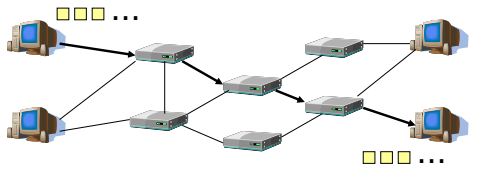
The Internet

BİL 448/548
Internet Security Protocols
Ali Aydın Selçuk

The Internet

A packet-switched network:

- Data to be transmitted is divided into “packets”
- Each packet is forwarded by “routers” towards the destination



TCP/IP Reference Model

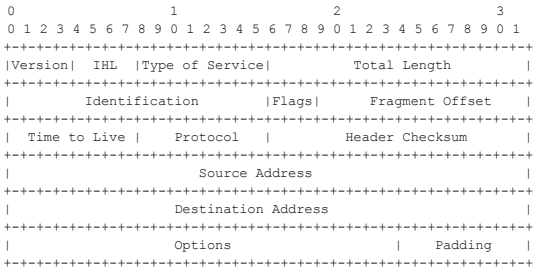
Application Layer (HTTP, FTP, SMTP, etc.)
Transport Layer (TCP, UDP)
Network Layer (IP)
Data Link Layer (PPP, Ethernet, etc.)
Physical Layer

- IP: delivery of packets to the destination
- TCP: reliability of the communication
- UDP: basic transport protocol

Network Layer

- Main protocol: IP
- Like the postal service: Forwards the packet hop by hop towards the destination address, and delivers it to the destination.
- “Best effort delivery”
- Some important fields in the header:
  - source address
  - destination address

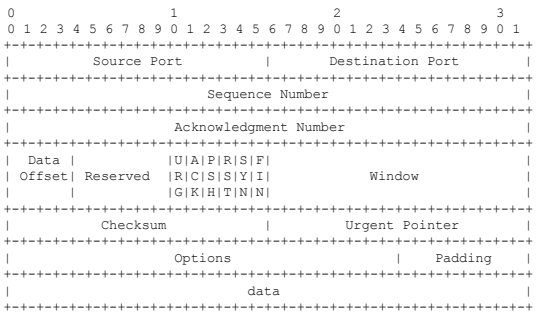
IPv4 Header



Transport Layer

- Main protocol: TCP (also UDP)
- Provides reliability on top of unreliable IP (~ a circuit switched network)
  - ordering of packets
  - detection & retransmission of lost / erroneous packets
  - congestion control
- Some important fields in the header:
  - source port, destination port
  - sequence number
  - checksum

TCP Header

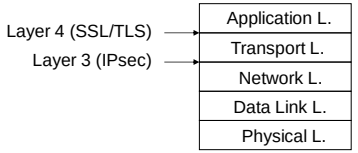


UDP Header

Securing Internet Communication

- Encrypting / authenticating the traffic
  - SSL / TLS
  - IPsec
- Application layer security
  - E-mail (PGP, S/MIME, etc.)
  - SSH
  - …
- Securing the infrastructure
  - DNSSEC
  - Routing security

Securing TCP/IP



Layer 3:
- can secure all IP comm., transparent to applications
- must be built into the OS

Layer 4:
- doesn't require OS modification; deployment easy

Encrypting the Traffic

SSL:
- Runs on top of TCP
- Encrypts traffic of a TCP connection (e.g., a web page)

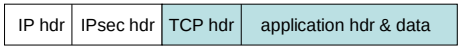
IPsec:
- Runs on top of IP
- Encrypts all the traffic between two IPsec hosts
- In tunnel mode, it encrypts all the traffic between two gateways (i.e., two subnets)

IPsec vs. SSL

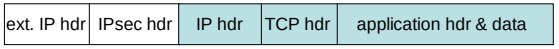
Basic TCP/IP packet:

SSL:

IPsec – transport mode:



IPsec – tunnel mode:



Securing the Internet Infrastructure

- Many critical Internet infrastructure protocols have no security protection.
- Messages are just assumed to be authentic.
- Critical examples:
  - DNS
  - Routing protocols

Domain Name System

- DNS makes it possible to use human-friendly hostnames instead of IP addresses.
- Responsible to translate hostnames to IP addresses (www.example.com → 192.0.43.10) for using it in TCP/IP.
- A critical part of the Internet infrastructure
- DNS responses are assumed to be authentic implicitly by applications and protocols.

Routing Protocols

- Responsible to compute the route between each source and destination on the Internet.
- internal: OSPF
  - Within an administrative domain (AS), every router broadcasts its link information to peers
  - Each router computes the shortest paths within AS
- external: BGP
  - Each AS shares its distance table with its neighbors
  - “Next hop” information is updated accordingly
- Routing updates are assumed authentic implicitly.

Cryptography & Internet

- Not an easy relationship
- The structure is not designed with security in mind; it is hard to add it later.
- The simpler the protocol (even if imperfect), the more deployment chance it has.
  - SSL, IPsec: mostly successful
  - Application layer: simple protocols are used successfully
  - Infrastructure protection: yet to see common deployment