Network Layer in Internet

Internetworking is a scheme for interconnecting multiple networks of **dissimilar technologies**

System of interconnected networks is called an ***internetwork*** or an ***internet***

- **Repeaters** – low- level devices that just amplify or regenerate weak signals
- **Multiprotocol-routers** – existing in **n/w layer** for dissimilar networks similar to bridges
- **Transport Gateways** – used to make connection between two networks at transport layer
- **Application Gateways** – used to connect two parts of an application in application layer
- **Half Gateway** – When 2 WANs run by different organization, **gateway** is halved and connected by a wire and a neutral protocol is used.

Hub- Broadcasts data from one port to all other ports in the network.

Switch- Intelligent device which sends data to particular port.

Bridge-store and forward devices that adds or deletes fields from frame header. Same function as switch but much more primitive and has lesser ports.

Router- Connects all computers from a LAN to internet using **same IP**.

Type of Internetworking:

- Internetworking is implemented in Layer 3 (Network Layer) of this model.
- The most notable **example** of internetworking is the Internet (capitalized).
- There are **three variants of internetwork** or Internetworking, depending on who administers and who participates in them :

1) **Extranet**
2) **Intranet**
3) **Internet**

Extranet

- An extranet is a network of **internetwork or Internetworking** that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more trusted organizations or entities.
- Technically,

✓ an extranet may also be **categorized** as a MAN, WAN, or other type of network,

✓ by definition, an extranet cannot consist of a single LAN;

✓ it must have at least one connection with an **external network.**

Intranet

- An intranet is a set of **interconnected networks or Internetworking**, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a **single administrative entity.**
- That **administrative entity** closes the intranet to the rest of the world, and allows only specific users.
- Most commonly, an **intranet** is the internal network of a company or other enterprise.
- A **large intranet** will typically have its own **web server** to provide users with browsable information.

Internet

- A specific **Internetworking**, consisting of a worldwide interconnection of
  - governmental,
  - academic,
  - public, and
  - private networks
- based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S.
- **Department of Défense** also home to the World Wide Web (WWW) and referred to as the **'Internet'** with a capital 'I' to distinguish it from other generic internetworks.
- Participants in the Internet, or their service providers, use **IP Addresses** obtained from address registries that control assignments.

Extranet

- An extranet is a network of **internetwork or Internetworking** that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more trusted organizations or entities.
- Technically,

✓ an extranet may also be **categorized** as a MAN, WAN, or other type of network,

✓ by definition, an extranet cannot consist of a single LAN;

✓ it must have at least one connection with an **external network.**

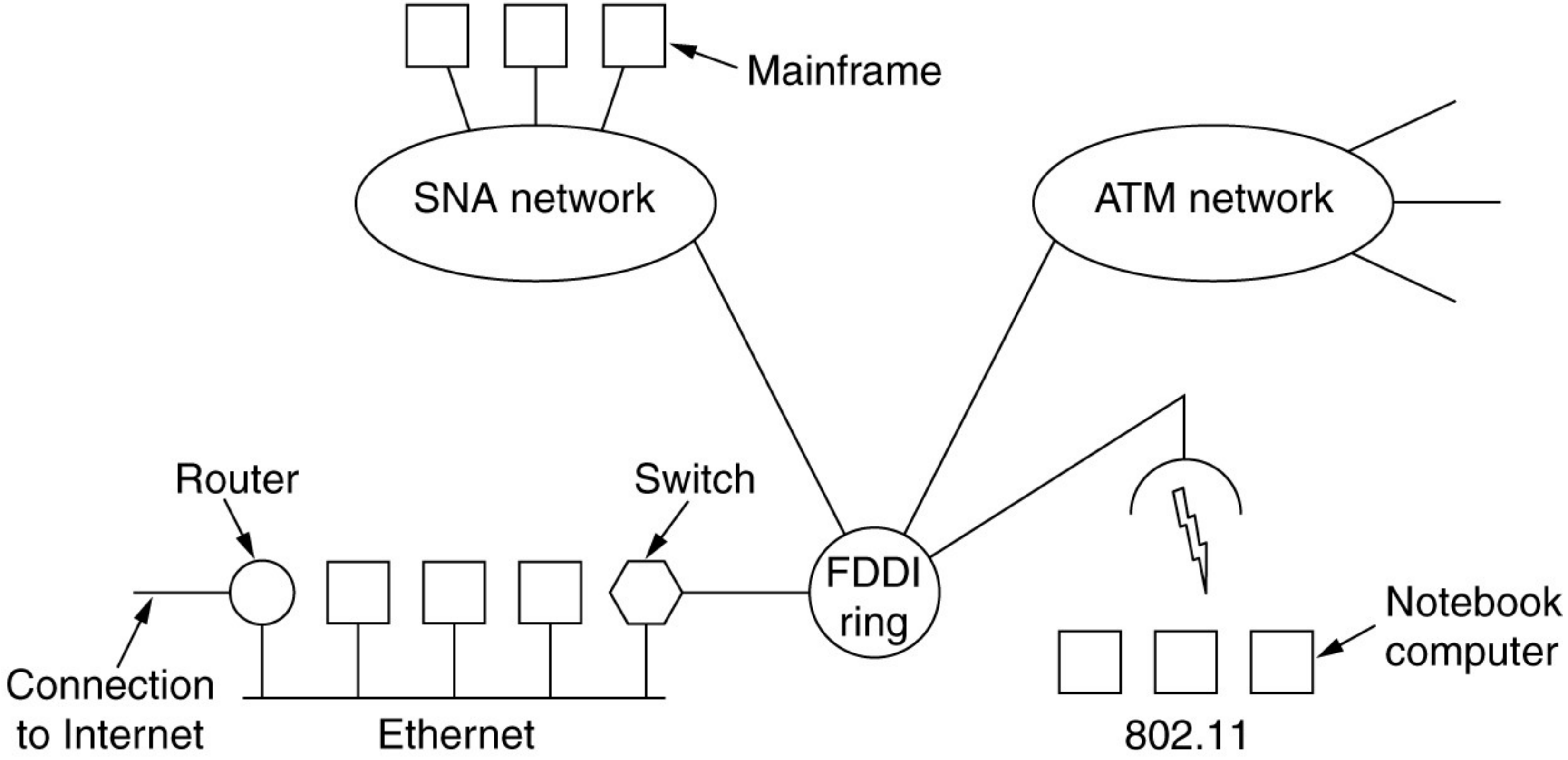
Intranet

- An intranet is a set of **interconnected networks or Internetworking**, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a **single administrative entity.**
- That **administrative entity** closes the intranet to the rest of the world, and allows only specific users.
- Most commonly, an **intranet** is the internal network of a company or other enterprise.
- A **large intranet** will typically have its own **web server** to provide users with browsable information.

Internet

- A specific **Internetworking**, consisting of a worldwide interconnection of
  - governmental,
  - academic,
  - public, and
  - private networks
- based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S.
- **Department of Défense** also home to the World Wide Web (WWW) and referred to as the **'Internet'** with a capital 'I' to distinguish it from other generic internetworks.
- Participants in the Internet, or their service providers, use **IP Addresses** obtained from address registries that control assignments.

Connecting Networks



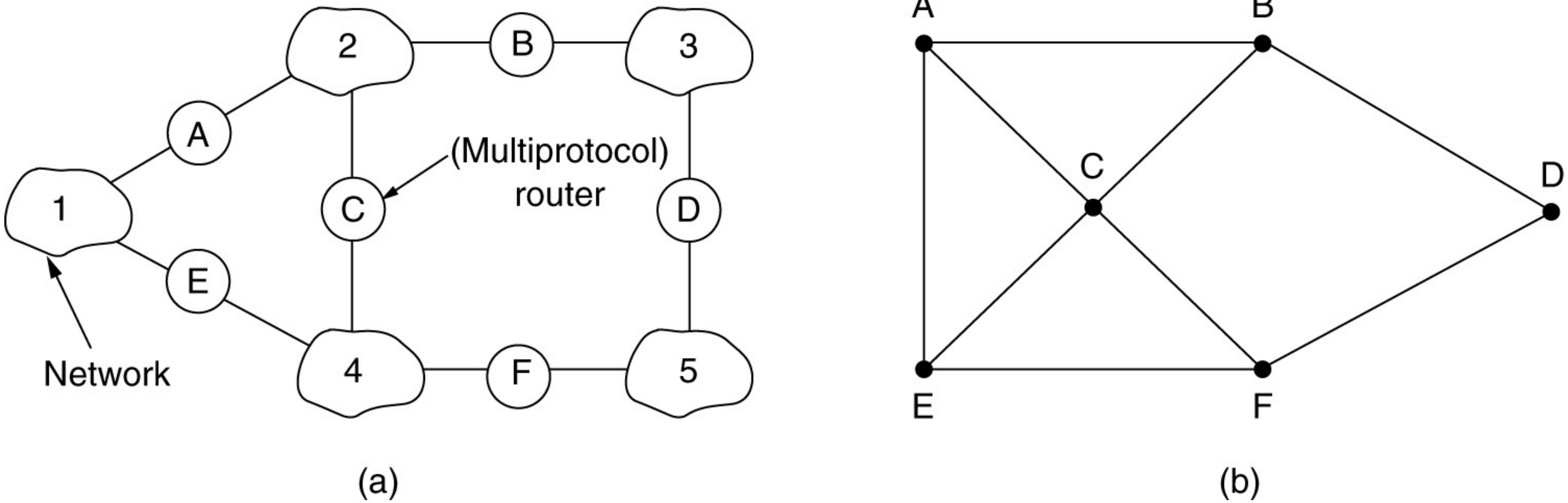
A collection of interconnected networks.

FDDI: Fiber Disturbed DataData Interface

ATM:Asynchronous Transfer Mode

Internetwork Routing

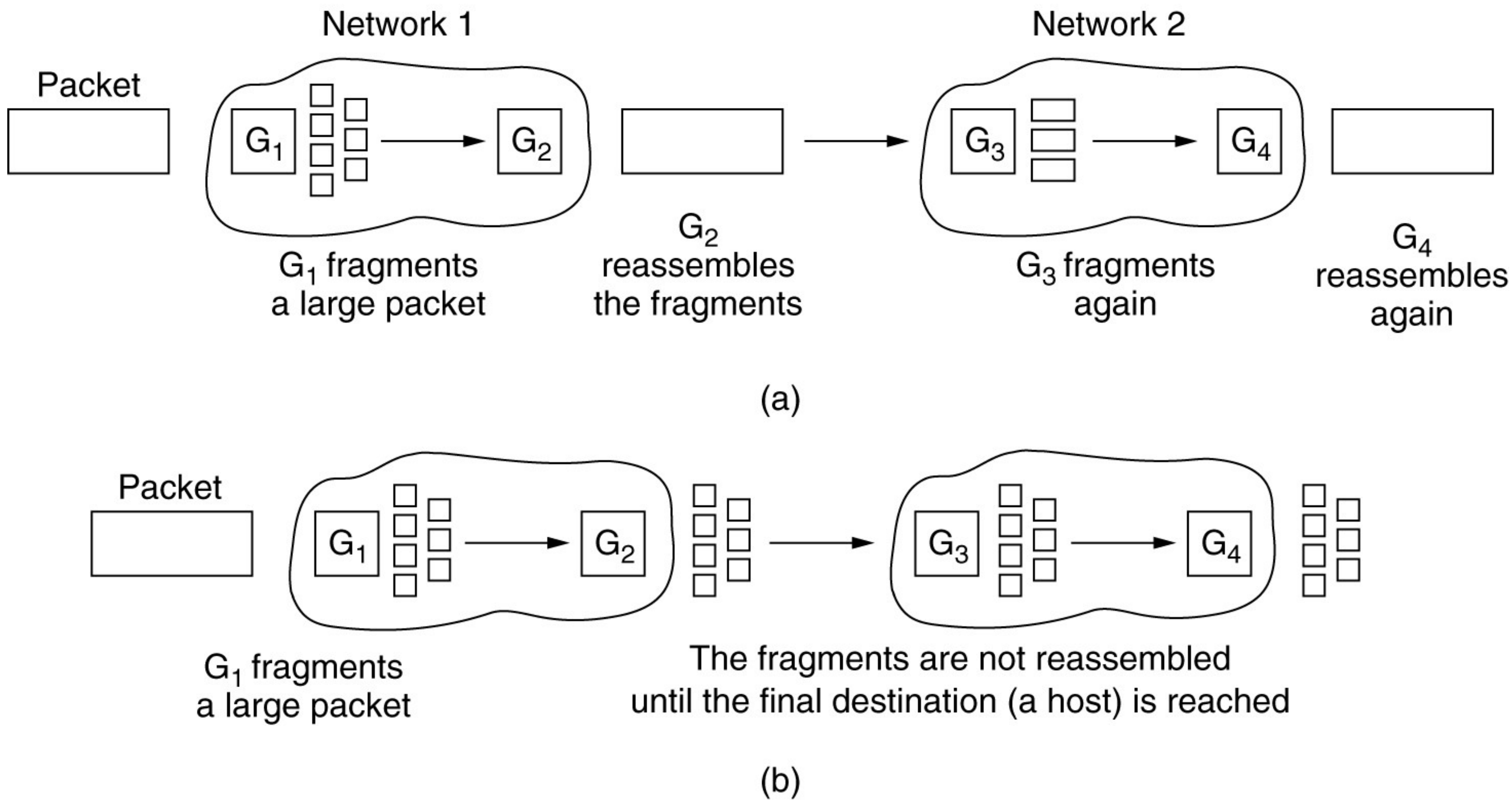
- **Routing through an internetwork** is similar to routing within a single subnet, but with some added complications.
- Fig. (a) in which five networks are connected by six routers.
- Making a **graph model** of this situation is complicated by the fact that every router can directly access every other router connected to any network to which it is connected.
- For example, **B** in Fig. (a) can directly access A and C via network 2 and also D via network 3.



(a) An internetwork. (b) A graph of the internetwork.

Fragmentation

Fragmentation of data packets: Splitting of data packets that are too large to be transmitted on the network



(a) Transparent fragmentation. (b) Nontransparent fragmentation.

The Network Layer in the Internet

- The IP Protocol
- IP Addresses
- Internet Control Protocols
- OSPF – The Interior Gateway Routing Protocol
- BGP – The Exterior Gateway Routing Protocol
- Internet Multicasting
- Mobile IP
- IPv6

Design Principles for Internet

- Make sure it works.
- Keep it simple.
- Make clear choices.
- Exploit modularity.
- Expect heterogeneity.
- Avoid static options and parameters.
- Look for a good design; it need not be perfect.
- Be strict when sending and tolerant when receiving.
- Think about scalability.
- Consider performance and cost.

Collection of Sub networks

At the network layer, the Internet can be viewed as a collection of **sub networks** or **Autonomous Systems** (ASes) that are interconnected.

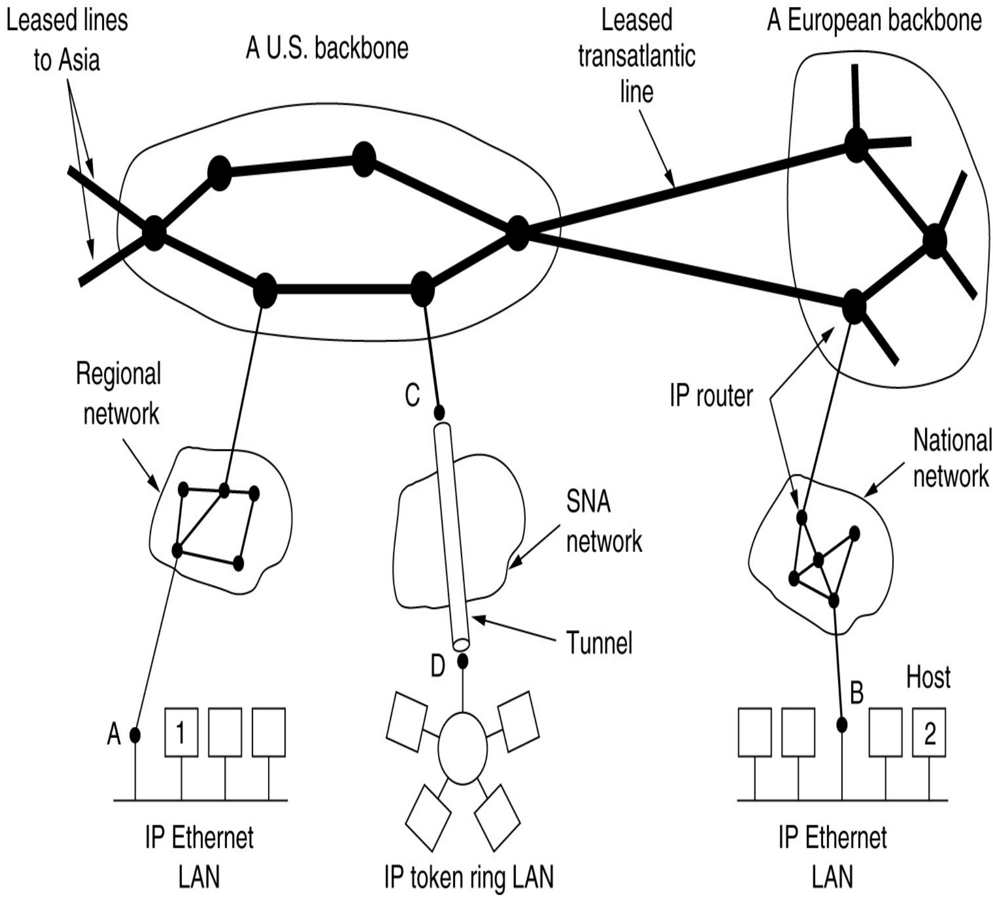
There is no real structure, but several major **backbones** exist.

These are **constructed** from high-bandwidth lines and fast routers.

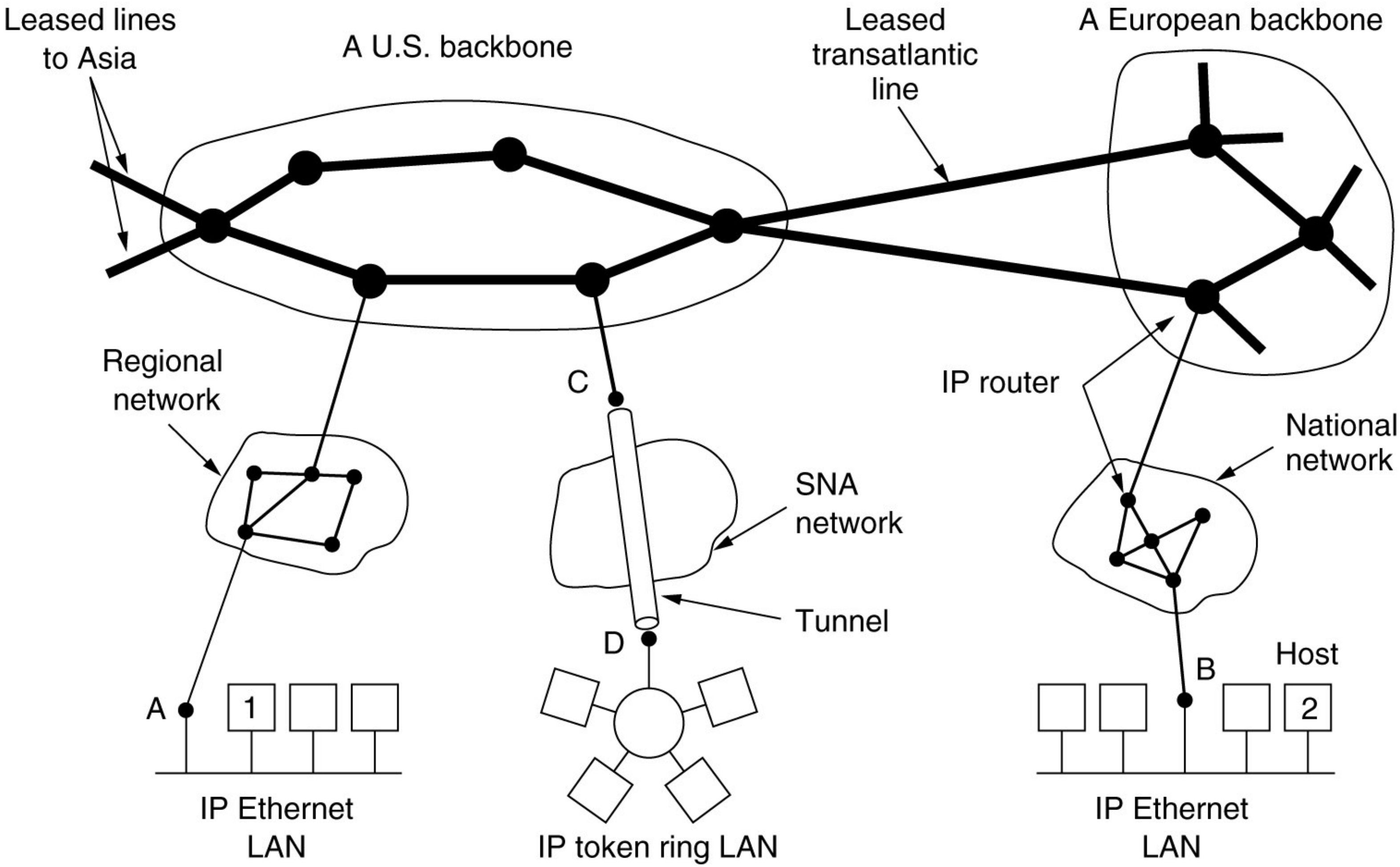
Attached to the **backbones** are regional (midlevel) networks

The glue that holds **the whole Internet** together is the network layer protocol, **IP (Internet Protocol).**

The **job** of the network layer is to provide a best-efforts way to transport datagram from source to destination



Collection of Sub networks

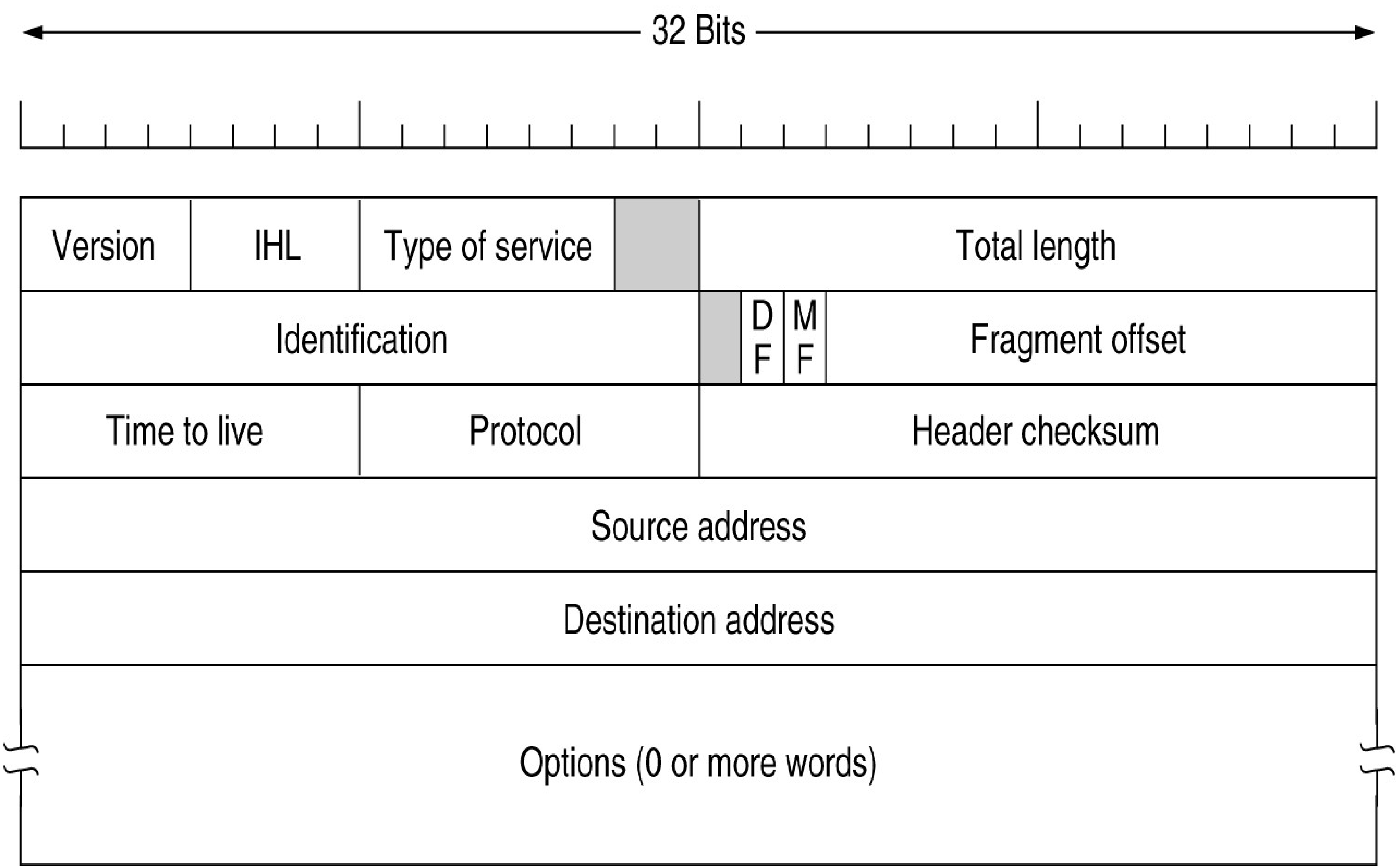


The Internet is an interconnected collection of many networks.

The IP Protocol

- IP datagram consists of a header part and a data part
- header has a 20-byte fixed part and a variable length optional part
- It is transmitted in big-endian order:
  - from left to right, with the high-order bit of the *Version field going first.*
  - *The SPARC is big endian; the Pentium is little-endian.*
  - *On little endian machines, software conversion is required on both transmission and reception*

The IP Protocol



The IPv4 (Internet Protocol) header.

The IP Protocol

- Version field
  - keeps track of which version of the protocol the datagram belongs to.
  - Currently a transition between IPv4 and IPv6 is going on
  - IPv5 was an experimental real-time stream protocol that was never widely used
- IHL field
  - Since the header length is not constant, IHL is provided to tell how long the header is, in 32-bit words.
  - The minimum value is 5, which applies when no options are present.
  - The maximum value of this 4-bit field is 15, which limits the header to 60 bytes, and thus the Options field to 40 bytes.

The IP Protocol

- Type of service field.
  - to distinguish between different classes of service
  - Various combinations of reliability and speed are possible.
  - For digitized voice, fast delivery beats accurate delivery.
  - For file transfer, error-free transmission is more important than fast transmission.

The IP Protocol

- Total length field
  - includes everything in the datagram—both header and data.
  - The maximum length is 65,535 bytes.
  - At present,this upper limit is tolerable, but with future gigabit networks,larger datagrams may be needed
- Identification field
  - needed to allow the destination host to determine which datagram a newly arrived fragment belongs to.
  - All the fragments of a datagram contain the same Identification value.

The IP Protocol

- two 1-bit fields: DF & MF
- DF stands for Don't Fragment.
  - It is an order to the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again.
  - the datagram must avoid a small-packet network on the best path and take a suboptimal route.
- MF stands for More Fragments.
  - All fragments except the last one have this bit set.
  - It is needed to know when all fragments of a datagram have arrived

The IP Protocol

- Fragment offset field:
  - 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, there is a maximum of 8192 fragments per datagram
- Time to live field
  - counter used to limit packet lifetimes.
  - It must be decremented on each hop. it just counts hops
  - When it hits zero, the packet is discarded and a warning packet is sent back to the source host.
  - Prevent datagrams from wandering around the

The IP Protocol

- Protocol field
  - tells it which transport process to give it to.
  - Possibilities are TCP, UDP and some others.
  - The numbering of protocols is global across the entire Internet.
- Header checksum field
  - verifies the header only.
  - Such a checksum is useful for detecting errors
  - using one's complement arithmetic and then take the one's complement of the result.
  - This algorithm is more robust than using a normal add.
  - Note that the Header checksum must be recomputed at each hop because at least one field (the Time to live field) always changes

The IP Protocol

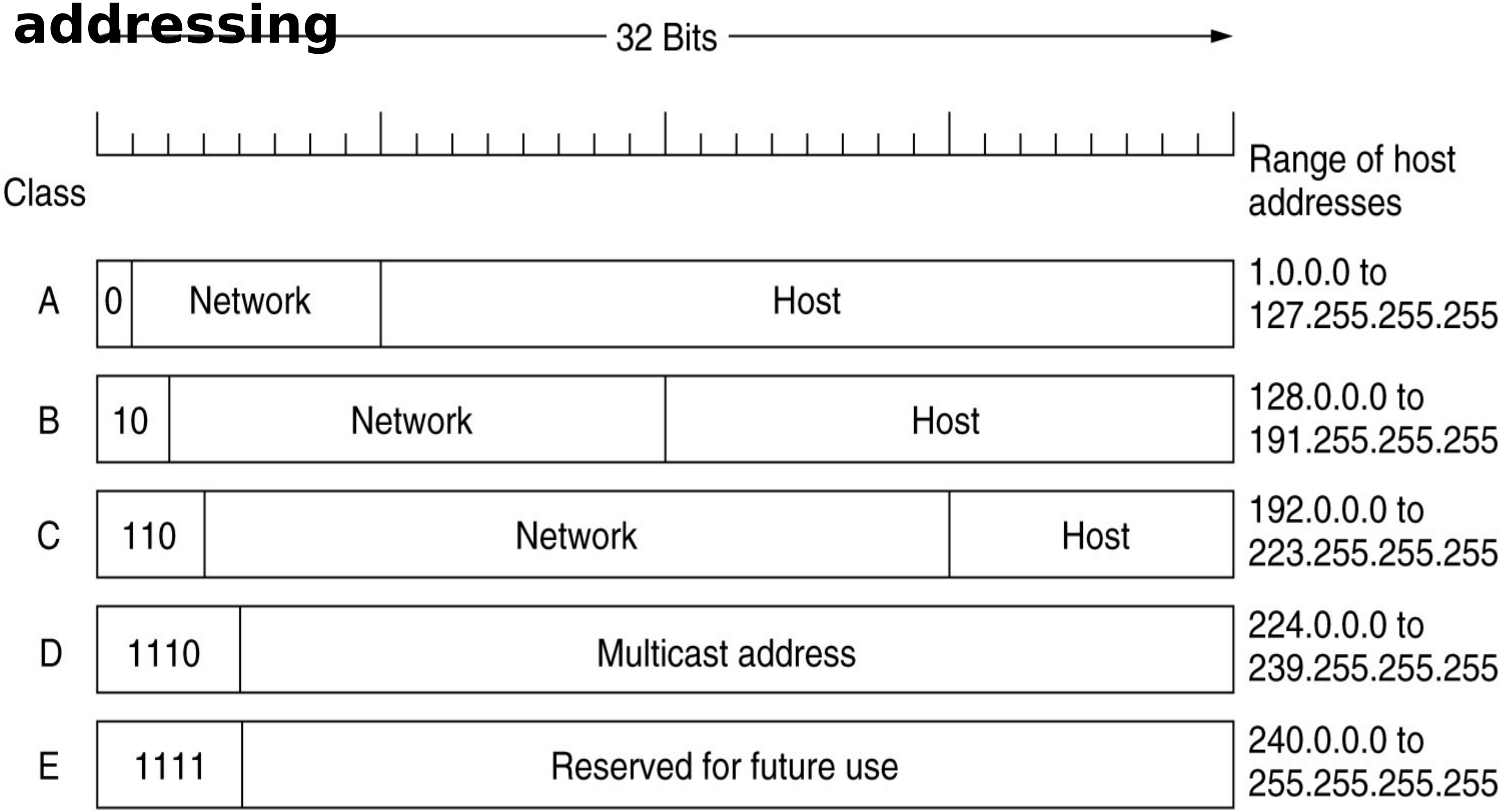
- Source address and Destination address
  - indicate the network number and host number.
  - Discussed in detail in IP addressing
- Options field
  - was designed to provide an escape to allow subsequent versions of the protocol
    - to include information not present in the original design,
    - to permit experimenters to try out new ideas, and
    - to avoid allocating header bits to information that is rarely needed.
  - The options are variable length.

IP Addresses

- Every host and router on the Internet has an IP address, which encodes its network number and host number.
- The combination is unique:
  - no two machines on the Internet have the same IP address.
- All IP addresses are 32 bits long & are used in the Source address and Destination address fields of IP packets.
- It is important to note that an IP address does not actually refer to a host.
- It really refers to a network interface, so if a host is on two networks, it must have two IP addresses.
- However, in practice, most hosts are on one network and thus have one IP address.

IP Addresses

For several decades, IP addresses were divided into the five categories. This allocation was called **classful addressing**

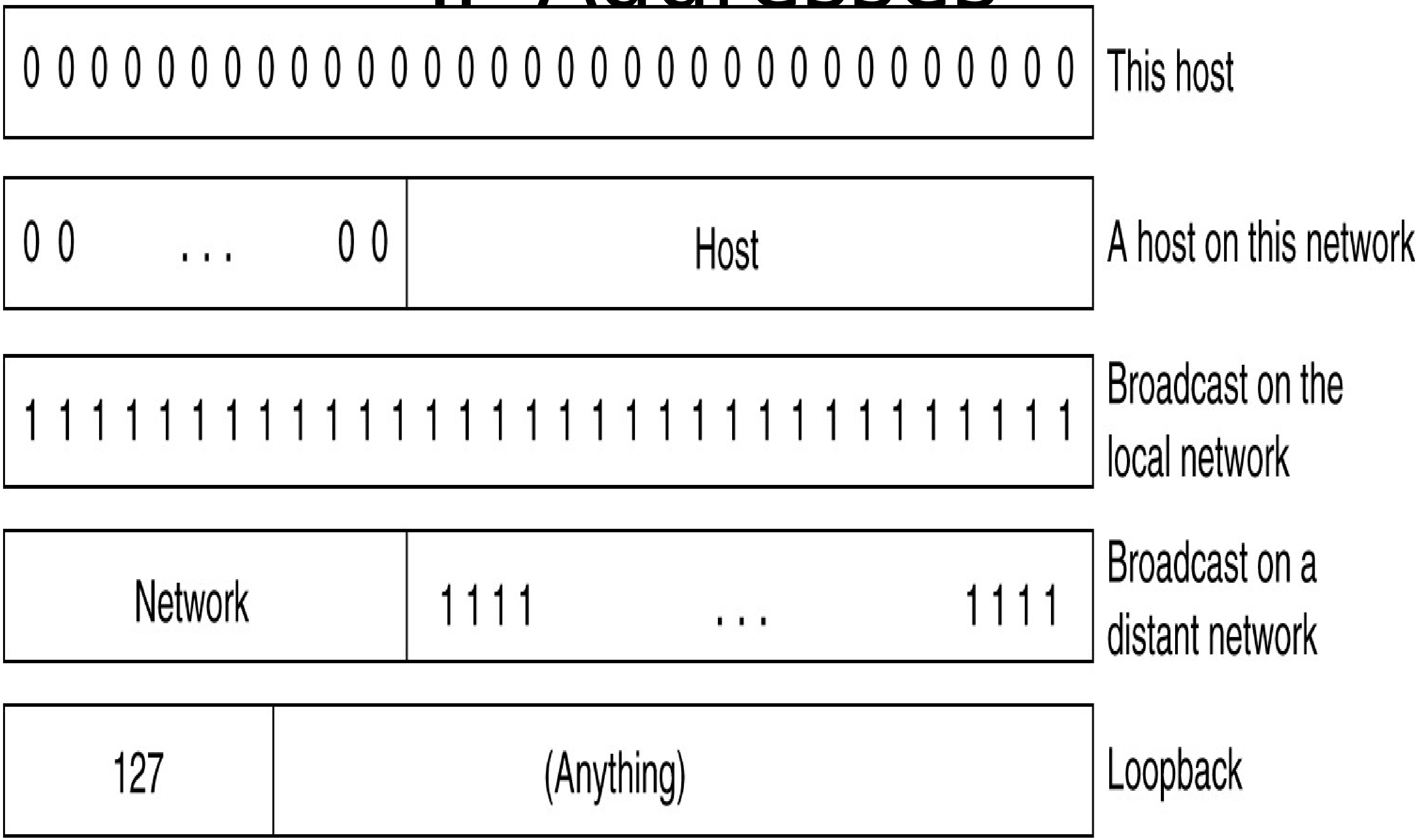


IP address formats.

IP Addresses

- Network numbers are managed by a nonprofit corporation called **ICANN (Internet Corporation for Assigned Names and Numbers)** to avoid conflicts
- Network addresses, which are 32-bit numbers, are usually written in **dotted decimal notation.**
- In this format, each of the 4 bytes is written in decimal, from 0 to 255.
- For example, the 32-bit hexadecimal address C0290614 is written as 192.41.6.20
- The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255.
- The values 0 and -1 (all 1s) have special meanings
  - value 0 means this network or this host.
  - value of -1 is used as a broadcast address to mean all hosts on the indicated network

IP Addresses



Special IP addresses.

The **IP address 0.0.0.0** is used by hosts when they are being booted.

IP addresses with 0 as network number refer to the **current network**.

The address consisting of all 1s allows **broadcasting** on the local network, typically a LAN.

The addresses with a proper network number and all 1s in the host field allow machines to send **broadcast packets** to distant LANs anywhere in the Internet

All addresses of the form **127.*xx.yy.zz*** are reserved for loopback testing.

- **Packets** sent to that address are not put out onto the wire;
- They are processed locally and treated as incoming packets.

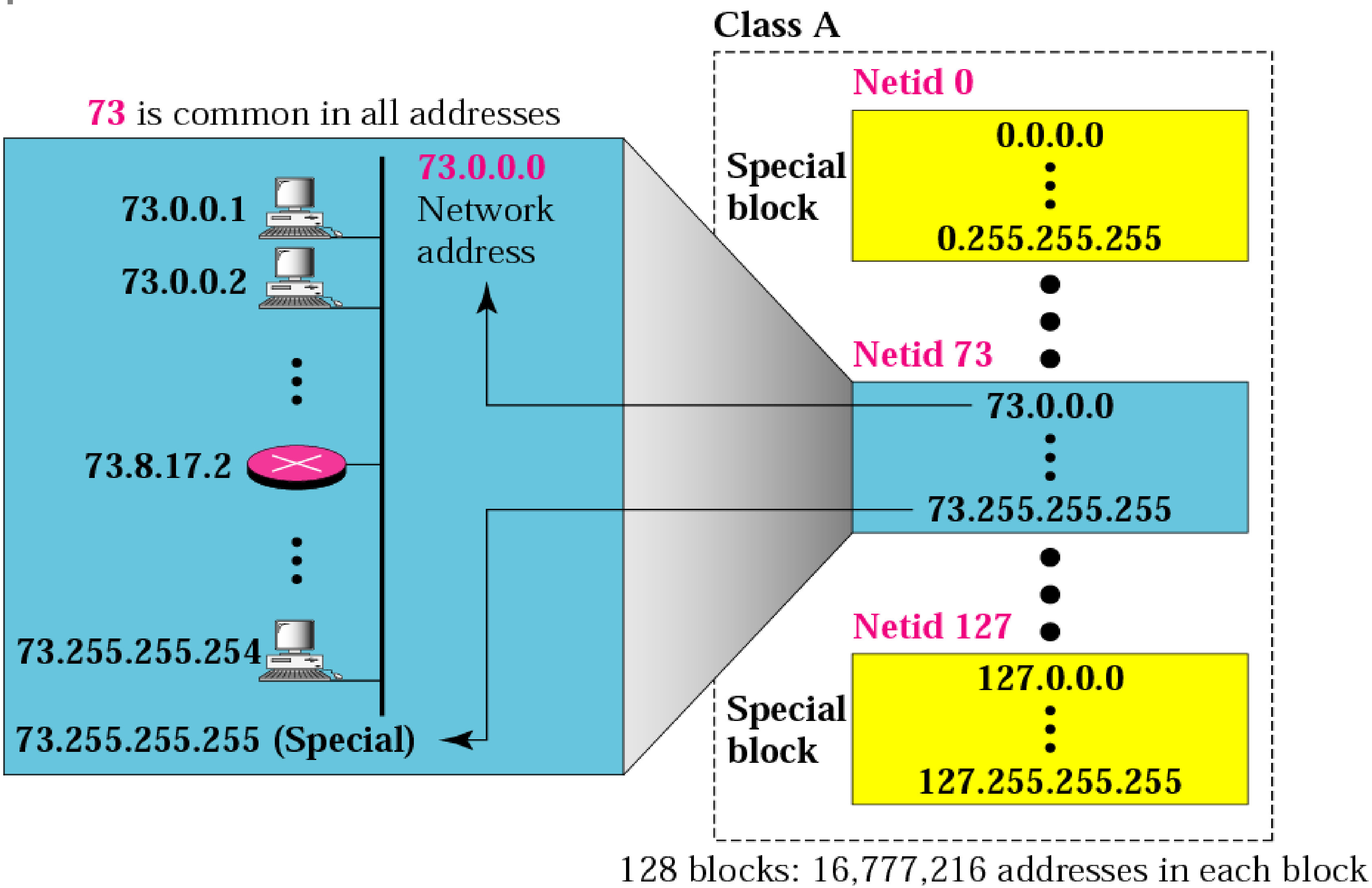
Class A

- The **first bit** of the first octet is always set to 0 (zero).
- Thus the first octet ranges from **1 – 127**, i.e.00000001 – 01111111
- Class A **addresses** only include IP starting from 1.x.x.x to 126.x.x.x only.
- The IP range 127.x.x.x is reserved for loopback.
- Class A IP address format is thus:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

- **IP address** belonging to class A are assigned to the networks that contain a large number of hosts.
- The **network ID** is 8 bits long.
- **The host ID** is 24 bits long.

Figure 4.7 *Blocks in class A*



Class A

- The **higher order bits** of the first octet in class A is always set to 0.
- The **remaining 7 bits** in first octet are used to determine network ID.
- The **24 bits of host ID** are used to determine the host in any network.
- The default sub-net mask for class A is 255.x.x.x.
- Therefore, class A has a total of:

➢ 2^7-2 = **126 network ID** **(**First is the network no. and the last is the broadcast no. So, (-2))

➢ 2^24-2 = **16,777,214 host ID**

Start adress:0.0.0.0

End address:127.255.255.255

Example :2.134.213.2

Class B

- An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.
- Thus the first octet ranges from **128 – 191** ie.,10000000 - 10111111
- Class B IP Addresses range from 128.0.x.x to 191.255.x.x.
- The default subnet mask for Class B is 255.255.x.x.
- Class B IP address format is **10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH**
- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

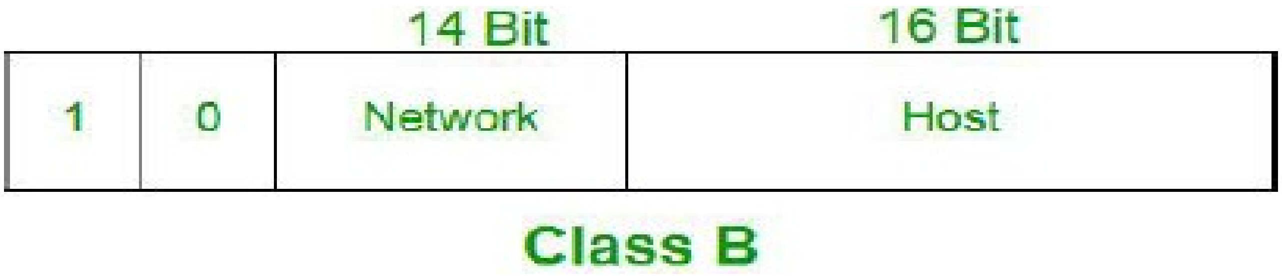
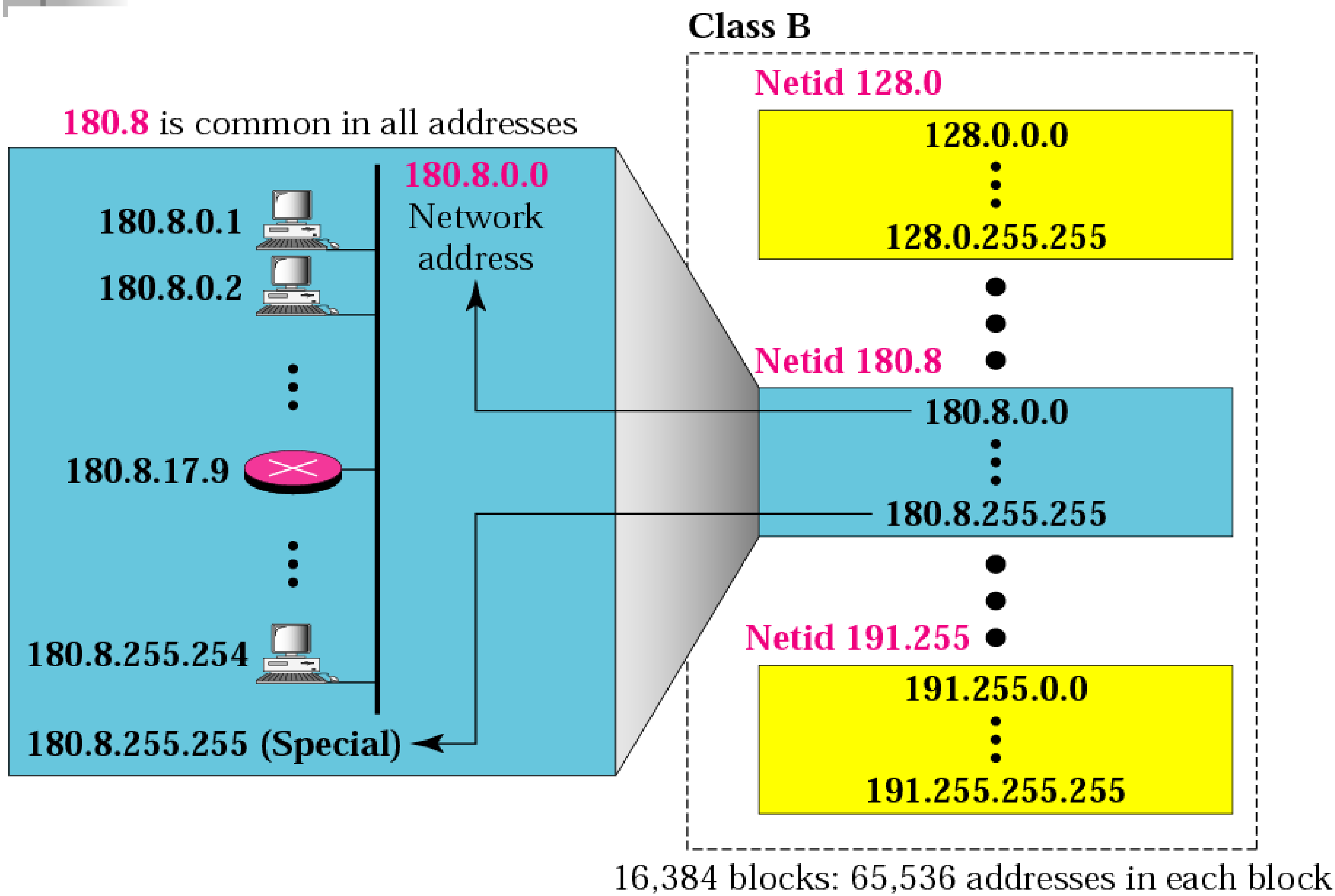


Figure 4.8 *Blocks in class B*



Class B

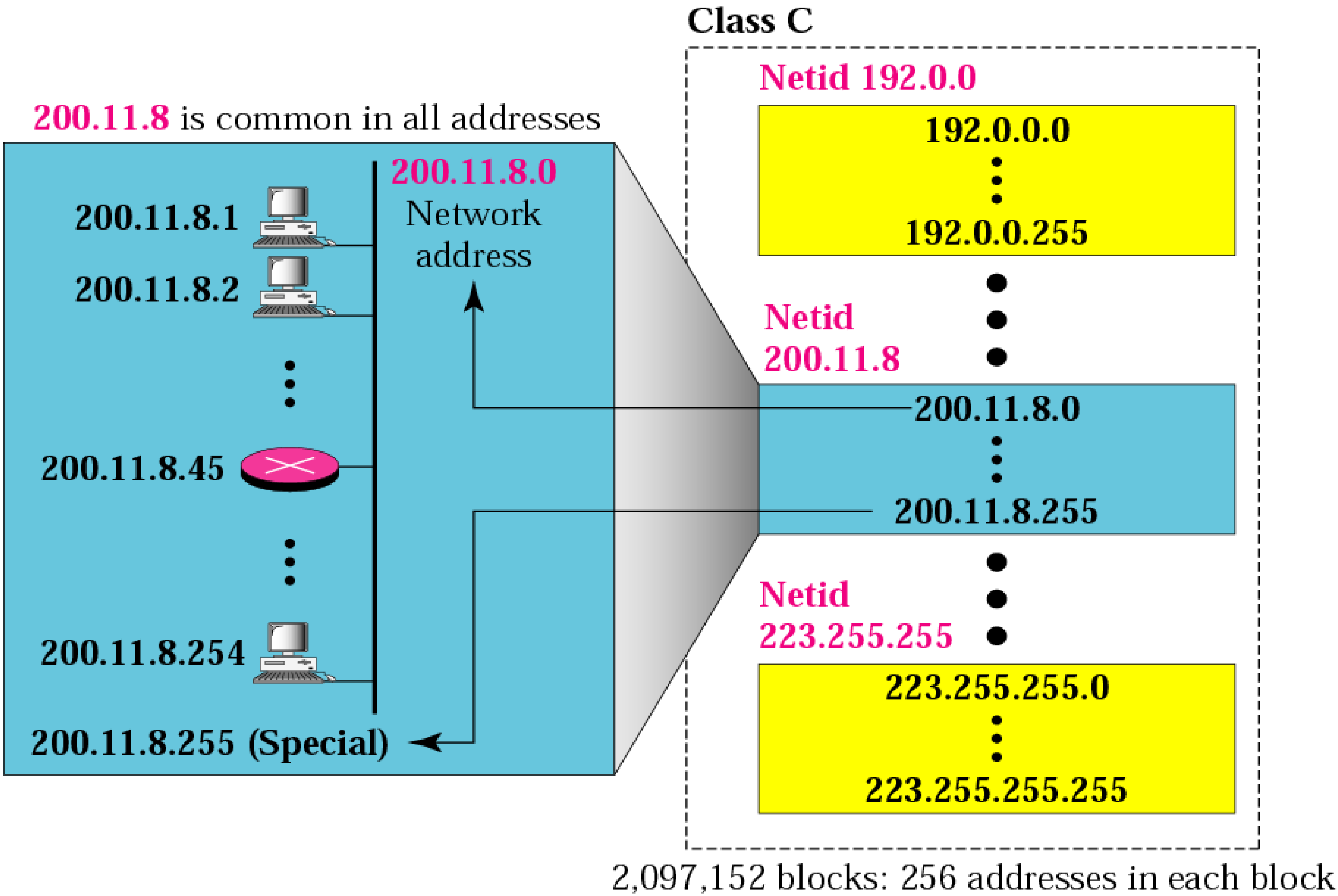
- The **network ID** is 16 bits long.
- The **host ID** is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to **10**.
- The remaining 14 bits are used to determine **network ID**.
- The 16 bits of **host ID** is used to determine the host in any network.
- The default sub-net mask for class B is 255.255.x.x.
- Class B has a total of:
  - 2^14 = 16384 network address
  - 2^16 = 65536 host address
- Ranges from 128.0.0.0 to 191.255.0.0 as class B
- Example :135.58.24.17

.

Class C

- The first octet of Class C IP address has its first 3 bits set to 110, that is:
- The first octet ranges from 192-223 ie.,11000000-11011111
- Class C IP addresses range from 192.0.0.x to 223.255.255.x.
- The default subnet mask for Class C is 255.255.255.x.
- Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH**
- IP address belonging to class C are assigned to small-sized networks.

Figure 4.9 *Blocks in class C*



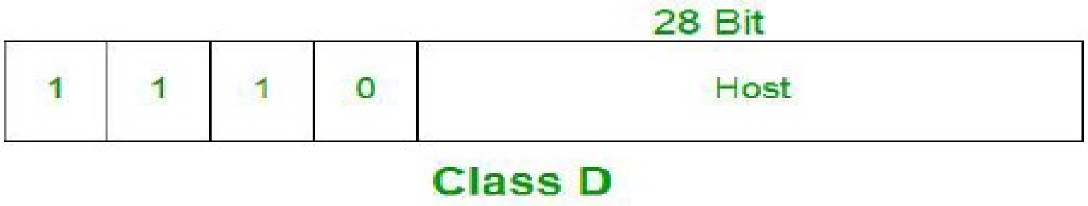
Suite

Class C

- The network ID is 24 bits long.
- The host ID is 8 bits long.
- The higher order bits of the first octet of IP addresses of class C are always set to 110.
- The remaining 21 bits are used to determine network ID.
- The 8 bits of host ID is used to determine the host in any network.
- The default sub-net mask for class C is 255.255.255.x. Class C has a total of
  - 2^21 = 2097152 network address
  - 2^8 = 256 host address
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.
- Example :192.168.178.1

Class D

- The first octet ranges from 224-239 ie., 11100000-11101111
- Class D has IP address rage from 224.0.0.0 to 239.255.255.255.
- Class D is reserved for **Multicasting**.
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.
- The **higher order bits** of the first octet of IP addresses belonging to class D are always set to 1110.
- The remaining bits are for the address that interested hosts recognize.
- Class D does not posses any sub-net mask.
- IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E

- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.
- IP addresses belonging to class E are reserved for experimental and research purposes.
- IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254.
- This class doesn't have any sub-net mask.
- The higher order bits of first octet of class E are always set to11

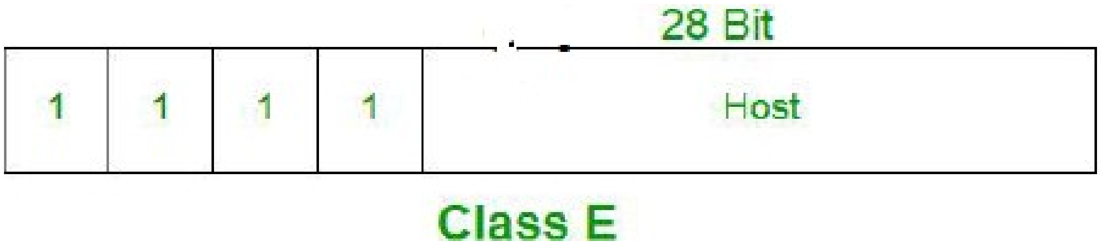
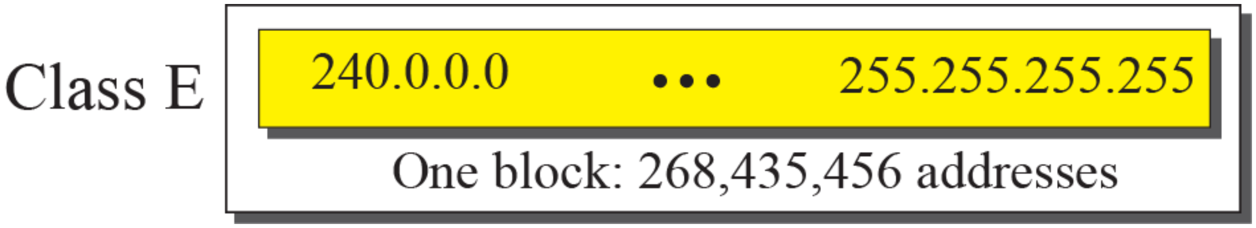


Figure *The single block in Class E*



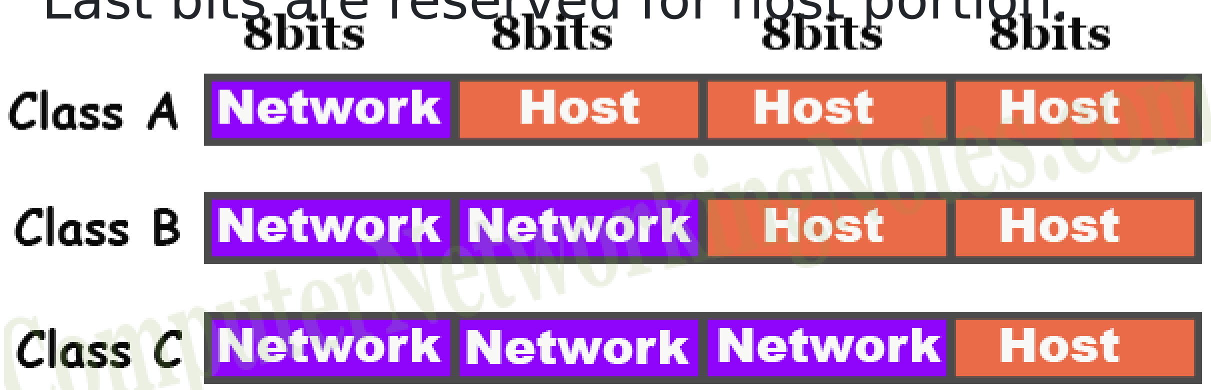
Range of special IP addresses:

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Addressing

In class A, B and C: -

- First 8, 16 and 24 bits are reserved for network portion respectively.
- Last bits are reserved for host portion.

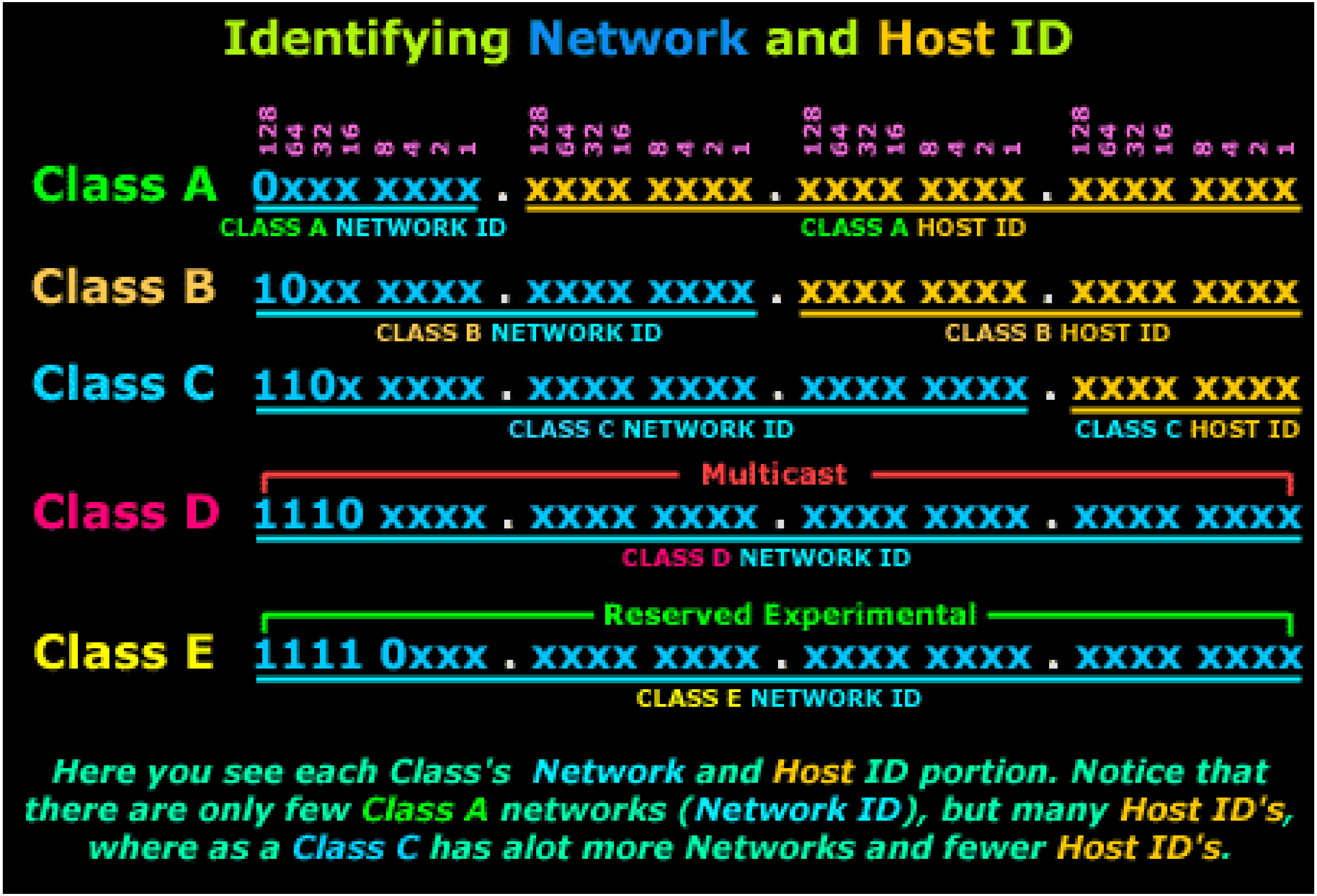


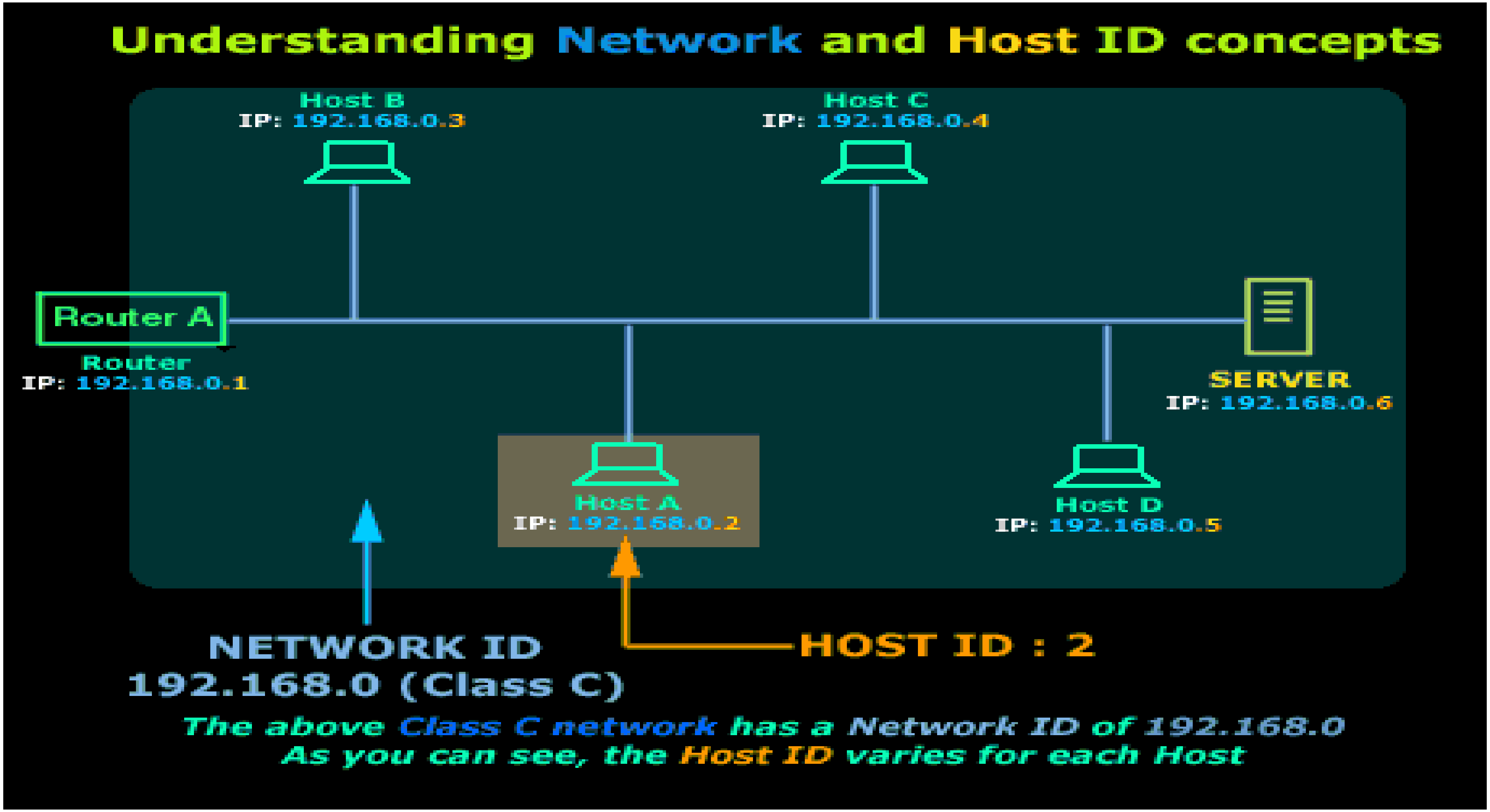
- Any **Class A** network has a total of 7 bits for the Network ID (bit 8 is always set to 0) and 24 bits for the Host ID.

To calculate how much 7 bits is:

- 2 to the power of 7 = 128 Networks
- 2 to the power of 24 = 16,777,216 hosts in each Network, of which 2 cannot be used because one is the Network Address and the other is the Network Broadcast address.

THE NETWORK AND NODE ID OF EACH CLASS





- A **small network** shown in the above picture, **Class C** IP Range for this network.
- Class C IP Addresses are for small networks.
- Looking now at Host A, its IP Address is 192.168.0.2.
- The Network ID portion of this IP Address is in blue, while the Host ID is in orange.

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

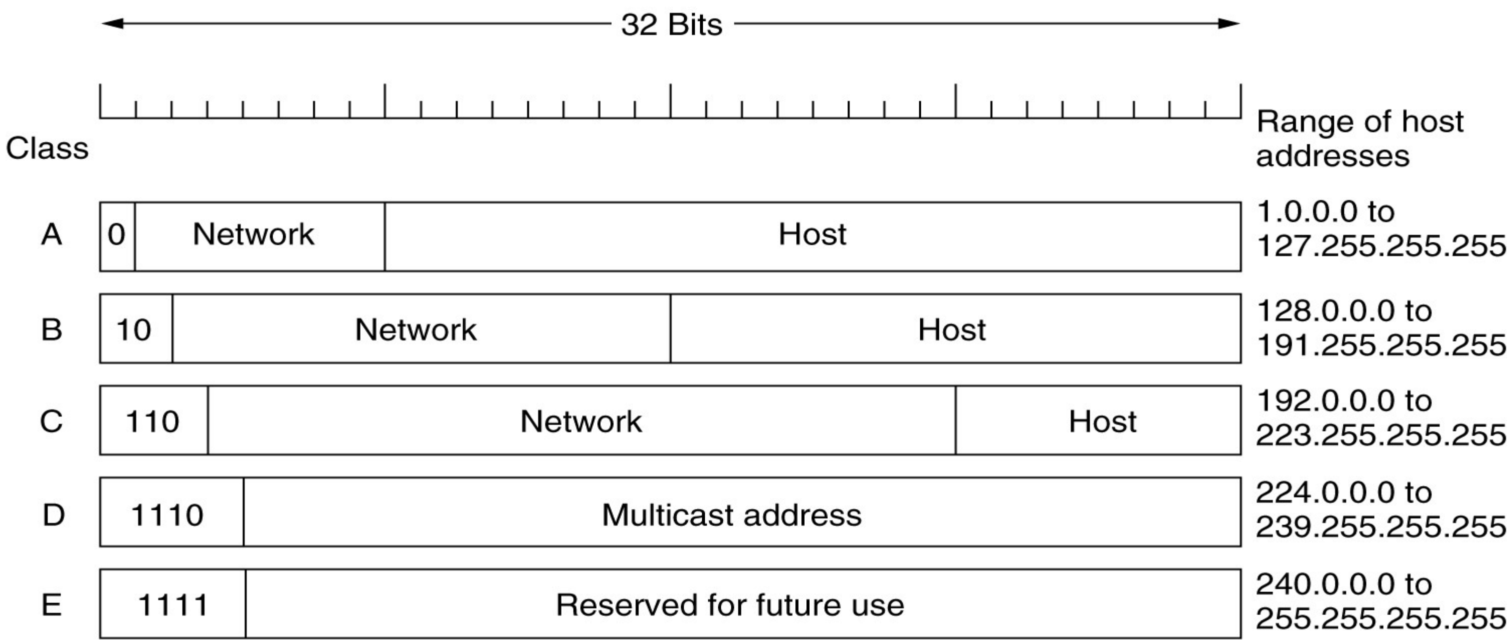
Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.



Problems with Classfull IP Addresses

Problem 1. Too few **network addresses** for large networks

- Class A and Class B addresses are gone

Problem 2. **Two-layer hierarchy** is not appropriate for large networks with Class A and Class B addresses.

- **Fix #1: Subnetting**

Problem 3. **Inflexible**. Assume a company requires 2,000 addresses

- Class A and B addresses are overkill
- Class C address is insufficient (requires 8 Class C addresses)
- **Fix #2: Classless Interdomain Routing (CIDR)**

Problem 4. Exploding Routing Tables: Routing on the **backbone Internet** needs to have an entry for each network address. The size of the routing tables started to outgrow the capacity of routers.

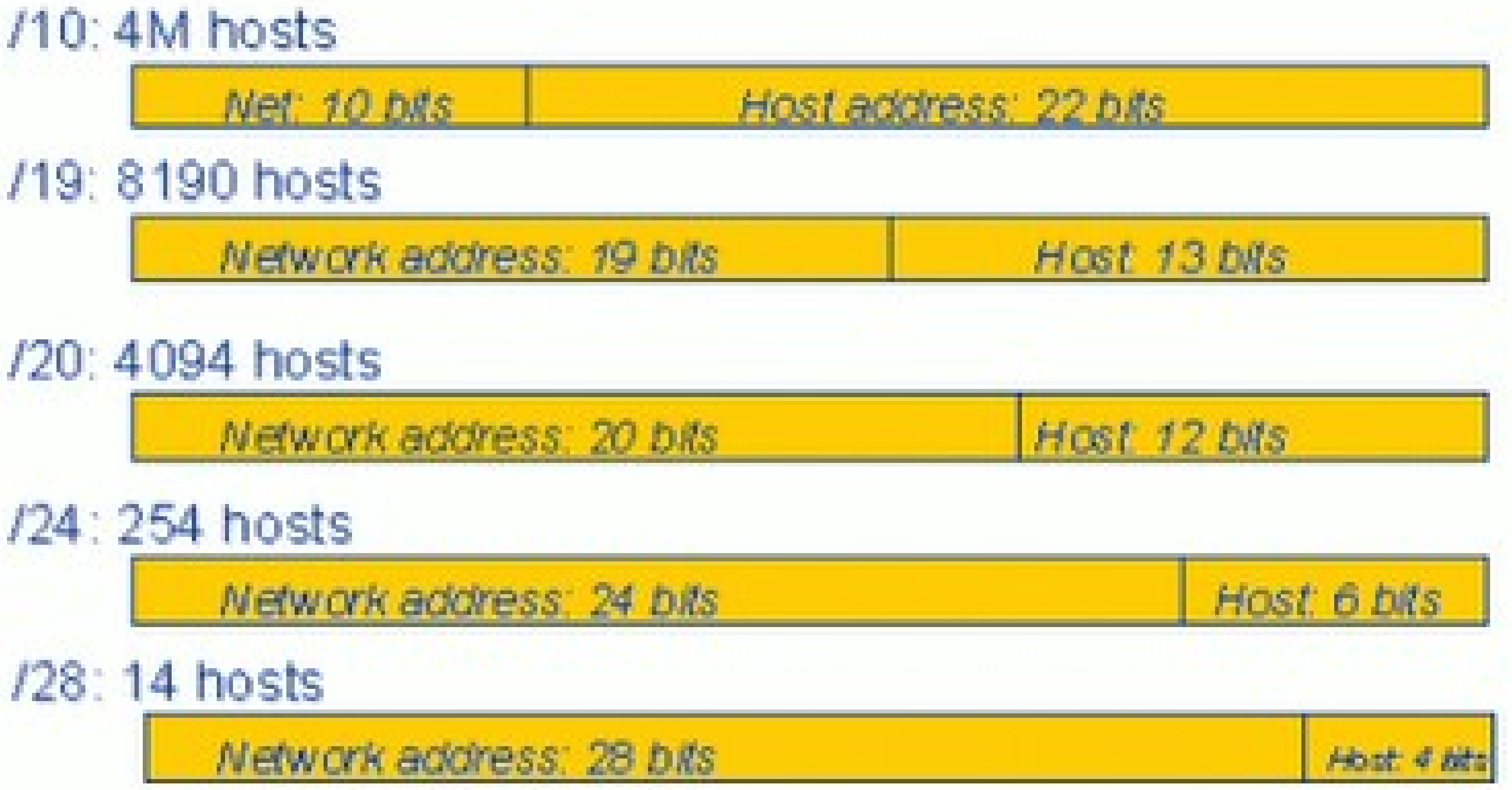
- **Fix #2: Classless Interdomain Routing (CIDR)**

Problem 5. The Internet is going to outgrow the 32-bit addresses

- **Fix #3: IP Version 6**

NO. OF NETWORKS	ADDRESSES PER NETWORK
2^7 (128)	2^{24} (16,777,216)
2^{14} (16,384)	2^{16} (65,536)
2^{21} (2,097,152)	2^8 (256)

IP Addresses
Classless addressing



Classless addressing uses a variable number of bits for the network and host portions of the address.

Problems with Classfull IP Addresses

Problem 1. Too few **network addresses** for large networks

– Class A and Class B addresses are gone

Problem 2. **Two-layer hierarchy** is not appropriate for large networks with Class A and Class B addresses.

– **Fix #1: Subnetting**

Problem 3. **Inflexible**. Assume a company requires 2,000 addresses

– Class A and B addresses are overkill

– Class C address is insufficient (requires 8 Class C addresses)

– **Fix #2: Classless Interdomain Routing (CIDR)**

Problem 4. Exploding Routing Tables: Routing on the **backbone Internet** needs to have an entry for each network address. The size of the routing tables started to outgrow the capacity of routers.

– **Fix #2: Classless Interdomain Routing (CIDR)**

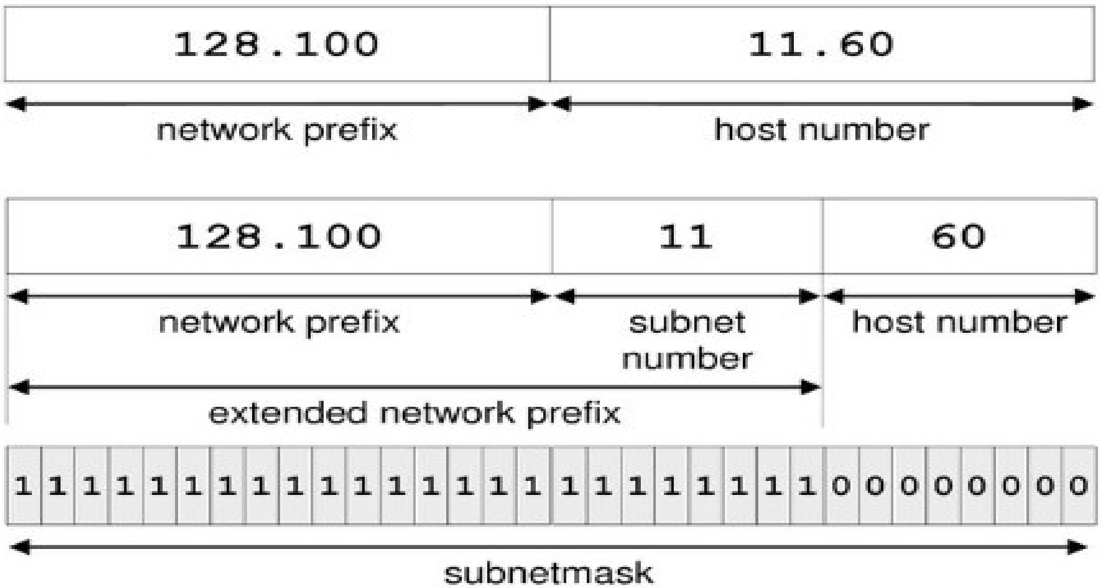
Problem 5. The Internet is going to outgrow the 32-bit addresses

– **Fix #3: IP Version 6**

NO. OF NETWORKS	ADDRESSES PER NETWORK
2^{7} (128)	2^{24} (16,777,216)
2^{14} (16,384)	2^{16} (65,536)
2^{21} (2,097,152)	2^{8} (256)

Subnetmask

- Start of the host number is indicated by prefix or netmask notation
- The netmask of the extended network prefix is called **subnetmask** (and the nework is called **subnet**)



Network Address and Mask

Network address – It identifies a **network** on internet.

Using this,

- we can find range of addresses in the network
- and total possible number of hosts in the network.

Mask (subnetting)

- It is a 32-bit binary number that **masks** an **IP address**, and divides the **IP address** into network address and host address.
- It gives the network address in the **address block**
- ✓ when **AND operation** is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).

Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved(existing state) and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Mask: 11111111 11111111 00000000 00000000

IP Address: 10000100 00000110 00010001 01010101

Then do an **AND operation**, it will produce

10000100 00000110 00000000 00000000

 which is equivalent to **132.6.0.0**

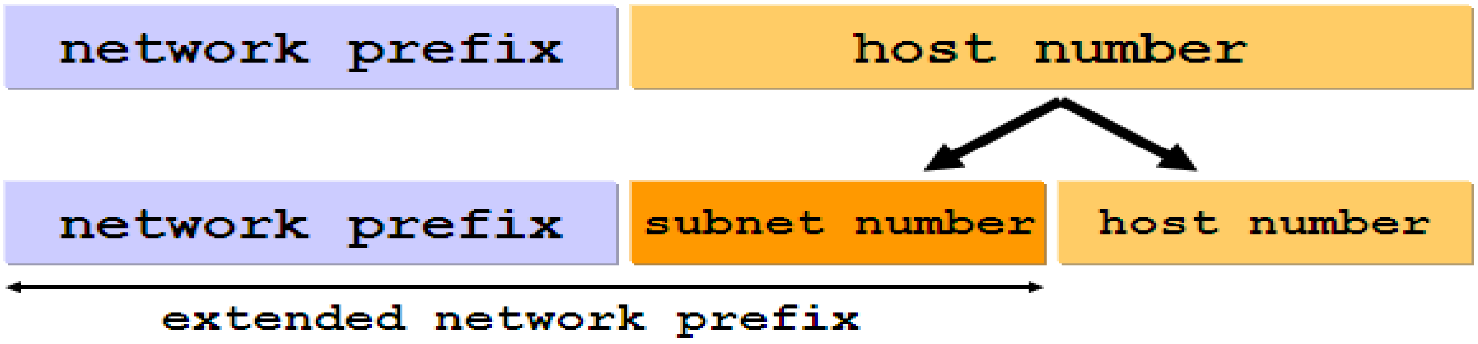
Subnetting

Basic Idea of Subnetting

•Split the host number portion of an IP address into a subnet number and a (smaller) host number.

•Result is a 3-layer hierarchy

•A **network** corresponds to a contiguous block of IP address space. This block is called a **prefix**



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

Subnets

- All the **hosts** in a **network** must have the same network number.
- ✓ This property of IP addressing can cause problems as networks grow.
- For **example**,
- ➢ consider a **university** that started out with one class B network used by the Computer Science Dept. for the computers on its Ethernet.
- ➢ A year later, the Electrical Engineering Dept. wanted to get on the Internet, so they bought a **repeater** to extend the CS Ethernet to their building.
- ➢ As time went on, many other departments acquired computers and the limit of **four repeaters** per Ethernet was quickly reached.
- ➢ A different **organization** was required.
- ➢ Getting a second network address would be hard to do since network addresses are scarce and the university already had enough addresses for over 60,000 hosts.
- The **problem** is the rule that a single class A, B, or C address refers to one network, not to a collection of LANs.
- As more and more organizations ran into this situation, a small change was made to the addressing system to deal with it.

Subnets

- A typical **campus network** with a main router connected to an **ISP** or regional network and numerous Ethernets spread around campus in **different departments**. (shown in fig)
- Each of the **Ethernets** has its own router connected to the **main router**

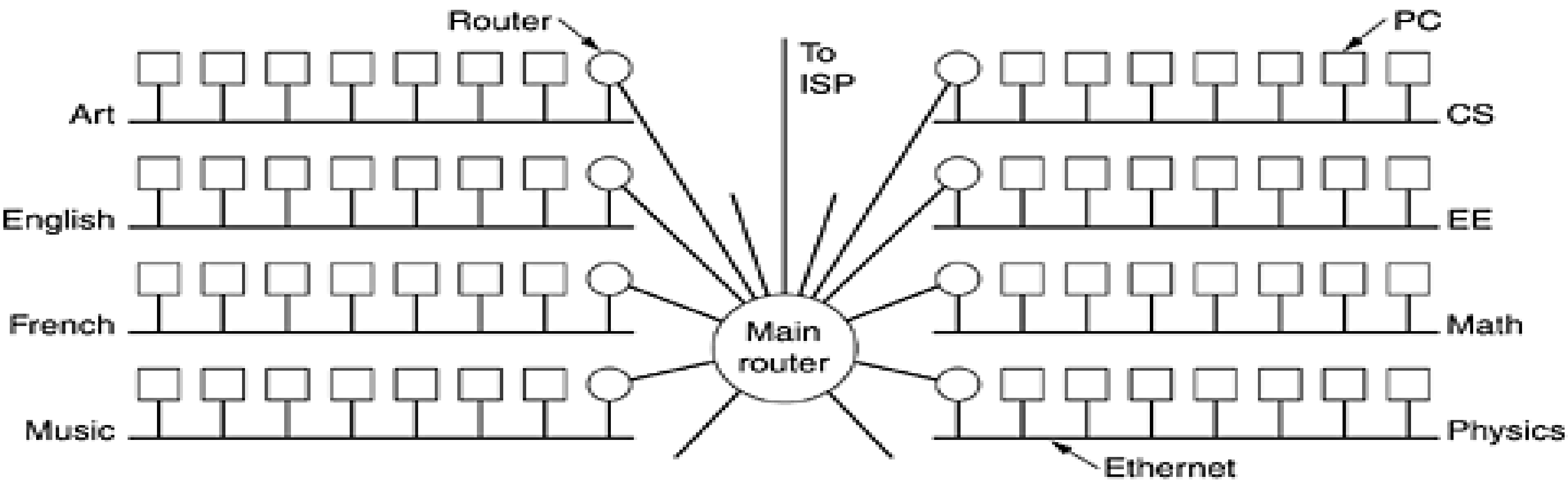
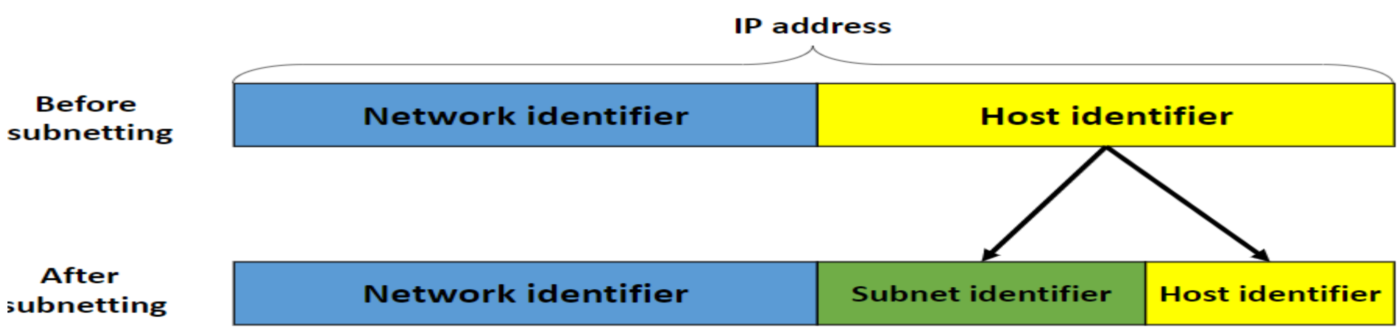


Fig.A campus network consisting of LANs for various departments



When a packet comes into the main router, how does the router know which subnet to give it to?

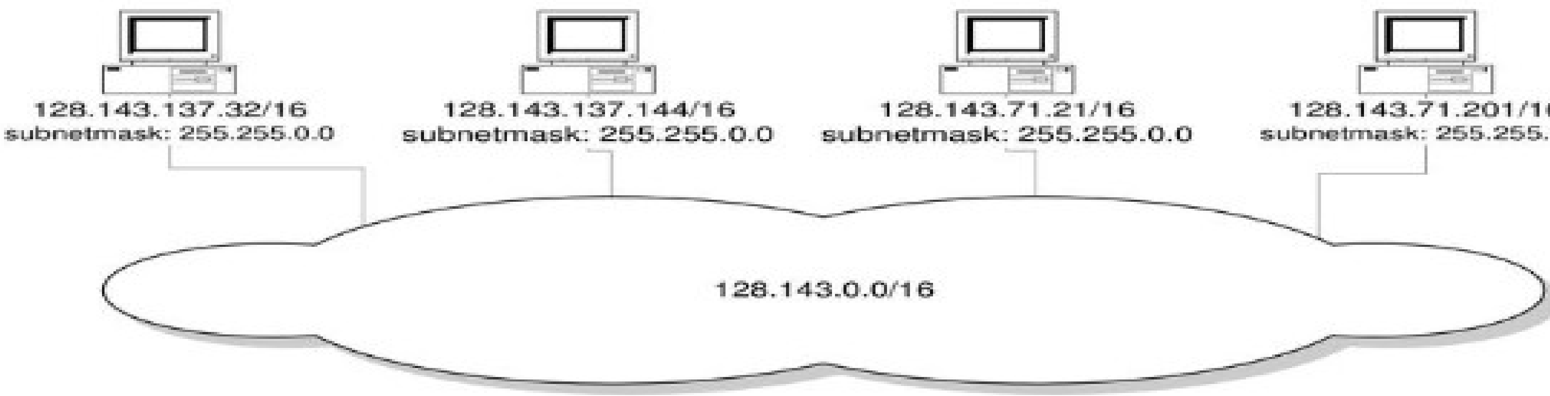
When a packet arrives, the **router** looks at the destination address of the packet and checks which subnet it belongs to.

- The router can do this by **ANDi**ng the destination address with the **mask** for each subnet and
- checking to see if the result is the corresponding **prefix**(a network corresponds to a contiguous block of IP address space).

Outside the network, the subnetting is not visible, so allocating a new subnet does not require contacting ICANN or changing any external databases.

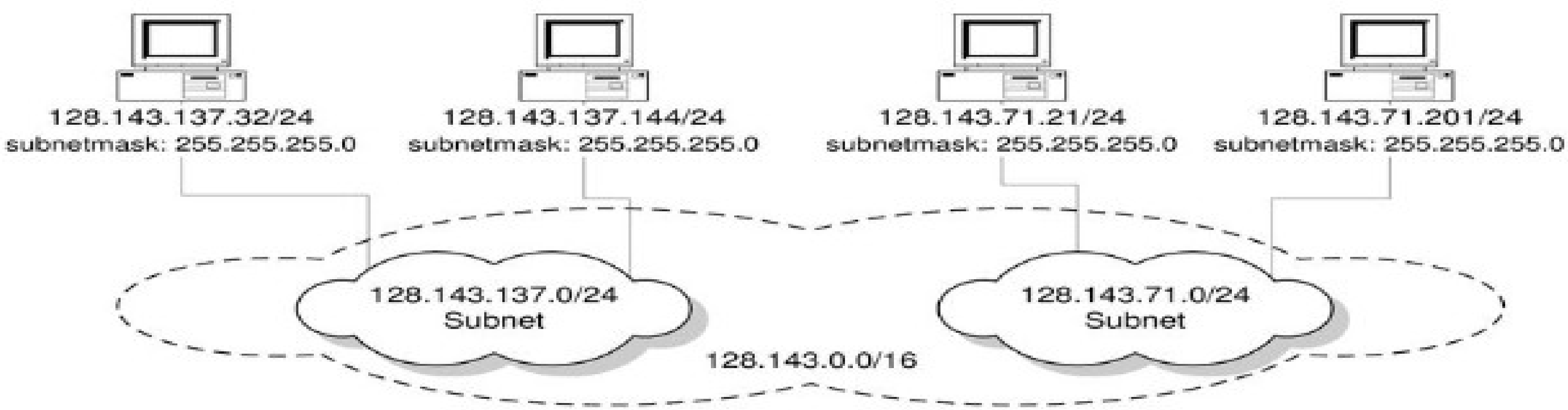
All hosts think that the other hosts are on the same network

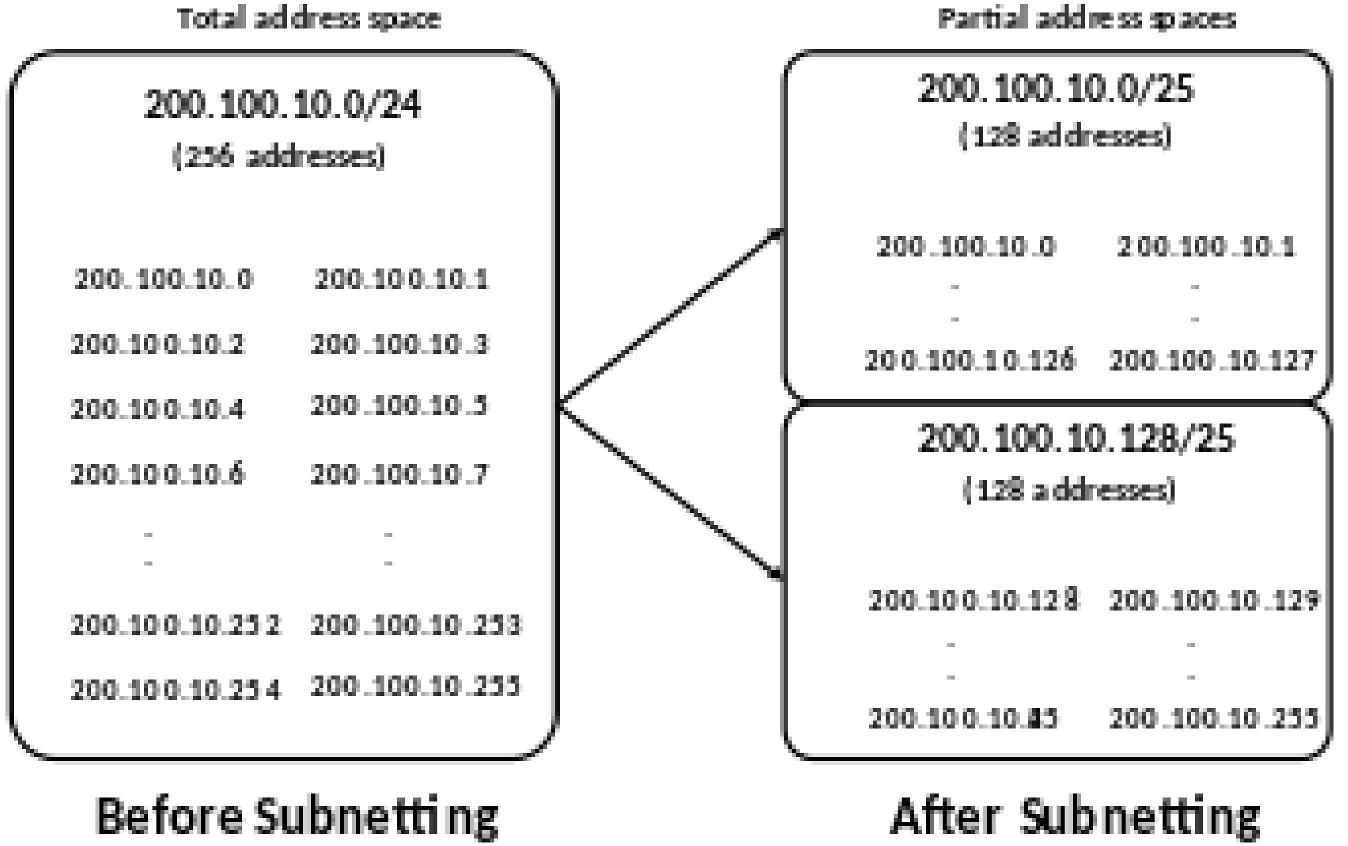
No Subnetting



Hosts with same extended network prefix belong to the same network

With Subnetting





- The concept of subnetting the IPv4 address space **200.100.10.0/24,**
- ➢ which contains 256 addresses, into two smaller address spaces,
- ✓ **200.100.10.0/25** and
- ✓ **200.100.10.128/25** with 128 addresses each.

Prefix Length	Subnet Mask	Subnet in Binary Network = N, Host = H, Borrowed = n Total IP addresses in /16 Network = 65536.	Available Network	Usable Host Per Network
/17	255.255.128.0	NNNNNNNN.NNNNNNNN.nHHHHHHH.HHHHHHHH 11111111.11111111.10000000.00000000	2^1=2	2^{15}-2 =32766
/18	255.255.192.0	NNNNNNNN.NNNNNNNN.nnHHHHHH.HHHHHHHH 11111111.11111111.11000000.00000000	2^2=4	2^{14}-2 =16382
/19	255.255.224.0	NNNNNNNN.NNNNNNNN.nnnHHHHH.HHHHHHHH 11111111.11111111.11100000.00000000	2^3=8	2^{13}-2 =8190
/20	255.255.240.0	NNNNNNNN.NNNNNNNN.nnnnHHHH.HHHHHHHH 11111111.11111111.11110000.00000000	2^4=16	2^{12}-2 =4094
/21	255.255.248.0	NNNNNNNN.NNNNNNNN.nnnnnHHH.HHHHHHHH 11111111.11111111.11111000.00000000	2^5=32	2^{11}-2 =2046
/22	255.255.252.0	NNNNNNNN.NNNNNNNN.nnnnnnHH.HHHHHHHH 11111111.11111111.11111100.00000000	2^6=64	2^{10}-2 =1022
/23	255.255.254.0	NNNNNNNN.NNNNNNNN.nnnnnnnH.HHHHHHHH 11111111.11111111.11111110.00000000	2^7=128	2^9-2 =510
/24	255.255.255.0	NNNNNNNN.NNNNNNNN.nnnnnnnn.HHHHHHHH 11111111.11111111.11111111.00000000	2^8=256	2^8-2 =254
/25	255.255.255.128	NNNNNNNN.NNNNNNNN.nnnnnnnn.nHHHHHHH 11111111.11111111.11111111.10000000	2^9=512	2^7-2 =126
/26	255.255.255.192	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnHHHHHH 11111111.11111111.11111111.11000000	2^{10}=1024	2^6-2 =62
/27	255.255.255.224	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnHHHHH 11111111.11111111.11111111.11100000	2^{11}=2048	2^5-2 =30
/28	255.255.255.240	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnHHHH 11111111.11111111.11111111.11110000	2^{12}=4096	2^6-2 =14
/29	255.255.255.248	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnHHH 11111111.11111111.11111111.11111000	2^{13}=8192	2^3-2 =6
/30	255.255.255.248	NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnHH 11111111.11111111.11111111.11111100	2^{14}=8192	2^2-2 =2

Table 5.1 Prefix lengths

/n	Mask	/n	Mask	/n	Mask	/n	Mask
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

Reserved network bits and host bits cannot be used in Subnetting

IP Class	First IP Address of class	Last IP Address of class	Default Subnet Mask	Default Network bits	Host bits	Reserved host bits
A	0.0.0.0	127.255.255.255	255.0.0.0	First 8 bits	9 to 30	31, 32
B	128.0.0.0	191.255.255.255	255.255.0.0	First 16 bits	17 to 30	31, 32
C	192.0.0.0	223.255.255.255	255.255.255.0	First 24 bits	25 to 30	31, 32

- A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle?

Mask	Binary	Hosts per subnet
255.255.240.0	11110000.00000000	**4,094**

- How do you subnet the Class C IP address 195.1.1.0 so as to have 10 subnets with a maximum of 12 hosts in each subnet.
- Current mask= 255.255.255.0
- Bits needs for 10 subnets =4 =2^4 =16 possible subnets
- Bits needs for 12 hosts = 4 = 2^4 = 16-2=14 possible hosts.
- So our mask in binary =**11110000**= **240** decimal
- Final Mask =**255.255.255.240**

Classless Addressing

- Classless addressing system is also known as **CIDR(Classless Inter-Domain Routing** or **super netting).**
- It is a way to allocate and specify the **Internet addresses** used in inter-domain routing.
- What happened in **classfull addressing** is that
- if any **company needs more than 254 host machines** but far fewer than the 65,533 host addresses,
- then the only option for the company is to take the class B address.
- Now suppose **company needs only 1000 IP addresses** for its host computers
- then in this (65533-1000=64533) IP addresses get wasted.

Classless Addressing

CIDR Notation

- CIDR IP addresses can be described as consisting of two groups of bits.

➢ The **most significant group** of bits denotes the **prefix** i.e., a network address that is used for the identification of a network or sub-network.

➢ The **least significant group** of bits is known as host identifier that determines the total number of bits in the address.

✓ It is used to signify the device on the work that will receive incoming information packets.

- A CIDR network address looks like this : **192.30.250.00/15**

➢ The **"192.30.250.00"** is the network address itself

➢ **"15"** says that the first **15 bits** are the network part of the address, leaving the last **17 bits** for specific host addresses.

- One **advantage** of classless addressing is that it sends subnet information.

Classless addressing

block ID | host ID

- Here there is no Class , only blocks
- **Notation** is x.y.z.w/n
- **/n** means mask(continues) ie no. of bits(or 1's) used to represent **block/network**.
- **eg.200.10.20.40 /28**
- Here 28 means no of 1's in the ad
- **Block ID** is 28 and **Host ID** is 4 (32-28) .
- 2^4 =16 host address
- **mask** of 200.10.20.40 is

1 1 1 1 1 1 1 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

11111111.11111111.11111111.11110000

Network/Block Address **Host**

- The no of possible addresses = 2^{32-n}

Q) 205.16.37.39/28, find the 1st and last addresses in the block. Also **find the no of addresses in the block**.

- **Binary representation** of a given address and **mask** are

11001101 00010000 00100101 00100111 (**address**)

11111111 11111111 11111111 11110000 (**mask**) 8+8+8+4= /28

(Total bits=32 (8 bits each) so 28bits 1 and other 4 bits 0)

1 1 1 1 1 1 1 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

- To get the **first address** in the block, set **32-28=4**.
- Rightmost bits to set to 0, so we get,

11001101 00010000 00100101 00100111 (address)

11001101 00010000 00100101 00100000 205.16.37.32

(last 4 bits of the original address is set to 0)

- To get the **last address** in the block , set **32-28=4**
- Rightmost bits to set to 1, so we get,

11001101 00010000 00100101 00100111 (address)

11001101 00010000 00100101 00101111 205.16.37.47

- So the no of addresses $= 2^{32-n} = 2^{32-28} = 2^4 = 16$

The no of addresses in the block = 16

CIDR

- **Number of Subnets:**
  - 2^n
  - n = Number of 1's in the Subnet ID
- **Number of available host addresses:**
  - $2^n - 2$
  - n = Number of 0's in the Host ID
  - Host ID cannot be all 0's or all 1's
- **Example:**
  - 11111111.11111111.11111000.00000000
  - 2^5 = 32 Subnets
  - $2^{11} - 2$ = 2046 Available hosts in each subnet

1 1 1 1 1 1 1 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

- **Without CIDR Notation**
  - 192.168.10.1
  - 255.255.255.248

IP address
Subnetmask (32-29=3)□last 3 bits 0□248

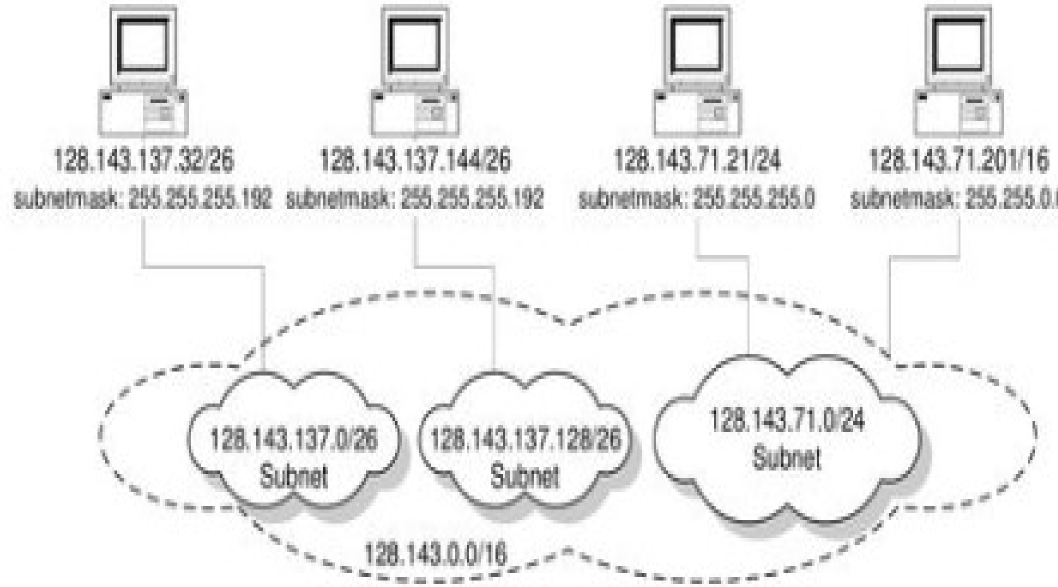
- **With CIDR Notation**
  - 192.168.10.1/29

29 means no of bits in the n/w ID
32-29=3 no of bits in host ID□ 2^3 □8
No of available host□2^3 - 2= 6

Classless addressing

CIDR Block Prefix	# of Host Addresses
/27	32 hosts
/26	64 hosts
/25	128 hosts
/24	256 hosts
/23	512 hosts
/22	1,024 hosts
/21	2,048 hosts
/20	4,096 hosts
/19	8,192 hosts
/18	16,384 hosts
/17	32,768 hosts
/16	65,536 hosts
/15	131,072 hosts
/14	262,144 hosts
/13	524,288 hosts

- **Subnetting**:
  - Subnets are created by extending the network prefix



- **Supernetting**:
  - Multiple prefixes can be summarized with a single prefix, by reducing the network prefix:

    128.143.0.0/16
    128.142.0.0/16 → 128.142.0.0/15

  - If neighboring networks have similar address blocks, supernetting reduces the size of routing tables
  - Route Aggregation: Routing table entries can be reduced, when prefixes can be collapsed and networks have the same outgoing interface

Sub netting	Super netting
A process of dividing a network into the sub networks.	A process of combining small networks into a larger network.
The number of bits of network addresses is increased.	The number of bits of host addresses is increased.
Mask bits are moved towards right of the default mask.	Mask bits are moves towards left of the default mask.
Sub netting is implemented using VLSM (variable length subnet mask)	Super netting is implemented using CIDR classless inter domain routing.
The objective is to reduce the address depletion.	The objective is to simplify and fasten the routing process.

Private IP Range

The IP number falls within one of the IP address ranges reserved for private uses by Internet standards groups.

These private IP address ranges exist:

- ✓ 10.0.0.0 through 10.255.255.255 (Class A)
- ✓ 169.254.0.0 through 169.254.255.255
- ✓ 172.16.0.0 through 172.31.255.255 (Class B)
- ✓ 192.168.0.0 through 192.168.255.255 (Class C)

Private IP addresses are typically used on **local networks** including home, school and business LANs including airports and hotels.

Devices with private IP addresses cannot connect directly to the Internet.

Instead, access to such devices must be brokered by a router or similar device that supports **Network Address Translation (NAT)**

NAT hides the private IP numbers but can selectively transfer messages to these devices, affording a layer of security to the local network.