Introduction to Networking

by Erol Seke

For the course “Computer Networks”

OSMANGAZI UNIVERSITY
Jobs brought in by the clients on punched papers

Operator feeds the punched cards into the computer

Output is received in paper form
Why do we use computer networks?

1. Communication
2. Resource sharing
3. Replication
4. Cost reduction

Major classification of computer networks

1. Multiple computers sharing data as wished (this is what we are interested in in this course)
2. Single computer with multiple processors (multiprocessor systems)
3. Multiple computers sharing everything and acting like a single computer (distributed system)

We analyse the computer networks using three criteria

1. Performance
2. Reliability
3. Security
**Performance**: amount of data transferred per unit time or conversely; time required to transfer the unit data

Depend on the
1. Number of users
2. Equipment
3. Protocols / Software
4. Type of medium

**Reliability**: Frequency of failure

3 important measurements are
1. Frequency of failure
2. The time it takes for recovery from failure
3. Robustness in catastrophe

**Security hazards**: 1. Data can be stolen
2. Data can be rendered useless (by viruses for example)
<table>
<thead>
<tr>
<th>Interprocessor distance</th>
<th>Processors in the same</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 m</td>
<td>system</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>10 m</td>
<td>room</td>
<td></td>
</tr>
<tr>
<td>100 m</td>
<td>building</td>
<td></td>
</tr>
<tr>
<td>1 km</td>
<td>campus</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>10 km</td>
<td>city</td>
<td></td>
</tr>
<tr>
<td>100 km</td>
<td>country</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>1000 km</td>
<td>continent</td>
<td></td>
</tr>
<tr>
<td>10000 km</td>
<td>planet</td>
<td>Internet</td>
</tr>
</tbody>
</table>
Line Configuration

- **Point-to-Point**: Host 1 to Host 2 via a dedicated link.
- **Multipoint**: Host 1, Host 2, and Host 3 share a common medium.

Diagram:

1. **Point-to-Point** connection between Host 1 and Host 2.
2. **Multipoint** connection involving Host 1, Host 2, and Host 3.
Transmission Modes

**Simplex**: One way transmission. One device can only transmit, the other one can only receive.

**Half-Duplex**: Each device can both transmit and receive but not at the same time.

**Full-Duplex**: Both devices can transmit and receive simultaneously.
Network Topologies

Fully connected networks (mesh)

Advantages:
• Performance is not shared (no traffic problem)
• It is robust. If one line fails it does not affect the rest.
• Privacy and security
• Fault identification is easier.

Disadvantages:
• High number of physical ports required.
• High amount of cabling.

Number of physical channels = \( \frac{n(n-1)}{2} \) where \( n = \# \) devices
Network Topologies

Star

Advantages:
• Cheaper, because …
• Devices need only one physical port
• Less cabling
• Robust. Failed cable affects only the connected host

Disadvantages:
• More cabling than bus topology
Network Topologies

Bus

Advantages:
- Minimal cabling
- Simplicity

Disadvantages:
- Fault isolation is difficult
- A fault downs the entire network
- Limited number of host on the network
Network Topologies

Ring

Advantages:
• Less cabling than star
• Collision-free
• ?

Disadvantages:
• Difficult management
• One fault downs the network
Network Topologies

Tree is a combination of multiple stars

Advantages:
1. Advantages of a star
2. Additional distance that can be covered by the network.
3. Each small star can be isolated from others.
Network Topologies

Hybrid means no particular topology but a mixture of others

The example illustrated has no alternative routes
Internet consists of virtually unlimited number of networks with unknown internal topologies and protocols
## Transmission Media Performance

<table>
<thead>
<tr>
<th>Media</th>
<th>Cost</th>
<th>Speed</th>
<th>Attenuation</th>
<th>EMI</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTP</td>
<td>Low</td>
<td>1 - 100 M</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>STP</td>
<td>Moderate</td>
<td>1 – 150</td>
<td>High</td>
<td>Mod</td>
<td>Low</td>
</tr>
<tr>
<td>Coax</td>
<td>Moderate</td>
<td>1M - 1 G</td>
<td>Mod</td>
<td>Mod</td>
<td>Low</td>
</tr>
<tr>
<td>Fiber</td>
<td>High</td>
<td>10 M - 2 G</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Radio</td>
<td>Moderate</td>
<td>1 – 10 M</td>
<td>Low- High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Microwave</td>
<td>High</td>
<td>1 – 10 G</td>
<td>Variable</td>
<td>High</td>
<td>Mod</td>
</tr>
<tr>
<td>Satellite</td>
<td>High</td>
<td>1 M – 10 G</td>
<td>Variable</td>
<td>High</td>
<td>Mod</td>
</tr>
<tr>
<td>Cellular</td>
<td>High</td>
<td>9.6 – 19.2 K</td>
<td>Low</td>
<td>Mod</td>
<td>Low</td>
</tr>
</tbody>
</table>
The model consists of seven layers, some in software form, some in hardware form.

OSI : Open Systems Interface
What do Individual Layers Do

**Application Layer:** is a user interface.
- 1. Virtual terminal
- 2. File management (access, transfer)
- 3. Mail services
- 4. Directory services

**Session Layer:** Does;
- 1. Dialog control
- 2. Session management

**Presentation Layer:** Does;
- 1. Format translation
- 2. Encryption & compression
- 3. Password validation

**Transport Layer:** Responsible for delivery of the entire messages. While transmitting it forms several packets from the messages and hands them to the network layer. When it receives a packet from N.L. it tries to build a complete package. Packets may arrive out of order.
- 1. Segmentation & reassembly for end to end message delivery.
- 2. Service-point addressing (different number for each program)

**Network Layer:** Responsible for the source-to-destination delivery of the packets. This also means the layer handles the logical addressing of host residing in different networks. That is N.L. does;
- 1. Switching
- 2. Routing (deciding which route to follow when transferring the packet)
- 3. Logical → Physical addressing conversion

**Data Link Layer:** Deals with the physical addressing of the devices. Also responsible for error free transmission, access control

**Physical Layer:** Deals with the mechanical and electrical specifications;
- 1. Cables
- 2. Connectors
- 3. Signaling standards (voltages, noise levels, encoding etc.)
### Comparison of OSI vs TCP/IP (of DoD)

<table>
<thead>
<tr>
<th>OSI</th>
<th>TCP/IP</th>
<th>Hybrit Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>Application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>Transport</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Network</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Data Link</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>Host - to Network</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>Physical</td>
</tr>
</tbody>
</table>

TCP/IP is created by a bunch of programmers (mostly graduate students) on the research money granted by DoD.

OSI is designed and standardized first by ISO, then created.
Protocols

Network layers talk to each other using a variety of languages, but corresponding layers must speak the same language.

The set of commands and “what to do next?”s in such a language is called the protocol.

The selection of physical media and corresponding layer (fiber, radio, cellular, ISDN, ATM) usually determines the data link layer protocols which involves framing, flow control, error detection/correction. The physical properties and protocols are dictated by the international standards, unless experimental and local.

Since layers depend on the layers below, upper layers’ communication languages (protocols) run on the protocols of the lower layers.

For LANs, the most common physical network standard and protocols running on it are ethernet LAN (defines data link and physical layers) and TCP/IP network layer protocol running on it.
<table>
<thead>
<tr>
<th></th>
<th>Frequency (MHz)</th>
<th>Symbol Encoding</th>
<th>Signal Rate (Mbaud)</th>
<th>Symbol Rate</th>
<th>Data Encoding</th>
<th>Data Bits/Symbol</th>
<th>Pairs/Transmit Channel</th>
<th>Number of Pairs Used</th>
<th>Minimum Cable Category Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>10BaseT</td>
<td>10</td>
<td>Manchester</td>
<td>10</td>
<td>10</td>
<td>None</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>100BaseT4</td>
<td>12.5</td>
<td>Multi-level, 2T/Hz</td>
<td>25</td>
<td>25</td>
<td>8B6T</td>
<td>8/6</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>100BaseTX</td>
<td>31.25</td>
<td>MLT-3</td>
<td>125</td>
<td>125</td>
<td>4B5B</td>
<td>4/5</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>100BaseT2</td>
<td>12.5</td>
<td>PAM5x5 (2D-PAM5)</td>
<td>25</td>
<td>12.5</td>
<td>None</td>
<td>4 (2x2)</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1000BaseT</td>
<td>31.25</td>
<td>4D-PAM5</td>
<td>125</td>
<td>31.25</td>
<td>None</td>
<td>8 (4x2)</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
Some Standards (by IEEE)

- **Upper Layers**
  - Network Layer
  - Data-Link Layer
  - Physical Layer

- **IEEE 802.1**
- **IEEE 802.2**

- **IEEE 802.3 (CSMA/CD)**
  - Broadband (PSK)
  - Baseband (Manchester)
  - 10 Broad 36

- **IEEE 802.4 (Token Bus)**
  - Datarate
  - Cable type/length
  - 10 Base 5
  - 10 Base 2
  - 10 Base T
  - 100 Base T

- **IEEE 802.5 (Token Ring)**
  - Two sublayers
    - Logical Link Control
    - Media Access Control
Hardware Address in an Ethernet

Ethernet is a LAN of computers (and like) connected with an ethernet adapter card.

All network interface devices have an address embedded in the interface device by the manufacturer. These addresses are unique worldwide (i.e. no two ethernet adapters with the same hardware address.)

Hardware addresses are 6 byte numbers usually written in hexadecimal as 00:0B:2B:5C:CA:71
Hardware addresses are 6 byte numbers usually written in hexadecimal as 00:0B:2B:5C:CA:71
UTP and RJ-45

Twisted Pairs

RJ-45 connector pinouts

<table>
<thead>
<tr>
<th>RJ45 Pin #</th>
<th>Wire Color</th>
<th>Wire Diagram</th>
<th>Signal*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>White/Orange</td>
<td></td>
<td>Transmit+</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td></td>
<td>Transmit-</td>
</tr>
<tr>
<td>3</td>
<td>White/Green</td>
<td></td>
<td>Receive+</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td></td>
<td>Unused</td>
</tr>
<tr>
<td>5</td>
<td>White/Blue</td>
<td></td>
<td>Unused</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td></td>
<td>Receive-</td>
</tr>
<tr>
<td>7</td>
<td>White/Brown</td>
<td></td>
<td>Unused</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td></td>
<td>Unused</td>
</tr>
</tbody>
</table>
1. Host-1 puts a packet destined to E2
2. The packet is only received by Host-2 since only it has E2 as hardware address
3. It acknowledges the reception by sending back an ACK packed, if necessary.

Questions:
1. How do hosts know each others hardware address, E1 and E2?
2. What do other hosts do while Host-1 and Host-2 are talking?
3. How do hosts know when to start sending data and occupy the network
Ethernet Frame (IEEE 802.3)

- Preamble: Alternating 1s and 0s
- Destination Address
- Source Address
- Type
- Data
- Padding
- Checksum
- CRC

Type ≤ 1500: Protocol
Type > 1500: Length of data

Higher order packet(s)

Just to satisfy the minimum length requirement

00:2B:C3:50:47:B3
(Addresses are examples only)

00:0B:2B:5C:CA:71
Reasoning for the Minimum Frame Length

The minimum length of an ethernet frame must be 64 bytes

Number of bits in a smallest frame

\[ 4 \times 2500 \approx \frac{64 \times 8}{10 \times 10^6} \times \frac{\frac{2}{3}}{3} \times 10^8 \]

bits/sec speed of electromagnetic wave in copper in m/sec

This minimum length is selected to make sure that the sending node is warned about the collision if it happens before the end of the frame is transmitted.
Encoding

**Unipolar**: techniques which use only one level of value.

**Bipolar**: techniques which use two levels of value.

Unipolar example

- Binary stream: 0 1 0 1 0 0 1 1
- Amplitude graph showing the voltage levels over time.
**NRZ** : Line is always positive or negative  
0 = Idle = No transmission

**NRZ-L** : (Non Return Zero - Level)  
Positive Voltage = 1  
Negative Voltage = 0

**NRZ-I** : (Inversion)  
Transition at the beginning means 1  
No transition at the beginning means 0

**RZ** : Return to zero between bits

![Waveform](image)

**Bipolar Alternate Mark Inversion (AMI)** :  
Level 0 = 0  
Alternating between + and - = 1

**Biphase** : Change in the middle of interval

**Manchester** :  
Inversion at the middle of the interval from + to - means 1  
Inversion at the middle of the interval from - to + means 0  
*(some books say the opposite)*

**Differential Manchester** :  
Inversion at the middle of each interval.  
Transition (inversion) at the beginning means 0  
No transition at the beginning means 1
<table>
<thead>
<tr>
<th>SIGNAL</th>
<th>PCM WAVEFORM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA VALUE</td>
<td>1 0 1 1 0 0 0 1 1 0 1 0</td>
<td><strong>DATA VALUES</strong> &lt;br&gt;For clarity, the data values at left are referred to below as 'One' and 'Zero' to distinguish them from the logic 1 and logic 0 states of the various PCM codes.</td>
</tr>
<tr>
<td>BIT RATE CLOCK</td>
<td></td>
<td><strong>CLOCK SIGNAL PHASE</strong> &lt;br&gt;The clock signal shown at left is at 0° phase angle. An inverted clock signal would be at 180° phase angle.</td>
</tr>
<tr>
<td>NRZ-L</td>
<td></td>
<td><strong>NON-RETURN TO ZERO — LEVEL</strong> &lt;br&gt;'One' is represented by logic 1 level. 'Zero' is represented by logic 0 level.</td>
</tr>
<tr>
<td>NRZ-M</td>
<td></td>
<td><strong>NON-RETURN TO ZERO — MARK</strong> &lt;br&gt;'One' is represented by a change in level at start of clock. 'Zero' is represented by no change in level at start of clock.</td>
</tr>
<tr>
<td>NRZ-S</td>
<td></td>
<td><strong>NON-RETURN TO ZERO — SPACE</strong> &lt;br&gt;'One' is represented by no change in level at start of clock. 'Zero' is represented by a change in level at start of clock.</td>
</tr>
<tr>
<td>BI9-L</td>
<td></td>
<td><strong>BI-PHASE — LEVEL (SPLIT PHASE)</strong> &lt;br&gt;A level change occurs at middle of every bit clock period. 'One' is represented by a 1-to-0 change at midclock. 'Zero' is represented by a 0-to-1 change at midclock.</td>
</tr>
<tr>
<td>BI9-M</td>
<td></td>
<td><strong>BI-PHASE — MARK</strong> &lt;br&gt;A level change occurs at beginning of every bit clock period. 'One' is represented by a change at midclock. 'Zero' is represented by no change at midclock.</td>
</tr>
<tr>
<td>BI9-S</td>
<td></td>
<td><strong>BI-PHASE — SPACE</strong> &lt;br&gt;A level change occurs at beginning of every bit clock period. 'One' is represented by no change at midclock. 'Zero' is represented by a change at midclock.</td>
</tr>
<tr>
<td>DBI9-M</td>
<td></td>
<td><strong>DIFFERENTIAL BI-PHASE — MARK</strong> &lt;br&gt;A level change occurs at middle of every bit clock period. 'One' is represented by no change at start of clock. 'Zero' is represented by a change at start of clock.</td>
</tr>
<tr>
<td>DBI9-S</td>
<td></td>
<td><strong>DIFFERENTIAL BI-PHASE — SPACE</strong> &lt;br&gt;A level change occurs at middle of every bit clock period. 'One' is represented by a change at start of clock. 'Zero' is represented by no change at start of clock.</td>
</tr>
<tr>
<td>DM-M</td>
<td></td>
<td><strong>DELAY MODULATION — MARK (MILLER CODE)</strong> &lt;br&gt;'One' is represented by a change in level at midclock. A 'Zero' after a 'One' causes no change in level. A 'Zero' after a 'Zero' makes level change at start of clock.</td>
</tr>
<tr>
<td>DM-S</td>
<td></td>
<td><strong>DELAY MODULATION — SPACE</strong> &lt;br&gt;'Zero' is represented by a change in level at midclock. 'One' after a 'Zero' causes no change in level. 'One' after a 'One' makes level change at start of clock.</td>
</tr>
</tbody>
</table>
Example

Draw waveforms for the NRZ-I, RZ, AMI, Manchester and Differential Manchester encodings
Example
IP Address

Since hosts can not know each others hardware address initially, we have software addresses assigned to hosts.

**IP (Internet Protocol) Address**: 4 byte number usually written as decimal quads as aaa.bbb.ccc.ddd

*example*: 193.140.12.97

Every computer on the Internet has an IP number.

IP addresses are assigned *uniquely* in a LAN.

(because of the reasons which will become clear later, they do not have to be worldwide unique *for some cases*)

IP address of the destination host must be known by the source host before the transmission of data.

---

Some info/reminder on CSMA/CD, TCP, IP protocols

IP is a network layer protocol working with IP numbers,
TCP is a transport layer protocol working with ports (special numbers indicating the type of the interaction)

CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection and defines the protocols used partly in data link and physical layers.

---

In an ethernet LAN running TCP/IP, TCP runs on IP which runs on CSMA/CD
**IP Protocol Datagram**

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>Type of Service</th>
<th>Total Packet Length (in bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet Number / Identification</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total Packet Length (in bytes)</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time to Live</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Options of 8 bits and/or padding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

IHL : Header length in 32 bit words. Between 5 and 15.
Total Packet Length : maximum is 65535 bytes including everything
Packet Number / Identification : All fragments of a datagram carry the same number.
DF : Don’t Fragment MF : More Fragments coming
Fragment Offset : position of the fragment in the datagram (in 8 bytes)
Typical TCP/IP on Ethernet Setup

All computers connected to an Ethernet LAN via an ethernet adapter card must have
1. An IP address unique within the network in order to be identified uniquely.
2. A gateway address if access to other networks is permitted and required
3. ?
How does it work?

Host-1 (source) checks to see if Host-2 (destination) is in the same network.

How?

N

Y

How?

Find out the Ethernet address E2 of the destination host

Prepare an ethernet frame with Source addresses : E1, IP1, Port1 Dest. Addresses : E2, IP2, Port2

How?

Wait for the line to clear and put the frame on the line

How?

Find out the Ethernet address Eg of the gateway (if IPg exists)

Prepare an ethernet frame with Source addresses : E1, IP1, Port1 Dest. Addresses : Eg, IP2, Port2
How to obtain Hardware address from IP address

1. Host-1 prepares a question broadcast frame, basically asking “Who has IP2?”
2. Host-1 releases the frame on the line
3. All hosts hearing this query must pay attention, but only Host-2 should reply.
4. From the answer Host-1 learns the hardware address of the Host-2 since the reply frame has it.
5. From now on Host-1 and Host-2 may use E2 and E1 while sending data to each other. (Question: for how long?)

The above procedure is called ARP: Address Resolution Protocol

Broadcast frames has all 1s in their destination address fields: FF:FF:FF:FF:FF:FF
How does Host-1 know that Host-2 is in the same network?

IP addresses are separated into two parts:
- Network address
- Host part

All hosts in a network use the same network address but unique host address.

In order to separate network address part from the IP address, we define another IP like number called:
- The Network Mask or Netmask

A typical netmask: 255.255.255.0 - a 4 byte number with all network bits are 1 and host bits are 0.

The network layer finds the network address by logically AND'ing the IP-address and netmask. If the destinations network address is the same as its own network address then it must be in the same network.

Example:
- IP address = 193.140.81.65
  - Netmask = 255.255.255.0
  - Gateway = 193.140.81.1
- Network address = 193.140.81.0

Gateway IP address must also be in the same network range.
IP classes

32 bit IP address range is separated into several subsections, called classes, as a standard.

Depending on the most significant 4 bits

- **Class A**: 0xxx : 1 - 126
- **Class B**: 10xx : 128 - 191
- **Class C**: 110x : 192 - 223
- **Class D**: 1110 : 224 - 239
- **Class E**: 1111 : 239 - 254

The class of the IP address also determines the network and host parts of the address

- **Class A**: nnn.nnn.nnn.nnn
- **Class B**: nnn.nnn.nnn.nnn
- **Class C**: nnn.nnn.nnn.nnn

Example: **193.140.128.167**

Some IP ranges are reserved for private use and are not routed to other networks. This means that these IPs can be used repeatedly (non-unique).

- A: 10.0.0.0 / 255.0.0.0
- B: 72.16.0.0 / 255.240.0.0
- C: 192.168.0.0 / 255.255.0.0
Name Resolving

We can not remember IP numbers. Certainly we can not keep several IP numbers in our memory. But we can remember names like [www.ogu.edu.tr](http://www.ogu.edu.tr). However machines work with numbers.

So a mechanism for converting such names to real IP addresses is invented: Name Service

The software and sometimes the computer which runs this software is called: Name Server

The IP address of the name server must also be known by the host so that it can ask the IP numbers. Name Servers are connected to each other with a hierarchy and query each other to perform a conversion.

---

Summary for IP setup

We must know and setup these numbers when setting up our computer for networking. These numbers are obtained from the network administrator or automatically from the ISP.

1. An IP address per network interface
2. A netmask per IP address
3. At least one gateway IP address if connecting to other networks (internet) is intended
4. At least one nameserver address if names are to be used.
Example Network:

Host-1: 220.165.18.5
Host-2: 220.165.18.11
Host-3: 220.165.18.104
Gateway: 220.165.18.1

Netmask = 255.255.255.0

The first and the last IP addresses in a network are not used because:
The first one (all 0s in host bits) is the network address
The last one (all 1s in host bits) is the broadcast IP address.

Gateway address is usually selected as the first valid address from
the range just to make it easy to remember.
Network Settings in MS-Windows

From the control panel

Other protocols, services and devices

Allows us to setup for more than one interface
We have only one interface and one gateway

Can have multiple Domain Name Server
IP Routing

Router between these two nets must pass the IP-packets to the appropriate networks

For this, a router must know which IP number is in which network. Such information are kept in tables in the memory of the router

Instead of filling the routing tables with all IP numbers which have the possibility to be used as destination IP address in an IP packet, it is better to assign all IP numbers in a network having the same network address and put network IP addresses in the routing tables.

Giving IP number and netmask pair to a router interface, router knows the location of a host having a particular IP number.

\[ I_A = 193.140.128.1/255.255.255.0 \text{ or } 193.140.128.1 / 24 \]

\[ I_B = 220.14.151.62/255.255.255.0 \text{ or } 220.14.151.62 / 24 \]

When router receives the packet and determine where to send it, it uses ethernet frames to deliver the data.
A packet sourced from a host in Net-1 and destined to another host in Net-3 must be received by Router-1 and sent to Router 2. This requires that an entry in the routing table of Router 1 about the road to Net-3. Router 1 shall deliver the data to $I_C$, and Router 2 will handle the rest of the job.

The required entry in the routing table of Router 1 shall be something like

\[
\text{Deliver packets destined to Net-3 to } I_C
\]

From now on, let us use the following notation to indicate a record in the routing table of the router

Destinations IP number or network IP address \quad \rightarrow \quad IP number of the next hop

For example

\[
193.140.141.0 / 24 \quad \rightarrow \quad 210.15.133.4
\]

this means “via”
The router is just another computer

The router is just another computer in the network, working as a gateway to outside world. It necessarily has interfaces to multiple networks.

Interface IP numbers of the routers must be selected from the same network just like any other host in the network.

As indicated in the picture router interface IPs belong to the connected network.

Router IP numbers are used as Gateway addresses when setting up network for a host (seen previously).
An example network

Let us assume that

- **A**: 193.140.128.0 / 24
- **B**: 193.140.141.0 / 24
- **C**: 193.140.140.0 / 24
- **D**: 220.15.53.0 / 24
- **E**: 220.15.54.0 / 24

**Additional routing table entries in R1**

- 220.15.53.0 / 24 → 193.140.141.2
- 220.15.54.0 / 24 → 193.140.141.2

**Additional routing table entries in R2**

- 193.140.128.0 / 24 → 193.140.141.1
- 193.140.140.0 / 24 → 193.140.141.1

Usually the first IPs are assigned to gateways.
The Default Route

Routing tables may have an entry to point the default route for the destinations for which no entry is found in the table.

If no route found for a destination IP address then the router will use the default route.

A neighbour network (connected to Internet?)

Routing table entries in R1

- B → I_{BE}
- E → I_{BE}
- Default → I_{default}

(Of course, the routers have entries for its interfaces but they are not shown here)
An example with default routes

Another network closer to Internet

Networks with only two hosts
**Repeater:** is an electronic device that operates on only the physical layer. It is just a regenerator that amplifies the bitstream before it gets too weak.
**Bridge:** Operating in both physical and datalink layers, these divide networks into smaller segments, therefore reducing the traffic. Just puts the frame on the other side if necessary.

1. **Simple Bridges:** address must be entered manually.
2. **Learning Bridges:** addresses are learned by the bridge over the time.
3. **Multiport Bridges:** if it has more than two segment connectors.
Routers: Living in network, datalink and physical layers, routers relay packets from one network to any number of possible destination networks. Unlike bridges, they hold any address to be used as routing information.

Routers are intelligent, behaving like any host on the network having the sole job of routing (forwarding) the packets to the direction previously learned and/or manually entered.
**Gateways:** Usually set up to operate like a router, gateways potentially do anything that can be done by a packet, since it has all the layers. It can **translate protocols** to support communication between two incompatible networks having incompatible protocols.

For example, a gateway may live in both a TCP/IP network and Apple Talk network and have them communicate. It is actually a router with some additional software.
END