ICT259 Computer Networking

Seminar 3: Network Layer and IP Addressing

Ms Wong Yoke Moon

Network Layer and IP Addressing

Objectives:

- **Explain the purpose and functions of the network layer in a data network.**
- **Outline the structure of an IPv4 address.**
- **Explain the importance of network segmentation and creating subnets as a network grows.**
- **Design an IP addressing scheme for a given network scenario.**
- **Explain the benefits of Variable Length Subnet Masking (VLSM).**
- **Calculate subnets with VLSM and apply to a network.**

Network Layer

Network layer or OSI Layer 3 uses the **four processes** to provide services to allow end devices to exchange data.

- **Addressing end devices** – Each end device must have unique IP address.
- **Encapsulation** – Encapsulates the transport layer protocol data unit (PDU) or segment into a packet.
- **Routing** – The process of selecting a path through a network or multiple networks to get to the destination device. To travel from one network to another network, it must pass through an intermediate device such as a router. The router upon receiving a packet will determine the best path and send the packet toward the destination device.
- **Decapsulation** – When the packet arrives at the network layer of the destination end device, the destination device checks the destination IP address in the IP header. If it matches its own IP address, the IP header is removed, and the transport layer segment is passed up to the transport layer.

Network Layer Protocols

Two commonly implemented network layer protocols:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

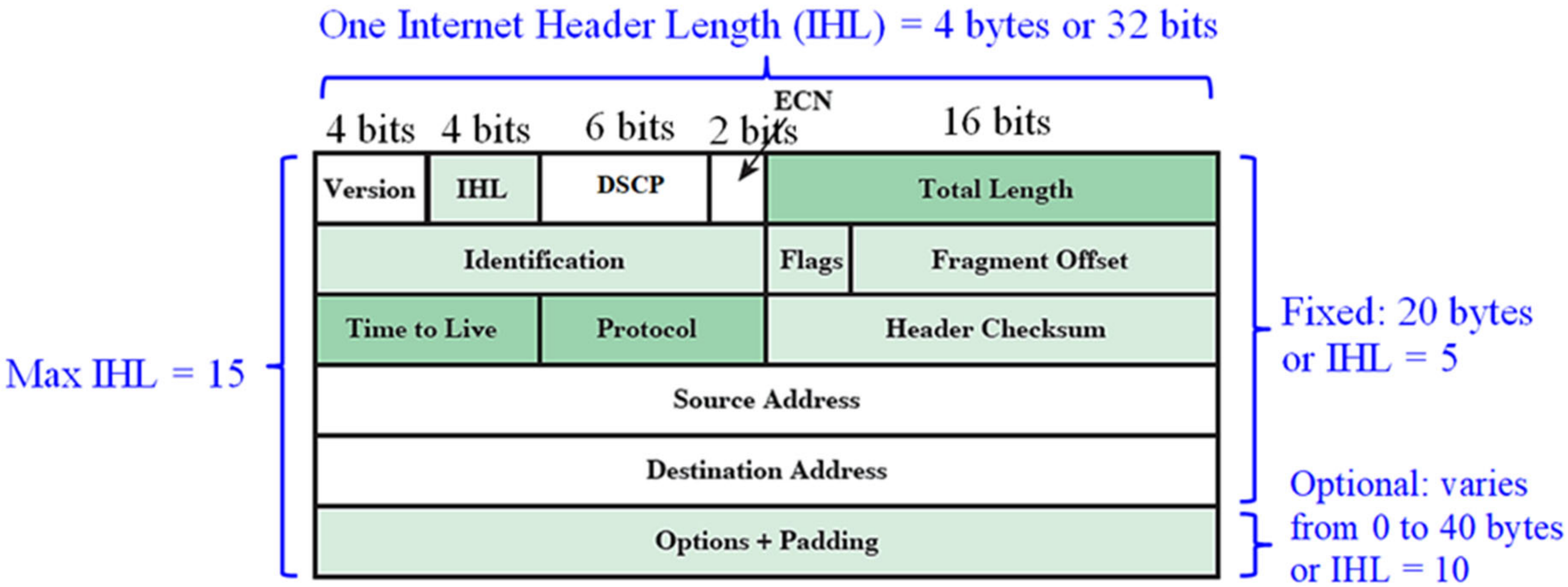
Characteristics of the IP Protocol

- **Connectionless -** There is no dedicated end-to-end connection is established before transmission.

- **Best Effort Delivery –** An unreliable delivery because the IP protocol does not guarantee that all packets sent by the source device are received by the destination device. IP does not have the capability to manage and track undelivered, corrupted or out of sequence packets. It is the functions of the upper layers, mainly the transport layer, to resolve these issues.

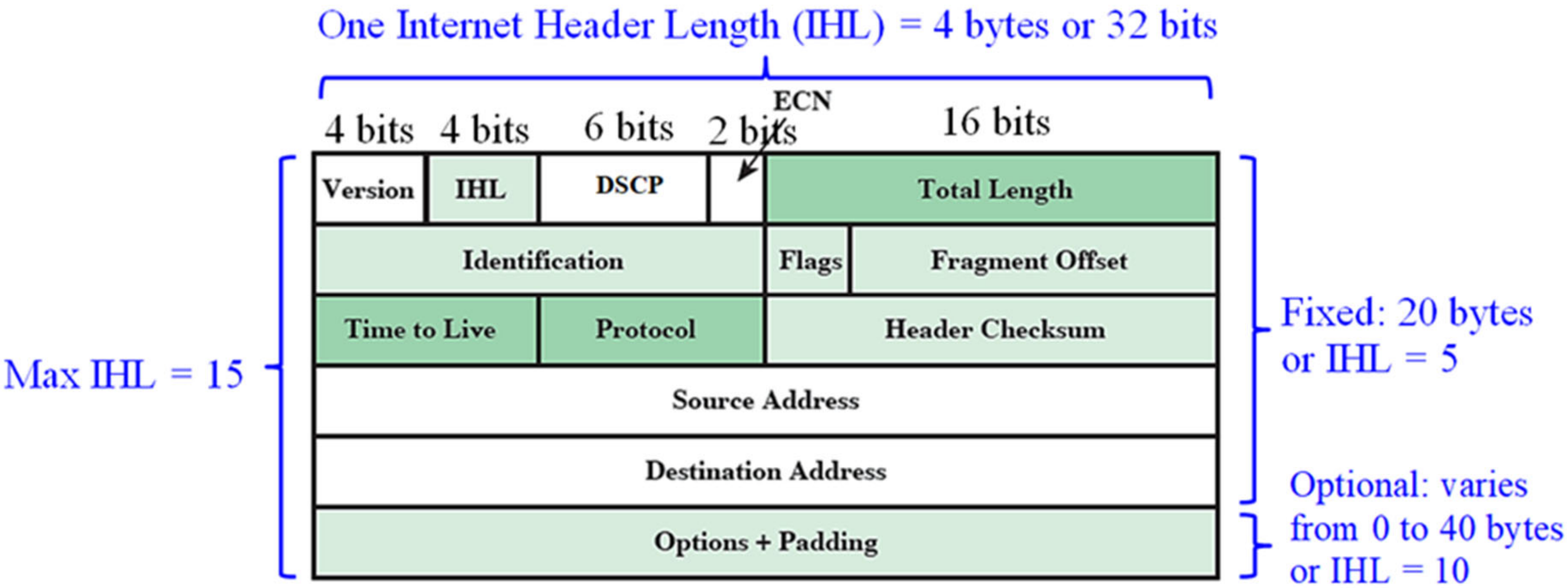
- **Media Independent -** IP is not tied to any particular physical medium that carry the data at the lower layers. It can operate over similar or mixed physical media such as copper, fiber optic or wireless.

IPv4 Packet Header



Fields	Description
Version	Contains the binary value of 0100 which indicates an IP version 4 packet
Internet Header Length (IHL)	Contains a 4-bit binary value that indicates the length of the IP header expressed as multiples of IHLs. One IHL is 4 bytes or 32 bits.
Differentiated Services or DiffServ (DS)	The DS field is an 8-bit field used by **routers to prioritize each packet**. The six most significant bits is the Differentiated Services Code Point (DSCP) and the last two bits are the Explicit Congestion Notification (ECN) bits.
Total Length	Total length of the IP packet (header and data included) in bytes.

IPv4 Packet Header



Fields	Description
Time to Live (TTL)	The TTL value defines the **lifetime of a packet**. This value is decremented by one by every router that handles the packet. When TTL reaches zero, the packet is discarded.
Protocol	Used to identify the **next level protocol**. The most common values are 1 (for ICMP), 6 (for TCP) and 17 (for UDP).
Source IP Address	A 32-bit value that represents the IP address of the device or interface that sends the packet.
Destination IP Address	A 32-bit value that represents the IP address of the device or interface that receives the packet.
Options + Padding	This field has a variable length for additional IP options. If the **length** of an IP packet header **is not a multiple of 4 bytes** after an option is added, 0s are padded to makeup for the shortfall.

Routing

How a Host Routes

A device can send a packet to three types of destinations:

- **Itself** – A device can ping itself by sending a packet to a special IPv4 address of **127.0.0.1** (*loopback address* or *loopback interface*, or "*localhost*"). Packets sent on a loopback address are re-routed back to the sending device without any modification. Its purpose is to test the TCP/IP protocol stack on the sending device.

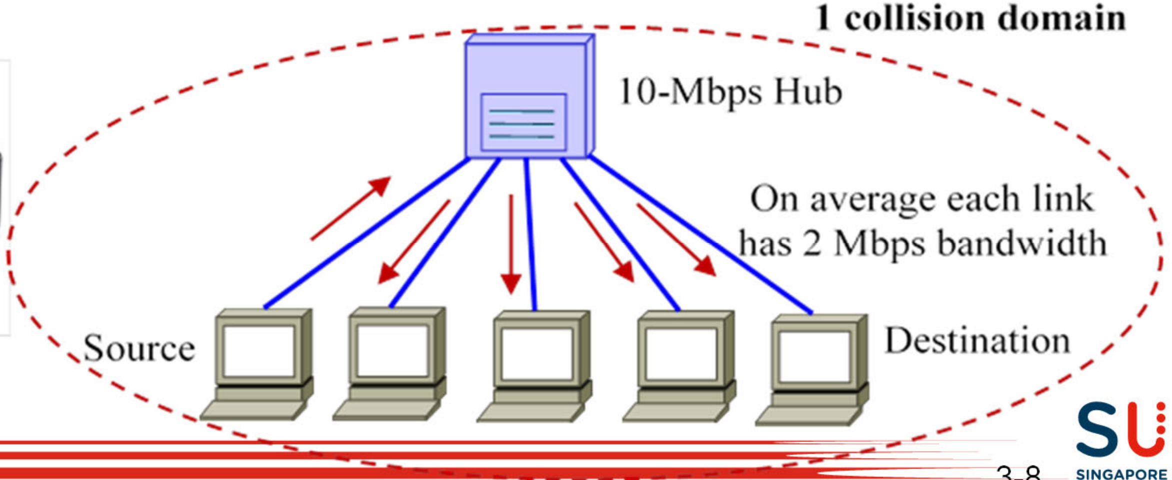
- **Same network** – Destination device is on the same network as the sending device. Both devices have the same network address.

- **Remote network** - Destination device is on a remote network. They have different network addresses.

Intermediate Devices

Hub

- A physical layer or OSI Layer 1 device. A hardware device with no software.
- Each port is a repeater, a circuit that retransmits whatever binary bit it receives, as such a hub is referred to as multiport repeater.
- When a hub receives an Ethernet frame at one of its ports, it transmits the frame to all other ports.
- A hub divides the 10-Mbps or 100-Mbps bandwidth among users. Due to this shared bandwidth, a hub is no longer popular.
- Devices on a hub must transmit in half duplex mode in order to avoid collisions.
- Hub uses CSMA/CD as the access method, thus collision can occurs in a hub environment.
- All devices connected to the hub and including the hub are in the same collision domain. A collision domain is an area of a network where frames can collide.



Intermediate Devices

Switch

- A data link layer or OSI Layer 2 device.
- Physically a switch looks like a hub, but with more ports.

Advantages of Switch over Hub

1. Switches can divide a local area network (LAN) into smaller and manageable segments and send frames to the destination device only.

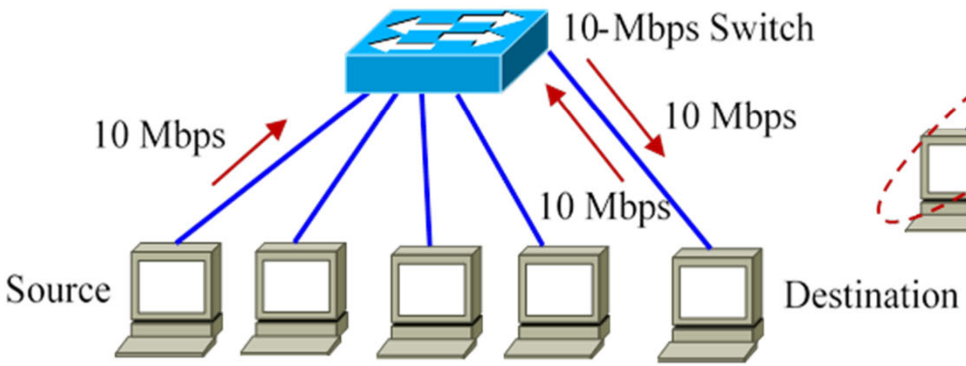
2. Switch has the capability to work on full duplex and half duplex.

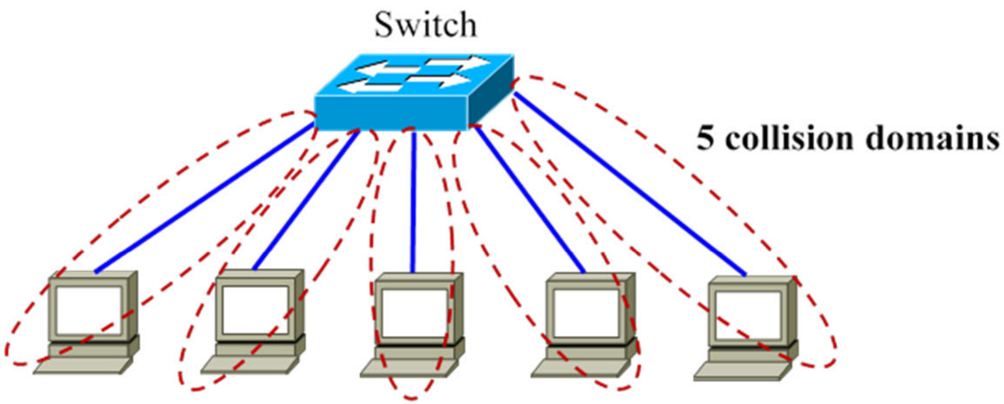
Intermediate Devices

Advantages of Switch over Hub

3. A switch has its own dedicated full bandwidth. A switch can allot its full 10-Mbps or 100-Mbps bandwidth to each device. If a switch is operating at full duplex, its effective bandwidth is double.
4. Each port on a switch is a collision domain. A switch can divide a big collision domain into many smaller collision domains. There is no collision between devices connected to a switch.

Due to these advantages, a switch is the preferred intermediate device for LAN.





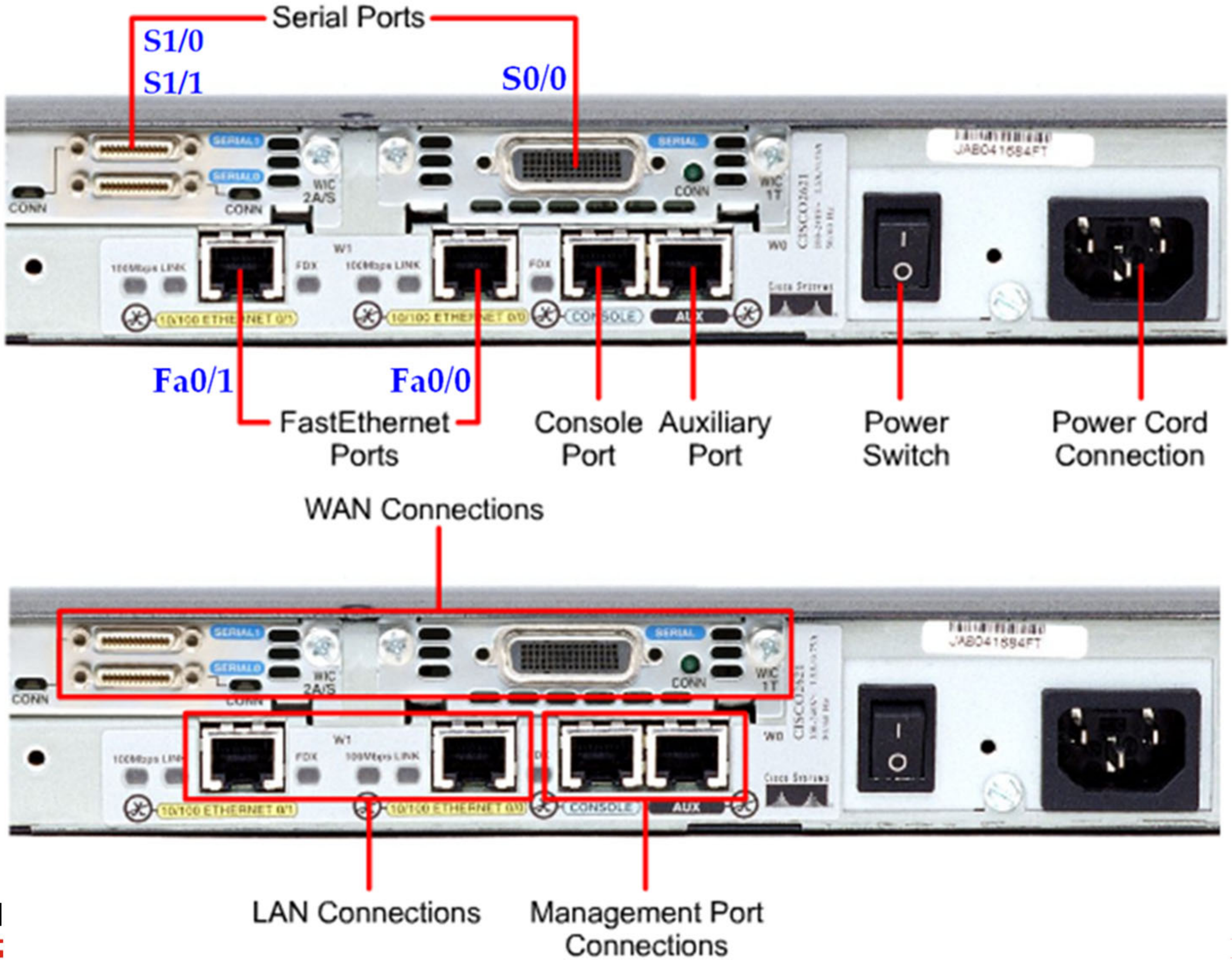
Intermediate Devices

Router

- A network layer or OSI Layer 3 device.
- Similar to switch, each port on a router is a collision domain.
- A router is like a computer with central processing unit (CPU), operating system, and memories like random-access memory (RAM), read-only memory (ROM), nonvolatile random-access memory (NVRAM), and flash.

Router

- Routers and switches have many types of ports and interfaces to connect to different devices.



SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Intermediate Devices

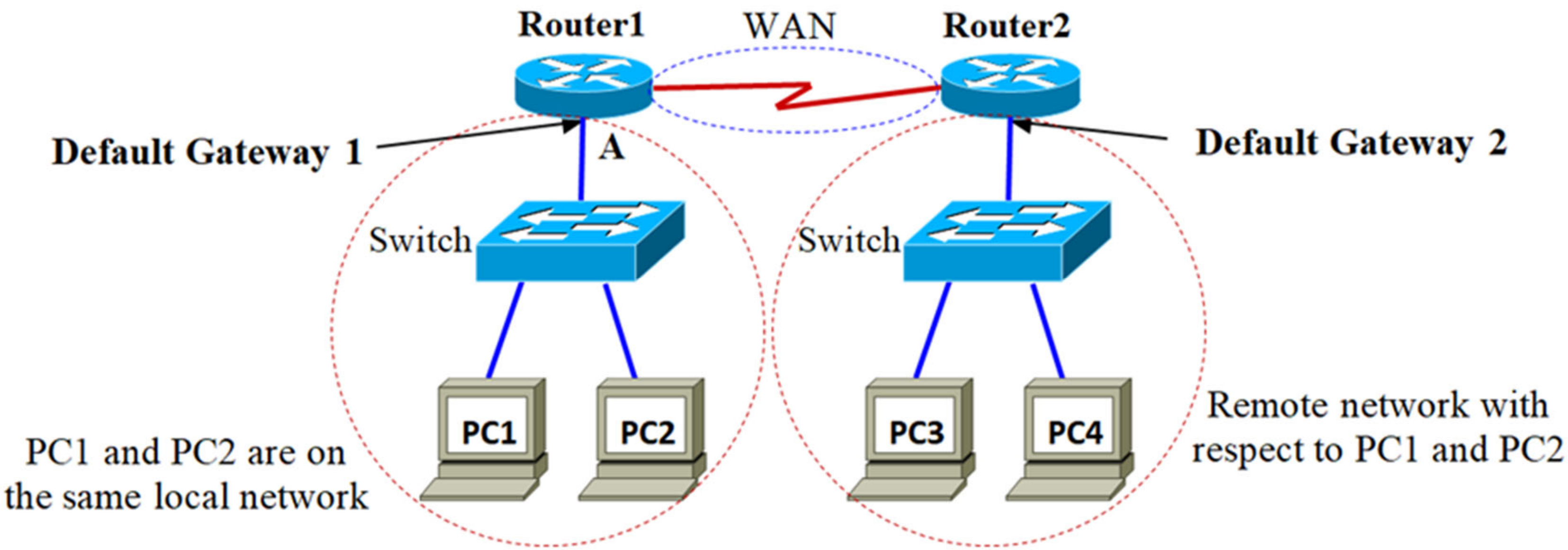
Connection to Console Port of a Cisco Device

- To configure a Cisco device via its console port, the console port has to be connected to a PC's serial communication port (COM1) if it is still available or a USB port.
- A special rollover UTP cable with a RJ-45 connector at one end and a DB-9 connector at the other end is designed for this purpose.
- If there is no COM1 port on the PC, you can connect to a USB port via a DB-9 to USB adapter.

Intermediate Devices

Role of a Router in a Network

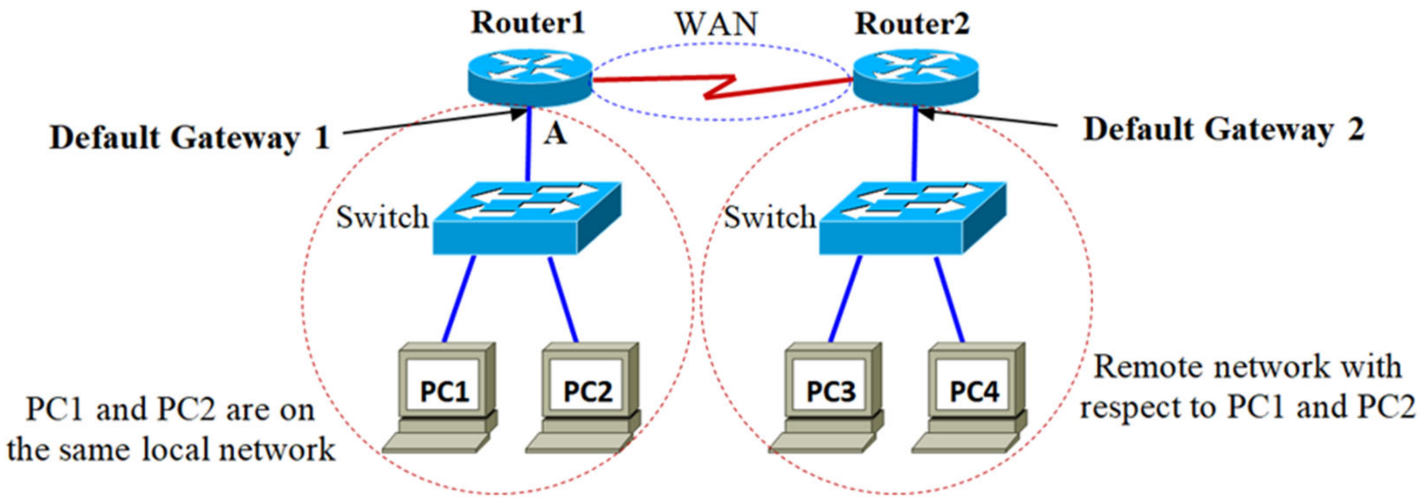
- One of the roles of the router in a network is to forward data packets from one network to another.
- Router is an intermediate device that connects networks.
- Two routers are used to connect the 3 networks shown below.
- PC1 and PC2 are on the same local network and they can communication with each other via the switch.
- If PC1 wants to communicate with PC3, PC 3 is regarded as in a remote network with respect to PC1 and needs the help of routers and routing.



Intermediate Devices

Default Gateway

- The point where a LAN connects the router.
- From the point of view of a PC, the default gateway of a PC is the exit point for packets from the PC to another network.
- It is also the entry point for packets from another network to the network of the PC.
- This default gateway has an IP address.
- At the router, it is the IP address of the router interface (point A) attached to the LAN of the PC.
- The IP address of PC and the router interface address must be in the same network.
- The default gateway of PC1 and PC2 is at Default Gateway 1.
- Similarly, the default gateway of PC3 and PC4 is at Default Gateway 2.



IP Addressing

For communication to take place, devices must be configured with unique addresses to identify them.

IPv4 Address Structure

- An IP address consists of 32 bits divided into four sections or bytes.
- Each byte is 8 bits separated by a dot.
- For human usability, it is expressed in four decimal numbers separated by a dot.
- This representation is commonly called *dotted decimal notation*.
- E.g. of a valid IP address: 176.15.13.11.

Network and Host Portions

- An IP address has a network portion (network ID) and a host portion (host ID).
- The network ID of the address must be identical for all devices in the same network.
- The host ID of the address must uniquely identify a specific device within the network.

	Network Portion		Host Portion	
IPv4 Address	176	. 15	13	. 11

IP Addressing

~~Arial~~ Subnet Mask

- A 32-bit pattern consisting of a series of 1s followed by 0s.
- It is used to identify the network and host portions of an IP address.
- The portion with all 1s in the subnet mask corresponds to the network portion of the IP address.
- Similarly, the portion with all 0s in the subnet mask corresponds to the host portion of the IP address.

	Network ID			Host ID		
IPv4 Address	176	.	15	13	.	11
subnet mask in decimal	255	.	255	0	.	0
subnet mask in binary	1111 1111	.	1111 1111	0000 0000	.	0000 0000

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

IP Addressing

Logical AND

- To determine the network address of an IP device, the IP address is logically ANDed in binary with the subnet mask.
- The result of the AND operation is the network address.
- E.g. Determine the network address of a host with IP address 176.15.13.11 and subnet mask 255.255.0.0.

IP address in decimal	176 .	15	13 .	11
IP address in binary	1011 0000 .	0000 1111	0000 1101 .	0000 1011
subnet mask in decimal	255 .	255	0 .	0
subnet mask in binary	1111 1111 .	1111 1111	0000 0000 .	0000 0000
result of AND operation	1011 0000 .	0000 1111	0000 0000 .	0000 0000
Network Address	176 .	15	0 .	0

- From the result, we can conclude that host 176.15.13.11 is on network 176.15.0.0 255.255.0.0.

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

IP Addressing

Prefix Length

- The *prefix length* or "*slash notation*" is a shorthand method of representing subnet mask.
- For example, what does **16** in 176.15.13.11/**16** mean?
- It means there are **16 bits set to 1** in the subnet mask.
- /16 => 1111 1111. 1111 1111. 0000 0000. 0000 0000 => 255.255.0.0.

Subnet Mask	Subnet Mask in 32-bit	Prefix Length
255.0.0.0	1111 1111. 0000 0000. 0000 0000. 0000 0000	/8
255.255.0.0	1111 1111. 1111 1111. 0000 0000. 0000 0000	/16
255.255.255.0	1111 1111. 1111 1111. 1111 1111. 0000 0000	/24
255.255.255.128	1111 1111. 1111 1111. 1111 1111. 1000 0000	/25
255.255.255.192	1111 1111. 1111 1111. 1111 1111. 1100 0000	/26
255.255.255.224	1111 1111. 1111 1111. 1111 1111. 1110 0000	/27
255.255.255.240	1111 1111. 1111 1111. 1111 1111. 1111 0000	/28
255.255.255.248	1111 1111. 1111 1111. 1111 1111. 1111 1000	/29
255.255.255.252	1111 1111. 1111 1111. 1111 1111. 1111 1100	/30

IP Addressing

Network, Host and Broadcast Addresses

- **Network Address**
  - Address of the entire network.
  - All hosts in the network have the same network address.
  - The host portion is all 0s.

- **Host Addresses** – Unique IP addresses assigned to devices in the network. The network ID is the same for all devices. The host ID is an assortment of 0s and 1s, but never all 0s or all 1s.
  - **First Host Address** – First usable host IP address in the network. The host ID always has all 0s and ends with a 1.
  - **Last Host Address** – Last usable host IP address in the network. The host ID always has all 1s and ends with a 0.

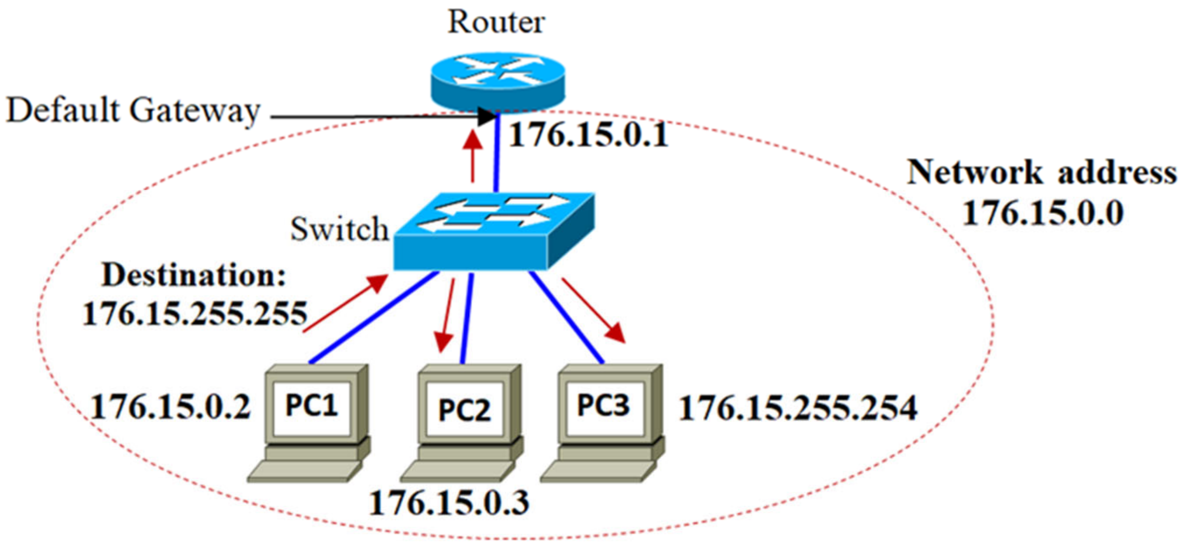
- **Broadcast Address**
  - An address to send data to all hosts in the network.
  - The host ID is all 1s.

IP Addressing

Network, Host and Broadcast Addresses

		Network ID	Host ID in binary	Address in Decimal
Network address		176. 15.	0000 0000. 0000 0000	176. 15. 0. 0
Host Addresses	1st host address	176. 15.	0000 0000. 0000 0001	176. 15. 0. 1
	2nd host address	176. 15.	0000 0000. 0000 0010	176. 15. 0. 2
	3rd host address	176. 15.	0000 0000. 0000 0011	176. 15. 0. 3
	.	.	.	.
	Last host address	176. 15.	1111 1111. 1111 1110	176. 15. 255. 254
Broadcast address		176. 15.	1111 1111. 1111 1111	176. 15. 255. 255

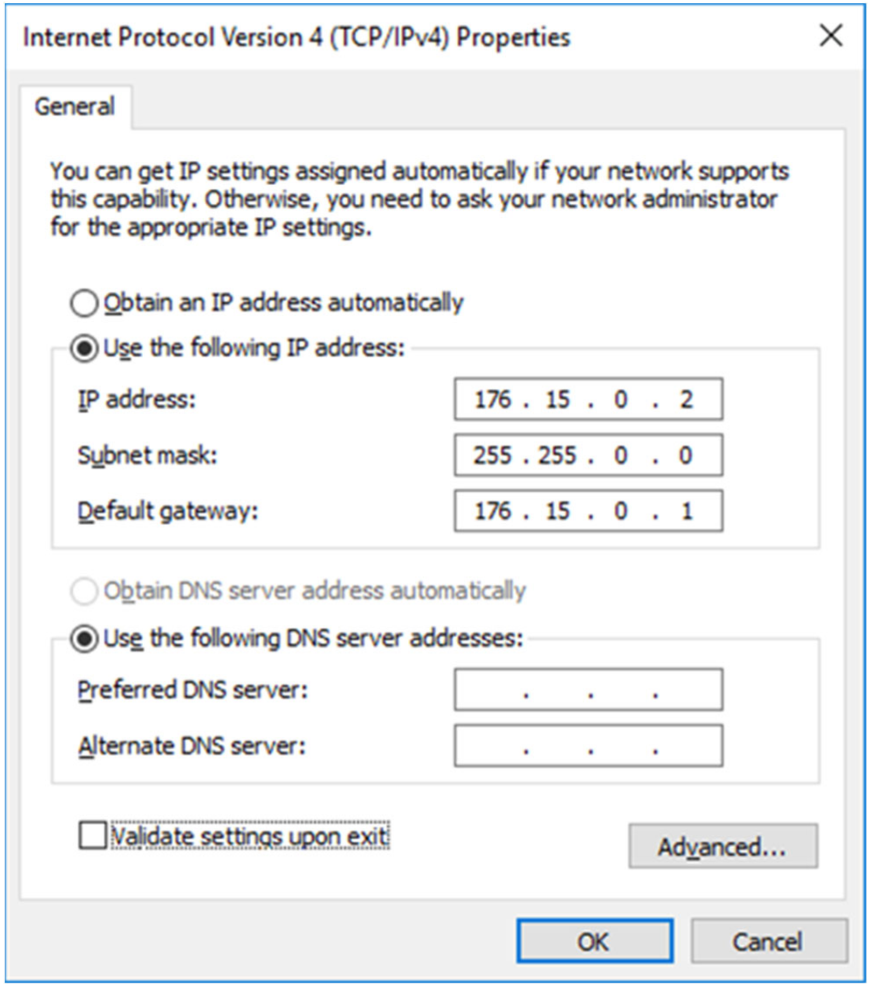
PC1 is sending a broadcast frame to all hosts with destination IP address of 176.15.255.255



IP Addressing

Static IP Address Assignment to a Host

- Devices can acquire an IP address either statically or dynamically.
- Static address is an address fixed to the device and it does not change.
- Some devices like network printers and servers need static addresses.
- A host can be configured with static IPv4 address through the host's adapter settings.



IP Addressing

Dynamic IP Address Assignment to a Host

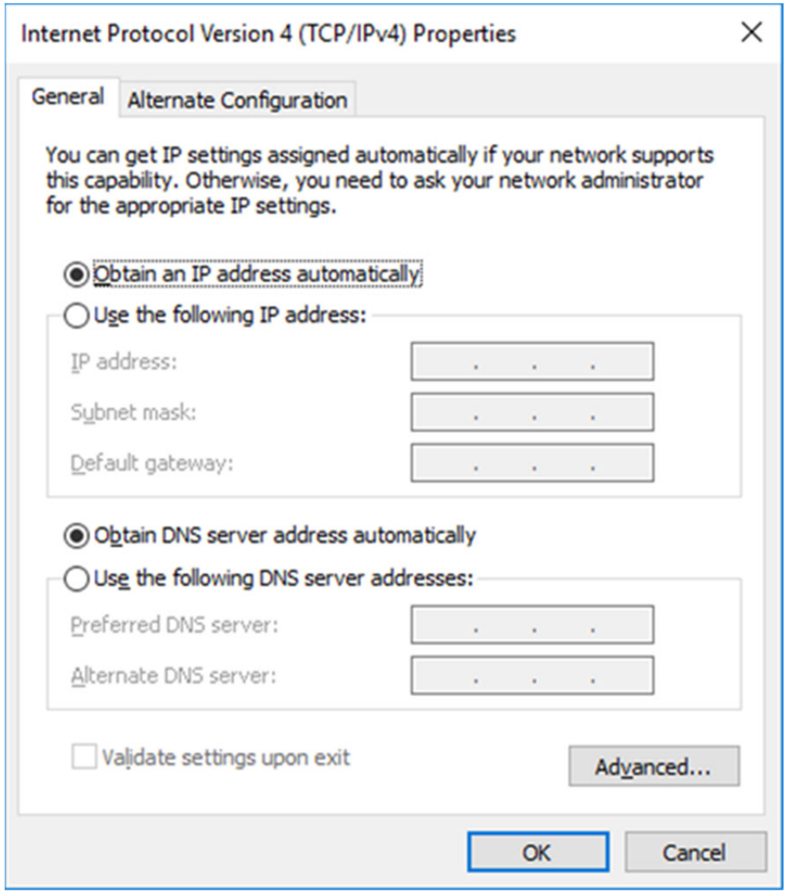
- Most network devices acquired their IP addresses dynamically using the Dynamic Host Configuration Protocol (DHCP).

- In DHCP, the host is regarded as a DHCP client that requests IP address information from a DHCP server.

- The DHCP server will allocate an IP address, subnet mask, default gateway and other related configuration information to the host.

- The advantage of using DHCP is that the address is not permanently assigned to the host, but "leased" for the duration of use.

- If the host is shutdown or disconnected from the network, the address is released back to the pool for reallocation.



IP Addressing

Unicast Communication

- IP addresses from 0.0.0.0 to 223.255.255.255 are for unicast communication.
- There are many addresses within this range that are reserved for special purposes.

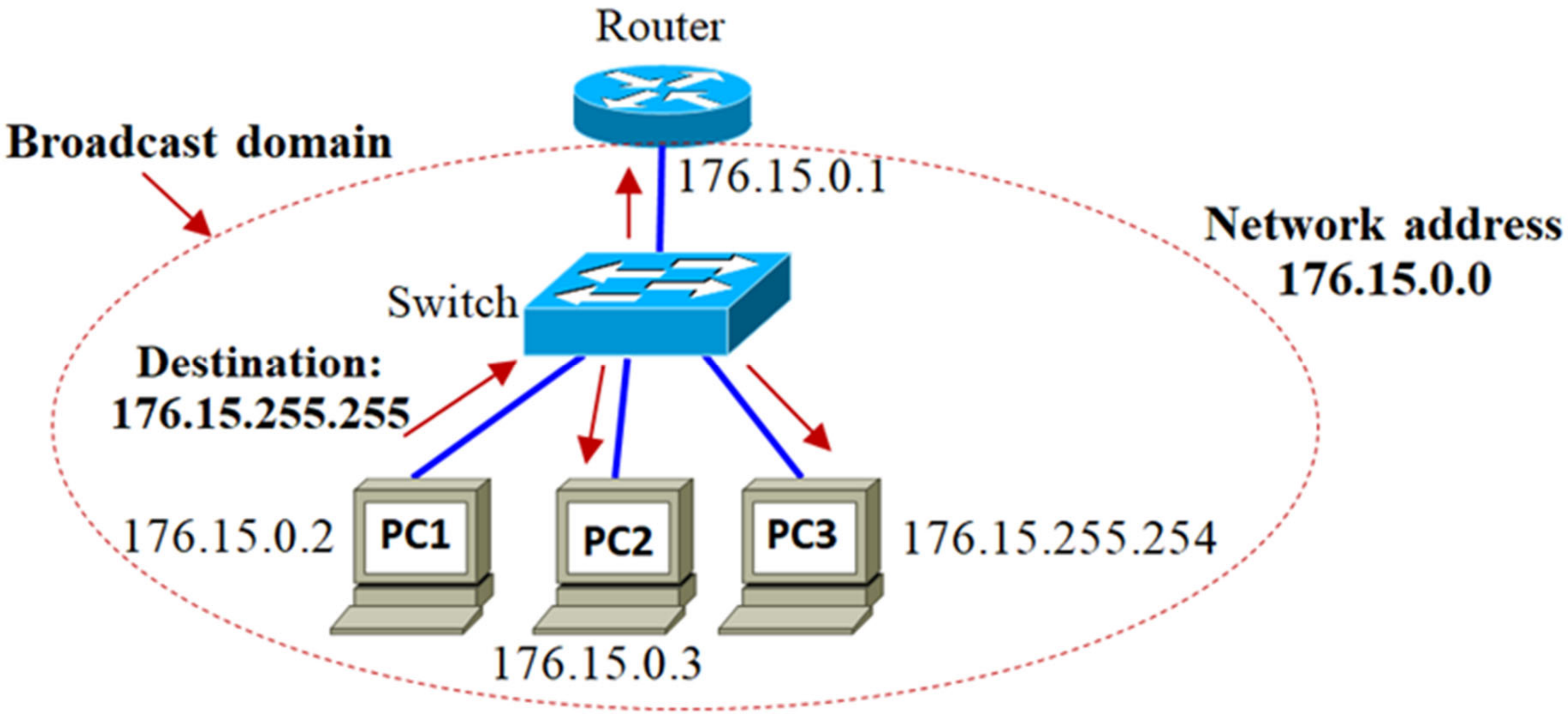
Multicast Communication

- IP addresses from 224.0.0.0 to 239.255.255.255 are reserved for multicast communication.
- The range of addresses between 224.0.0.0 and 224.0.0.255 are reserved for multicast groups on a local network.
- A router connected to a local network will not forward packets with addresses reserved for local multicast groups.
- Each multicast group corresponds to a single multicast destination address.
- A host needs to join or subscribe to the multicast group in order to receive packets sent to the group.

IP Addressing

Broadcast Communication

- When a host sends a broadcast frame, all the devices that receive the frame are in the same broadcast domain.
- The extent of a broadcast domain is the same as the network.
- E.g. PC1 is sending a broadcast frame to all hosts with destination IP address of 176.15.255.255.



IP Addressing

Broadcast Communication

1. Limited Broadcast

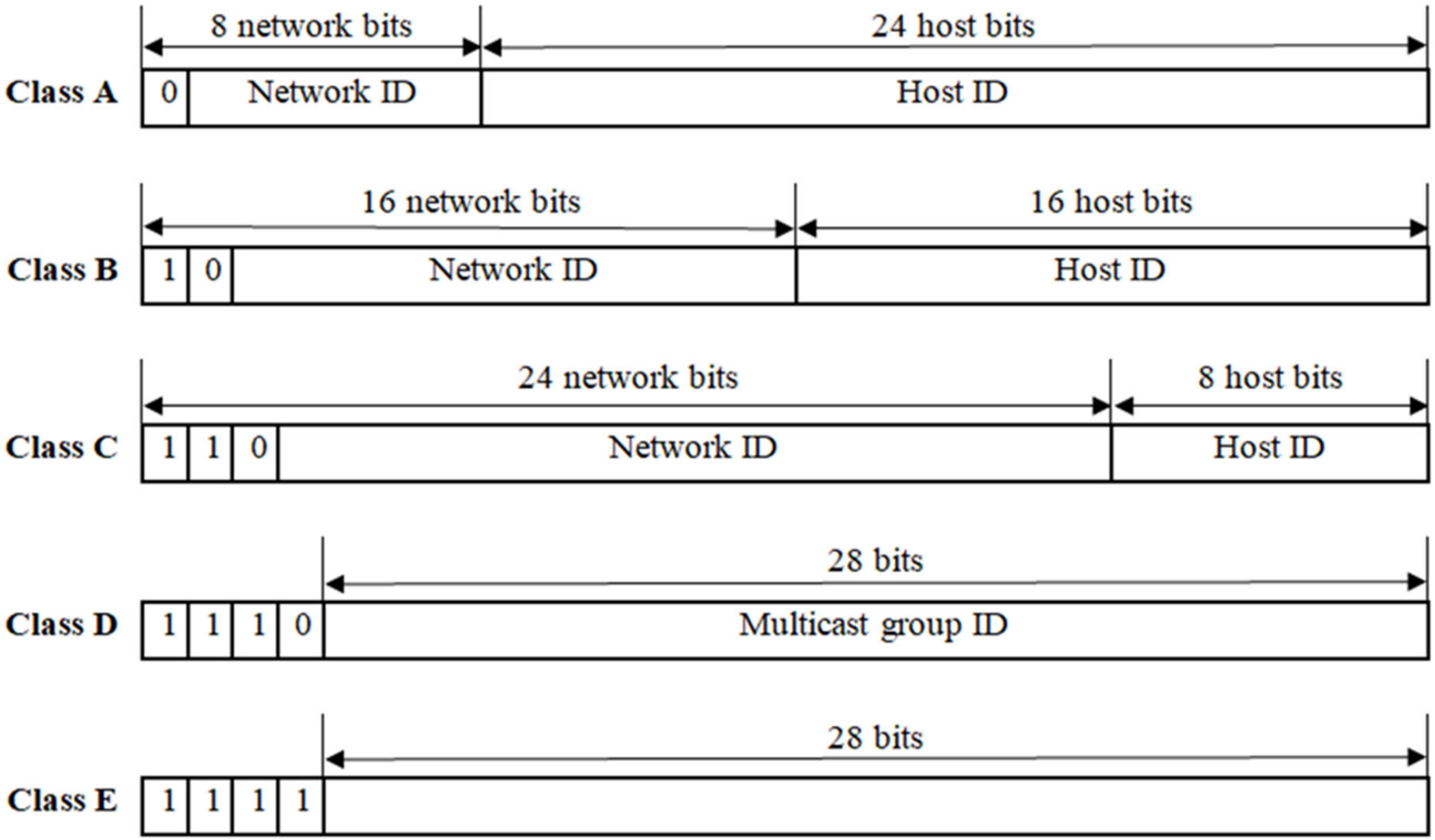
- A *limited broadcast* is sent to all hosts in the local network.
- The local or limited broadcast address is 255.255.255.255.
- This address is not a routable address, which means a router upon receiving it will not forward, but discard it.
- By default, routers do not forward broadcasts. Thus, routers separate broadcast domains.

2. Directed Broadcast

- A *directed broadcast* address is sent to all hosts on a specific network.
- E.g. the directed broadcast address for network 176.15.0.0/16 is 176.15.255.255.
- This address is routable, which means the router will forward it to the end router connected to the destination network if the router is configured to forward broadcasts.

Types of IPv4 Addresses

Classful Addressing



Class E is reserved for experimental purposes

Types of IPv4 Addresses (Additional)

Classful Addressing

	Address range	Network address range				
Class A	0.0.0.0 - 127.255.255.255		N	H	H	H
			(0 000 0000). 0.	0. 0.	0. 0.	0 0*
		1.0.0.0 –	(0 000 0001). 1.	0. 0.	0. 0.	0 0
		126.0.0.0 *	(0 111 1110). 126.	0. 0.	0. 0.	0 0
			(0 111 1111). 127.	0. 0.	0. 0.	0 0*
Class B	128.0.0.0 - 191.255.255.255		N	N	H	H
		128.0.0.0 –	(10 00 0000). 128.	(0000 0000). 0.	0. 0.	0 0
		191.255.0.0	(10 11 1111). 191.	(1111 1111). 255.	0. 0.	0 0
Class C	192.0.0.0 - 223.255.255.255		N	N	N	H
		192.0.0.0 –	(110 0 0000). 192.	(0000 0000). 0.	(0000 0000). 0.	0 0
		223.255.255.0	(110 1 1111). 223.	(1111 1111). 255.	(1111 1111). 255.	0 0

* 0.0.0.0 is reserved and 127.0.0.0 is the loopback address. Both cannot be assigned to hosts.

Types of IPv4 Addresses

Classful Addressing

- Classes A, B and C are unicast IP addresses with the exception of some special addresses within their ranges.
- These addresses can be allocated to hosts and interfaces.
- This course will focus on these three classes.
- Class D addresses are for multicasting and Class E is reserved for experimental purposes.

	Address range	Network address range	Network ID bits	Max number of network	Host ID bits	Number of usable host IP addresses
Class A	0.0.0.0 - 127.255.255.255	**1**.0.0.0 – **126**.0.0.0 *	8	$2^7 - 2 =$ 126 *	24	$2^{24} - 2 =$ 16,777,214
Class B	128.0.0.0 - 191.255.255.255	**128**.0.0.0 – **191.255**.0.0	16	$2^{14} =$ 16,384	16	$2^{16} - 2 =$ 65,534
Class C	192.0.0.0 - 223.255.255.255	**192**.0.0.0 – **223.255.255**.0	24	$2^{21} =$ 2,097,152	8	$2^8 - 2 = 254$
Class D	224.0.0.0 - 239.255.255.255					
Class E	240.0.0.0 - 255.255.255.255					

* 0.0.0.0 is reserved and 127.0.0.0 is the loopback address. Both cannot be assigned to hosts.

Types of IPv4 Addresses

Classful Addressing

Must remember the range of the first byte for classes A, B and C.

- Class A: 1 – 127
- Class B: 128 -191
- Class C: 192 -223

	Address range	Network address range	Network ID bits	Max number of network	Host ID bits	Number of usable host IP addresses
Class A	0.0.0.0 - 127.255.255.255	**1**.0.0.0 – **126**.0.0.0 *	8	$2^7 - 2 =$ 126 *	24	$2^{24} - 2 =$ 16,777,214
Class B	128.0.0.0 - 191.255.255.255	**128**.0.0.0 – **191**.255.0.0	16	$2^{14} =$ 16,384	16	$2^{16} - 2 =$ 65,534
Class C	192.0.0.0 - 223.255.255.255	**192**.0.0.0 – **223**.255.255.0	24	$2^{21} =$ 2,097,152	8	$2^8 - 2 = 254$
Class D	224.0.0.0 - 239.255.255.255					
Class E	240.0.0.0 - 255.255.255.255					

* 0.0.0.0 is reserved and 127.0.0.0 is the loopback address. Both cannot be assigned to hosts.

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Types of IPv4 Addresses

Classful Addressing

- The values of the last column are calculated by the formula:

Number of usable host IP addresses = $2^{(\text{host bits})} - 2$

- There is a need to subtract 2 for the following two reasons:
- All 0s in the host bits is the IP address of the network. E.g. if it is a Class A address with network ID: X, then X.0.0.0 is the IP address of the network.
- All 1's in the host bits is the broadcast address of the network. E.g. if it is a Class A address with network ID: X, then X.255.255.255 is the network's broadcast address.
- These 2 addresses cannot be used for host addresses, so the subtraction by 2.

	Address range	Network address range	Network ID bits	Max number of network	Host ID bits	Number of usable host IP addresses
Class A	0.0.0.0 - 127.255.255.255	**1**.0.0.0 – **126**.0.0.0 *	8	$2^7 - 2 =$ 126 *	24	$2^{24} - 2 =$ 16,777,214
Class B	128.0.0.0 - 191.255.255.255	**128**.0.0.0 – **191**.255.0.0	16	$2^{14} =$ 16,384	16	$2^{16} - 2 =$ 65,534
Class C	192.0.0.0 - 223.255.255.255	**192**.0.0.0 – **223**.255.255.0	24	$2^{21} =$ 2,097,152	8	$2^8 - 2 = 254$
Class D	224.0.0.0 - 239.255.255.255					
Class E	240.0.0.0 - 255.255.255.255					

* 0.0.0.0 is reserved and 127.0.0.0 is the loopback address. Both cannot be assigned to hosts.

Public and Private IPv4 Addresses

Public Addresses

- Unique addresses that can be accessed over the Internet.
- Not all available IP addresses can be used over the Internet. Some of these addresses are reserved for organisations to be used for their internal networks. These addresses are called private addresses.
- Due to the depletion of IPv4 address space, *private IPv4 addresses* were introduced. Private IP addresses are not unique and can be used by any organization.

Private Address Ranges

• Class A: 10.0.0.0/8	or	10.0.0.0	to	10.255.255.255
• Class B: 172.16.0.0/12	or	172.16.0.0	to	172.31.255.255 **(refer to next slide)**
• Class C: 192.168.0.0/16	or	192.168.0.0	to	192.168.255.255

- Private IP addresses are not allowed on the Internet and will be discarded by Internet routers.
- In order for hosts using private addresses to be able to access the Internet, Network Address Translation (NAT) is used to translate each private address to a ~~private~~ public address.
- This is usually done by the router that connects the internal network to the ISP's network.

Public and Private IPv4 Addresses (additional)

Private Address Ranges

- **Class B: 172.16.0.0/12 or 172.16.0.0 to 172.31.255.255 (refer to Table)**

Class B	N	SN	H	H	H
IP Address	172. 172.	(0001 0000). 16.		0. 0.	0 0
Subnet Mask	255. 255.	(1111 0000). 240.		0. 0.	0 0
First Address	172. 172.	(0001 0000. 16.		0000 0000. 0.	0000 0000) 0
Second Address	172. 172.	(0001 0000. 16.		0000 0000. 0.	0000 0001) 1
Last Address	172. 172.	(0001 1111. 31.		1111 1111. 255.	1111 1111) 255

Wastage of Addresses in Classful Addressing

- In classful addressing, many IP addresses are wasted.
- E.g. consider an organization that needs a network with 300 hosts and is given a Class B address.
- A Class B address can have $2^{16} - 2$ or 65,534 hosts. Thus 65,534 - 300 or 65,234 addresses are wasted.
- To overcome this wastage, classless addressing was introduced.

Classless Addressing

- In ***classless addressing*** the number of bits used for the network IDs and host IDs are of variable length.

- In comparison, the network ID of classful addressing is fixed for each class.

- In classless addressing, we can increase the number of network bits so that the same classful network address can be allocated to different networks.

Classless Addressing Example

- If the Class A network address 32.0.0.0 is allocated to an organization, many host addresses would be wasted.
- In classless addressing, we can increase the number of network bits and allocate it to different organisations.
- For instance, if we want to use the network address 32.0.0.0 to allocate to 4 different organisations, we will need 2 additional network bits. Two bits can give the following four combinations: 00, 01, 10, 11. These four combinations will be part of the network IDs to be assigned to the four organisations respectively.

	Network ID	Number of Host ID bits	Number of usable host IP addresses
Classful addressing	32 (0010 0000).	24	$2^{24} - 2 = 16,777,214$
Classless addressing	32 (0010 0000). **00**	22	$2^{22} - 2 = 4,194,302$
	32 (0010 0000). **01**	22	$2^{22} - 2 = 4,194,302$
	32 (0010 0000). **10**	22	$2^{22} - 2 = 4,194,302$
	32 (0010 0000). **11**	22	$2^{22} - 2 = 4,194,302$

Classless Addressing Example

- The network addresses for the four organisations can be allocated as shown.
- For network or subnet address, the host ID portion is always all 0s.

	Network ID	Number of Host ID bits	Number of usable host IP addresses
Classful addressing	32 (0010 0000).	24	$2^{24} - 2 = 16,777,214$
Classless addressing	32 (0010 0000). **00**	22	$2^{22} - 2 = 4,194,302$
	32 (0010 0000). **01**	22	$2^{22} - 2 = 4,194,302$
	32 (0010 0000). **10**	22	$2^{22} - 2 = 4,194,302$
	32 (0010 0000). **11**	22	$2^{22} - 2 = 4,194,302$

Organisation / Subnet Number	Network ID	Host ID	Subnet Address
Organisation 1 / Subnet 0	32. (**00**	000000). 0.0	32.**0**.0.0
Organisation 2 / Subnet 1	32. (**01**	000000). 0.0	32.**64**.0.0
Organisation 3 / Subnet 2	32. (**10**	000000). 0.0	32.**128**.0.0
Organisation 4 / Subnet 3	32. (**11**	000000). 0.0	32.**192**.0.0

Subnet Mask	255. (11	000000). 0. 0
	255. 192. 0. 0 or /10	

Subnetting an IPv4 Network

- A subnetwork or subnet is a logical division of an IP network.
- Subnetting is the process of dividing a network into two or more subnets.
- Subnetting improves network performance and reduces network congestion by creating smaller broadcast domains.
- Subnetting does not change how the outside world sees the network, but there are additional structures within the organization.
- Each subnet in a divided network has its own unique IP address.

Four Subnetting Steps

To correctly subnet a given network address into subnet addresses, ask yourself the following questions:

1. How many bits do I need to borrow from the host ID to be used as **subnet bits**?
2. What is the resultant **subnet mask** after the borrowing?
3. What are the **subnet addresses**?
4. What **range of host addresses** can I use in each subnet?

Step 1: How Many Bits to Borrow?

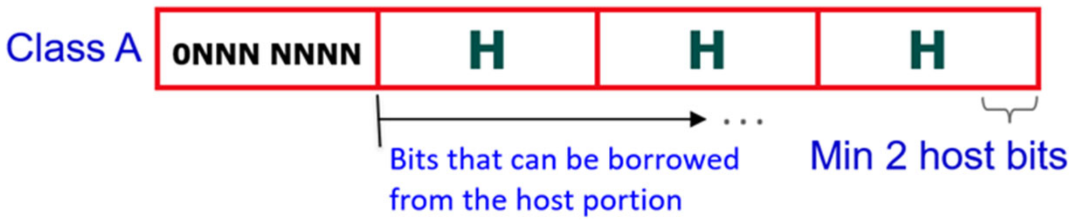
- First, you need to know the class of the network address.
- From the class, you will know the number of available host bits to borrow for subnet ID.
- The number of host bits for the first three classes are:
  - Class A: 24 host bits
  - Class B: 16 host bits
  - Class C: 8 host bits

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Four Subnetting Steps

Step 1: How Many Bits to Borrow?

- To create subnets, we borrow some host bits from the host portion starting from the most significant host bits.
- You can borrow as many host bits as needed to be subnet bits, but must leave at least 2 host bits in the host portion regardless of network class.



- The reason to leave at least 2 host bits:
  - ➢ If 1 host bit is left, number of host addresses = $2^1 - 2 = 0$.
  - ➢ If 2 host bits are left, number of host addresses = $2^2 - 2 = 2$.
- These calculations are based on the following formula:

Number of usable host IP addresses = $2^{(\text{host bits})} - 2$

- Next, you must know either the number of subnets you need or the number of hosts per subnet you need.
- If ***N*** is the required **number of subnets** and ***n*** is the **bits borrowed from the host portion**, then

$$2^n \geq N$$

Four Subnetting Steps

Step 1: How Many Bits to Borrow?

- Calculators are not allowed in exam for this course.
- You are expected to remember these powers of 2:

$2^0 = 1$	$2^6 = 64$
$2^1 = 2$	$2^7 = 128$
$2^2 = 4$	$2^8 = 256$
$2^3 = 8$	$2^9 = 512$
$2^4 = 16$	$2^{10} = 1024$
$2^5 = 32$	

Four Subnetting Steps

Step 1: How Many Bits to Borrow?

Example 1: If you are given the network address **210.93.45.0/24**, and would like to have **at least 5 subnets**. How many subnet bits do you need? How many host addresses can you have per subnet?

- First, you need to know the class.
  - By examining the first byte of the IP address, you know it is a Class C address, which has 8 host bits.
  - After subtracting the 2 host bits, there are 6 bits available to be borrowed.
- Next, you need to decide on the number of bits to borrow.
  - If n is the bits borrowed to fulfil 5 subnets, then $2^n \geq 5$.
  - n must be at least 3 ($2^3 \geq 5$). If no other reason is stated, you will borrow the least number of bits that can meet the requirement. Thus, 3 subnet bits is used.
- Lastly, you can calculate the number of host addresses per subnet.
  - After borrowing 3 host bits for subnets, there are 5 host bits left.
  - This gives $2^5 – 2 =$ 30 host IP addresses per subnet.

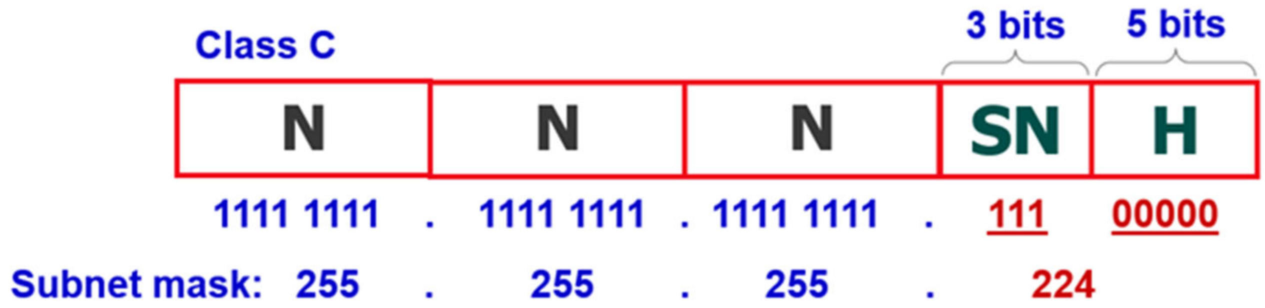
110N NNNN	N	N	SN	H
Class C			3 bits	5 bits

Four Subnetting Steps

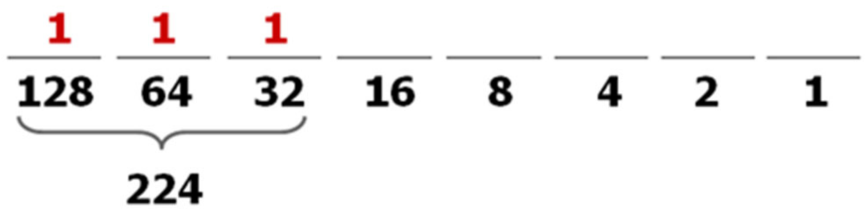
Step 2: What is the Resultant Subnet Mask?

Example 1: If you are given the network address **210.93.45.0/24**, and would like to have **at least 5 subnets** (with 3 bits borrowed). What is the Resultant Subnet Mask?

- If there is subnetting, the network and subnet portions are represented by 1s and the host portion by 0s.
- The resultant subnet mask is 255.255.255.224 or /27



- You can determine part of the value of the subnet mask by adding up the decimal value of the bits we borrowed.



Four Subnetting Steps

Step 2: What is the Resultant Subnet Mask?

Example 1: If you are given the network address **210.93.45.0/24**, and would like to have **at least 5 subnets** (with 3 bits borrowed). What is the Resultant Subnet Mask?

- You are expected to remember the decimal value for the binary bits shown below.

Bits borrowed from host portion: begin from the left

128	64	32	16	8	4	2	1 ← Value at each bit position		
0	0	0	0	0	0	0	0	=	0
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

Four Subnetting Steps

Step 3: What are the Subnet Addresses?

Example 1: If you are given the network address **210.93.45.0/24**, and would like to have **at least 5 subnets** (with 3 bits borrowed). What are the Subnet Addresses?

You may notice that Subnet 0 is the network address.

Class C	N	N	N	SN	H
Network address	210.	93.	45.	0	
Subnet 0 address	210.	93.	45.	**000** 00000 0	
Subnet 1 address	210.	93.	45.	**001** 00000 32	
Subnet 2 address	210.	93.	45.	**010** 00000 64	
Subnet 3 address	210.	93.	45.	**011** 00000 96	
Subnet 4 address	210.	93.	45.	**100** 00000 128	
Subnet 5 address	210.	93.	45.	**101** 00000 160	
Subnet 6 address	210.	93.	45.	**110** 00000 192	
Subnet 7 address	210.	93.	45.	**111** 00000 224	

5 required subnets

Unused subnets

Four Subnetting Steps

Step 4: What Range of Host Addresses can I use in Each Subnet?

Example 1: If you are given the network address **210.93.45.0/24**, and would like to have **at least 5 subnets** (with 3 bits borrowed). Give the range of host addresses for the first 5 subnets.

- The range of host addresses for Subnet 1 is shown below.

Class C	N	N	N	SN	H
Network address	210.	93.	45.	0	
Subnet 1 address	210.	93.	45.	**001** 00000 = 32	
Range of host addresses for Subnet 1	210.	93.	45.	001 **00001** = 33 001 **00010** = 34 001 **00011** = 35 . . 001 **11110** = 62	
Broadcast address for Subnet 1	210.	93.	45.	**001** 11111 = 63	

First host

There are 5 host bits, so the number of host addresses = $2^5 - 2 = 30$

Last host

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Four Subnetting Steps

Step 4: What Range of Host Addresses can I use in Each Subnet?

Example 1: If you are given the network address **210.93.45.0/24**, and would like to have **at least 5 subnets** (with 3 bits borrowed). Give the range of host addresses for the first 5 subnets.

- The range of host addresses for the first 5 subnets is shown below.

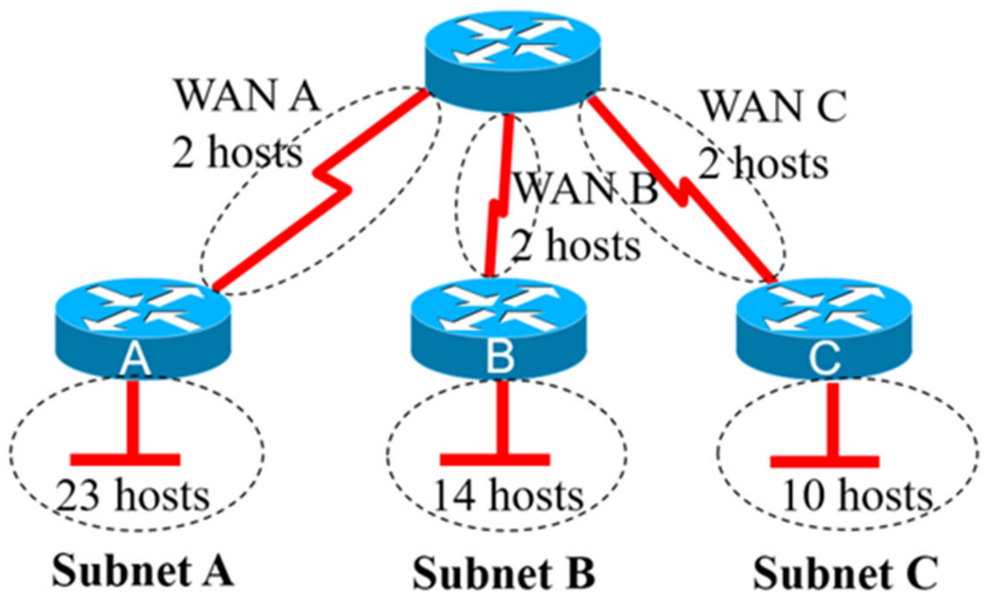
	1st Host IP Address →	To Last Host IP Address
Subnet 0	210.93.45. *000* ***00001*** 210.93.45. *1*	210.93.45. *000* ***11110*** 210.93.45. *30*
Subnet 1	210.93.45. *001* ***00001*** 210.93.45. *33*	210.93.45. *001* ***11110*** 210.93.45. *62*
Subnet 2	210.93.45. *010* ***00001*** 210.93.45. *65*	210.93.45. *010* ***11110*** 210.93.45. *94*
Subnet 3	210.93.45. *011* ***00001*** 210.93.45. *97*	210.93.45. *011* ***11110*** 210.93.45. *126*
Subnet 4	210.93.45. *100* ***00001*** 210.93.45. *129*	210.93.45. *100* ***11110*** 210.93.45. *158*

Fixed Subnet Length Subnetting Wastes Addresses

- In Example 1, the subnetting was performed using fixed subnet length.
- That is each subnet is allocated with the same number of IP addresses.
- This is fine if all the subnets have the same requirements.
- This is usually not the case.

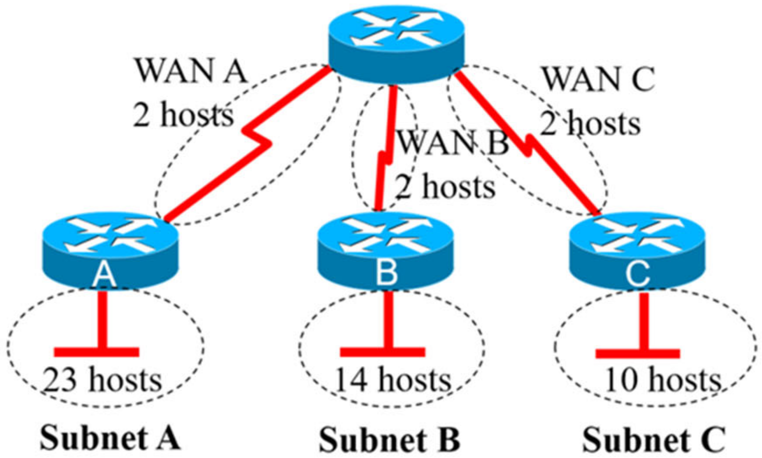
Example 2: A company is given the network address **192.168.10.0/24** with requirements as shown below.

- Six subnets require at least 3 subnet bits ($2^3 \geq 6$).
- To maximize the host bits, we will use 3 subnet bits.
- Class C address => 5 remaining host bits.
- This gives 30 ($2^5 - 2$) host addresses per subnet.
- All the subnets have the same subnet mask of 255.255.255.224 or /27 (24 network bits, 3 subnet bits and 5 host bits).



Fixed Subnet Length Subnetting Wastes Addresses

- Based on 30 available host addresses per subnet obtained in Example 2, let us examine the wastage of IP addresses in fixed length subnetting.



Subnet	Number of usable host addresses	Number of required host addresses	Number of unused host addresses
Subnet A	30	23	7
Subnet B	30	14	16
Subnet C	30	10	20
WAN A	30	2	28
WAN B	30	2	28
WAN C	30	2	28

- The solution to this inefficiency is to use ***Variable Length Subnet Mask (VLSM)***.

Variable Length Subnet Mask (VLSM)

- In VLSM, the number of bits to borrow depends on the need of each subnet.
- Thus, the subnet mask varies from subnet to subnet.
- In VLSM, always **start the subnetting with the largest subnet**, then down to the smallest subnet.
- The network is first subnetted to meet the needs of the largest subnet, and then the subnets are subnetted again.
- We will use Example 2 to illustrate the VLSM process in 4 steps.

Variable Length Subnet Mask (VLSM)

Example 2: A company is given the network address **192.168.10.0/24**.

Step 1: Subnetting to Meet the Need of the Largest Subnet

- We will subnet based on the largest subnet of 23 hosts.
- We need 5 host bits ($2^5 - 2 \geq 23$).
- Class C address => leaves 3 bits for subnets.
- Network 192.168.10.0/24 is subnetted into 8 equal-sized subnets as shown.

Network portion	Host portion	Dotted Decimal
192.168.10.	0000 0000	192.168.10.0/24

Subnet No.	Network portion	SN	H	Dotted Decimal	Allocation
0	192.168.10.	000	00000	192.168.10.0/27	Subnet A
1	192.168.10.	001	00000	192.168.10.32/27	Subnet B
2	192.168.10.	010	00000	192.168.10.64/27	Subnet C
3	192.168.10.	011	00000	192.168.10.96/27	Unused or available for future expansion
4	192.168.10.	100	00000	192.168.10.128/27	
5	192.168.10.	101	00000	192.168.10.160/27	
6	192.168.10.	110	00000	192.168.10.192/27	
7	192.168.10.	111	00000	192.168.10.224/27	To be subnetted further

Variable Length Subnet Mask (VLSM)

Example 2: A company is given the network address **192.168.10.0/24**.

Step 2: Deciding on the Allocation and Choosing a Subnet to Subnet Further

- Allocate the first 3 subnets to Subnet A, B and C respectively.
- Recall: WAN subnets have the most wastage in addresses since it requires only two usable addresses. To avoid this, use VLSM to further divide a subnet. The last subnet (Subnet 7) will be further subnetted.
- With VLSM, Subnets 3 to 6 can be made available for future expansion.

Network portion	Host portion	Dotted Decimal
192.168.10.	0000 0000	192.168.10.0/24

Subnet No.	Network portion	SN	H	Dotted Decimal	Allocation
0	192.168.10.	**000**	00000	192.168.10.0/27	Subnet A
1	192.168.10.	**001**	00000	192.168.10.32/27	Subnet B
2	192.168.10.	**010**	00000	192.168.10.64/27	Subnet C
3	192.168.10.	**011**	00000	192.168.10.96/27	Unused or available for future expansion
4	192.168.10.	**100**	00000	192.168.10.128/27	
5	192.168.10.	**101**	00000	192.168.10.160/27	
6	192.168.10.	**110**	00000	192.168.10.192/27	
7	192.168.10.	**111**	00000	192.168.10.224/27	To be subnetted further

Variable Length Subnet Mask (VLSM)

Step 3: Subnetting a Subnet

- Each WAN subnet needs only 2 usable addresses, 2 host bits is sufficient to meet the need. This is based on the formula:

  Number of usable host IP addresses = $2^{(\text{host bits})} - 2$

- Setting 2 bits for host ID, allows 3 more bits to be borrowed for subnet ID. This extra 3 bits can give an addition of 8 sub-subnets ($2^3 = 8$). This gives a total of 6 bits for Subnet ID. Figure below shows how Subnet 7 is subnetted to create more subnets.
- VLSM reduces the amount of address wastage and free up many address spaces.

Subnet No.	Network portion	SN	H	Dotted Decimal
7	192.168.10.	111	00000	192.168.10.224/27

3 more bits borrowed from Subnet 7 ↓

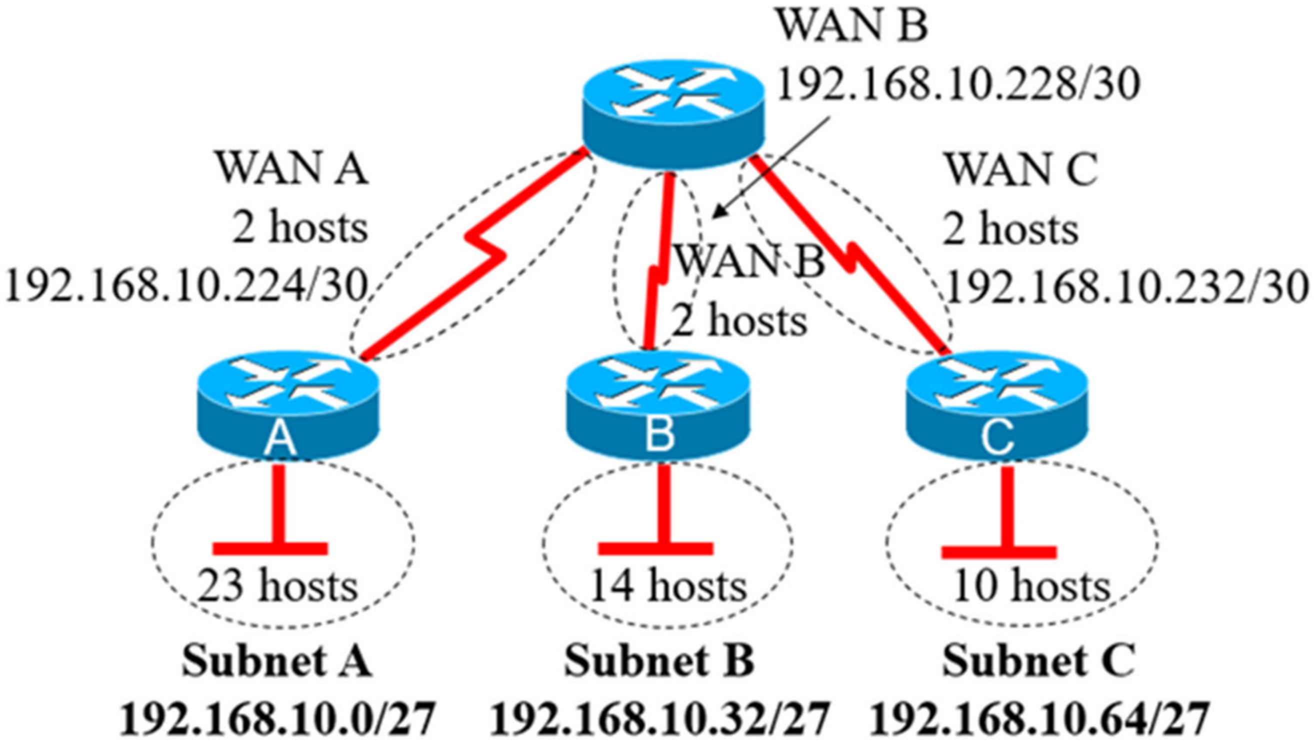
Sub-Subnet	Network portion	SN	H	Dotted Decimal	Allocation
7:0	192.168.10.	111 000	00	192.168.10.224/30	WAN A
7:1	192.168.10.	111 001	00	192.168.10.228/30	WAN B
7:2	192.168.10.	111 010	00	192.168.10.232/30	WAN C
7:3	192.168.10.	111 011	00	192.168.10.236/30	Unused or available for future expansion
7:4	192.168.10.	111 100	00	192.168.10.240/30	
7:5	192.168.10.	111 101	00	192.168.10.244/30	
7:6	192.168.10.	111 110	00	192.168.10.248/30	
7:7	192.168.10.	111 111	00	192.168.10.252/30	

Variable Length Subnet Mask (VLSM)

Example 2: A company is given the network address **192.168.10.0/24**.

Step 4: Assigning Addresses to the Network Topology

- The calculated subnet addresses are assigned to the network topology as shown below.



Variable Length Subnet Mask (VLSM)

Example 2: A company is given the network address **192.168.10.0/24**.

Step 4: Assigning Addresses to the Network Topology

- The calculations for the host addresses are shown below.

	Network portion	SN	H	Dotted Decimal
Subnet A: First Host	192.168.10.	000	00001	192.168.10.1/27
Subnet A: Last Host	192.168.10.	000	11110	192.168.10.30/27
Subnet B: First Host	192.168.10.	001	00001	192.168.10.33/27
Subnet B: Last Host	192.168.10.	001	11110	192.168.10.62/27
Subnet C: First Host	192.168.10.	010	00001	192.168.10.65/27
Subnet C: Last Host	192.168.10.	010	11110	192.168.10.94/27

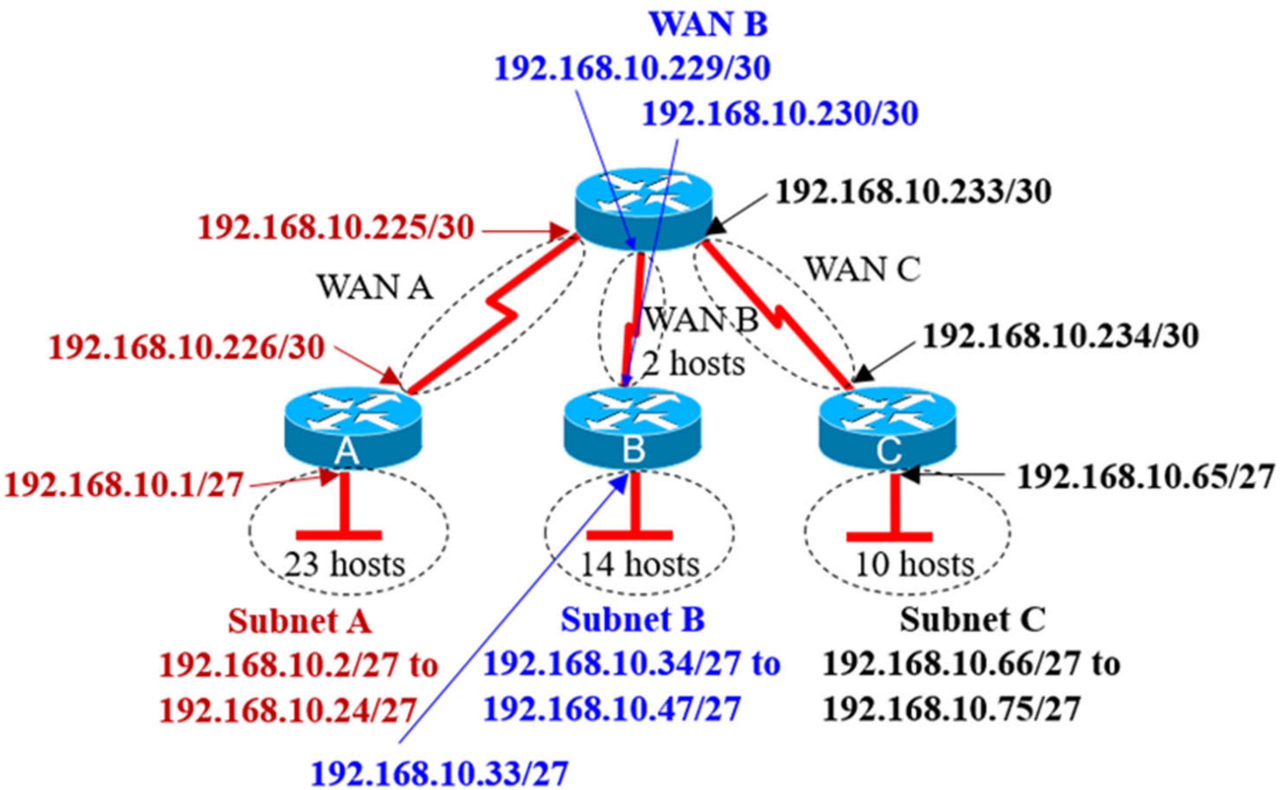
	Network portion	SN	H	Dotted Decimal
WAN A: First Host	192.168.10.	111 000	01	192.168.10.225/30
WAN A: Last Host	192.168.10.	111 000	10	192.168.10.226/30
WAN B: First Host	192.168.10.	111 001	01	192.168.10.229/30
WAN B: Last Host	192.168.10.	111 001	10	192.168.10.230/30
WAN C: First Host	192.168.10.	111 010	01	192.168.10.233/30
WAN C: Last Host	192.168.10.	111 010	10	192.168.10.234/30

Variable Length Subnet Mask (VLSM)

Example 2: A company is given the network address **192.168.10.0/24**.

Step 4: Assigning Addresses to the Network Topology

- The IP address of the first host of each LAN is usually assigned to the default gateway.
- The other hosts in the LAN will be assigned starting from the second host IP address. Figure below shows the assignment of host addresses to the network topology.



Fixed Length vs Variable Length Subnet Mask

- In classful **fixed length subnet mask**, the number of bits to borrow are **based on** whether the emphasis is on the **subnet or host requirements**.
- In **VLSM**, the number of bits to borrow are **based on the host requirements** so as not to waste host addresses.

Summary

- The network layer uses Addressing, Encapsulation, Routing and Decapsulation to provide services to allow end devices to exchange data across the network.
- The 3 basic characteristics of IP are Connectionless, Best Effort Delivery and Media Independent.
- Hub, Switch and Router are intermediate networking devices with different features and functions.
- An IPv4 address has a network portion and a host portion.
- The subnet mask is used to identify the network and host portions of an IPv4 address.
- The 5 classes of IPv4 addresses are from Class A to E.

Summary

- **The 4-steps of subnetting using fixed subnet length are:**
  1. Decide on the number of bits to borrow for subnetting
  2. Obtain the resultant subnet mask
  3. Work out the subnet addresses
  4. Work out the range of host addresses for each subnet

- **Fixed subnet length subnetting wastes IP addresses.**

- **Variable Length Subnet Masking (VLSM) is the solution to this wastage.**

- **The 4-steps of subnetting using VLSM are:**
  1. Subnet the network based on the need of the largest subnet
  2. Decide on the allocation and choose a subnet to further subnet
  3. Subnet the chosen subnet
  4. Assign addresses to the problem scenario

Thank You.