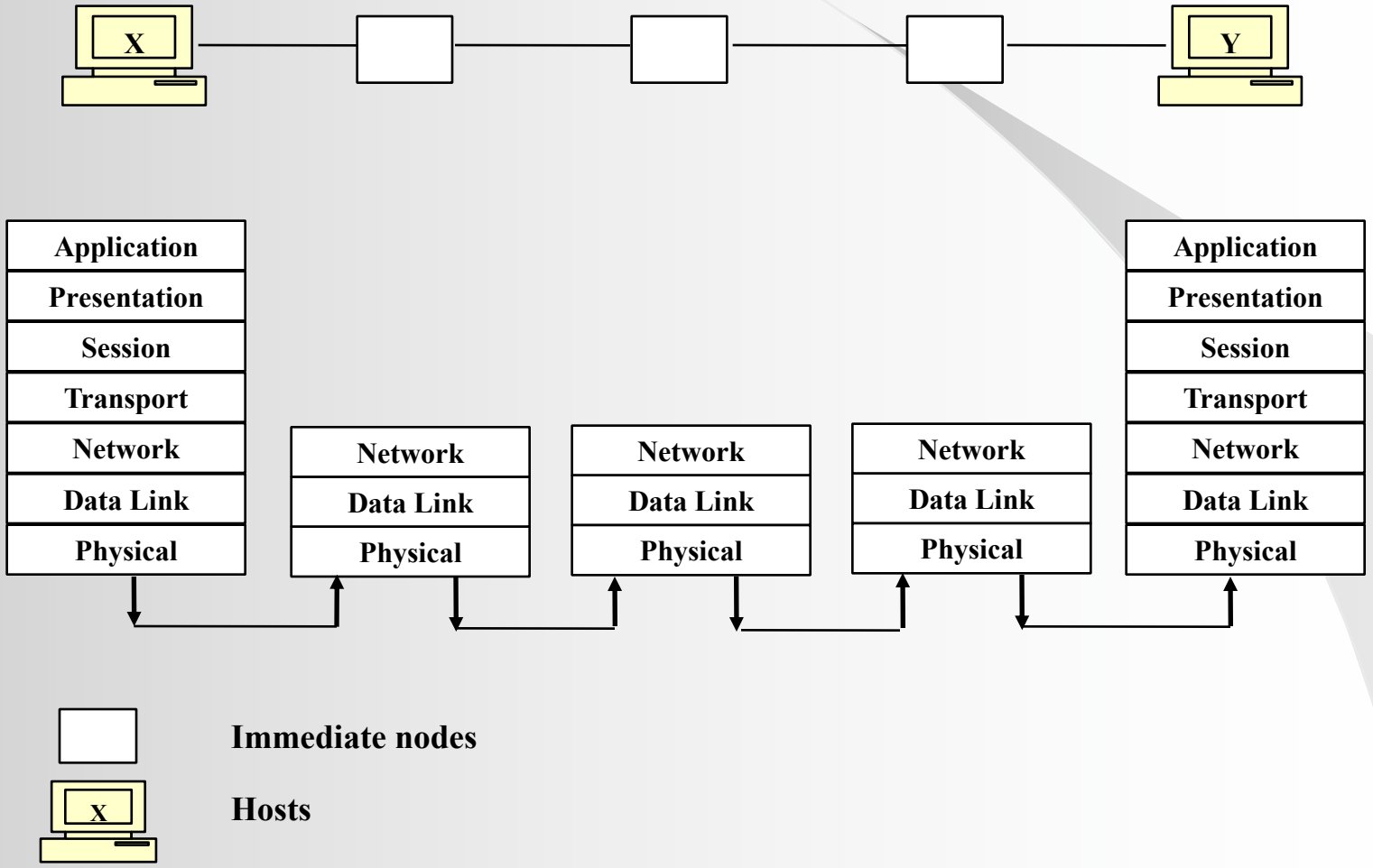
TCP/IP Protocols



TCP/IP versus OSI

- TCP/IP Protocols are considered to be standards around which the Internet has developed. The OSI model however is a **"generic, protocol-independent standard."**
- TCP/IP appears to be a more simpler model because it has fewer layers
  - TCP/IP combines the presentation and session layer issues into its application layer
  - TCP/IP combines the OSI data link and physical layers into the network access layer
- TCP/IP is considered to be a more credible model because TCP/IP protocols are the standards around which the internet was developed, where as in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool

TCP/IP Communication



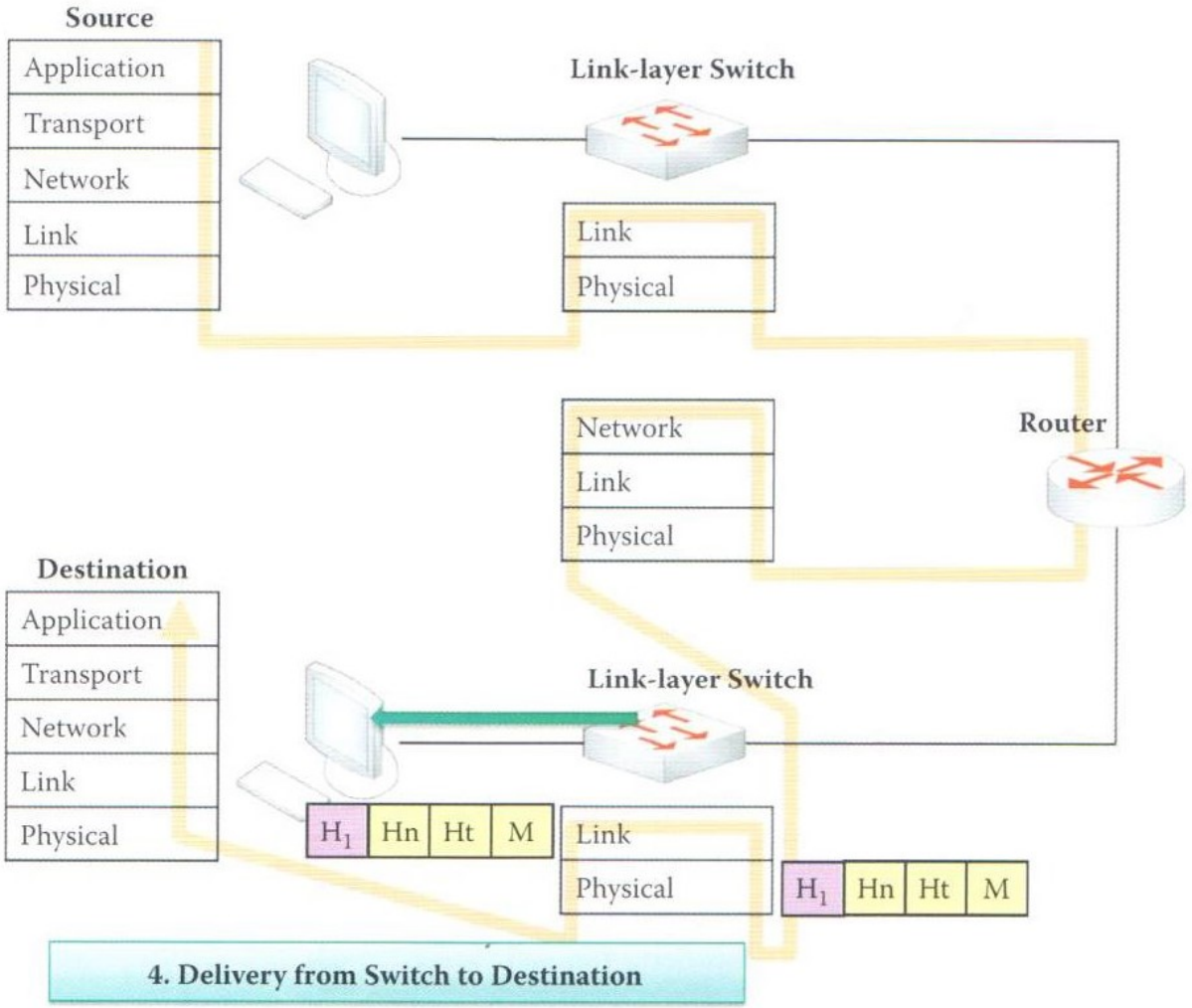
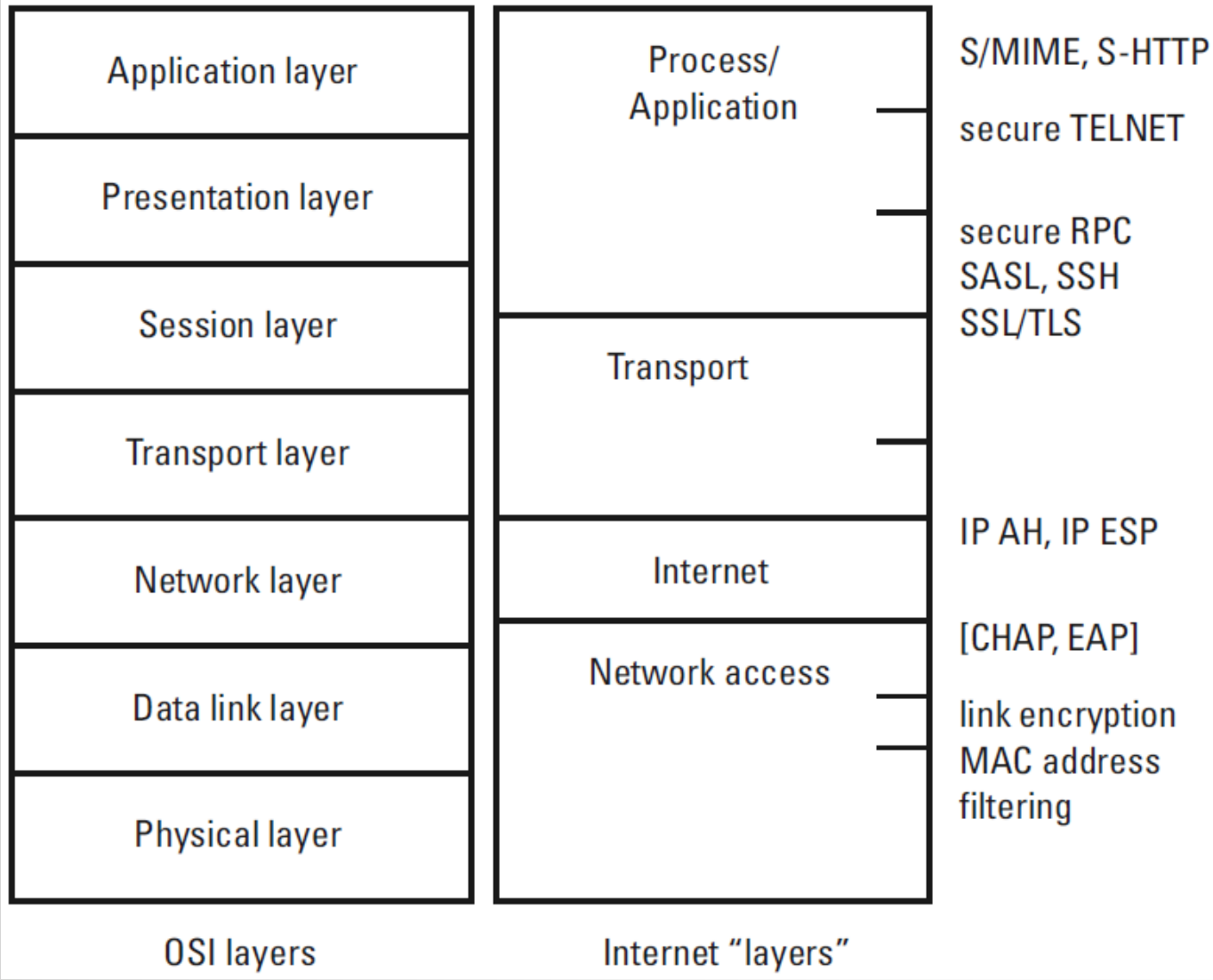


FIGURE I.35 Delivery from switch to destination.

Security Mechanisms at Different Layers



Layer N and Layer N-1

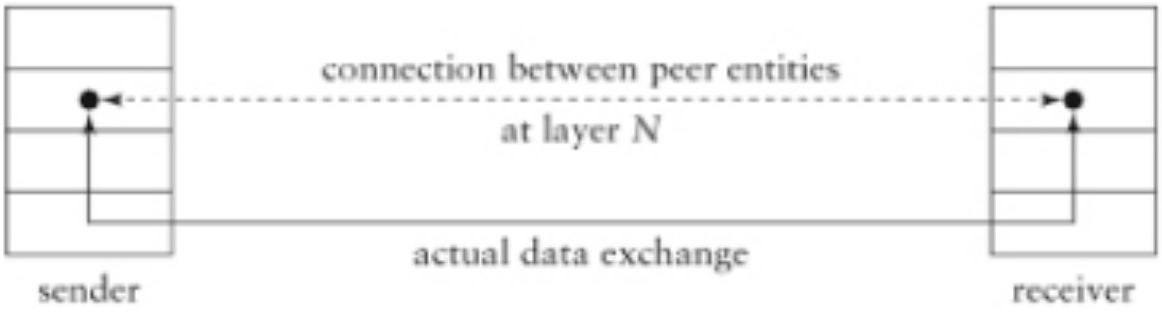


Figure 16.2: Virtual Connection at Layer N

Figure 16.3: Processing an (N)-PDU

PDU = Protocol Data Unit

Security Implementation in Layers

- To implement security in Layer N, it can use Layer N-1 as follow:

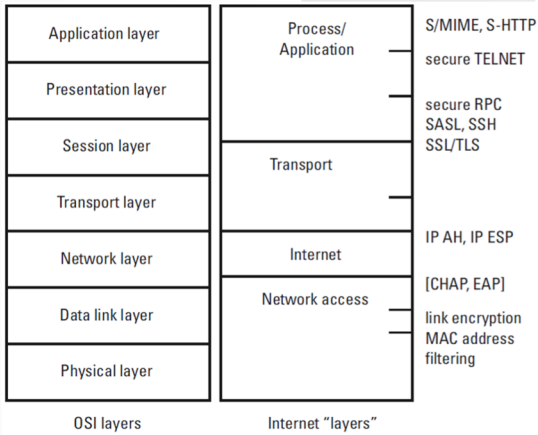
1. The Layer N can be aware of the security services at the Layer N-1:
   - the Layer N protocol has to change its calls so that they can explicitly refer to the security facilities provided
2. Layer N-1 security services could be transparent:
   - the Layer N protocol does not have to change

Security at the Physical or Data Link Layers

- Advantage: provide secure point-to-point communication
- Disadvantages:
  - Cannot extend protection across heterogeneous networks
  - If link-level encryption is used, each link must be equipped on both ends with an encryption device. Additionally, a message must be decrypted at each intermediate node so that the higher-level protocols can read their control information, and then encrypted again.
  - Key management is extremely complex
  - Because the message is decrypted at each device, it is exposed to attacks at each intermediate node, which is a severe disadvantage

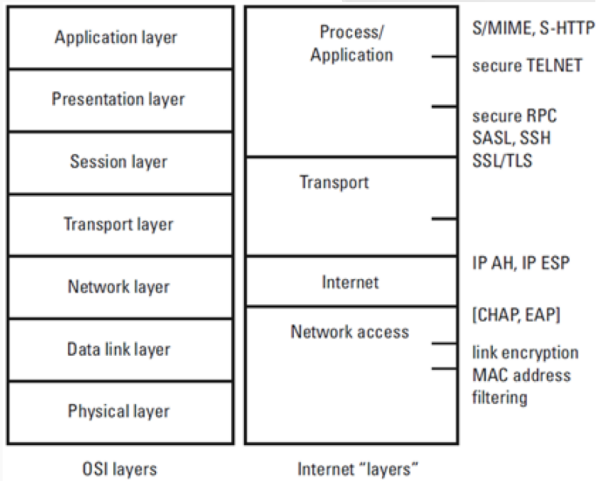
Security at the Internet Layer

- Advantages:
  - It is transparent to users and applications: a single tunnel secures all communications between the devices, regardless of traffic type (TCP, UDP, SNMP) or applications (email, client-server, database)
  - The security software is installed and maintained by experienced system administrators, which makes it less likely to contain malicious code
- Disadvantages
  - Internet-layer security requires changes to the underlying operating system
  - It is necessary that all communicating hosts use compatible versions of network security software
- E.g. VPN with IPsec



Security at the Transport Layer

- Disadvantages:
  - **Each application** must be security aware, i.e. use corresponding function calls: each security application is secured one at a time
  - The transport security library must be installed and maintained by the system administrator so that all applications running on a host can use it
- Advantage:
  - The applications running on the internal hosts need not be security aware
  - Some enterprises use special purpose SSL VPN gateways that are deployed at the edge of the corporate network and serve as a proxy to internal applications, e.g. email, file servers
- E.g. VPN tunnel using SSL

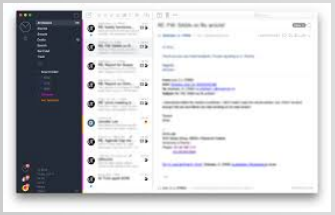


SSH client

Transport layer

SSH server

Require proper mail ports binding



Mail client

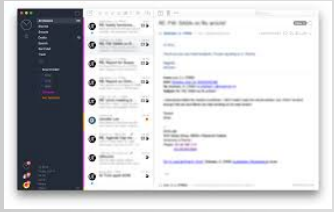
Mail server (need not be security aware)

IPsec VPN

Internet layer

IPsec client

Does require proper mail ports binding



Mail client

Security at the Application Layer

- Advantages:
  - It involves no changes in the operating system since only a secure application must be installed
  - It offers better end-to-end security since the setup and cryptographic computations take place outside the operating system
  - The security functionality can be developed to fulfill the application requirements exactly
- Disadvantages:
  - It may require more complex negotiations and setup between communicating processes
  - Secure applications are often installed by inexperienced users, which makes the danger of malicious code quite high
- E.g. e-banking login

Which layer to implement security? Protocol Selection Criteria

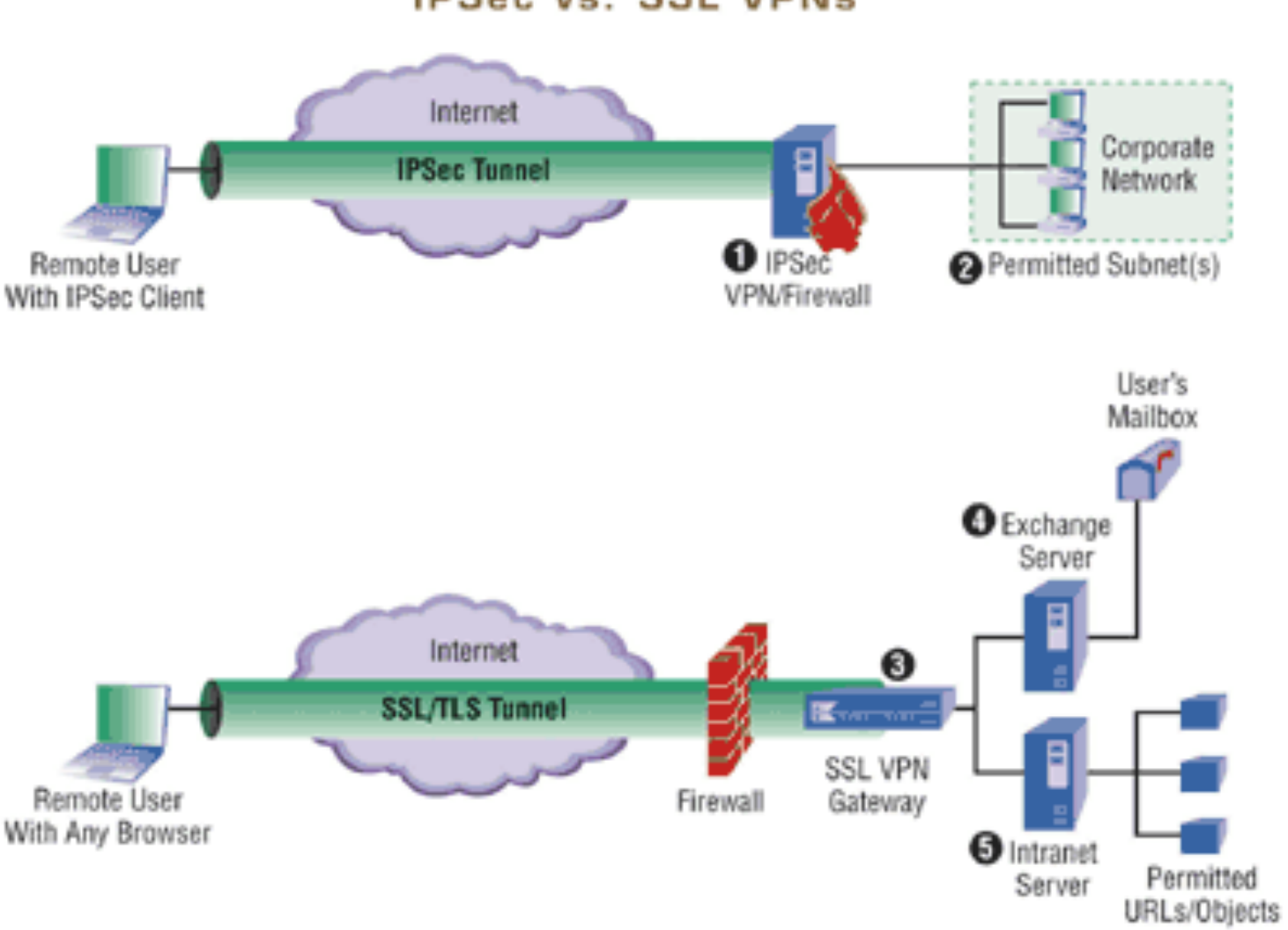
- Who should be authenticated? Host or user?
- Is end-to-end security a requirement, or is it sufficient to implement a perimeter protection?
- How much should security implementation and maintenance cost? E.g. experience system administrator cost
- Will the security extensions allow interoperability among different platforms? If not, additional cost to support those not interoperable
- Are the security protocols based on inter-industry standards and supported by multiple vendors? If not, why?

Should I use SSL or IPsec?

What is SSL?
What is IPsec?

IPSec vs. SSL

FIGURE 1



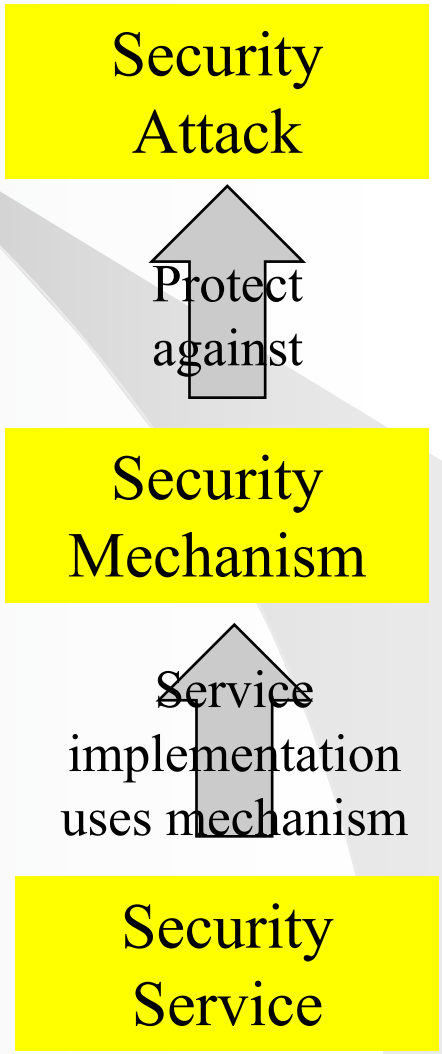
IPSec VPN gateways ❶ are usually implemented on the perimeter firewall, and permit or deny remote host access to ❷ entire private subnets. SSL VPN gateways ❸ are usually deployed behind the perimeter firewall, with rules that permit or deny access to application services or data. In this example, SSL users have access to their own mailboxes on ❹ an Exchange Server and to a subset of URLs hosted on ❺ an intranet Web server.

Should I use IPsec or SSL to provide remote access?

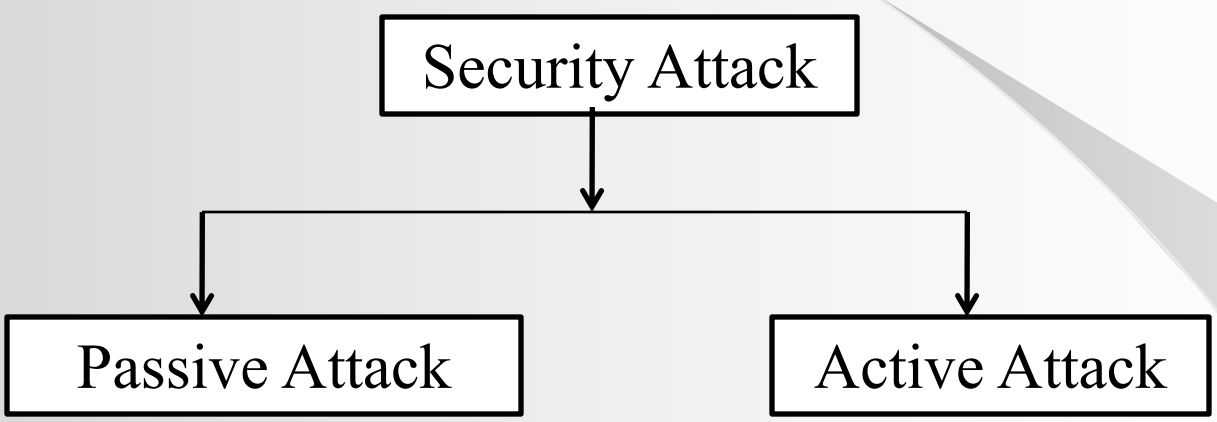
	SSL	IPsec
Applications	Web-enabled applications, file sharing and emails	All IP-based services
Encryption	Strong but vary	Strong and consistent
Authentication	One or two way authentication	Strong: two way authentication
Users	Sales, marketing, …	HR, finance, IT staff, ..
Accessibility	Casual access	Formal access with controlled user base
Complexity	Moderate	High
Easy of use	Very high	Moderate
Scalability	High	High

OSI Security Architecture

- **Security attack** – Any action that compromises the security of information owned by an organization
- **Security mechanism** – A mechanism that is designed to detect, prevent, or recover from a security attack
- **Security services** – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service



X.800 - The OSI Security Architecture



- Eavesdropping on or monitoring of transmission to
  - obtain message content
  - perform traffic analysis

- Modification of data stream or creation of false data stream to
  - masquerade
  - replay
  - modify messages
  - modify control information
  - infiltration
  - perform denial of service

Vulnerabilities and flaws

- Weak cryptographic algorithms
- Cryptographic design vulnerabilities
- Software implementation vulnerabilities
- Hardware implementation vulnerabilities
- Trust model vulnerabilities
- Social engineering and human factors
- Bad failure-recovery procedures

X.800 - The OSI Security Architecture

Security Mechanisms

- Encipherment
- Digital signature
- Access control
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

Security Services

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

Relationship between security services and mechanisms

	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			