IT 4505
Section 3

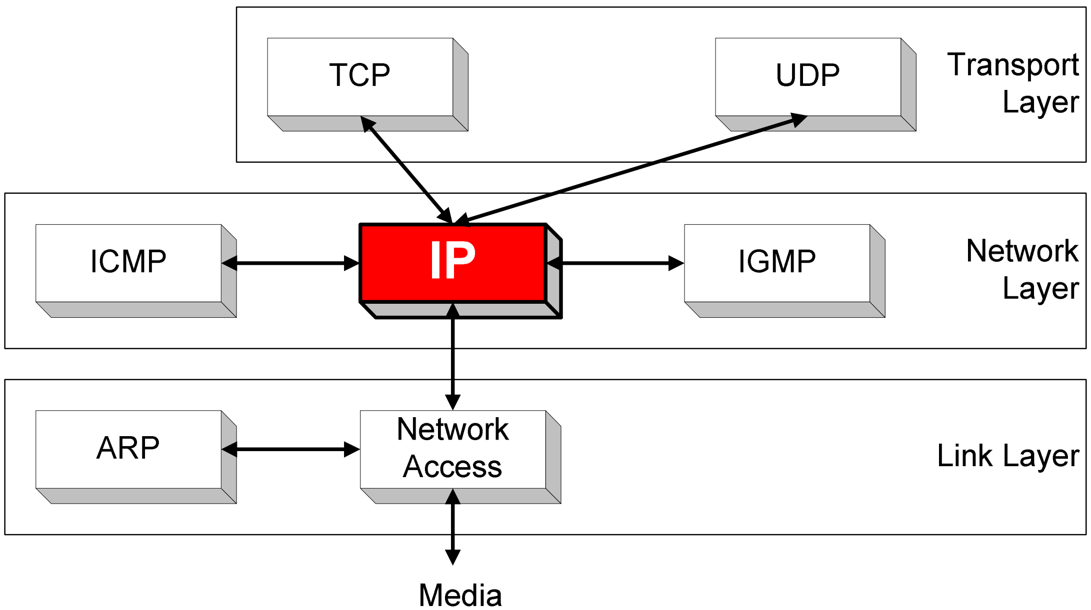
Internet protocol suite

3.1 Introduction - Internet protocol

- The most widely used protocol for internetworking is the Internet Protocol (IP).
- IP attaches a header to upper-layer (e.g., TCP) data to form an IP datagram.
- The header includes
    - ✓ source and destination addresses
    - ✓ Information used for fragmentation
    - ✓ Reassembly
    - ✓ Time to-live field
    - ✓ Type-of-service
    - ✓ Checksum.

Introduction cont.

- IP (Internet Protocol) is a Network Layer Protocol.



- At present, the widely installed version of IP is 4 (IPV4). But because of the problems such as depletion of IP addresses available in IPV4,the newer version IPV6 is being gradually implemented in networks. It is specified in RFC 791.

3.1.1 History of Internet protocols

- IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers.
- Initially developed as part of the research network developed by the United States *Defense Advanced Research Projects Agency* (*DARPA* or *ARPA*).
- The ARPAnet began in 1973.
- The first major version of IP, Internet Protocol Version 4 (IPv4).

3.1.2 Internet Protocol stack

- A machine on the Internet runs the TCP/IP protocol stack and sends the IP packets to all the other machines on the Internet using the IP address.
- Protocol stacks are typically based either on the OSI model or on the TCP/IP model.
- Today's the Internet is actually a collection of many thousands of networks that use the TCP/IP protocol stack.
- The Internet protocol stack consists of five layers: the physical, link, network, transport, and application layers.

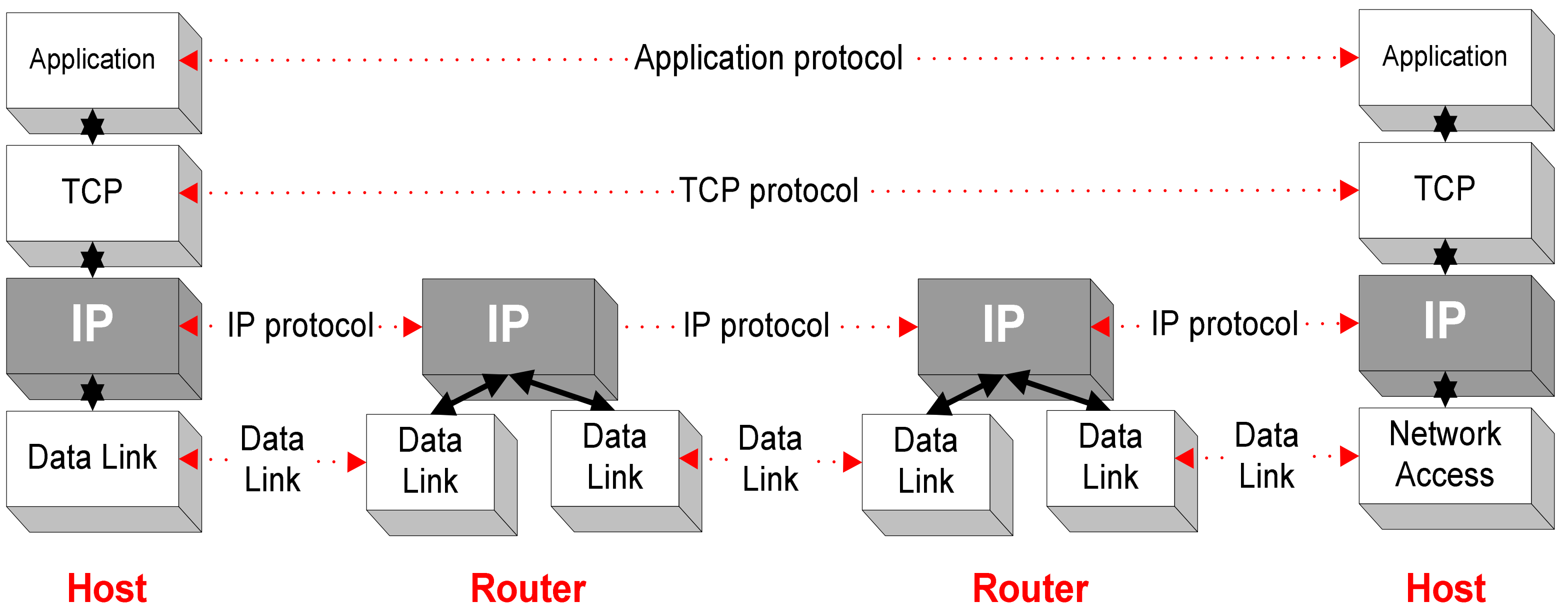
Five-layer Internet protocol stack

1.3.3 IP Addressing and Routing

- The IP header is tagged with the source IP address, the destination IP address, and other meta-data needed to route and deliver the datagram.
- Each datagram has two components: a header and a payload.
- IP header is tagged with the source IP address, the destination IP address.
- The payload is the data that is transported.
- The address space is divided into networks and sub networks.
- IP routing is performed by all hosts, but most importantly by routers.
- Routers communicate with one another via specially designed routing protocols.
- IP routing is also common in local networks.

IP Addressing and Routing cont.

- IP is the highest layer protocol which is implemented at both routers and hosts



IP Datagram Format

bit # 0 7 8 15 16 23 24 31

<table>
<tr><td>version</td><td>header length</td><td>DS</td><td>ECN</td><td colspan="4">total length (in bytes)</td></tr>
<tr><td colspan="4">Identification</td><td>0</td><td>D F</td><td>M F</td><td>Fragment offset</td></tr>
<tr><td colspan="2">time-to-live (TTL)</td><td colspan="2">protocol</td><td colspan="4">header checksum</td></tr>
<tr><td colspan="8">source IP address</td></tr>
<tr><td colspan="8">destination IP address</td></tr>
<tr><td colspan="8">options (0 to 40 bytes)</td></tr>
<tr><td colspan="8">payload</td></tr>
</table>

← 4 bytes →

- 20 bytes ≤ Header Size < 2^4 x 4 bytes = 60 bytes
- 20 bytes ≤ Total Length < 2^{16} bytes = 65536 bytes

Fields of the IP Header

- **Version (4 bits)**: current version is 4, next version will be 6.
- **Header length (4 bits)**: length of IP header, in multiples of 4 bytes
- **DS/ECN field (1 byte)**
  - This field was previously called as Type-of-Service (TOS) field. The role of this field has been re-defined, but is “backwards compatible” to TOS interpretation
  - Differentiated Service (DS) (6 bits):
    - Used to specify service level (currently not supported in the Internet)
  - Explicit Congestion Notification (ECN) (2 bits):
    - New feedback mechanism used by TCP

Fields of the IP Header

- **Identification (16 bits):**

  Unique identification of a datagram from a host.
  Incremented whenever a datagram is transmitted

- **Flags (3 bits):**

  - First bit always set to 0
  - DF bit (Do not fragment)
  - MF bit (More fragments)

  Will be explained later→ Fragmentation

Fields of the IP Header

- **Time To Live (TTL) (1 byte):**
  - Specifies longest paths before datagram is dropped
  - Role of TTL field: Ensure that packet is eventually dropped when a routing loop occurs

Used as follows:

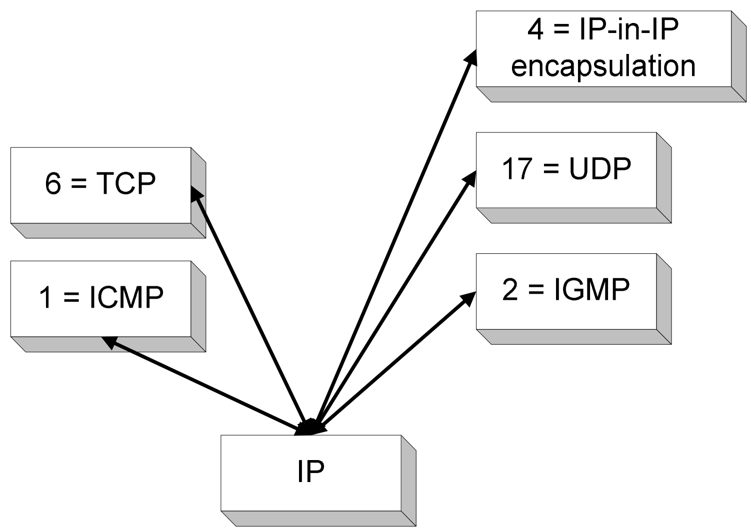
  - Sender sets the value (e.g., 64)
  - Each router decrements the value by 1
  - When the value reaches 0, the datagram is dropped

UCSC

BIT

Fields of the IP Header

- **Protocol (1 byte):**
  - Specifies the higher-layer protocol.
  - Used for demultiplexing to higher layers.



- **Header checksum (2 bytes):**

  A simple 16-bit long checksum which is computed for the header of the datagram.

Fields of the IP Header

- **Options:**
  - Security restrictions
  - Record Route: each router that processes the packet adds its IP address to the header.
  - Timestamp: each router that processes the packet adds its IP address and time to the header.
  - (loose) Source Routing: specifies a list of routers that must be traversed.
  - (strict) Source Routing: specifies a list of the only routers that can be traversed.
- **Padding:**

  Padding bytes are added to ensure that header ends on a 4-byte boundary

Maximum Transmission Unit

- Maximum size of IP datagram is 65535, but the data link layer protocol generally imposes a limit that is much smaller

  Example:

  - Ethernet frames have a maximum payload of 1500 bytes

    → IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes

- The limit on the maximum IP datagram size, imposed by the data link protocol is called **maximum transmission unit (MTU)**

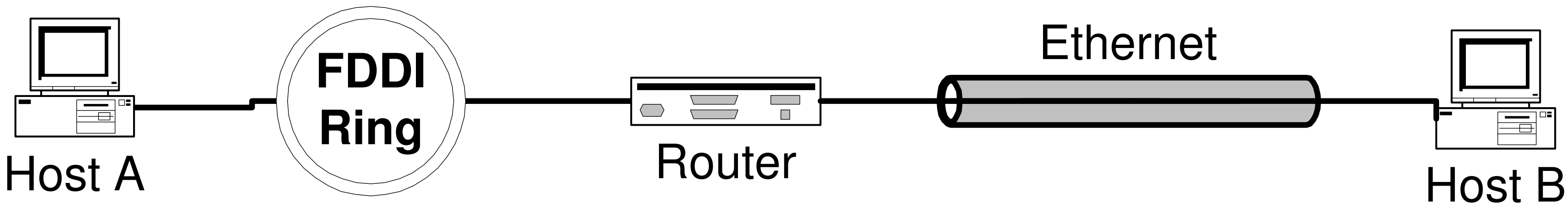
- MTUs for various data link protocols:

Ethernet:	1500	FDDI:	4352
802.3:	1492	ATM AAL5:	9180
802.5:	4464	PPP:	negotiated

IP Fragmentation

- What if the size of an IP datagram exceeds the MTU?
  IP datagram is fragmented into smaller units.

- What if the route contains networks with different MTUs?



MTUs: FDDI: 4352 Ethernet: 1500

- **Fragmentation**:
  - IP router splits the datagram into several datagram
  - Fragments are reassembled at receiver

IP Address

What is an IP Address?

- ❑ An IP address is a unique global address for a network interface
- ❑ Exceptions:
  - Dynamically assigned IP addresses
  - IP addresses in private networks
- ❑ An IP address: (IPV4)
  - is a **32 bit long** identifier
  - encodes a network number (**network prefix**) and a **host number**

Network prefix and host number

- The network prefix identifies a network and the host number identifies a specific host (actually, interface on the network).

network prefix	host number

- **How do we know how long the network prefix is?**
  - **Before 1993:** The network prefix is implicitly defined (**class-based addressing**)

  or
  - **After 1993:** The network prefix is indicated by a **netmask. (classless inter domain routing)**

Dotted Decimal Notation

- IP addresses are written in a so-called ***dotted decimal* notation**
- Each byte is identified by a decimal number in the range [0..255]
- **Example:**

10000000	10001111	10001001	10010000
1st Byte	2nd Byte	3rd Byte	4th Byte
= 128	**= 143**	**= 137**	**= 144**

128.143.137.144

Example

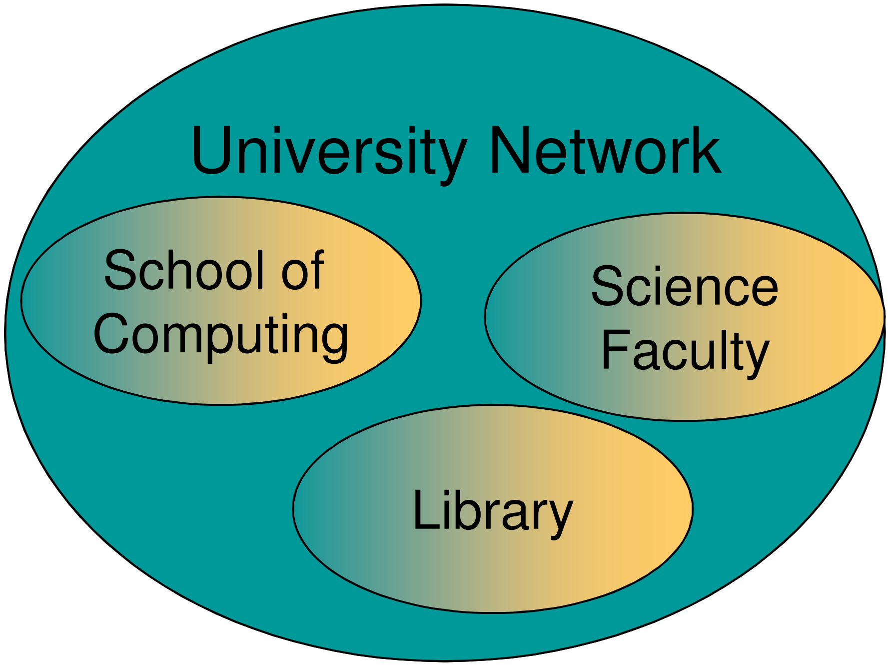
- **Example**: www.cmb.ac.lk

192.248.16	89

- Network address is: **192.248.16.0 (or 192.248.16)**
- Host number is: **89**
- Netmask is: **255.255.255.0** (or **ffffff00)**
- Prefix or CIDR notation: **192.248.16.89/24**
  - » Network prefix is 24 bits long

3.1.4 Subnetting

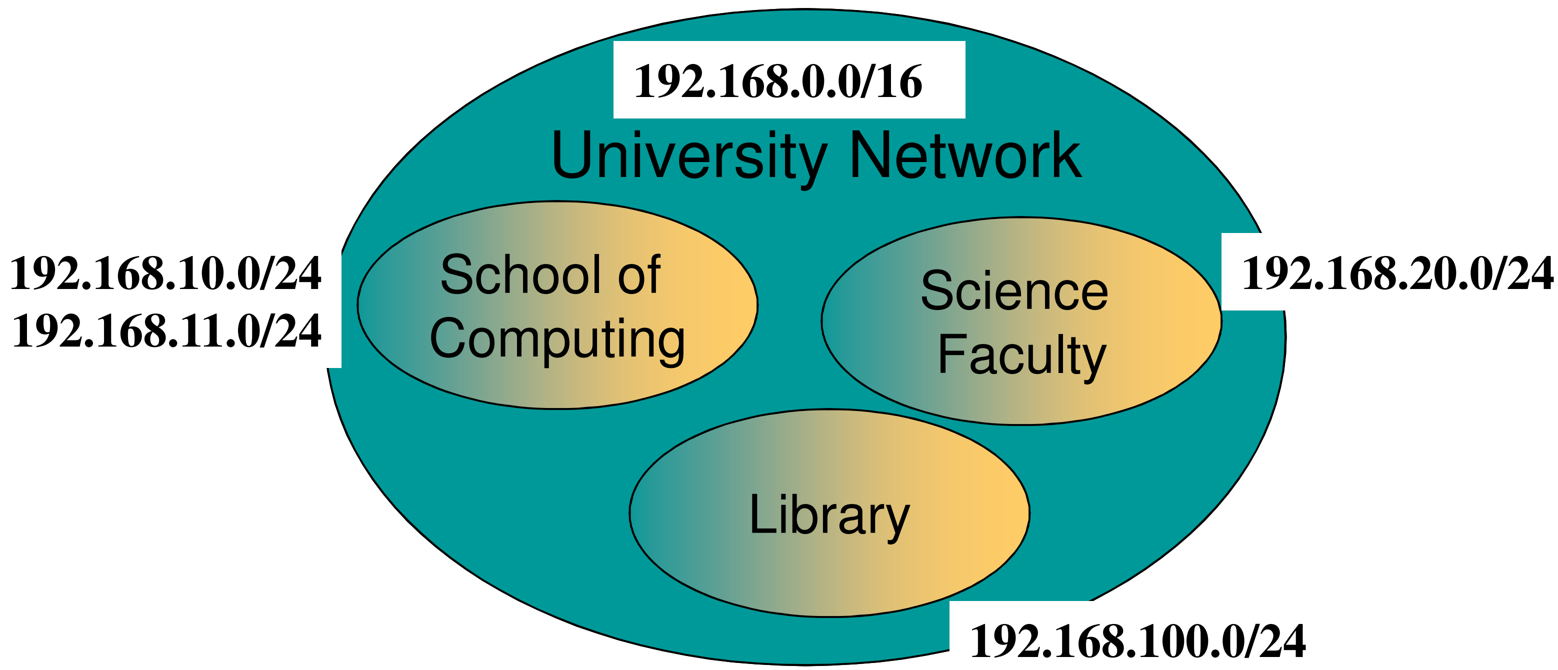
- **Problem**: Organizations have multiple networks which are independently managed
  - **Solution 1:** Allocate a separate network address for each network
    - Difficult to manage
    - From the outside of the organization, each network must be addressable.
  - **Solution 2:** Add another level of hierarchy to the IP addressing structure



→ **Subnetting**

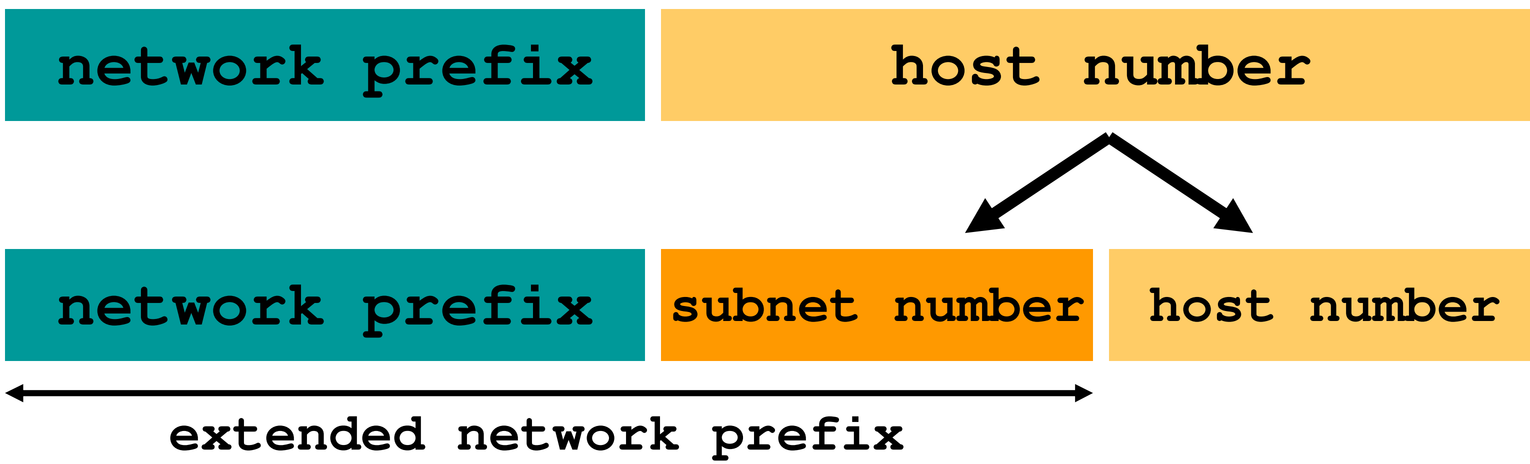
Address assignment with subnetting

- Each part of the organization is allocated a range of IP addresses (subnets or subnetworks)
- Addresses in each subnet can be administered locally



Basic Idea of Subnetting

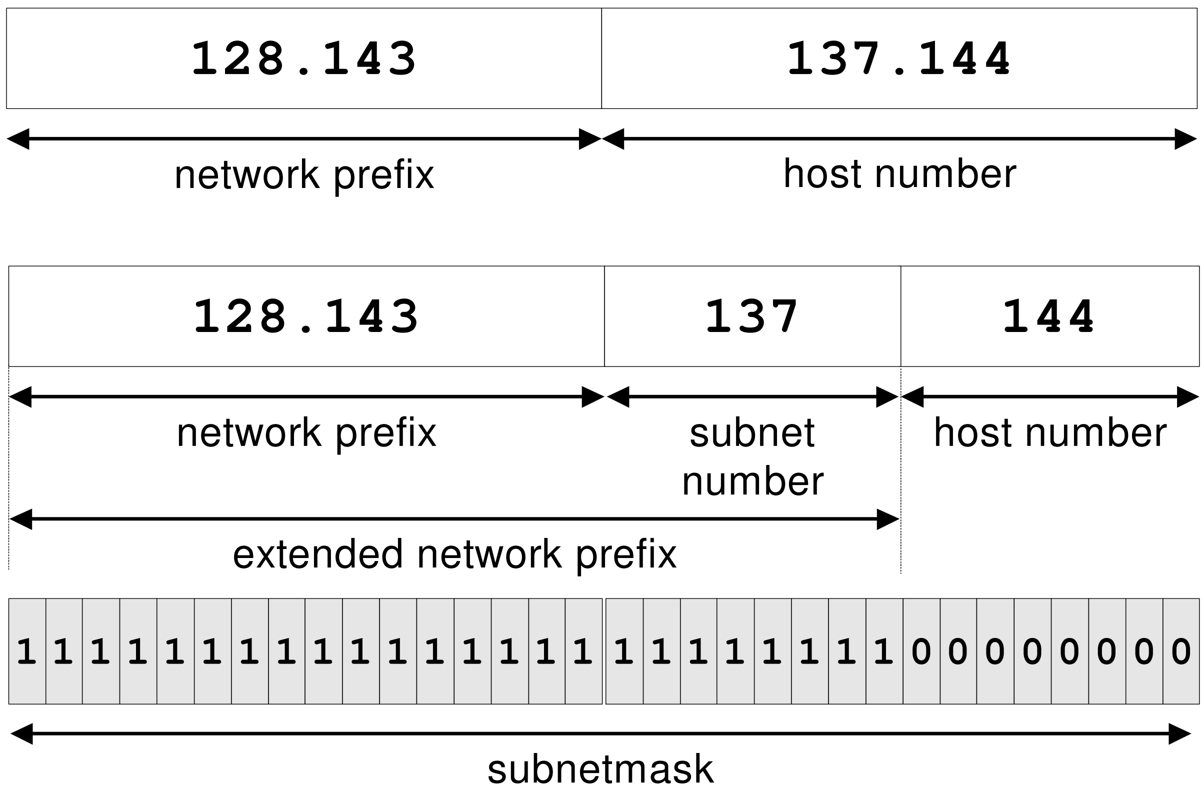
- Split the host number portion of an IP address into a **subnet number** and a (smaller) **host number**.
- Result is a 3-layer hierarchy



- Then:
  - Subnets can be freely assigned within the organization
  - Internally, subnets are treated as separate networks
  - Subnet structure is not visible outside the organization

Subnetmask

- Routers and hosts use an **extended network prefix (subnetmask)** to identify the start of the host numbers



Advantages of Subnetting

- With subnetting, IP addresses use a 3-layer hierarchy:
  - Network
  - Subnet
  - Host
- Reduces router complexity. Since external routers do not know about subnetting, the complexity of routing tables at external routers is reduced.
- Note: Length of the subnet mask need not be identical at all subnetworks.

Variable Length Subnet Masking (VLSM)

is the process by which we take a major network address and use different subnet masks at different points.

A fixed length mask has the advantage of simplicity. It will be easy for the network staff/users to remember the subnet mask. However, if we have to keep the subnet mask the same we encounter severe problems concerning addressing space.

Some useful tips on VLSM:

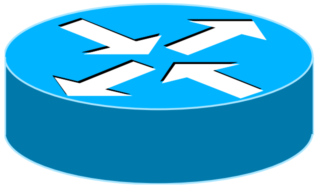
- Use as few different masks as possible
- Keep lookup table to figure out the masks for a given subnet
- Make sure not to overlap subnets with VLSM

When do we need to use different subnet masks?

Unicast & Multicast Routing

What is Routing?

- Finding a path between a source and destination (path determination)
- Moving information across an internetwork from a source to a destination (switching)
- Very complex in large networks because of the many potential intermediate nodes.



- Delivery models in which a source sends to a single destination (called **unicast),** to all destinations **(**called **broadcast),** and to a group of destinations (called **multicast**).

UCSC

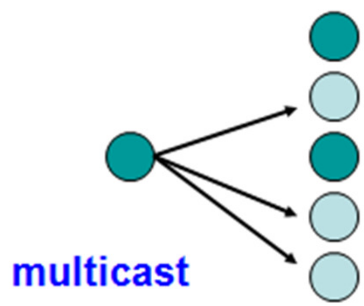
BIT

3.1.6 Multicast Routing

- Sending a message to a group of receivers is called **multicasting, and the routing algorithm** used is called **multicast routing algorithm.**
- each group is identified by a multicast address and routers know the groups to which they belong
- Ex:

  MOSPF (Multicast OSPF)

  DVMRP (Distance Vector Multicast Routing Protocol)



3.1.5 Unicast Routing

- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting.**
- unicast is a special case of multicast and source sends data to a single destination.