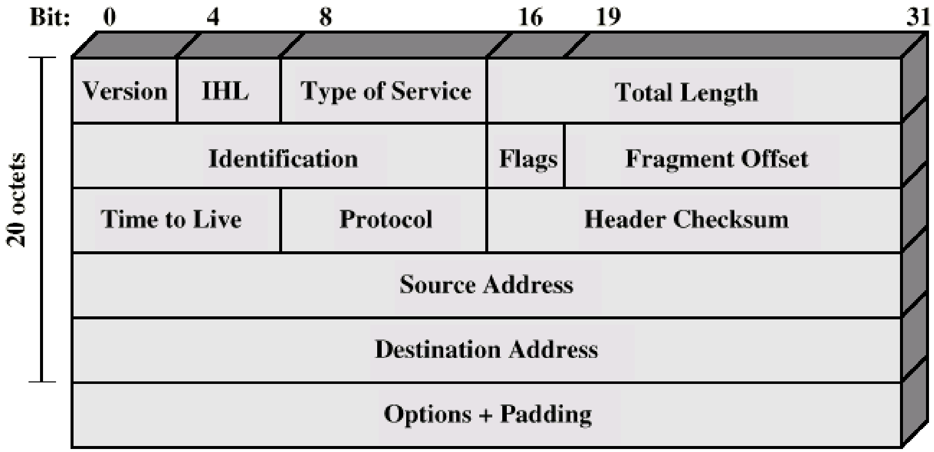
Internet Protocol - IP



Bit: 0 4 8 16 19 31

20 octets

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options + Padding

All Internet transport protocols use the Internet Protocol (IP) to carry data from source host to destination host.

IP Features

- IP is a connectionless or datagram internetwork service, providing no end-to-end delivery guarantees.
- IP datagrams may arrive at the destination host damaged, duplicated, out of order, or not at all.

IP Features

- The layers above IP are responsible for reliable delivery service when it is required.
- The IP protocol includes provision for addressing, type-of-service specification, fragmentation and re-assembly, and security.
- The datagram or connectionless nature of IP is a fundamental and characteristic feature of the Internet architecture.

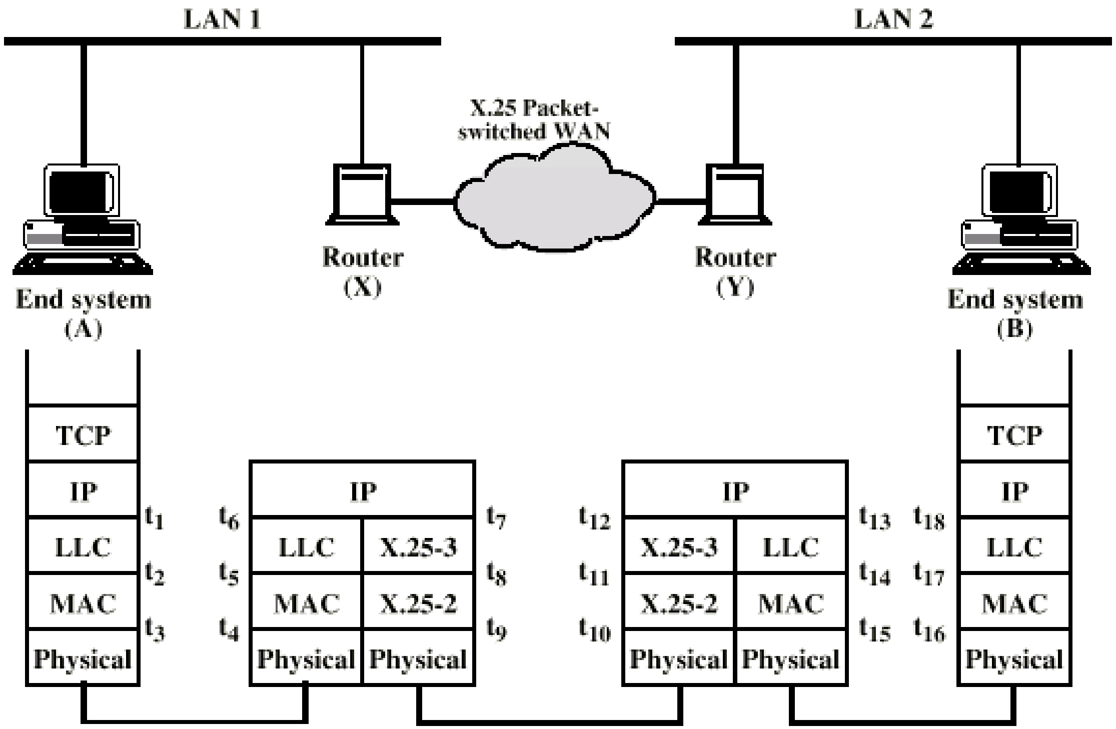
Connectionless Operation of Internet Protocol

- Corresponds to datagram mechanism in packet switched network
- Each N-PDU treated separately
- Network layer protocol common to all DTEs and routers
  - Known generically as the internet protocol
- Internet Protocol
  - Internet Protocol developed for ARPANET
  - RFC 791 (Get it and study it)
- Lower layer protocol needed to access particular network

Connectionless IP Internetworking

- Advantages
  - Flexibility
  - Robust
  - No unnecessary overhead
- Unreliable
  - Not guaranteed delivery
  - Not guaranteed order of delivery
    - Packets can take different routes
  - Reliability is responsibility of next layer up (e.g. TCP)

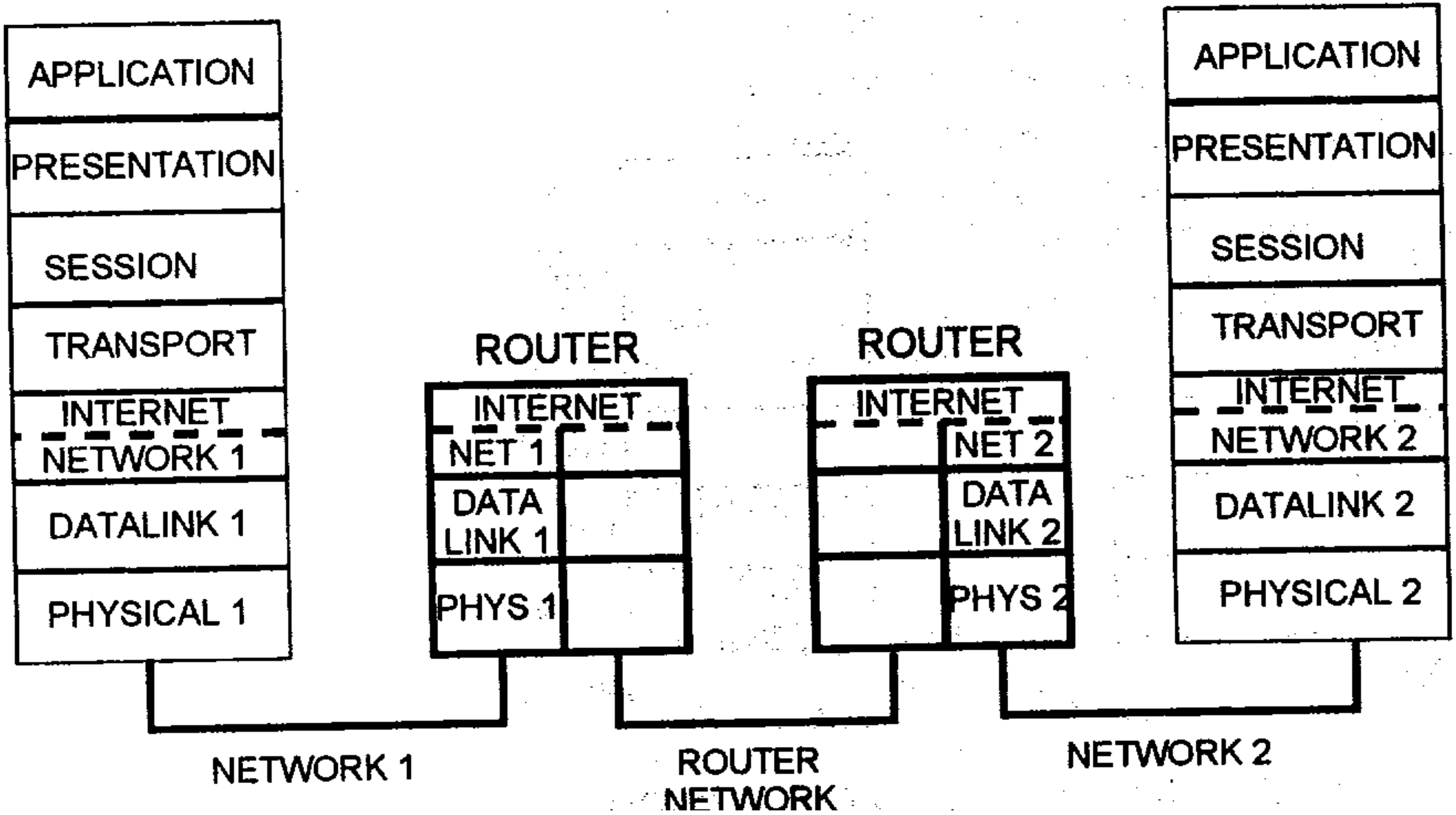
IP Operation



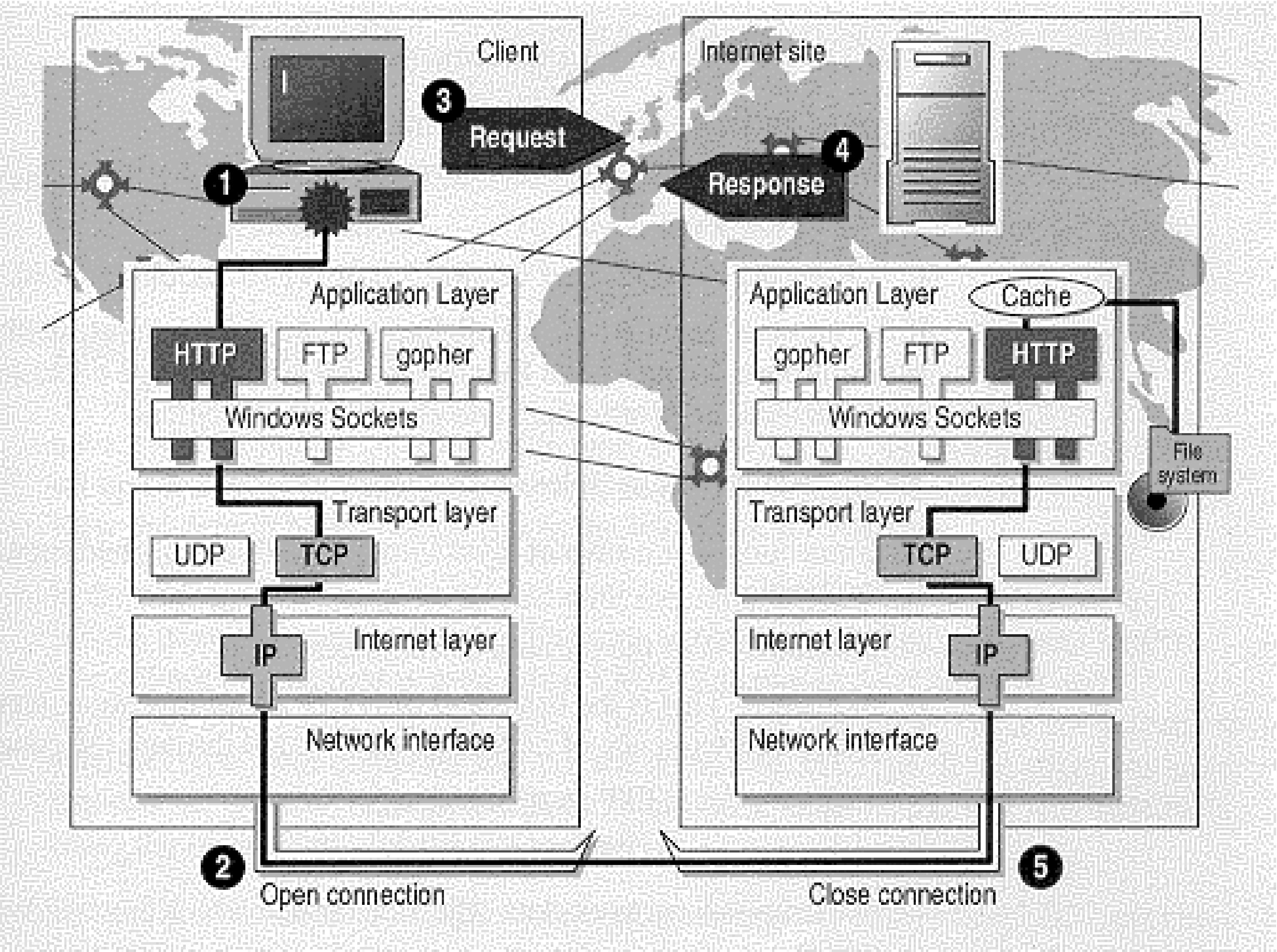
t_1, t_6, t_7, t_{12}, t_{13}, t_{18}			IP-H	TCP-H	Data	
t_2, t_5		LLC1-H	IP-H	TCP-H	Data	
t_3, t_4	MAC1-H	LLC1-H	IP-H	TCP-H	Data	MAC1-T
t_8, t_{11}		XP-H	IP-H	TCP-H	Data	
t_9, t_{10}	XL-H	XP-H	IP-H	TCP-H	Data	XL-T
t_{14}, t_{17}		LLC2-H	IP-H	TCP-H	Data	
t_{15}, t_{16}	MAC2-H	LLC2-H	IP-H	TCP-H	Data	MAC2-T

TCP-H	=	TCP header	MACi-T	=	MAC trailer
IP-H	=	IP header	XP-H	=	X.25 packet header
LLCi-H	=	LLC header	XL-H	=	X.25 link header
MACi-H	=	MAC header	XL-T	=	X.25 link trailer

Router-based Networking



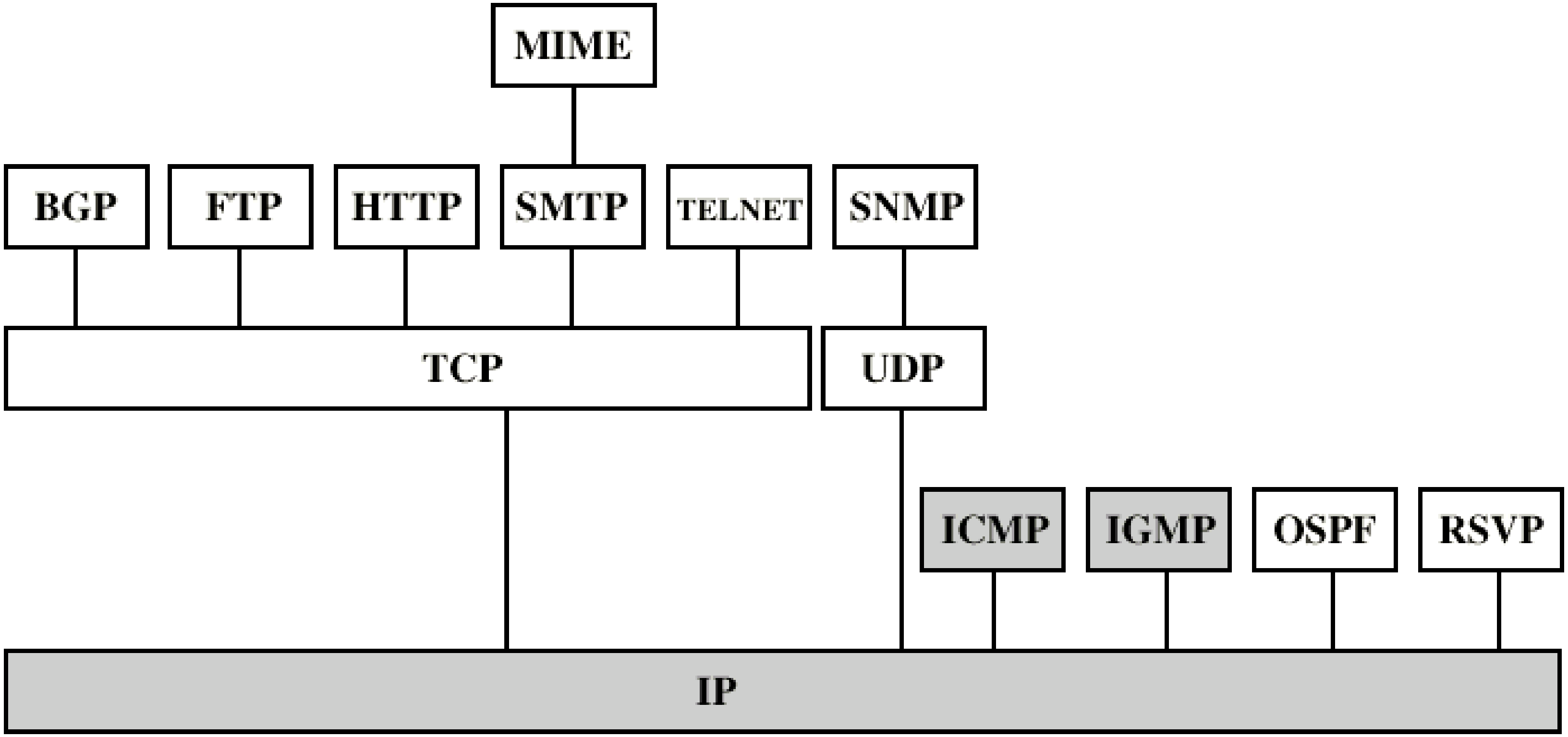
IP and Other Protocols



IP and Other Protocols

Application Presentation	FTP	Telnet	SMTP	HTTP	Ping	DNS
Session	SSL					
Transport	TCP		UDP		ICMP	
Network	IP					
Datalink	LLC	HDLC	PPP	LAP-B	LAP-F	LAP-D
	Ethernet	Token Ring	FDDI	ATM	DQDB	Frame Relay
Physical	Optical Fiber	UTP	Coaxial Cable	Microwave	Satellite	STP

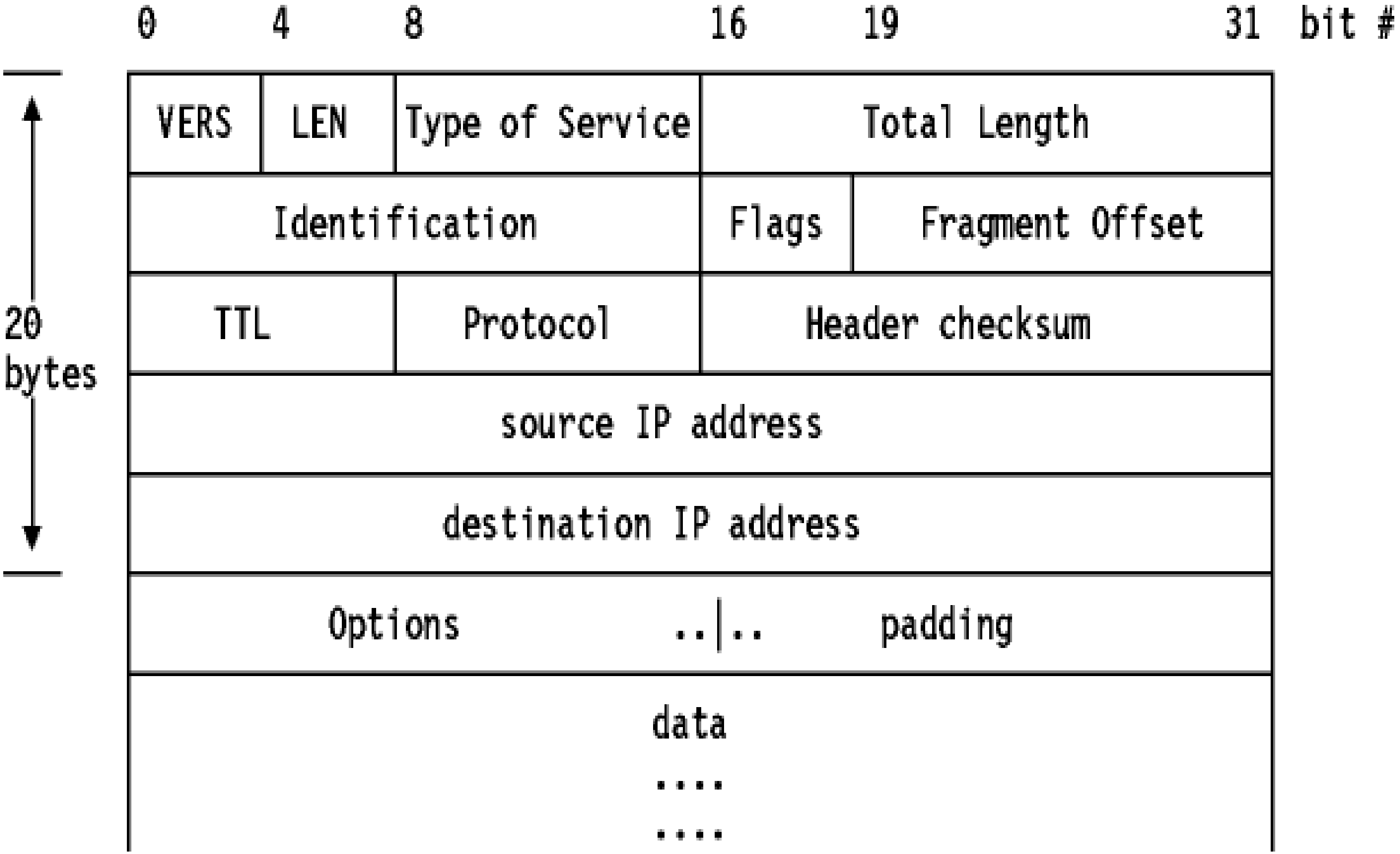
Internetworking Protocols



IP provides several services:

- **Addressing.** IP headers contain 32-bit addresses which identify the sending and receiving hosts. These addresses are used by intermediate routers to select a path through the network for the packet.
- **Fragmentation.** IP packets may be split, or fragmented, into smaller packets. This permits a large packet to travel across a network which can only handle smaller packets. IP fragments and reassembles packets transparently.
- **Packet timeouts.** Each IP packet contains a Time To Live (TTL) field, which is decremented every time a router handles the packet. If TTL reaches zero, the packet is discarded, preventing packets from running in circles forever and flooding a network.
- **Type of Service.** IP supports traffic prioritization by allowing packets to be labeled with an abstract type of service.
- **Options.** IP provides several optional features, allowing a packet's sender to

IP Datagram Format



0 4 8 16 19 31 bit #

20 bytes

VERS | LEN | Type of Service | Total Length

Identification | Flags | Fragment Offset

TTL | Protocol | Header checksum

source IP address

destination IP address

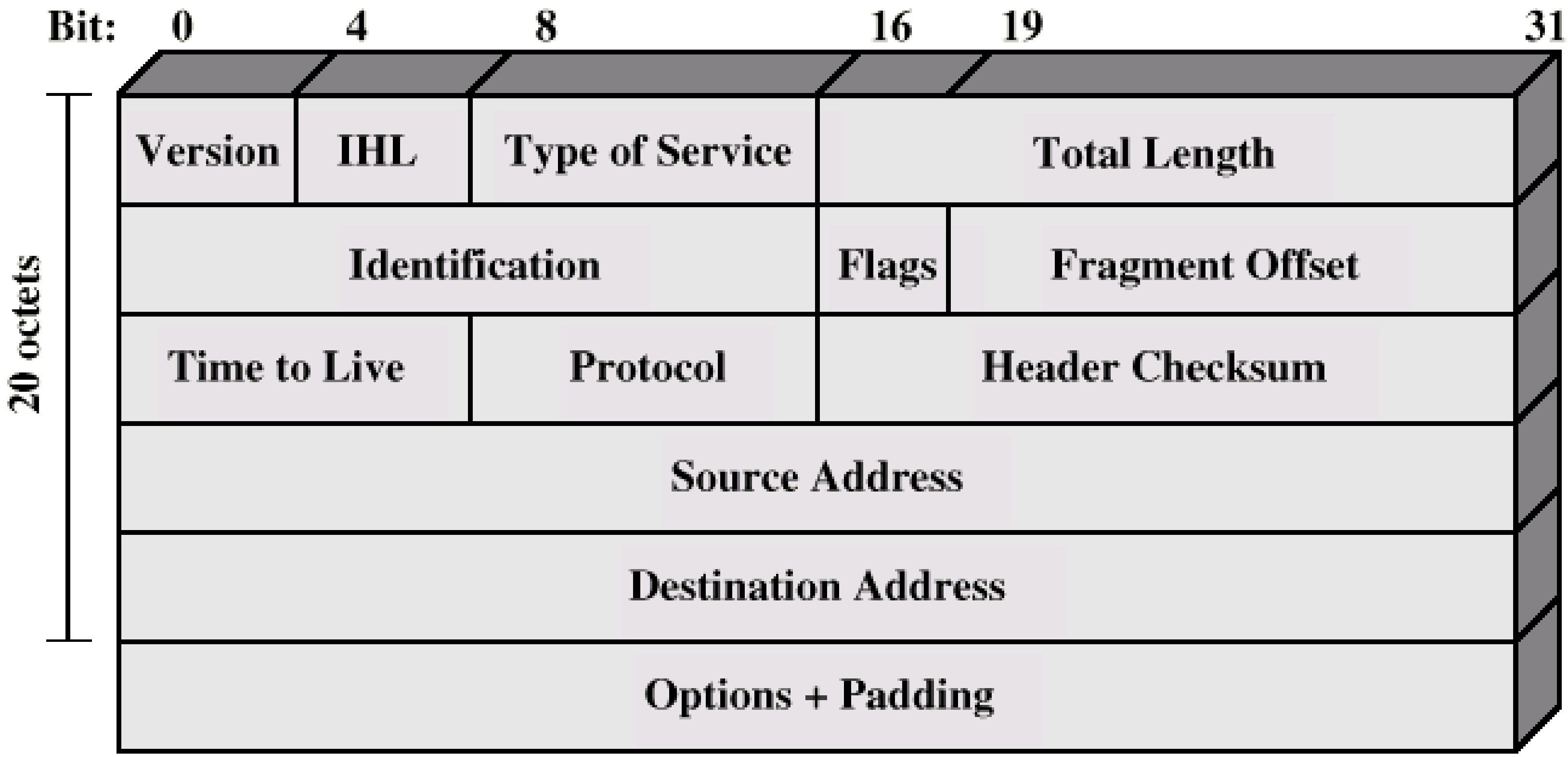
Options ..|.. padding

data

....

....

Internet Protocol Packet Header



Bit: 0 4 8 16 19 31

20 octets

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

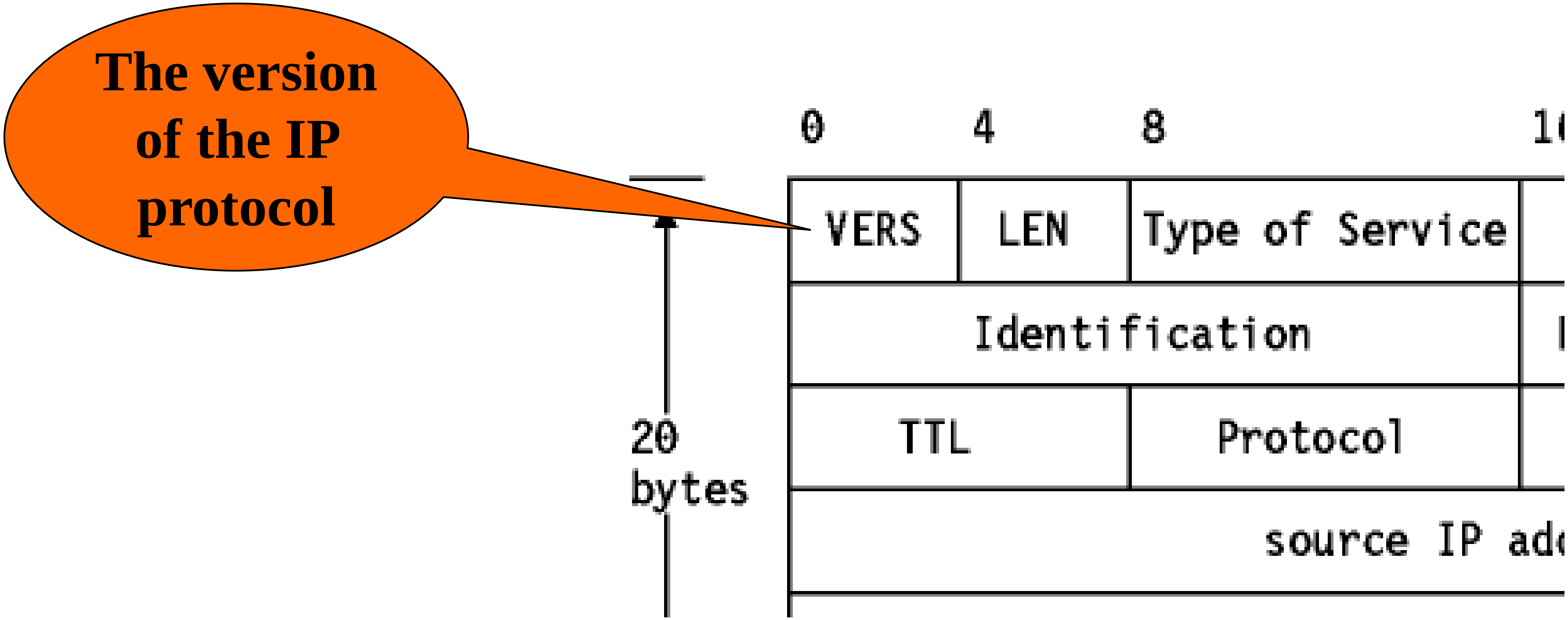
Source Address

Destination Address

Options + Padding

VERS - Version

- The version of the IP protocol. The current version is 4. 5 is experimental and 6 is IPng (see IP: The Next Generation (IPng)).



The version of the IP protocol

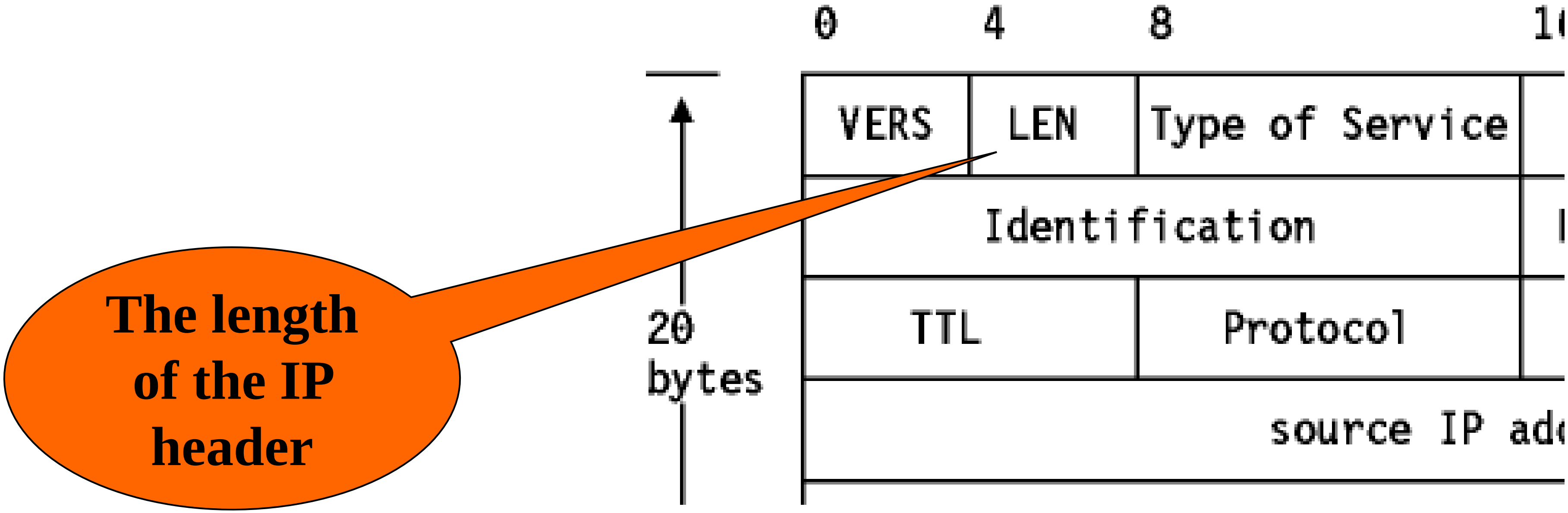
0 4 8 1

VERS	LEN	Type of Service
Identification		
TTL		Protocol
source IP ad		

20 bytes

LEN - Length

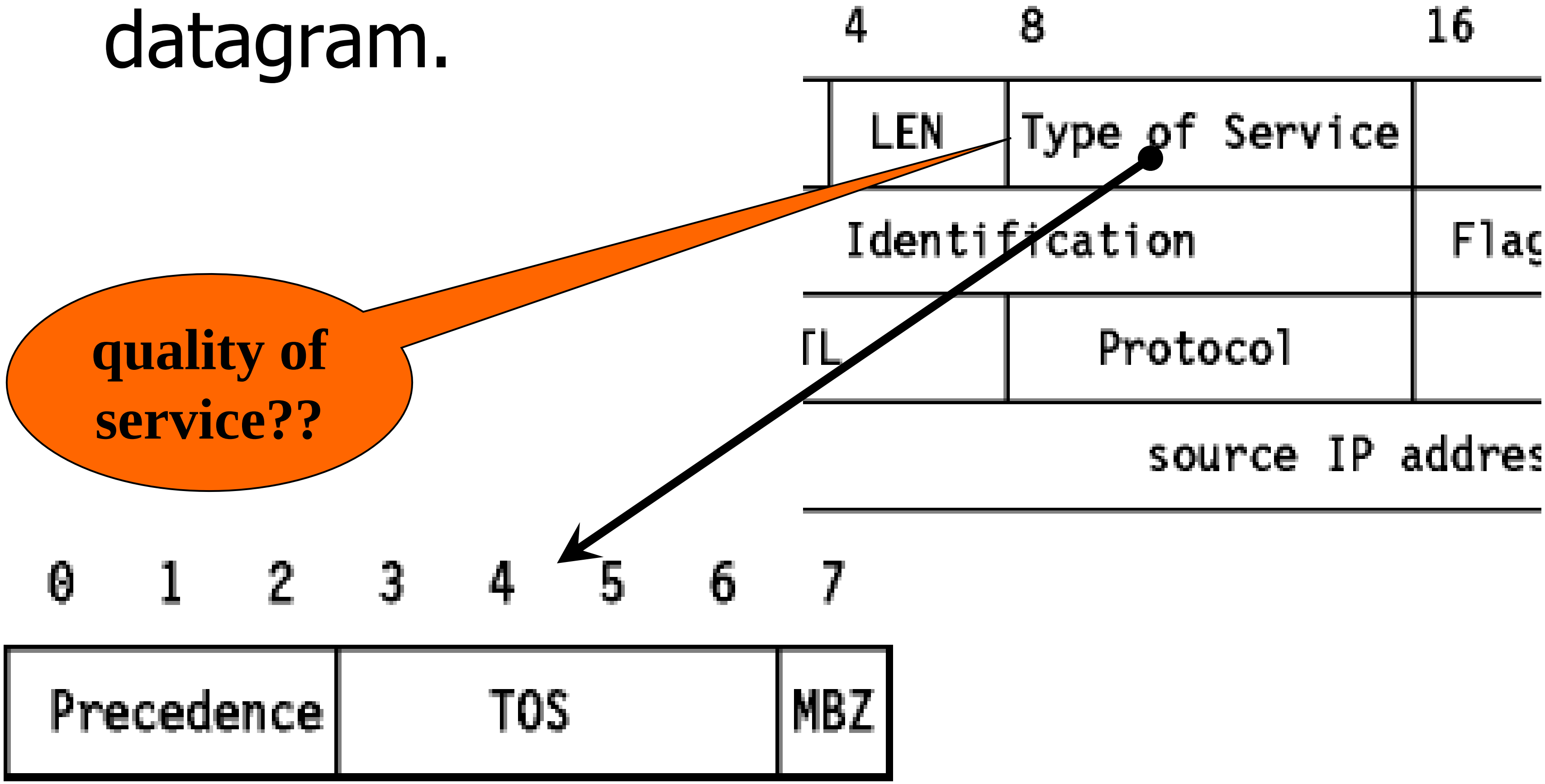
- The length of the IP header counted in 32-bit quantities. This does not include the data field.



The length of the IP header

Type of Service

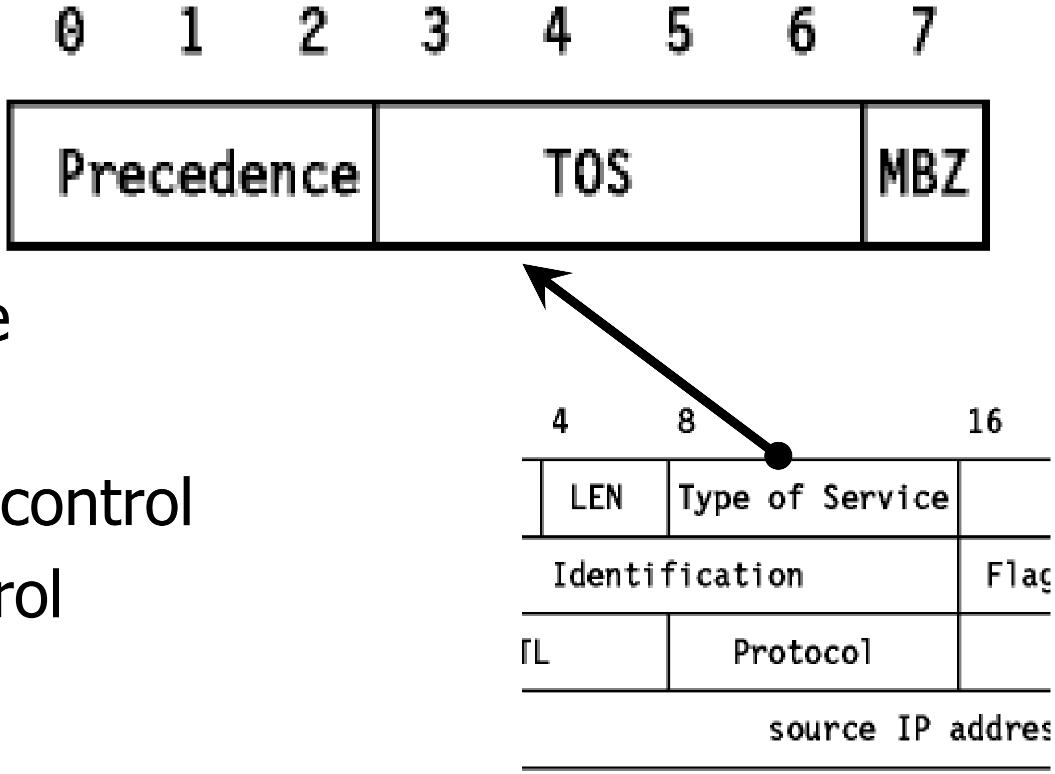
- The type of service is an indication of the quality of service requested for this IP datagram.



0	1	2	3	4	5	6	7
Precedence			TOS				MBZ

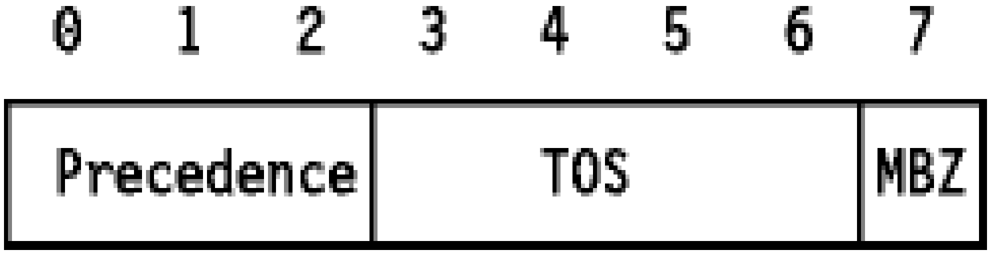
Type of Service - Precedence

- Is a measure of the nature and priority of this datagram:
  - 000 Routine
  - 001 Priority
  - 010 Immediate
  - 011 Flash
  - 100 Flash override
  - 101 Critical
  - 110 Internetwork control
  - 111 Network control



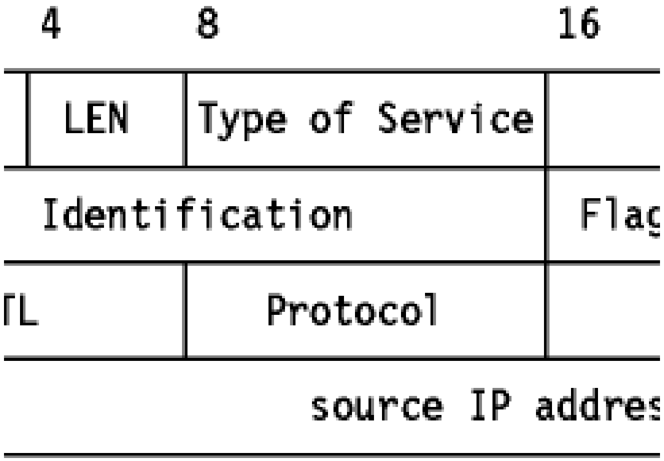
TOS - Type Of Service

- Specifies the type of service value:
- 1000 Minimize delay
- 0100 Maximize throughput
- 0010 Maximize reliability
- 0001 Minimize monetary cost
- 0000 Normal service
- A detailed description of the type of service can be found in the RFC 1349



0 1 2 3 4 5 6 7

Precedence | TOS | MBZ



4 8 16

LEN | Type of Service

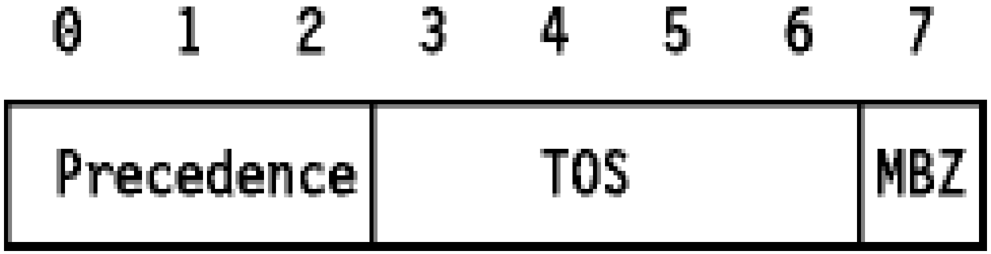
Identification | Flag

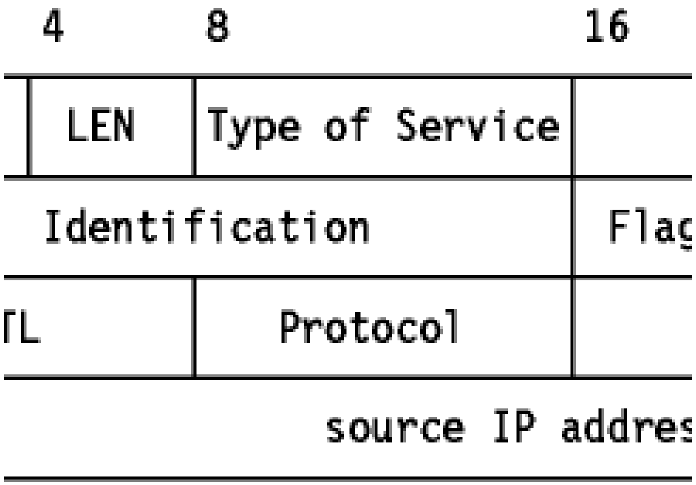
TL | Protocol

source IP addres

MBZ - Must Be Zero

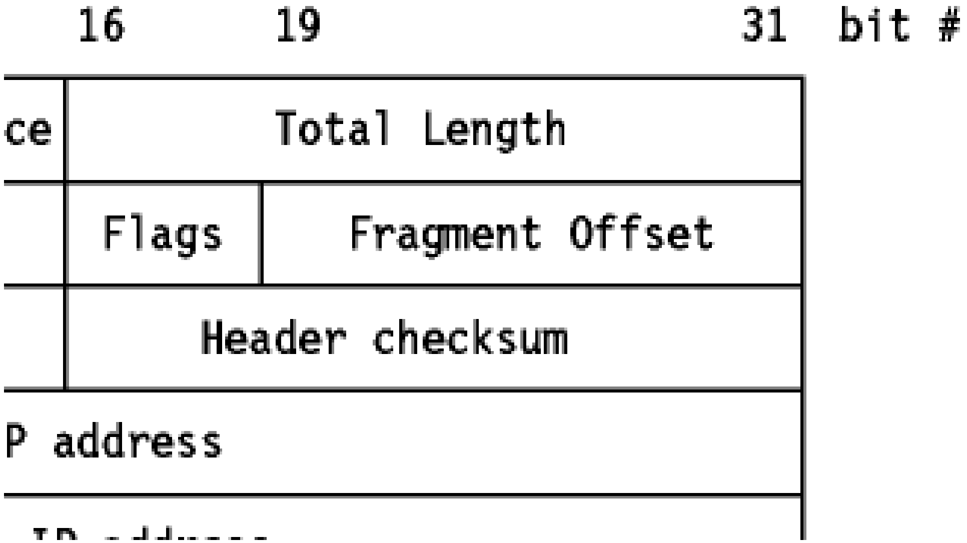
- Reserved for future use ("must be zero" unless participating in an Internet protocol experiment which makes use of this bit)





Total Length

- Total length of the IP datagram in bytes
- Maximum size is 64k because there are 16 bits for it
- That means a single IP datagram cannot be bigger than 65536 bytes including the header



16 19 31 bit #

ce | Total Length

Flags | Fragment Offset

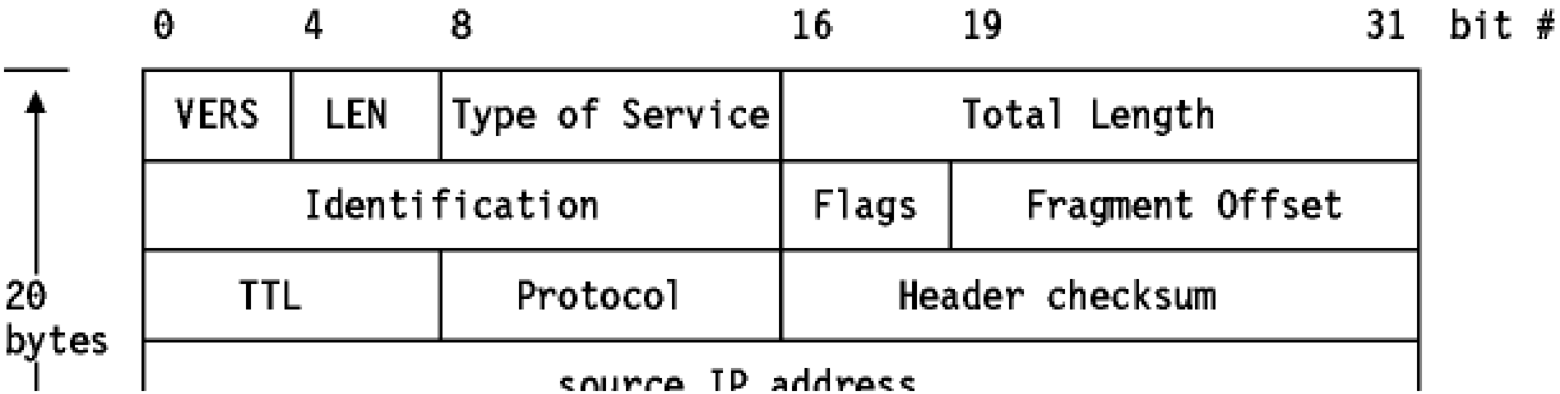
Header checksum

P address

IP address

Fragmentation Related Information

- ⌘ The next 32 bits contain information related to fragmentation
- ⌘ This information can be used to reassemble a fragmented IP datagram
- ⌘ Fragmentation means that on its way a single IP datagram was broken into smaller IP datagrams because the intervening network was unable to carry the original datagram because it was too big



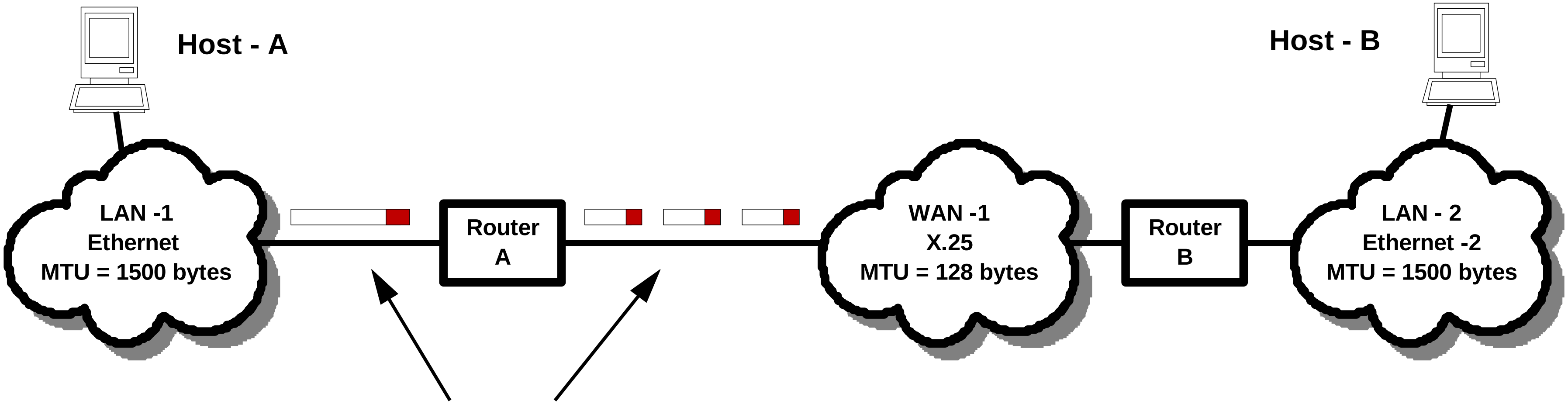
0	4	8	16	19	31 bit #
VERS	LEN	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
TTL		Protocol	Header checksum		
source IP address					

Why Fragment?

- When an IP datagram travels from one host to another, it can cross different physical networks. Physical networks have a maximum frame size, called the Maximum Transmission Unit (MTU), which limits the length of a datagram that can be placed in one physical frame. Therefore, a scheme has been put in place to fragment long IP datagrams into smaller ones, and to reassemble them at the destination host. IP requires that each link has an MTU of at least 68 bytes, so if any network provides a lower value than this, fragmentation and re-assembly must be implemented in the network interface layer in a way that is transparent to IP. 68 is the sum of the maximum IP header length of 60 bytes and the minimum possible length of data in a non-final fragment (8 bytes). IP implementations are not required to handle unfragmented datagrams larger than 576 bytes, but most implementations will handle larger values, typically slightly more than 8192 bytes or higher, and rarely less than 1500.

Why Fragment?

Host - A in LAN -1 is commnicating
with Host - B in LAN -2 using IP



Router A has to perform
fragmentation of IP datagrams
when forwarding them from
LAN-1 to WAN-1

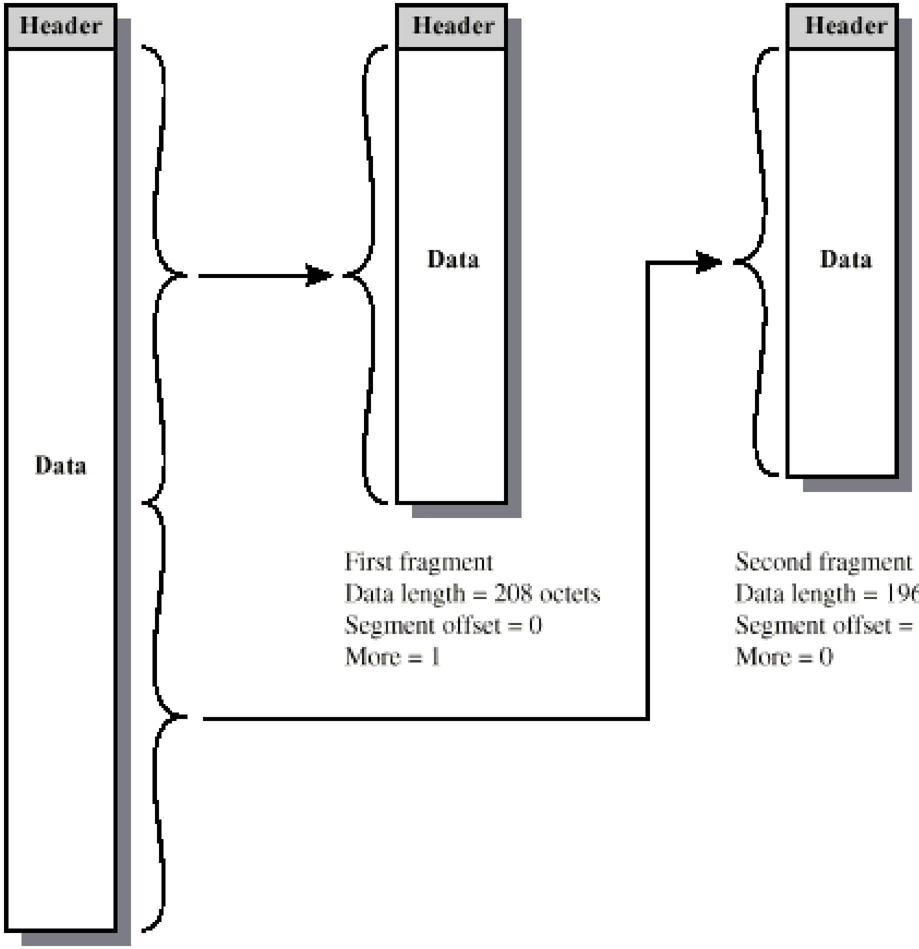
Fragmentation Procedure

- An unfragmented datagram has all-zero fragmentation information. That is, the more fragments flag bit is zero and the fragment offset is zero. When fragmentation is to be done, the following steps are performed:

Fragmentation Procedure

- The DF flag bit is checked to see if fragmentation is allowed. If the bit is set, the datagram will be discarded and an error will be returned to the originator using ICMP.
- Based on the MTU value, the data field is split into two or more parts. All newly created data portions must have a length which is a multiple of 8 bytes, with the exception of the last data portion.

Fragmentation Example



Original datagram
Data length = 404 octets
Segment offset = 0
More = 0

First fragment
Data length = 208 octets
Segment offset = 0
More = 1

Second fragment
Data length = 196 octets
Segment offset = 26 64-bit units
More = 0

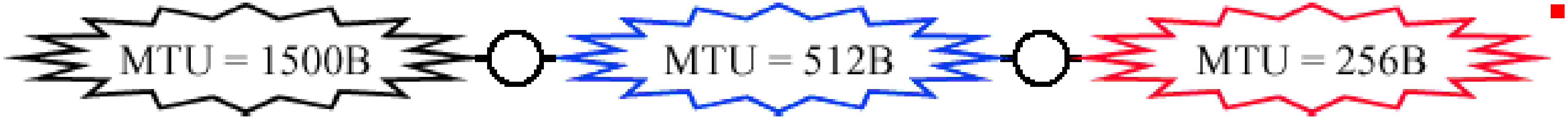
Fragmentation Procedure - 2

- All data portions are placed in IP datagrams. The header of these datagrams are copies of the original one, with some modifications:
  - The more fragments flag bit is set in all fragments except the last.
  - The fragment offset field in each is set to the location this data portion occupied in the original datagram, relative to the beginning of the original unfragmented datagram. The offset is measured in 8-byte units.
  - If options were included in the original datagram, the high order bit of the option type byte determines whether or not they will be copied to all fragment datagrams or just to the first one. For instance, source route options have to be copied in all fragments and therefore they have this bit set.
  - The header length field is of the new datagram is set.
  - The total length field of the new datagram is set.
  - The header checksum field is re-calculated.

Fragmentation Procedure - 3

- Each of these fragmented datagrams is now forwarded as a normal IP datagram.
- IP handles each fragment independently, that is, the fragments may traverse different routers to the intended destination, and they may be subject to further fragmentation if they pass through networks that have smaller MTUs.

Fragmentation



ID = 12345, More = 1
Offset = 160W, Len = 1500B
	ID = 12345, More = 1
	Offset = 0W, Len = 512B
		ID = 12345, More = 1
		Offset = 0W, Len = 256B

		ID = 12345, More = 1
		Offset = 32W, Len = 256B

	ID = 12345, More = 1
	Offset = 64W, Len = 512B
		ID = 12345, More = 1
		Offset = 64W, Len = 256B

		ID = 12345, More = 1
		Offset = 96W, Len = 256B

	ID = 12345, More = 1
	Offset = 128W, Len = 476B
		ID = 12345, More = 1
		Offset = 128W, Len = 256B

		ID = 12345, More = 1
		Offset = 160W, Len = 220B

Reassembley Procedure

- At the destination host, the data has to be reassembled into one datagram. The identification field of the datagram was set by the sending host to a unique number (for the source host, within the limits imposed by the use of a 16-bit number). As fragmentation doesn't alter this field, incoming fragments at the receiving side can be identified, if this ID field is used together with the Source and Destination IP addresses in the datagram. The Protocol field is also to be checked for this identification.

Reassembley Procedure - 2

- In order to reassemble the fragments, the receiving host allocates a buffer in storage as soon as the first fragment arrives. A timer routine is then started. When the timer timeouts and not all of the fragments have been received, the datagram is discarded. The initial value of this timer is called the IP datagram time-to-live (TTL) value. It is implementation dependent, and some implementations allow it to be configured; for example AIX Version 3.2 provides an ipfragttl option with a default value of 60 seconds.

Re-assembly Procedure - 3

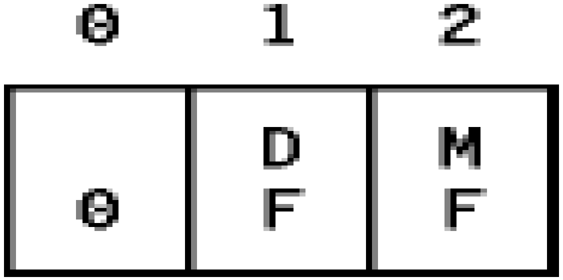
- When subsequent fragments of the datagram arrive, before the timer expires, the data is simply copied into the buffer storage, at the location indicated by the fragment offset field. As soon as all fragments have arrived, the complete original unfragmented datagram is restored, and processing continues, just as for unfragmented datagrams.

Fragmentation Fields

- **Identification** - A unique number assigned by the sender to aid in reassembling a fragmented datagram. Fragments of a datagram will have the same identification number.
- **Fragment Offset -** Used with fragmented datagrams, to aid in reassembly of the full datagram. The value is the number of 64-bit pieces (header bytes are not counted) that are contained in earlier fragments. In the first (or only) fragment, this value is always zero.

Flags

- Where:
- 0 Reserved, must be zero
- DF Don't Fragment:
  - 0 means allow fragmentation
  - 1 means do not allow fragmentation
- MF More Fragments: 0 means that this is the last fragment of this datagram, 1 means that this is not the last fragment.



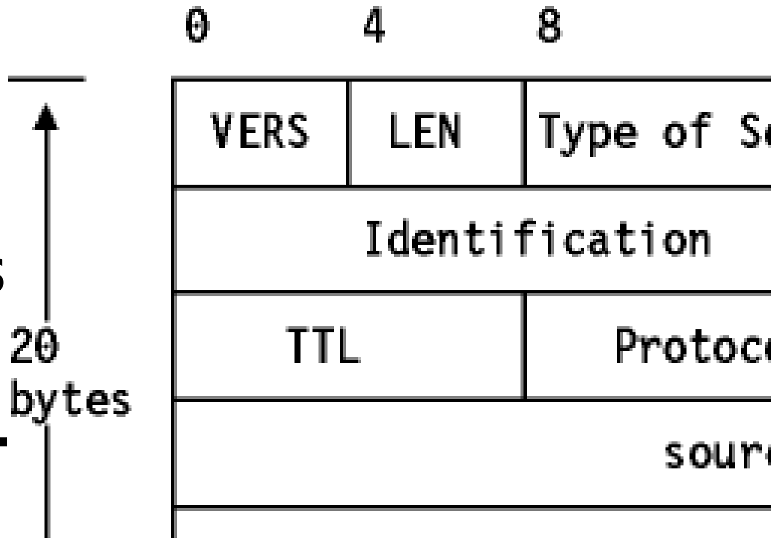
0	1	2
0	DF	MF

Dealing with Failure in Re-assembly

- Re-assembly may fail if some fragments get lost
- Need to detect failure
- Re-assembly time out
  - Assigned to first fragment to arrive
  - If timeout expires before all fragments arrive, discard partial data
- Use packet lifetime (time to live in IP)
  - If time to live runs out, kill partial data

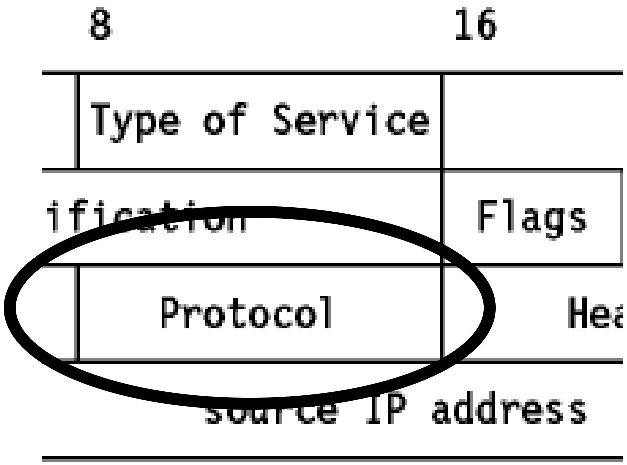
TTL - Time To Live

- Specifies the time (in seconds) this datagram is allowed to travel. Each router where this datagram passes is supposed to subtract from this field its processing time for this datagram. Actually a router is able to process a datagram in less than 1 second; thus it will subtract one from this field, and the TTL becomes a hop-count metric rather than a time metric. When the value reaches zero, it is assumed that this datagram has been traveling in a closed loop and it is discarded. The initial value should be set by the higher-level protocol which creates the datagram.



Protocol- Protocol Number

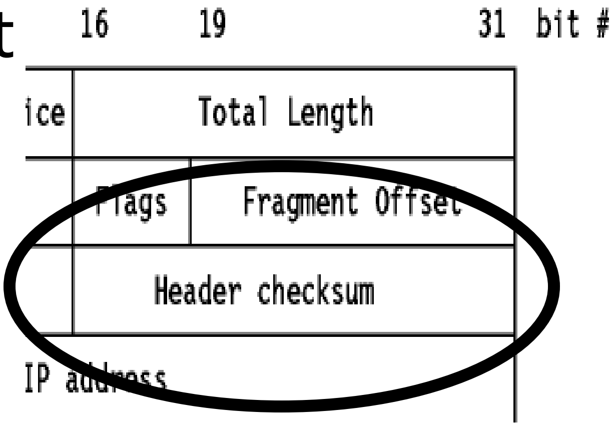
- Indicates the higher-level protocol to which IP should deliver the data in this datagram. Some important values are:
  - 0 Reserved
  - 1 Internet Control Message Protocol (ICMP)
  - 2 Internet Group Management Protocol (IGMP)
  - 3 Gateway-to-Gateway Protocol (GGP)
  - 4 IP (IP encapsulation)
  - 5 Stream
  - 6 Transmission Control (TCP)
  - 8 Exterior Gateway Protocol (EGP)
  - 9 Private Interior Routing Protocol
  - 17 User Datagram (UDP)
  - 89 Open Shortest Path First



- The full list can be found in STD 2 - Assigned Internet Numbers.

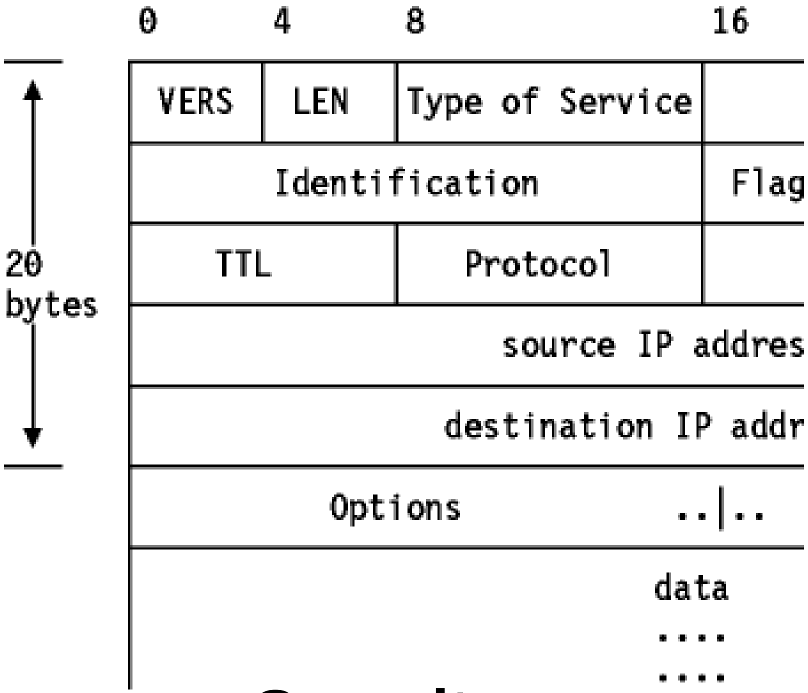
Header Checksum

⌘ Is a checksum on the header only. It does not include the data. The checksum is calculated as the 16-bit one's complement of the one's complement sum of all 16-bit words in the header. For the purpose of this calculation, the checksum field is assumed to be zero. If the header checksum does not match the contents, the datagram is discarded because at least one bit in the header is corrupt, and the datagram may even have arrived at the wrong destination.



Options

- Various options regarding this datagram, including how to route it, how to identify it (security labeling), how to trace the places through which it passes, how to time-stamp it for delay measurement, etc.



- Security
- Source routing
- Route recording
- Timestamping

Options

- Options – Up to 40 bytes of option data added by source host or intermediate routers
  - 1 byte Option id, followed by an optional 1 byte Option length, followed by Option data
  - Padded to a multiple of 4 bytes
  - 5 options currently defined
    - Security – Security identifier
    - Strict source routing – Complete route specified
    - Loose source routing – List of required routers to pass through
    - Record route – Each router appends its address to the list
    - Timestamp – Each router appends address & timestamp
    - stream id (used for voice) for reserved resources,

IP Options Coding

Type	Length	Value
1B	1B	*n*B

Flag Copy	Class	Number
1b	2b	5b

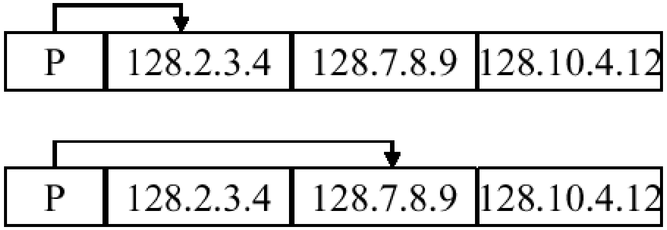
- Flag Copy: 0 = Copy the option only into the first fragment of a fragmented datagram
  1 = Copy into all fragments
- Class: 0 =User or control, 1=Reserved, 2=Diagnostics, 3=reserved

IP Options

Class	Number	Length	Description
0	0	0	End of Options
0	1	0	No Op
0	2	11	Security
0	3	Var	Loose Source Routing
0	7	Var	Record Route
0	8	4	Stream ID (obsolete)
0	9	Var	Strict Source Routing
2	4	Var	Internet Time-Stamp

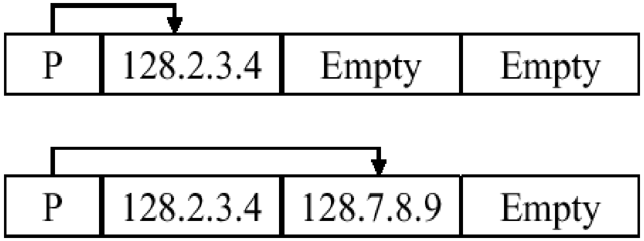
IP Source Routing

Code	Length	Pointer	Router Data



Route Recording

Code	Length	Pointer	Route Data

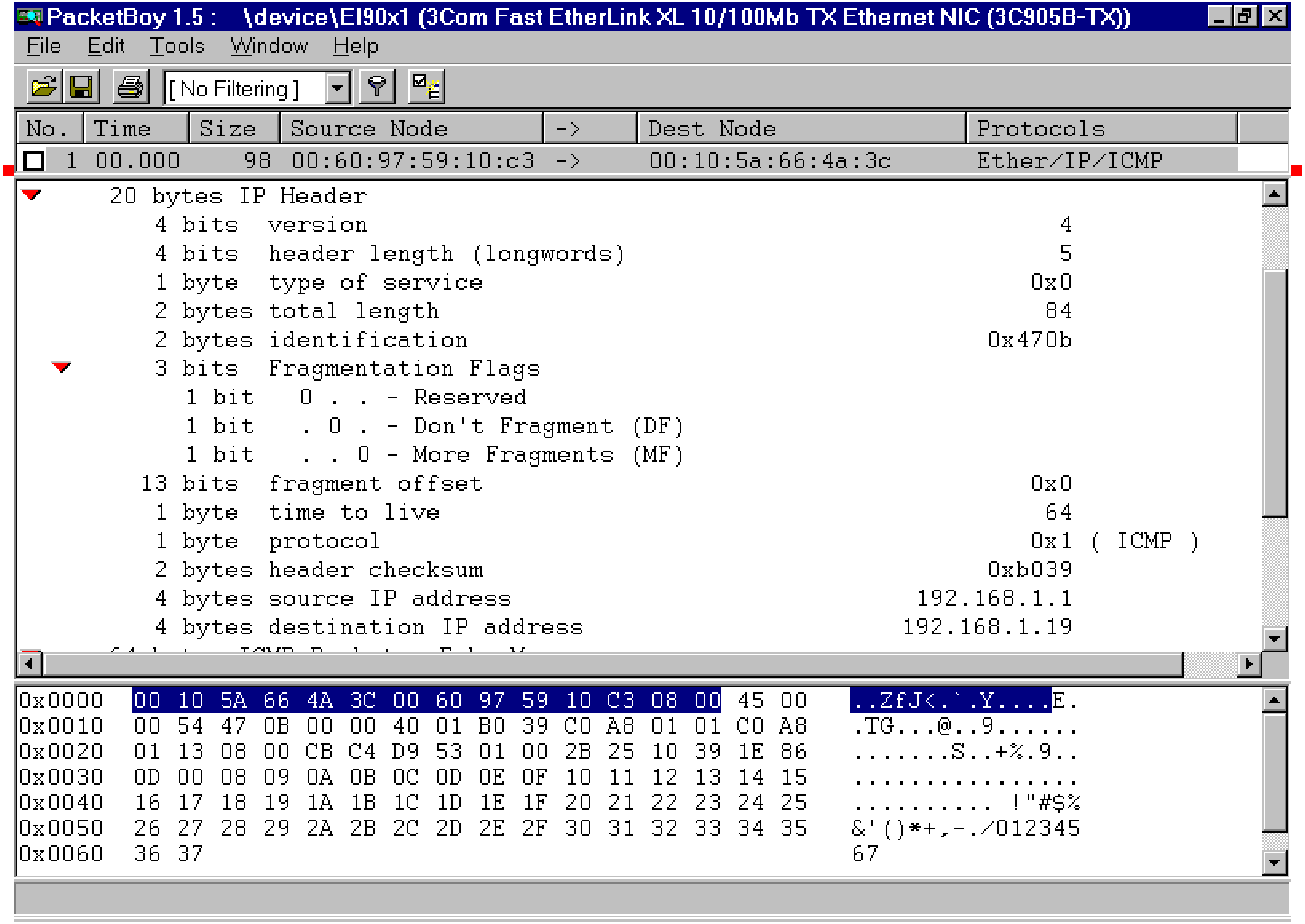


Timestamp Option

Code	Length	Pointer	Data

Oflw	Flags	IP Address 1	Timestamp 1

IP Address *n*	Timestamp *n*


PacketBoy 1.5 : \device\El90x1 (3Com Fast EtherLink XL 10/100Mb TX Ethernet NIC (3C905B-TX))
File
Edit
Tools
Window
Help
[No Filtering]

```
No.  Time     Size  Source Node          ->   Dest Node            Protocols
□ 1  00.000     98  00:60:97:59:10:c3    ->   00:10:5a:66:4a:3c    Ether/IP/ICMP
```

```
      20 bytes IP Header
          4 bits   version                                      4
          4 bits   header length (longwords)                    5
          1 byte   type of service                            0x0
          2 bytes  total length                                84
          2 bytes  identification                          0x470b
          3 bits   Fragmentation Flags
            1 bit    0 . . - Reserved
            1 bit    . 0 . - Don't Fragment (DF)
            1 bit    . . 0 - More Fragments (MF)
         13 bits   fragment offset                            0x0
          1 byte   time to live                                64
          1 byte   protocol                                   0x1  ( ICMP )
          2 bytes  header checksum                         0xb039
          4 bytes  source IP address                  192.168.1.1
          4 bytes  destination IP address            192.168.1.19
```

```
0x0000  00 10 5A 66 4A 3C 00 60 97 59 10 C3 08 00 45 00   ..ZfJ<.`.Y....E.
0x0010  00 54 47 0B 00 00 40 01 B0 39 C0 A8 01 01 C0 A8   .TG...@..9......
0x0020  01 13 08 00 CB C4 D9 53 01 00 2B 25 10 39 1E 86   .......S..+%.9..
0x0030  0D 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15   ................
0x0040  16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25   .......... !"#$%
0x0050  26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35   &'()*+,-./012345
0x0060  36 37                                             67
```

IP Addresses

- To be able to identify a host on the internet, each host is assigned an address, the *IP address*, or *Internet Address*.
- The standards for IP addresses are described in *RFC 1166 -- Internet Numbers*.
- When the host is attached to more than one network, it is called *multi-homed* and it has one IP address for each network interface.

IP Addresses

- An IP Address is a 32 bit binary number.
- IP addresses are used by the IP protocol to uniquely identify a host on the internet.
- IP datagrams (the basic data packets exchanged between hosts) are transmitted by some physical network attached to the host and each IP datagram contains a source IP address and a destination IP address.

The Dotted Decimal Notation

- IP addresses are usually represented in a dotted decimal form (as the decimal representation of four 8-bit values concatenated with dots).
- For example 128.2.7.9 is an IP address with 128.2 being the network number and 7.9 being the host number.
- The rules used to divide an IP address into its network and host parts are explained below.

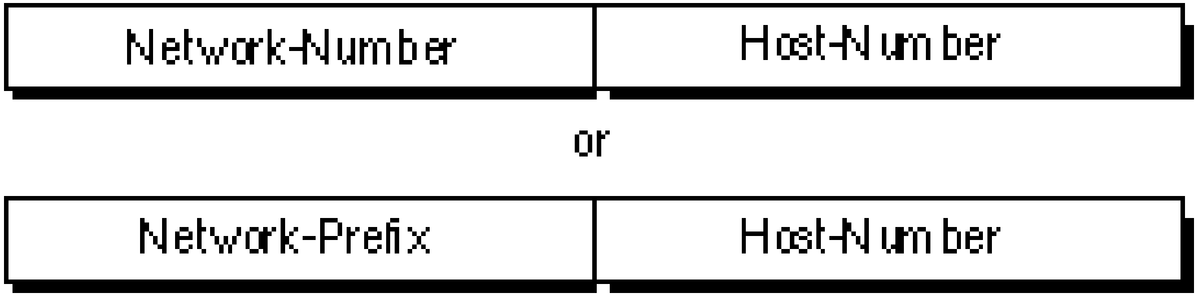
IP Address Example

- The binary format of the IP address 128.2.7.9 is:
- 10000000 00000010 00000111 00001001
- IP address is made of four groups of decimal numbers between 0 - 255 separated by dots.
- Some of the numbers are special (like 0.0.0.0 or 255.255.255.255) and are used to designate the default gateway, a broadcast or multicast address, or some reserved numbers for the developers to play with.

Parts of an IP Address

- A part of the address designates the network numbers, and the remaining part designates the host number. So, we may say an IP address has the format NETWORK.HOST.
- The *network number* part of the IP address is centrally administered by the Internet Network Information Centre (the InterNIC) and is unique throughout the Internet.
- The IP address consists of a pair of numbers:
  - IP address = <network number><host number>

Parts of an IP Address



Network-Number | Host-Number

or

Network-Prefix | Host-Number

Network Number Assignment

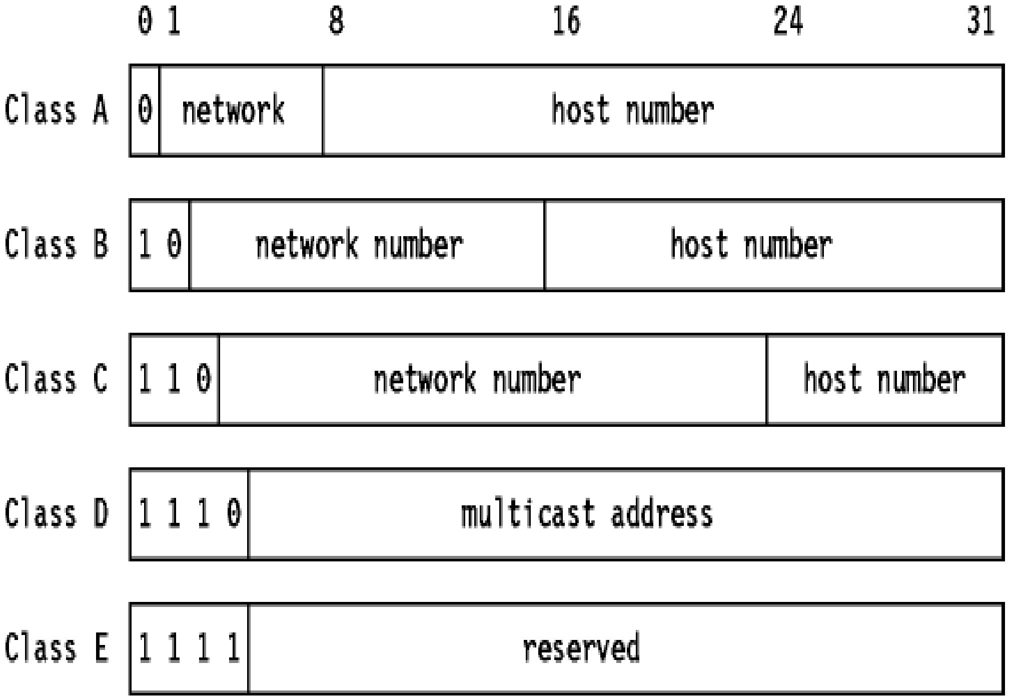
- One point to note about the split of an IP address into two parts is that this split also splits the responsibility for selecting the IP address into two parts. The network number is assigned by the InterNIC, and the host number by the authority which controls the network.
- The host number can be further subdivided: this division is controlled by the authority which owns the network, and not by the InterNIC.

IP Address Classes

- Traditionally, the conventions are that there are three main types of IP networks.
- Class A
- Class B
- Class C
- There are also:
- Class D
- Class E

Assigned Classes of Internet Addresses

- The first bits of the IP address specify how the rest of the address should be separated into its network and host part.
- The terms *network address* and *netID* are sometimes used instead of network number, but the formal term, used in RFC 1166, is network number. Similarly, the terms *host address* and *hostID* are sometimes used instead of host number.



	0 1	8	16	24	31
Class A	0	network	host number		
Class B	1 0	network number		host number	
Class C	1 1 0	network number			host number
Class D	1 1 1 0	multicast address			
Class E	1 1 1 1	reserved			

Class A Network Addresses

- Class A networks use the first octet (8 bits) to designate the network, with the first (high-order) bit set to 0.
- The last three octets designate the host.
- So the Class A network addresses are 1.H.H.H to 127.H.H.H, where H is used to designate the host address octets.
- Class A addressing allows for 127 networks.
- Class A addresses use 7 bits for the network number giving 126 possible networks (out of every group of network and host numbers, two have a special meaning). The remaining 24 bits are used for the host number, so each networks can have up to 2^{24} - minus 2 (16,777,214) hosts.

Class B Network Addresses

- Class B networks use two octets to designate the network and two to designate the host.
- The network part must begin with 10. The Class B networks are 128.x.H.H to 191.x.H.H, where x is any number between 0 and 255.
- Class B addresses use 14 bits for the network number, and 16 bits for the host number giving 16,382 Class B networks each with a maximum of 65534 hosts.

Class C Network Addresses

- ⌘Class C networks use three octets to designate the network and only one to designate the host.
- ⌘The network part begins with 110.
- ⌘The Class C networks are 192.x.x.H to 223.x.x.H, which allows for 2,097,152 networks.
- ⌘ Class C addresses use 21 bits for the network number and 8 for the host number giving 2,097,150 networks each with up to 254 hosts.

IP Address Class’ Host Accommodation

- As you can see, there are very few Class A networks, but each of them can accommodate millions of hosts. A Class B network supports only 65,534 hosts, while Class C only 254 hosts (all 0 and 1 combinations are not allowed).

Other Address Classes

- There is also a Class D address (starts with 1110) used for multicasting, which is used to address groups of hosts in a limited area.
- Class E addresses are reserved for future use. Class E (1111) addresses are reserved for the nerds.

Special Addresses

- IP Address Notation
  - {<network>, <host>}
  - {<network>, <subnet>, <host>}
  - -1 value means a component consisting of all 1's
- {0,0} = This host on this network
- {0,<host>} = Specific host on this network
- {-1, -1} = Local broadcast
  - Broadcast to all hosts on this network
- {<network>, -1} = Directed broadcast
  - Broadcast to all hosts on <network>

Special Addresses Cont.

- {<network>, <subnet>, -1} = Directed broadcast
  - Broadcast to all hosts on <subnet> of <network>
- {<network>, -1, -1} = Directed broadcast
  - Broadcast to all hosts on all subnets of <network>
- {<127>, <any>} = Loopback address
  - Packet never leaves the NIC
  - Should never appear on the network

IP Address Space Shortage

- It is clear that a class A address will only be assigned to networks with a huge number of hosts, and that class C addresses are suitable for networks with a small number of hosts. However, this means that medium-sized networks (those with more than 254 hosts or where there is an expectation that there may be more than 254 hosts in the future) must use Class B addresses. The number of small- to medium-sized networks has been growing very rapidly in the last few years and it was feared that, if this growth had been allowed to continue unabated, all of the available Class B network addresses would have been used by the mid-1990s. This is termed the IP Address Exhaustion problem. The problem and how it is being addressed are discussed in The IP Address Exhaustion Problem.

IP Address Space Shortage

- Over the next few years, conventional computers will be joined by Personal Digital Assistants, Mobile Phones with data processing capability, smart set-up boxes with integrated web browsers, and from copy machines to kitchen appliances.
- With the proliferation of PCs and the Internet growing like bread with too much yeast, they are running out of addresses - and therefore some solutions are proposed to conserve address space, and even to change the system. But - so far - most existing routers work on 'Class' assumption.

IPv4 - Problems

- The decision to standardize on a 32 bit address space meant that there were only 2^{32} (4,294,967,296) IPv4 addresses available.
- During the early days of the Internet, the seemingly unlimited address space allowed IP addresses to be allocated based on requests rather than its actual need.

IPv4 - Problems

- The class A, B, and C octet boundaries were easy to understand and implement, but they did not foster efficient allocation of addresses.

IPv4 - Problems

- Class C, which supports 254 hosts, is too small.
- Class B, which supports 65534 hosts is too large.
- In the past, sites with several hundred hosts have been assigned as single Class B address rather than couple of Class C addresses.
- Unfortunately, this has resulted in a premature depletion of the Class B network address space.

Classless Inter-Domain Routing

- CIDR was officially documented in September 1993 in RFC 1517, 1518, 1519, 1520
- Eliminates the traditional concept of Class A, B and C networks and replaces it with concept of “network prefix”
- CIDR supports the deployment of arbitrary size networks rather than the standard 8-bit, 16-bit, or 24 bit network numbers associated with classful addressing.

Classless Inter-Domain Routing

- Good News - CIDR is working.
- Bad News - Recent growth trends indicate that the number of Internet routes is beginning to increase at an exponential rate.

Private Internets

- Another approach to conservation of the IP address space is described in *RFC 1597 - Address Allocation for Private Internets*. Briefly, it relaxes the rule that IP addresses are globally unique by reserving part of the address space for networks which are used exclusively within a single organization and which do not require IP connectivity to the Internet. There are three ranges of addresses which have been reserved by IANA for this purpose:

- *10.0.0.0* A single Class A network
- *172.16 through 172.31* 16 contiguous Class B networks
- *192.168.0 through 192.168.255* 256 contiguous Class C networks

Private Internets

- Any organization may use any addresses in these ranges without reference to any other organization. However, because these addresses are not globally unique, they cannot be referenced by hosts in another organization and they are not defined to any external routers.
- Routers in networks not using private addresses, particularly those operated by Internet service providers, are expected to quietly discard all routing information regarding these addresses.

Private Internets

- Routers in an organization using private addresses are expected to limit all references to private addresses to internal links; they should neither advertise routes to private addresses to external routers nor forward IP datagrams containing private addresses to via external routers.
- Hosts having only a private IP address do not have IP-layer connectivity to the Internet. This may be desirable and may even be a reason for using private addressing. All connectivity to external Internet hosts must be provided with circuit level gateways or application gateways.

IP Configuration Parameters

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server

IP Address

- Identifies the computer/host
- Either assigned/configured statically by the administrator or
- May be assigned dynamically through DHCP

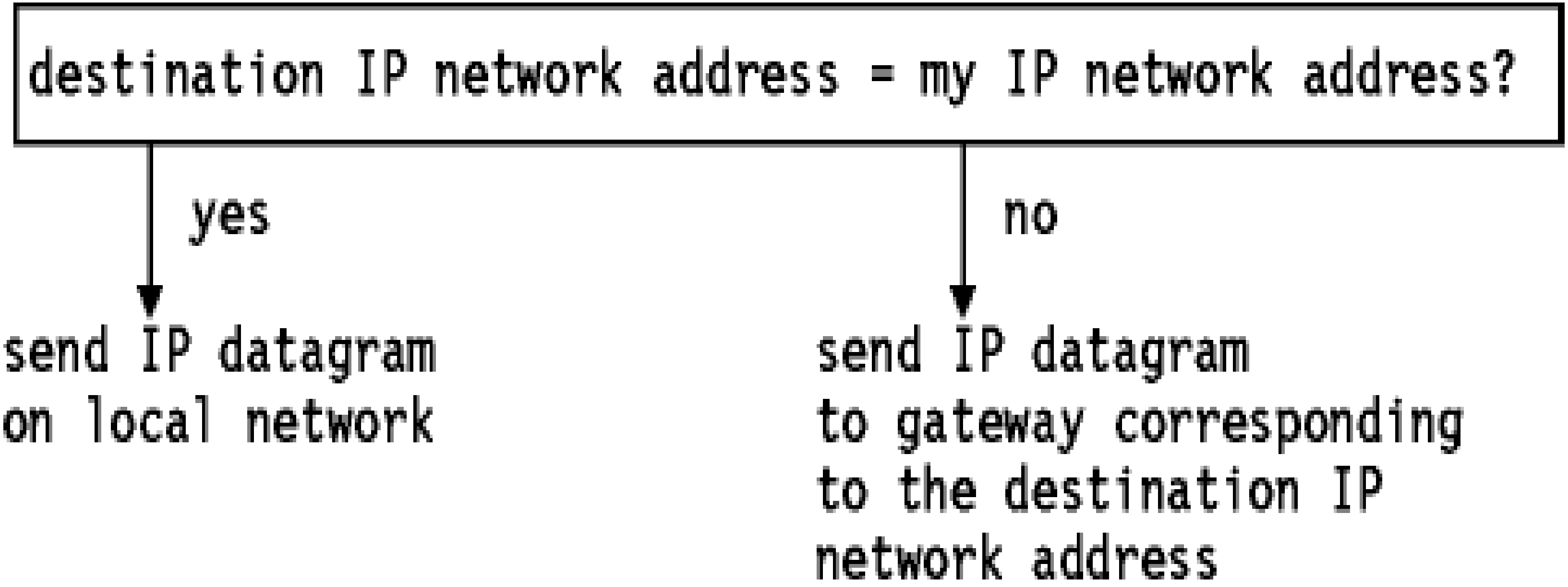
Subnet Mask

- 32 bit integer, like the IP address
- Indicates the size of the subnet
- Used to generate Network Address
- IP address and Subnet Mask are logically ANDed to produce the Network ID of the source and detination

Default Gateway

- The Way Out of the Subnet
- Router

How IP Operates at a Host



destination IP network address = my IP network address?

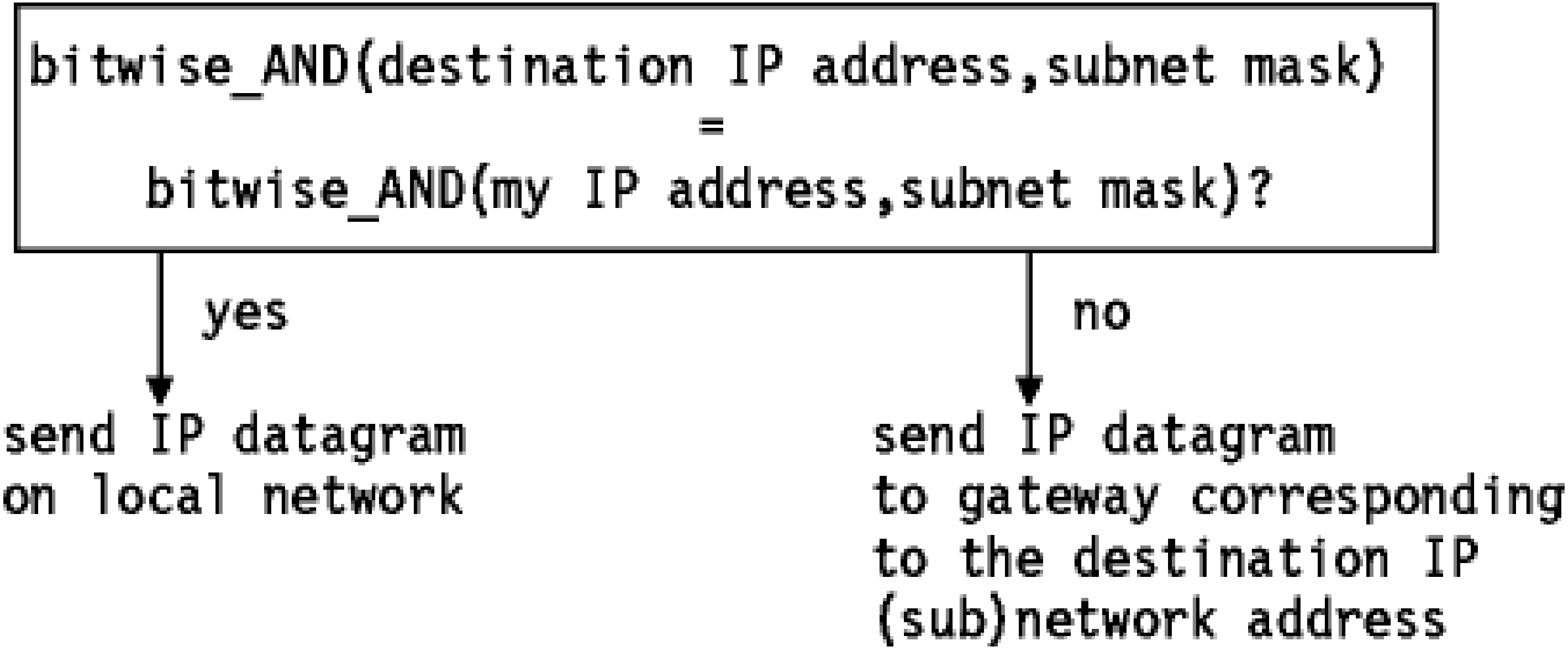
yes

no

send IP datagram on local network

send IP datagram to gateway corresponding to the destination IP network address

How IP Operates at a Host



bitwise_AND(destination IP address,subnet mask)
=
bitwise_AND(my IP address,subnet mask)?

yes

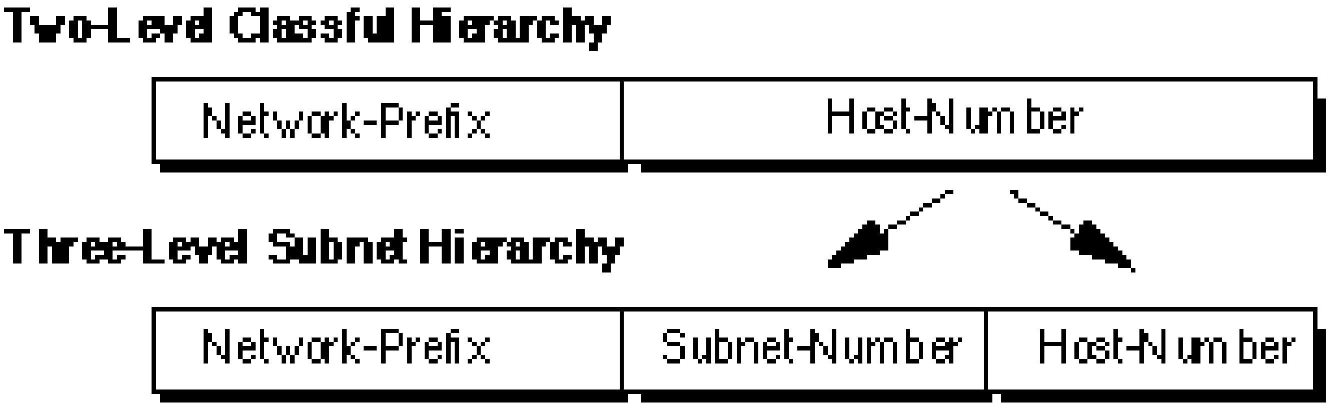
send IP datagram
on local network

no

send IP datagram
to gateway corresponding
to the destination IP
(sub)network address

Subnetting

- Subnetting -
  - In 1985, RFC 950 defined a standard procedure to support the subnetting, or division, of a single Class A, B, or C network number into smaller pieces.



Two-Level Classful Hierarchy

Network-Prefix | Host-Number

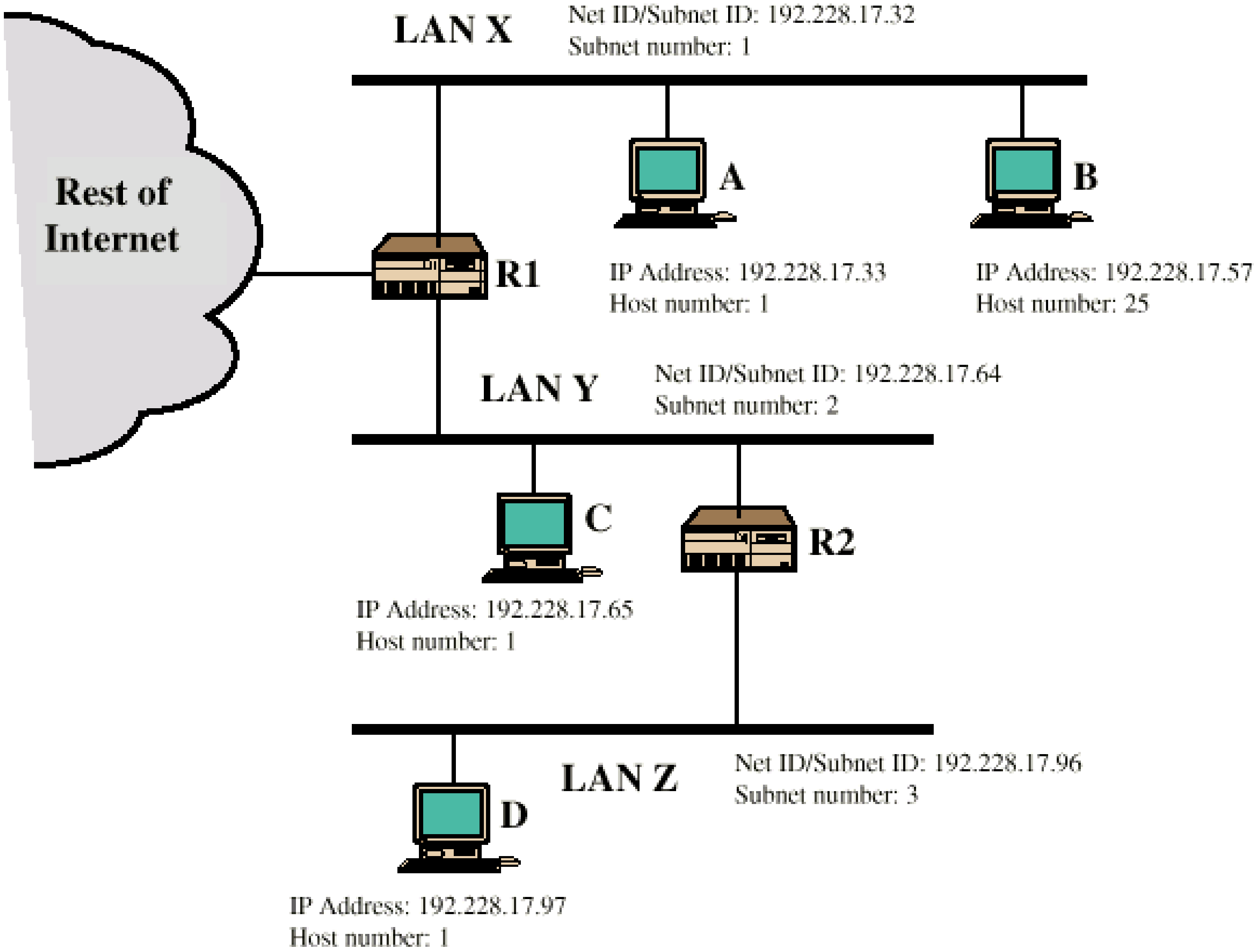
Three-Level Subnet Hierarchy

Network-Prefix | Subnet-Number | Host-Number

Subnets and Subnet Masks

- Allow arbitrary complexity of internetworked LANs within organization
- Insulate overall internet from growth of network numbers and routing complexity
- Site looks to rest of internet like single network
- Each LAN assigned subnet number
- Host portion of address partitioned into subnet number and host number
- Local routers route within subnetted network
- Subnet mask indicates which bits are subnet number and which are host number

Routing Using Subnets


LAN X
Net ID/Subnet ID: 192.228.17.32
Subnet number: 1
Rest of Internet
R1
A
B
IP Address: 192.228.17.33
Host number: 1
IP Address: 192.228.17.57
Host number: 25
LAN Y
Net ID/Subnet ID: 192.228.17.64
Subnet number: 2
C
R2
IP Address: 192.228.17.65
Host number: 1
LAN Z
Net ID/Subnet ID: 192.228.17.96
Subnet number: 3
D
IP Address: 192.228.17.97
Host number: 1

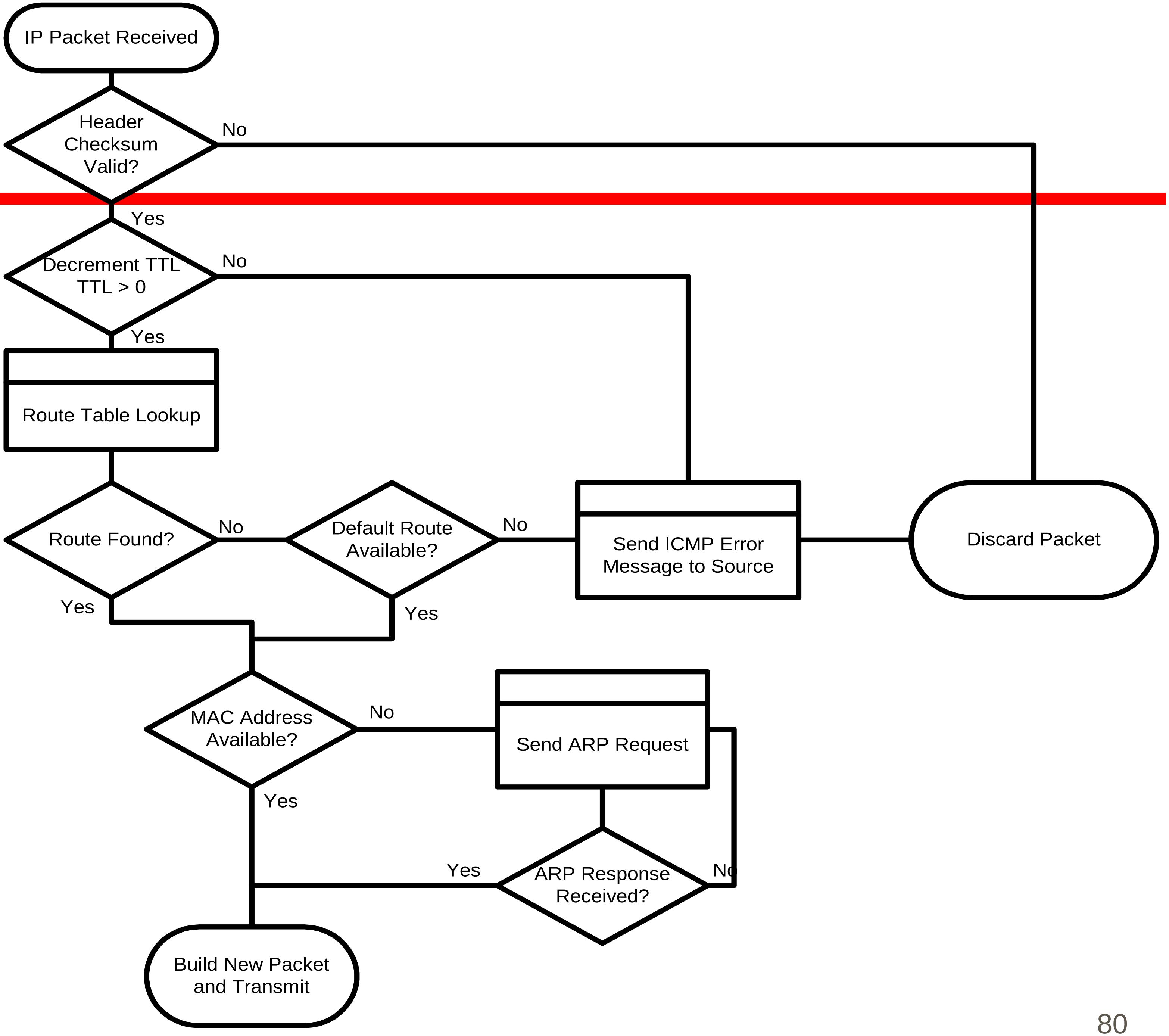
Practice with Subnets - 1

- The IP address of a host is 140.128.34.79. The subnet mask is 255.255.255.192. What is the IP broadcast address for the network that this host is attached to?

Practice with Subnets - 2

- Acme Incorporated, a fictional company that you work for, has been allocated a class B network by the InterNIC. Acme's network number is 135.48.0.0. You are the network administrator for Acme's WAN. Acme has offices in 12 different cities with the head office located in Utopia. Each of the 11 branch offices is connected to the head office with a leased line with IP routers on both ends. The maximum number of computers in any branch office or head office is 1500. Show how you would subnet the Class B IP address space of Acme to accommodate all the offices. Indicate, in the form of a table, for each of the subnet, IP address range for subnet, the subnet network number, the broadcast address and the subnet mask to be used.

IP Forwarding



IP Packet Received

Header Checksum Valid?

No

Yes

Decrement TTL
TTL > 0

No

Yes

Route Table Lookup

Route Found?

No

Yes

Default Route Available?

No

Yes

Send ICMP Error Message to Source

Discard Packet

MAC Address Available?

No

Yes

Send ARP Request

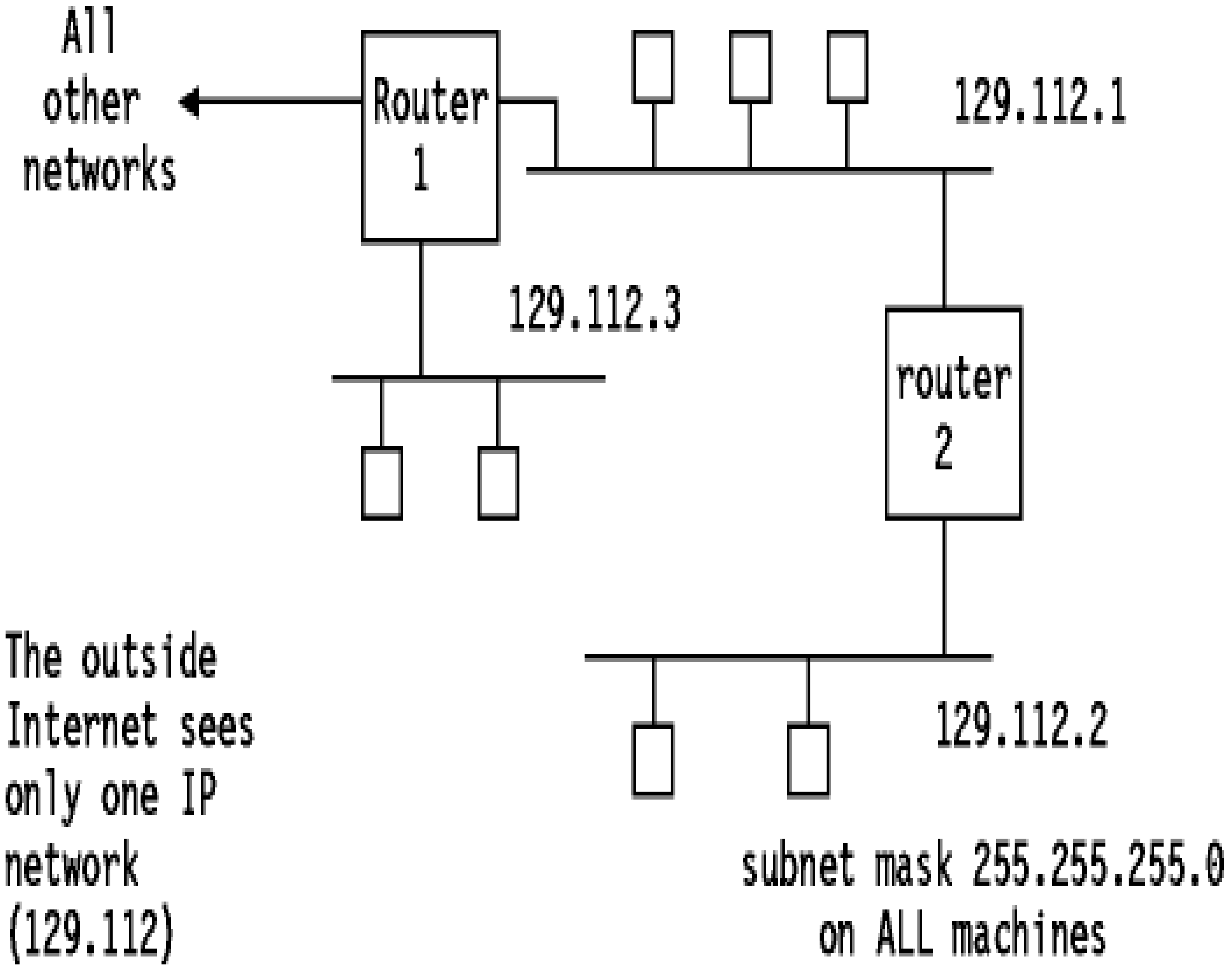
ARP Response Received?

Yes

No

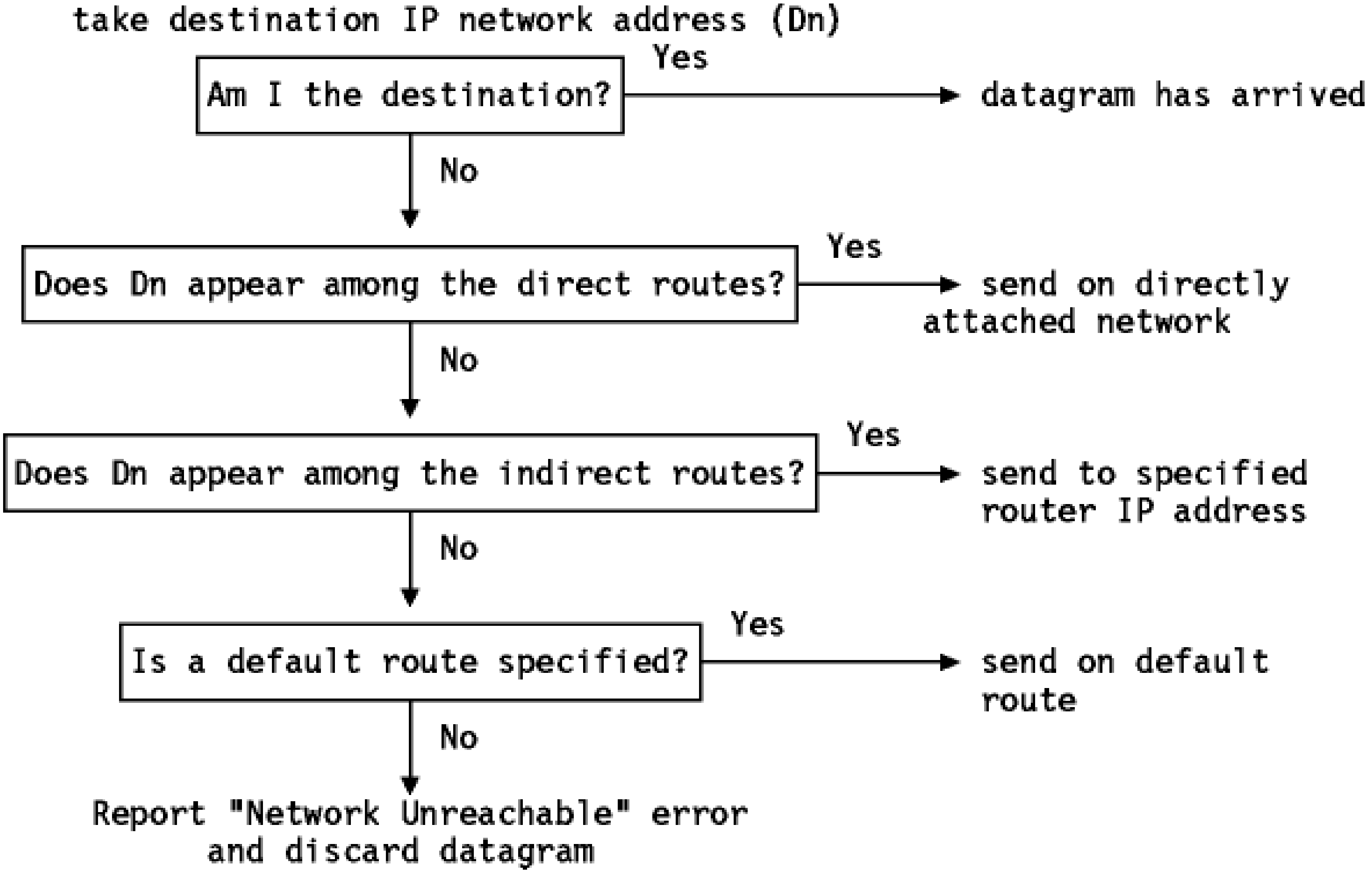
Build New Packet and Transmit

How IP Operates


All other networks
Router 1
129.112.1
129.112.3
router 2
129.112.2
The outside Internet sees only one IP network (129.112)
subnet mask 255.255.255.0 on ALL machines

- *Figure: A Subnet Configuration* - Three physical networks form one IP network. The two routers are performing slightly different tasks. Router 1 is acting as a router between subnets 1 and 3 and as a router between the whole of our network and the rest of the internet. Router 2 acts only as a router between subnets 1 and 2.

IP Routing Algorithm at a Router



take destination IP network address (Dn)

Am I the destination? — Yes → datagram has arrived

No

Does Dn appear among the direct routes? — Yes → send on directly attached network

No

Does Dn appear among the indirect routes? — Yes → send to specified router IP address

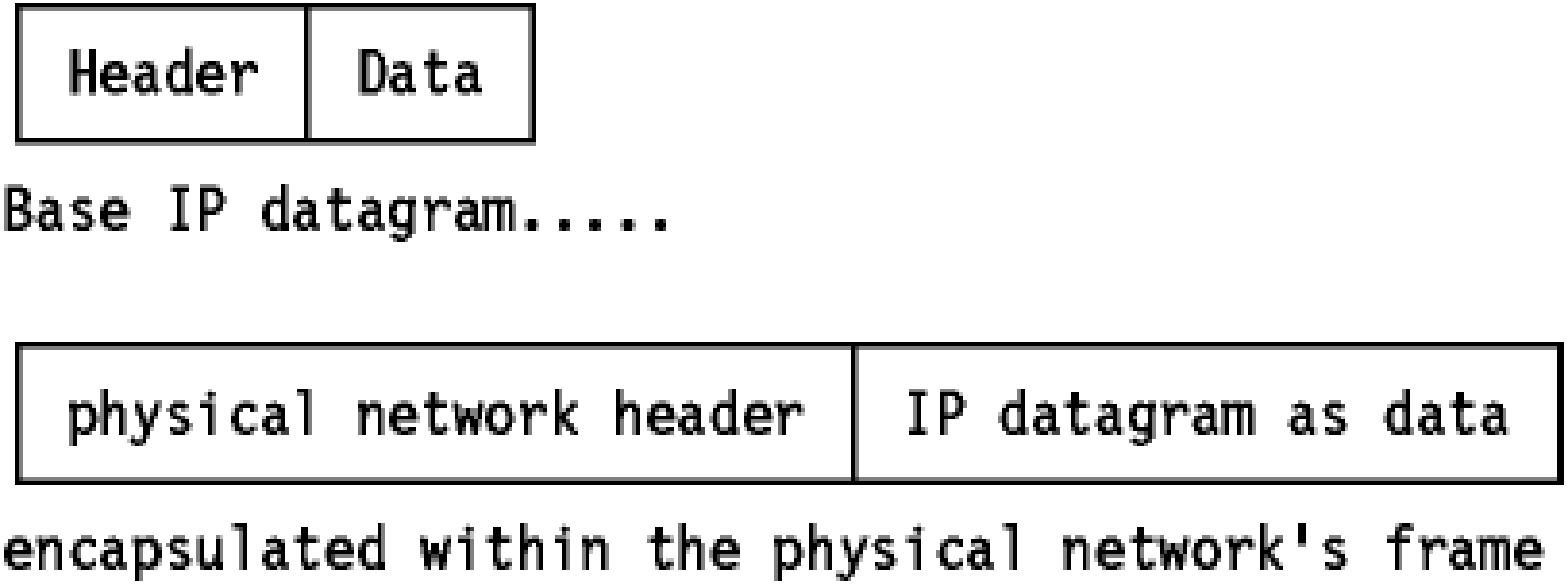
No

Is a default route specified? — Yes → send on default route

No

Report "Network Unreachable" error and discard datagram

IP Datagram Encapsulation



Header | Data

Base IP datagram.....

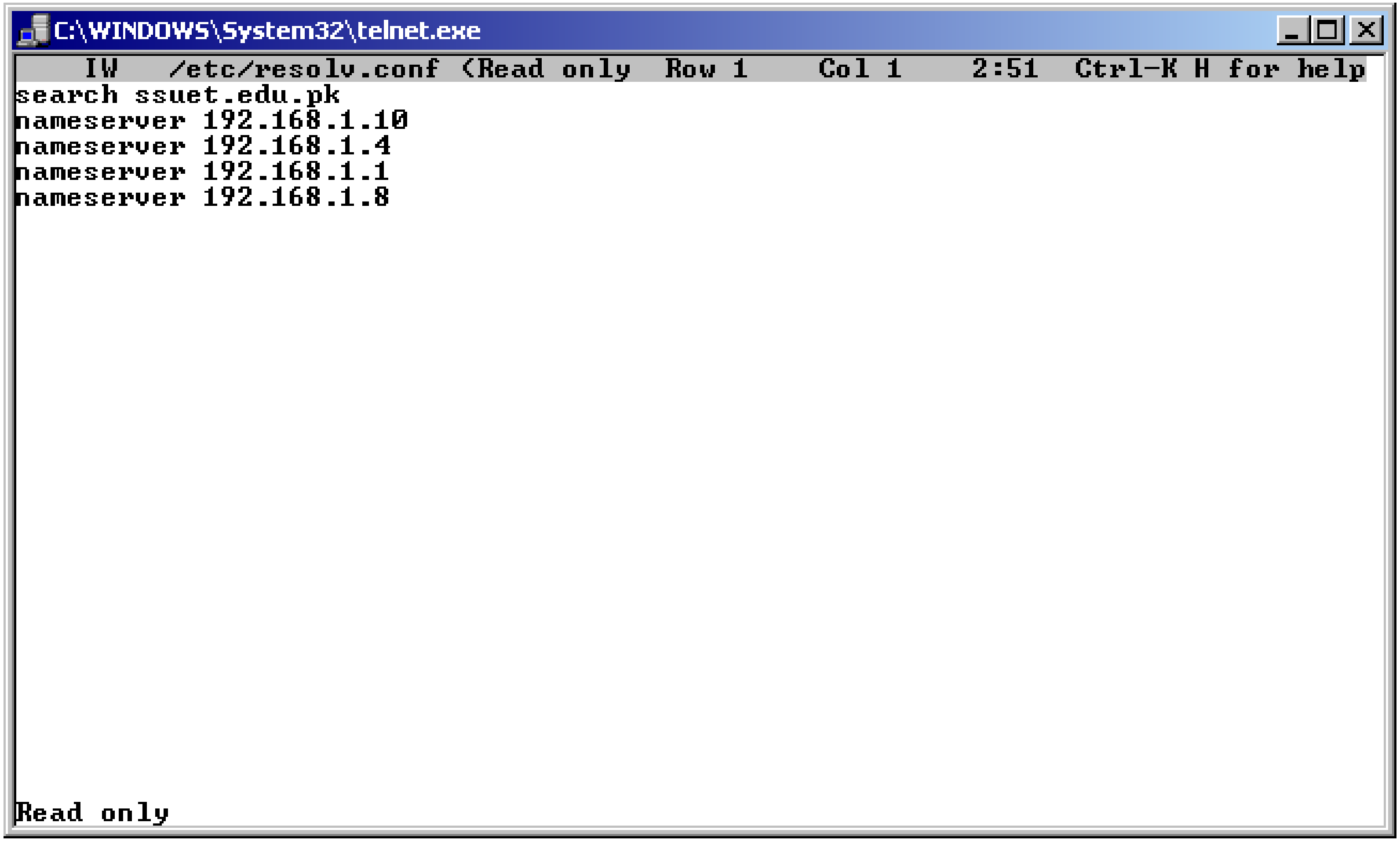
physical network header | IP datagram as data

encapsulated within the physical network's frame

DNS Server

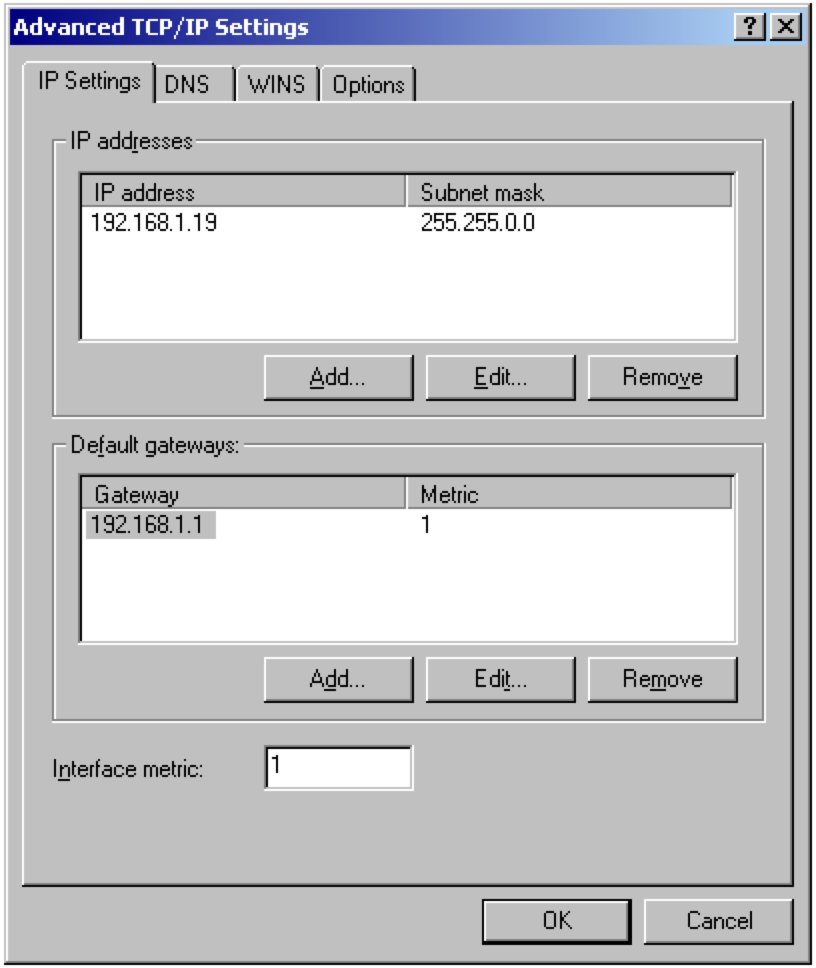
- DNS is a TCP/IP Service operational on a network to convert human-friendly host names to actual IP addresses
- The DNS client software is part of the TCP/IP implementation of all hosts
- The DNS Server software is running on hosts designated as DNS Servers

DNS Configuration on a UNIX Host - /etc/resolv.conf



```
    IW    /etc/resolv.conf (Read only   Row 1      Col 1      2:51    Ctrl-K H for help
search ssuet.edu.pk
nameserver 192.168.1.10
nameserver 192.168.1.4
nameserver 192.168.1.1
nameserver 192.168.1.8









Read only
```

TCP/IP Configuration on a Windows NT Host



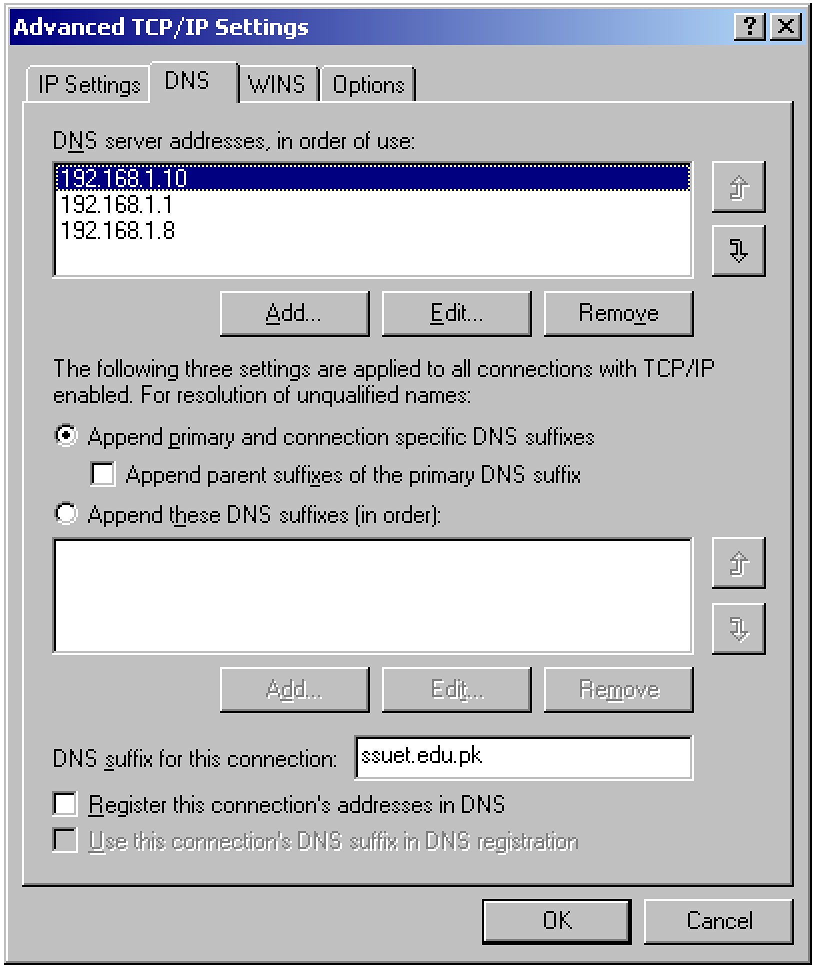
IP addresses

IP address	Subnet mask
192.168.1.19	255.255.0.0

Default gateways:

Gateway	Metric
192.168.1.1	1

Interface metric: 1



DNS server addresses, in order of use:

192.168.1.10
192.168.1.1
192.168.1.8

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

□ Append parent suffixes of the primary DNS suffix

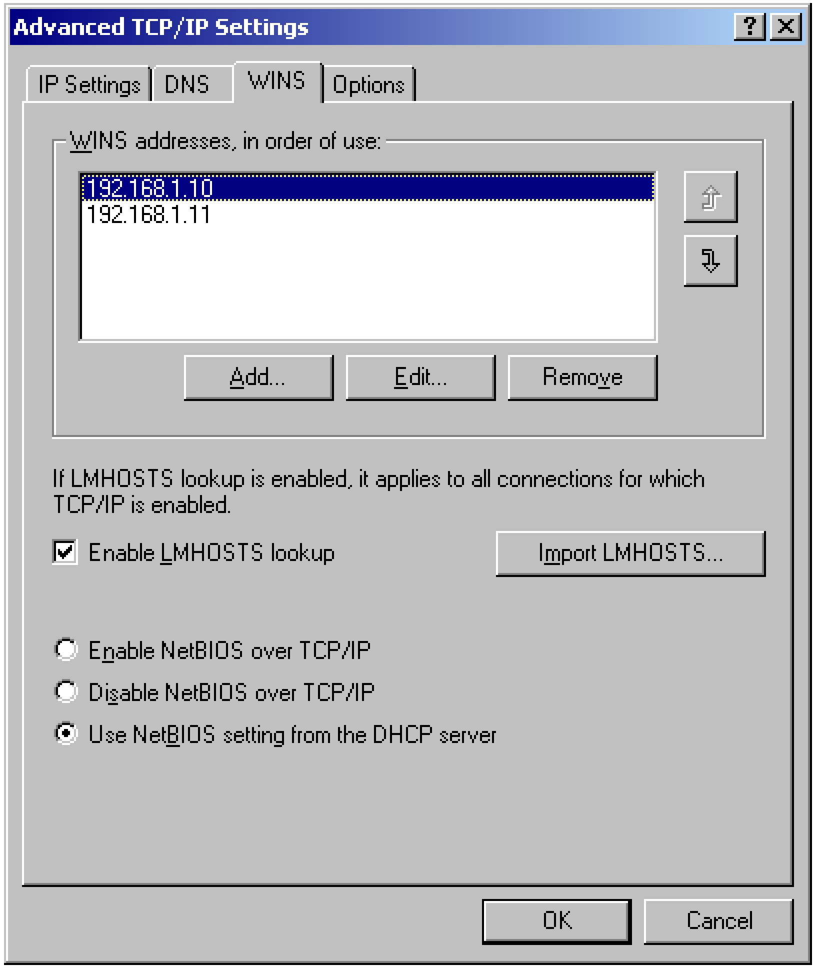
○ Append these DNS suffixes (in order):

DNS suffix for this connection: ssuet.edu.pk

□ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

TCP/IP Configuration on a Windows NT Host



Advanced TCP/IP Settings

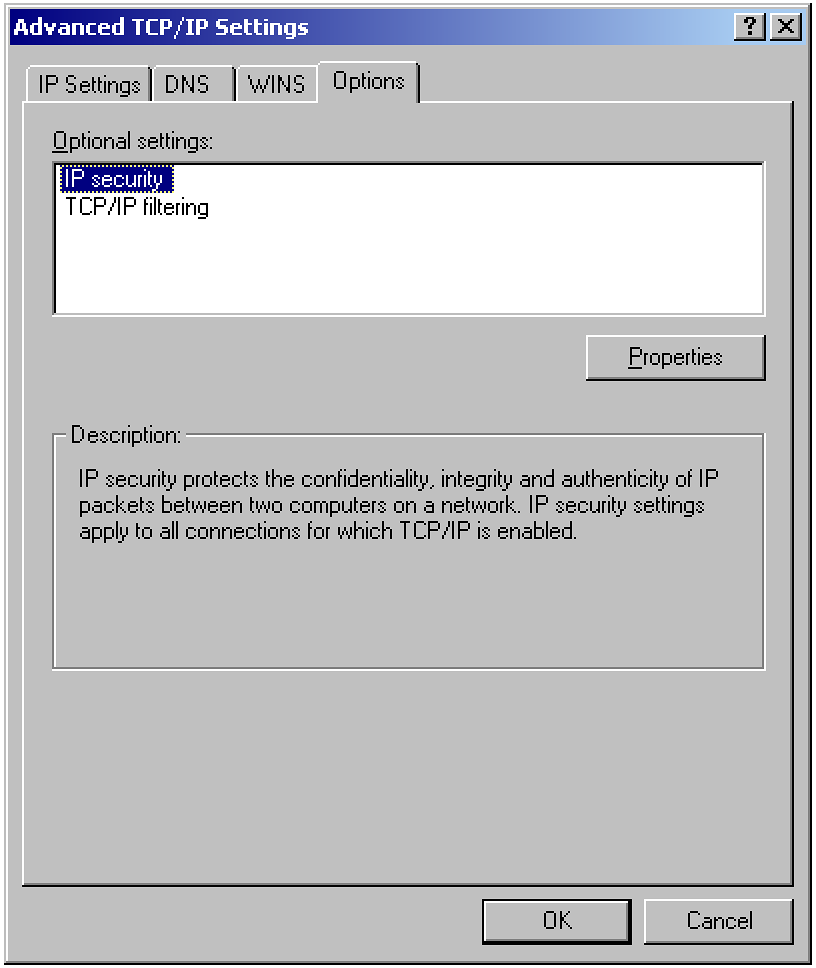
WINS addresses, in order of use:

192.168.1.10
192.168.1.11

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

○ Enable NetBIOS over TCP/IP
○ Disable NetBIOS over TCP/IP
● Use NetBIOS setting from the DHCP server



Advanced TCP/IP Settings

Optional settings:

IP security
TCP/IP filtering

Description:

IP security protects the confidentiality, integrity and authenticity of IP packets between two computers on a network. IP security settings apply to all connections for which TCP/IP is enabled.

Address Resolution

- To send a datagram to a certain IP destination, the target IP address must be translated or mapped to a physical address.
- This may require transmissions on the network to find out the destination's physical network address.
- For example, on LANs the Address Resolution Protocol, discussed in Address Resolution Protocol (ARP), is used to translate IP addresses to physical MAC addresses.

What’s wrong with IP V4?

- Addressing
  - Current addressing scheme allows for over 2 million networks, but most are Class “C” which are too small to be useful
  - Most of the Class “B” networks have already been assigned
- Quality of Service
  - IPv4 does not implement QoS functionality

What’s wrong with IP V4?

- Security
  - IP packets can be easily snooped from the network
  - No standard for authentication of the user to a server
  - No standard for encryption of data in packets
- Packet Size
  - Maximum packet size is 216 – 1 (65,535)
  - May be too small considering newer, faster networks

IPv6 Solutions

- Addressing
  - Addresses now 128 bits long (3.4 x 10^{34} addresses)
    - Theoretically yields 665,570,793,348,866,943,898,599 IP addresses per square meter of the earth’s surface.
    - Routing analysis shows practical values between 1564 and 3,911,873,538,269,506,102 IP addresses per square meter
  - Address auto-configuration
- Quality of Service
  - Flow control and QoS options allow for better connections of high bandwidth and high reliability applications

IPv6 Solutions Cont.

- Security
  - Extension headers allow for standard encryption of data and standard authentication of users to hosts
- Packet Size
  - Extension headers allow for larger packets