Network Level

Lenuta Alboaie
adria@info.uaic.ro

Content

- Network Level
  - IPv4 Problem
    - Context
    - Characteristics
    - Subnets
  - Private Networks
  - ICMP
  - Address Resolution
  - IPv6 - overview
    - Details -> Future Course

Context

- **Initial Situation**

Before the Internet, only nodes from the same network could communicate with each other

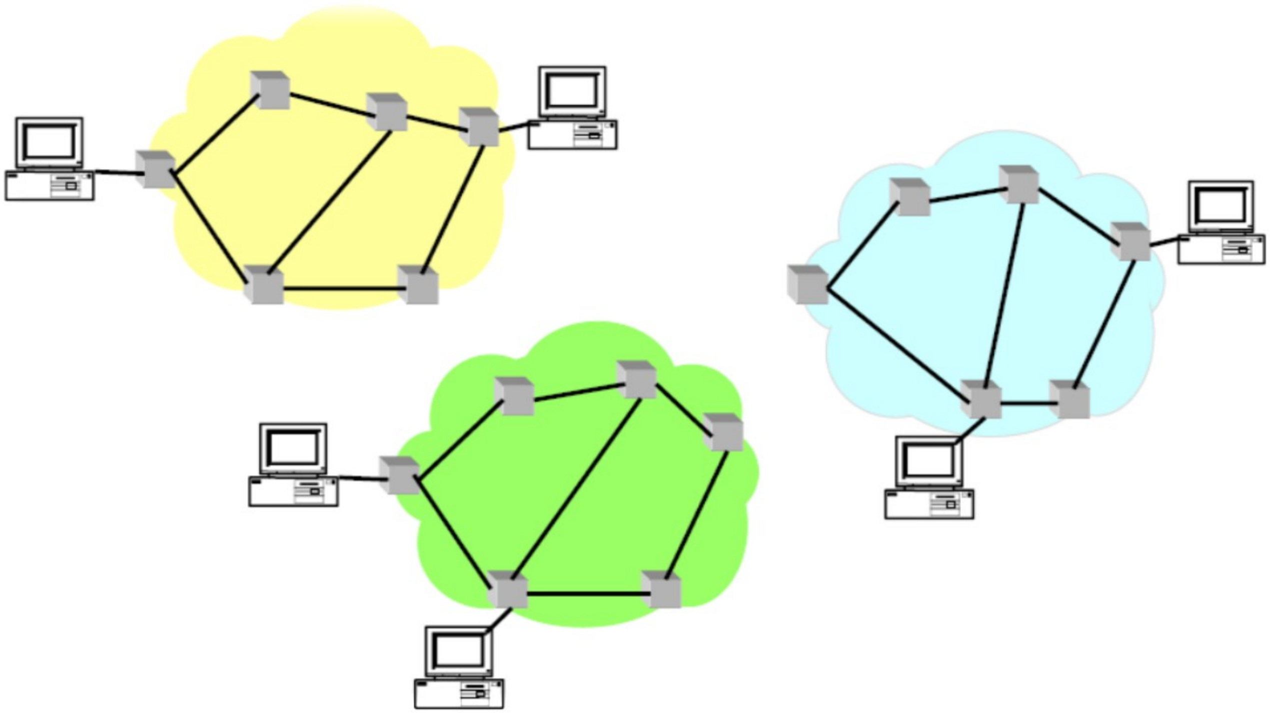
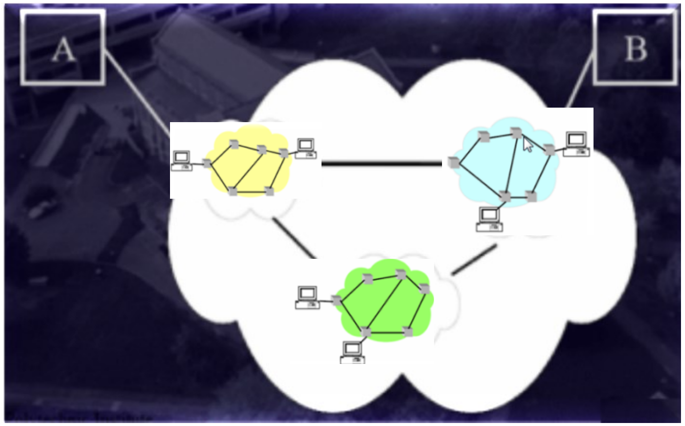


Figure: Individual Network

Considerations

- Problem
  - How to carry packages in a heterogeneous environment?

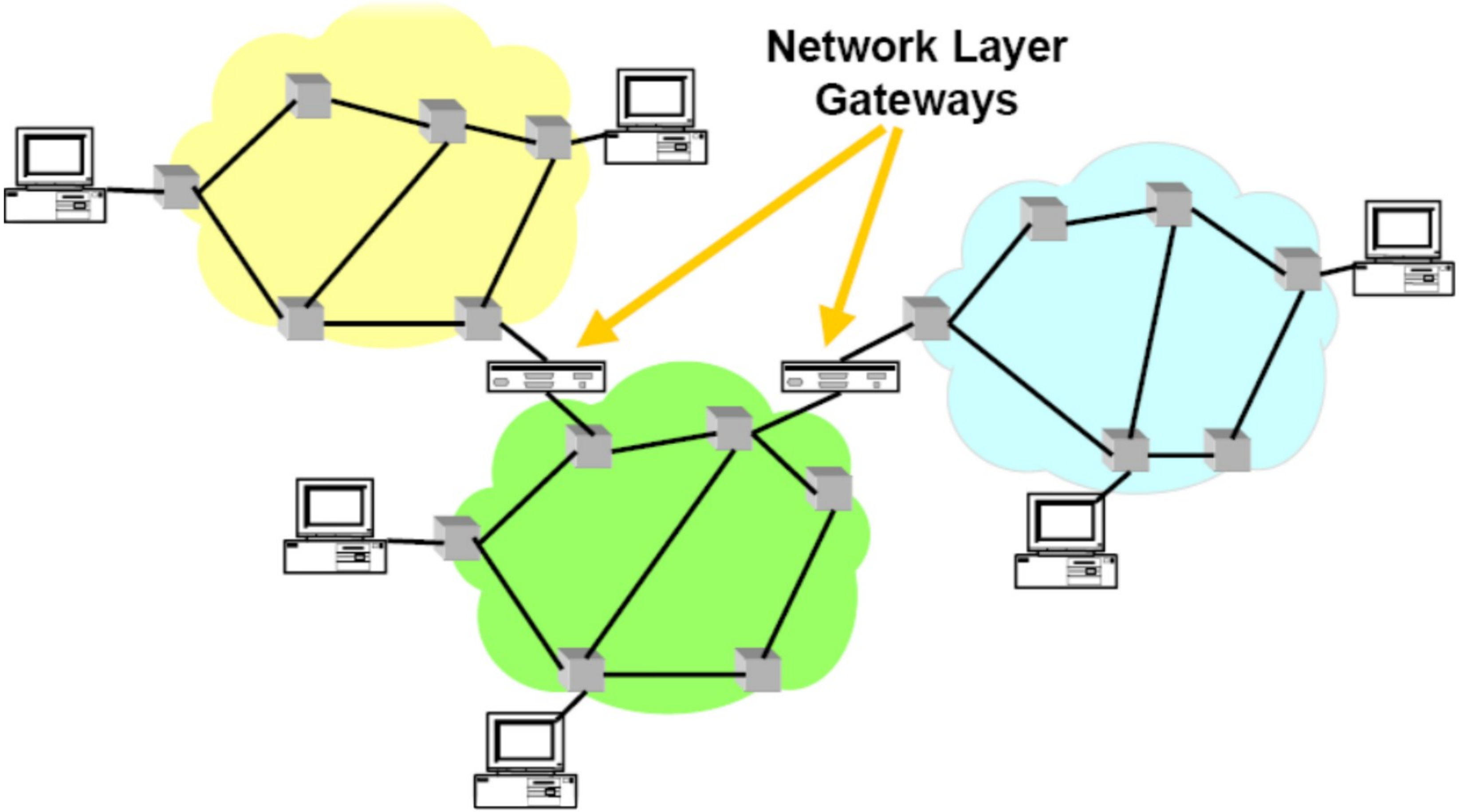


- **Heterogeneity**
  - At lower levels: how to make the interconnection of a large number of independent networks?
  - At higher levels: how to provide support for a wide variety of applications?

- **Scaling:** how could we handle a large number of nodes and applications in such a system of interconnected networks?

Solution

- **IP – Internet Protocol**



Network Level

- IP protocol is used for autonomous systems (AS - Autonomous Systems) in order to interconnect

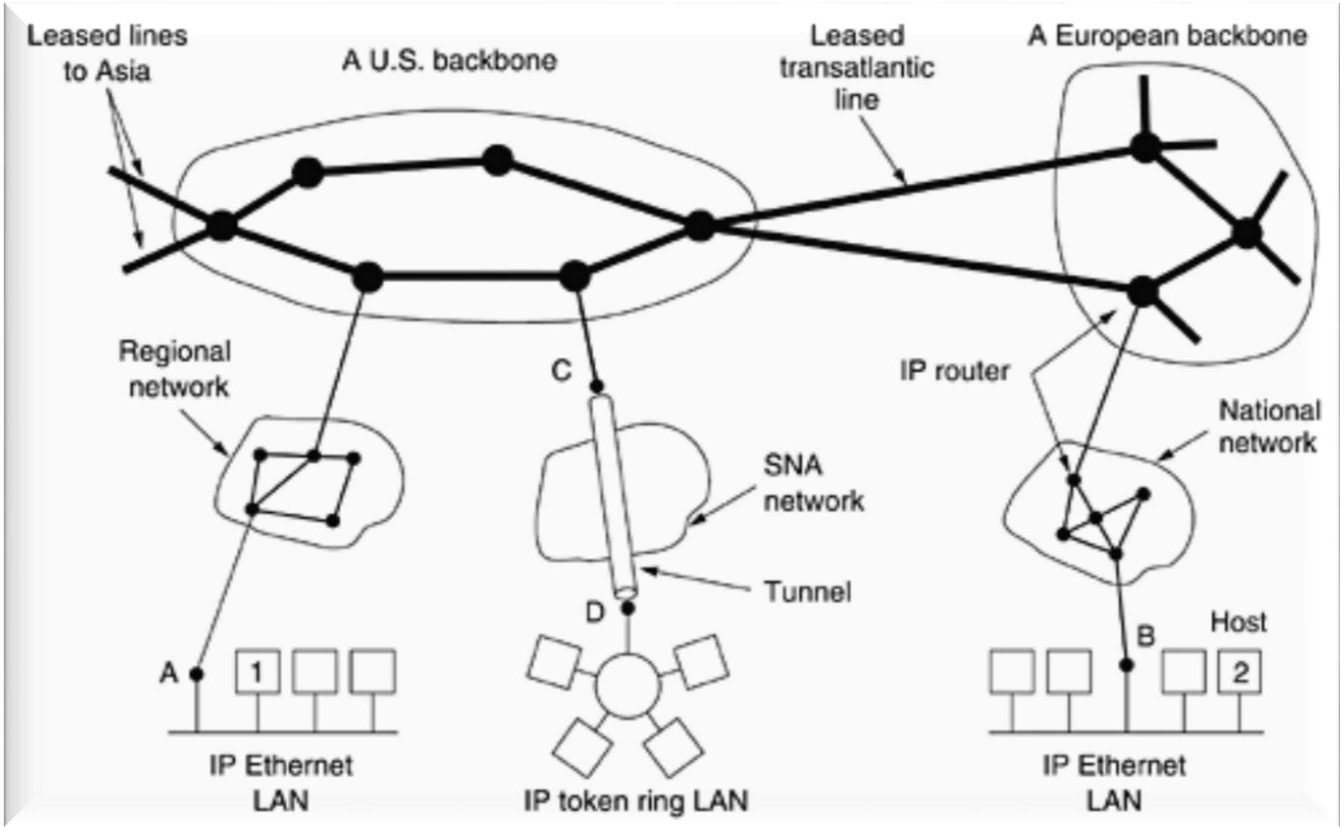


Figure: Internet - collection of interconnected networks

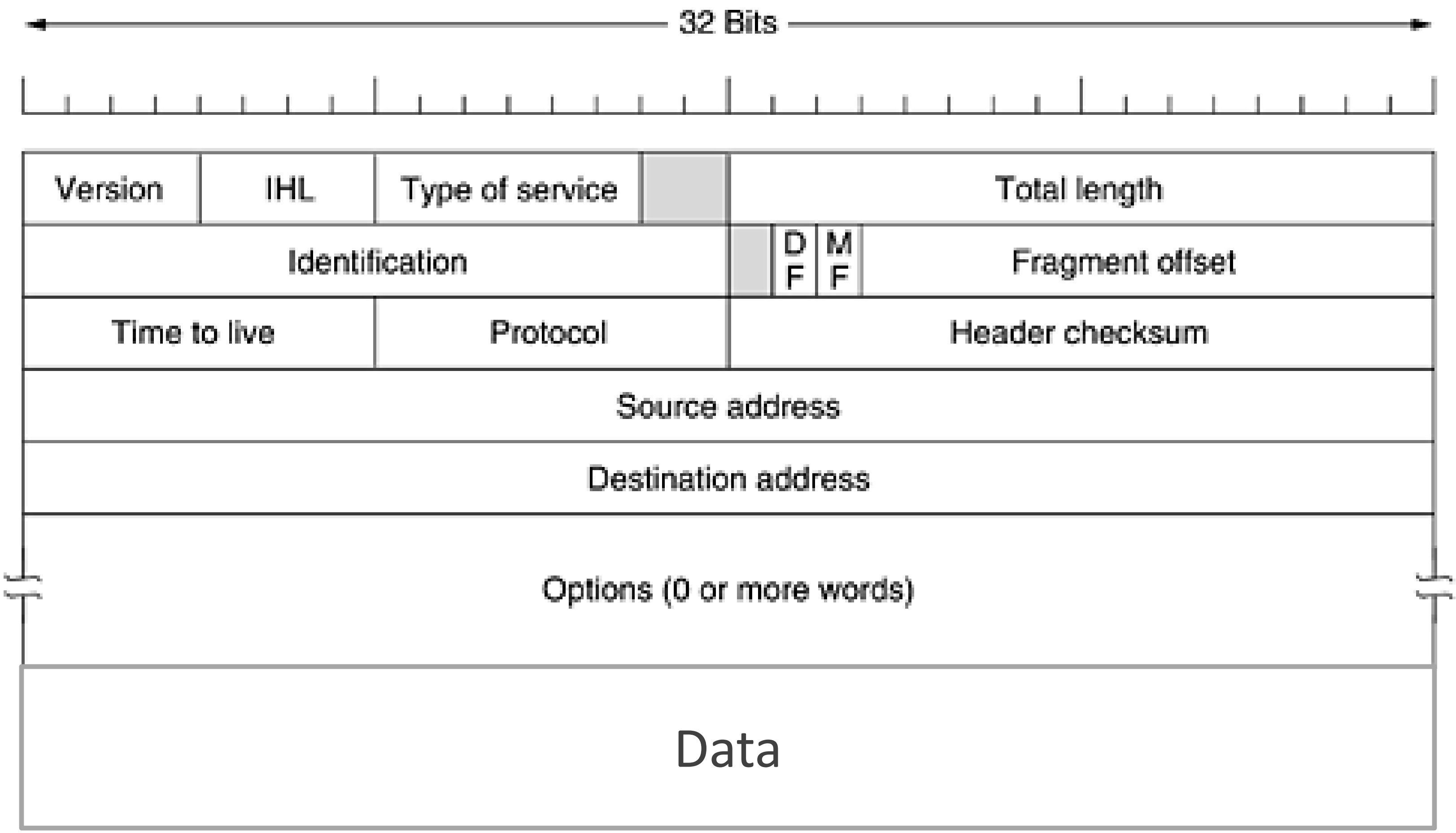
[Computer Networks, 2003 Andrew S. Tanenbaum]

Network Level

- Role: offers connectionless services to transport **datagrams** from source to destination; source and destination can be in different networks
- Each datagram is independent from the others
- This level does not guarantee the right transmission (loss, multiplier,…)
- +…Future Course

IP Protocol

- **IPv4 Datagram**



[Computer Networks, 2003
Andrew S. Tanenbaum]

IP Protocol

- **IPv4 Datagram**
  - Common values for *Version* field are:
    - 4 – IP Protocol (RFC 791)

    (6 for IPv6 protocol (RFC 1883))

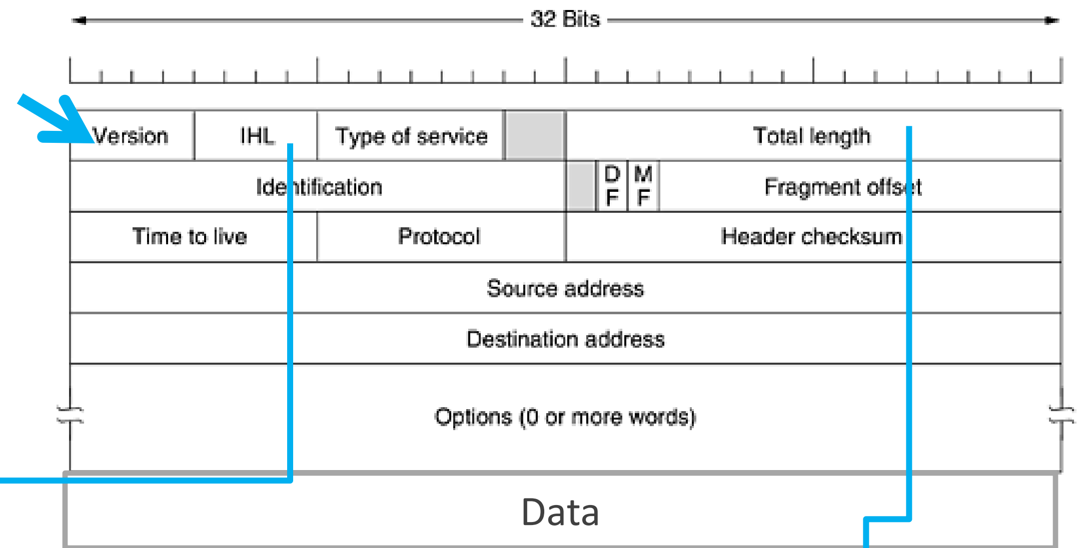


Figure: IPv4 Datagram

Specify the datagram header length

Specify the size of the entire datagram

IP Protocol

- **IPv4 Datagram**
  - *Type of service* *the* field allows the host to communicate to the subnet (e.g. routers) what type of service is desired

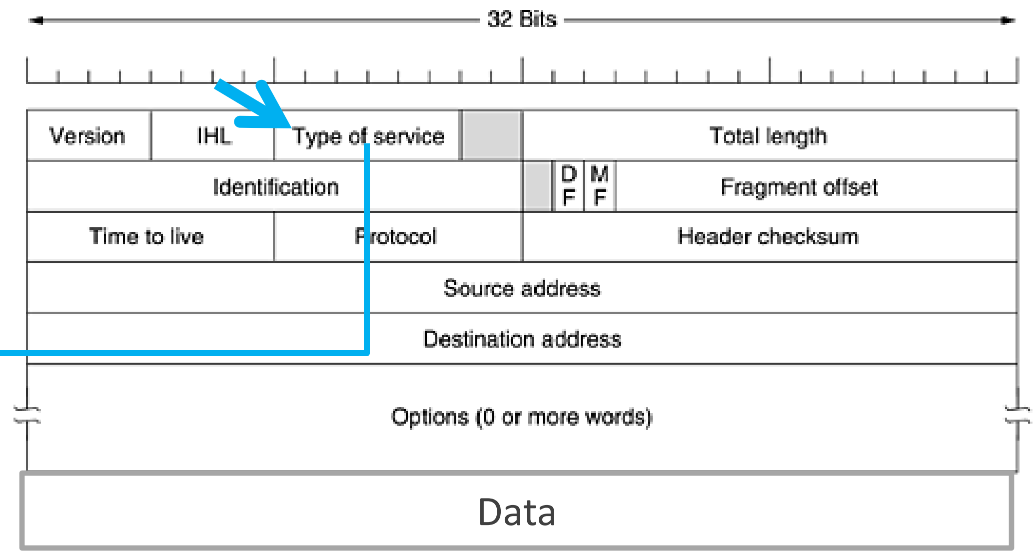


Figure: IPv4 Datagram

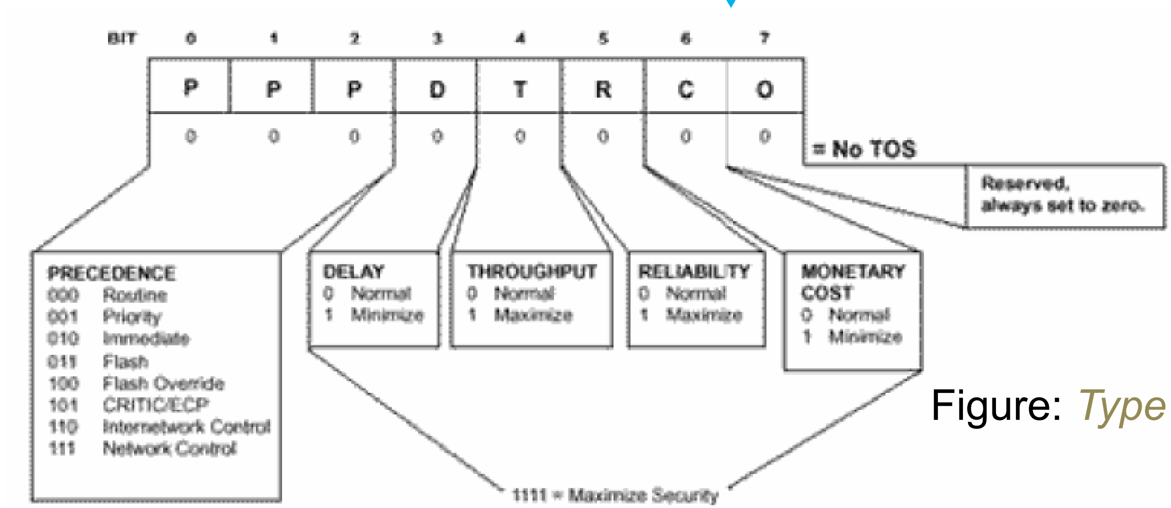
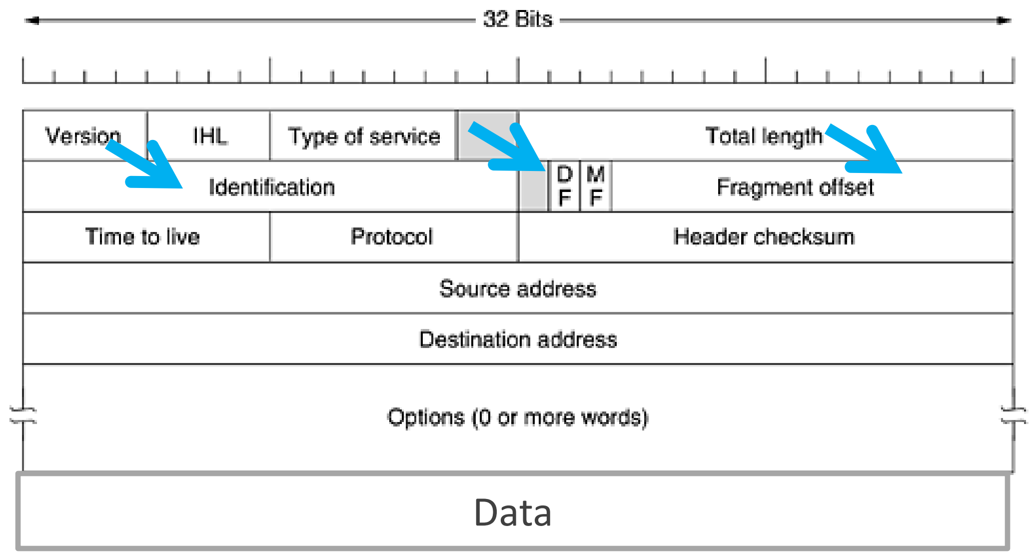


Figure: *Type of Service* Field

IP Protocol

- **IPv4 Datagram**
  - *Identification* field allows the host to identify if the received segment is part of one datagram

Figure: IPv4 Datagram



- Flags:
  - *DF (Don't Fragment)* – rooters can't fragment the indicated datagram
  - *MF (More Fragments)* – signals that the packet is a fragment, followed by others; last fragment has this bit 0
- *Fragment offset* field - represents the fragment placed in a datagram

IP Protocol

- **IP Datagram**
  - Datagram's Fragmentation:
    - Each fragment has the same structure as the IP datagram
    - Reassembly of datagrams is performed by the receiver
    - If a fragment of a datagram is lost, the datagram is destroyed (an ICMP - Internet Control Message Protocol message is sent to the sender)
    - Fragmentation mechanism has been used for some attacks - *firewall piercing* (a "special“ fragment is considered as part of a connection already established, so that it can pass through a firewall)

IP Protocol

- **IP Datagram**
  - Datagram Filtering:
    - It is accomplished by a *firewall*: it allows access from the outside in the internal network, according to some policy, certain types of packets ((used by certain protocols / services)
      - Forestall a series of attacks regarding security
      - The firewall can be software or hardware
      - The firewall can function as a proxy or a gateway

IP Protocol

- **Proxy- role and architecture:**
  - Indirect access to other networks (Internet) to hosts on the local network (via *proxy*)
  - The proxy allows an Internet connection sharing
  - The *proxy* can be software or hardware
  - May play roles such us: *firewall* or *cache server*
  - Used to improve the performance (e.g., caching, flow control), filtering messages, ensuring anonymity

IP Protocol

- **IPv4 Datagram**
  - *TTL (Time to Live)* field specifies the lifetime of the package;

  the number is decremented by every router through which the packet passes

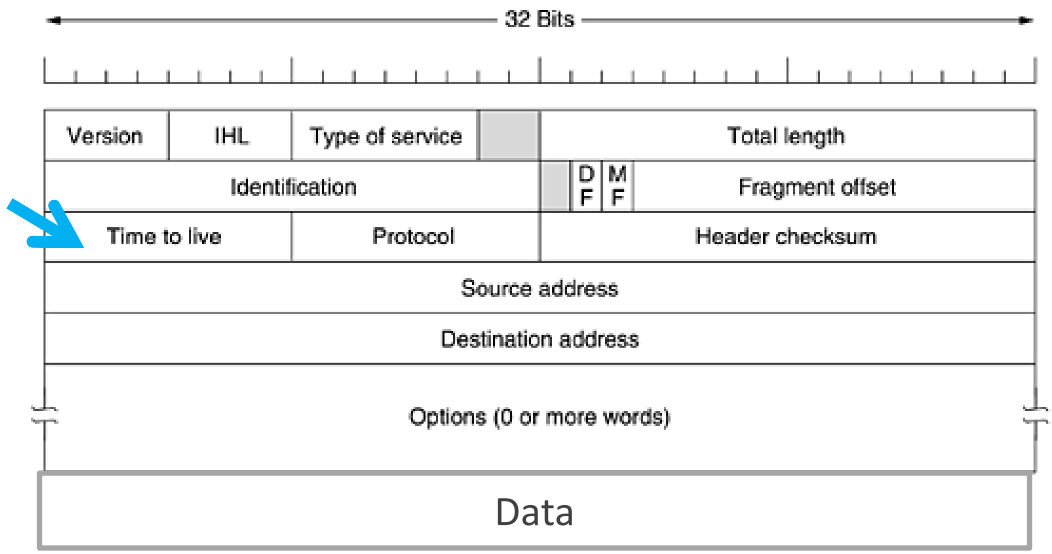
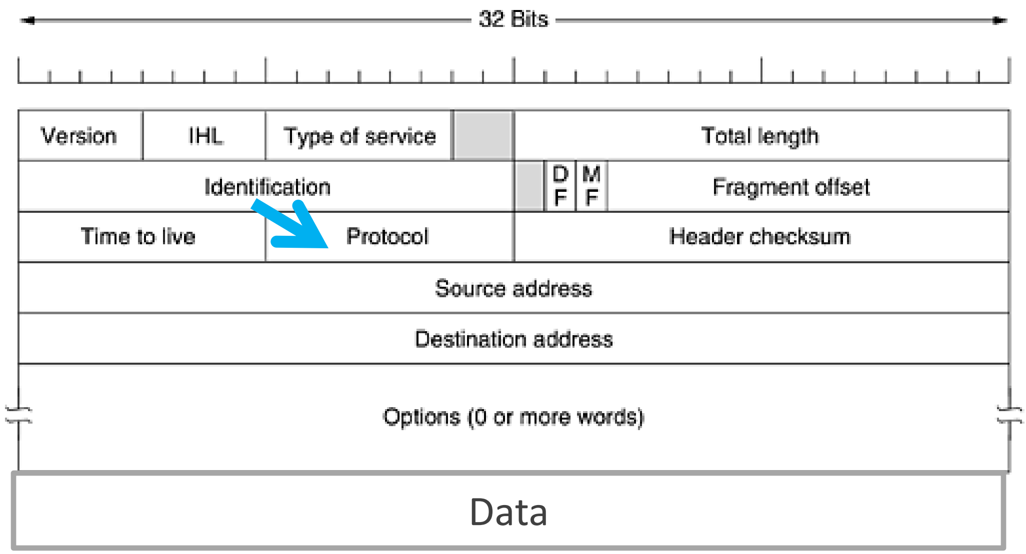


Figure: IPv4 Datagram

IP Protocol

- **IPv4 Datagram**
  - *Protocol* field specifies the protocol (from the superior level) intended to process the datagram

Figure: IPv4 Datagram

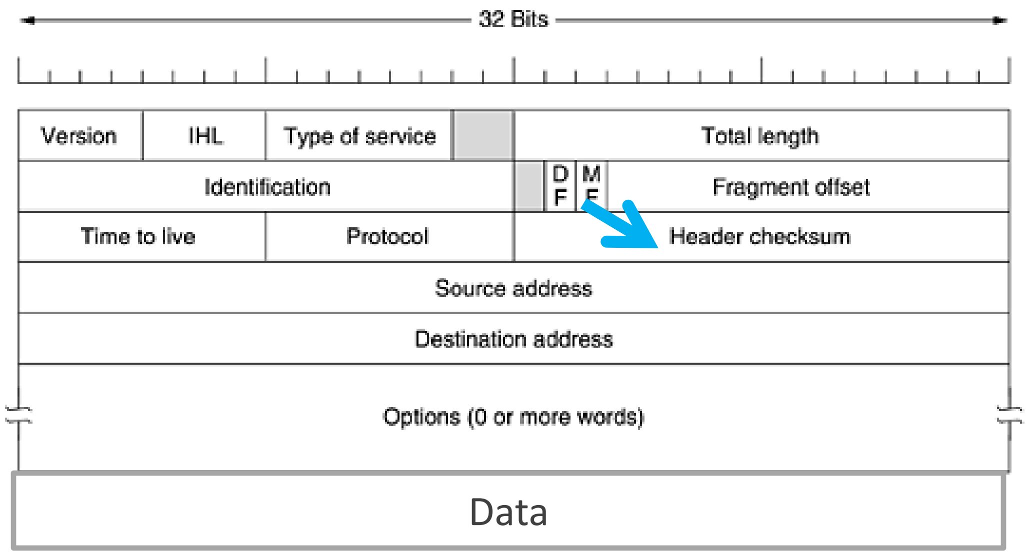


- 1 ICMP (*Internet Control Message Protocol*)
- 2 IGMP (*Internet Group Message Protocol*)
- 6 TCP (*Transmission Control Protocol*)
- 17 UDP (*User Datagram Protocol*)
- … etc.(RFC 1700)

IP Protocol

- **IPv4 Datagram**
  - *Header checksum field* used for detection; if an error occurs the datagram is destroyed

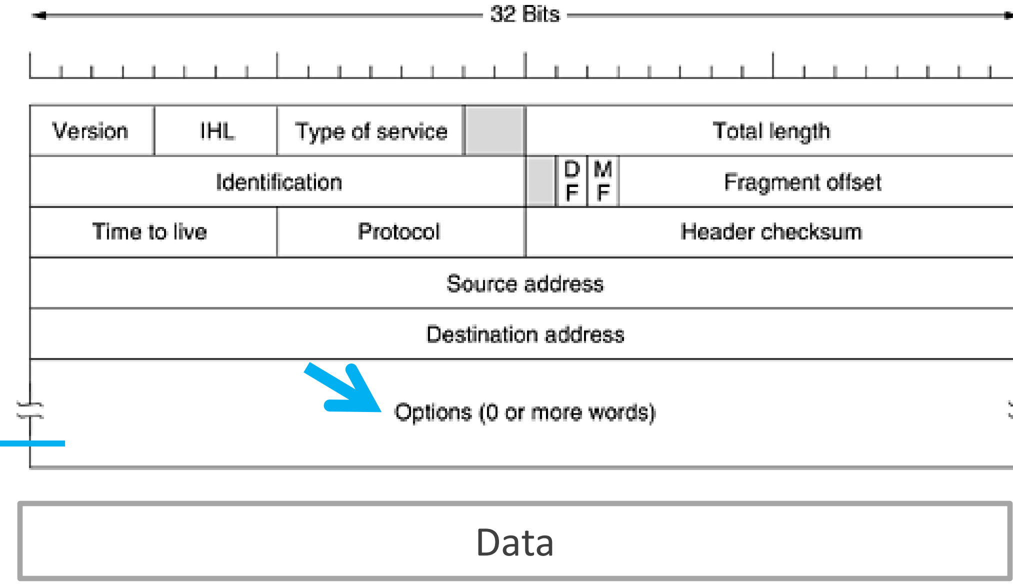
Figure: IPv4 Datagram



IP Protocol

- **IPv4 Datagram**
  - *Options* Field

Figure: IPv4 Datagram



Options	Details
Security	Mention if the datagram is a “secret” one
Strict source routing	Show full path to go
Loose source routing	Indicates a list of routers that should not be skipped
Record route	Each rooter adds its own IP
Timestamp	Each rooter adds its own IP and a timestamp

IP Protocol

- **IPv4 Datagram**
  - *Source address* and *Destination address* fields indicate the source address and the destination address

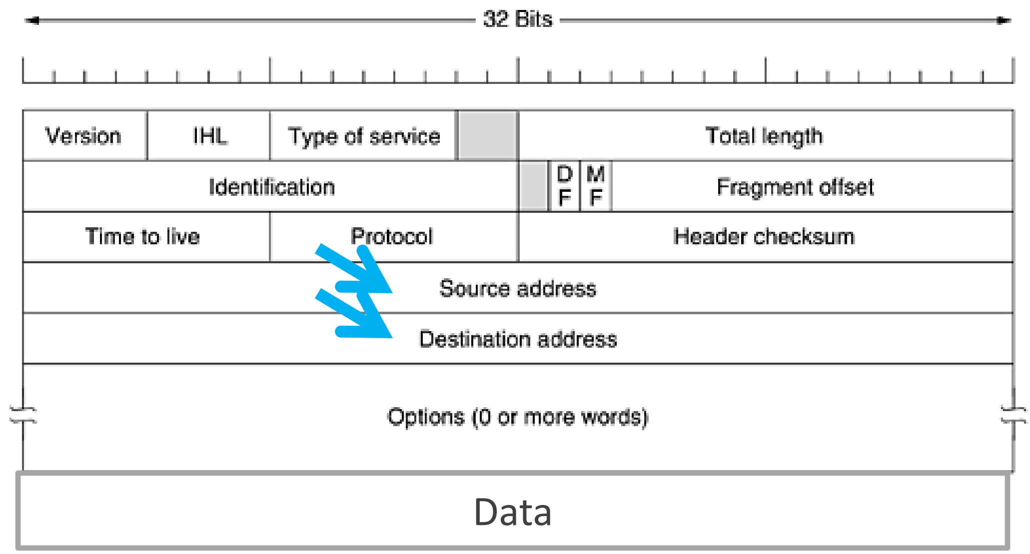


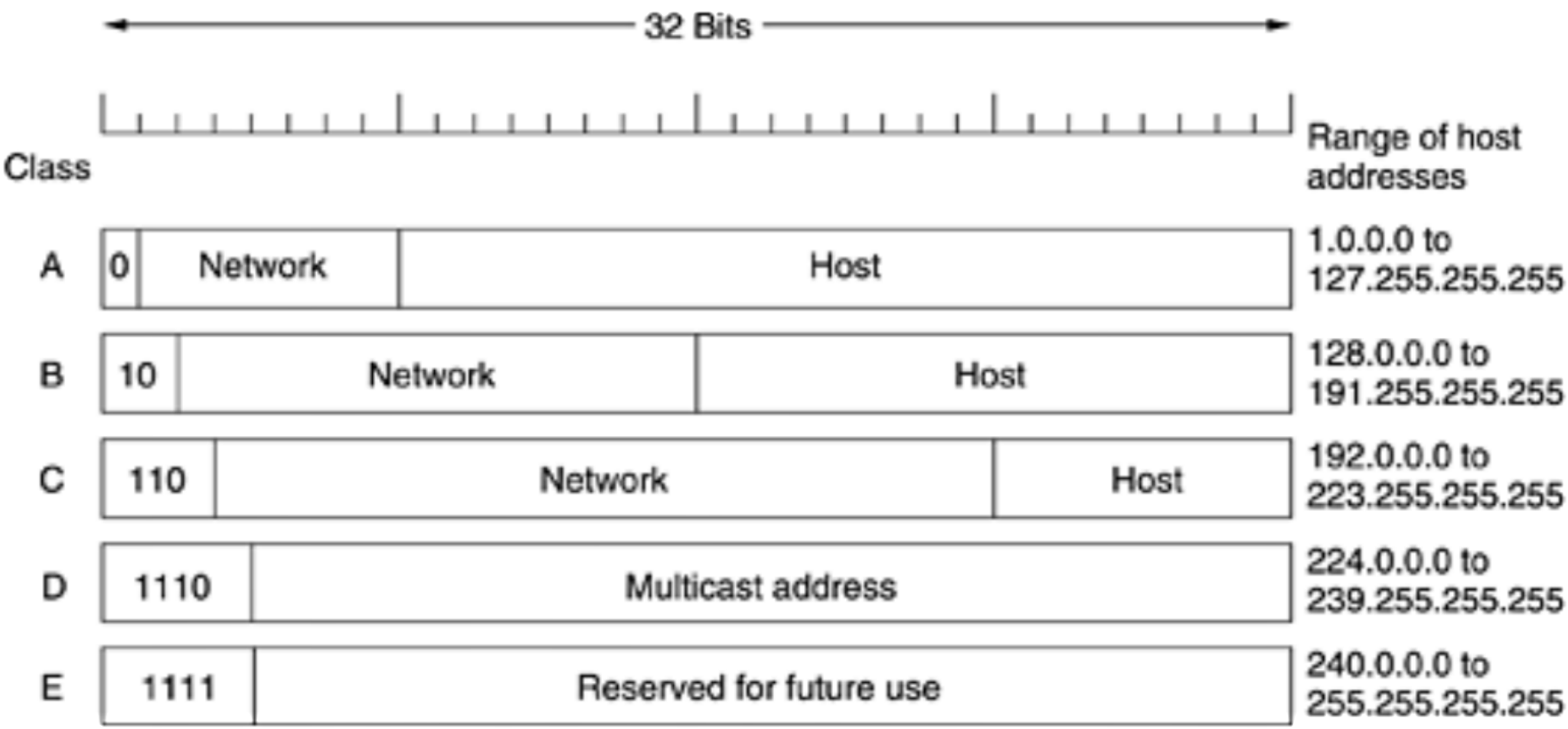
Figure: IPv4 Datagram

IP Protocol

- **IPv4 Addresses**
  - Each IP address includes a network identifier(NetID) and a host identifier (HostID)
  - Each network interface has a single IPv4 address
  - An IPv4 address has a length of 32 bits
  - Initially (RFC 791) there was a division into network classes: A,B,C,D,E

IP Protocol

- **IPv4 Addresses**



[Computer Networks, 2003
Andrew S. Tanenbaum]

IP Protocol

- **IPv4 Addresses**
  - Class A: 128 possible networks, 2^{24} hosts/network
  - Class B: 2^{14} possible networks, 2^{16} hosts/network
  - Class C: over 2 million networks, 255 hosts/network
  - Network Identifier(NetID) is assigned by a central authority (NIC – *Network Information Center*)
  - Host Identifier(HostID) is assigned locally by a network administrator
  - Example: 85.122.23.145 – Class A (in decimal notation convention)

    0101 0101 0111 1010 0001 0111 1001 0001
  - For IPv6, hexadecimal representation is recommended

IP Protocol

- **IPv4 Addresses**
  - An interface network has assigned a unique IP address
  - A host can have multiple NICs, therefore it has multiple IP addresses
  - The hosts of the same network have the same network identifier (the same NetID)
  - *Broadcast* addresses have HostID's bites equaled to 1
  - The IP address in which all HostID's bites are 0 is called a network address – refers to the hole network
    - Example: 85.122.23.0 (ne*twork address* for a host such us 85.122.23.145 and 85.122.23.1)
  - 127.0.0.1 – *loopback* address (*localhost*)

IP Protocol

- **IPv4 Addresses**
  - From the address space, some addresses are reserved: (RFC 1918):
    - 0.0.0.0 – 0.255.255.255
    - 10.0.0.0 – 10.255.255.255 (private addresses)
    - 127.0.0.0 – 127.255.255.255 (*loopback* addresses)
    - 172.16.0.0 - 172.31.255.255 (private addresses)
    - 192.168.0.0 - 192.168.255.255 (private addresses)
  - Private addresses : addresses that are not accessible to the outside (the "real“Internet), but only in the organization's intranet

Private Networks

- Aspects:
  - The exponential growth of the hosts number
  - Not all hosts offer resources available on the Internet

  Solution: NAT (*Network Address Translation*) – RFC 3022, 4008
  - The private addresses can be reused (RFC 1918)
  - It is based on replacing the private IP address with a public IP address (*IP masquerading*)

Private Networks

- Functionality:

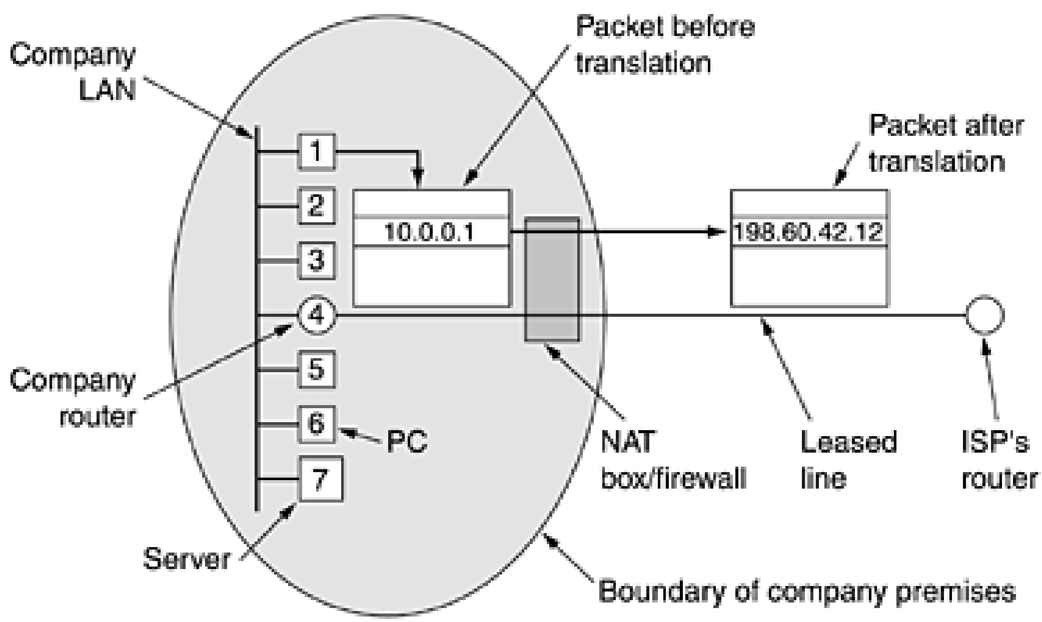


Figure: NAT mechanism

- Routers normally ignore datagrams containing private addresses => private IP addresses can be used in the organization's intranet
- Access to the outside (the "real“ Internet) is achieved via a gate (mediating gateway) that rewrites the source IP addresses / destination

[Computer Networks, 2003 Andrew S. Tanenbaum]

IP Protocol

- **Subnets using network masks**
  - It appeared as a solution to the problem of IP address space`s exhaustion
  - Simplify Routing
  - Subnets cannot be detected externally

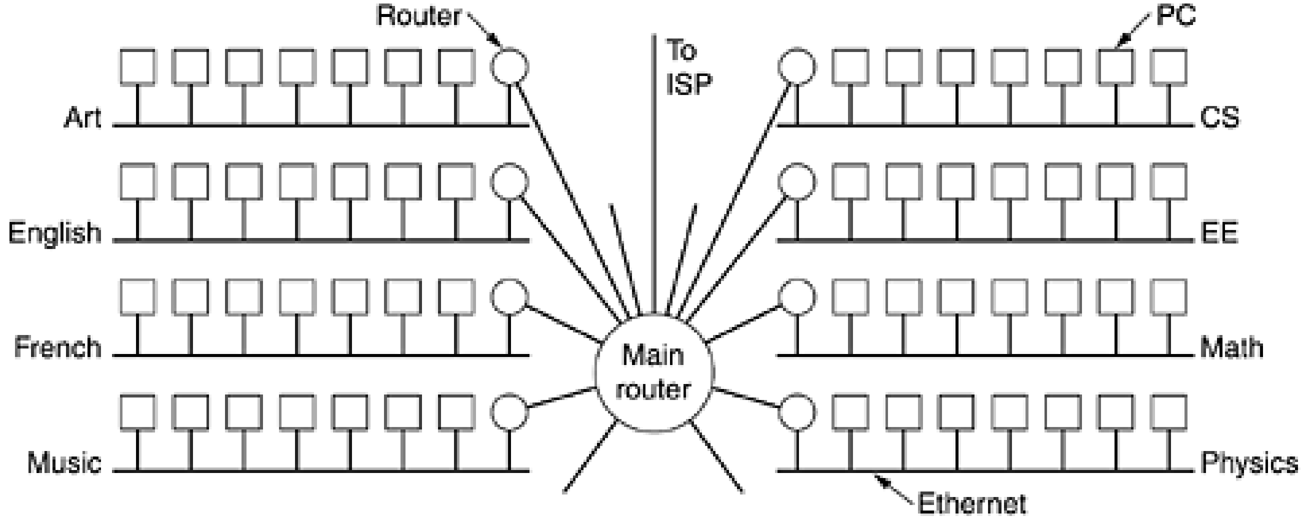
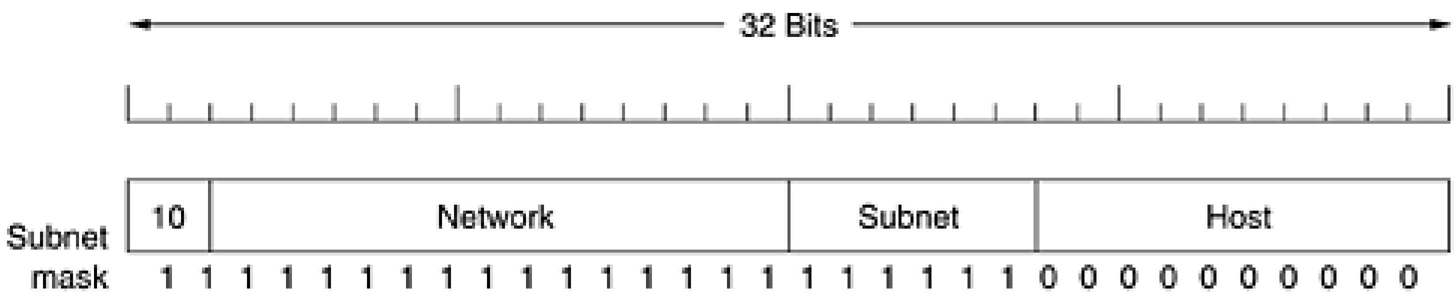


Figure: A campus network

IP Protocol

- **Subnets using network masks**
  - Division into subnetworks will be made via the network mask(*netmask*): NetID bits are 1, HostID bits are 0
  - Subnet identifier (SubnetID) is generally used to group computers based on physical topology



Example. One way to create a subnet in a B network

IP Protocol

- **Subnets using network masks**
  - Example:
    - Let’s consider the IP address: 160.0.6.7

      10100000 00000000 00000110 00000111
    - Network mask: 255.255.252.0

      11111111 11111111 11111100 00000000
    - Network address: 160.0.4.0

      10100000 00000000 00000100 00000000

  Network address = network mask AND IP address

- Default subnet masks:
  - 255.0.0.0 - Class A
  - 255.255.0.0 - Class B
  - 255.255.255.0 - Class C

IP Protocol

- **Convention mark**: x.x.x.x/m means that we apply an m bits mask to the IP specified x.x.x.x address
- Example:
  - 10.0.0.0/12 – it applies a 12-bits mask to 10.0.0.0 address, we select possible values for the last 20 bits (=32-12)
  - 85.122.16.0/20 – it applies a 20-bit mask to 85.122.16.0 address

Network Level

- Protocols
  - ICMP (RFC 792)
  - ARP (RFC 826)
  - RARP (RFC 903)
  - BOOTP (RFC 951,1048,1084)
  - DHCP
- From IPv4 to IPv6

ICMP Protocol

- **ICMP – Internet Control Message Protocol**
  - Used to exchange control messages
  - Use IP
  - ICMP messages are processed by the IP software, not by the user processes
  - Messages types

Message Type	Description
8 Echo Request	Ask if a host is active
0 Echo Replay	“Yes, I’m active”
3 Destination Unreachable	The package can’t be delivered (e.g. DF is set)
5 Redirect	The message is not correctly routed
11 Time Exceeded	Time elapsed (TTL=0) <- (e.g. loop, congestions, low values for time)
… etc (RFC 792)	http://www.iana.org/assignments/icmp-parameters

Protocolul ICMP

- Used by:
  - ping command (Packet Internet Gropher)
  - traceroute command
    - A package with TTL=1 (1 hop) is sent
    - The first router ignores the packet and sends back an ICMP message "*time-to-live exceeded*"
    - A package with TTL=2 is sent (2 hops)
    - The second router ignores the packet and sends back an ICMP message "*time-to-live exceeded*"
    - Repeat until it has received a response from the destination or has reached the maximum number of hops

Address resolution

- **IP addresses <-> hardware addresses (physical)**
  - The process of finding the hardware address of a host, knowing its IP address is called address resolution(*address resolution*) – ARP protocol (RFC 826)
    - ARP –broadcast protocol (each host receives a request for a physical address, and the answer is given by the one in question)
  - The process of finding the IP address based on the hardware address is called *reverse address resolution* –RARP Protocol (RFC 903)
    - Used to boot workstations without disks
    - BOOTP (RFC 951,1048,1084)
    - DHCP (*Dynamic Host Configuration Protocol*) RFC 2131,2132

IPv6

- Context:
  - Issues in IPv4 addresses world:
    - The exponential growth of the hosts` number
    - Very large routing tables
    - Complex configurations, more and more users (and increasing)
    - Failure to ensure QoS
  - Pressure from mobile operators

IPv6

- Objectives for a new protocol:
  - Support for billions of hosts
  - Reducing routing tables
  - Simplifying Protocol
  - Support for mobile hosts
  - Compatibility with the old IP
  - Support for future developments of the Internet
  - RFC 2460, 2553

IPv6

- 6 June 2012

IPv6

- Aspects:
  - IPv6 addresses are 16 bytes in length - 2^{128} addresses
  - Note: 16 hexadecimal numbers, 2 digits each, separated by “:”
    - Example: 2001:0db8:0000:0000:0000:0000:1428:57ab
    - If one or more groups of 4 digits is 0000, the zeros may be omitted and replaced (once) with "::“
    - Example: 2001:0db8::1428:57ab
  - To maintain compatibility, public IP addresses are considered a subset of IPv6 address space
  - IPv4 addresses in IPv6 can be written as: 10.0.0.1 -> ::10.0.0.1 or 0:0:0:0:0:0:A00:1

IPv6

- ICMPv6
  - ICMP provides functions (reporting data transmission, errors, etc.) plus:
    - Neighbor Discovery(*Neighbor Discovery Protocol – NDP*) - Replaces the ARP
    - Multicast listener discovery(*Multicast Listener Discovery*) – replaces IGMP (*Internet Group Management Protocol*)
  - Details in RFC 4443

IPv6

- ... More -> Optional Course

Summary

- Network Level
  - IPv4 Problem
    - Context
    - Characteristics
    - Subnets
  - Private Networks
  - ICMP
  - Address Resolution
  - IPv6 - overview
    - Details -> Future Course

Questions?