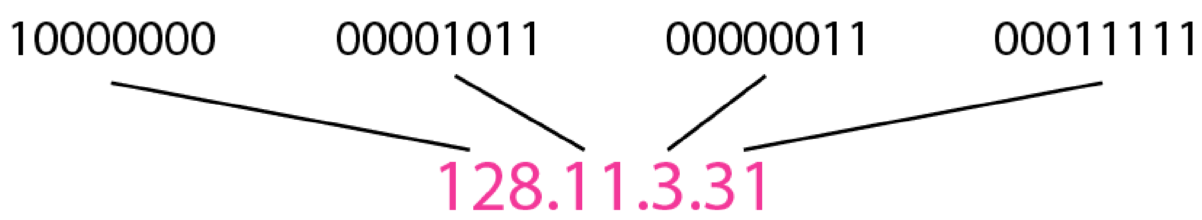
Unit 2

Topics	Resource
IPv4 addresses, Address space, Notations - Classful addressing- problem solving	Forouzan
Two level hierarchy - Three level hierarchy- subnet mask - Address aggregation- problem solving.	Forouzan
Special addresses. Special Blocks and Special addresses in each block. Introduction to IPv6 address.	Forouzan
Classless addressing - Variable length blocks- Two level addressing- Block allocation - Sub netting- problem solving	Bhushan Trivedi
Private address, Network addresses translation - Super netting.	Forouzan
Intermediate devices - Hub, Repeaters, Switch, Bridge- Gateways -Structure of a ROUTER	Forouzan

IPv4 addresses, Address space, Notations -Classful addressing-problem solving

IPv4 Address ,address space

- The IPv4 addresses are unique and universal.
- An IPv4 address is 32 bits long.
  - The address space of IPv4 is 2^{32} (4,294,967,296)
  - Notation.
    - Binary notation
    - Dotted-decimal notation



IPv4

- 32 bits long
  - An **IPv4 address is a 32-bit address that *uniquely and universally defines the connection*** of a device (for example, a computer or a router) to the Internet.
- Unique and Universal.
  - Two devices on the Internet can never have the same address at the same time
  - Addressing system must be accepted by any host that wants to be connected to the Internet.

IPV4 NOTATIONS

IP Address: Binary Notation – 32-bit / 4-byte representation with a space inserted between each octet (byte)

IP Address: Decimal Notation – 4-number decimal representation with a decimal dot separating the numbers

- each decimal number corresponds to a byte
  ⇒ each decimal number ∈ [0, 255]

10000000 00001011 00000011 00011111

128.11.3.31

IP address = network part + host part

network part: assigned by global authority (ICANN) to organization

host part: assigned by local authority to particular machine

Example [IP Address Conversion]

Change the following IP addresses from binary to dotted decimal notation.

(a) 10000001 00001011 00001011 11101111 ⇒ 129.11.11.239
(b) 11111001 10011011 11111011 00001111 ⇒ 249.155.251.15

•An easier way to remember IP addresses is by assigning to them a name.

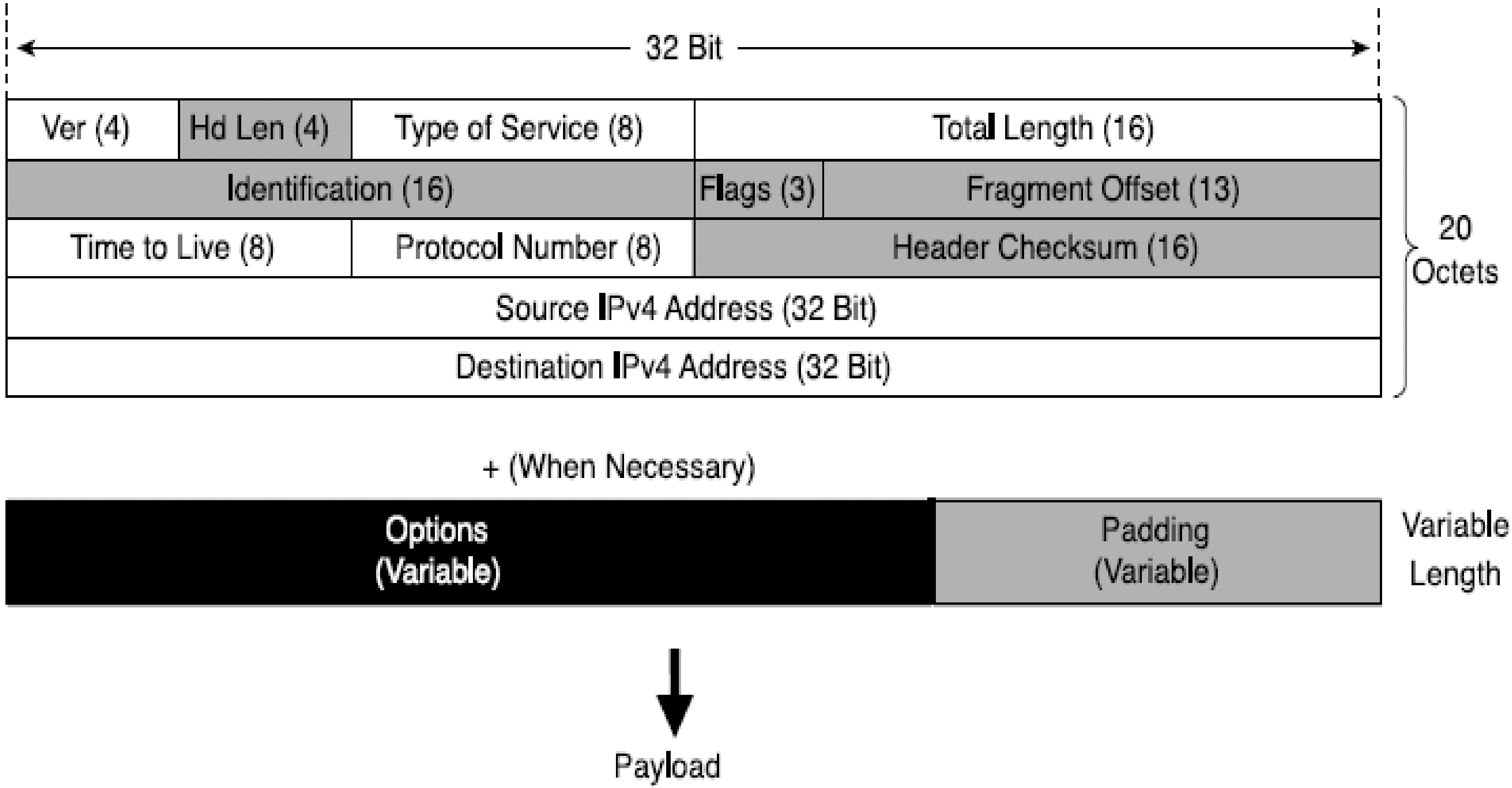
•(e.g., www.google.com), which is resolver through the Domain Name System (DNS).

•Strictly speaking, an IP address identifies an **interface that is capable of sending and** receiving IP datagrams.

•One system can have multiple such interfaces.

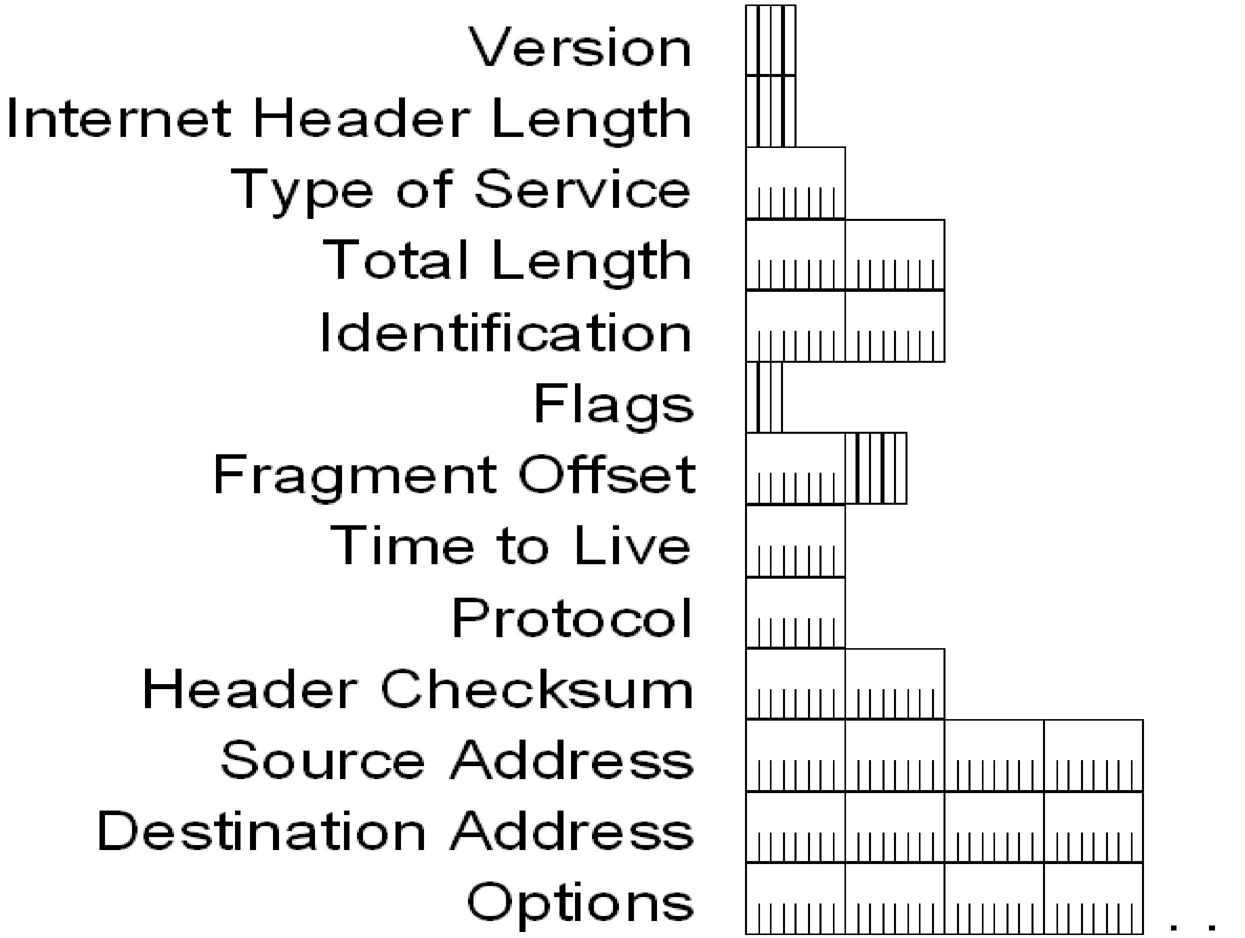
•Usually, hosts have only one interface (thus, one IP address), whereas routers have many interfaces (thus, many IP addresses).

IPv4 Header Structure



- basic IPv4 header contains 12 fields.
- each field of the IPv4 header has a specific use.
- Shaded field are removed in IPv6.

IPv4 Header - Review



IPv4 Header - Review

- **Version (4 bits)**
  - Indicates the version of IP and is set to 4.
- **Internet Header Length (4 bits)**
  - Indicates the number of 4-byte blocks in the IPv4 header.
  - Because an IPv4 header is a minimum of 20 bytes in size, the smallest value of the Internet Header Length (IHL) field is 5.
- **Type of Service (4 bits)**
  - Indicates the desired service expected by this packet for delivery through routers across the IPv4 internetwork.

IPv4 Header - Review

- **Total Length (16 bits)**
  - Indicates the total length of the IPv4 packet (IPv4 header + IPv4 payload) and does not include link layer framing.
- **Identification (16 bits)**
  - Identifies this specific IPv4 packet.
  - The Identification field is selected by the originating source of the IPv4 packet. If the IPv4 packet is fragmented, all of the fragments retain the Identification field value so that the destination node can group the fragments for reassembly.
- **Flags (3 bits)**
  - Identifies flags for the fragmentation process.
  - There are two flags—one to indicate whether the IPv4 packet might be fragmented and another to indicate whether more fragments follow the current fragment.
- **Fragment Offset (13 bits)**
  - Indicates the position of the fragment relative to the original IPv4 payload.

IPv6 Packet Format

IPv4 Header - Review

- **Time to Live (8 bits)**
  - Indicate the maximum number of links on which an IPv4 packet can travel before being discarded.
  - Originally used as a time count with which an IPv4 router determined the length of time required (in seconds) to forward the IPv4 packet, decrementing the TTL accordingly. When the TTL equals 0,an ICMP Time Expired-TTL Expired in Transit message is sent to the source IPv4 address and the packet is discarded.
- **Protocol (8 bits)**
  - Identifies the upper layer protocol.
  - For example, TCP uses a Protocol of 6, UDP uses a Protocol of 17, and ICMP uses a Protocol of 1.
  - The Protocol field is used to demultiplex an IPv4 packet to the upper layer protocol.

IPv6 Packet Format

IPv4 Header - Review

- **Header Checksum (16 Bits)**
  - Provides a checksum on the IPv4 header only.
  - The IPv4 payload is not included in the checksum calculation as the IPv4 payload and usually contains its own checksum..
- **Source Address (32 bits)**
  - Stores the IPv4 address of the originating host.
- **Destination Address (32 bits)**
  - Stores the IPv4 address of the destination host.
- **Options (multiple of 32 bits)**
  - Stores one or more IPv4 options.

Types of addressing

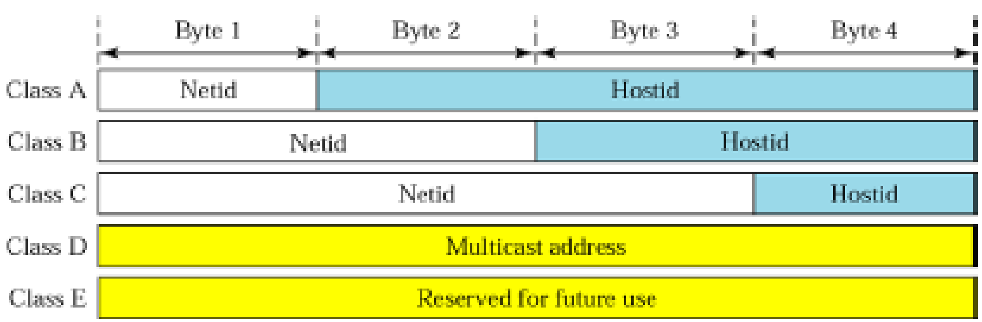
- Classful Addressing
- Classless Addressing

Classful Addressing and Problem solving

Classful IP Addressing

Classful IP Addressing – supports addressing of different size networks by dividing address space into 5 classes: A, B, C, D, E

- an IP address in classes A, B, and C is divided into Netid and Hostid
- class A addresses (1-byte Netid): get assigned to organizations with a large number of hosts or routers – there are only <u>126 class A networks</u> with up to 16 million hosts in each
- class B addresses (2-byte Netid): allow around 16,000 networks and around 64,000 hosts per each network
- class C addresses (3-byte Netid): allow around 2 million networks and around 254 hosts per each network

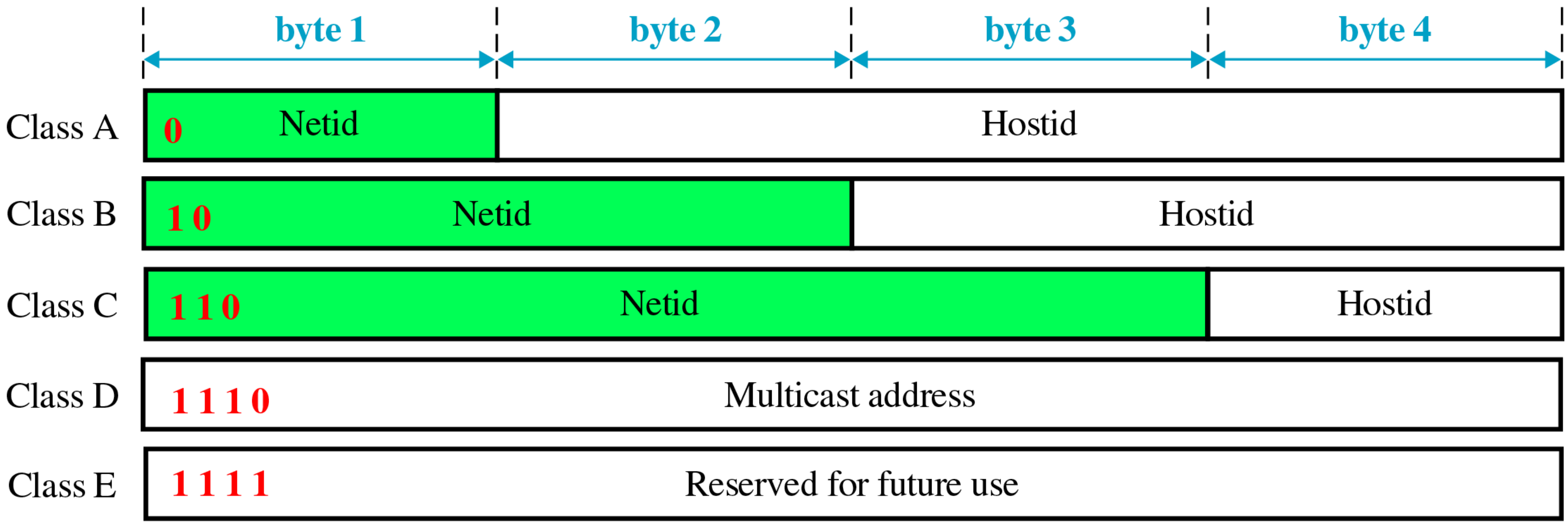


While many class A and B addresses are wasted, the number of addresses in class C is smaller than the needs of most organizations.

How do we know if an IP address is a class-A / B or C!?

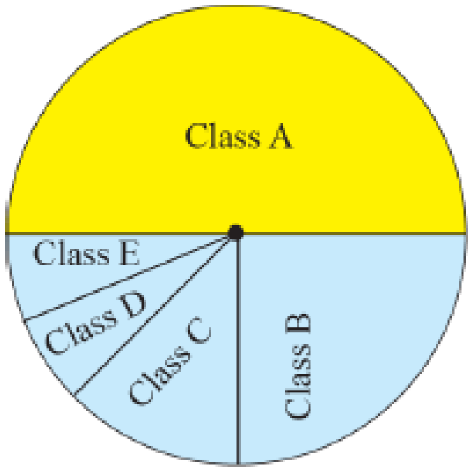
Classful Addressing

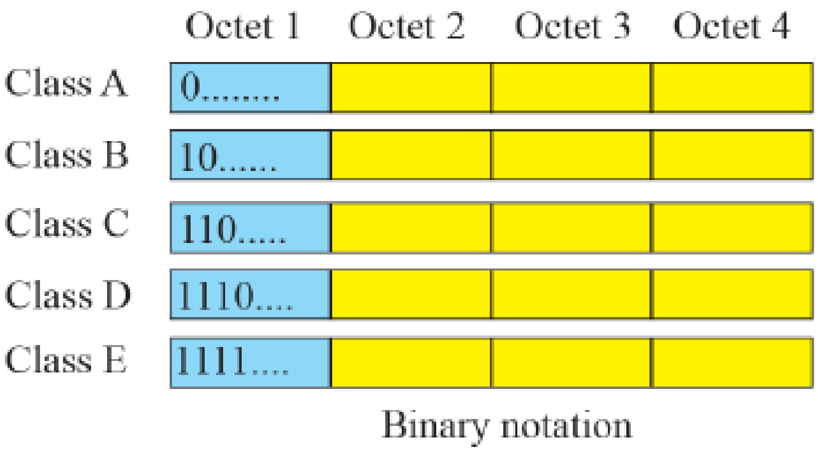
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.



Classful IP Addressing (cont.)

Occupation of Address Space by Class





Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Classful Addressing – Class Range

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

127.0. 0.1- loop back address- looped upto NIC card

Example 19.1

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Example 19.2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 19.4

Find the class of each address.

a. <u>**0**</u>0000001 00001011 00001011 11101111

b. <u>**110**</u>00001 10000011 00011011 11111111

c. <u>**14**</u>.23.120.8

d. <u>**252**</u>.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; the class is A.

d. The first byte is 252; the class is E.

Table 19.1 ***Number of blocks and block size in classful IPv4 addressing***

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Note

In classful addressing, a large part of the available addresses were wasted.

Table 19.2 *Default masks for classful addressing*

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	**11111111** 00000000 00000000 00000000	**255**.0.0.0	/8
B	**11111111 11111111** 00000000 00000000	**255.255**.0.0	/16
C	**11111111 11111111 11111111** 00000000	**255.255.255**.0	/24

CIDR- Classless Inter Domain Routing

Note

Classful addressing, which is almost obsolete, is replaced with classless addressing.

Note

In IPv4 addressing, a block of
addresses can be defined as
x.y.z.t /*n*
in which x.y.z.t defines one of the addresses and the /*n* defines the mask.

Note

The first address in the block can be found by setting the rightmost
32 – n bits to 0s.

Example 19.6

A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block?

Solution

The binary representation of the given address is

11001101 00010000 00100101 00100111

If we set 32−28 rightmost bits to 0, we get

11001101 00010000 00100101 0010000

or

205.16.37.32.

This is actually the block shown in Figure 19.3.

Note

The last address in the block can be found by setting the rightmost 32 – n bits to 1s.

Example 19.7

Find the last address for the block in Example 19.6.

Solution

The binary representation of the given address is

11001101 00010000 00100101 00100111

If we set 32 − 28 rightmost bits to 1, we get

11001101 00010000 00100101 00101111

or

205.16.37.47

This is actually the block shown in Figure 19.3.

Note

The number of addresses in the block can be found by using the formula 2^{32-n}.

Example 19.8

Find the number of addresses in Example 19.6.

Solution

The value of n is 28, which means that number of addresses is 2^{32-28} or 16.

Example 19.9

Another way to find the first address, the last address, and the number of addresses is to represent the mask as a 32-bit binary (or 8-digit hexadecimal) number. This is particularly useful when we are writing a program to find these pieces of information. In Example 19.5 the /28 can be represented as

11111111 11111111 11111111 11110000

(twenty-eight 1s and four 0s).

Find

a. The first address
b. The last address
c. The number of addresses.

Example 19.9 (continued)

Solution

a. The first address can be found by ANDing the given addresses with the mask. ANDing here is done bit by bit. The result of ANDing 2 bits is 1 if both bits are 1s; the result is 0 otherwise.

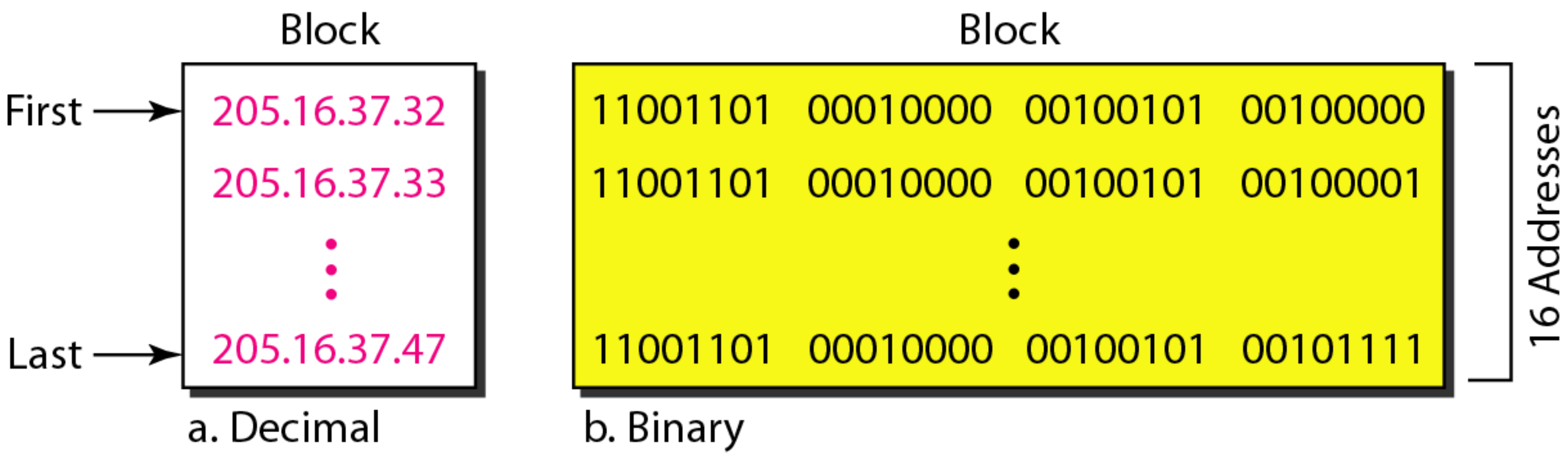
Address:	11001101	00010000	00100101	00100111
Mask:	**11111111**	**11111111**	**11111111**	**11110000**
First address:	11001101	00010000	00100101	00100000

Example 19.9 (continued)

b. *The last address can be found by ORing the given addresses with the complement of the mask. ORing here is done bit by bit. The result of ORing 2 bits is 0 if both bits are 0s; the result is 1 otherwise. The complement of a number is found by changing each 1 to 0 and each 0 to 1.*

Address:	11001101	00010000	00100101	00100111
Mask complement:	**00000000**	**00000000**	**00000000**	**00001111**
Last address:	11001101	00010000	00100101	00101111

Figure 19.4 *A network configuration for the block 205.16.37.32/28*



Note

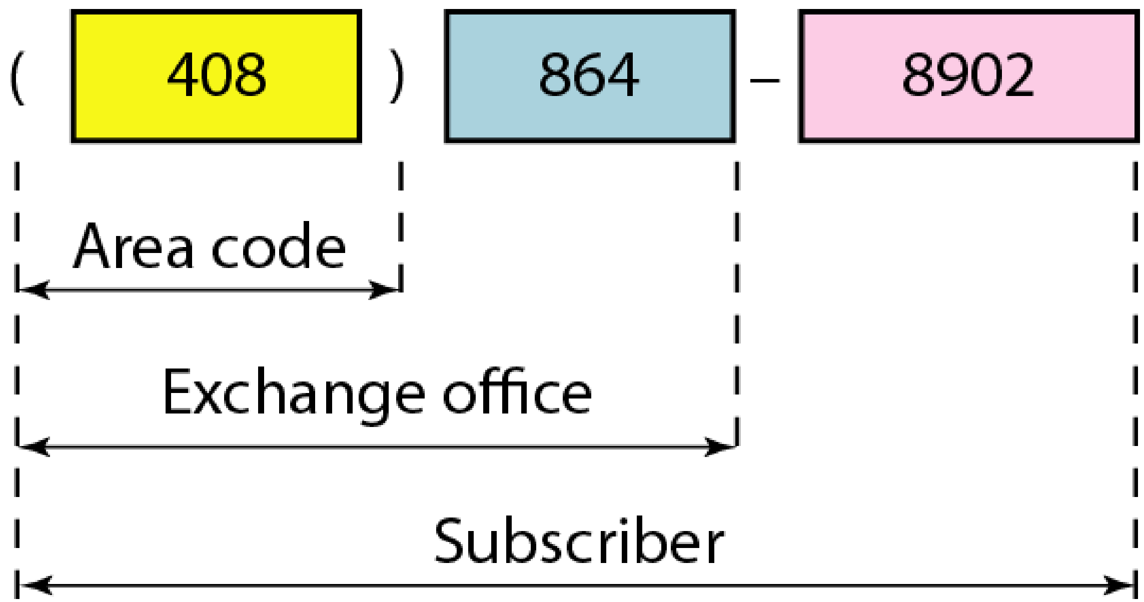
The first address in a block is
normally not assigned to any device;
it is used as the network address that represents the organization
to the rest of the world.

Two level hierarchy - Three level hierarchy- subnet mask - Address aggregation- problem solving.

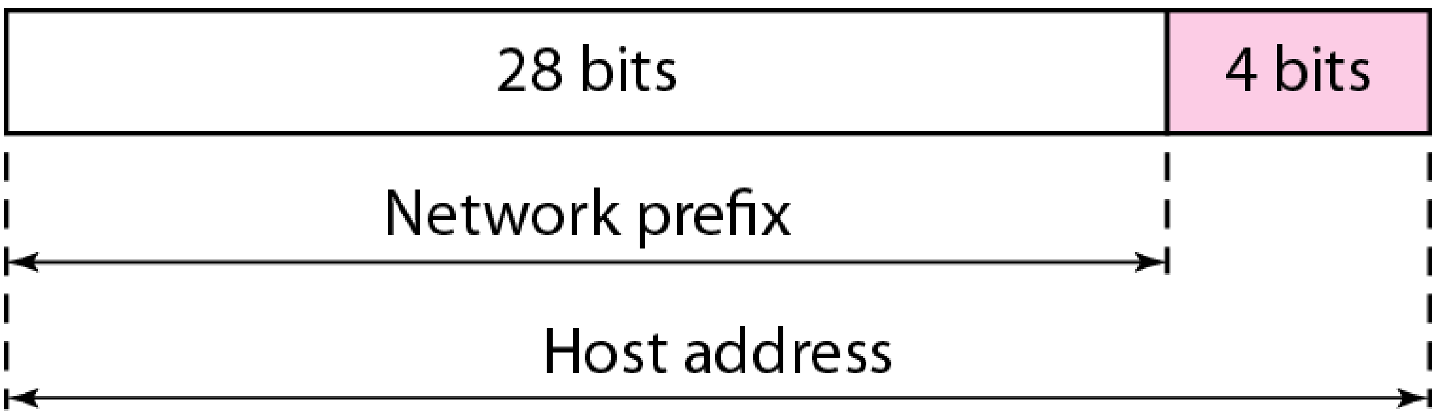
Hierarchy of IPv4 Addressing

- Each address in the block can be considered as a two-level hierarchical structure: the leftmost *n* bits (prefix) define the network; the rightmost 32 − *n* bits define the host.
- Why Hierarchy?

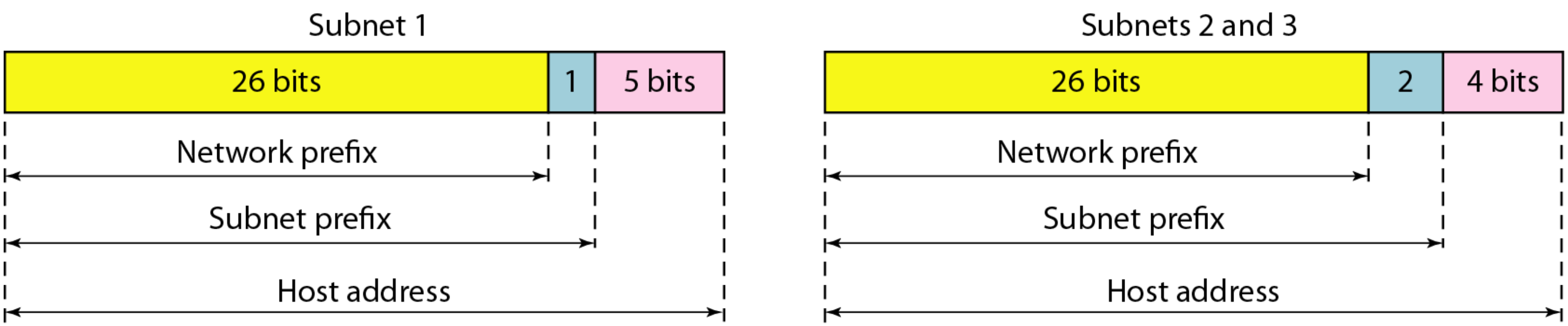
Figure 19.5 *Two levels of hierarchy in an IPv4 address*



Two Level of Hierarchy



Three Level of Hierarchy



Address Aggregation

- IP Address Aggregator is a utility developed to automate minimization process and convert bunch of IPv4 addresses into smallest continuous range(s) possible. IP aggregation is commonly performed by network engineers working with BGP & routers.
- This utility will help webmasters to configure server firewalls, apache, address masks and so on.

Special addresses.
Special Blocks and Special addresses in each block.
Introduction to IPv6 address.

Special Addresses

- *This-host* address
- *Limited-broadcast* address
- *Loopback* address
- *Private* addresses
- *Multicast* addresses.

Special Addresses

This-host Address

- The only address in the block 0.0.0.0/32 is called the this-host address.
- It is used whenever a host needs to send an IP datagram but it does not know its own address to use as the source address.

Special Addresses

Limited-broadcast Address

- The only address in the block 255.255.255.255/32 is called the limited-broadcast address.
- It is used whenever a router or a host needs to send a datagram to all devices in a network.
- The routers in the network, however, block the packet having this address as the destination;
- the packet cannot travel outside the network.

Special Addresses

Loopback Address

- The block **127.0.0.0/8** is called the *loopback* address.
- A packet with one of the addresses in this block as the destination address never leaves the host; it will remain in the host.
- Any address in the block is used to test a piece of software in the machine.
- For example, we can write a client and a server program in which one of the addresses in the block is used as the server address. We can test the programs using the same host to see if they work before running them on different computers.

MULTICAST ADDRESS

- The block 224.0.0.0/**4** is reserved for multicast addresses

Classes and Blocks

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size

The classful addressing wastes a large part of the address space

Table 19.1 *Number ofblocks and block size in classfulIPv4 addressing*

Class	*Number ofBlocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

INTRODUCTION to Internet Protocol, Version 6 (IPv6)

IPv6 Address Space

IPv4 32-bits

IPv6 128-bits

2^{32} = 4,294,967,296

2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

$2^{128} = 2^{32} * 2^{96}$

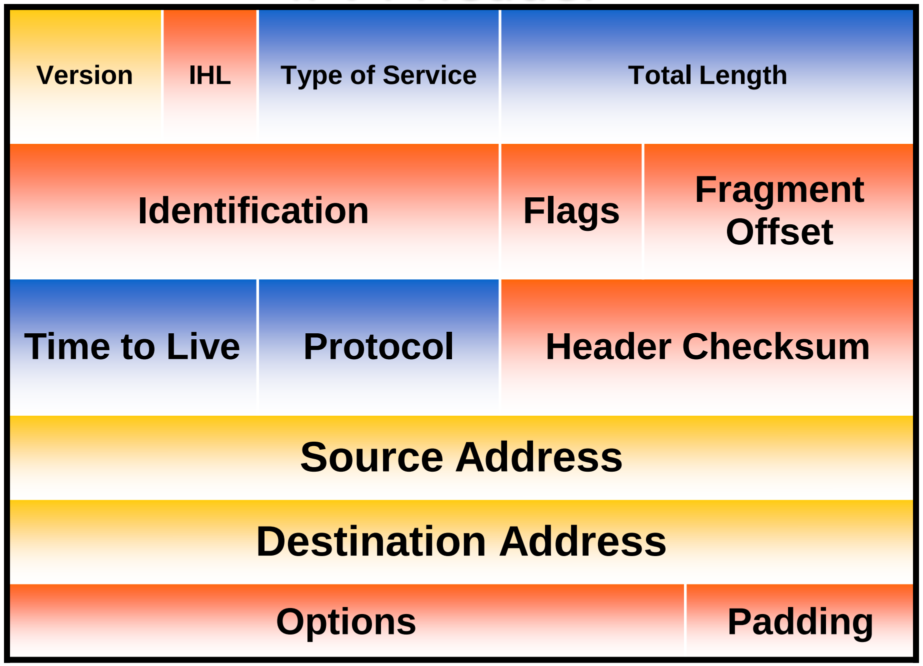
2^{96} = 79,228,162,514,264,337,593,543,950,336 times the number of possible IPv4 Addresses (79 trillion trillion)

Why IPv6?

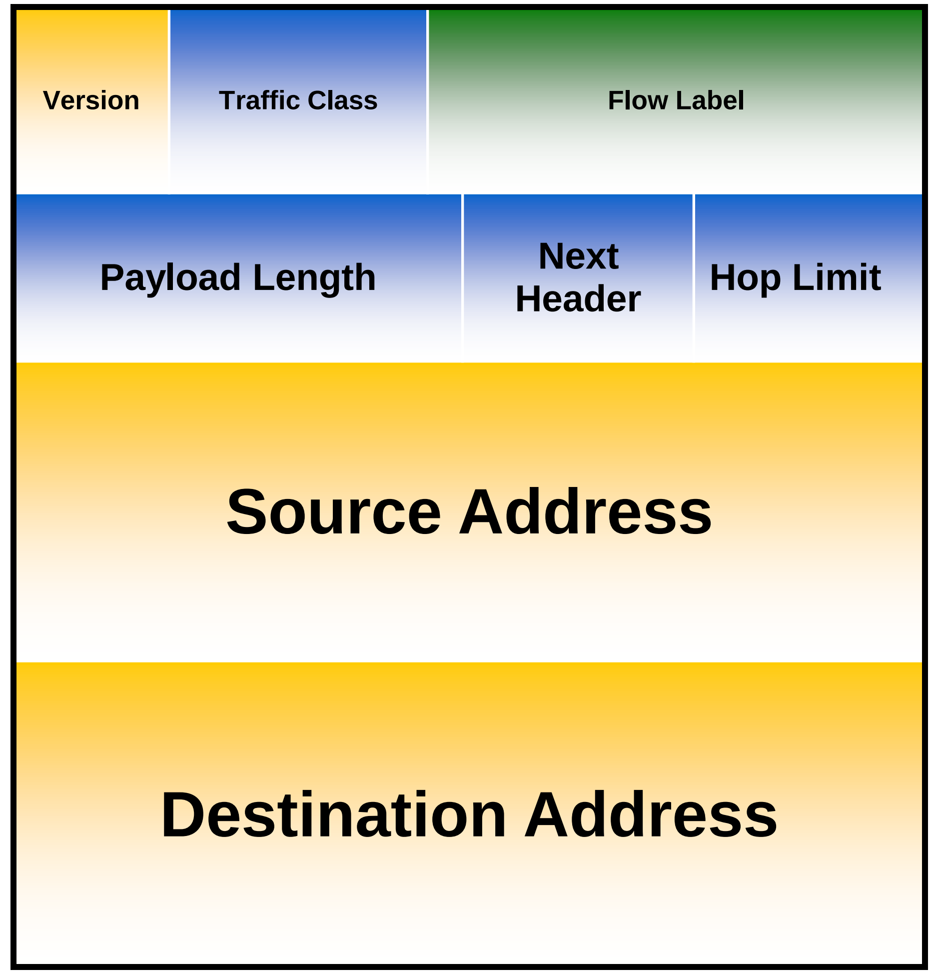
- Deficiency of IPv4
- Address space exhaustion
- New types of service → Integration
  - Multicast
  - Quality of Service
  - Security
  - Mobility (MIPv6)
- Header and format limitations

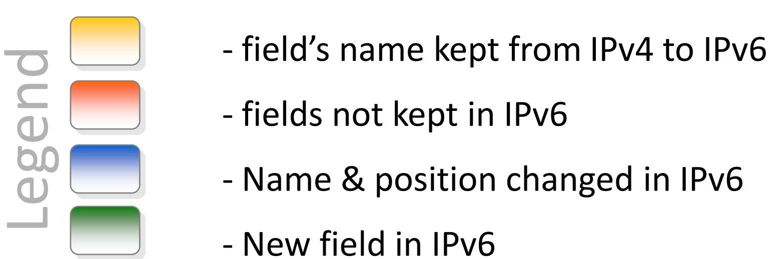
IPv4 & IPv6 Header Comparison

IPv4 Header



IPv6 Header





IPv6 Header Fields

- Based on these rules, RFC 2460 defines the following IPv6 header fields:

1. **Version (4 bits)**
   - 4 bits are used to indicate the version of IP and is set to 6

- **Traffic Class (8 bits)**
   - same function as the Type of Service field in the IPv4 header.

1. **Flow Label (20 bits)**
   - identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups within those packets.
   - set by the source and should not be changed by routers along the path to destination.

IPv6 Header Fields

4. **Payload Length (16 bits)**
   - With the header length fixed at 40 bytes, it is enough to indicate the length of the payload to determine the length of the entire packet.

5. **Next Header (8 bits)**
   - Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6).

6. **Hop Limit (8 bits)**
   - In IPv6, the IPv4 TTL was appropriately renamed Hop Limit because it is a variable that is decremented at each hop, and it does not have a temporal dimension.

IPv6 Header Fields

7. Source IPv6 Address (128 bits)

- Stores the IPv6 address of the originating host.

8. Destination IPv6 Address (128 bits)

- Stores the IPv6 address of the current destination host.

Values of the Next Header Field

Value (in decimal)	Header
0	Hop-by-Hop Options Header
6	TCP
17	UDP
41	Encapsulated IPv6 Header
43	Routing Header
44	Fragment Header
46	Resource ReSerVation Protocol
50	Encapsulating Security Payload
51	Authentication Header
58	ICMPv6
59	No next header
60	Destination Options Header

Basis for differences	IPv4	IPv6
Size of IP address	IPv4 is a 32-Bit IP Address.	IPv6 is 128 Bit IP Address.
Addressing method	IPv4 is a numeric address, and its binary bits are separated by a dot (.)	IPv6 is an alphanumeric address whose binary bits are separated by a colon (:). It also contains hexadecimal.
Number of header fields	12	8
Length of header filed	20	40
Checksum	Has checksum fields	Does not have checksum fields
Example	12.244.233.165	2001:0db8:0000:0000:0000:ff00:0042:7879
Type of Addresses	Unicast, broadcast, and multicast.	Unicast, multicast, and anycast.
Number of classes	IPv4 offers five different classes of IP Address. Class A to E.	IPv6 allows storing an unlimited number of IP Address.
Configuration	You have to configure a newly installed system before it can communicate with other systems.	In IPv6, the configuration is optional, depending upon on functions needed.
VLSM support	IPv4 support VLSM (Virtual Length Subnet Mask).	IPv6 does not offer support for VLSM.
Fragmentation	Fragmentation is done by sending and forwarding routes.	Fragmentation is done by the sender.

Basis for differences	IPv4	IPv6
Routing Information Protocol (RIP)	RIP is a routing protocol supported by the routed daemon.	RIP does not support IPv6. It uses static routes.
Network Configuration	Networks need to be configured either manually or with DHCP. IPv4 had several overlays to handle Internet growth, which require more maintenance efforts.	IPv6 support autoconfiguration capabilities.
Best feature	Widespread use of NAT (Network address translation) devices which allows single NAT address can mask thousands of non-routable addresses, making end-to-end integrity achievable.	It allows direct addressing because of vast address Space.
Address Mask	Use for the designated network from host portion.	Not used.
Security	Security is dependent on applications - IPv4 was not designed with security in mind.	IPSec(Internet Protocol Security) is built into the IPv6 protocol, usable with a proper key infrastructure.
Packet size	Packet size 576 bytes required, fragmentation optional	1208 bytes required without fragmentation
IP to MAC resolution	Broadcast ARP	Multicast Neighbour Solicitation
Optional Fields	Has Optional Fields	Does not have optional fields. But Extension headers are available.
Dynamic host configuration Server	Clients have approach DHCS (Dynamic Host Configuration server) whenever they want to connect to a network.	A Client does not have to approach any such server as they are given permanent addresses.
Mapping	Uses ARP(Address Resolution Protocol) to map to MAC address	Uses NDP(Neighbour Discovery Protocol) to map to MAC address

Advantages of IPv6 over IPv4

- Larger address space
- Better header format
- New options
- Allowance for extension
- Support for resource allocation
- Support for more security
- Support for mobility

Classless addressing - Variable length blocks- Two level addressing- Block allocation - Sub netting- problem solving

Classless Addressing

- **To overcome address depletion** and give **more organizations access to the Internet**, classless addressing was designed and implemented.

Classless Addressing

Address Blocks

- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a **BLOCK (RANGE) OF ADDRESSES**.
- The size of the block (the number of addresses) varies based on the nature and size of the entity.
- **For example:**
  - **A household → only two addresses**
  - **A large organization → given thousands of addresses.**
  - **An ISP, as the Internet service provider → given thousands or hundreds of thousands based on the number of customers it may serve.**

Restriction

To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

- Addresses in a block must be contiguous, one after another.
- Number of addresses in a block must be a power of 2 (I, 2, 4, 8, ...).
- First address must be evenly divisible by the number of addresses.

Mask or subnet Mask

- A better way to define a block of addresses is to **select any address in the block and the mask.**
- A mask is a 32-bit number in which
  - ***n leftmost bits* are 1 s**
  - **32 - *n rightmost bits are O s.***
- *In classless addressing the mask* for a block can take any value from 0 to 32.
- It is very convenient to give just the value of ***n preceded by a slash*** *(CIDR notation).*

Network Address

- Can be found by **setting the 32 - *n rightmost* bits in the binary notation of the address to Os.**
- *Example*

  A block of addresses is granted to a small organization. We know that one of the addresses is **205.16.37.39/28.** What is the first/network address in the block?

Solution

- The binary representation of the given address is **11001101 00010000 00100101 00100111.**
- If we set 32 - 28 rightmost bits to 0, we get **11001101 0001000 00100101 00100000** or **205.16.37.32.**

Broadcast Address

- Can be found by setting the 32 - *n rightmost* bits in the binary notation of the address to 1 s.
- ***Example:***

  A block of addresses is granted to a small organization. We know that one of the addresses is **205.16.37.39/28.** What is the last/broadcast address in the block? Solution

- The binary representation of the given address is 11001101 00010000 00100101 00100111.
- If we set 32 - 28 rightmost bits to 1, we get 11001101 00010000 00100101 00101111 or 205.16.37.47.

Number of Addresses

- The number of addresses in the block is the **difference between the last and first address.**
- It can easily be found using the formula .

$$2^{32-n}$$

- **<u>Eg</u>**: Find the number es in above Example.

Soln

- The value of *n is 28, which means that number of addresses is or 16.*

$$2^{32-28}$$

Example

- Another way to find the network address, the broadcast address, and the number of addresses is to represent the mask as a 32-bit binary (or 8-digit hexadecimal) number.

Eg: **/28** can be represented as

11111111 11111111 11111111 11110000 (twenty-eight Is and four Os).

Find

- Network address
- Broadcast address
- The number of addresses

Network/subnet address

- Found by ANDing the given addresses with the mask.
- ANDing here is done bit by bit. The result of ANDing 2 bits is 1 if both bits are Is; the result is 0 otherwise.
- Address: 11001101 00010000 00100101 00100111
- Mask: 11111111 11111111 11111111 11110000

Network

address/

neid/

subnet address: 11001101 00010000 00100101 00100000

(or)

` **205.16.37.32.**

Broadcast address

- Found by ORing the given addresses with the complement of the mask. ORing here is done bit by bit.
- The result of ORing 2 bits is 0 if both bits are Os; the result is 1 otherwise.
- The complement of a number is found by changing each 1 to 0 and each 0 to 1.

- Address: 11001101 00010000 00100101 00100111
- Mask : 00000000 00000000 00000000 00001111
- Broadcast

add: 11001101 00010000 00100101 00101111

(or)

205.16.37.47.

Number of addresses

- The number of addresses can be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it.
- Mask complement:

  000000000 00000000 00000000 00001111

- Number of addresses: 15 + 1 =16

Subnetting

Subnetting - which allows you to take one larger network and break it into many smaller networks.

Reduced network traffic
Optimized network performance
Simplified management
Facilitated spanning of large geographical distances

Subnet Masks

Every machine on the network must know which part of the host address will be used as the subnet address

Default Subnet Mask

Class	Format	Default Subnet Mask
A	Net.Node.Node.Node	255.0.0.0
B	Net.Net.Node.Node	255.255.0.0
C	Net.Net.Net.Node	255.255.255.0

Subnetting Class C Addresses

The Binary Method: Subnetting a Class C Address
The first subnet mask available with a Class C address, which borrows two bits from subnetting. For this example, we are using 255.255.255.192.

192=11000000 Two bits for subnetting, 6 bits for defining the hosts in each subnet. What are the subnets?

01000000=64 (all host bits off)
or
10000000=128 (all host bits off)

Subnet 64

Subnet	Host	Meaning
01	000000=64	The network (do this first)
01	000001=65	The first valid host
01	111110=126	The last valid host
01	111111=127	The broadcast address (do this second)

Subnet 128

Subnet	Host	Meaning
10	000000=128	The subnet address
10	000001=129	The first valid host
10	111110=190	The last valid host
10	111111=191	The broadcast address

The Alternate Method: Subnetting a Class C Address

1. How many subnets does the subnet mask produce?
2. How many valid hosts per subnet?
3. What are the valid subnets?
4. What are the valid hosts in each subnet?
5. What is the broadcast address of each subnet?

Here is how you determine the answers to the five questions:
1. How many subnets? 2x–2=amount of subnets. X is the amount of masked bits, or the 1s. For example, 11000000 is 22–2. In this example, there are 2 subnets.
2. How many hosts per subnet? 2x–2=amount of hosts per subnet. X is the amount of unmasked bits, or the 0s. For example, 11000000 is 26–2. In this example, there are 62 hosts per subnet.
3. What are the valid subnets? 256–subnet mask=base number. For example, 256–192=64. Keep adding the variable to itself until you reach the subnet mask.
4. What are the valid hosts? Valid hosts are the numbers between the subnets, minus all 0s and all 1s.
5. What is the broadcast address for each subnet? Broadcast address is all host bits turned on, which is the number immediately preceding the next subnet.

Practice Example 2: 255.255.255.224

In this example, you will subnet the network address 192.168.10.0 and subnet mask 255.255.255.224.

TABLE 3.7 The Class C 255.255.255.224 Mask

Subnet 1	Subnet 2	Subnet 3	Subnet 4	Subnet 5	Subnet 6	Meaning
32	64	96	128	160	192	The subnet address
33	65	97	129	161	193	The first valid host
62	94	126	158	190	222	Our last valid host
63	95	127	159	191	223	The broadcast address

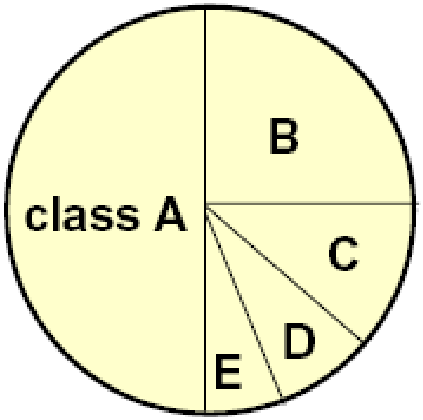
IP Address Table

class	initial bits	#bit net	#bit host	range
A	0	7	24	0.0.0.0 127.255.255.255
B	10	14	16	128.0.0.0 191.255.255.255
C	110	21	8	192.0.0.0 223.255.255.255
D	1110	28	-	224.0.0.0 239.255.255.255
E	11110	27	-	240.0.0.0 247.255.255.255

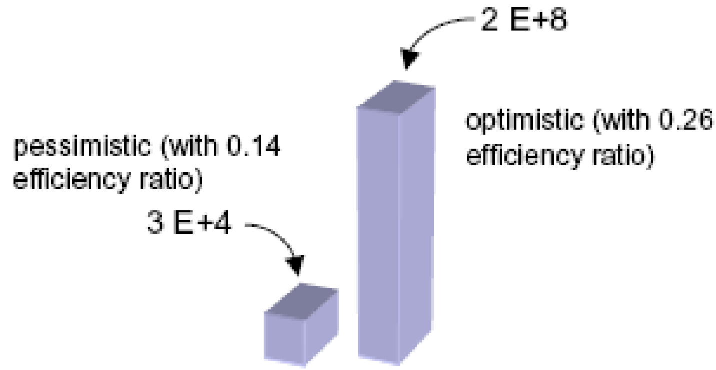
class	address spaces	usable
A	2^24=16677216	166777214
B	2^16=65536	65534
C	2^8 =256	254

Problems with Class assignment

- class A takes 50% range, class B 25%, class C 12.5%
- These leads to :
  - address wasteful (specially in class A)
  - running out of IP address

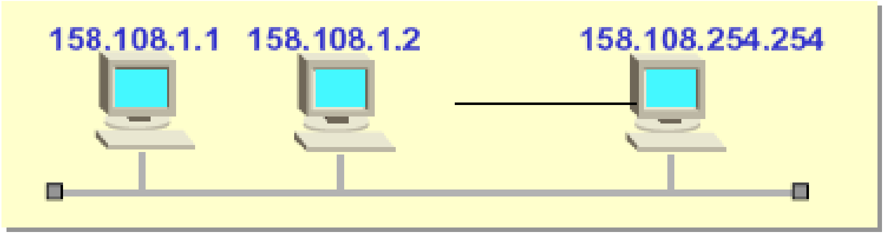


Population counts in the network with 32 bits address format [RFC1715]

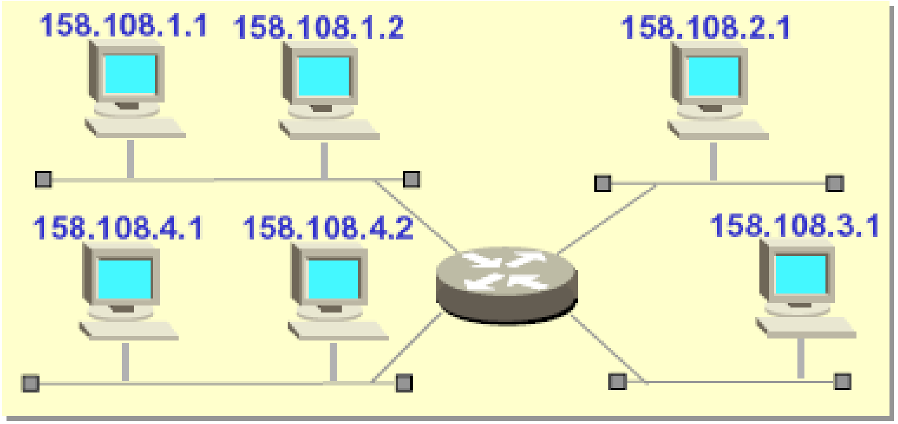


Problem with large networks

- Class B "Flat network" more than 60000 hosts
  - How to manage?
  - Performance?

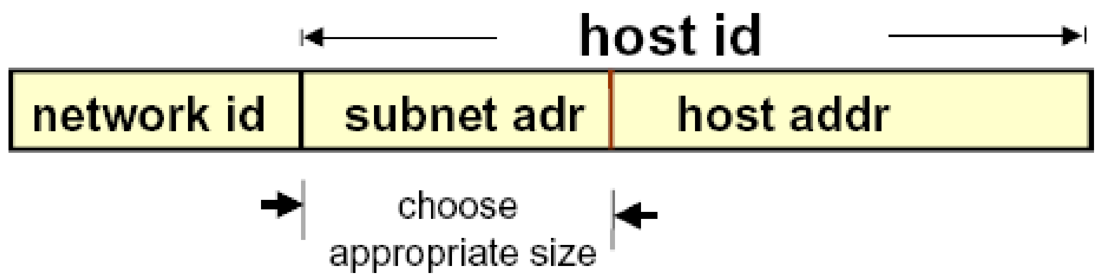


- Class B "subdivided network" to smaller groups with router



How to assign subnet

- Divide host id into 2 pieces



- Class B address such as 158.108 might use its third byte to identify subnet e.g.
  - subnet#1 158.108.1.X x=host addr range from 1-254
  - subnet#2 158.108.2.X

Subnet mask bits

- use contiguous subnet mask

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255

Subnet Class B Example

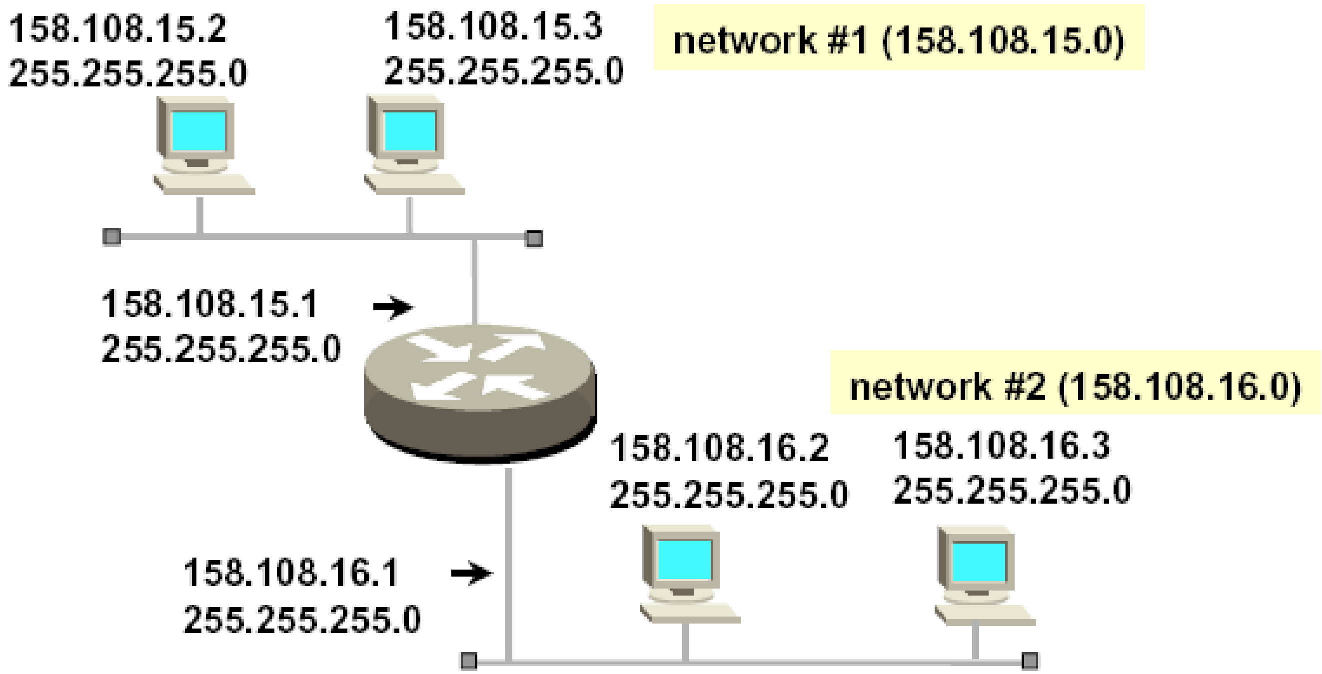
- 255.255.0.0 (0000 0000 0000 0000)
  - 0 subnet with 65534 hosts (default subnet)
- 255.255.192.0 (1100 0000 0000 0000)
  - 2 subnets with 16382 hosts
- 255.255.252.0 (1111 1100 0000 0000)
  - 62 subnets with 1022 hosts
- 255.255.255.0 (1111 1111 0000 0000)
  - 254 subnets with 254 hosts
- 255.255.255.252 (1111 1111 1111 1100)
  - 16382 subnets with 2 hosts

Subnet Class C Example

- 255.255.255.0 (0000 0000)
  - 0 subnet with 254 hosts (default subnet)
- 255.255.255.192 (1100 0000)
  - 2 subnets with 62 host
- 255.255.255.224 (1110 0000)
  - 6 subnets with 30 hosts
- 255.255.255.240 (1111 0000)
  - 14 subnets with 14 hosts

Class B Subnet with router

- router is used to separate network



Type of Subnetting

- **Static Subnetting** - all subnets in the subnetted network use the same subnet mask
  - pros: simply to implement, easy to maintain
  - cons: wasted address space (consider a network of 4 hosts with 255.255.255.0 wastes 250 IP)

- **Variable Length Subnetting** - the subnets may use different subnet masks
  - pros: utilize address spaces
  - cons: required well-management

Private address, Network addresses translation -Super netting.

PUBLIC & PRIVATE ADDRESSES IN IPV4

- If direct (routed) or indirect (proxy or translator) connectivity to the Internet is desired, there are two types of addresses employed on the Internet
  - **Public addresses**
  - **Private addresses**

Public addresses

- Public addresses are assigned by NETWORK INTERFACE CARD (NIC) - A network interface card (NIC) is a **circuit board or card that is installed in a computer** so that it can be connected to a network.
- Consist of class-based network IDs or blocks of CIDR-based addresses (called CIDR blocks) that are guaranteed to be globally unique to the Internet.
- When the public addresses are assigned, **routes are programmed into the routers of the Internet** so that traffic to the assigned public addresses can reach their locations.

Public Addresses

- Public ip are the ip that can be accessed by every one (i,e) every user has the access to this ip's.

  E.g: Yahoo.com, Google.com etc are the pubic ip's.

Private Addresses

- Private IP addresses are used for numbering the computers in a private network including **home, school/Colleges/Universities and business LANs in airports and hotels** which makes it possible for the computers in the network to communicate with each other.
- Private ip's are the ip that cannot be accessed by every one(i,e) they are privately owned by an organization / private concern. Only the user of that organisation has the access to this ip's.

Eg : SRM University

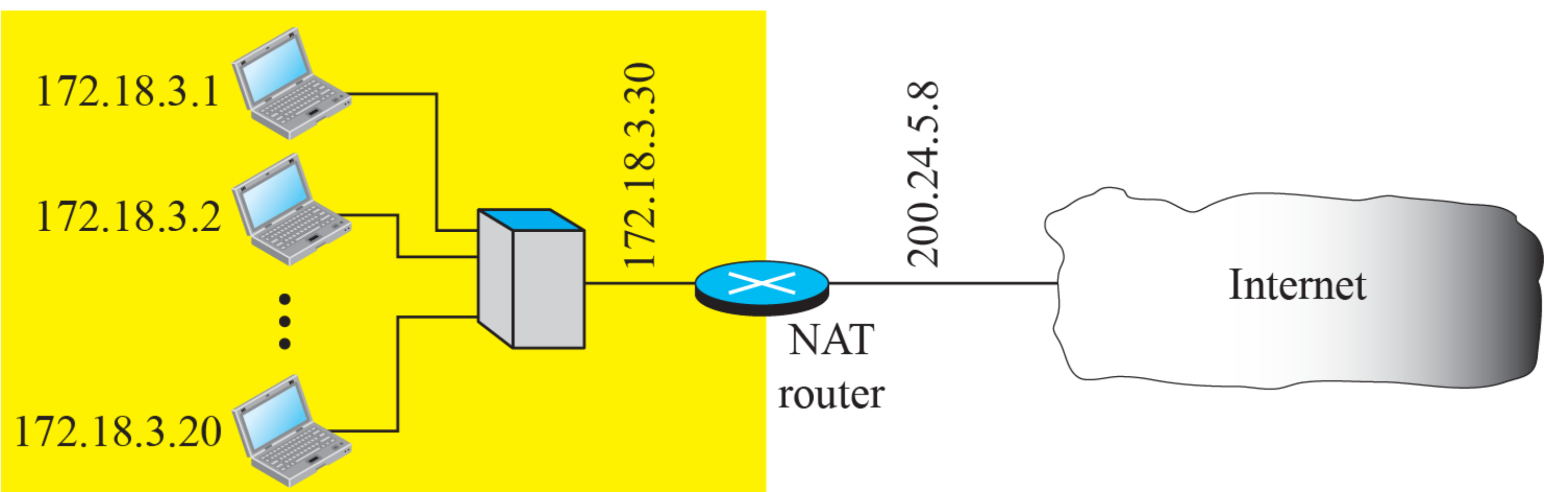
Range of private ip

- Four blocks are assigned as private addresses: 10.0.0.0/**8**, 172.16.0.0/**12**, 192.168.0.0/**16**.
- Range of private IP address are

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

NAT – Network Address Translation

- A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks.
- Allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (atleast one) for communication with the rest of the world.

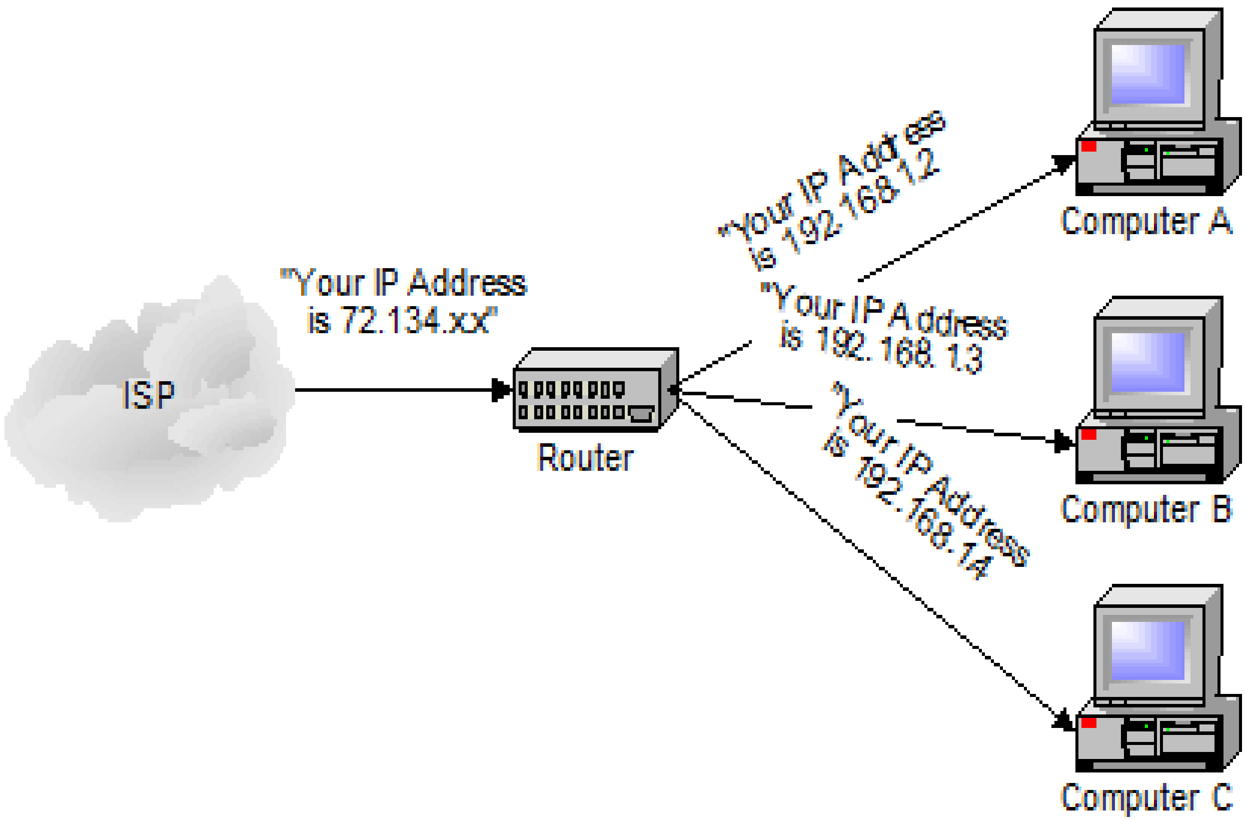


Site using private addresses

NAT – Network Address Translation

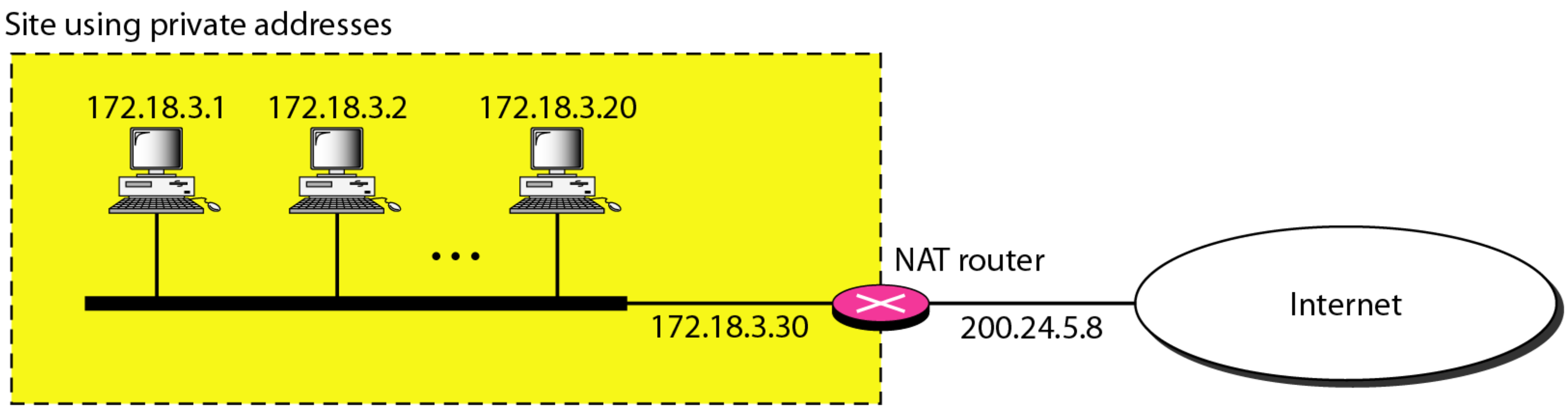
- It is the way that the router *translates* the IP addresses of packets that cross the internet/local network boundary.
  - When computer "A" sends a packet out "from" that of computer "A" – 192.168.1.2. When the router passes that packet on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP.
  - It also keeps track, so that if a response comes back from somewhere on the internet, the router knows to do the translation in reverse – replace the internet IP address with the local IP address for machine "A" and then send that response packet on to machine "A".
- NAT is not restricted to private-to-public address translation, though that is the most common application.
- NAT can also perform public-to-public address translation, as well as private-to-private address translation.

Example



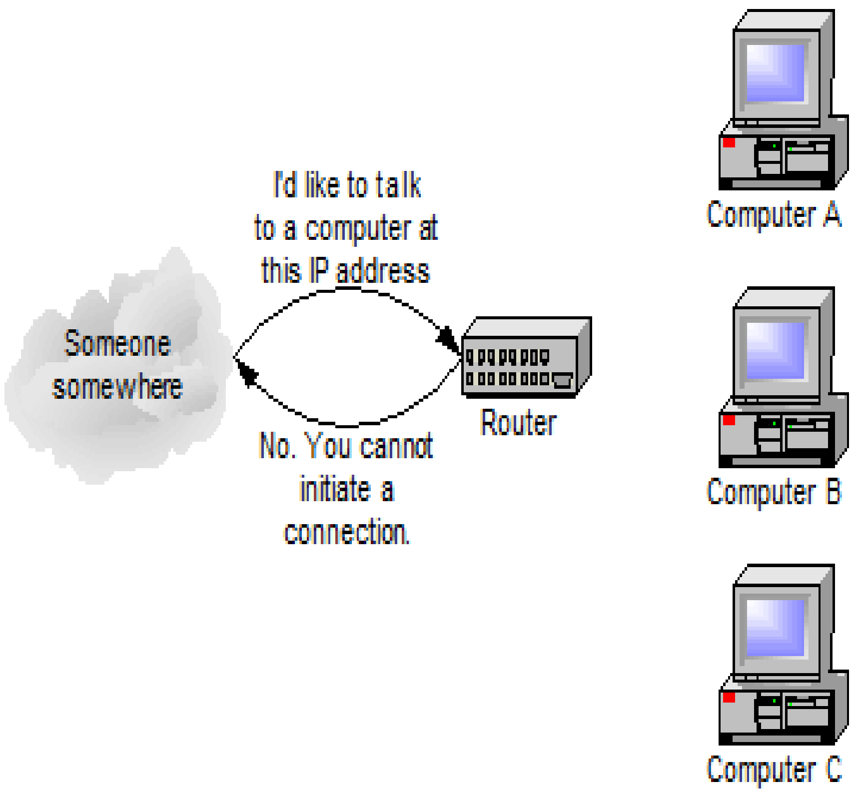
"Your IP Address
is 72.134.xx"
ISP
Router
"Your IP Address
is 192.168.1.2
"Your IP Address
is 192.168.1.3
"Your IP Address
is 192.168.1.4
Computer A
Computer B
Computer C

Figure 19.10 *A NAT implementation*



Network Address Translation (NAT)

- Benefits
  - Use of a single IP address among many devices in a network
  - Use of a dynamic IP address for home user for sharing
- Drawbacks
  - Machines on the internet cann initiate communications to loc machines – they can only respor to communications initiated l those local machines. The n effect is that the router then al: acts as a firewall.



Subnetting vs supernetting

Subnetting:

- Divide a large address block into smaller sub-groups.
  - If an organization was granted a large block in class A or B, it could divide the addresses into **several contiguous groups and assign each group to smaller networks (called subnets).**
- Use of flexible net mask.

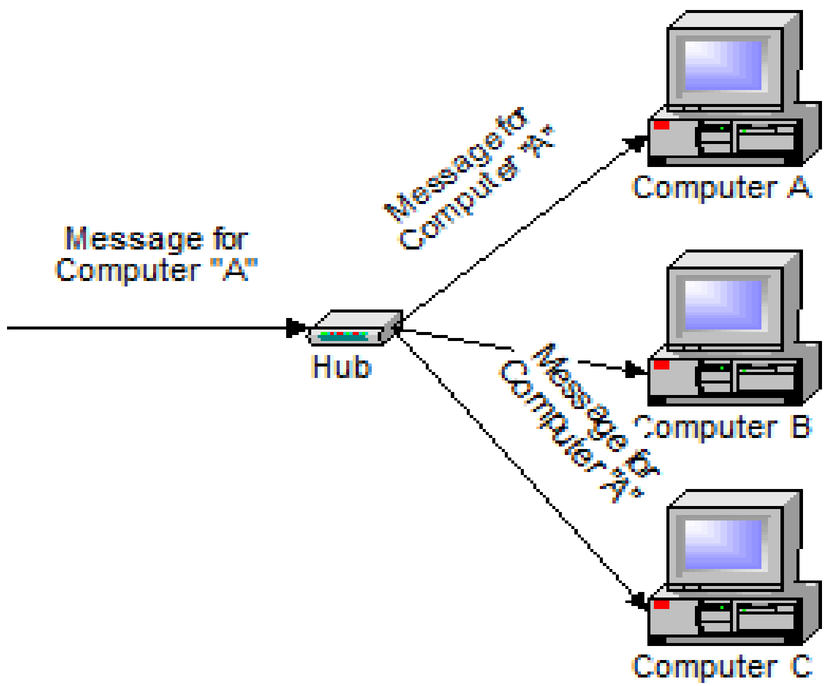
Supernetting

- In supernetting, an organization can combine several class C blocks to create a larger range of addresses.
- In other words, several networks are combined to create a supernetwork or a supemet.
- **For example:**
  - An organization that needs 1000 addresses can be granted four contiguous class C blocks.

Intermediate devices - Hub, Repeaters, Switch, Bridge- Gateways -Structure of a ROUTER

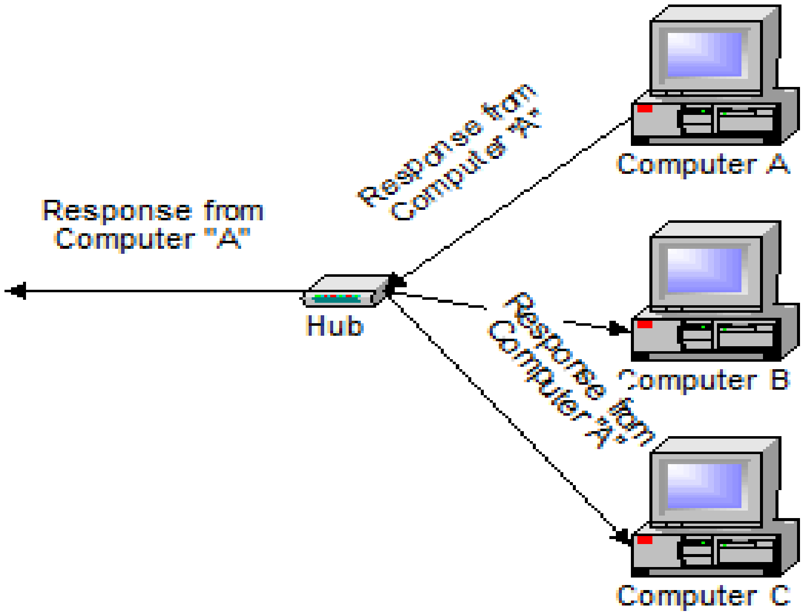
Intermediate devices - Hubs

- A **hub** is typically the least expensive, least intelligent, and least complicated. Its job is very simple – anything that comes in one port is sent out to the others. That is it broadcasts everything.
- If a message comes in for computer "A", that message is sent out all the other ports, regardless of which one computer "A" is on:



Hubs

- And when computer "A" responds, its response also goes out to every other port on the hub:



- Every computer connected to the hub "sees" everything that every other computer on the hub sees. The computers themselves decide if they are the targeted recipient of the message and when a message should be paid attention to or not.

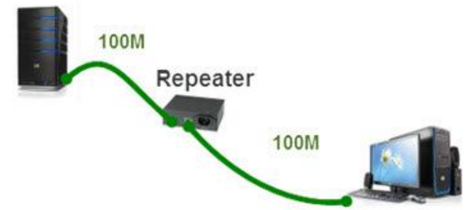
Types of Hub

- **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

Drawbacks

- Hubs cannot filter data, so data packets are sent to all connected devices.
- They do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Repeaters



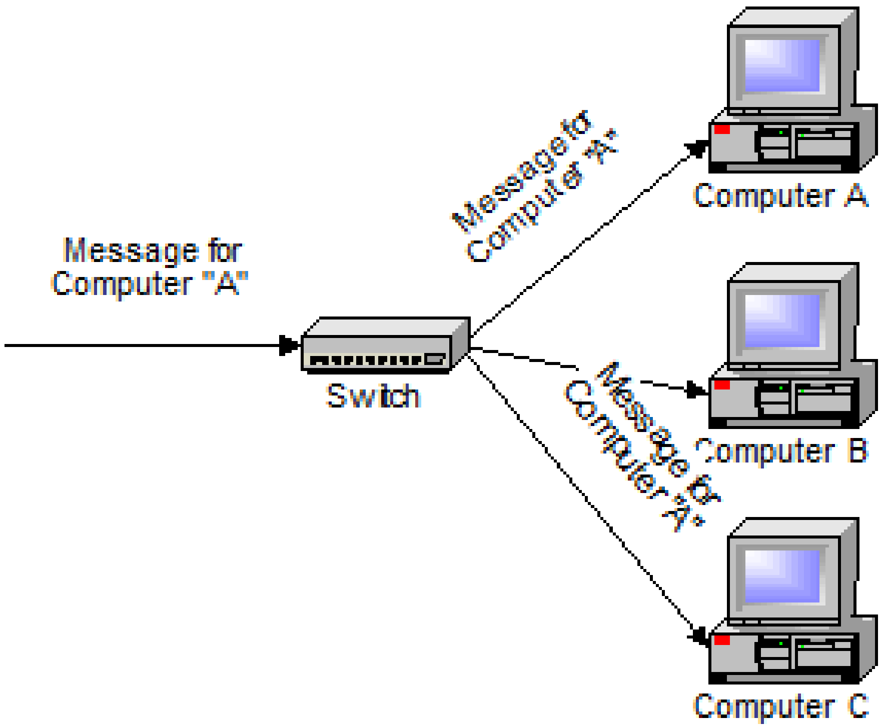
Ethernet Repeaters

- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- They do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device.

Because the functionality of repeaters has been built in to other devices, such as hubs and switches, repeaters are rarely used.

Switches

- A **switch** does essentially what a hub does, but more efficiently.
- By paying attention to the traffic that comes across it, it can "learn" where particular addresses are.
- Initially, a switch knows nothing and simply sends on incoming messages to all ports:

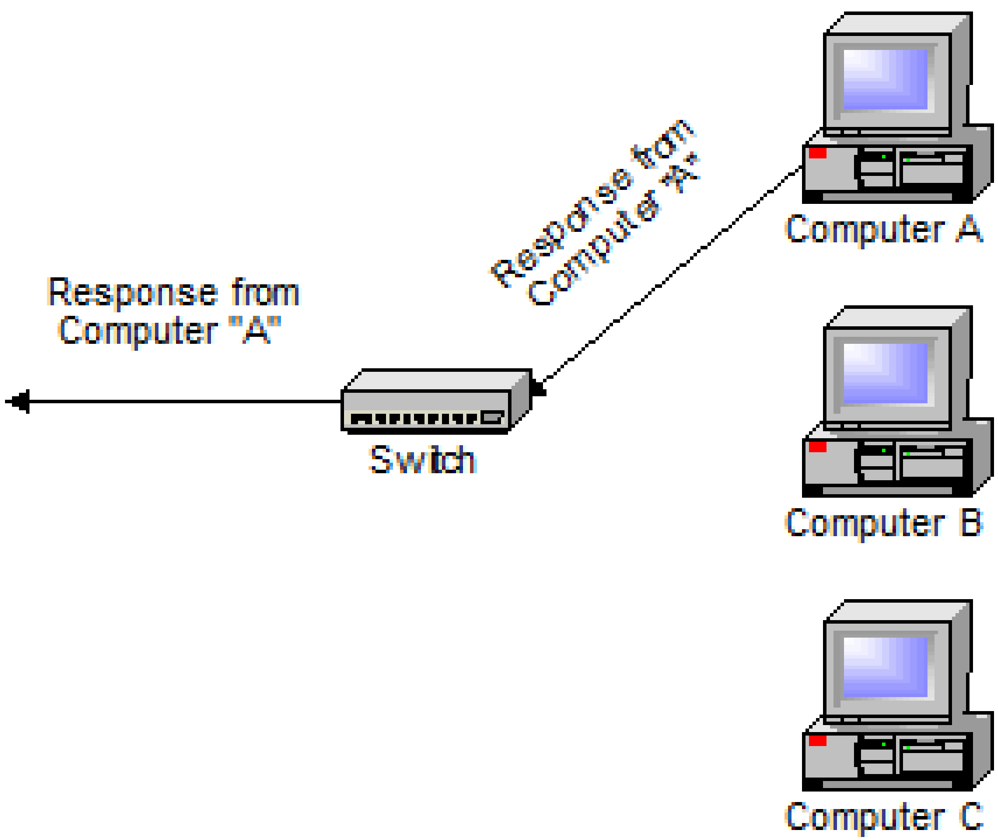


A 32-port Ethernet switch.

NETGEAR 5 port Network Switch

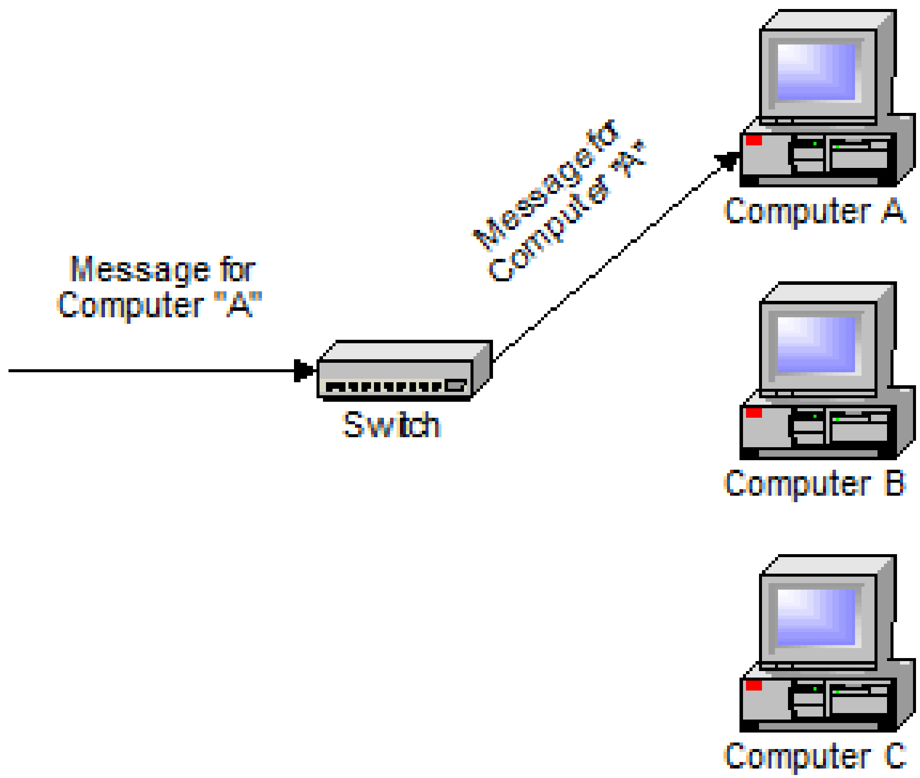
Switches

- Even accepting that first message, however, the switch has learned something – it knows on which connection the sender of the message is located.
- Thus, when machine "A" responds to the message, the switches only need to send that message out to the one connection:



Switches

- In addition to sending the response through to the originator, the switch has now learned something else – it now knows on which connection machine “A” is located.
- That means that subsequent messages destined for machine “A” need only be sent to that one port:

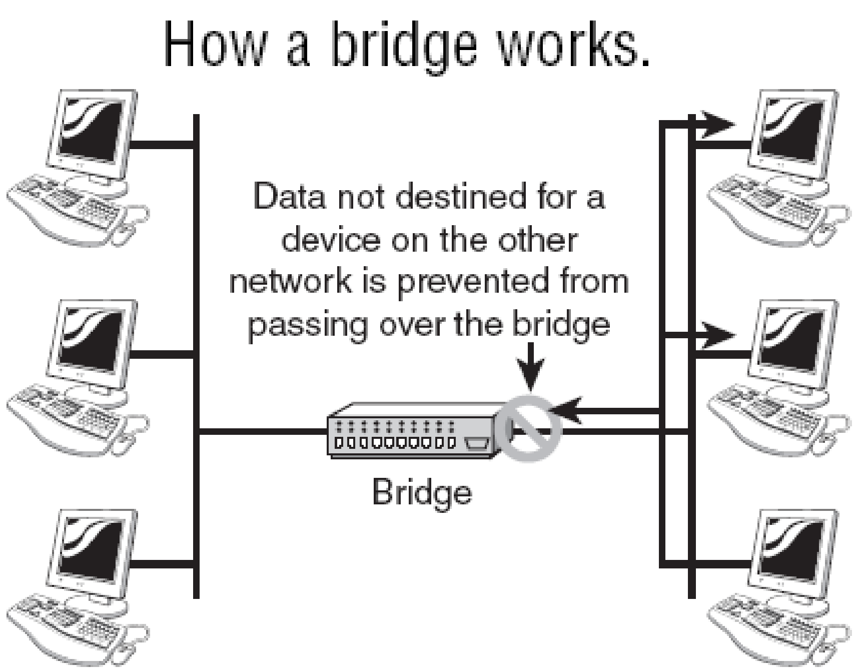


Switches

- Switches learn the location of the devices that they are connected to almost instantaneously.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- The net result is that most network traffic only goes where it needs to rather than to every port.
- On busy networks, this can make the network *significantly* faster.

Bridge

- A bridge operates at data link layer.
- A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.



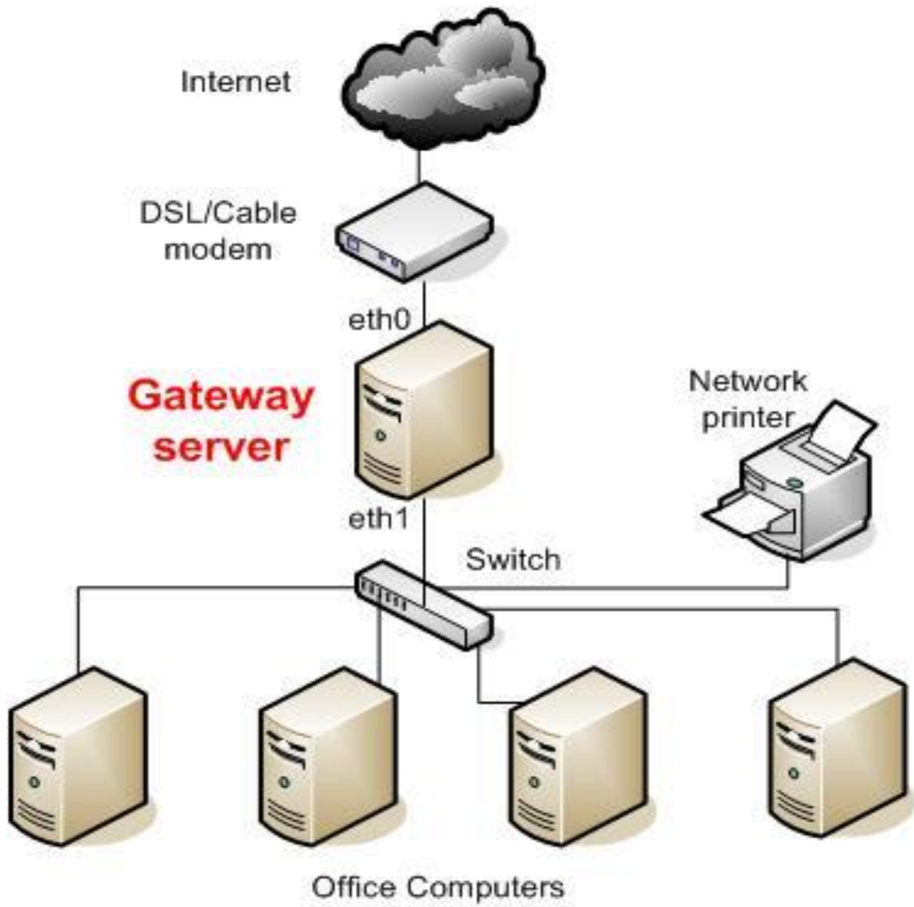
Types of Bridges

- **Transparent Bridges:-**
  - These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary.
  - These bridges make use of two processes i.e. **bridge forwarding and bridge learning**.
- **Source Routing Bridges:-**
  - In these bridges, routing operation is performed by source station and the frame specifies which route to follow.
  - The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.
- **Translational bridge:-**
  - A translational bridge can convert from one networking system to another.
  - It translates the data it receives.
  - Translational bridges are useful for connecting two different networks, such as Ethernet and Token Ring networks.

Gateway

- A gateway, is a passage to connect two networks together that may work upon different networking models.
- They basically work as the ***messenger agents*** that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called **protocol converters** and can operate at any network layer.
- The term gateway is applied to any device, system, or software application that can perform the function of translating data from one format to another.
- The key feature of a gateway is that it converts the format of the data, not the data itself.

Gateway


Internet
DSL/Cable modem
eth0
Gateway server
eth1
Network printer
Switch
Office Computers

Router

- Routers are network devices that literally route data around the network.
- By examining data as it arrives, the router can determine the destination address for the data; then, by using tables of defined routes, the router determines the best way for the data to continue its journey.
- Router is mainly a Network Layer device. Routers normally connect LANs and WANs together.

Cisco Router

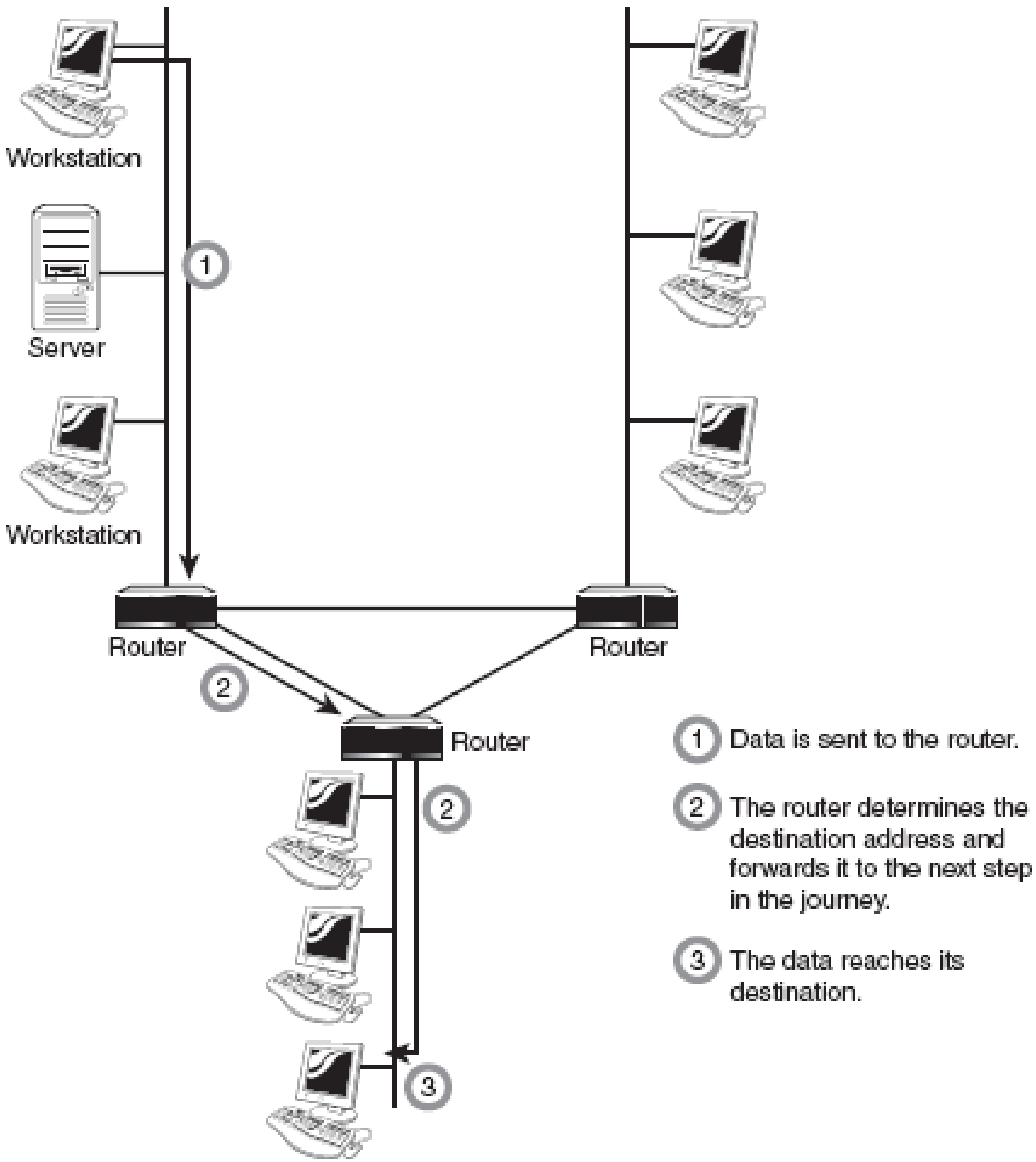
Router

- Unlike bridges and switches, which use the ***hardware-configured MAC address*** to determine the destination of the data, routers use the ***software-configured network address*** to make decisions.
- This approach makes routers more functional than bridges or switches, and it also makes them more complex because they have to work harder to determine the information.

- **Functionality:**
- When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

- **Routing tables** play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be *updated* and *complete*.
- The two ways through which a router can receive information are:
- **Static Routing**: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.

FIGURE 3.12 The basic function of a router.



Brouters

- Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a *bridge* when forwarding data between networks, and serving as a *router* when routing data to individual systems. Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.
- Brouters are rare and their functionality is embedded into the routers functioned to act as bridge as well.

PROBLEMS –SUBNETTING NUMERALS

* FIXED LENGTH SUBNET MASK (FLSM - EQUAL SIZED SUBNETS)

CLASSLESS ADDRESSING:

Q 1) Using Class "C" Address:

An organization is granted with the IP address 192.16.2.0/24. The administrator wants to create 4 Subnets. Calculate the following.

1) Find the Subnet Mask
2) No. of hosts in each Subnet
3) First and Last host address of each Subnet.
4) Network and Broadcast address of each Subnet.

SOLUTION:

Given is class "C" address

$\boxed{192.16.2.0/24}$

Need to create 4 Subnets.

To find "n": $\boxed{2^n \geq \text{No. of Subnets}}$

$2^n \geq 4$

No. of network bits $\boxed{n = 2}$

$n \Rightarrow$ No. of host bits to be borrowed.

$\therefore$ '2' bits to be borrowed.

1) To find Subnet Mask:

$\boxed{192.16.2.00}\underbrace{000000}_{\text{Hostid}}$ $/26$

Net id — 2 bits borrowed

$\therefore$ Subnet Mask is

11111111.11111111.11111111.11000000

(or) $\boxed{255 \cdot 255 \cdot 255 \cdot 192}$

2) To find no. of hosts in each Subnet (h):

$\left.\begin{array}{l}\text{No. of host bits}\\ h\end{array}\right\} = 6$

$\therefore$ Total No. of hosts $= 2^6 = 64$

$\left.\begin{array}{l}\text{No. of usable}\\ \text{(or) Valid hosts}\end{array}\right\} = 64 - 2$ (Excluding Network + Broadcast address)

$= 62$

3) T

3) To find the First host, Last host, Network and Broadcast Address:

$$\underbrace{192.16.2.}_{\text{Remains Unchanged}}\boxed{00}000000$$

00
01
10
11

⇒ Four Subnets.

* Subnet (1) : 00

(3)

Net id : 192.16.2.00000000

192.16.2.0/26

Broadcast : 192.16.2.00111111

192.16.2.63/26

∴ First Host : 192.16.2.1/26

Last Host : 192.16.2.62/26

* Subnet (2) : 01

* Subnet 2 : 01

Net id : 192.16.2.01|000000

192.16.2.64/26

Broadcast : 192.16.2.01/111111

192.16.2.127/26

First Host : 192.16.2.65/26

Last Host : 192.16.2.126/26

* Subnet 3 : 10

Net id : 192.16.2.10/000000

192.16.2.128/26

Broadcast : 192.16.2.01/111111

192.16.2.191/26

First Host : 192.16.2.129/26

Last Host : 192.16.2.190/26

* Subnet 4 : 11

Net id : 192.16.2.11|000000

192.16.2.192/26

Broadcast : 192.16.2.11/111111

192.16.2.255/26

First Host : 192.16.2.193/26

Last Host : 192.16.2.254/26

2) Using Class "B" address

IP address: 172.168.0.0/16

Create 32 Subnets.

To find n:

$$2^n \geq 32$$

$$\boxed{n = 5}$$

172.168.00000|000.000

1) To find Subnet Mask:

255.255.248.0

11111111.11111111.11111000.00000000

2) To find the number of hosts in each subnet.

No. of host bits = 11 bits

∴ Total No. of hosts = 2^{11} = 2048

No. of usable hosts = 2048 − 2 = 2046

3) To find the network, Broadcast, First Host and Last Host address of first and Last Subnet

a) Subnet 00000: [FIRST SUBNET]

Net id : 172.168. 00000/000. 00000000

172.168.0.0

First Host id: 172.168.1.0

Last Host id: 172.168.6.254

Broadcast id: 172.168. 00000/111.11111111

172.168.7.255

b) Subnet 11111: [LAST SUBNET]

Net id: 172.168.$\underbrace{11111}_{}$/000. 00000000

172.168.248.0

First Host id: 172.168.248.1

Last Host id: 172.168.255.254

Broadcast id: 172.168.$\underbrace{11111/111}_{}$. 11111111

172.168.255.255

Q3) Using class A Address:

An organization is granted with IP address 10.0.0.0/21. The administrator wants to create 200 fixed length subnets.

(i) First and Last Network's Address

(ii) Usable first and last host ID for the first and last network

(6)

(iii) Broadcast id for the first + Last Network.

(iv) How many no. of hosts possible to connect in each network.

SOLUTION: N/w address

(i) Subnet 1: 10.0.0.0

Subnet 200: $10.0.\underbrace{00000110.00111}_{199}$

(ie) 10.0.6.56

200 no. of subnet means from 0 to 199

(ii) First network

FH : 10.0.0.1

LH : 10.0.0.6

FH - First Host

LH - Last Host

No. of hosts in each Subnet $\Big\} = 2^h = 2^3 = 8$

So $\boxed{10.0.0.0 \text{ to } 10.0.0.7}$

FH is => 10.0.0.1

LH is => 10.0.0.6

LAST SUBNET:

LAST SUBNET:

FH : 10.0.6.57

LH : 10.0.6.62

Scanned b

(iii) Broadcast id:

For First Subnet : 10.0.0.7

For Last Subnet (200th) : 10.0.6.63

(iv) How many hosts?

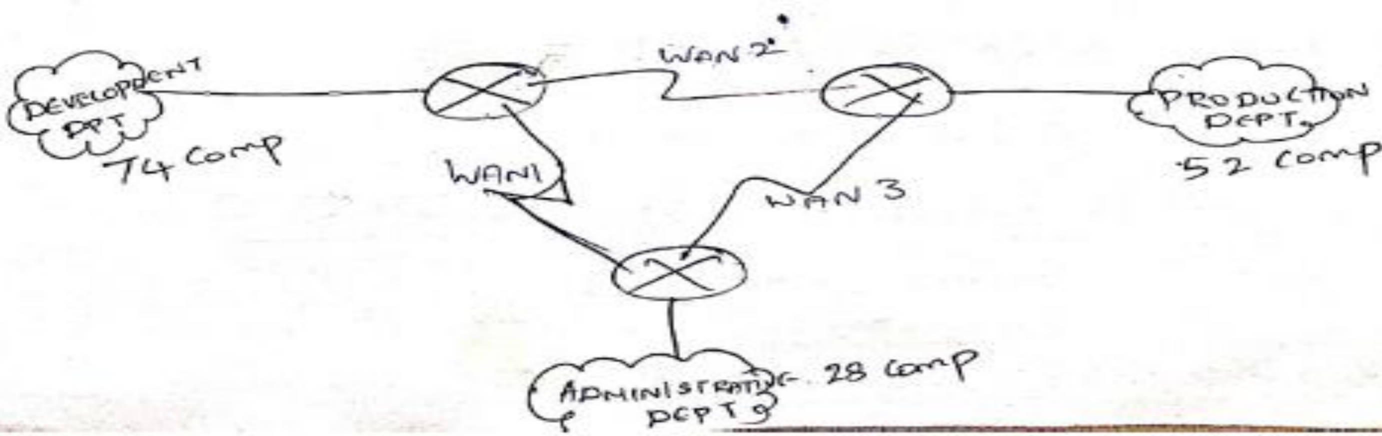
$2^n = 2^3 = 8$ hosts.

VLSM (VARIABLE LENGTH SUBNET MASK)

Q 1) Assume you are a network administrator at a Software Company, ~~for~~ which has three departments Connected via WAN link & granted with 192.16.1.0.

* Development department has 74 Computers
* Production department has 52 Computers
* Administrative department has 28 Computers.

All departments are Connected with each other via WAN link. Each WAN link requires two IP addresses.



SOLUTION:

*** Step 1:**

First order all networks according to the host requirement (ie) in Descending Order (Largest to Smallest)

Subnet	Segment	Hosts
1	Development	74 + 2 (Net id + Broad cast id)
2	Production	62 + 2
3	Administrative	28 + 2
4	WAN Link 1	2
5	WAN Link 2	2
6	WAN Link 3	2

192.16.1.0

(i) Development: (76 hosts)

Formula: $2^h \geq 76$

$\boxed{h = 7}$ host bits

Hence CIDR is $/24+1 = /25$

∴ Customized subnet mask is

$$\underbrace{11111111.11111111.11111111.1}_{\text{Network bits (25)}}\underbrace{0000000}_{\text{Host bits (7)}}$$

=> $\boxed{255.255.255.128/25}$ New subnet mask

②
74
52
28
2
2
2
160

Class "c" Address is enough

SRM

(9)

Range of Address

- Hence NetId : 192.16.1.0

FH : 192.16.1.1

LH : 192.16.1.126

Broadcast : 192.16.1.127

* (ii) PRODUCTION DEPARTMENT : (54 Hosts)

$2^h \geq 54$

$\therefore \boxed{h = 6}$ [Host bits]

Hence CIDR is /24+2 = /26

Customized subnet mask is

$\underbrace{11111111.11111111.11111111.11}_{\text{Network bits (26)}}\underbrace{000000}_{\text{Host bits (6)}}$

$\rightarrow$ $\boxed{255.255.255.192/26}$ => New subnet mask.

Range of Address

NetId : 192.16.1.128

FH : 192.16.1.129

LH : 192.16.1.190

Broadcast id : 192.16.1.191.

* (iii) ADMINISTRATIVE DEPARTMENT (30 Hosts)

$2^h \geq 30$

$\therefore \boxed{h = 5}$ [Host bits]

Hence

CIDR is $/24+3 = /27$

Customized Subnet mask is

$$\underbrace{11111111.11111111.11111111.111}_{\text{Network bits (27)}}\underbrace{00000}_{\text{Host bits (5)}}$$

New Subnet Mask will be $\boxed{255.255.255.224\ /27}$

Range of Address

Net id : 192.16.1.192

First Host : 192.16.1.193

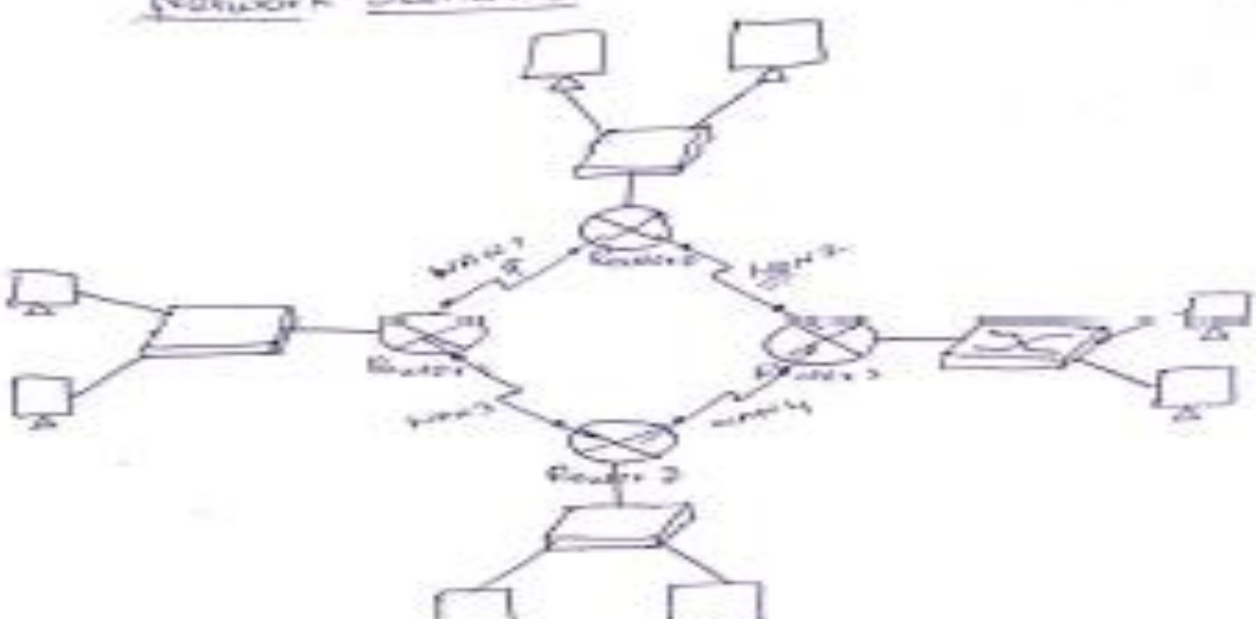
Last Host : 192.16.1.222

Broadcast id : 192.16.1.223

Q2) Assume that you are a network administrator at Technosoft Solutions. The Company has 4 floors, which are Connected with each other via WAN links and it has been granted with an IP address 172.16.0.0. Do the Subnetting for given IP address Satisfying all floor's requirements.

1. Call-Centre floor needs 4000 hosts
2. Data-Centre floor needs 2000 hosts
3. Operations floor needs 1000 hosts
4. Executive office floor needs only 100 hosts
5. Each WAN link requires two IP addresses.

Network Scenario



Soln:

Given the no. of hosts as 4000, 2000, 1000 & 100. Given class B (172.16.0.0) network. So default Mask is 255.255.0.0

(i) For 4000 hosts

$2^h - 2 \geq 4000$.

$\therefore \boxed{h = 12}$

CIDR is /20

Customized subnet mask will be

11111111.11111111.11110000.00000000

(ie) 255.255.240.0

Block Size is $2^{12} = 4096$

Formula $\therefore$ $\boxed{\text{No. of Blocks} = \frac{2^h}{256}}$

$= \frac{4096}{256}$

$= 16$ blocks.

Hence the range is

$\boxed{172.16.0.0/20 \text{ to } 172.16.15.255/20}$ for 4000 hosts

(ii) For 2000 hosts:

$$2^h - 2 \geq 2000$$

$\boxed{h = 11}$ (host bits)

CIDR is /21

Customized Subnet mask will be

11111111.11111111.11111000.00000000

(or) 255.255.248.0

Block Size is $2^{11} = 2048$

$\therefore$ No. of Blocks $= \frac{2^h}{256}$

$= \frac{2048}{256}$

$= \underline{8}$ blocks

Hence the range is

$\boxed{172.16.16.0/21 \text{ to } 172.16.23.255/21}$

for 2000 hosts.

(iii) For 1000 hosts:

$$2^h - 2 \geq 1000$$

$$\boxed{h = 10} \text{ (host bits)}$$

∴ CIDR is /22

Customized Subnet mask is

11111111.11111111.11111100.00000000

(iv) $\boxed{255.255.252.0}$

Block size is $2^h = 2^{10} = 1024$

No of Blocks $= \frac{2^h}{256}$

$= \frac{1024}{256}$

$= \underline{4}$ blocks

Hence the range is

$\boxed{172.16.24.0/22 \text{ to } 172.16.27.255/22}$ for 1000 hosts

(ii) For 100 hosts.

$$2^h - 2 \geq 100$$

$\boxed{h = 7}$ (Host bits)

CIDR is /25

Customized Subnet mask will be

11111111.11111111.11111111.10000000

(ie) $\boxed{255.255.255.128}$

Block size is $2^h = 2^7 = 128$

No. of Blocks $= \frac{2^h}{256}$

$= \frac{128}{256} = \frac{1}{2}$ (Half of the block)

Hence the range is

$\boxed{172.16.28.0/25 \text{ to } 172.16.28.127/25}$

for 100 hosts

For WAN Links:

There are 4 WAN links. Each WAN link requires 4 IP addresses.

(In question, they have given that each WAN requires 2 + 1(Net Id) + 1 (Broadcast id) = 4 IP addresses (In total)

Hence the Complete range will be:

172.16.0.0/20 to 172.16.15.255/20 [4000 Hosts]

172.16.16.0/21 to 172.16.23.255/21 [2000 Hosts]

172.16.24.0/22 to 172.16.27.255/22 [1000 Hosts]

172.16.28.0/25 to 172.16.28.127/25 [100 hosts]

172.16.28.128/25 to 172.16.28.131/25 for WAN 1

172.16.28.132/25 to 172.16.28.135/25 for WAN 2

172.16.28.136/25 to 172.16.28.139/25 for WAN 3

172.16.28.140/25 to 172.16.28.143/25 for WAN 4