Security of Network

Prof. Dr. Eşref ADALI

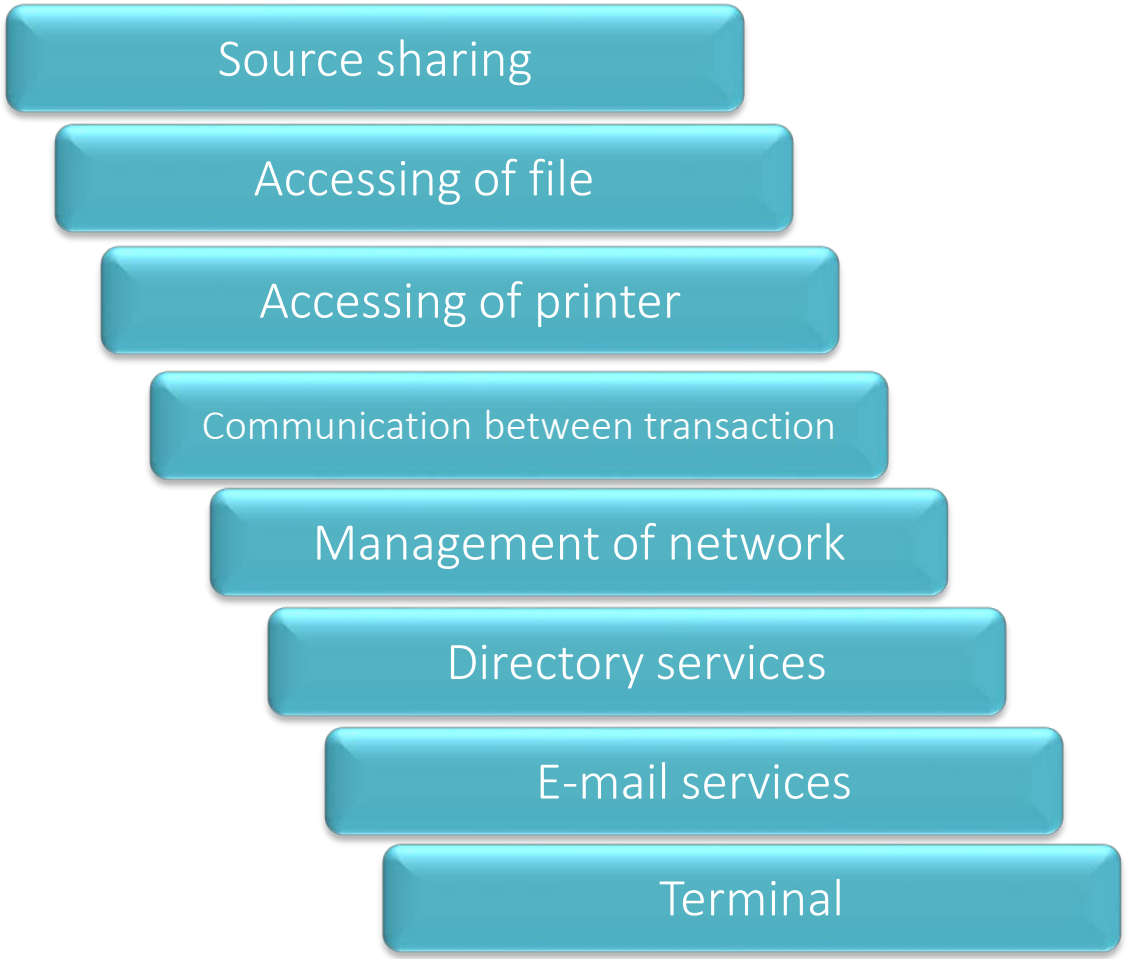
www. Adalı.net

ISO/OSI Protocol

Layer No	Layer Name	Objective
7	Application	Software Application software
6	Presentation	
5	Session	
4	Transport	Middle layer: Between hardware and software
3	Network	Hardware Hardware for network
2	Data Link	
1	Physical	

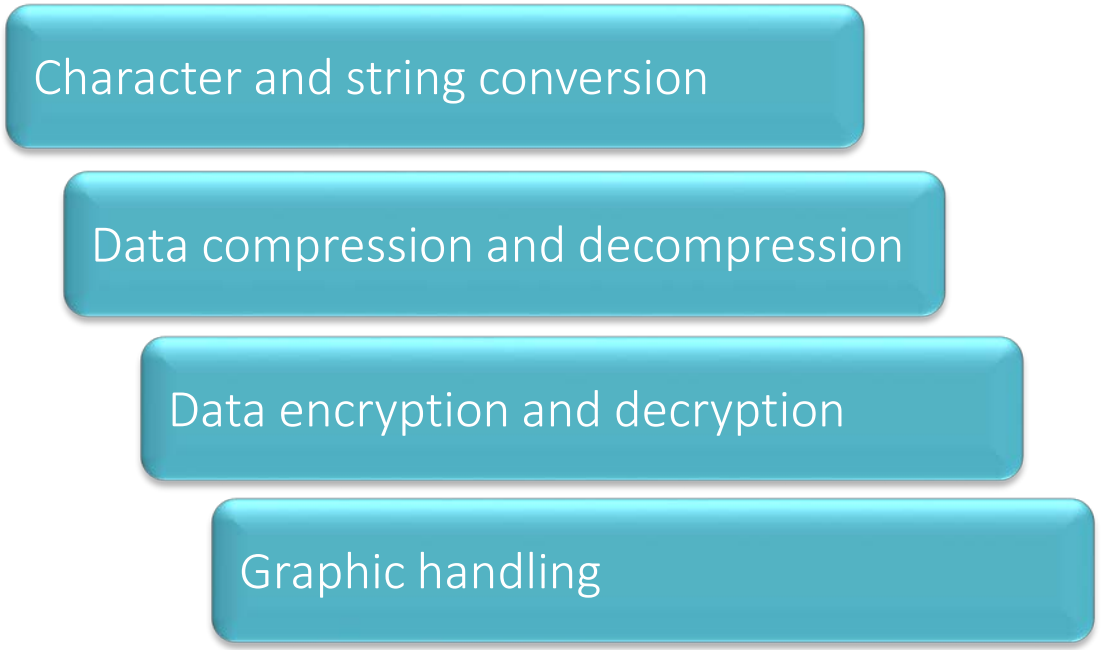
Published in 1980 by ISO (International Standard Organization)

Application Layer



- This layer interacts with software applications that implement a communicating component.
- Some standards : http, https, frt, smtp

Presentation Layer



- Presents data to the application layer in an accurate, well-defined and standardized format.
- Some standards： PICT, TIFF, JPEG, MIDI, MPEG, HTML

Session and Transport Layers

Session

- Controls the connections between multiple computers.
- Establishes, controls and ends the sessions between local and remote applications.

Transport

- Responsible for end-to-end communication over a network.
- Provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.
- Also responsible for the management of error correction,

Network and Data Link Layers

Network

- Provides data routing paths for network communication. Data is transferred in the form of packets via logical network paths in an ordered format controlled by the network layer.
- Responsible of logical connection setup, data forwarding, routing and delivery error reporting.

Data link

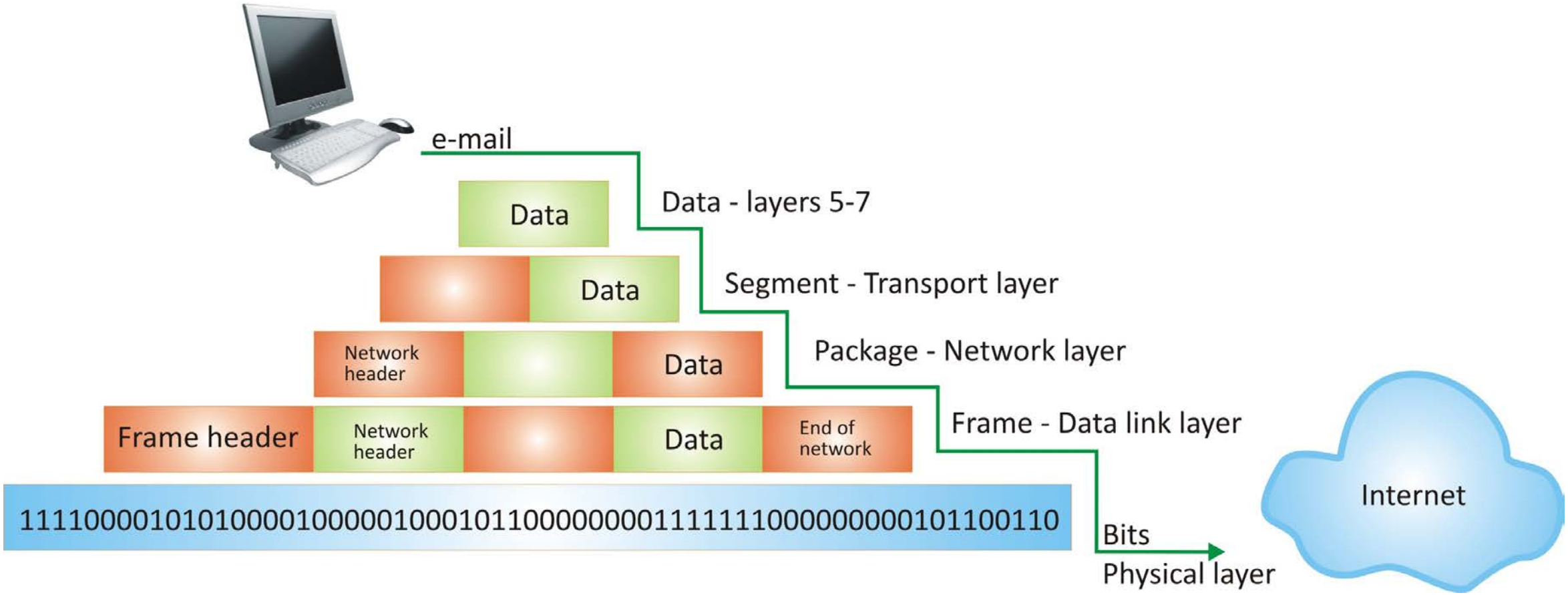
- This layer is used for the encoding, decoding and logical organization of data bits.
- Data packets are framed and addressed by this layer which has two sublayers.
    1. Media access control (MAC) layer. It is used for source and destination addresses.
    2. Logical link control. It manages error checking and data flow over a network.

Physical Layer

The physical layer deals with bit-level transmission between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.

Examples : 10BaseT, 100 BaseT, UTP, RJ-45, IEEE 802.5

Steps of e-mail in OSI

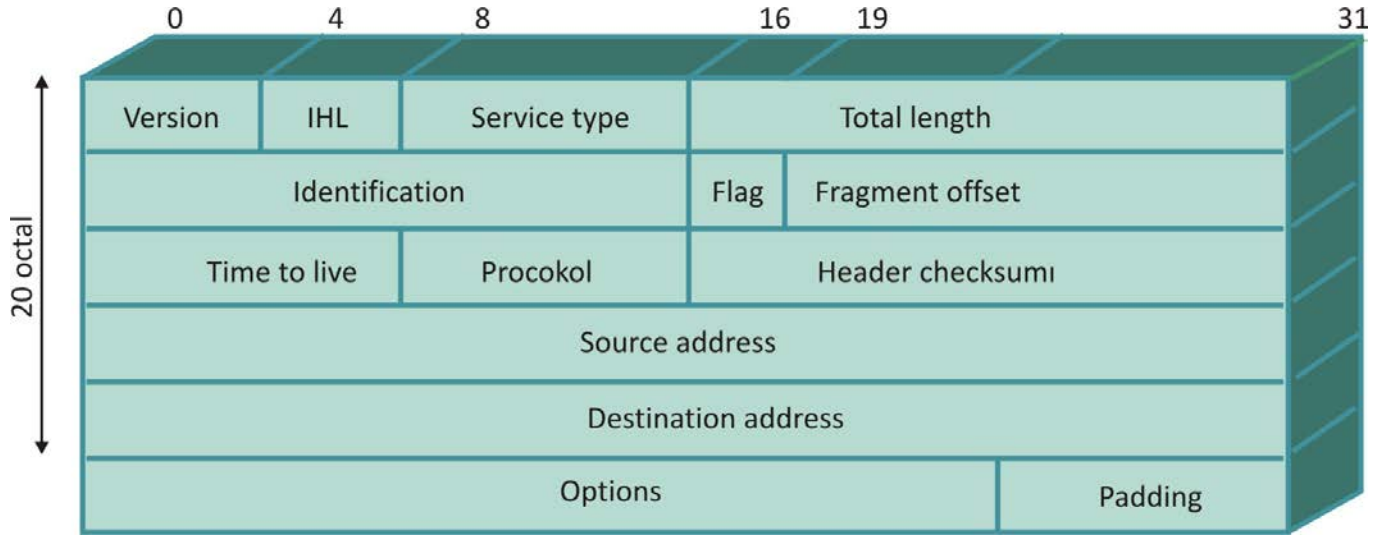


ISO/OSI and TCP/IP Protocols

Layer No	ISO/OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
		Network access
2	Data Link	
1	Physical	Physical

- TCPI/IP is developed by DoD (Department of Defense), in 1980.
- Firstly is used for ARPANET then Internet
- Has two layers:
  1. Upper : Consists of application and transport layer
  2. Lower : Consists of Network and network access layer

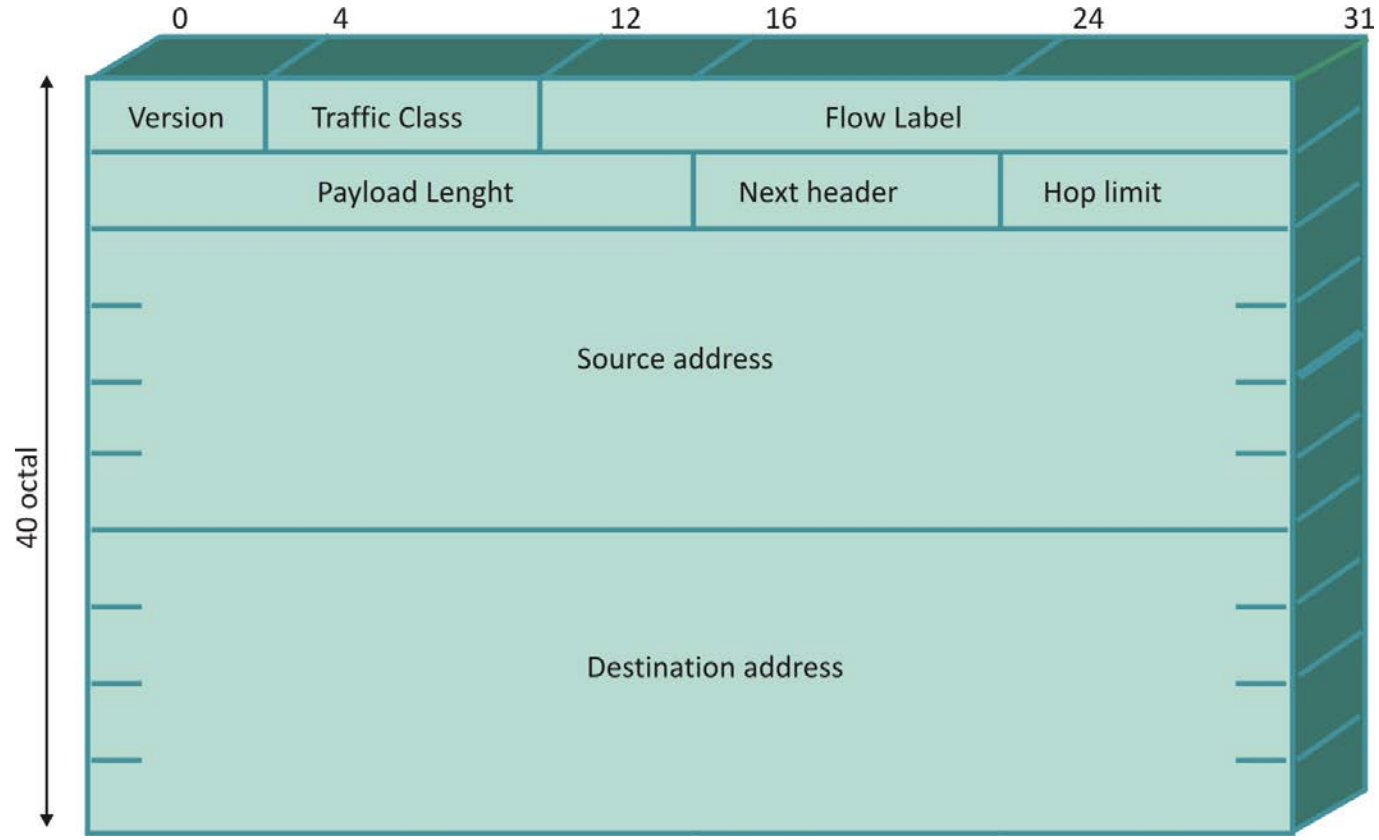
Header of IPv4



IHL : Internet Header Length
TTL : Time to Live

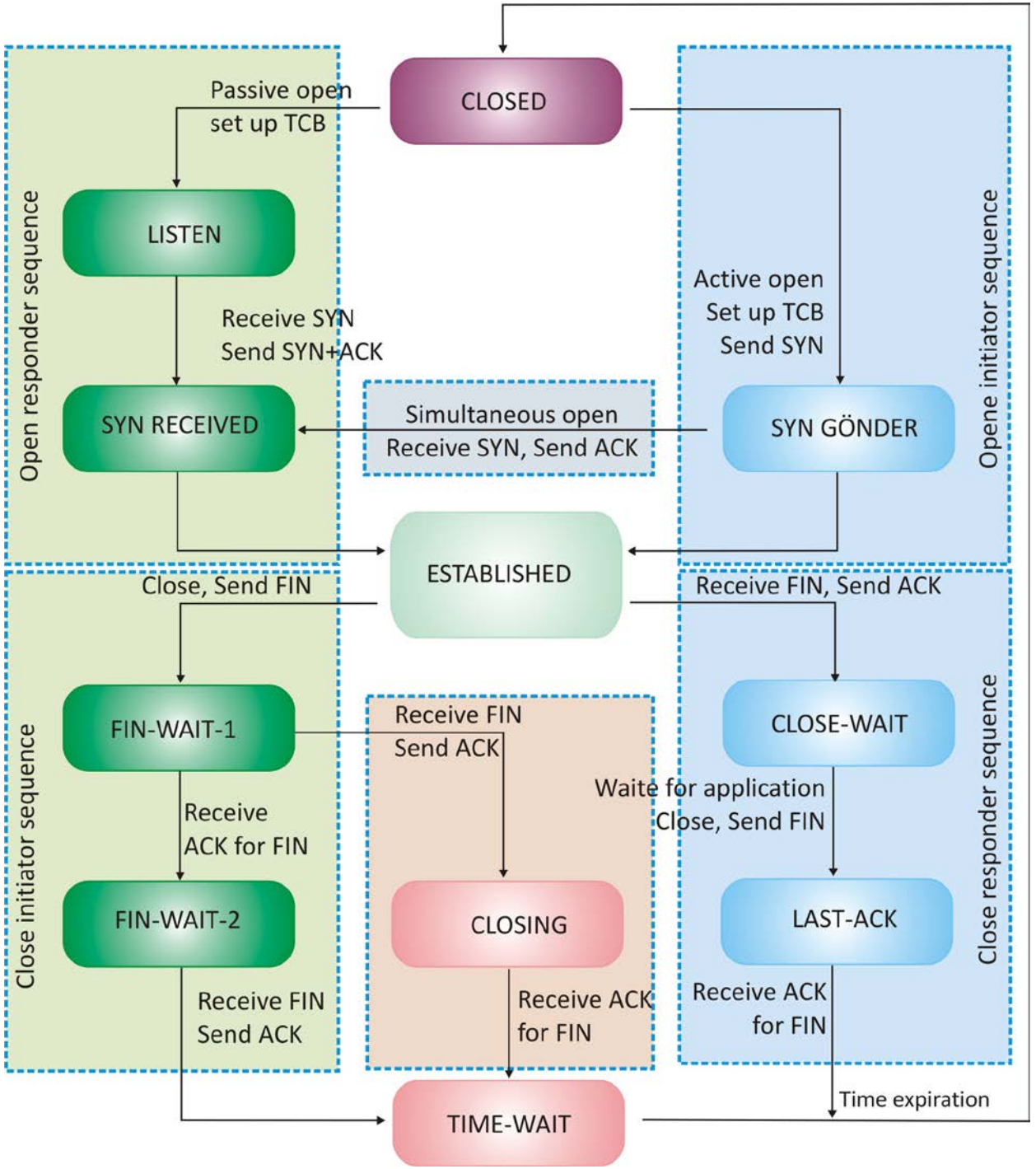
Developed in 1981

Header of IPv6



Developed in 1990

Open and Close a Session in TCPI/IP

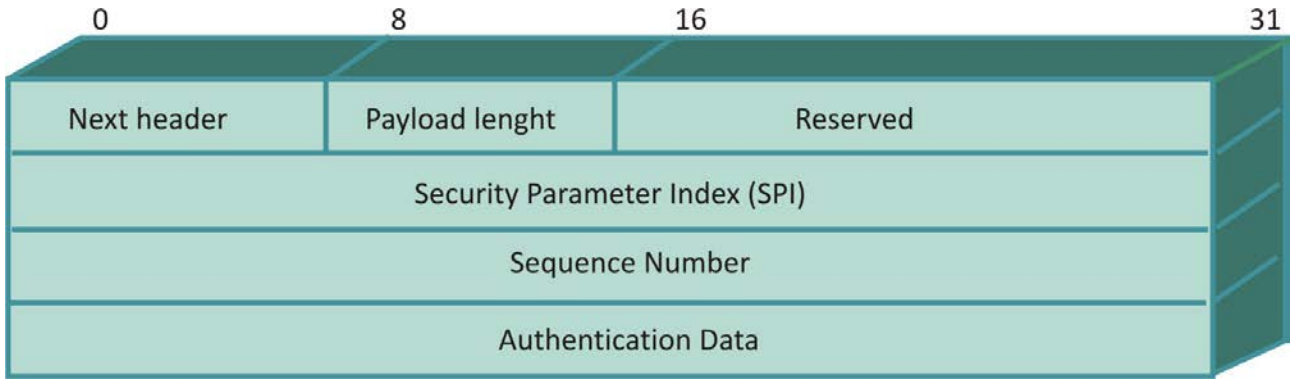


Security of TCPI/IP v4

Attacks

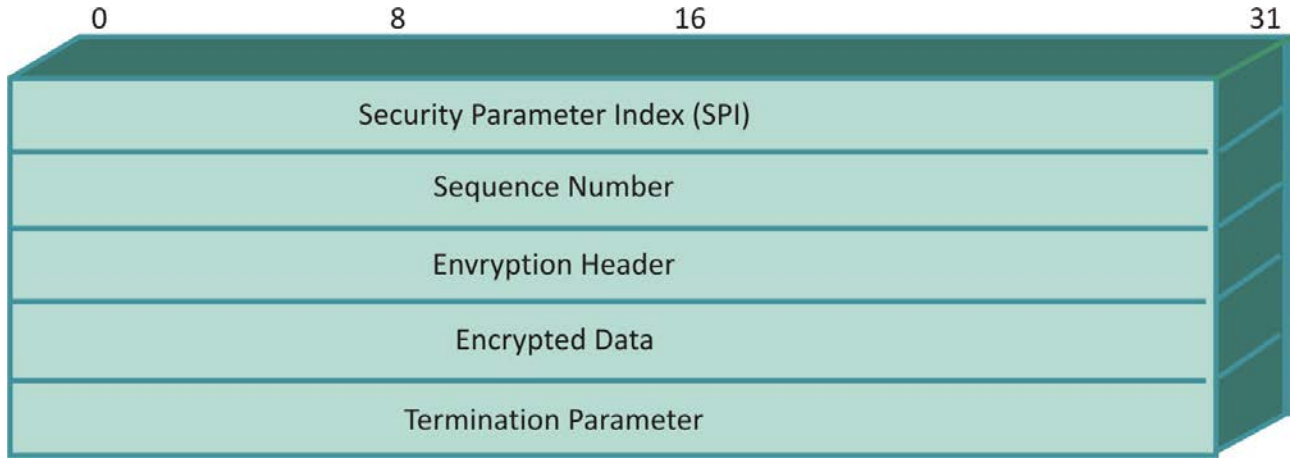
- SYN Attack
- IP spoofing, DDos attacks
- Guessing of Initial Sequence Number
- Source redirection
- ICMP (Internet Control Message Protocol) attacks.
- DNS spoof ing
- Missing of unique ID

Security of TCPI/IP v6



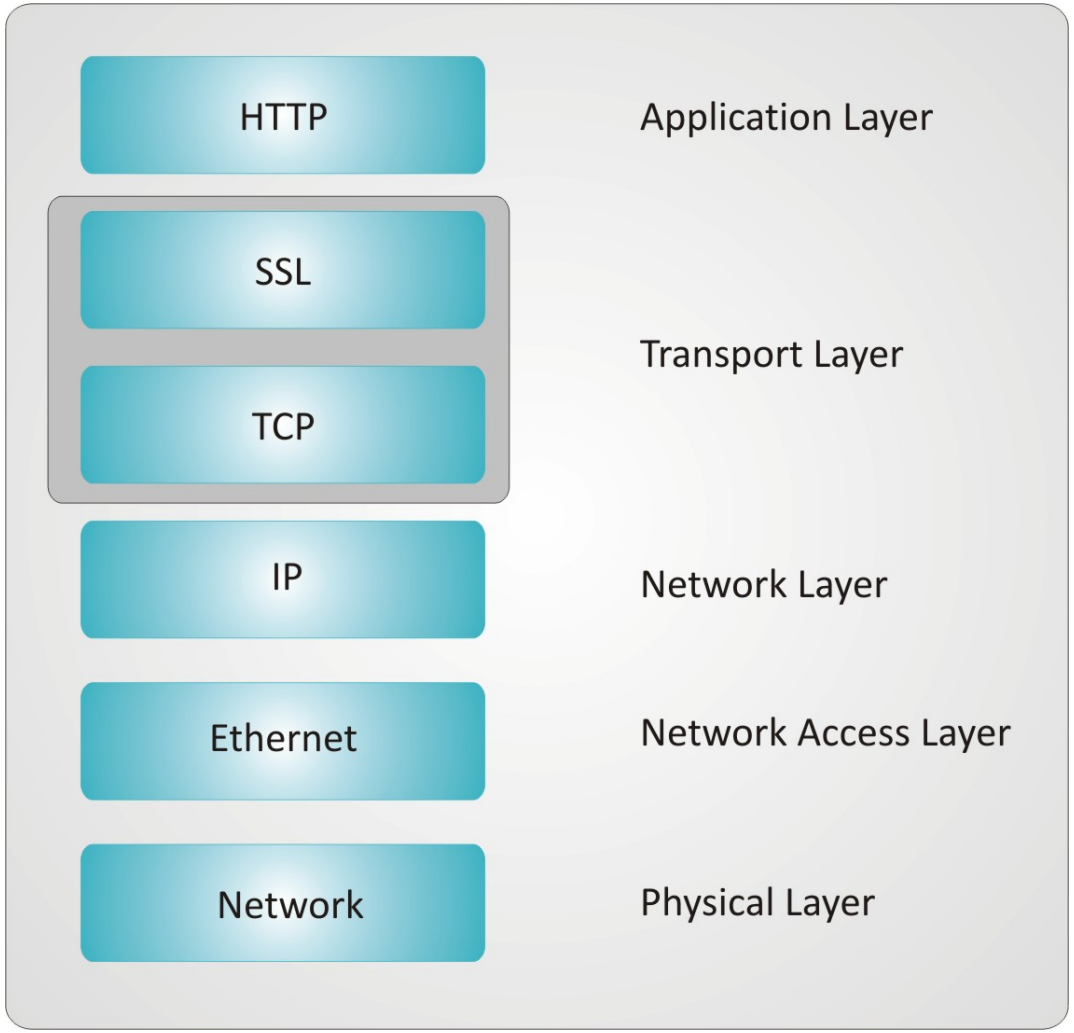
Authentication Header

Encryption Header

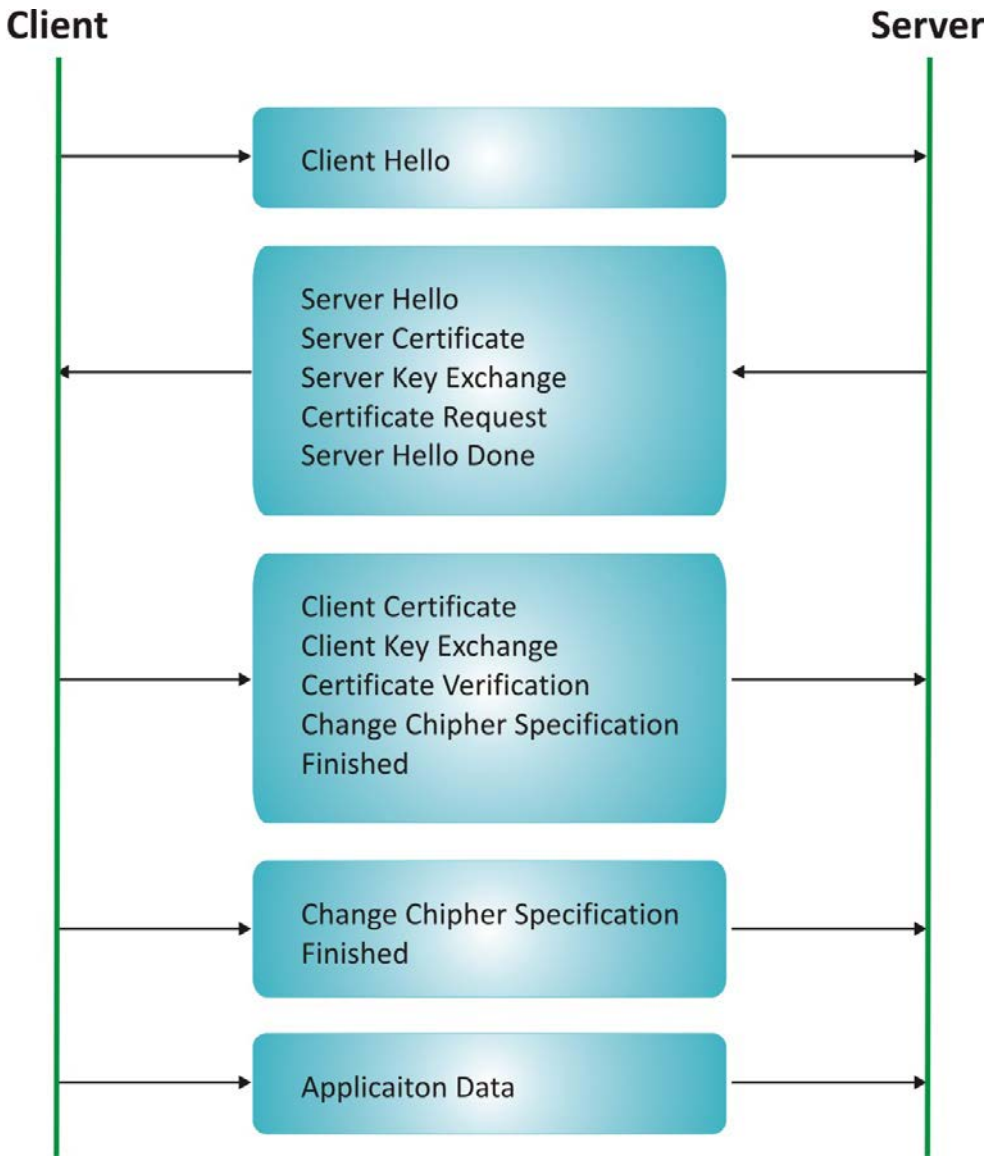


SSL/TSL

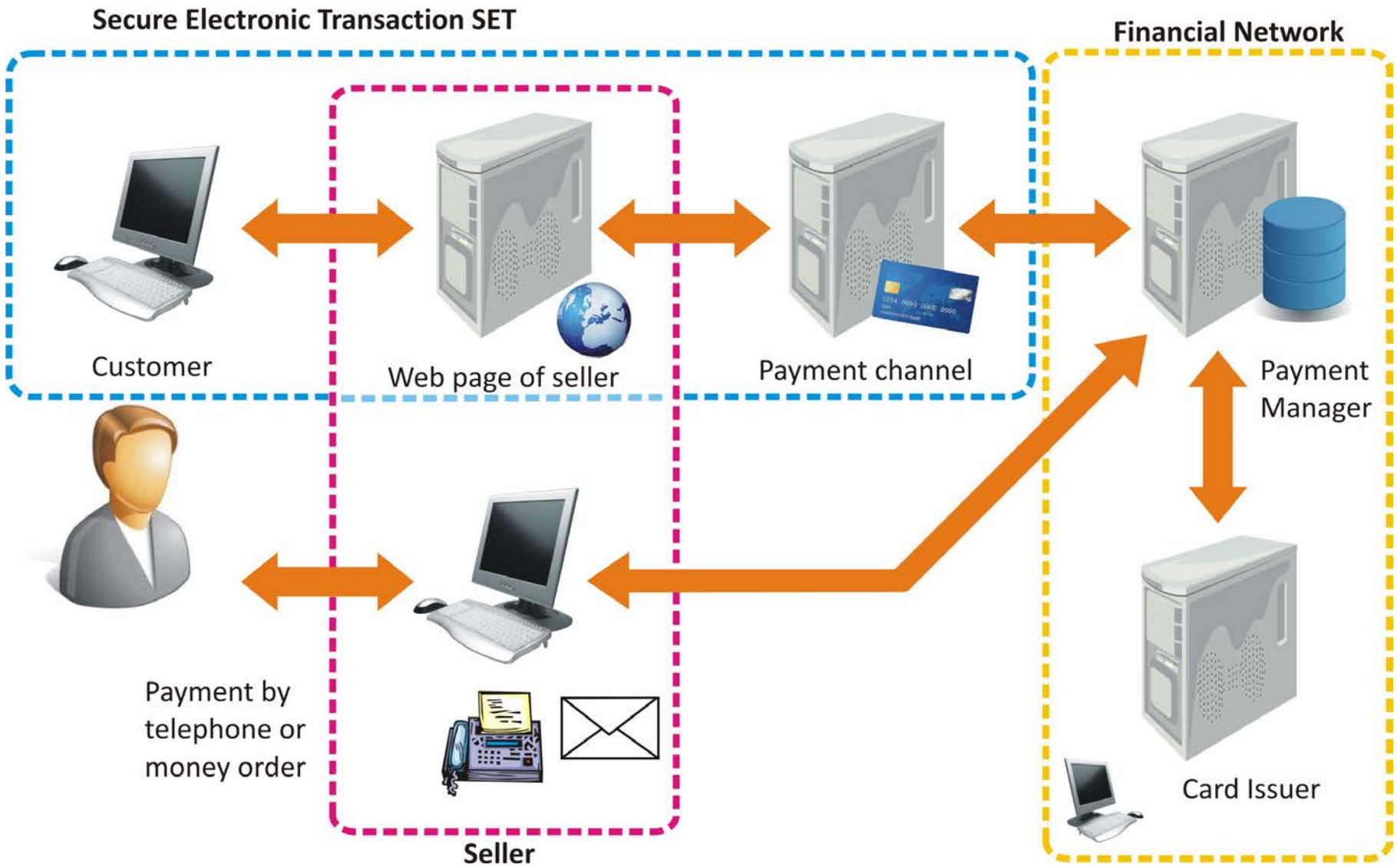
SSL : Secure Sockets Layer
TSL : Transport Layer Security



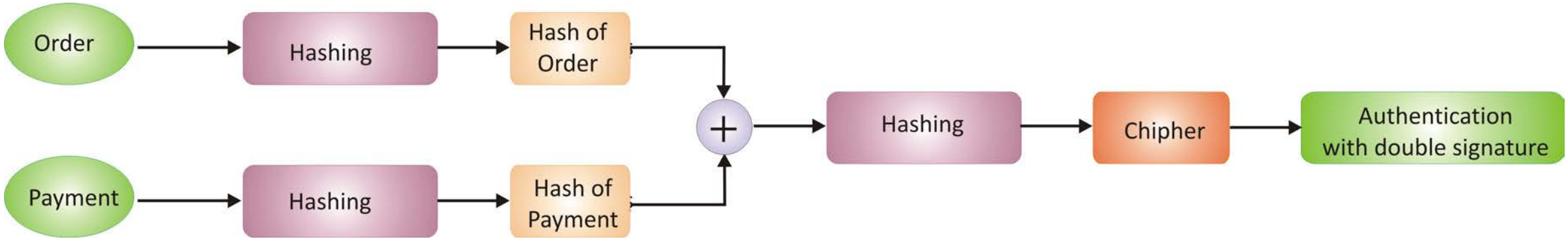
Handshaking in SSL



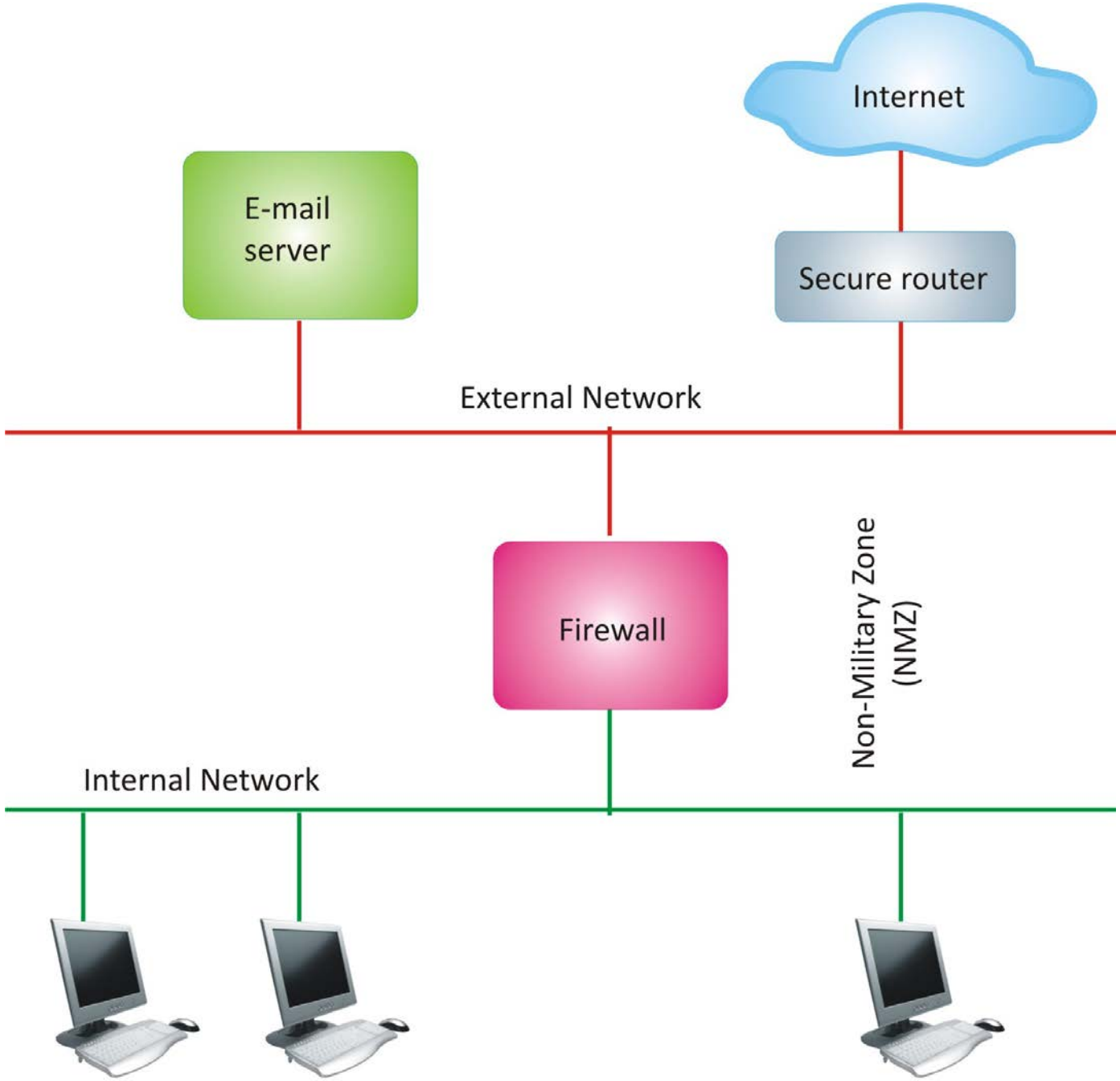
Secure Electronic Transaction (SET)



Order and Payment Process



Firewall


Internet
E-mail server
Secure router
External Network
Firewall
Non-Military Zone (NMZ)
Internal Network