A very easy... network
Two philosophers example

Kenyan philosopher

Indonesian philosopher

Translator

Language

Translator

Engineer

Communication Device

Engineer
Internet Layers

Application
Transport
Network
Link

Application
Transport
Network
Link

Application
Transport
Network
Link

Application
Transport
Network
Link

Physical Layer

Ethernet
Fiber Optics
Wi-Fi
Communication Channel

• Communication models in a network typically use a **stack** of layers
  – Higher layers use the services of lower layers via encapsulation
  – A layer can be implemented in hardware or software
  – The bottommost layer must be in hardware

• A network device may implement several layers

• A communication channel between two nodes is established for each layer
  – **Actual** channel at the bottom layer
  – **Virtual** channel at higher layers
Virtual Circuit vs Packet Switching

• Virtual Circuit
  – Legacy phone network
  – Single route through sequence of hardware devices established when two nodes start communication
  – Data sent along route
  – Route maintained until communication ends

• Packet switching
  – Internet
  – Data split into packets
  – Packets transported independently through network
  – Each packet handled on a best efforts basis
  – Packets may follow different routes
Packet Switching
Packet Switching
Packet Switching
Packet Switching

A
B
C
D
E
F

1 2 3
Encapsulation

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

• A network protocol $N_1$ can use the services of another network protocol $N_2$
  – A packet $p_1$ of $N_1$ is encapsulated into a packet $p_2$ of $N_2$
  – The payload of $p_2$ is $p_1$
  – The control information of $p_2$ is derived from that of $p_1$
Internet Packet Encapsulation

Application Layer
Transport Layer
Network Layer
Link Layer

Frame Header | Frame Data | Frame Footer

IP Header | IP Data

TCP Header | TCP Data

Application Packet

Computer Networks: Intro
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).
Data Transportation across Entities

- The OSI model assumes that not all layers are horizontally connected to the same layer of the other machine.
- Instead data transmission takes place by having data propagate down and use the physical layer to communicate.
- The communication medium then routes the data to the receiving physical entity.
- Data is then propagated up the layers.
- Each layer packages or unpackages the data a little.
- Layers may perform other transformations on the data.
- Thus it is necessary that a layer be able to reverse its own transformation, allowing communication across machines.
TCP/IP Model Mapped onto OSI
Network Attacks

- **Standard Flow**
  - Source → Destination

- **Block (DoS)**
  - Source → Destination

- **Wiretapping (sniffing)**
  - Source → Destination

- **Wiretapping (passive MitM)**
  - Source → Destination

- **Tampering (active MitM)**
  - Source → Destination

- **Creation (spoofing)**
  - Source → Destination
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
- In regular mode, each network interface gets the frames intended for it
- Traffic sniffing can be accomplished by configuring the network interface to read all frames (promiscuous mode)
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
• The next three can be assigned by organizations as they please, with uniqueness being the only constraint
• Organizations can utilize MAC addresses to identify computers on their network
• MAC address can be reconfigured by network interface driver software
Switch

• A switch is a common network device
  – 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 learns 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
MAC Address Filtering

- A switch can be configured to provide service only to machines with specific MAC addresses
- Allowed MAC addresses need to be registered with a network administrator
- A **MAC spoofing attack** impersonates another machine
  - Find out MAC address of target machine
  - Reconfigure MAC address of rogue machine
  - Turn off or unplug target machine
- **Countermeasures**
  - Block port of switch when machine is turned off or unplugged
  - Disable duplicate MAC addresses
Viewing and Changing MAC Addresses

- Viewing the MAC addresses of the interfaces of a machine
  - Linux & OS X: `ifconfig`
  - Windows: `ipconfig /all`

- Changing a MAC address in Linux
  - Stop the networking service: `/etc/init.d/network stop`
  - Change the MAC address: `ifconfig eth0 hw ether <MAC-address>`
  - Start the networking service: `/etc/init.d/network start`

- Changing a MAC address in Windows
  - Open the Network Connections applet
  - Access the properties for the network interface
  - Click “Configure …”
  - In the advanced tab, change the network address to the desired value

- Changing a MAC address requires administrator privileges
Internet Protocol

• **Connectionless**
  – Each packet is transported independently from other packets

• **Unreliable**
  – Delivery on a best effort basis
  – No acknowledgments
  – Packets may be lost, reordered, corrupted, or duplicated

• **IP packets**
  – Encapsulate TCP and UDP packets
  – Encapsulated into link-layer frames

![Data link frame diagram](image_url)
IP Functions

• IP is charged with providing 4 primary 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)

<table>
<thead>
<tr>
<th>v</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td>fragmentation info</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>prot.</td>
</tr>
<tr>
<td>source</td>
<td></td>
</tr>
<tr>
<td>destination</td>
<td></td>
</tr>
</tbody>
</table>
IP Vulnerabilities

- Unencrypted transmission
  - Eavesdropping possible at any intermediate host during routing

- No source authentication
  - Sender can spoof source address, making it difficult to trace packet back to attacker

- No integrity checking
  - Entire packet, header and payload, can be modified while en route to destination, enabling content forgeries, redirections, and man-in-the-middle attacks

- No bandwidth constraints
  - Large number of packets can be injected into network to launch a denial-of-service attack
  - Broadcast addresses provide additional leverage
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
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
- time exceeded
- echo response
Wireshark

- Wireshark is a packet sniffer, protocol analyzer used for network troubleshooting, analysis and protocol development
- Wireshark allows for capturing of raw data from the network and for analysis
- Has a large number of plugins, including ones which allow for viewing certain protected packet content.
- Usually requires that it be run in administrator mode because of security risks associated with the program
- When run in promiscuous mode (requires specific permissions on Linux), captures traffic across the network, not only addressed to its specific MAC address
- Freely available on www.wireshark.org