LAU
الجامعة اللبنانية الأميركية
Lebanese American University

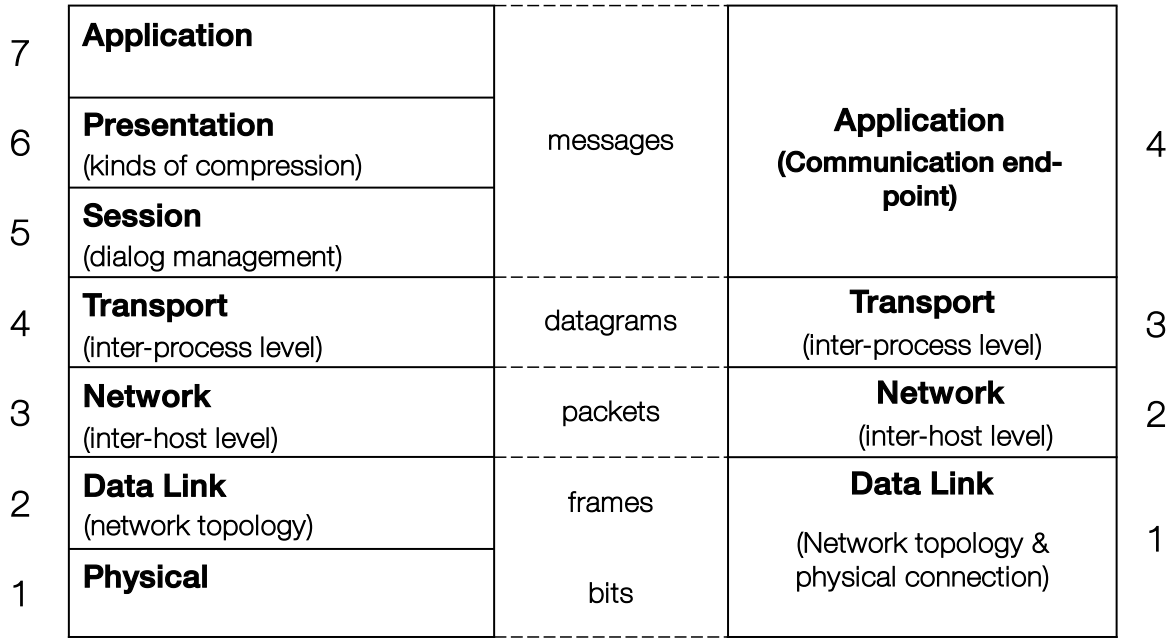
CSC 634: Networks Programming

Lecture 02: Review of Basic Networking Concepts

Instructor: Haidar M. Harmanani

7-Layer OSI Model

7	**Application**	messages
6	**Presentation** (kinds of compression)	messages
5	**Session** (dialog management)	messages
4	**Transport** (inter-process level)	datagrams
3	**Network** (inter-host level)	packets
2	**Data Link** (network topology)	frames
1	**Physical**	bits



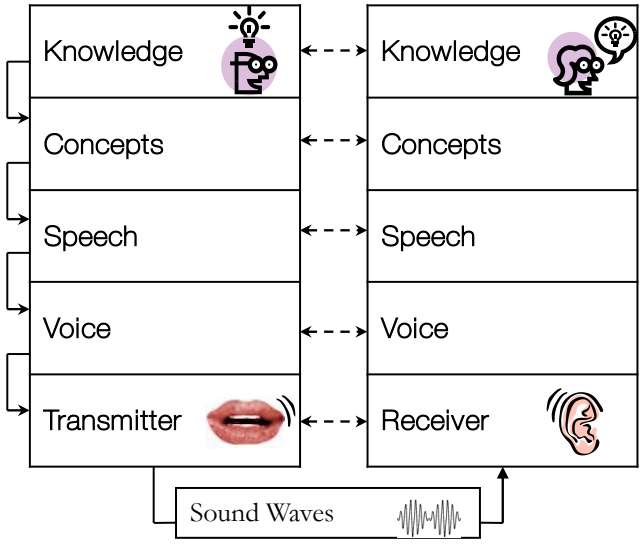
4-Layer Simplified Model of TCP/IP

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

Review of Basic Networking Concepts

Layering and Protocol Family

- Layering is decomposition of task into subsystems (pieces), designed as sequence of horizontal layers.
- As result, each layer:
  - Focuses on providing a particular function
  - is built in terms of one layer below
  - provides means to building various types of upper neighbor
  - layer.
- Protocol Family (Suite) is set of interfaces between layers or inside layer.
- Peer-to-Peer Protocol is the protocol used between two entities of the same layer.



7-Layer OSI Model

7	**Application**	messages
6	**Presentation** (kinds of compression)	messages
5	**Session** (dialog management)	messages
4	**Transport** (inter-process level)	datagrams
3	**Network** (inter-host level)	packets
2	**Data Link** (network topology)	frames
1	**Physical**	bits

OSI Model: Open System Interconnection Model

ISO: International Standard Organization

The 7-Layer OSI Model, developed by ISO (1984), is the guide, providing a detailed standard for describing of a network.

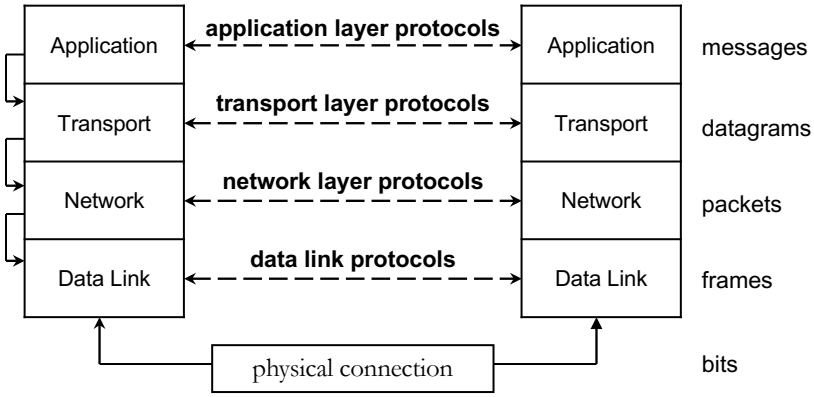
Advantage of layering is to provide well-defined interfaces between the layers, when change in one layer doesn't affect an adjacent layer.

4-Layer Simplified Model of TCP/IP

- TCP/IP Protocol Suite actually was developed (1980-83) before formulation of 7-layer ISO OSI Model (1984).
- It implements 4-layer Simplified Communication Model:

7	**Application**			
6	**Presentation** (kinds of compression)	messages	**Application** (communication end-point)	4
5	**Session** (dialog management)			
4	**Transport** (inter-process level)	datagrams	**Transport** (inter-process level)	3
3	**Network** (inter-host level)	packets	**Network** (inter-host level)	2
2	**Data Link** (network topology)	frames	**Data Link** (network topology & physical connection)	1
1	**Physical**	bits		

Protocol Suite For 4-Layer TCP/IP Model



Protocol Suite for 4-Layer TCP/IP Model contains 4 types of peer-to-peer protocols:

- Application Layer protocols – end-point communication
- Transport Layer protocols – inter-process communication
- Network layer protocols – inter-host communication
- Data Link protocols – topology-specific interface with physical network

TCP/IP Model and Protocol Suite

TFTF: Trivial File Transfer Protocol

UDP: User Datagram Protocol

TCP: Transmission Control Protocol

IP: Internet Protocol

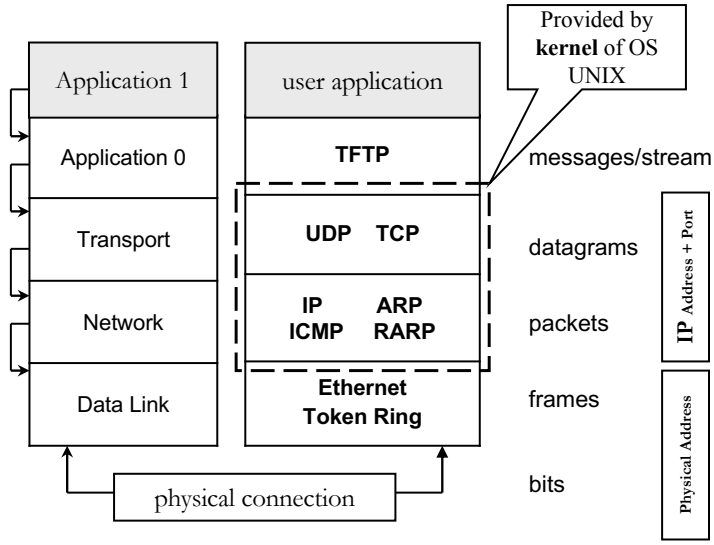
ICMP: Internet Control Message Protocol

ARP: Address Resolution Protocol

RARP: Reverse Address Resolution Protocol

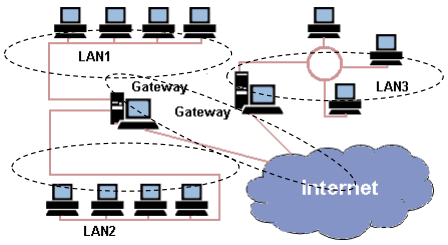
Ethernet: A local area network architecture with broadcast bus topology

Token Ring: A local area network architecture with ring topology and token passing scheme



Network

- LAN: Local Area Network is a computer network comprises a local area, like a home, office, or group of buildings.
- WAN: Wide Area Network is a computer network covering a broad geographical area.
  - Largest and most well-known example of a WAN is the Internet.



Network Type	Technology	Speed
LAN	Coaxial cable, fiber optics, Wi-Fi (wireless technology)	4 Mbit/s – 2 Gbit/s
MAN	Coaxial cable, microwave link	56 Kbit/s – 155 Mbit/s
WAN	Telephone lines, microwave link, satellite channels	9.6 Kbit/s – 45 Mbit/s

Gateway is a system, that interconnects two or more networks

Scientific Justification For Local Area Networks

- The locality principle

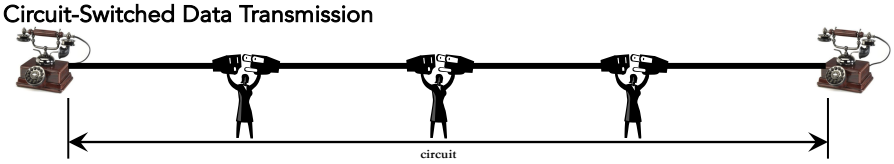
A computer is more likely to communicate with computers that are nearby than with computers that are distant

Communication Activities

- Data Transmission
  - Communication Networks can be divided into two basic types by method of data transmission: circuit-switched and packet-switched.
- Encapsulation
  - Encapsulation is hiding of object data from rest of the world. For protocol suite this means adding of control information to data when going one layer down.
- Multiplexing and Demultiplexing
  - Multiplexing means "to combine many into one". For network this means combining of data accepted from different functionalities of neighbor layer.
  - Demultiplexing is reverse of multiplexing.
- Routing
  - Routing is making decision, what route the packet should take.
  - Static Routing is based on precomputed information.
  - Dynamic Routing is depends on state of network configuration in the specific moment of time.
- Fragmentation and Reassembling
  - Fragmentation (or segmentation) is breaking up of a packet into smaller pieces (MTU – maximal transmission unit)
  - Reassembling is reverse of fragmentation, it is restoring of original packet from smaller pieces used for transmission.

Communication Networks can be divided into two basic types by method of data transmission: circuit-switched and packet-switched.

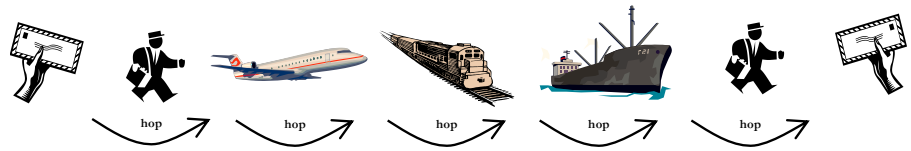
Circuit-Switched Data Transmission



- Non-shared dedicated communication line is established
- Information transmitted without division
- Connection established once, then all data transmitted through this connection.

The TCP/IP Internet uses packet-switched data transmission, provided by IP (Network) layer, responsible for forwarding of IP packets.

Packet-Switched Data Transmission

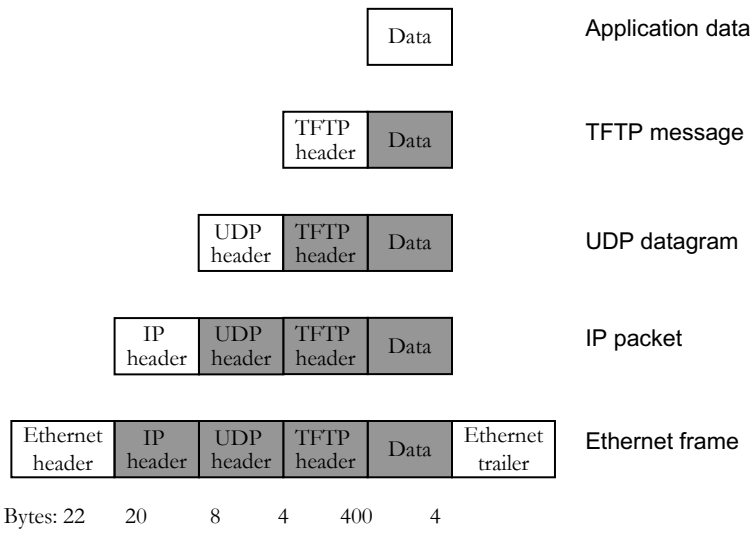


- Shared communication links are used instead of dedicated line
- Information is divided into pieces – packets.
- Each packet contains the address of destination and separately routed over shared data links.

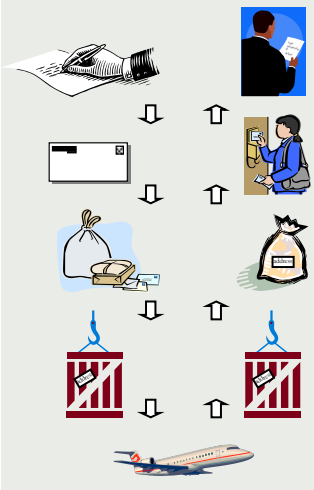
Data Transmission Method

Data Encapsulation in TCP/IP

Encapsulation is hiding of object data from rest of the world.
For protocol suite this means adding of control information to data when going one layer down.



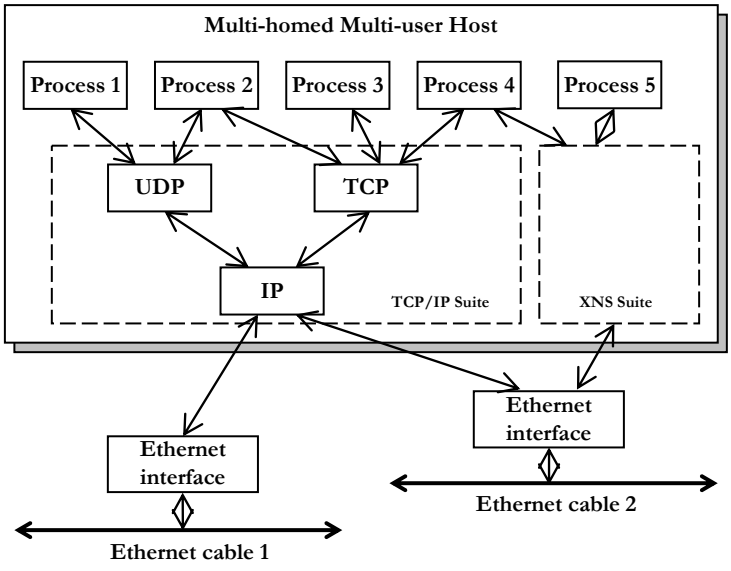
Example. Data encapsulation during mail delivery

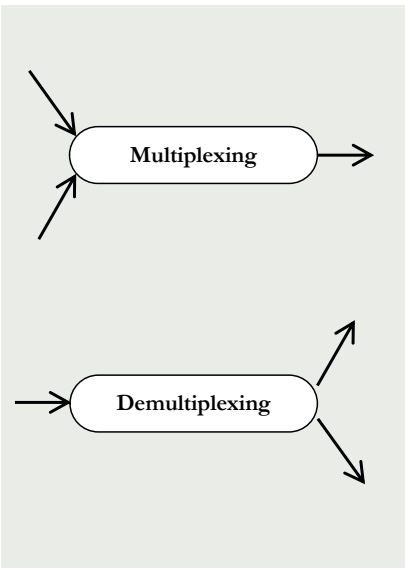


Multiplexing and Demultiplexing in TCP/IP Example.

- Multiplexing means "to combine many into one".
- For network this means combining of data accepted from different functionalities of neighbor layer.
- Demultiplexing is reverse of multiplexing.

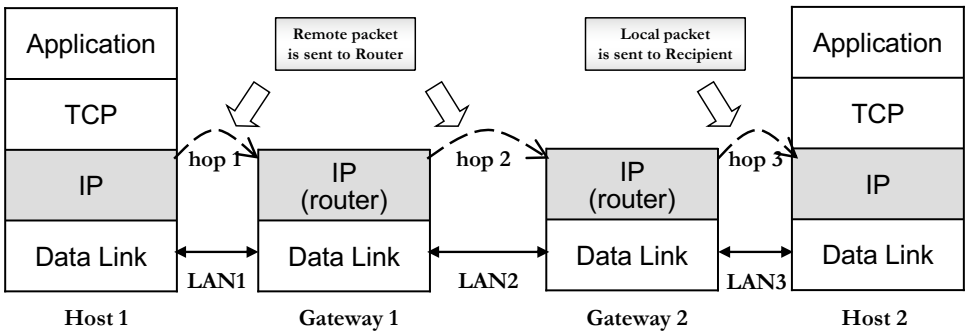
Multiplexing and Demultiplexing in TCP/IP Example.





Routing

Router is "intelligent" gateway, making a decision, what **route** (path) the packet should take.



In TCP/IP routing is made on IP Layer. Each packet could have its own route.

The TCP/IP Internet uses Distributed Dynamic Routing.

Distributed Dynamic Routing

uses a mixture of global and local information to make routing decision.

Fragmentation and Reassembling

Fragmentation

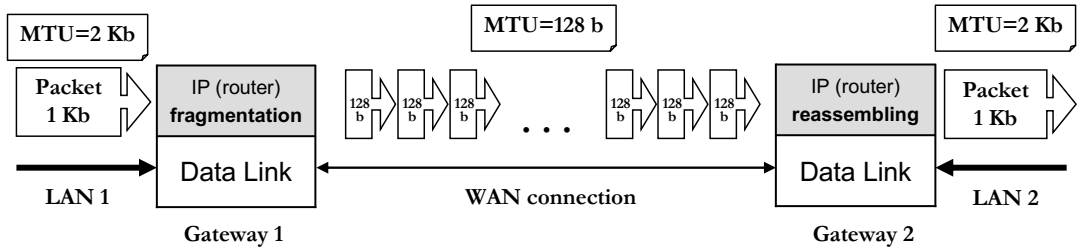
is breaking up of a packet into smaller pieces (transmission units).

Maximal Transmission Unit (MTU)

is maximal packet size held by network layer, depending on Data Link characteristics

Reassembling

is reverse of fragmentation.



In TCP/IP fragmentation and reassembling is done at IP layer.

The IP layer performs these activities depending on requirement of specific Data Link layers,

hiding the technological differences between the networks.

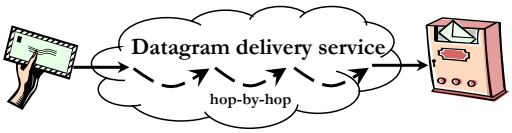
Modes of Communication Service

Communication Service provided between two peer entities at any layer of the OSI Model.

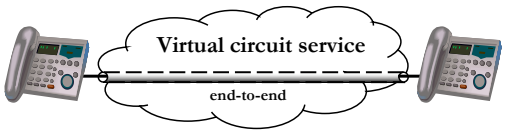
Connection Mode

Connectionless Service

- **Provides *hop-by-hop* transmission of separate messages.**
- **Each message transmitted independently and contains all the information (address) required for delivery.**



Connection-Oriented Service



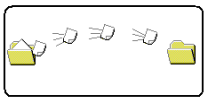
- **Provides establishment of dedicated *end-to-end virtual circuit* for data transmission.**
- **Connection-oriented data exchange involves three following steps:**
  - **Connection establishment (performed once, requires overhead activity)**
  - **Data transfer (can be lengthy)**
  - **Connection termination**

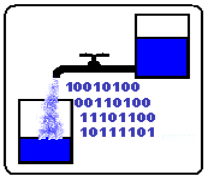
The dedicated circuit is called *virtual,* because it could be provided even on network with packet-switched data transmission.

A connection-oriented service is often used when more than one message is to be exchanged between the two peer entities.

Data Stream Format

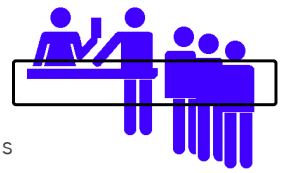
- Message Service
  - Provides record boundaries .
- Byte Stream
  - Does not provide record boundaries.
- Full-duplex - connection allows data to be transferred in both directions in the same time.
- Half-duplex:
  - Connection allows data to be transferred in both direction, but only one side to transfer at a time
- Simplex
  - connection allows data to be transferred only in one direction (one end can only transmit and the other end can only receive.)





Reliability

- Service is Reliable if it provides Sequencing and Error Control.
- Most of reliable services provide also Flow Control.
- Sequencing
  - Data is received by the receiver in the same order as it is transmitted by the sender.
- In a packet-switched network, it is possible for two consecutive packets to take different routes, and thus arrive at their destination in a different order from the order in which they were sent.
- Error Control
  - Guarantees that error-free data is received at the destination.
- There are two conditions that can generate errors:
  - data gets corrupted (modified during transmission),
  - the data gets lost.
- The network implementation has to provide for recovery from both these situations
- Flow control (pacing)
  - Assures that the sender does not send data at a rate faster than the receiver can process the data.
- If Flow Control is not provided, it is possible for the receiver to lose data because of lack of resources.



Summary: Communication Activities and Service Modes

		Communication Activities					Communication Service Modes		
Model Layer	**Protocol**	**Data Transmission**	**Encapsulation**	**Multiplexing/ Demultiplexing**	**Routing**	**Fragmentation/ Reassembling**	**Connection Mode**	**Data Stream Format**	**Reliability**
Application	**application protocols**		**(application-depended)**	**combine/split of data from different Transport (south) protocols**		**(application-depended)**	**(application-depended)**	**(application-depended)**	**(application-depended)**
Transport	**TCP**		**hide Application layer data**	**combine/split of data from different Application (north) processes**		**brake up (/recompose) stream into (from) IP packets**	**connection-oriented**	**full-duplex (bi-directional) byte stream**	**reliable (sequencing, error control, flow control)**
	UDP						**connection-less**	**datagram delivery**	**unreliable**
Network	**IP**	**Packet - switched (hop-by-hop)**	**hide Transport layer data**	**combine/split of data from different Transport (north) and Data Link (south) protocols**	**distributed dynamic routing**	**brake up (/recompose) packet into (/from) transition units**	**connection-less**	**packet delivery**	**unreliable**
Data Link	**Ethernet/ Token Ring**	**frame transmission in LAN**	**hide Network layer data**	**combine/split of data from different Network (north) protocols**					

Communication Services Provided by TCP/IP Protocol Suite

- Network Layer
- IP – Internet Protocol
  - Provides unreliable connectionless packet delivery service, containing:
    - Routing,
    - Fragmentation / Reassembling,
    - Multiplexing / Demultiplexing.
  - Works with different Data Link protocols and topologies, hiding the technological differences between the networks.

Communication Services Provided by TCP/IP Protocol Suite

- Transport Layer
  - UDP – User Datagram Protocol
    - Provides unreliable connectionless datagram delivery service.
  - TCP – Transmission Control Protocol
    - Provides reliable connection-oriented full-duplex byte stream service
    - over unreliable connectionless packet-switched IP Network.

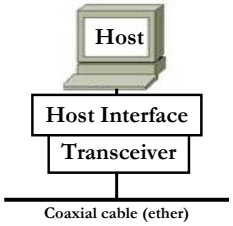
Topology

- Mathematical term
- Roughly interpreted as "geometry for curved surfaces"

Data Link Connection and Topology

- Specifies general "shape" of a network
- Handful of broad categories
- Often applied to LAN
- Primarily refers to interconnections
- Hides details of actual devices

Data Link Connection and Topology



Transceiver

This is communication device capable of transmitting and receiving of signals.

Performs analog - digital - analog translation.

Host Interface

It provides physical address associated with interface hardware and filters incoming packets

Bus Topology

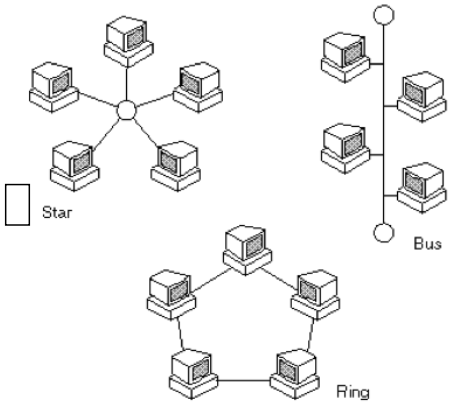
The main characteristic of this topology is that it is a passive structure :when a node is down, the network is not affected .

Ring Topology

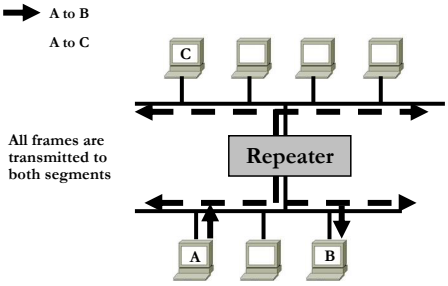
This kind of topology is less efficient and reliable but it is quite cheap .As soon as two lines are cut the network no longer works.

Star Topology

This topology is quite efficient and cheap .Most small local networks is built on this model by using a central *Hub* that connects computers together. A hub can imitate different network topology configurations.



Data Link Equipment



Repeater is a hardware component that transmits frames from one wire and places them on another.

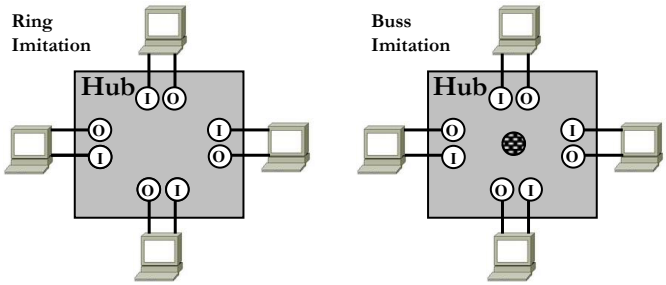
Repeaters are a simple way to extend a LAN segment.

Bridge is a hardware component that filters frames according to destination address.

Bridges are used to connect multiple segments.

Hub is a common connection point for devices in a network.

Hub can imitate a bus or a ring or could be more sophisticated. In this case it called Switch.



Data Link Protocols: Ethernet

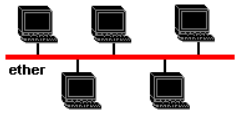
Ethernet is broadcast bus technology with best effort delivery.

Was developed in the beginning of 70-s by Xerox corporation. Following development and standardizing was performed by DIX (Digital, Intel, Xerox) in 1979-1980. In 1983 it was approved as standard by IEEE .

Currently Fast Ethernet is one of most popular LAN technologies.

IEEE (Institute of Electrical and Electronics Engineers) - professional world-wide society for electronics and electrical engineers)

Technology description:
- Each host interface has preset unique 48 bit physical address.
- Transceiver senses when ether is in use and detects collisions.
- When data is transmitted, all hosts connected to the bus can hear the transmission.
- In case of collision both hosts wait for a random amount of time, before sending the information again.



Collision
occurs when two devices on a network try to transmit information at the same time

Ethernet Frame

P	DA	SA	L/T	Data	CRC
Bytes: 8	**6**	**6**	**2**	**46-1500**	**4**

P: Preamble for synchronizing. The last byte is SFD, start of Frame Delimiter

DA: Destination Address

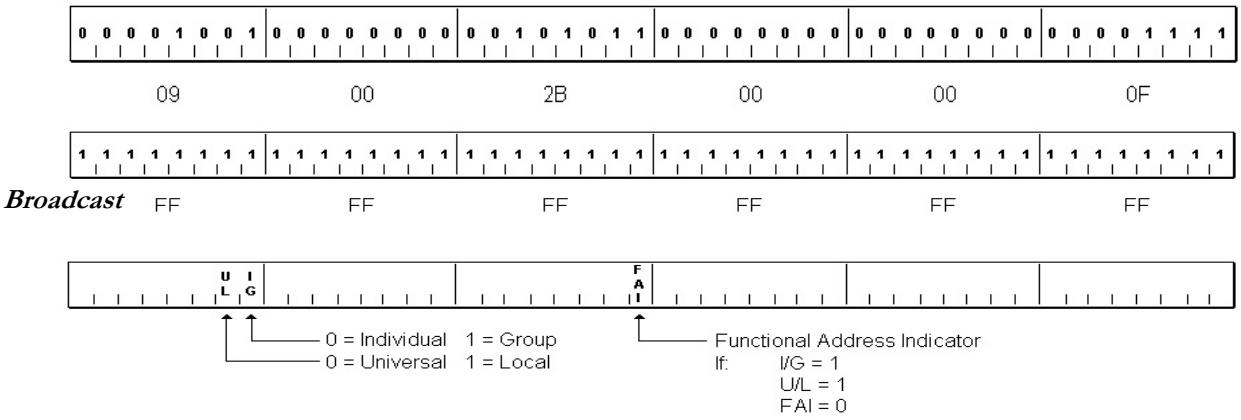
SA: Source Address

L/T: (Length/Type) Length of Data and optional ID of upper level protocol

CRC: Cyclic Redundancy Check sum

Ethernet Addressing

- Each station assigned by unique 48-bit address
- Address assigned when network interface card (NIC) manufactured



Quick Note: Promiscuous Mode

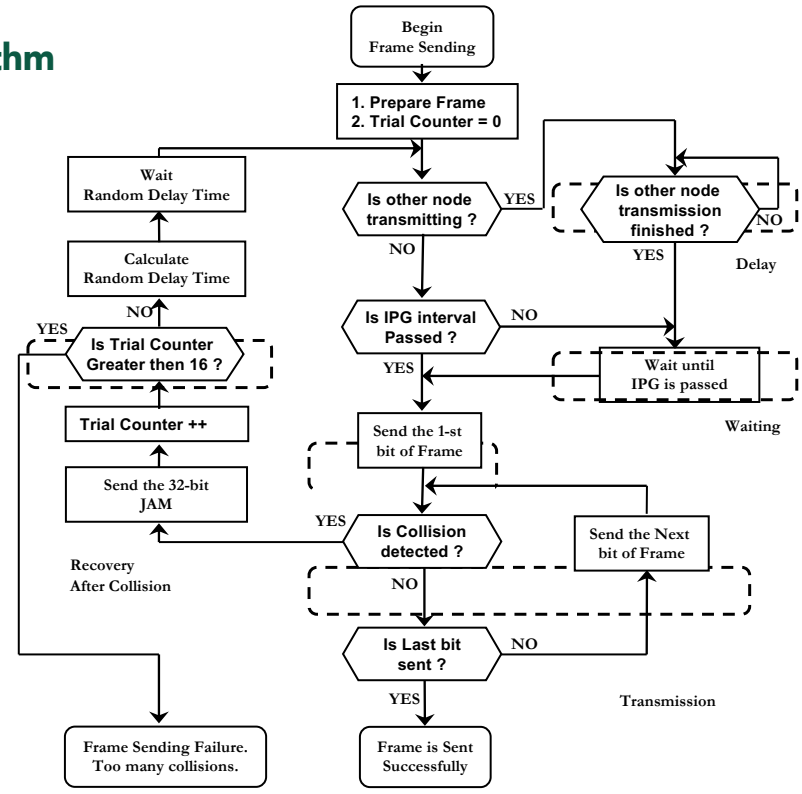
- Designed for testing / debugging
- Allows interface to accept all packets
- Available on most interface hardware
- Network Analyzer
  - Device used for testing and maintenance
  - Listens in promiscuous mode
  - Produces
    - Summaries (e.g., % of broadcast frames)
    - Specific items (e.g., frames from a given address)

Ethernet CSMA/CD algorithm

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

IPG: Inter-Packet Gap

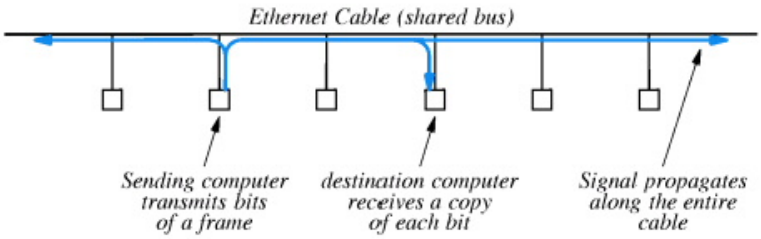
JAM: 32 bit frame for collision signaling



Ethernet CSMA/CD algorithm

- (1) Adapter obtains a network layer packet and prepares an Ethernet frame
- (2) If the adapter senses the channel
  - If idle, then start to transmit
  - If busy, wait until it senses no energy (plus 96 bit times) and then transmit.
- While transmitting
  - Monitor the presence of signal energy coming from other adapters
  - If frame is transmitted without detecting signal energy from other adapters, then done.
- (4) If the adapter detects signal energy from other adapters while transmitting:
  - Stop transmitting the frame
  - Transmit a 48-bit jam signal
- (5) After aborting, start the exponential back-off algorithm
  - when transmitting a frame, after experiencing the n^{th} collision in a row for this frame, the adapter chooses a value K at random from {0, 1, 2, …, 2^m-1} where m = min (n , 10)
  - Adapter waits K * 512 bits times
  - Go back to Step 2

Ethernet CSMA/CD



Backoff After Collision

- When collision occurs
  - Wait random time t1, $0 \leq t1 \leq d$
  - Use CSMA and try again
- If second collision occurs
  - Wait random time t2, $0 \leq t2 \leq 2*d$
- Double range for each successive collision
- Called exponential backoff

Exponential Back-off Algorithm

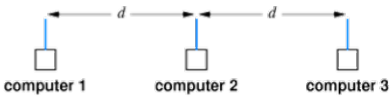
- Let 1 Slot Time = 512 bit times
- Upon 1st collision, randomly choose among {0,1} slot delay
- Upon 2nd collision, randomly choose among {0,1,2,3} slot delay
- Up to a maximum of 16 transmission attempts with a range of delay from {0 to 1024} bit times: $0 \leq r < 2^m-1$
  - r is the random number generated, m = MIN(n,10) and where n is the n-th retransmission attempt

The Collision Domain

- Minimum length frame must be ≥ Maximum RTT of the Ethernet segment
- Minimum frame is 512 bits
  - Requires 46 bytes of data whether the upper layer has them or not
- Distances decrease as speed increases
- Full-duplex mode eliminates the collision domain

Media Access on a Wireless Net

- Limited range
  - Not all stations receive all transmissions
  - Cannot use CSMA/CD
- Example in diagram
  - Maximum transmission distance is d
  - Stations 1 and 3 do not receive each other's transmissions



CSMA/CA

- Used on wireless networks
- Both sides send small message followed by data transmission
  - "X is about to send to Y"
  - "Y is about to receive from X"
  - Data from sent from X to Y
- Purpose: inform all stations in range of X or Y before transmission
- Known as Collision Avoidance (CA)

Data Link Protocols: Token Ring

Token Ring is deterministic technology with predictable delay.

Was developed in 1980 – 1985 by IBM. Approved as standard by IEEE.

Technology description:

This is not continuous wire, consists of connections among host interfaces, connecting to Ring by means of Multiple Access Units (MAU). (No more than 8 hosts per MAU).

Physical address is configurable by means of switches.

Control frame named "Token" is passed from one host to another, allowing to this host (and only this) to send the packet.

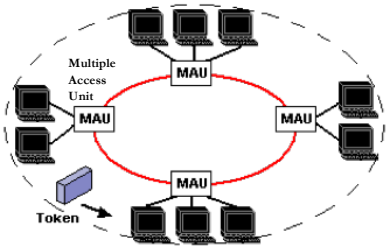
To send the frame, host performs the following steps:
- waits for the arriving Token
- converts it to data frame and copies to the next host in the Ring
- waits for the frame to return after delivery
- deletes the frame and sends out a new Token

Each moment of time no more than 1 host sends the data, all other hosts copy the data by chain.

Host interface could be in following modes:
- transmit mode – sending host
- copying mode – all other hosts in ring
- recovery mode – recovery in case of token loss

When copying host recognizes its destination address, it cleans refuse bit.

Sender, accepting the original frame, detects if frame was delivered, checking the refuse bit.

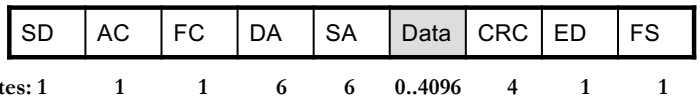


Fist connected to Ring host accepts the status of Active Monitor. It responsible for:

- Token creation and recovery
- Check frame delivery timeout
- Deletion of frames not deleted by other hosts.
- Notification of other hosts about its presence in Ring (sends "Active Monitor Present" frame)
- In case of Active Monitor problem, other hosts compete to accept its status.

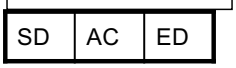
In Token Ring collisions never occur.
This ensures good performance of network under big loads (30%-40%)

Token Ring Data Frame



Bytes:	1	1	1	6	6	0..4096	4	1	1

Token Ring "Token"



1	1	1	

SD - Start Delimiter

AC - Access Control - packet priority, type (token/data), active monitor bit

FC - Frame Control

DA - Destination Address

SA - Source Address

CRC - Cyclic Redundancy Check sum

ED - End Delimiter - contains 1 bit – Last Packet bit, Error flag bit

FS - Frame Status - contains Parity bit (copy indicator),
Refuse bit (destination reached)

ETR – Early Token Release technology

After sending of frame, the same host generates new Token. As result, many sequential frames could circulate in the Ring in the same time. But no more than one Token could present in each moment of time.

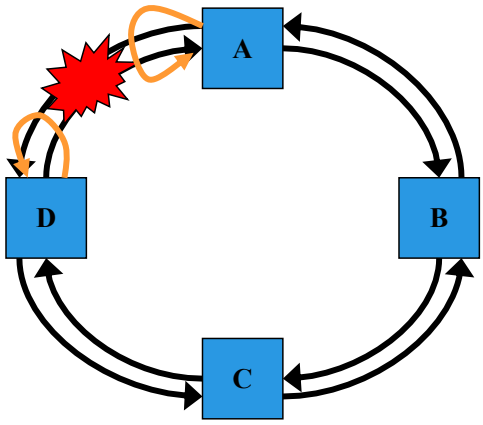
This technology improves the performance of Token Ring.

FDDI Terminology

- FDDI
  - Uses optical fibers
  - High reliability
  - Immune to interference
- CDDI
  - FDDI over copper
  - Same frame format
  - Same data rate
  - Less noise immunity

Fiber Distributed Data Interconnect (FDDI)

- Uses fiber instead of copper wire
- Not susceptible to electrical interference
- Dual Counter-rotating rings
- Self-healing



FDDI Properties

- Shared
  - Multiple computers connect to network
- Ring
  - Computers are in a circle
- Token passing ring
  - Token passes from station to station
  - Station waits for token to transmit
  - Guarantees fairness

Other Network Technologies

- ATM – Asynchronous Transfer Mode
  - Connection oriented
  - Designed to carry voice and data
- Wireless Network Technologies

Another Example of a Physical Star Topology

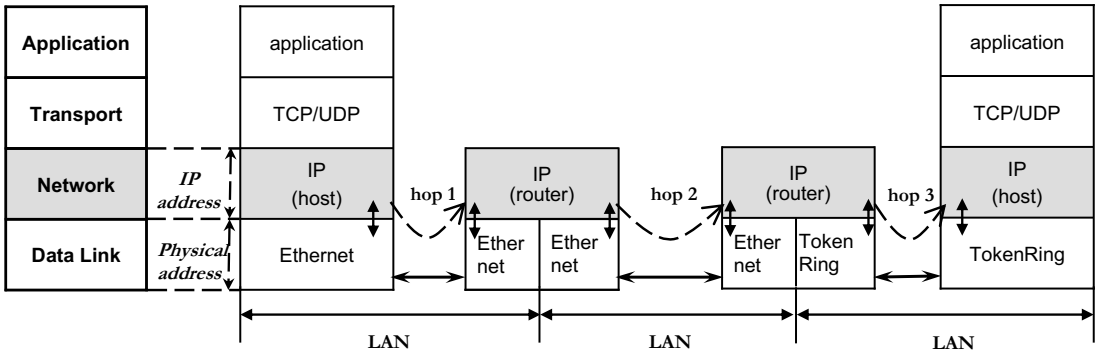
- Asynchronous Transfer Mode (ATM)
- Designed by telephone companies
- Intended to accommodate
  - Voice
  - Video
  - Data

Network Layer: Internet Protocol

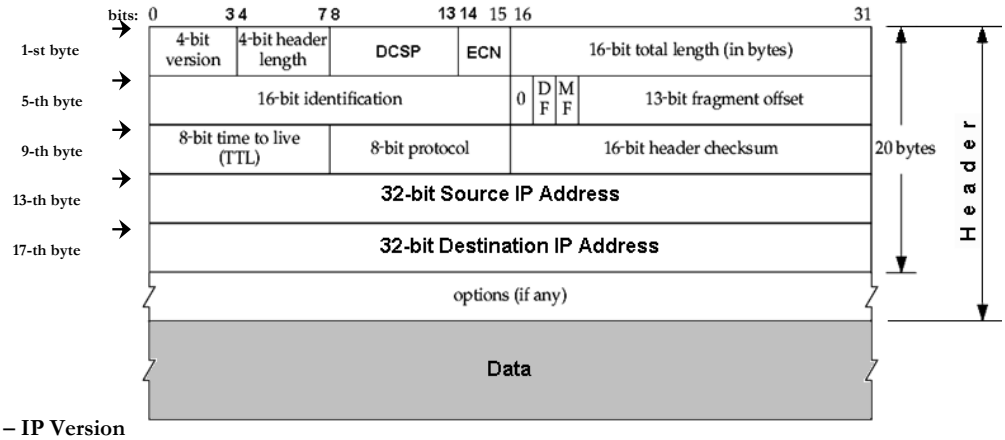
Internet Protocol (IP)
Provides **unreliable connectionless packet delivery** service, containing:

- **Routing,**
- **Fragmentation / Reassembling,**
- **Multiplexing / Demultiplexing.**

Works with different Data Link layers, hiding the technological differences between the networks.



Internet Protocol: IP(v4) Packet Structure



- **Version – IP Version**
- **Header length – IP Header total length in 32bit words (max = 15*4=60 bytes)**
- **DSCP, ECN – type of service fields, used by upper protocols**
- **Total Length – total packet length (header + data).**
- **Identification, DF (don't fragment), MF (more fragments), Fragment Offset – used for fragmentation and reassembly.**
- **TTL - time-to-live – maximal number of hops, set by the sender, decremented by each router.**
- **Protocol - upper layer protocol (1=ICMP, 2=IGMP, 6=TCP, 17=UDP).**
- **Header Checksum - calculated over just the IP header including any options.**
- **Source IP address (32 bit)**
- **Destination IP address (32-bit)**
- **Options (<=40 bytes) , used by upper protocols**

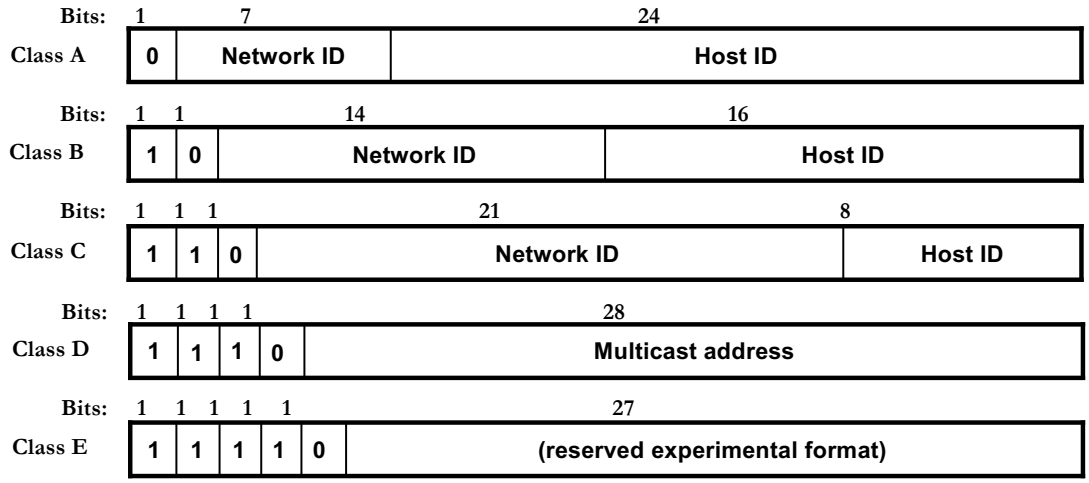
Internet Address Formats

- Internet Address (IP address) is mandatory unique logical address which must have every host in Internet.
- IP Address (IPv4) is 32-bit number.
- Decimal Dotted Notation is human-oriented representation of IP Address as sequence of 4 decimal numbers
- separated by dot.
- The IP Address has internal structure. There are 5 classes of IP Address:

Class	Range	Networks Per Class *	Hosts Per Network *
A	0.0.0.0 to 127.255.255.255	2^7 – 2 = 126	2^24 – 2 = 16,777,214
B	128.0.0.0 to 191.255.255.255	2^14 – 2 = 16,382	2^16 – 2 = 65,534
C	192.0.0.0 to 223.255.255.255	2^21 – 2 = 2,097,150	2^8 – 2 = 254
D	224.0.0.0 to 239.255.255.255	N/A	N/A
E	240.0.0.0 to 247.255.255.255	N/A	N/A

Note:
The 2 types of bit sequences:
• All Bits equal 1
• All Bits equal 0
are not used as Network IDs and Host IDs

Internet Address Formats



Netmask

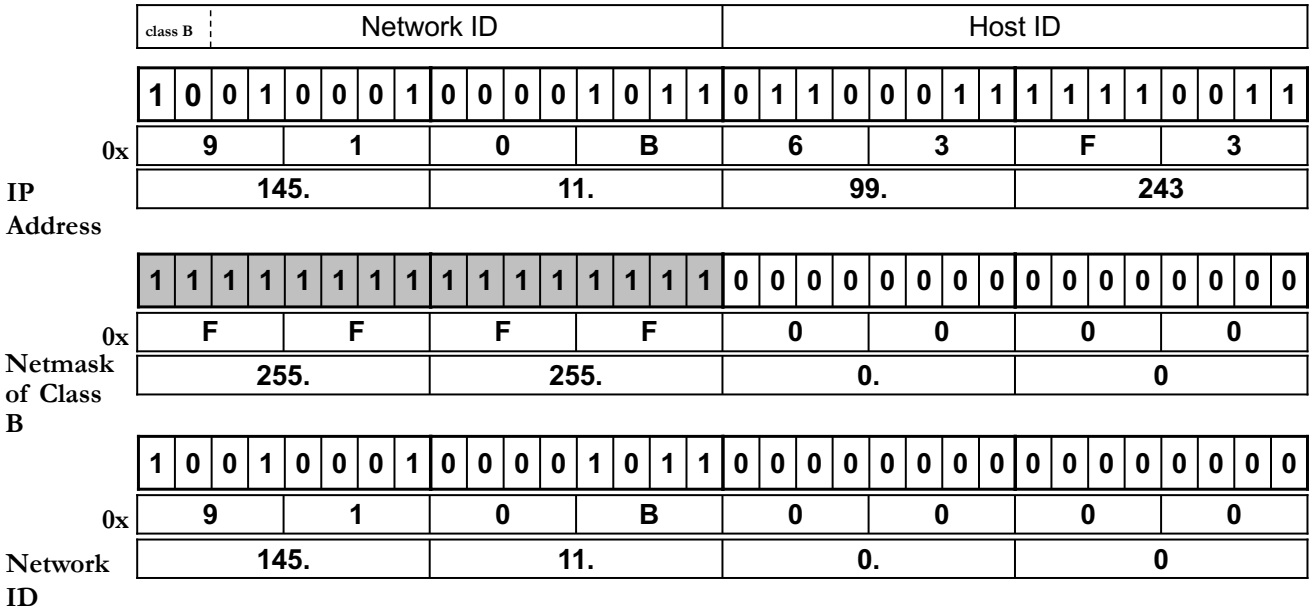
Gateways, to locate the network, need only Network ID part of IP Address and don't need to know the location of every host. This is important concept of routing.
To calculate Network ID from IP Address, Gateways use Netmask.

```
NETWORK_ID = IP_ADDRESS & NETMASK
```

Class	Network ID	Netmask
A	1 byte	255. 0. 0. 0
B	2 bytes	255. 255. 0. 0
C	3 bytes	255. 255. 255. 0

Netmask: Example

Calculation of Network ID for IP Address = 145.11.99.243 (Class B)



Network ID and Subnet ID

IP Addresses are assigned by specific authority: InterNIC- *Internet Network Information Center.*

The InterNIC assigns only Network IDs. The assignment of Host IDs is responsibility of local site system administrator.

IP addresses are often subnetted. Subnet adds additional level to the address hierarchy:

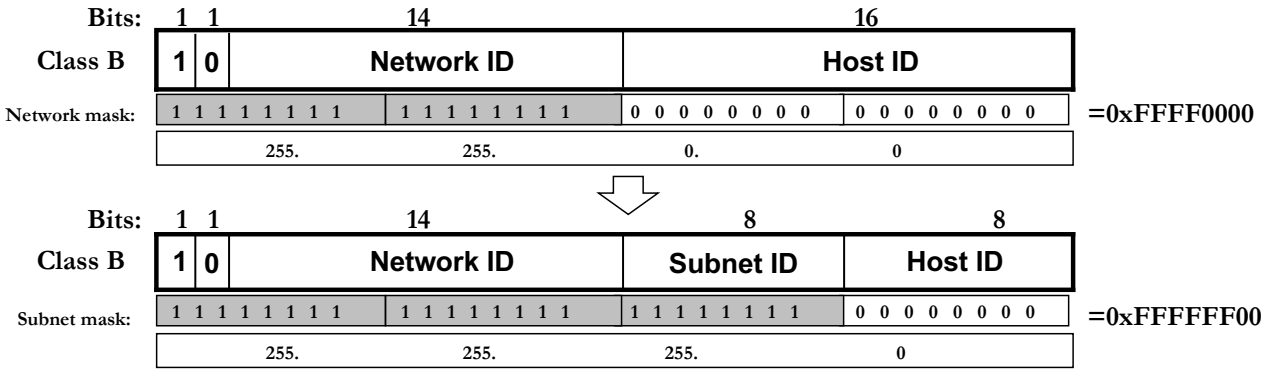
- Network ID (assigned to site)
- Subnet ID (chosen by site)
- Host ID (chosen by site)

All the hosts on a given subnet share a common Subnet Mask, and this mask specifies the boundary between the subnet ID and the host ID. Bits of 1 in the subnet mask cover the network ID and subnet ID, and bits of 0 cover the host ID.

```
SUBNETWORK_ADDR      = IP_ADDRESS & SUBNET_MASK
```


Network ID and Subnet ID: Example

Subnetting of Network with Class B address, using 8 bit Subnet ID.

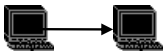


In the example above local gateway needs only 8 bits of Subnet ID for routing. Adding new host to existing sub-network will not require any changes to the internal gateways.

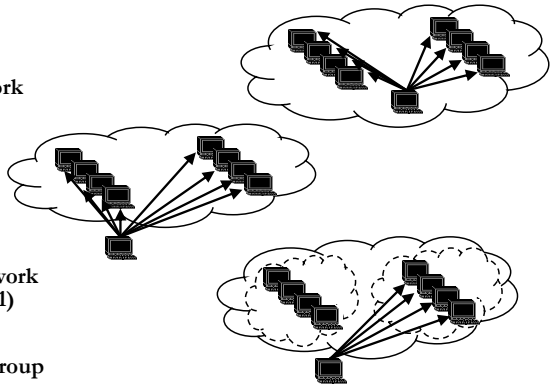
Types of Destination IP Address

There are three ***Destination Types*** of IP addresses**:**

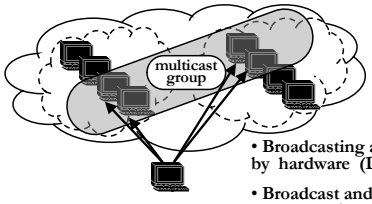
- ***Unicast*** **(destined for a single host)**



- ***Broadcast*** **(destined for all hosts on a given network)**
  - **Limited Broadcast to all hosts inside local network (Network ID = all 1, Host ID = all 1)**
  - **Net-Directed Broadcast to all hosts of other local network (Network ID = *netID,* Host ID = all 1)**
  - **Subnet-Directed Broadcast to all hosts in specific sub-network (Network ID = *netID*, Subnet ID = *subnetId*, Host ID = all 1)**



- ***Multicast*** **(destined for a set of hosts that belong to a multicast group or sub-network).**
  - **Multicast Address is a special type of address that is recognizable by multiple hosts joined a Multicast Group .**
  - **A Multicast Address is sometimes known as a Functional Address or a Group Address.**
  - **Hosts that are interested in receiving data flowing to a particular group must join the group using:**
    - **IGMP -** Internet Group Management Protocol .



- **Broadcasting and Multicasting needs support by hardware (Data Link layer).**
- **Broadcast and Multicast addresses could not be used as Source IP Address**

Special Case IP Addresses

Loopback Addresses

By convention, the address 127.0.0.1 is assigned to the Loopback Interface.
Anything sent to this IP address loops around and becomes IP input without ever leaving the machine.
This address id often used when testing a client and server on the same host.
Any address on the network 127/8 can be assigned to the loopback interface, but 127.0.0.1 is and is often configured automatically by the IP stack.
(This address is known as INADDR_LOOPBACK)

Unspecified Address

The address consisting of 32 zero bits is Unspecified Address.
It is only permitted to appear as the source address in packets sent by a node that is bootstrapping before the node learns its IP address.
(This address is known as INADDR_ANY).

Private Addresses

Three address ranges are set aside for "Private Internets".
These are the networks that do not connect directly to the public Internet.
Small sites use these private addresses and Network Address Translation (NAT) to a single public IP address visible to the Internet.

Class	Range	Number of addresses
A	10.0.0.0 to 10.255.255.255	16,777,216
B	172.16.0.0 to 172.31.255.255	1,048,576
C	192.168.0.0 to 192.168.255.255	65,536

NAT - Network Address Translation
Also known as Network Masquerading or IP-masquerading is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall.

It is most commonly used to enable multiple hosts on a private network to access the Internet using a single public IP address.

Multihoming and Address Aliases

Multihomed Host: A host with multiple interfaces where each interface must have a unique IP address. (Loopback interface is not counted)

A router, by definition, is multihomed since it forwards packets from one interface to another one. But, a multihomed host is not a router unless it forwards packets.

There are two types of Multihoming:

- ***Physical Multihoming*: Host has multiple physical interfaces, each interface has its own IP address.**
- ***Logical Multihoming* : Newer hosts have the capability to assigning multiple IP addresses to the same physical interface. Each additional IP address, after the first (primary), is called an *Alias* or *Logical Interface*.**

Multihomed Network

This is a network that has multiple connections to the Internet.
For example, some sites have two connections to the Internet instead of one, providing a backup capability.

ifconfig

UNIX/LINUX utility for configuring network interface parameters

```
$ ifconfig -a
eth0    Link encap:Ethernet  HWaddr 00:11:25:0C:DE:88
          inet addr:145.9.228.95  Bcast:145.9.228.255  Mask:255.255.255.0
          inet6 addr :fe80::211:25ff:fe0c:de88/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2295264 errors:0 dropped:0 overruns:0 frame:0
          TX packets:783513 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:319104166) 304.3 MiB  (TX bytes:75720636) 72.2 MiB(
          Base address:0x2000 Memory:e8100000-e8120000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr:: :1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:804848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:804848 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:49311882) 47.0 MiB  (TX bytes:49311882) 47.0 MiB)
```


Domain Name System

Domain Name System (DNS): A distributed database that provides the mapping between IP addresses and hostnames. Hostnames are more suitable for human use, than IP addresses.

The DNS is *distributed* because no single site on the Internet knows all the information.
Each site maintains its own database of information and runs a DNS Server program that other systems across the Internet (clients) can query. The DNS provides the protocol that allows clients and servers to communicate with each other.

Applications access the DNS through a *Resolver*. The resolver contacts one or more *name servers* to do the mapping.

nslookup
UNIX utility for DNS information access

```
$nslookup gate88.mot.com
Server:  abcde.mot.com
Address  :145.19.17.68

Name :gate88.mot.com
Address  :145.19.238.87
```

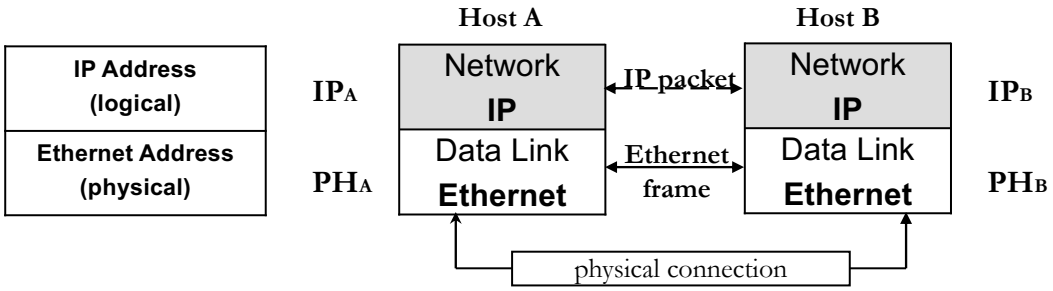
The DNS Name Space is *Hierarchical Tree*.
The InterNIC maintains the top-level domains:

- **Generic Domains (com, edu, gov, int, mil, net, org)**
- **Country Domains (us, uk, lb, ru, etc.)**

InterNIC delegates responsibility to others for specific *Zones*. A *Zone* is a subtree of the DNS tree that is administered separately. Many second-level domains then divide their zone into smaller zones.
To accept the DNS information, every Name Server must know how to contact the *Root Name Servers.* The root server tells the requesting server to contact another server, and so on.

A fundamental property of the DNS is *Caching.*
Name Server caches accepted {IP Address ; Hostname} information for following reuse.

Address Resolution



- Address Resolution Problem: I want to send IP packet to another host with known IP Address. What is Physical Address of that host?
  - Known: IPA, PHA, IPB.
  - Unknown: PHB
- Reverse Address Resolution Problem: I'm diskless workstation. What is my own IP address ?
  - Known: PHA.
  - Unknown: IPA.

ARP

ARP – Address Resolution Protocol

Solves Address Resolution Problem by providing *dynamic mapping* from an IP Address to the corresponding Physical Address on the same physical network.

ARP Request is *Ethernet Broadcast* frame (Destination Ph Address = 0xFFFFFFFFFFFF) is sent to all hosts in physical network.

Only the host, recognizing its own IP Address in the Request, sends the ARP Reply, containing its Physical address.

ARP Cache

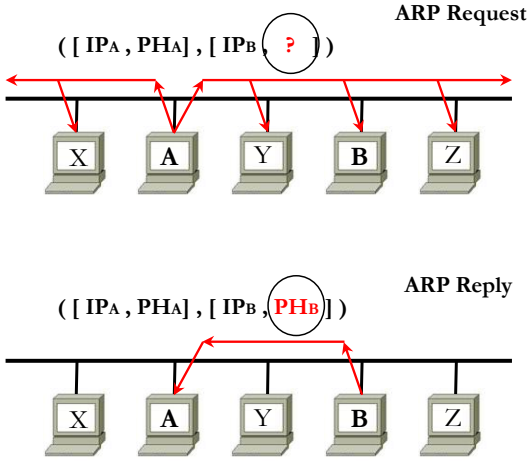
• Maintains the recent mappings from Internet addresses to Physical addresses.

• Removes its entries after expiration time

Proxy ARP

Lets to Router to answer ARP requests, addressed to another physical network, substituting router's physical address instead of target foreign host address.

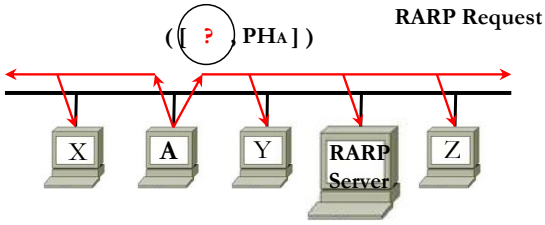
Then, accepting the frame, router forwards it to the target foreign host.



arp
UNIX utility for ARP Cache access

```
$arp –a
sun (140.252.13.33) at 8:0:20:3:f6:42
svr4 (140.252.13.34) at 0:0:c0:c2:9b:26
```

RARP Protocols



RARP – Reverse Address Resolution Protocol: Solves Reverse Address Resolution Problem. Used by diskless hosts during its initialization (bootstrap).

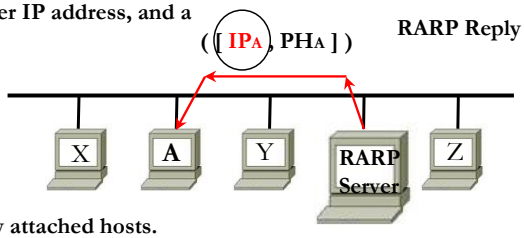
RARP Request is *Ethernet Broadcast* frame, sent to all hosts in physical network.

Only the RARP Server, containing the required information, sends RARP Reply, containing IP Address of requestor.

RARP Server serves single LAN. It could be multiple RARP Servers in LAN. They handle *Distributed Data Base* of IP Addresses.

RARP Servers provide delay mechanism to avoid simultaneous response to requestor from multiple RARP Servers in the same time.

BOOTP – Bootstrap Protocol



- Enables a diskless workstation to discover its own IP address, BOOTP Server IP address, and a file to be loaded into memory to boot the machine.
- Needs manual pre-configuration of the host information.
- Could be routed and serve more than one LAN.

DHCP – Dynamic Host Configuration Protocol

- Allows *dynamic* allocation of network addresses and configurations to newly attached hosts.
- Allows recovery and reallocation of network addresses through a *leasing mechanism*.
- Does not require manual pre-configuration of the host information.
- Could be routed and serve more than one LAN.

ICMP

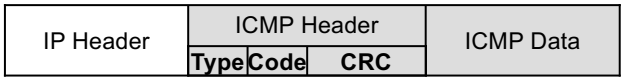
ICMP - Internet Control Message Protocol.

ICMP handles Error and Control information messages between routers and hosts.

These messages are normally generated by and processed by the TCP/IP networking software.

Example of usage: *ping* and *traceroute* programs use ICMP.

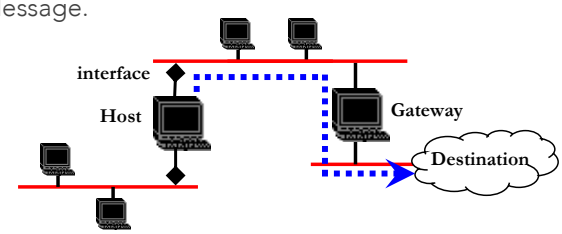
ICMP Message



Type	Description	Query	Error
0	echo reply (ping reply)	*	
3	destination unreachable		*
4	quench (flow control)		*
5	redirect (use another router)		*
8	echo request (ping request)	*	
9	router advertisement (reply to solicitation)	*	
10	router solicitation (request for advertisement)	*	
11	time exceeded (TTL=0)		*
12	parameter problem (bad IP header)		*
13	time stamp request (what time is it now)	*	
14	timestamp reply (current time is…)	*	
17	address mask request (give my subnet mask)	*	
16	address mask reply (your subnet mask is …)	*	

IP Routing: Routing Table

- Routing Table
  - The IP layer has a Routing Table in memory that it searches each time it receives a datagram to send.
  - The Routing Table contains the following information:
  - Destination
    - IP Address of Destination Host (flag "H") or Destination Network (no flag "H")
  - Gateway
    - IP Address of Hop Router for Remote Network (flag "G") or IP Address of Local Host in Directly Connected Network (no flag "G")
  - Flag
    - "U"- route is up, "G"- route to Remote Network via Gateway, "H" - route to specific Host,
  - "D"- route was added because of an ICMP Redirect Message.
  - Ref
    - The number of times the route used to establish a connection.
  - Use
    - The number of transmitted packages
  - Interface
    - The Network Interface used by route

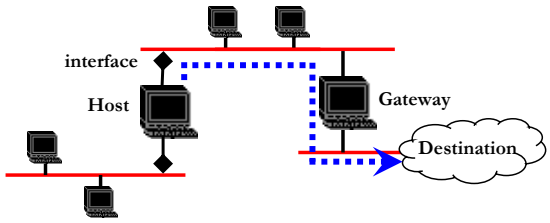


IP Routing: Routing Table

UNIX Utilities:

route: Utility for manual manipulation with Routing Table

netstat: Utility, showing network status

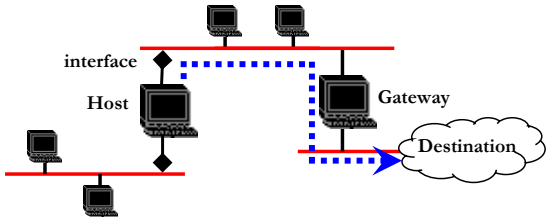



```
# netstat -nr
Routing Table: IPv4
Destination   Gateway      Flags Ref Use     Interface
------------ ------------ ----- --- ------- ---------
127.0.0.1     127.0.0.1    UH      1     298   lo0
default       175.16.12.1  UG      2   50360
175.16.12.0   175.16.12.2  U      40  111379   bge0
175.16.2.0    175.16.12.3  UG      4    1179
175.16.1.0    175.16.12.3  UG     10    1113
175.16.3.0    175.16.12.3  UG      2    1379
175.10.4.3    175.16.12.5  UGH     1    1119
```

- Loopback Route (Local Host) via interface lo0
- Default Router 175.16.12.1
- Directly Connected Network 175.16.12.0 via interface bge0
- Route to Remote Network 175.16.2.0 via Gateway 175.16.12.3
- Route to Remote Network 175.16.1.0 via Gateway 175.16.12.3
- Route to Remote Network 175.16.3.0 via Gateway 175.16.12.3
- Route to Remote Host 175.10.4.3 via Gateway 175.16.12.5

IP Routing: Routing Table

- Routing Table: The IP layer has a Routing Table in memory that it searches each time it receives a datagram to send.
- The Routing Table contains the following information:
  - Destination: IP Address of Destination Host (flag "H") or Destination Network (no flag "H")
  - Gateway: IP Address of Hop Router for Remote Network (flag "G") or IP Address of Local Host in Directly Connected Network (no flag "G")
  - Flags: "U"- route is up, "G"- route to Remote Network via Gateway, "H" - route to specific Host, "D"- route was added because of an ICMP Redirect Message.
  - Ref: The number of times the route used to establish a connection.
  - Use: The number of transmitted packages
  - Interface: The Network Interface used by route



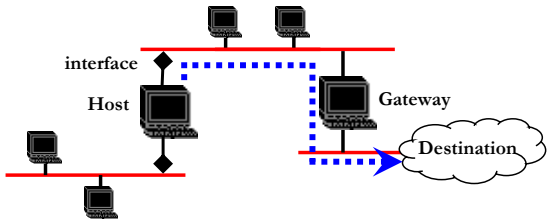
IP Routing: Routing Table

UNIX Utilities:

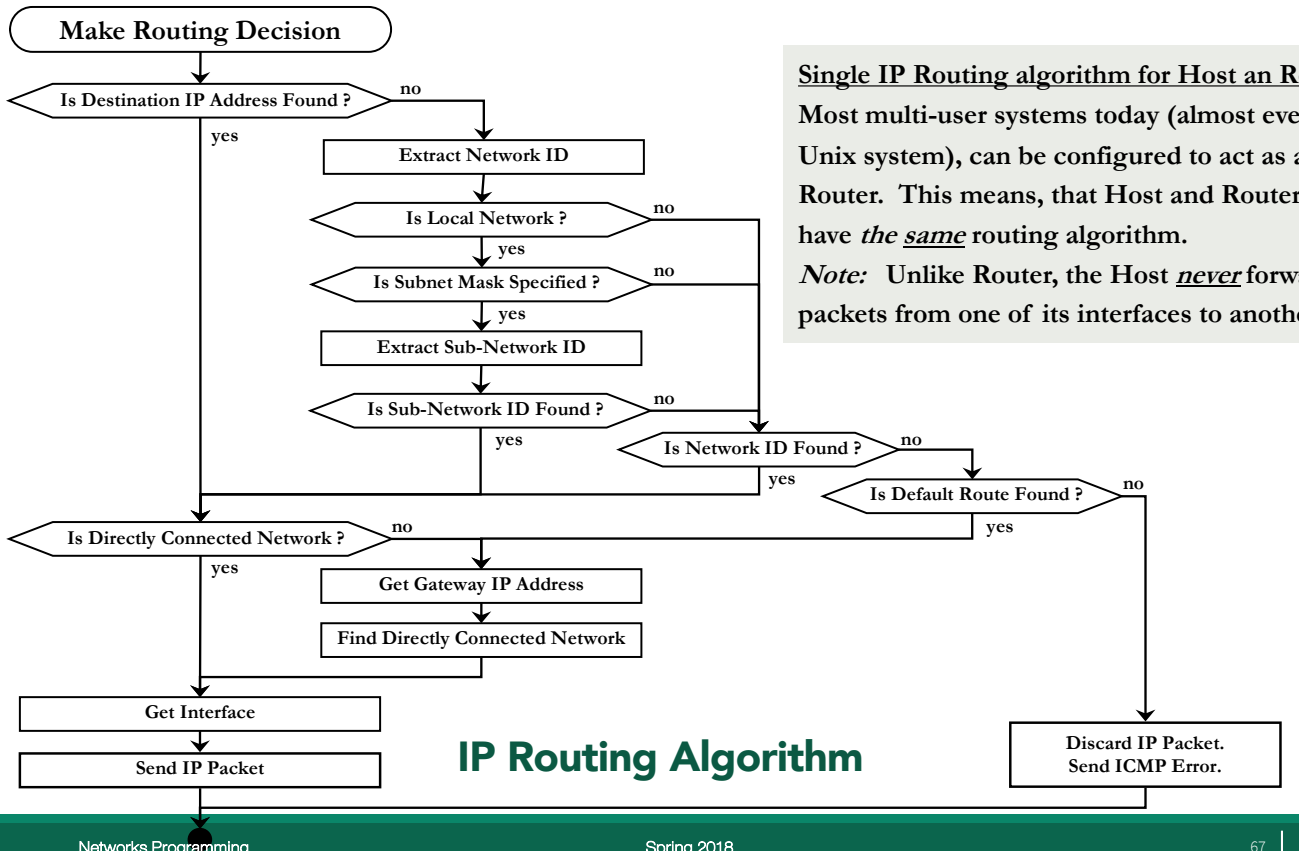
route - Utility for manual manipulation with Routing Table

netstat - Utility, showing network status

```
# netstat -nr
Routing Table: IPv4
Destination   Gateway       Flags Ref Use      Interface
------------ ------------ ----- --- ------- ---------
127.0.0.1     127.0.0.1     UH      1     298   lo0
default       175.16.12.1   UG      2   50360
175.16.12.0   175.16.12.2   U      40  111379   bge0
175.16.2.0    175.16.12.3   UG      4    1179
175.16.1.0    175.16.12.3   UG     10    1113
175.16.3.0    175.16.12.3   UG      2    1379
175.10.4.3    175.16.12.5   UGH     1    1119
```



- Loopback Route (Local Host) via interface lo0
- Default Router 175.16.12.1
- Directly Connected Network 175.16.12.0 via interface bge0
- Route to Remote Network 175.16.2.0 via Gateway 175.16.12.3
- Route to Remote Network 175.16.1.0 via Gateway 175.16.12.3
- Route to Remote Network 175.16.3.0 via Gateway 175.16.12.3
- Route to Remote Host 175.10.4.3 via Gateway 175.16.12.5



Single IP Routing algorithm for Host an Router

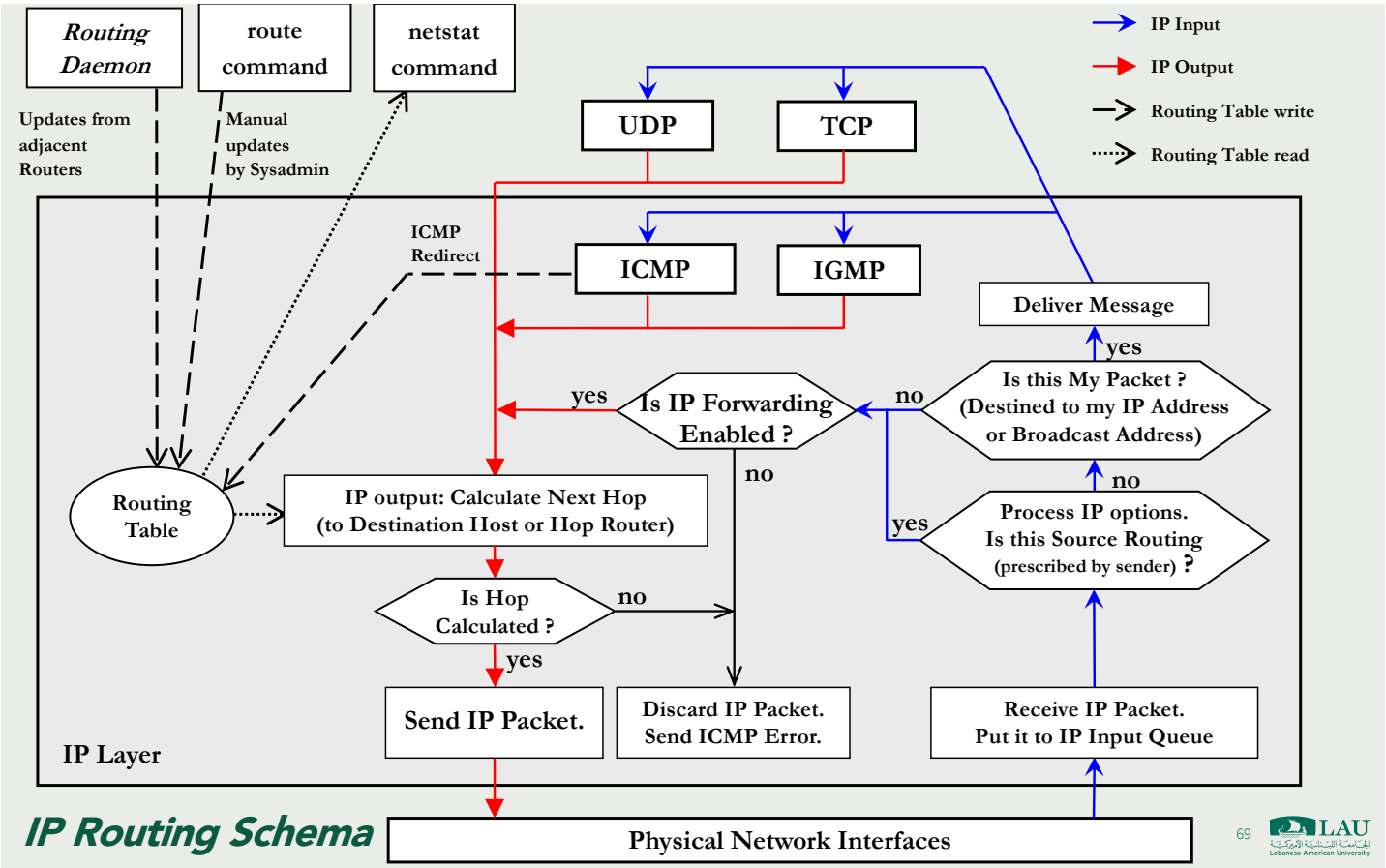
Most multi-user systems today (almost every Unix system), can be configured to act as a Router. This means, that Host and Router could have *the same* routing algorithm.

Note: **Unlike Router, the Host *never* forwards packets from one of its interfaces to another.**

IP Routing Algorithm

Static and Dynamic IP Routing

- Static Routing
  - During Static Routing the Routing Table:
    - created during interface configuration
    - added by the route command
    - or created by an ICMP redirect (if the wrong "default" was used)
  - It is fine if the network is small, has a single connection point to other networks and does not have redundant routes (which could be used if a primary route fails)
- Dynamic Routing
  - During Dynamic Routing the Routing Table also updated by Routing Daemon process.
    - the Routing Daemon is running on the Router
    - communicates with another Routers using a Routing Protocol
    - dynamically updates the kernel's routing table with information it receives from neighbor routers
- Routing Protocols are separated to:
  - IGP: Interior (Intra-Domain) Gateway Protocols
    - Used between the Routers of one autonomous system
    - Examples: RIP – Routing Information Protocol , OSPF - Open Shortest Path First protocol.
  - EGP
    - Exterior (Inter-Domain) Gateway Protocols
    - Used between the Routers of different autonomous systems.
    - Example: BGP – Border Gateway Protocol



IP Routing Schema