UMKB/Computer Science Department/M1RTIC

(2023/2024)

Advanced Networks 2

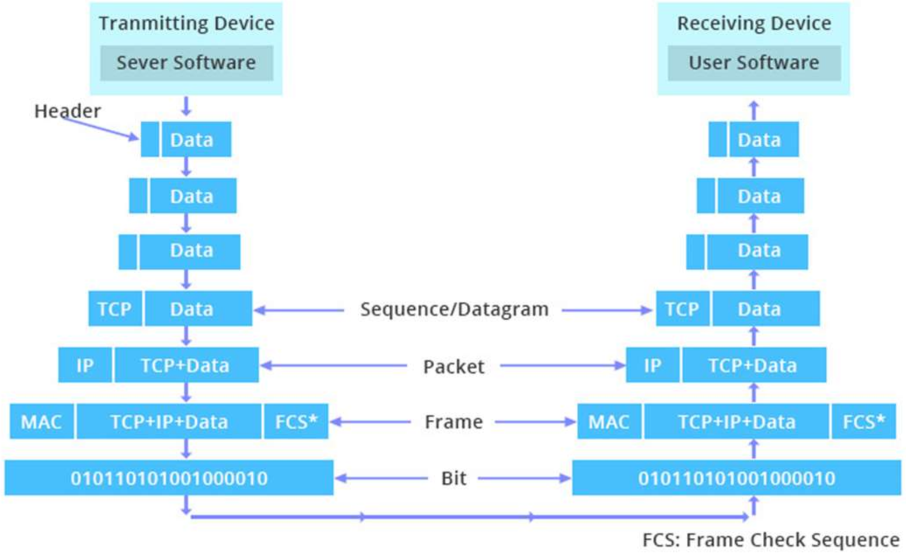
Dr. AYAD Soheyb

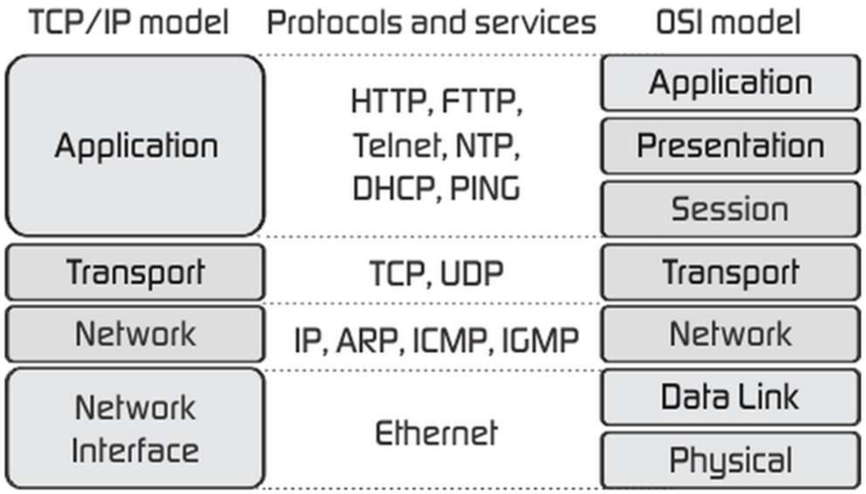
V 1.1

Content

- IPv4 (Reminder)
- Routing Protocols
- IPv6
- IPv4 & IPv6 coexistence
- Mobile IP
- NDN (Named Data Networking)

Reminder





TCP/IP model	Protocols and services	OSI model
Application	HTTP, FTTP, Telnet, NTP, DHCP, PING	Application Presentation Session
Transport	TCP, UDP	Transport
Network	IP, ARP, ICMP, IGMP	Network
Network Interface	Ethernet	Data Link Physical

Network/Internet Layer

IP protocol

Role 1: Route data packets between devices across different networks.

Role 2: Uses IP addresses to uniquely identify devices on the network.

Types of IP addresses:

IPv4: 32-bit addresses (e.g. 192.168.1.1).

IPv6: 128-bit addresses (e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Features: Best effort ! No mechanism to guarantee reliability.

Connectionless: No prior connection establishment between hosts before sending data.

How it works: Divides data into packets to route them across the network based on a source address and a destination address in the header of the packet.

Network/Internet Layer

Reliability in the IP protocol

IP protocols are considered “unreliable”. This does not mean that they do not send data correctly over the network, but that they do not offer any guarantees for the packets sent regarding the following:

- data corruption.
- order of arrival of packets (packet A may be sent before packet B, but packet B may arrive before packet A)
- packet loss or destruction
- packet duplication

Network/Internet Layer

Reliability in the IP protocol

- In terms of reliability, the only service offered by an IP protocol is to ensure that transmitted packet headers are not wrong (error) through the use of checksums.

- If a packet's header includes an error, its checksum will be invalid and the packet will be destroyed without being transmitted. If a packet is destroyed, no notification is sent to the sender.

- **Reliability is delegated to higher-level protocols. The main reason is to reduce the level of complexity of routers in order to allow them to have greater speed.**

Internet Protocol version 4
IPv4

- **IPv4** is the first version of Internet Protocol (IP) to be widely deployed, and which still forms the basis of the majority of communications on the Internet in 2024, compared to **IPv6.**

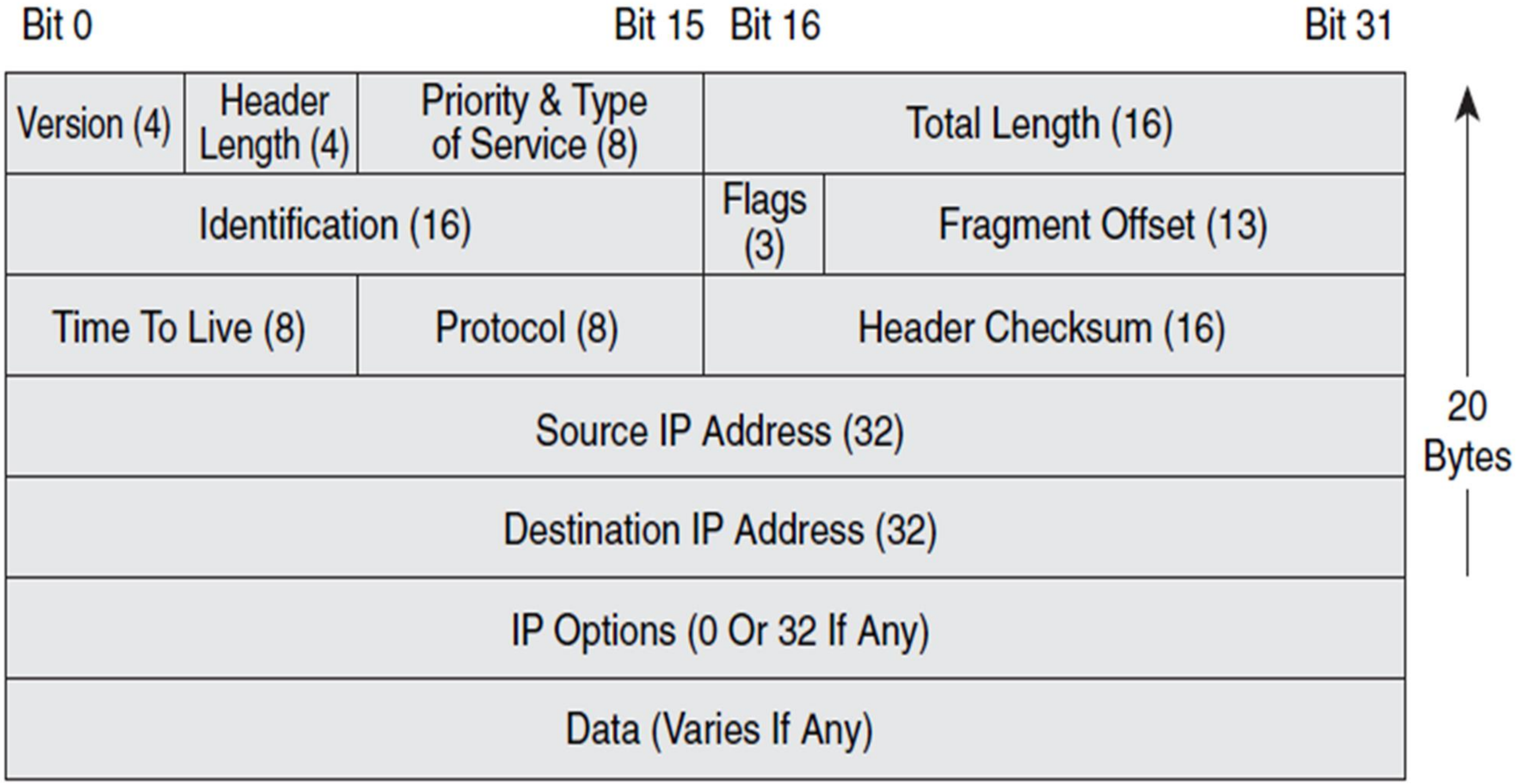
- It is described in **RFC 791** of September 1981, replacing RFC 760, defined in January 1980.

- Versions 1 to 3 **(IPv1, IPv2 and IPv3)** of the protocol remained experimental. They were used between 1977 and 1979. IEN notes (Internet Experiment Notes) describe these versions of the protocol prior to the modern IPv4 version.

- The **IPv5** protocol is an experimental version used as part of the study of the Internet Stream Protocol, a protocol itself is experimental.

- The first field of an IP protocol packet is made up of 4 bits which indicate the version of the protocol used. The value 0100 (4 in binary) is used for IPv4, 0110 (6 in binary) for IPv6. The value 0101 (5 in binary) is used for the Internet Stream Protocol.

IP protocol header



Bit 0 Bit 15 Bit 16 Bit 31

Version (4) | Header Length (4) | Priority & Type of Service (8) | Total Length (16)

Identification (16) | Flags (3) | Fragment Offset (13)

Time To Live (8) | Protocol (8) | Header Checksum (16)

Source IP Address (32)

Destination IP Address (32)

IP Options (0 Or 32 If Any)

Data (Varies If Any)

20 Bytes

IP protocol header

Version = Version d’IP

Header Length = Longueur de l’entête IP (en mots de 32 bits), La valeur est comprise entre 5 et 15, car il y a 20 octets minimum et on ne peut dépasser 40 octets d'options.

Priority & Type of Service = de 8 bits utilisé da pour spécifier la priorité et le traitement que doivent recevoir les paquets de données pendant leur acheminement à travers le réseau. Bien qu'il soit principalement destiné à la gestion de la qualité de service (QoS), il est peu utilisé dans les réseaux modernes, car d'autres mécanismes, comme le **DiffServ (Differentiated Services)**, ont pris le relais.

Il se décline au fil des RFC. Au départ (RFC 791) -> En septembre 2001 (RFC 3168)

Bits 0-2: Priority.
Bit 3: 0 = Normal Delay, 1 = Low Delay.
Bits 4: 0 = Normal Throughput, 1 = High Throughput.
Bits 5: 0 = Normal Reliability, 1 = High Reliability.
Bit 6-7: Reserved for Future Use.

IP protocol header

Total Length = Nombre total d'octets du datagramme, en-tête IP comprise.

Identification= Numéro permettant d'identifier les fragments d'un même paquet.

Flags =

Bit 1 : actuellement inutilisé.

Bit 2 : DF (Don't Fragment) lorsque ce bit est positionné à 1, il indique que le paquet ne peut pas être fragmenté. Si le routeur ne peut acheminer ce paquet (taille du paquet supérieure à la MTU Maximum transmission unit), il est alors rejeté.

Bit 3 : MF (More Fragments) quand ce bit est positionné à 1, on sait que ce paquet est un fragment de données et que d'autres doivent suivre. Quand il est à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

Fragment Offset = Position du fragment par rapport au paquet de départ.

IP protocol header

Time To Live (TTL)= Ce champ indique le nombre maximal de routeurs a travers lesquels la trame peut passer. Ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit la trame. Cela évite l'encombrement du réseau.

Protocol = Ce champ indique quel protocole est utilisé
Quelques protocoles transportés :

1 = ICMP   8 = EGP
2 = IGMP   11 = GLOUP
4 = IP   (encapsulation)   17 = UDP
5 = Stream   36 = XTP
6 = TCP   46 = RSVP

Header Checksum = Ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de la trame.

Adresse IP source = Ce champ représente l'adresse IP de la machine émettrice.

Adresse IP destination = Adresse IP du destinataire du message.

IPv4 addressing

- To facilitate the routing of packets through a network, the IPprotocol set uses a logical address called an IP address (RFC 791).

- This IP address is encoded on 32 bits. Maximum 4,294,967,296 addresses.

1010100111000111010001011000100

↓

10101001   11000111   01000101   10001001

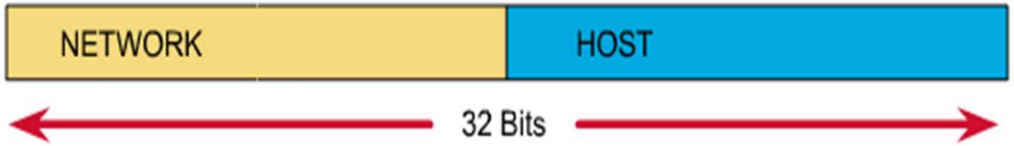
- We represent each byte of an IPv4 address using a dotted decimal (this is called “dotted decimal notation”).

```
10101001  11000111  01000101  10001001
   169   .   199   .   69    .  137
```

Components of an IPv4 address

An IP address has two portions:

- Network
- Host



These two portions can be combined to constitute three types of address:

Network address: the address that refers to the network. All bits of the host part are set to 0

Broadcast address: a specific address, used to send data to all hosts on the network. All bits of the host part are 1

Host addresses: Addresses assigned to devices on the network. The bits of the host part are formed by 0s and 1s (not all 0, not all 1)

How to precise the portions ?

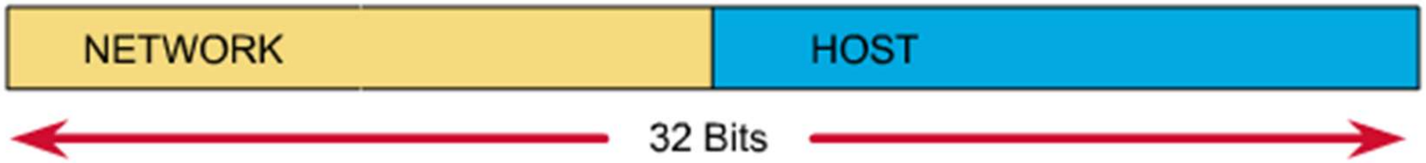
Network mask

The network mask allows to define:

- The portion associated to the network in an IP address
- The portion associated to the hosts

A sequence of 1s followed by a sequence of 0s

- The 1s are associated with the network portion
- The 0s are associated with the host portion



11111111111111110000000000000000

Note: the length of the prefix corresponds to the number of 1 bits in the subnet mask

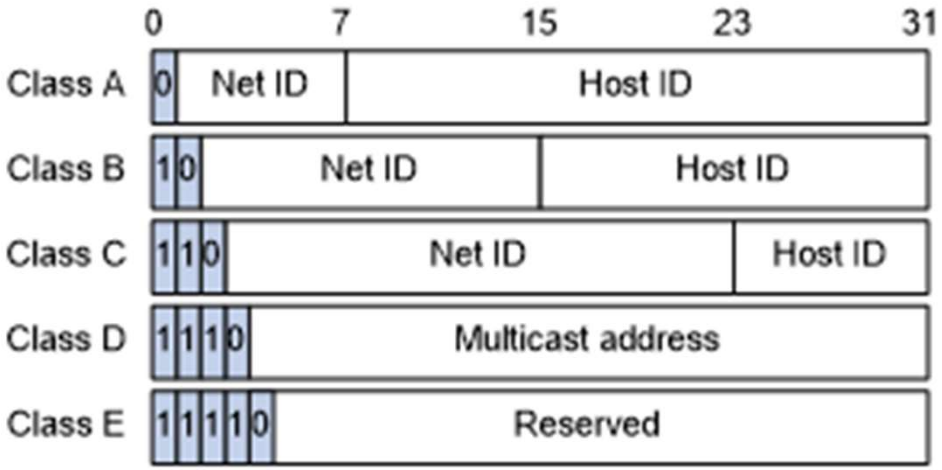
```
Example :
/16 ➔ 11111111 11111111 00000000 0000000➔ 255.255.0.0
```

IP address classes

Assigning IP addresses to classes is known as classful addressing. The classes were determined by the IANA (Internet Assigned Numbers Authority).

Each IP address is divided into a network ID and the host ID. Furthermore, a bit, or a sequence of bits, located at the start of each address, determines the class of the address.

Address classes allow addressing to be adapted according to the size of the network.



Class A

- The Class A address uses only the first byte (8 bits) of the 32-bit number to indicate the network address.

- The remaining three bytes of the 32-bit number are used for host addresses. The first bit of a class A address is always "0".

- Since the first bit is 0, the smallest number that can be represented is 00000000 (decimal value 0), and the largest number that can be represented is 01111111 (decimal value 127).

- However, these two network numbers, 0 and 127, are reserved and cannot be used as network addresses.

- Any address starting with a value between 1 and 126 in the first byte of the 32-bit number is a Class A address.

Class B

- The Class B address uses two of four bytes (16 bits) to indicate the network address.
- The remaining two bytes are used for host addresses.
- The first two bits of the first byte of a class B address are always 10 in binary.
- The remaining six bits on the first byte can be 1s or 0s. Thus, the smallest number that can be represented with a class B address is 10000000 (decimal value 128), and the largest number that can be represented is 10111111 (decimal value 191).
- Any address starting with a value between 128 and 191 in the first byte is a class B address.

Class C

- In a Class C address, the first three bytes (24 bits) of the IP address identify the network portion, and the remaining byte is reserved for the host portion.

- A class C address begins with 110 in binary.

- So, the smallest number that can be represented is 11000000 (decimal value 192), and the largest number that can be represented is 11011111 (decimal value 223).

- If an address contains a number between 192 and 223 in the first byte, it is a class C address.

Class D

- Class D was created to allow multicasting in an IP address.

- A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses.

- Therefore, a single station can transmit a single datagram flow to multiple destinations simultaneously. Class D, like other address categories, is mathematically limited.

- The first 4 bits of a Class D address must be 1110. Therefore, the first byte range for Class D addresses is 11100000 to 11101111, or 224 to 239

- An IP address that begins with a value between 224 and 239 in the first octet is a class D address. This is also called IGMP

- Class D address range is between 224.0.0.0 and 239.255.255.255

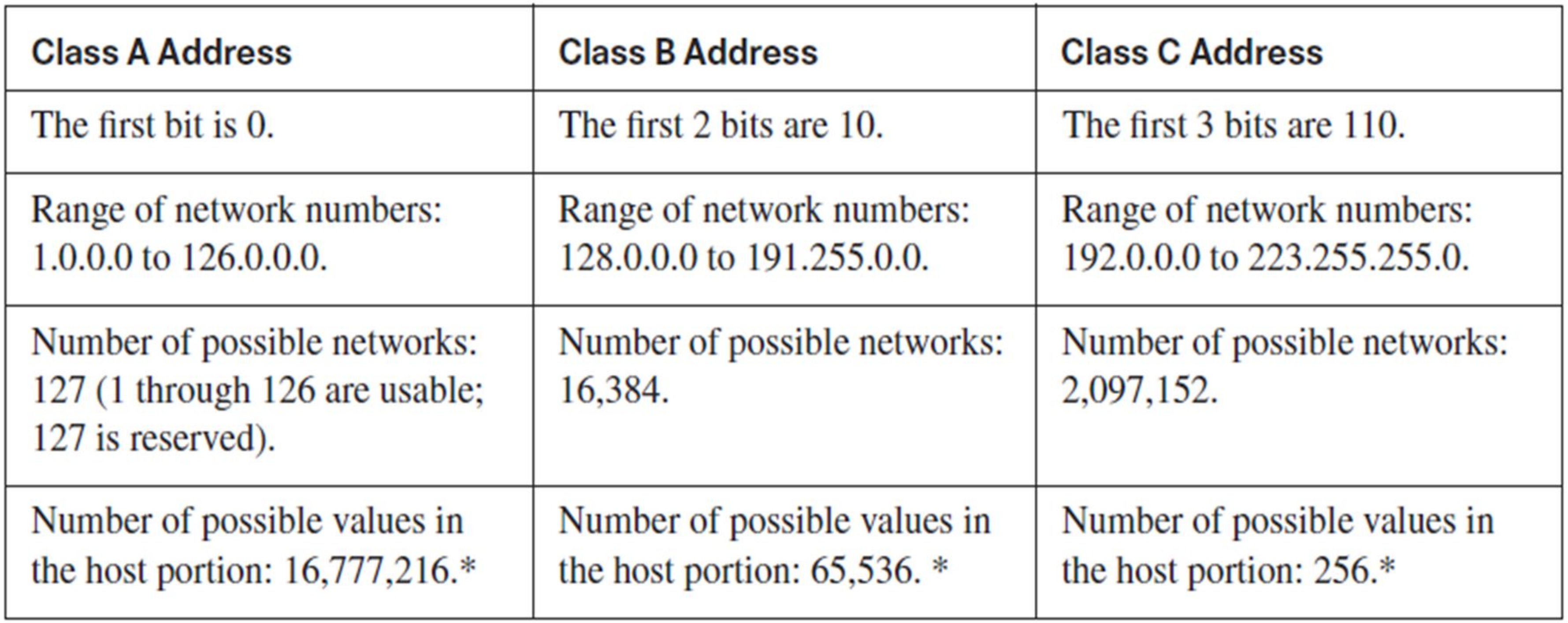
Class E

- Although Category E has been defined, the Internet Engineering Task Force (IETF) reserves addresses in this class for its own research.

- Therefore, no Class E addresses have been released for use in the Internet.

- The first 4 bits of a class E address are always 1111, so the first byte range for class E addresses is 11110000 to 11111111, or 240 and 255.

IP address ranges

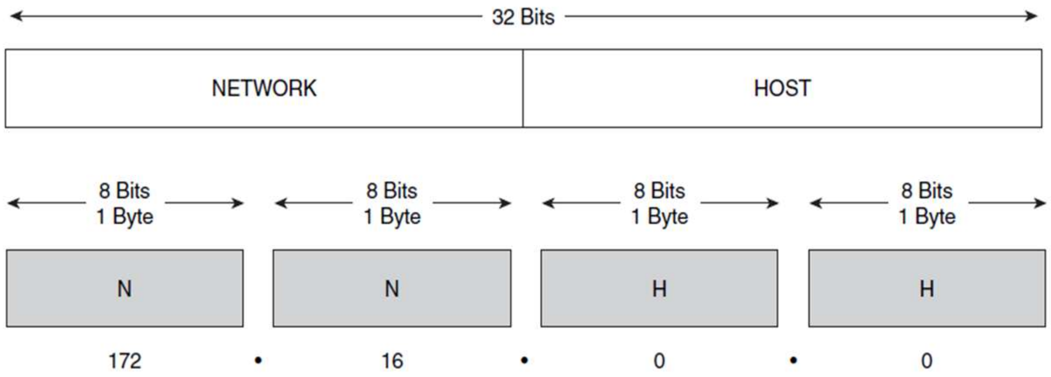


Class A Address	Class B Address	Class C Address
The first bit is 0.	The first 2 bits are 10.	The first 3 bits are 110.
Range of network numbers: 1.0.0.0 to 126.0.0.0.	Range of network numbers: 128.0.0.0 to 191.255.0.0.	Range of network numbers: 192.0.0.0 to 223.255.255.0.
Number of possible networks: 127 (1 through 126 are usable; 127 is reserved).	Number of possible networks: 16,384.	Number of possible networks: 2,097,152.
Number of possible values in the host portion: 16,777,216.*	Number of possible values in the host portion: 65,536. *	Number of possible values in the host portion: 256.*

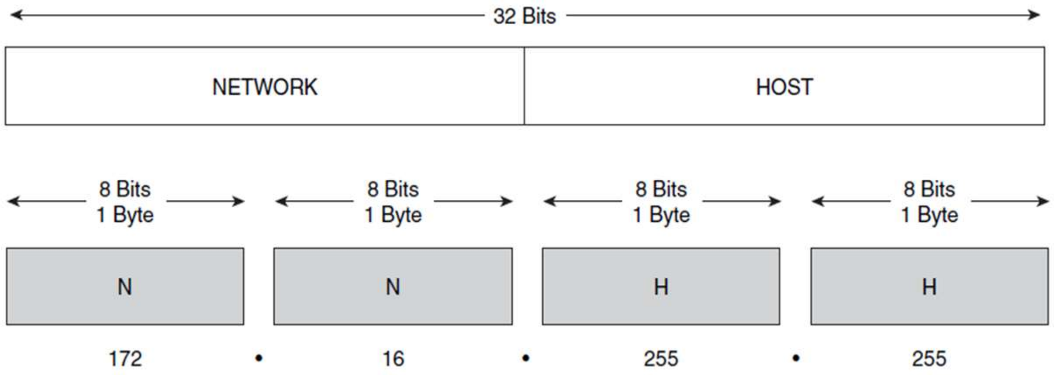
The number of usable hosts is two less than the total possible number because the host part must be non-zero and cannot be all 1s.

Reserved IP addresses

Reserved IP addresses



Network address : All bits in host part = 0



Broadcast Address: All bits in host part = 1

Network address

- **An IP address with all host bits occupied by binary 0 is reserved for the network address.**
- So, in an example Class A network, 10.0.0.0 is the IP address of the network including host 10.1.2.3.
- In an example of a Class B network, the IP address 172.16.0.0 is a network address, while 192.16.1.0 would be a Class C network.
- Help to identify the broadcast domain and routing processes.
- A router uses the network's IP address when it looks up the destination network location in its IP routing table.

Network address

The network address is calculated using the following logical equation:

Network Address = IP Address AND Subnet Mask

AND is the logical AND operator in binary, for which here is the corresponding truth table:

Table de vérité de ET ou AND		
Adresse IP	**Masque**	**Adresse réseau**
0	0	0
0	1	0
1	0	0
1	1	1

Example:

Consider the following IP address **192.168.0.10** in a class C network

Calculating the network address gives:

192.168.0.0, written in dotted decimal form.

Ip	**11000000.10101000.00000000.00001000**
ET	.
Masque	11111111.11111111.11111111.00000000
=	11000000.10101000.00000000.00000000

Directed broadcast address

- Broadcast IP addresses end with binary 1 in all the host portion of the address (the host field).

- A directed broadcast is sent to all hosts on a particular network. This type of broadcast allows a broadcast to be sent to all hosts on a network that is not local.

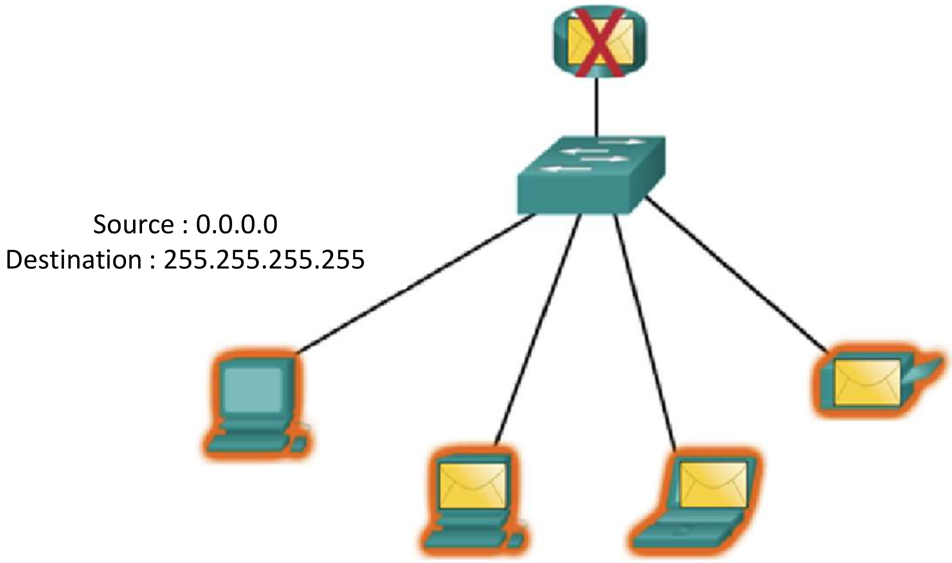
- For example, for a host outside the 172.16.4.0/24 network to communicate with all hosts on that network, the packet's destination address must be 172.16.4.255.

- Although routers do not route directed broadcasts by default, they can be configured to do so.

- **Routers in a local network use broadcast IP to send Hello packets to all endpoints, switches, and other routers to maintain network interactions and discover neighboring devices.**

Local broadcast address (limited)

- If an IP device wants to communicate with all devices on the local network, it sets the destination address to all 1s (255.255.255.255) and forwards the packet.
- Local brodcast never pass the router
- Example of use: search for a DHCP server, search for a MAC address
- We talk about broadcast domain



Local loopback address

- The loopback address is a special address used by the host to send communications to itself.

- The loopback address provides a shortcut for communication between TCP/IP applications and services (netapps) running on the same machine.

- If two services on the same host use loopback addresses instead of assigned host addresses, the lower layers of the TCP/IP protocol stack can be bypassed.

- The IP addresses pool for loopback is **127.0.0.0** to **127.255.255.255.**

APIPA windows & AVAHI linux

- These protocols allow machines to communicate, on a local network, in the absence of configuration by static address or dhcp server.

- Addresses 169.254.0.0 to 169.254.255.255 are reserved for address assignment in the above case.

Often called: the **dead network**

- These addresses are ignored by routers and cannot be used to communicate outside the local network.

Network ID

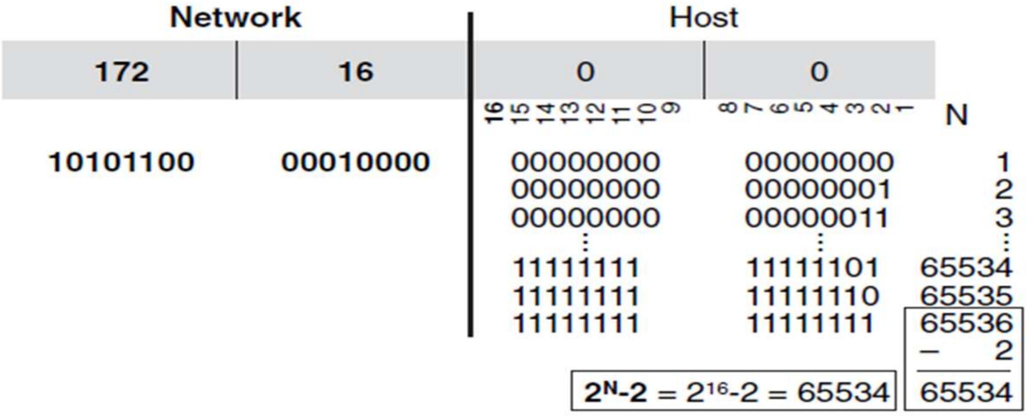
- The network part of an IP address is also called the network ID.
- It is important because most hosts on a network may only communicate directly with devices on the same network.
- If hosts need to communicate with devices that have interfaces assigned to a different network ID, there must be a network device to route data between these networks (Router, etc.).

Host ID

- Each class of a network allows a fixed number of hosts. In a Class A network, the first byte is assigned to the network, leaving the last three bytes to be assigned to the hosts.

- On a Class B network for example, the first two bytes are allocated to the network, leaving the last two bytes to be allocated to the hosts. On this type of network, the maximum number of hosts is: $2^{16} – 2 =$ 65 534.

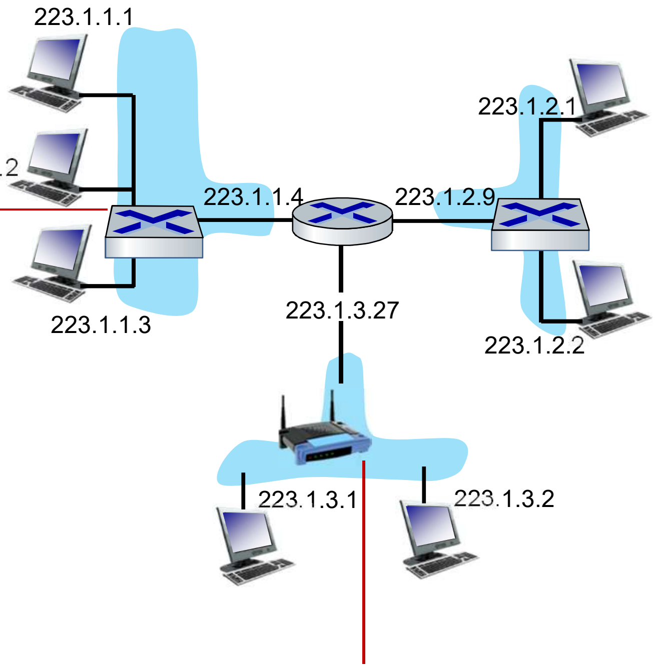
The following figure illustrates how to calculate the host addresses available on a network.



IP addressing

- IP address: 32-bit identifier associated with each host or router *interface*

Q: how are interfaces actually connected?

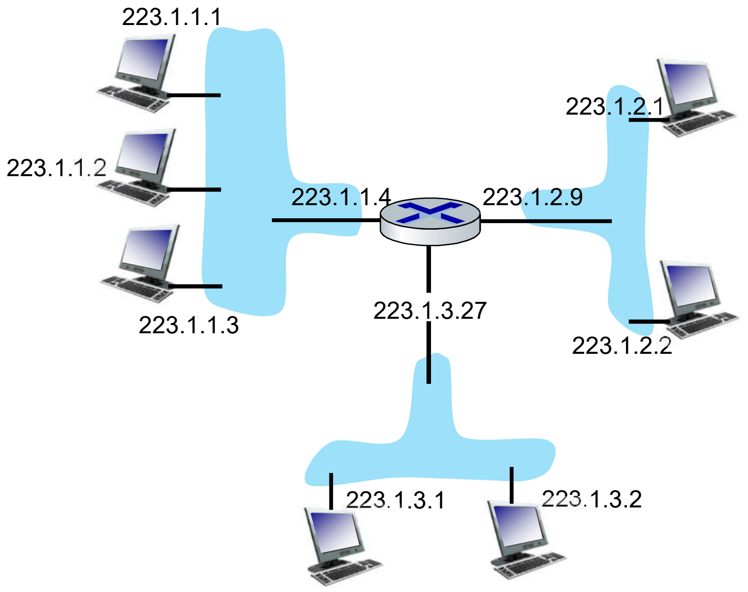


A: wired Ethernet interfaces connected by Ethernet switches

A: wireless WiFi interfaces connected by WiFi base station

Subnets

- *What's a subnet ?*
  - device interfaces that can physically reach each other without passing through an intervening router

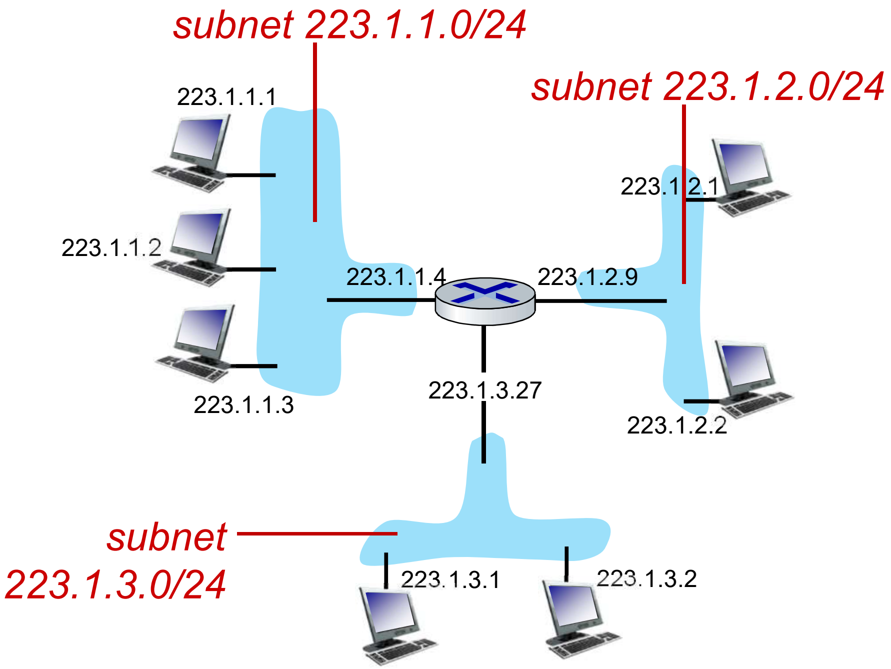


network consisting of 3 subnets

Subnets

Recipe for defining subnets:

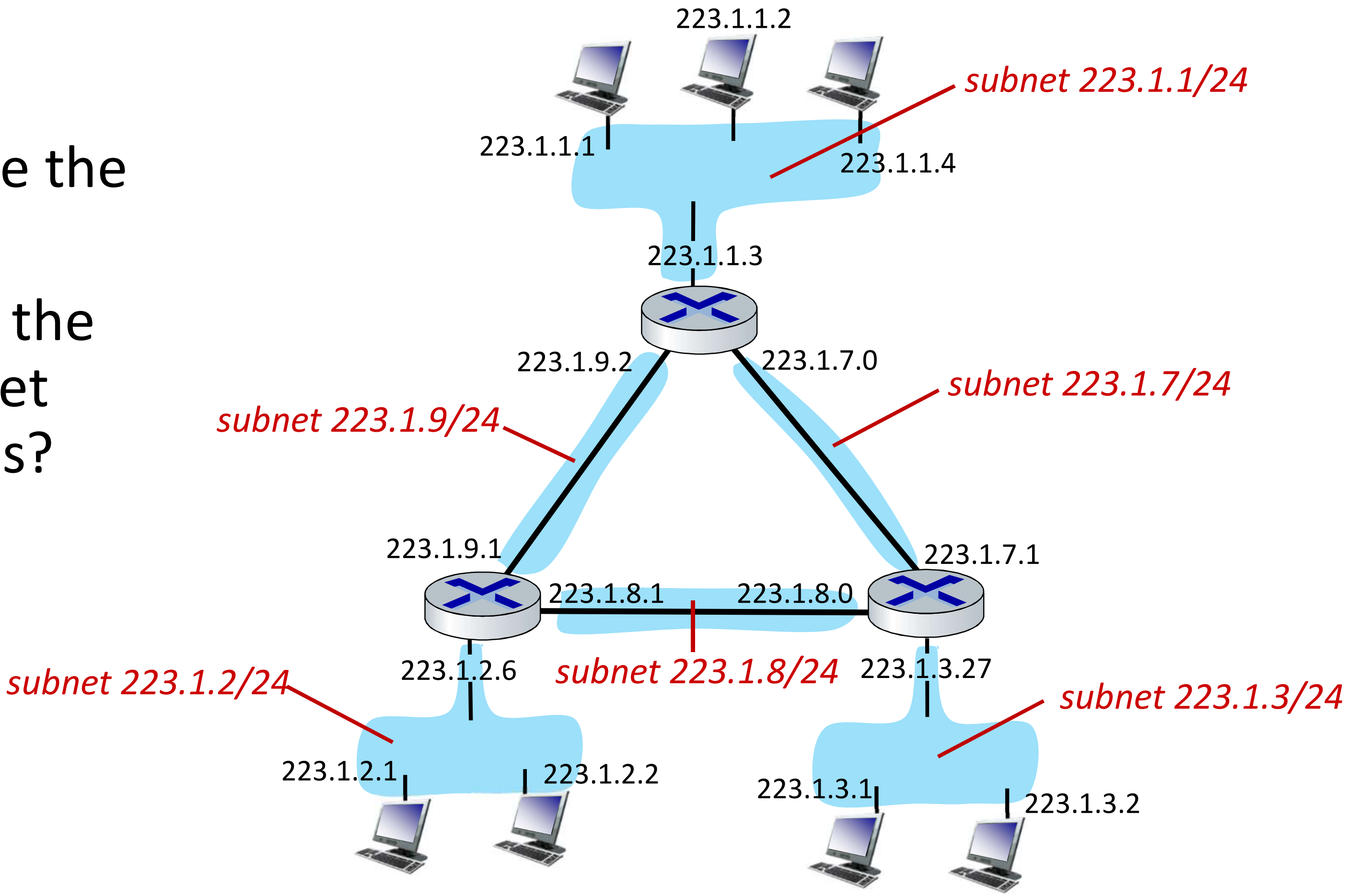
- detach each interface from its host or router, creating "islands" of isolated networks
- each isolated network is called a *subnet*



subnet mask: /24
(high-order 24 bits: subnet part of IP address)

Subnets
(classful based subnetting)

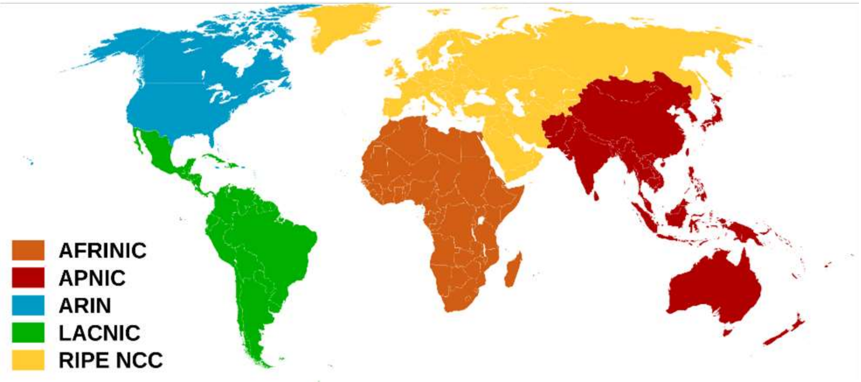
- where are the subnets?
- what are the /24 subnet addresses?



Public IP addresses

- The stability of the Internet depend directly from the uniqueness of public network addresses.
- Originally, an organization called InterNIC (Internet Network Information Center) was responsible for ensuring uniqueness of internet ip addresses . IANA (Internet Assigned Numbers Authority) succeeded it.

To obtain an IP address or block of addresses, you must contact an Internet service provider. They will then contact their appropriate regional registry with one of the following organizations:



Class	Public IP addresses
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

Private IP addresses

While Internet hosts require a globally unique IP address, private hosts that are not connected to the Internet can use any valid address as long as it is unique on the private network.

In 1994, the IETF published RFC 1597, indicating that many organizations were using TCP/IP and IP addresses, but were not connected to the Internet. The **RFC 1918** update to this document suggested that a block of available IP address space could be defined separately for private networks.

Three blocks of IP addresses (one class A network, 16 class B networks and 256 class C networks) were designed for private, internal use. Addresses in this range are not routed over the Internet backbone. Internet routers are configured to ignore private addresses.

When a network that uses private addresses needs to connect to the Internet, these private addresses must be converted to public addresses. This conversion process is the NAT system. The network device responsible for running the NAT system is usually a router.

Class	Private IP Networks	mask	Number of networks
A	10.0.0.0	/8	1
B	172.16.0.0 To 172.31.0.0	/12	16
C	192.168.0.0 To 192.168.255.0	/16	256

Limits of classful addressing

Classful assignment of IP addresses often wastes many addresses, which leads to the a lack of IPv4 addresses

For example, a company with a network of 260 hosts would need to be assigned a Class B address with more than 65,000 addresses.

Operating systems and some routing protocols still use classful addressing to assign a default mask to an address.

Solution →

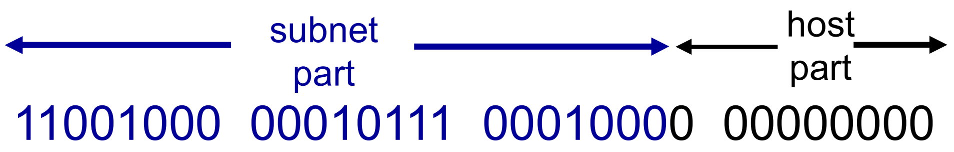
Divide the classes of IPv4 A, B or C addresses into subaddresses pools

This technique called **classless subnetting (CIDR)** was formalized in 1985 with the **RFC950** document.

IP addressing: CIDR representation

CIDR: Classless InterDomain Routing (pronounced “cider”)

- subnet portion of address of arbitrary length
- address format: a.b.c.d/x, where x is the number of bits with 1 value in the network masque (network or sub-network)



subnet part

host part

11001000 00010111 00010000 00000000

200.23.16.0/23

Subnetting

- What is subnetting?
  - Subdivision of a classful network into several subnetworks

- Interest
  - Create networks adapted to needs (number of existing machines)
  - Limit the size of broadcast domains
  - Management flexibility (connect heterogeneous architectural networks: IP Telephony, Computers, Imprements, etc.)