

King Fahd University of Petroleum & Minerals

Electrical Engineering Department

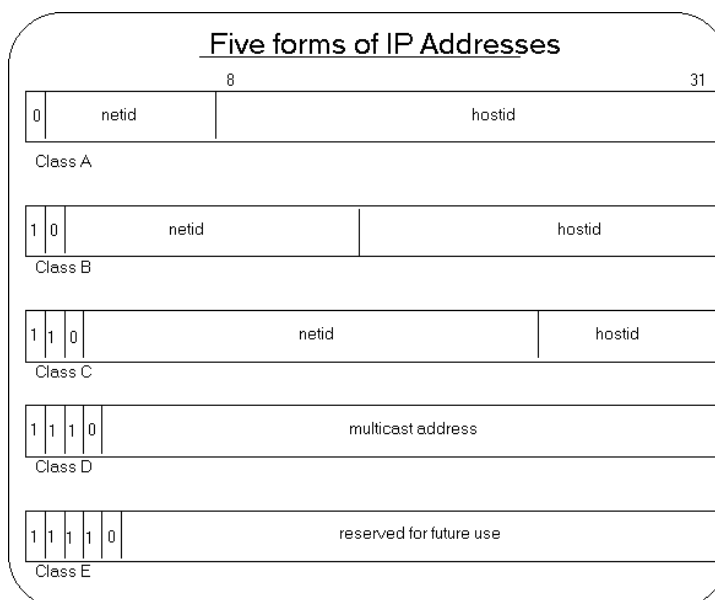
EE 400, Experiment # 2

IP Addressing and Subnetting: Establishing Elementary Networks using Hubs, Switches and Routers.

Objectives:

After this experiment, the students shall be able to explain the need and significance of assigning IP addresses statically or dynamically, its associated subnet mask, default gateway, and DNS servers. They shall be able to identify and use hubs, layer-2 switches, routers and layer-3 switches appropriately to establish an elementary network.

IP addressing:



	Net ID	First Host	Last Host	Net ID (bytes)	Host ID (bytes)	Size of Net
Class A				1	3	Huge # of Host, Less # of NW
First Network	1.0.0.0	1.0.0.1	1.255.255.254			
Last Network	126.0.0.0	126.0.0.1	126.255.255.254			# of Host = # of NW
Class B				2	2	
First Network	128.1.0.0	128.1.0.1	128.1.255.254			Huge # f NW, Less # of Hosts
Last Network	191.254.0.0	191.254.0.1	191.254.255.254			
Class C				3	1	
First Network	192.0.1.0	192.0.1.1	192.0.1.254			
Last Network	223.255.254.0	223.255.254.1	223.255.254.254			

Class D: a multicast address. (224.0.0.0 - 240.0.0.0)

Class E: reserved for future use. (241.0.0.0 - 248.0.0.0)

Special forms of Internet Addresses

For class C address, only 254 hosts can be supported because

- 0 is reserved for boot process
- 255 reserved for broadcast

0.0.0.0 – Default route

0.host_number - host on this net.

255.255.255.255 - Limited broadcast (local net).

net_number.255 - Directed broadcast for the specified net. (e.g 196.15.32.255

broadcast to all hosts of the 196.15.32.0 network.)

127.anything - Loop back test

Given the above parameters, this system allows for the following combinations of valid Internet network and host addresses:

To determine the number of possible networks or hosts, use the formula $2^n - 2$, where n is the number of bits in the network or host space. The subtraction of 2 is for the actual network and broadcast address.

Class	Possible Networks	Possible Hosts
A	126	16,777,214
B	16,384	65,534
C	2,097,152	254

Several networks are reserved for private use and cannot be used on the Internet. They include:

Class	Address Range
A	10.x.x.x
B	172.16.x.x through 172.31.x.x
C	192.168.x.x

These addresses are commonly used for corporate intranets and for testing.

IP Subnetting (Refer to Appendix C for more reading)

Subnetting is a Technique used to allow a single IP network address to span multiple physical networks. IP hosts should support subnetting. Subnetting is done by using some of the bits of the host-id part of the IP address as a physical network identifier. The subnet mask is used to

determine the bits of the network identifier. All hosts on the same network should have the same subnet mask.

An example of Subnetting:

The Class B network 128.10.0.0 can be subnetted using the first 8 bits of the host-id, to span 254 different physical networks. The subnet mask for this case is 255.255.255.0 The subnetworks are: 128.10.1.0, 128.10.2.0, ..., 128.10.254.0 . Each of the subnetworks can have up to 254 different hosts:

128.10.X.1, 128.10.X.2, ..., 128.10.X.254 .

If there is a need for less physical nets and more hosts in each one, less host-id bits can be used for subnetting. For example: With the subnet mask 255.255.254.0, 126 different subnets are available with up to 510 hosts in each one.

Many Class A and B networks do not contain as many hosts as they could. This situation causes a lot of address space waste. Subnetting better utilizes the address space by dividing these big networks to smaller ones.

IP Subnetting examples

Class C subnetting example.

In Host ID, 3 bits are used for subnet, 5 are used for Hosts

Only $(2^5 = 32) - 2 = 30$ Host are allowed for each subnet because

- 31 used for broadcast
- 0 used for bootup

Only $2^3 - 2 = 8 - 2 = 6$ subnets are allowed because

- 0 is not allowed
- All 1's are used for broadcast.

Subnet mask for Host ID field will be $(1110\ 0000)_b = (224)_d$

Thus full Subnet mask will be 255.255.255.224

Cabling Categories:

Cable categories represent the amount of twist per unit length in the cable that results in better shielding effect in the cable thus increasing the capability of the cable to carry high speed data.

- *Category 1:* suitable for voice only (1950s)
- *Category 2:* suitable for voice and low data rates (less than 4 Mbps). (1960s)
- *Category 3:* suited for voice and data rates up to 10 Mbps. Uses 4 twisted-pairs. Standard for most telephone installations. (1991)
- *Category 4:* consists of 4 twisted-pairs. Suitable for data rates up to 16 Mbps. Support fast Token Ring networks. (1993)
- *Category 5:* consists of 4 twisted-pairs. Suitable for data rates up to 100 Mbps. Supports 100Base-TX. (1994)
- *Category 6:* consists of 4 twisted-pairs. Suitable for data rates up to 1 Gbps. Supports 1000Base-TX. (1994)

Straight-Through and Crossover Cable Pin outs:

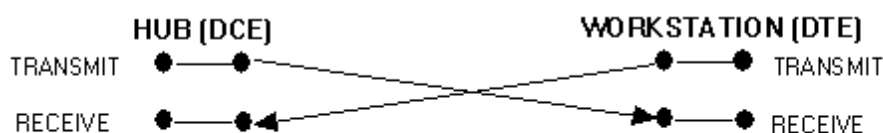
Cables ending in RJ45's may be wired up in two ways: **straight through** and **crossover**. A straight through cable connects pins N at both ends, whereas a crossover cable has the various pairs crossed over. Whether a straight through or crossover cable is required will depend on the types of network equipment and how they are interlinked.

The schematics of crossover and straight-through cables are shown in below.

Straight-Through Cable Schematic	Crossover Cable Schematic

MDI / MDI-X ports:

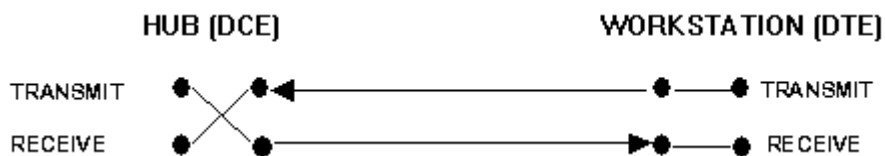
Consider the connection between a hub (DCE) and a workstation (DTE), shown in the figure below



The connection between a DCE and a DTE using a crossover cable.

There must be a point of crossover between the DCE and DTE for data to be successfully exchanged. Above figure shows a cable with the transmit and receive pairs crossed over. On a hub most of the ports will connect to DTE's (workstations, PCs etc.) and at some point a signals crossover must be affected. Equipment manufacturers are aware of this situation so the industry accepted standard is that all ports on hubs and switches which do not have a

media conversion capability have crossovers already built in. In such cases (the vast majority) only a straight-through cable is required to connect to a DTE. Figure below shows the DCE (hub) with a built in crossover port. Visually it is not easy to distinguish between straight-through and crossover cables so it is preferable to avoid having both types of cable in an installation. Using hubs and switches with crossover ports built in is a way of eliminating the need for crossover cables altogether. Ports on such equipment are often marked **MDI-X (Media Dependant Interface-Internally Crossed over)**. Uplink ports (e.g. 100BaseT) will not usually have built-in crossover and may be marked **MDI (Media Dependant Interface)**.



The connection between a DCE and DTE using a straight through cable because the port of the DCE is already crossed over internally. Many hubs and switches feature ports which are switchable between crossover for DTE connection and straight-through for cascading or uplinking, all others being MDI-X only, or unmarked.

LAN Devices:

Network Interface Card (For further reading on the subject, refer to Text book, sec 6.2)

Network interface cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable.

Many NIC adapters comply with Plug-n-Play specifications. On these systems, NICs are automatically configured without user intervention, while on non-Plug-n-Play systems, configuration is done manually through a setup program and/or DIP switches.

Cards are available to support almost all networking standards, including the latest Fast Ethernet environment. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Full duplex networking is another option, where a dedicated connection to a switch allows a NIC to operate at twice the speed.

Repeater :

A repeater is a device used to extend the network length and topology beyond what can be achieved by a single cable segment. It is used to re-time and amplify the individual signals and has no concept of packets.

Repeaters, also called hubs or concentrators, are bit level devices. What this means that they do not examine the data packets that travel through them. They have no knowledge of addresses associated with the source or the destination. The basic operation of a repeater is to

repeat traffic. Any data arriving on one port will be amplified and repeated out all ports (except the port on which it was received).

Repeaters were originally designed with only two ports and were used to increase the size of coax cable-based networks. This way, different lengths of coax cable could be attached to the repeater to extend the size of the network. This would allow the network to reach all areas of large or tall buildings. Data would be repeated from one cable segment to the other.

When the coax cabling was replaced by concentrators or hubs, the concentrators were, in fact, just repeaters with many more ports. Now, data received on one port would be replicated anywhere from twice to hundreds of times and transmitted to attached stations. The repeater also had the ability to track how much traffic was crossing through it.

Repeaters may also be linked together for even greater distances, but it is recommended that the data should not need to cross more than four repeaters. This is because each time the data gets repeated it may be slightly distorted. If there are too many distortions, original signal may be unreadable.

A very important fact to note about hubs is that they only allow users to share Ethernet. A network of hubs/repeaters is termed a "shared Ethernet," meaning that all members of the network are contending for transmission of data onto a single network (collision domain). This means that individual members of a shared network will only get a percentage of the available network bandwidth.

Repeaters support all standard LAN protocols and cabling types, and a repeater can translate between different cabling. Today, repeaters are being replaced called a bridge.

Bridge and Layer-2 Switch:

A bridge operates at layer 2 of the OSI model and offers several functions, including expansion of networks beyond normal physical limitations, overcoming station count limitations, packet storage and forwarding, and keeping local traffic local by building an address table (SAT) of where devices are located within the network.

Bridges offer several advantages over repeaters, including:

- **Expansion of network** - because of regeneration issues, packets can only be repeated a limited number of times. Bridges eliminate the problem by copying and recreating new packets before forwarding them.
- **Overcoming station count limitations** - each type of LAN (Ethernet, token ring, FDDI) has a maximum number of users allowed on one segment. Bridges allow for the creation of multiple bridging segments.
- **Packet storage and forwarding** – bridges receive the packet, examine it, and then determine where it needs to go. If there is other traffic on the destination port, the bridge buffers (stores) the packet until the port is able to accept more traffic.
- **Keeping local traffic local** – the bridge's ability to read packets and identify addresses enables it to determine where a destination is located. This eliminates sending packets to segments that do not contain the destination.

- **Translating between different speeds** – bridges are required to interface between networks of different speeds (e.g., Ethernet's 10, 100, and 1000 Mbps)
- **Translating traffic between LAN protocols** – bridges, acting as interpreters, have the ability to translate packets between other LAN protocols such as Ethernet, token ring, FDDI, and ATM.

Bridges fit into the network in a similar fashion as repeaters and they support all the capabilities of repeaters (amplifications of signals, etc.). However, bridges have increased intelligence and can perform additional functions.

The repeater repeats all traffic that goes through it, so if I had a 24-port repeater and a packet came in one port, it would be repeated out 23 other ports. This is because the repeater does not know where to send it. A bridge, though, is aware of the individual packets and the addressing that is used. A bridge that receives that same packet examines it and resends it only to the port that has the destination address attached to it. Obviously, this is a better way to handle traffic.

Besides having the ability to examine packets and forward based on addresses, bridges have the ability to learn where the different addresses are located on the network. This means the bridge will learn which PC is located on which port, and it also keep track of this address if the PC is moved. Bridges can also be used to separate repeated networks. Bridges support all protocol and media types, and even have the ability to translate one LAN protocol to another.

Routers :

Routers perform their function at layer 3 of the OSI Model and are used to forward messages across an extended network based on network layer addresses (logical addressing), not MAC layer addresses. They route messages from end-station to end station, allowing multiple paths between them. Routers can also be used to provide better traffic isolation and security by using access lists that control who can communicate through the router. Routers are used to forward traffic on the internet.

Routers offers several advantages over repeaters and bridges. These include:

- **Isolation of broadcast traffic** – routers prevent the flow of broadcast traffic from one LAN to another.
- **Path selection** – routers can use the best path that physically exists between source and destination. Some routers allows for load balancing over redundant paths.
- **Flexibility** – routers can support any desired protocol or network topology.
- the total size of the network interconnected with routers is, for all practical purposes, unlimited (e.g., the Internet)
- Routers supports layer 1,2,and 3 functionality.

Note : Routers are more intelligent than bridges, but they are not plug-and-play routers must be configured by a human.

Routers are designed to separate different parts of the network into what are called sub-nets, which are subdivisions of the the total network. This division of the network is done to

support the different requirements of the organization, and it allows a network manager to separate and control traffic in the different sub-nets. Routers are often used to separate the network for the purpose of security. Doing this allows a network manager to keep some traffic inside a sub-net and allows other traffic to cross sub-net boundaries. An example of using routers and sub-nets would be a large company that has divided their network up based on departments. Sales might be one sub-net, marketing on another sub-net, and engineering on another sub-net. All these sub-nets would form the complete network, and within each sub-net is a collection of users connected to bridges or repeaters.

Routers support all the capabilities of bridges and repeaters along with network layer (layer3) protocols.

Layer-3 Switches:

Networks started as a collection of computers connected by a single cable.

The next evolution of networks was the introduction of the repeater. The repeater allowed the larger networks (Distance and size) and eliminated the cable as a single point of failure. The problem was that traffic was flooded everywhere.

The next evolution was the bridge. Originally, bridges were designed to separate networks into different sections, and this cut down on the amount of flooded traffic. Bridges could then used to interconnect groups of users connected to repeaters.

Next came the router. With the routers, logical groupings could be defined, traffic could be better controlled. Now you had networks with users connected to repeaters, the repeater connected to bridges and the bridges connected to routers, with each network network device doing its own thing.

A switch operates at layer 1, layer 2, and layer 3 (sometimes layer 4) and allows users to use a single device to support multiple capabilities. Now, using one device, some traffic can be repeated, some bridged, and some routed, all based on where the traffic needs to go. This is called switching. Switches combine the intelligence of repeaters, bridges, and routers into one networking device. Some of the advantages to using single box for all three functions are listed as follows:

- Save time – one device to manage
- Single device required for spare
- Reconfigure instead of move/replace
- Single version of software need for upgrading network.

Switches look like repeaters or bridges and allow direct connection to the PCs or to other switches, bridges, or routers, These devices are designed with much more intelligence built in, and the network manager can configure any port, or groups of ports , to act as repeaters, bridges, or routers. the idea here is that you do not need to purchase and manage three different types of devices in your network – you can purchase one type of device and configure it the way you need it.

Exercise:

1. Students will distribute themselves in four groups A, B, C and D.
2. Connect computers in groups A and B to Hub 1 and Switch 1 respectively.
3. Connect computers in groups C and D to Switch 2 and Switch 3 respectively.

Phase 1

4. Assign IP addresses and subnet masks of the computers in each group as depicted in the figure 2.1. Groups A and B belong to the one subnet and Groups C and D belong to other subnet.
5. Interconnect group A and group B by connecting Hub 1 and Switch 1 with the help of Straight cable.
6. Verify the end-to-end link between computers of group A and B by pinging each other.
7. Repeat steps 4, 5 and 6 for group C and D with Switch 2 and Switch 3.

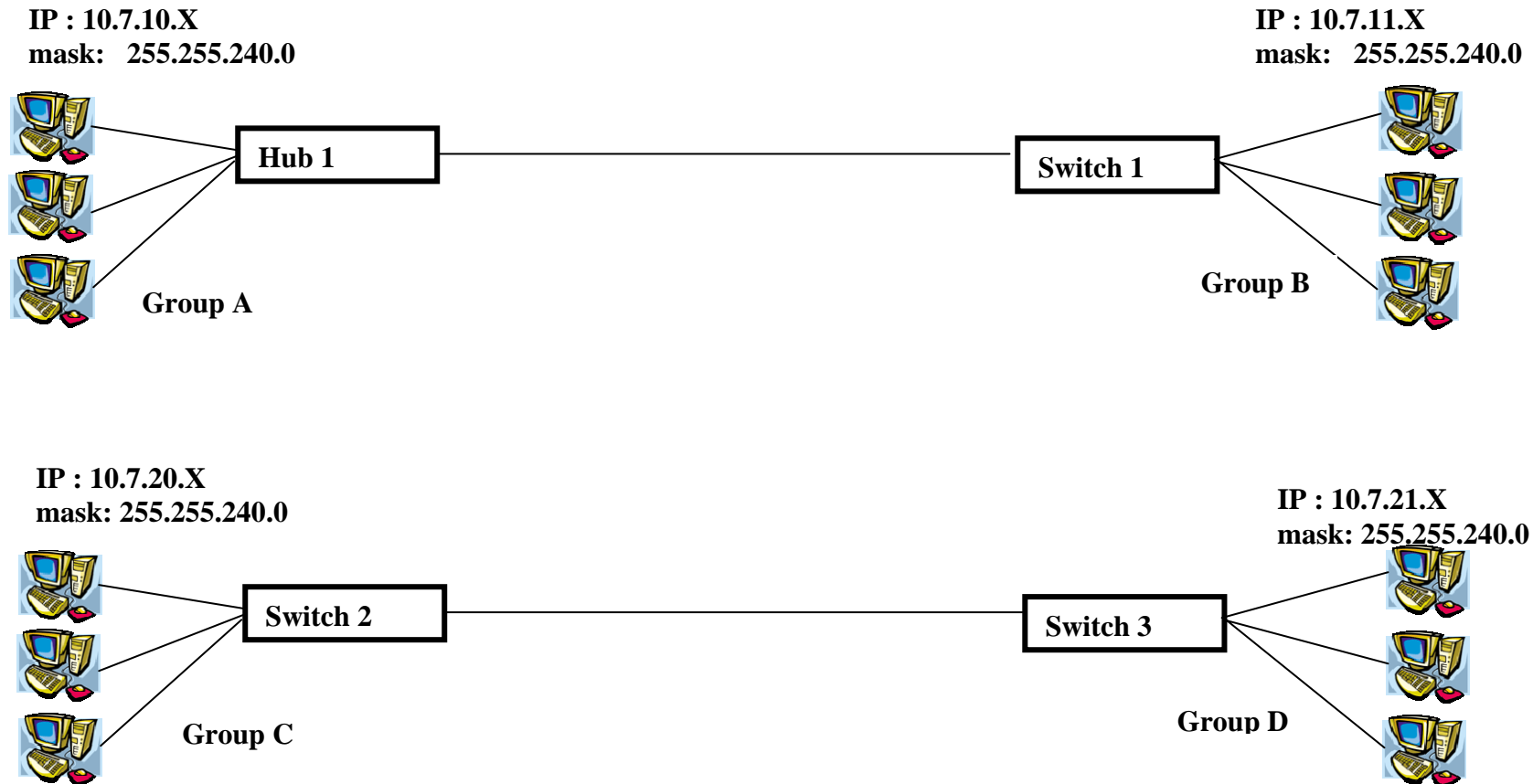
Phase 2

8. Assign IP addresses and subnet masks of the computers in each group as depicted in the figure 2.2.
9. Now interconnect group A and group C by connecting Hub1 and Switch 2 with the help of Straight cable.
10. Verify the inability of communication between computers of group A and C by pinging each other.
11. Repeat steps 8, 9 and 10 for group B and D.

Phase 3

12. Assign IP addresses and subnet masks of the computers in each group as depicted in the figure 2.3.
13. Interconnect group A and group C by connecting Hub 1 and Switch2 through Router1 interfaces FastEthernet0/0 and FastEthernet0/1 respectively.
14. Verify the end-to-end link between computers of group A and C by pinging each other.
15. Repeat steps 12, 13 and 14 for group B and D using Router2.

Figure 2.1: Phase 1



Where X = your computer number

Figure 2.2: Phase 2

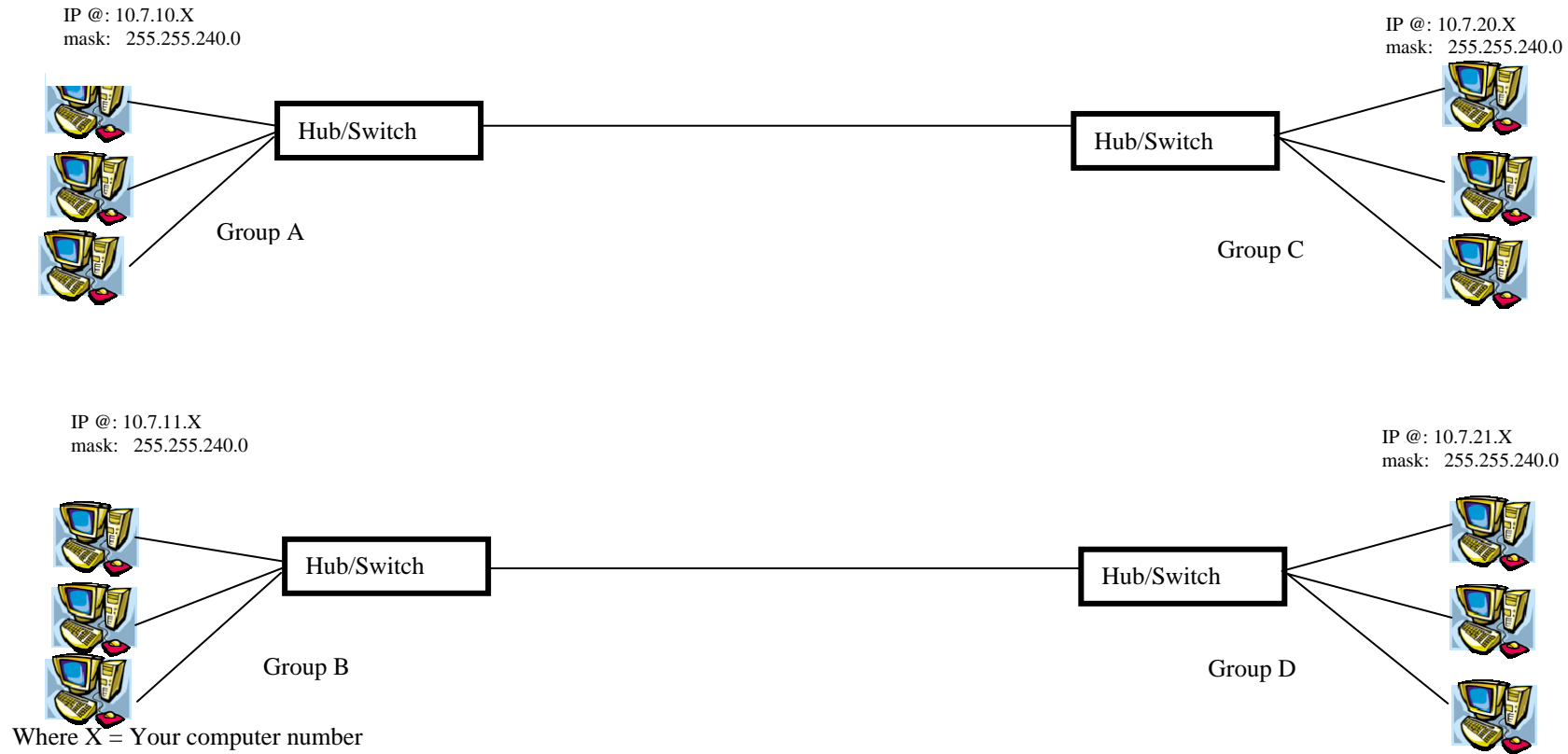
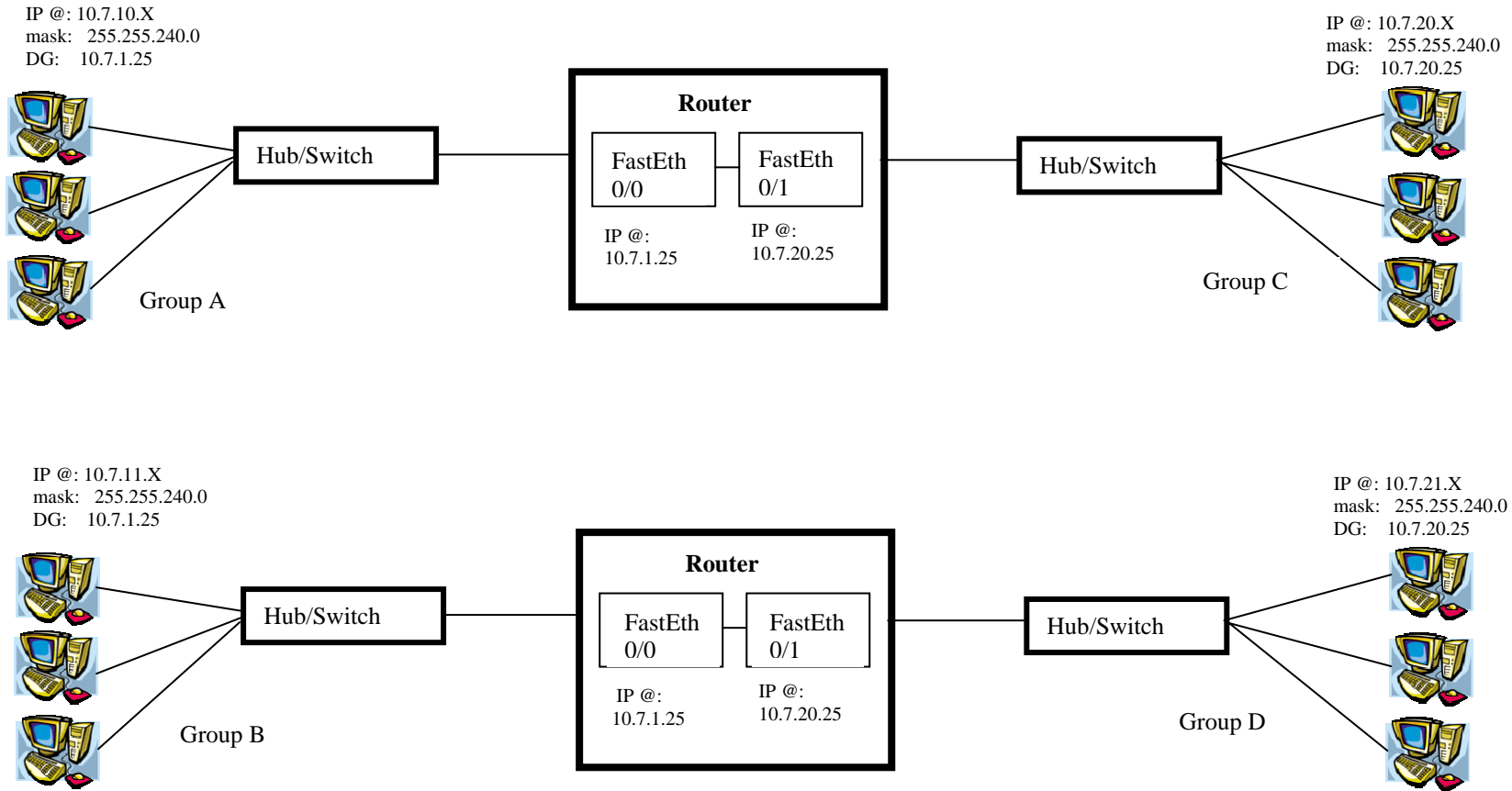


Figure 2.3: Phase 3



Where X = Your computer number

