20MCA13-Computer Networks

UNIT 4-Network layer in the internet

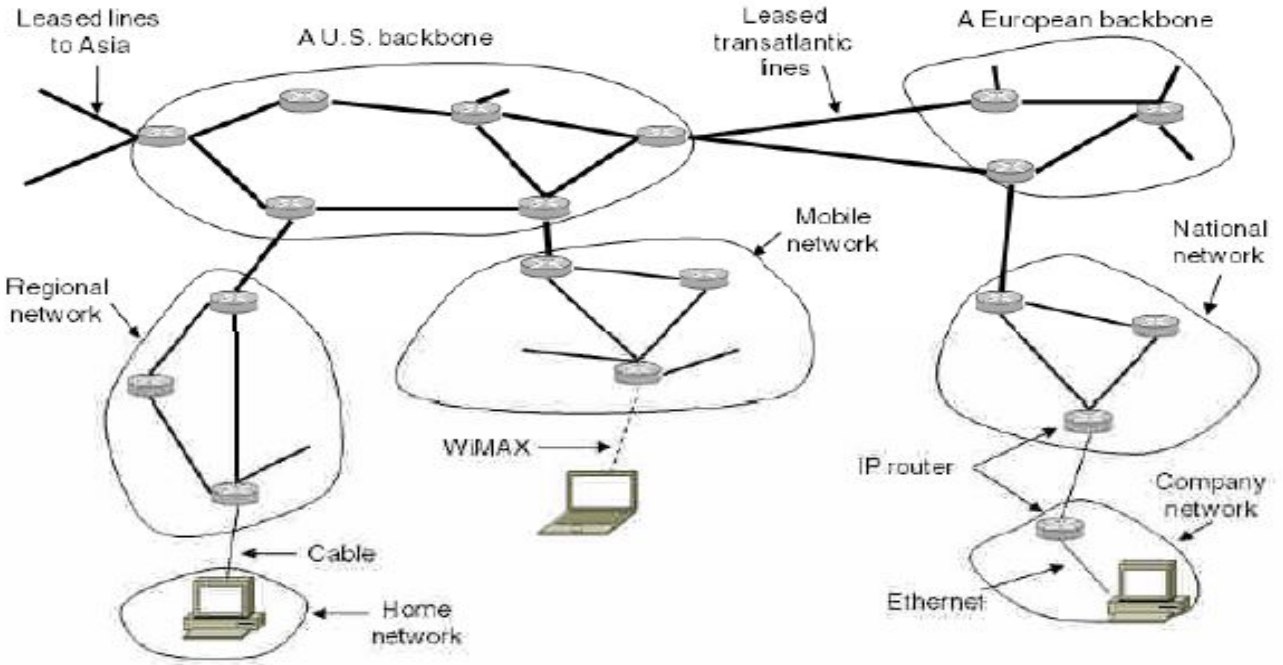
Network Layer Principles

1. Make sure it works
2. Keep it simple
3. Make clear choices
4. Exploit modularity
5. Expect heterogeneity
6. Avoid static options and parameters
7. Look for good design (not perfect)
8. Strict sending, tolerant receiving
9. Think about scalability
10. Consider performance and cost

Network layer in the Internet

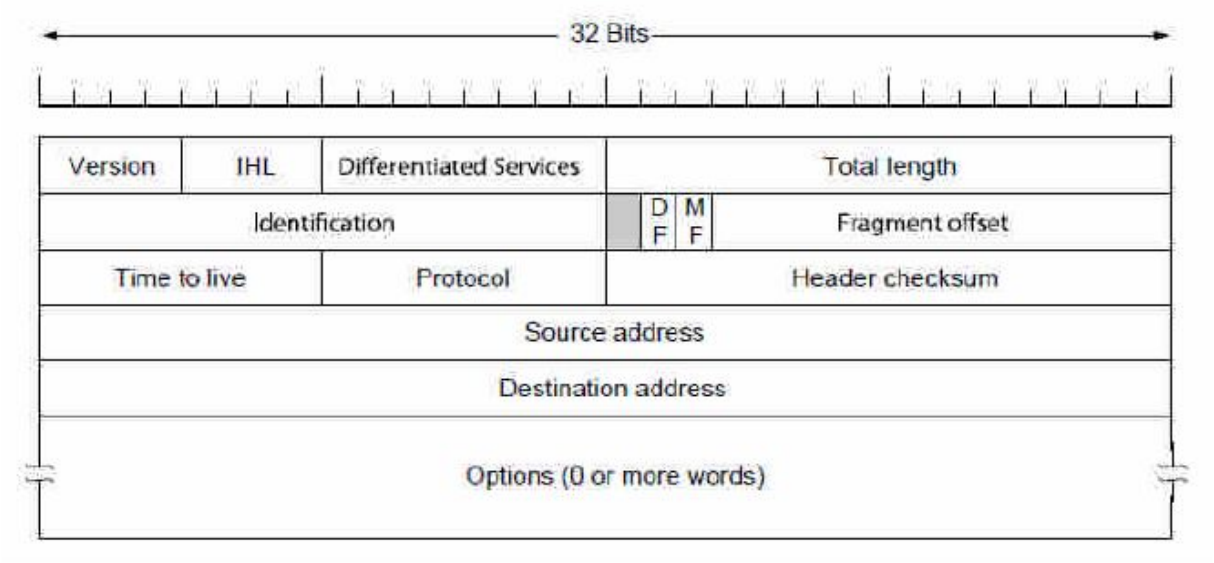
- The IP Version 4 Protocol
- IP Addresses
- IP Version 6
- Internet Control Protocols
- Label Switching and MPLS
- OSPF—An Interior Gateway Routing Protocol
- BGP—The Exterior Gateway Routing Protocol
- Internet Multicasting
- Mobile IP

- The Internet can be viewed as a collection of networks or ASes that are interconnected.
    - Tier 1 networks: the biggest of the backbones
- IP is the network layer protocol for internetworking
    - Best-effort service



The Internet is an interconnected collection of many networks.

The IP Version 4 Protocol (1)



The IPv4 (Internet Protocol) header.

- An IP datagram consists of a header part and a body or *payload part.*
  - The header has a 20-byte fixed part and a variable length optional part.
  - Transmitted in big endian: from left to right, with the high-order bit of the *Version field going first.*
    - The *Version field keeps track of which version of the protocol the* datagram belongs to.
    - The IHL field tells how long the header is, in 32-bit words.
      - The minimum value is 5 when no options are present.
      - The maximum value is 15, which limits the header to 60 bytes, and thus the options field to 40 bytes.
- The *Differential services(called Type of Service originally)* field was and is still intended to distinguish between different classes of services. The remaining are 2 unused bits.
  - Originally the 6-bit field contained, from left to right, a three-bit *Precedence field and three flags, D,T and R.*
    -

The three flag bits allow the host to specify what it cares most about from the set {Delay,Throughput, Reliability}.

– In practice, current routers ignore the *Type of Service field altogether.*

• IETF changes the field slightly to accommodate differentiated services.

– Top 6 bits are used to indicate which of service classes each packet belongs to. These classes include four queueing priorities, three discard probabilities, and the historical classes.

– The bottom 2 bits are used to carry explicit congestion notification (ECN).

– The *Total length includes everything in the datagram-both* header and data, with a maximum length 65535 bytes.

- *Identification field* determines which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same ID value.
  – An unused bit and two 1-bit fields
- DF stands for ``Don't fragment."
- *MF stands for ``More fragments" All fragments except the last one have this bit set*
- *Fragment offset tells where in the current datagram* this fragment belongs
  • All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit.
  • Since 13 bits are provided, a maximum of 8192 fragments per datagram, giving a maximum datagram length 65536 bytes, one more than the *Total length field.*

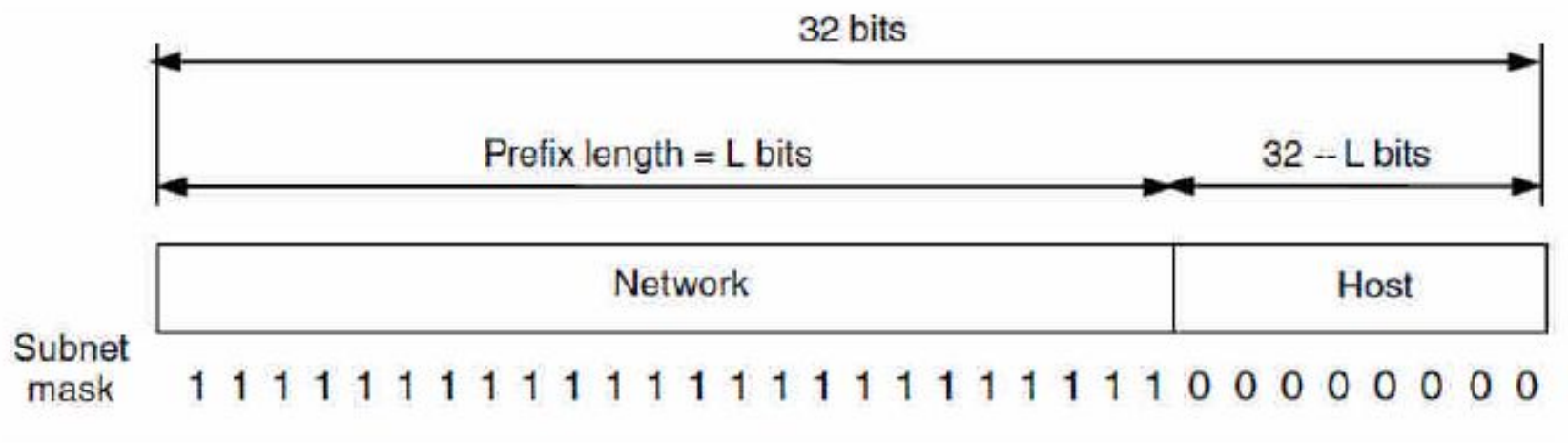
- *Time to live(TtL) field is a counter used to limit packet lifetimes*
    - •supposed to count time in seconds
    - •counts hops and as it hits zero, the packet is discarded

      and a warning packet is sent back to the source host
- *Protocol field tells the network layer which transport process to* give it to
    - • TCP, UDP, and some others (RFC 1700, www.iana.org)
- *Header checksum verifies the header only*
    - • recomputed at each hop, as at least one field always changes (the *Time to live field)*

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Some of the IP options.

IP Addresses



- Hierarchical addresses, unlike Ethernet address
  - Written in dotted decimal notation, like 140.122.185.141
  - Prefixes are written by given the lowest IP address in the block and the size of the block.
    - The size is determined by the number of bits in the network portion.
    - E.g., 128.208.0.0/24
  - **Subnet mask**
    - The length of the prefix corresponds to a binary mask of 1s in the network portion.
  - Advantage: Routers can forward packets based only the network portion of the addresses.
  - Disadvantage:
    - The IP address of a host depends on *where it is located in the* network.
    - Wasteful of addresses.

- Subnet
  - Split a block of addresses into several parts for internal use as multiple networks.

E.g.

- Computer Science (a/17): 10000000 11010000 1|xxxxxxx xxxxxxxx
- Electrical Eng.(a/18) : 10000000 11010000 00|xxxxxx xxxxxxxx

CIDR –Classless InterDomain Routing

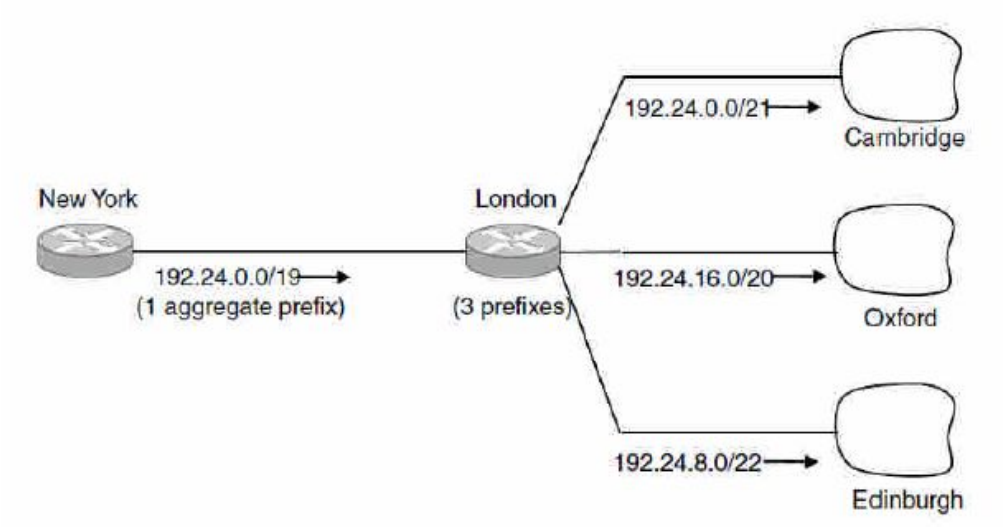
- A single routing table for all networks consisting of an array of *(IP address, subnet mask, outgoing line) triples.*
  – When a packet comes in, its destination IP address is first extracted.
  – The routing table is scanned entry by entry, masking the destination address and comparing it to the table entry looking for a match.
- multiple entries with different subnet mask lengths match, in which case the longest mask (the **longest matching prefix** or the most specific route) is used.
- Routing table explosion issues, particularly for routers in the ISPs and backbones (in the **default-free zone)**
  – Solution: **Route aggregation by combining multiple small prefixes** into a single larger prefix.
- The resulting larger prefix is sometimes called a **supernet.**
- **Aggregation is heavily used throughout the Internet to** reduce the size of routing tables.

IP Addresses (3)

University	First address	Last address	How many	Prefix
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

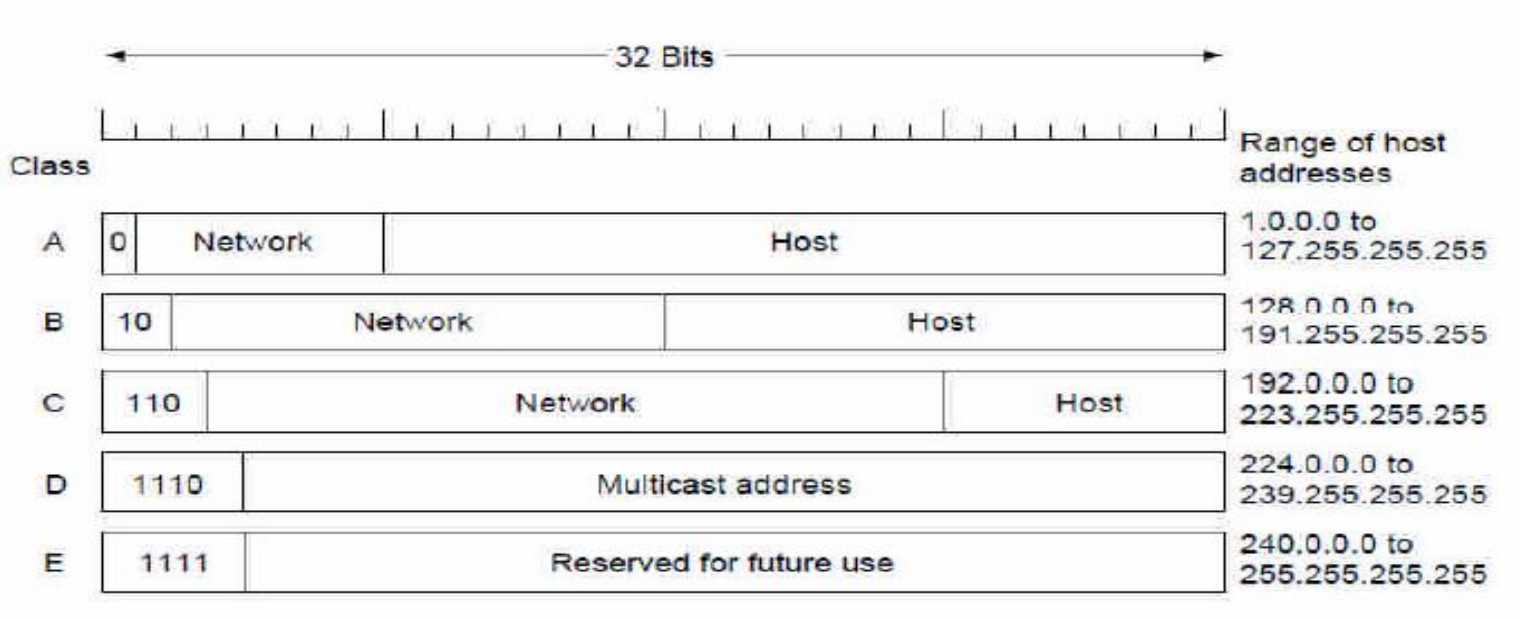
A set of IP address assignments

IP Addresses (4)



Aggregation of IP prefixes

IP Addresses (6)



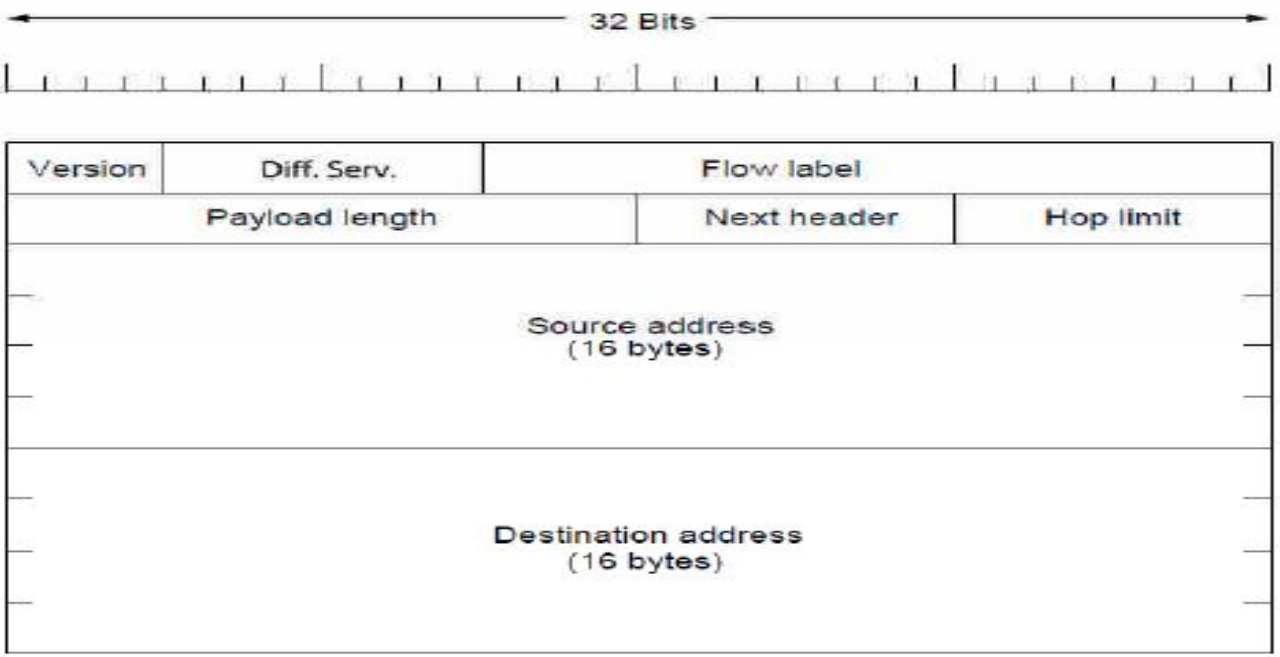
IP address formats

- To resolve issues on IPv4 address shortage:
  - Dynamic assignment
  - Feasible for dial up networking and mobile terminals
  - Impractical for business customers
  - NAT (Network Address Translation, described in RFC 3022) and private IP address
  - Replace by IPv6

IP Version 6 Goals

- Support billions of hosts
- Reduce routing table size
- Simplify protocol
- Better security
- Attention to type of service
- Aid multicasting
- Roaming host without changing address
- Allow future protocol evolution
- Permit coexistence of old, new protocols. . .

IP Version 6 (1)



The IPv6 fixed header (required).

- Compare the IPv4 header with the IPv6 header:
  – The *IHL field is gone because the IPv6 has a fixed* length
  – The *Protocol field was taken out because the Next* header field tells what follows the last IP header.
  – All the fields relating to fragmentation were removed because IPv6 takes a different approach to fragmentation
- All IPv6 conformant hosts and routers must support packets of 1280 bytes (a minimum).
  – When a host sends an IPv6 packet that is too large, the router that is unable to forward it drops the packet and sends back an error message
  Checksum field is gone.

Internet Control Protocols

– ICMP
    - The Internet Control Message Protocol
– ARP (NDP: Neighbor Discovery Protocol, for IPv6)
        - The Address Resolution Protocol
– DHCP
        - The Dynamic Host Configuration Protocol

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and Echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

The principal ICMP message types.

ARP

- Data link layer hardware does not understand Internet address.
  – LAN interface boards only understand LAN addresses.
- The Ethernet address has 48 bits.
  – How do IP addresses get mapped onto data link layer address?
- One solution is to have a configuration file somewhere in the system that maps IP addresses onto Ethernet address.
- A better solution is for a host to output a broadcast packet onto the Ethernet and to get a reply. The protocol for asking and getting a reply is called ARP.

- ARP is defined in RFC 826
- – The advantage of using ARP over configuration files is the simplicity
- – Some optimizations to make ARP more efficient:
    - It caches ARP results
    - Have the host which issues ARP requests include its IP to
- Ethernet mapping in the ARP packet.
    - Have every machine broadcast its mapping when it boots.
        – This broadcast is generally done in the form of an ARP looking for its own IP address known as a **gratuitous ARP.**
            » There should not be a response, but it makes an entry in everyone's ARP cache.
            » If a response does arrive, two machines have been assigned the same IP address.

DHCP

- Given an Ethernet address, what is the corresponding IP address?
  - DHCP (**Dynamic Host Configuration Protocol)**
- With DHCP, each network must have a DHCP server.
- Allow both *manual IP address assignment and automatic a*ssignment.
- DHCP, in RFCs 2131 and 2132
- Relay DHCP discover packets
  - To find its IP address, a newly-booted machine broadcasts a DHCP DISCOVER packet.

– If the DHCP server is not directly attached to the network, the router will be configured to receive DHCP broadcasts and relay them to the DHCP server.

– How long should an IP address be allocated?

  – A fixed period of time, by **IP leasing techniques with renewal.**