Introduction to Computer Networks
Network Communication

• Communication in modern networks is characterized by the following fundamental principles
  – Packet switching
  – Stack of layers
  – Encapsulation
Packet Switching

• Data split into packets
• Each packet is
  – Transported **independently** through network
  – Handled on a **best efforts** basis by each device
• Packets may
  – Follow different routes between the same endpoints
  – Be dropped by an intermediate device and never delivered
Packet Switching
Packet Switching
Packet Switching
Packet Switching
Stack of Layers

- Network communication models use a **stack of layers**
  - Higher layers use services of lower layers
  - Physical channel at the bottommost layer
- A network device implements several layers
- A communication channel between two devices is established for each layer
  - **Actual** channel at the bottom layer
  - **Virtual** channel at higher layers
Internet Stack (simplified)

Browser
OpenSSL
OS
OS

Server
OpenSSL
OS
OS

Firmware
Firmware
OS
OS

HTTP
TLS
TCP

IP
ARP
IP
ARP
IP
ARP

Application
Security
Reliability
Internet Routing
LAN Routing
Physical

Introduction to Computer Networks
Encapsulation

• A packet typically consists of
  – Control information: header and footer
  – Data: payload

• A protocol P uses the services of another protocol Q through encapsulation
  – A packet p of P is encapsulated into a packet q of Q
  – The payload of q is p
  – The control information of q is derived from that of p
Internet Packet Encapsulation

Application Layer

Transport Layer

Network Layer

Link Layer
Internet Packet Encapsulation

Data link frame
- IP packet
- TCP or UDP packet
- Application packet

Data link header
- IP header
- TCP or UDP header
- Application packet

Data link footer
The OSI Model

• The **OSI** (Open System Interconnect) Reference Model is a network model consisting of seven layers
• Created in 1983, OSI is promoted by the International Standard Organization (ISO)
TCP/IP Model Mapped onto OSI

7. Application
   - Name System
     - DNS
   - Host Config
     - BOOTP
   - Network Mgmt
     - SNMP
   - File Transfer
     - FTP
   - E-Mail & News
     - RFC822 / MIME
     - SMTP
     - POP / IMAP
     - NNTP
   - WWW & Gopher
     - HTTP
     - Gopher
     - "m" Commands
     - IRC

6. File Sharing
   - NFS

5. Interactive
   - Telnet

4. Transport
   - User Datagram Protocol (UDP)
   - Transmission Control Protocol (TCP)

3. Internet
   - Internet Protocol (IP/IPv4, IPv6)
   - IP NAT
   - IPsec
   - Mobile IP
   - Neighbor Discovery (ND)
   - ICMP/ICMPv4, ICMPv6
   - IP Routing Protocols
     - RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP

2. Network Interface
   - Serial Line Interface Protocol (SLIP)
   - Point-to-Point Protocol (PPP)
   - (LAN/WLAN/WAN Hardware Drivers)
Network Attacks

Standard Flow

Block (DoS)

Wiretapping (sniffing)

Wiretapping (passive)

Tampering (active)

Creation (spoofing)
Network Interfaces

• Network interface: device connecting a computer to a network
  – Ethernet card
  – WiFi adapter
• A computer may have multiple network interfaces
• Packets transmitted between network interfaces
• Most local area networks, (including Ethernet and WiFi) broadcast frames
MAC Addresses

• Most network interfaces come with a predefined MAC address

• A MAC address is a 48-bit number usually represented in hex
  – E.g., 00-1A-92-D4-BF-86

• The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  – E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92, 00-0a-95 ??????

• The next three can be assigned by organizations as they please, with uniqueness being the only constraint
Switch

• A **switch** performs routing in a local area network
  – Operates at the link layer
  – Has multiple interfaces, each connected to a computer

• Operation of a switch
  – Learn the MAC address of each computer connected to it
  – Forward frames only to the destination computer
Combining Switches

- Switches can be arranged into a tree
- Each port the MAC addresses of the machines in the segment (subtree) connected to it
- Frames to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored
Internet Protocol Functions

• **Addressing**: In order to deliver data, IP needs to be aware of where to deliver data to, and hence includes addressing systems.

• **Fragmentation and Reassembly**: IP packets are carried across networks which may have different maximum packet length.

• **Data Encapsulation and Packaging** are used to encapsulate TCP or UDP packets into a specific form before transmission over IP.

• **Routing**: IP might be required to communicate across networks, and communicate with networks not directly connected to the current network.
IP Addresses and Packets

• IP addresses
  – IPv4: 32-bit addresses
  – IPv6: 128-bit addresses
• Address subdivided into network, subnet, and host
  – E.g., 128.148.32.110
• Broadcast addresses
  – E.g., 128.148.32.255
• Private networks
  – not routed outside of a LAN
  – 10.0.0.0/8
  – 172.16.0.0/12
  – 192.168.0.0/16

• IP header includes
  – Source address
  – Destination address
  – Packet length (up to 64KB)
  – Time to live (up to 255)
  – IP protocol version
  – Fragmentation information
  – Transport layer protocol information (e.g., TCP)
IP Routing

- A router bridges two or more networks
  - Operates at the network layer
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address

- Routing table
  - Maps ranges of addresses to LANs or other gateway routers
Routing Examples

LAN A

client

gateway

server A

router

router

router

router

router

server B

LAN B

router

gateway
Internet Routes

• Internet Control Message Protocol (ICMP)
  – Used for network testing and debugging
  – Simple messages encapsulated in single IP packets
  – Considered a network layer protocol

• Tools based on ICMP
  – **Ping**: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  – **Traceroute**: sends series ICMP packets with increasing TTL value to discover routes
Traceroute

echo request, TTL = 1

time exceeded

echo request, TTL = 2

time exceeded

echo request, TTL = 3

time exceeded

echo request, TTL = 4

echo response
Wireshark

- Packet sniffer and protocol analyzer
- Captures and displays network packets for analysis
- Supports plugins
- Usually requires administrator privileges because of security risks associated with the program
- When run in promiscuous mode, captures traffic across the network
- Freely available on www.wireshark.org