# CONNECT DEVICES- SWITCHING

## Objective of Lesson 6:

On Completion of this lesson, the students will be able to:
Categorize different types of Connect Devices.

Explain how to work the Connect Devices.

Describe the switching methods.

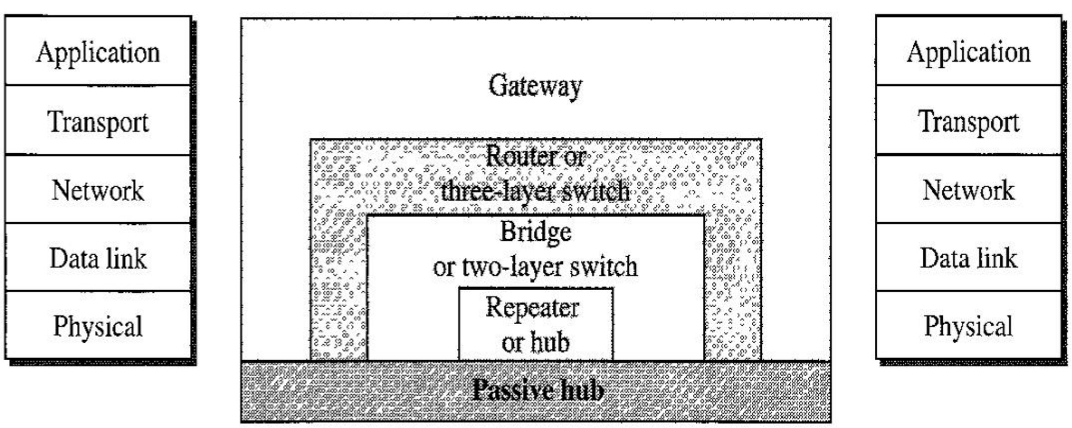
Classify the switching methods.

Explain circuit switching network, packet switching network and virtual circuit network.

## 1. Connect Devices:

LANs do not normally operate in isolation. They are connected to one another or to the Internet. To connect LANs, or segments of LANs, we use connecting devices. Connecting devices can operate in different layers of the Internet model.

The connecting devices can be divided into five different categories based on the layer in which they operate in a network, as shown in the next figure.



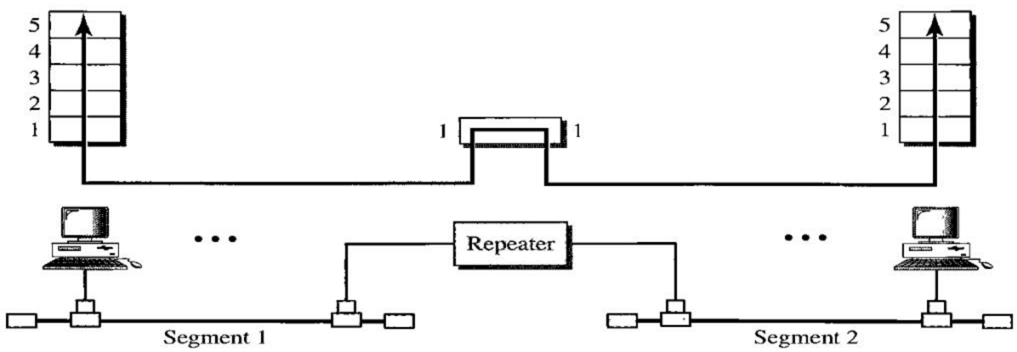

### 1.1. Passive Hubs

A passive hub is just a connector. It connects the wires coming from different branches.

## 1.2. Repeaters

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN, as shown in the following figure. We have to note:

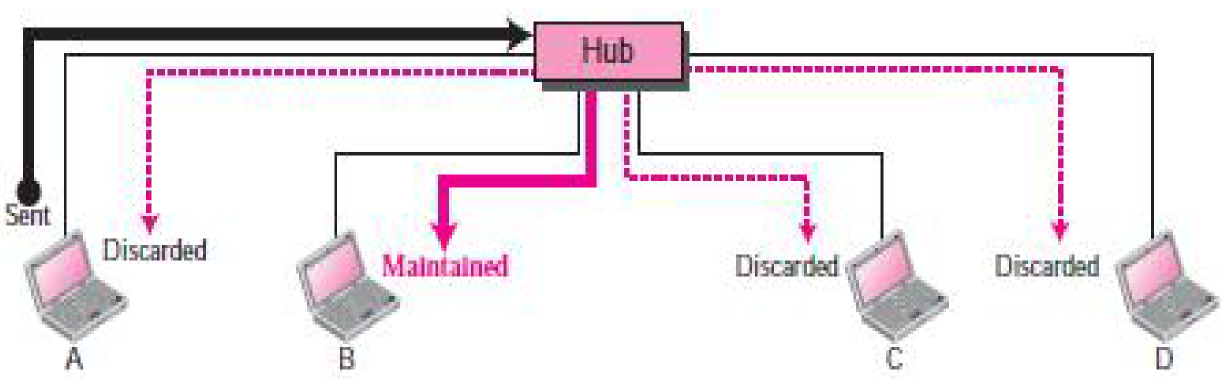
1. A repeater connects segments of a LAN (not separate LANs).




A repeater is a regenerator, not an amplifier.

A repeater forwards every bit; it has no filtering capability.

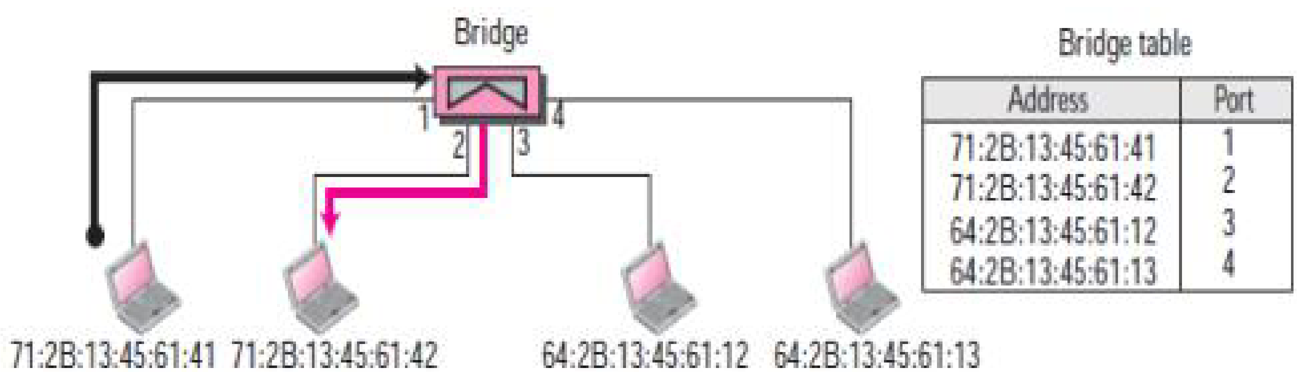
The location of a repeater on a link is vital. A repeater placed on the line before the legibility of the signal becomes lost can still read the signal well enough to determine the intended voltages and replicate them in their original form.



5. An active hub is actually a multiport repeater.

### 1.3. Bridges

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame. A bridge has a table used in filtering decisions. In the next figure, we have a LAN with four stations that are connected to a bridge. If a frame destined for station 71:2B:13:45:61:42 arrives at port 1, the bridge consults its table to find the departing port. According to its table, frames for 71:2B:13:45:61:42 should be sent out only through port 2; therefore, there is no need for forwarding the frame through other ports.




### 1.4. Two-Layer Switch

When we use the term *switch,* we must be careful because a switch can mean two different things. We must clarify the term by adding the level at which the device operates. We can have a two-layer switch or a three-layer switch. A **two-layer switch** performs at the physical and data link layer; it is a sophisticated bridge with faster forwarding capability.

### 1.5. Routers

A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the

Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.

### 1.6. Gateway

A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model.

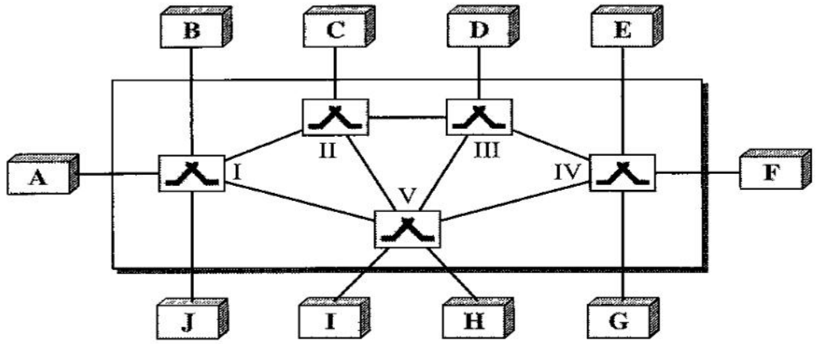
## SWITCHING

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). Drawback of these methods:

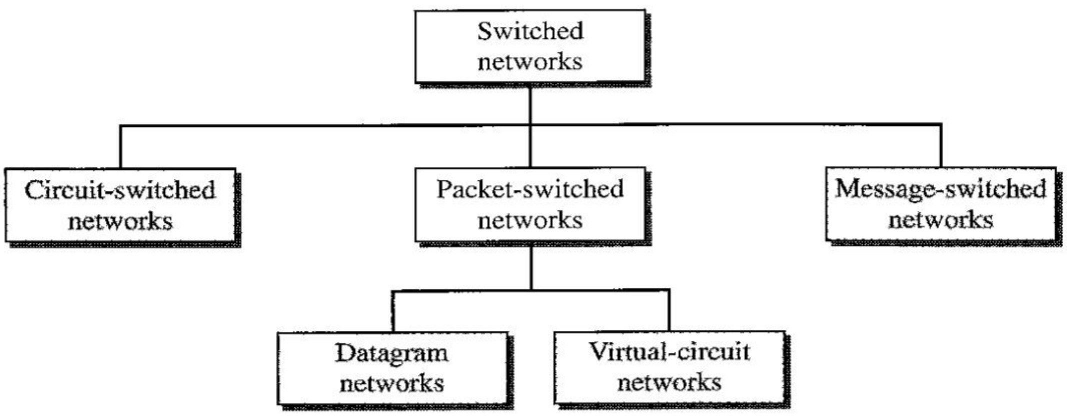
- Impractical and wasteful when applied to very large networks.
- Require too much infrastructure and then cost-efficient.
- The majority of those links would be idle most of the time.

Other topologies employing multipoint connections, such as a bus the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. See the figure:




Traditionally, three methods of switching have been important: **circuit switching**, **packet switching**, and **message switching**. The first two are commonly used today. Packet-switched networks can further be divided into two subcategories-virtual-circuit networks and datagram networks-as shown in the following figure:




## 1. Circuit-Switched Networks

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM. There are several important points in this network:

Circuit switching takes place at the physical layer. (reserving physical channel before sending the data)

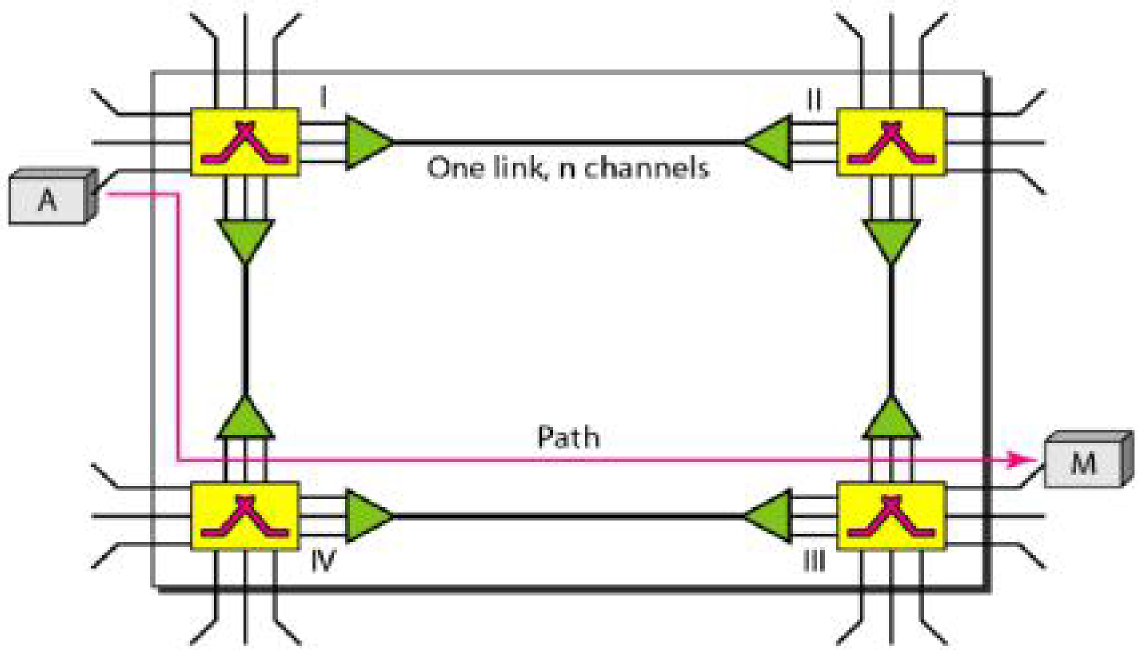
Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.

## 1.1. Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

## 1.2. Setup Phase

To understand this phase we can give one example as shown in the following figure:




System A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I.

Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV.

Switch IV finds a dedicated channel between itself and switch III.

Switch III informs system M of system A's intention at this time.

System M sends acknowledgment in the opposite direction to system A.

Only after system A receives this acknowledgment is the connection established.

### 1.3. Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

### 1.4. Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

### 1.5. Efficiency

More efficiency if it is used in telephone networks. But in the computer network not, why?

In a telephone network, people normally terminate the communication when they have finished their conversation (releasing resources). However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time (reserved resources cannot be utilized well.)

### 1.6. Delay:

The delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

Delay caused by the setup is the sum of four parts: the propagation time of the source computer request, the request signal transfer time, the propagation time of the acknowledgment from the destination computer, and the signal transfer time of the acknowledgment.

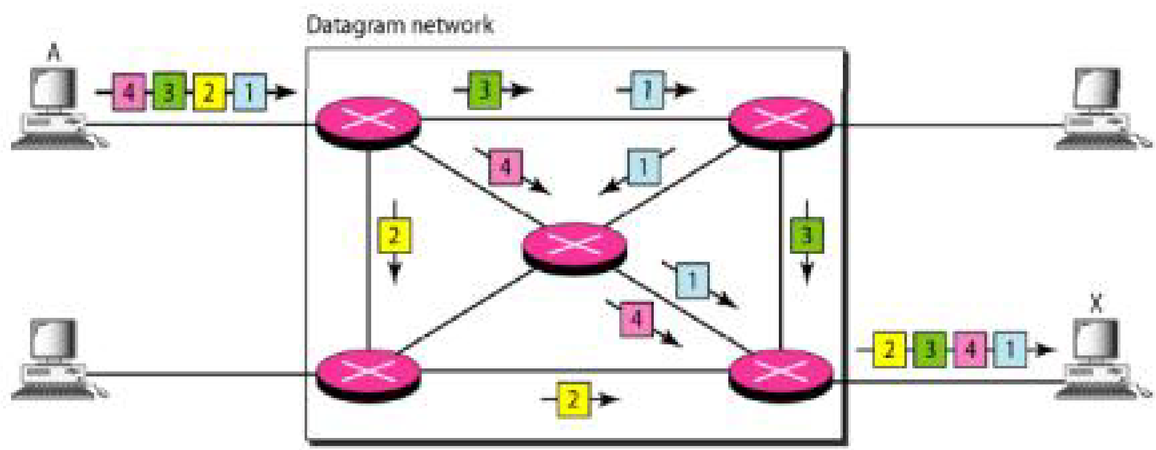
The delay due to data transfer is the sum of two parts: the propagation time and data transfer time.

The third part is the time needed to tear down the circuit.

## 2. Datagram Networks

Generally, in a packet-switched network, there is no resource reservation; resources are allocated on demand.

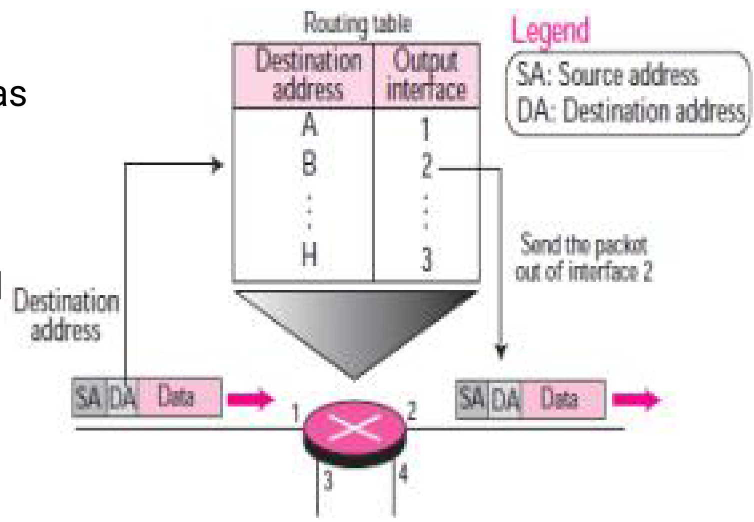
In a datagram network, each packet is treated independently of all others. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer (no reservation, we need address during the data transfer). The following figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers.




We can note that all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. The datagram networks are sometimes referred to as connectionless networks. There are no setup or teardown phases.

### 2.1. Routing Table

If there are no setup or teardown phases, how are the packets routed to their destination in a datagrams network? In this type of network, each switch (or packet switch) has a routing table which is based on the **destination address**. The routing tables are **dynamic** and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit-switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over.




## 2.2. Destination Address

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is used to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual-circuit-switched network, remains the same during the entire journey of the packet.

## 2.3. Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.

## 2.4. Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message. The total delay can be given by:

Total delay = $3T + 3\tau + w_1 + w_2$

### 3. Virtual-Circuit Networks

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- As in a circuit-switched network, all packets follow the same path established during the connection.
- As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local authority (it defines what should be the next switch and the channel on which the packet is being carried), not end-to-end authority.

#### 3.1. Addressing

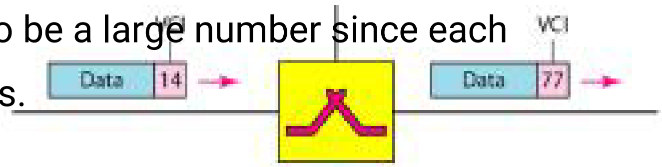
In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

##### 3.1.1. Global Addressing

A source or a destination needs to have a global address. The address can be unique in the scope of the network or internationally if the network is part of an international network. However, the global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

##### 3.1.2. Virtual- Circuit Identifier

The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI. The figure shows how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCIs.



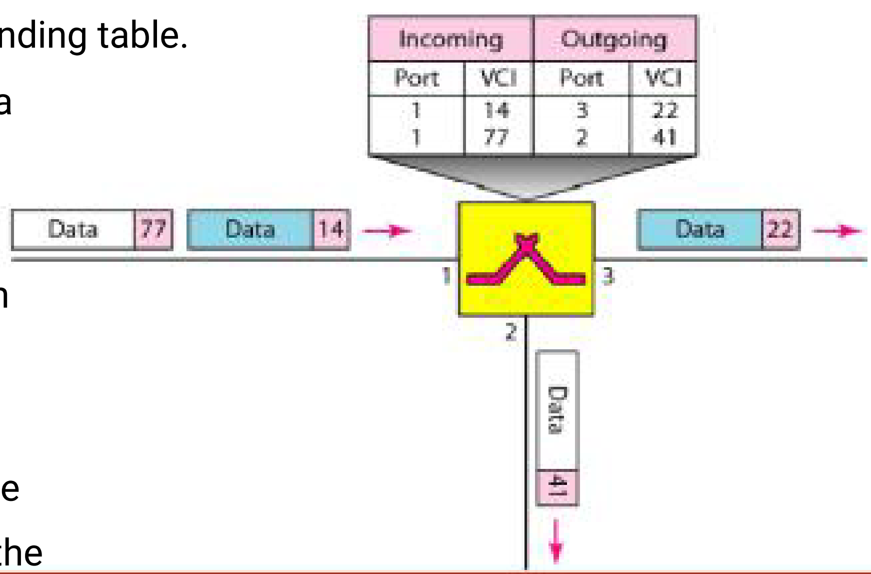

## 3.2. Three Phases

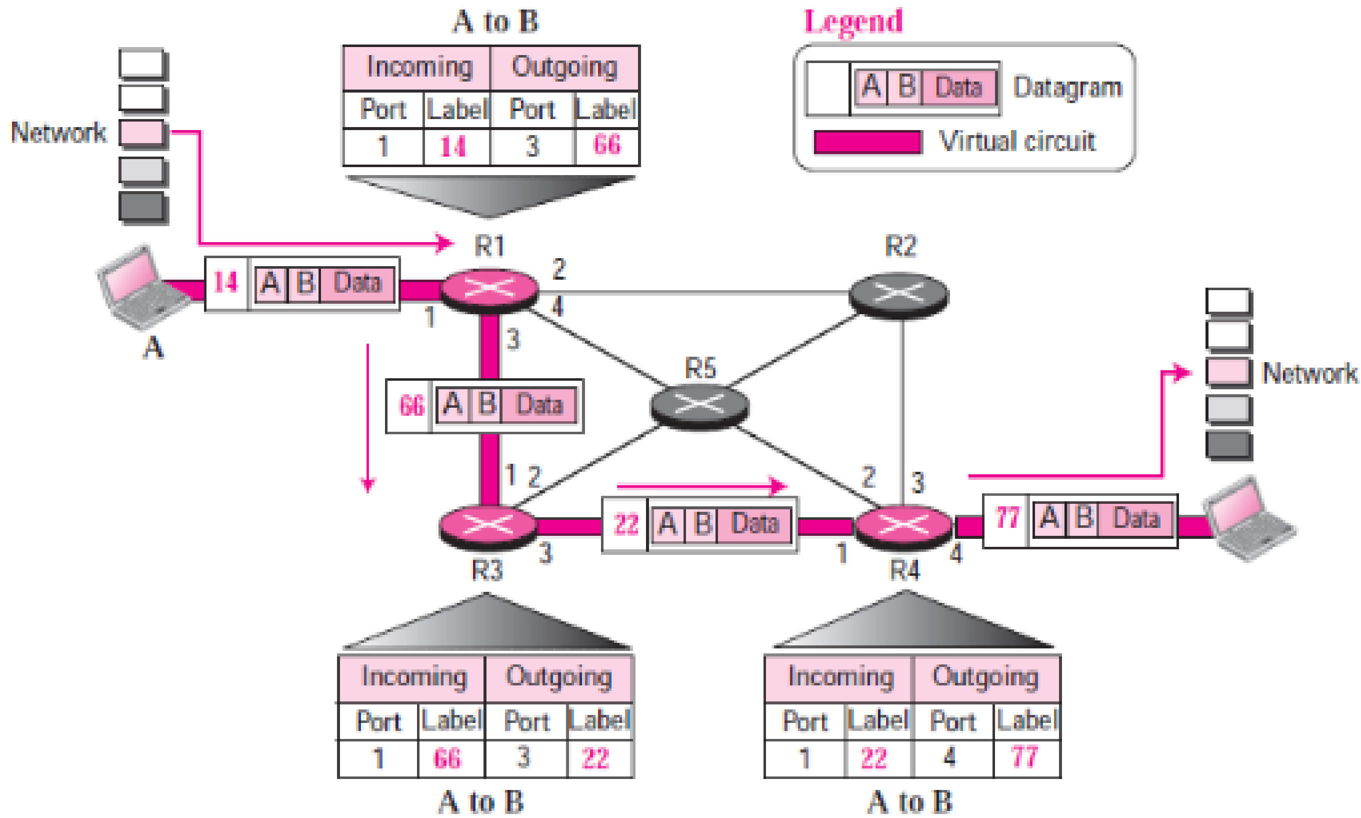
As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry.

### 3.2.1. Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. The following figure shows such a switch and its corresponding table.

The next figure shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame. The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message.






### 3.2.2. Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the **setup request** and the **acknowledgment**.

**Setup Request:** setup request frame is sent from the source to the destination. The next figure shows the process.

Source A sends a setup frame to R1.

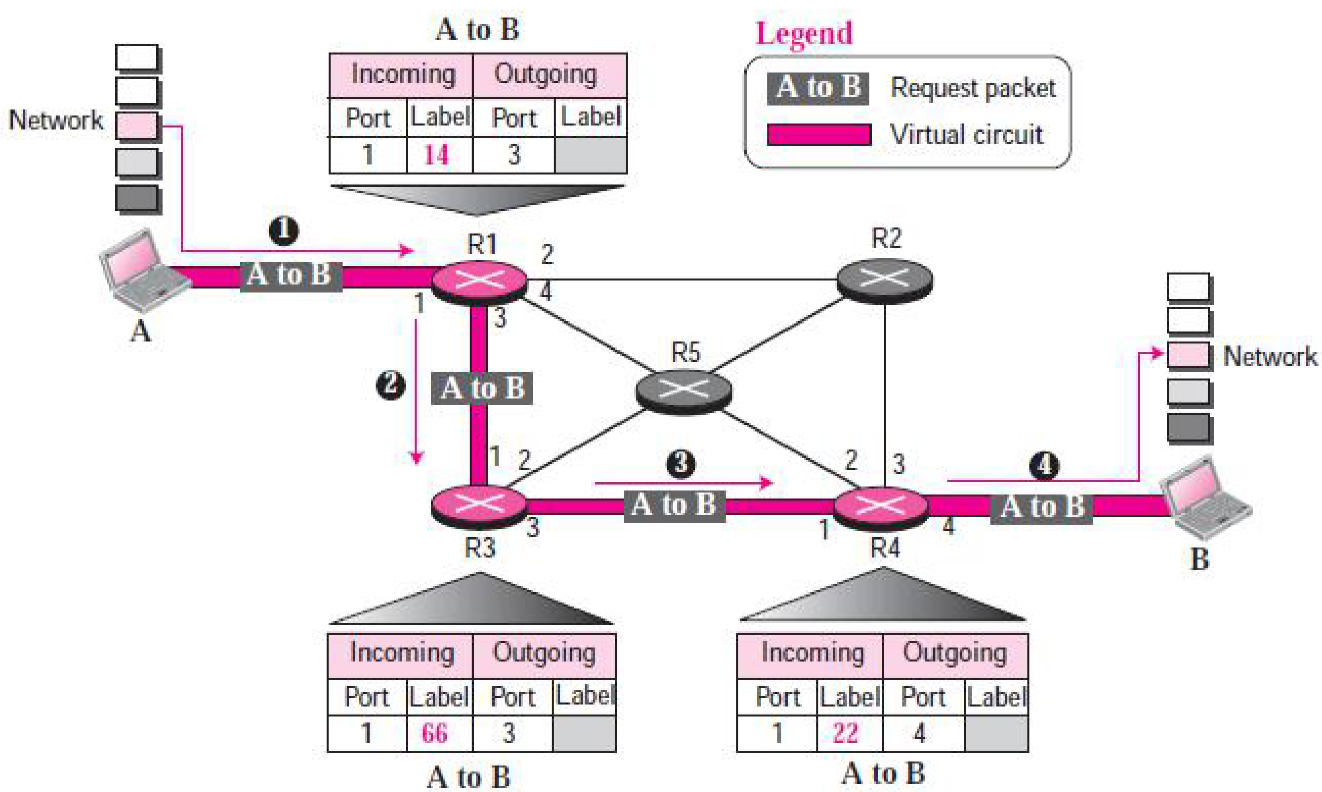
R1 receives the setup request frame. It knows that a frame going from A to B goes out through **port 3**. The switch, in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming **port (1)** and chooses an

available incoming **VCI (14)** and the outgoing **port (3)**. It does not yet know the outgoing **VCI**, which will be found during the acknowledgment step. The switch then forwards the frame through **port 3** to **R2**.

**R3** receives the setup request frame. The same events happen here as at **R1**; three columns of the table are completed: in this case, incoming **port (1)**, incoming **VCI (66)**, and outgoing **port (3)**.

**R4** receives the setup request frame. Again, three columns are completed: incoming **port (1)**, incoming **VCI (22)**, and outgoing **port (4)**.

Destination **B** receives the setup frame, and if it is ready to receive frames from **A**, it assigns a **VCI** to the incoming frames that come from **A**, in this case 77. This **VCI** lets the destination know that the frames come from **A**, and no other sources.



Acknowledgment: A special frame, called the acknowledgment frame, completes the entries in the switching tables. The next figure shows the process.

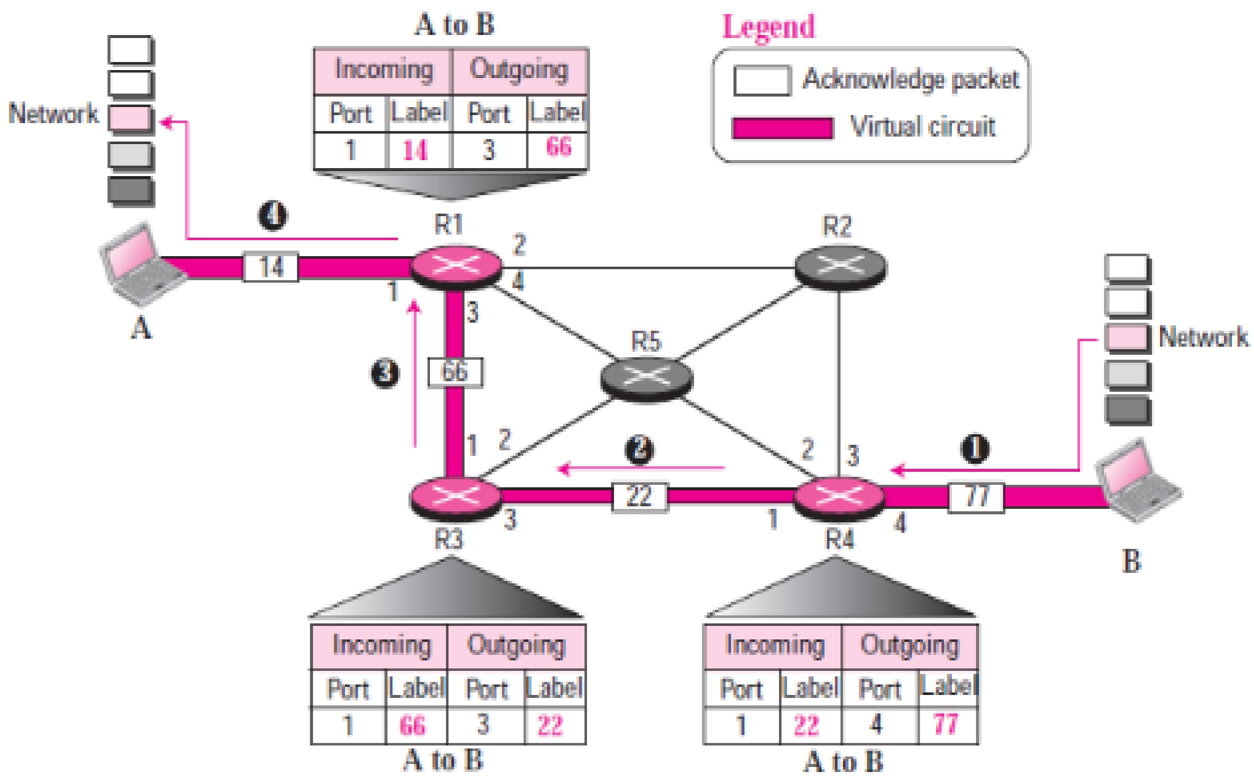
The destination sends an acknowledgment to R4. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. R4 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for R4.

R4 sends an acknowledgment to R3 that contains its incoming VCI in the table, chosen in the previous step. R3 uses this as the outgoing VCI in the table.

R3 sends an acknowledgment to R1 that contains its incoming VCI in the table, chosen in the previous step. R1 uses this as the outgoing VCI in the table.

Finally R1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

10. The source uses this as the outgoing VCI for the data frames to be sent to destination B.




### 3.2.3. Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

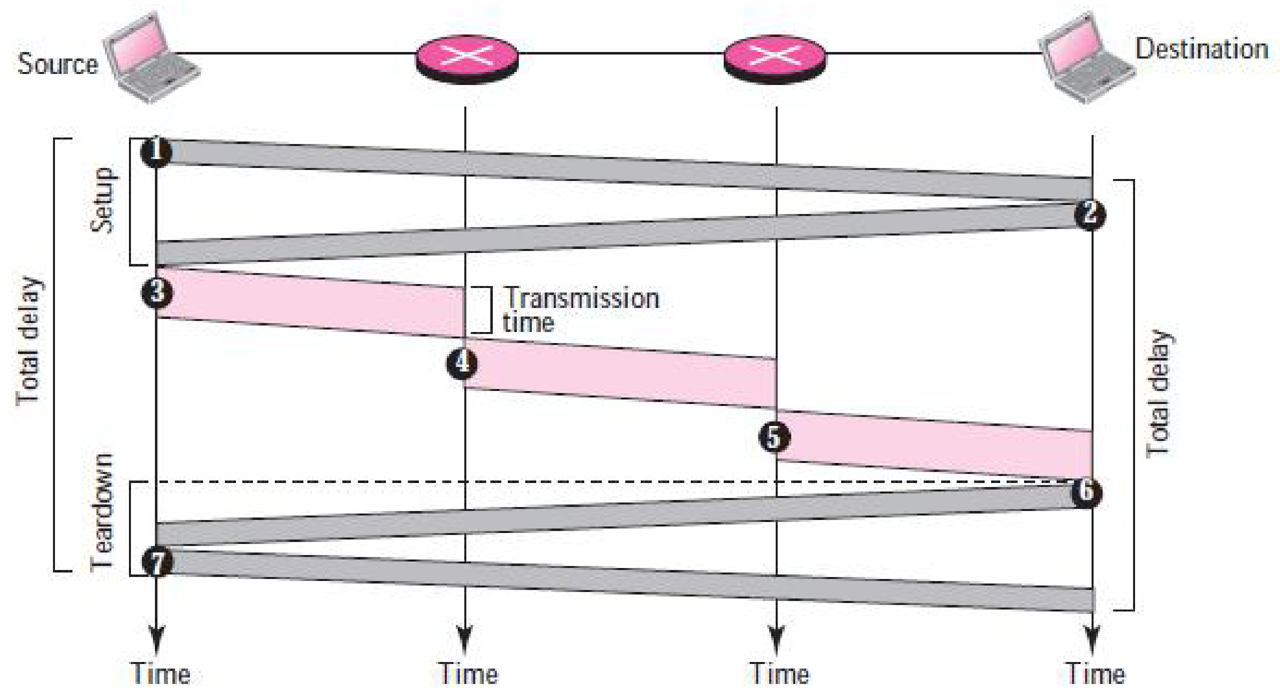
## 3.3. Efficiency

As mentioned earlier, resource reservation in a virtual-circuit network can be made during the setup or can be on-demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it.

### 3.4. Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. The total delay time is given by:

$$\text{Total delay} = 3T + 3\tau + \text{setup delay} + \text{teardown delay}$$




### 4. Performance Measurement:

One important issue in networking is the performance of the network-how good is it?

4.1. **Bandwidth**: One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second.

4.2. **Throughput**: it is a measure of how fast we can actually send data through a network. A link may have a bandwidth of B bps, but we can only send T bps

through this link with T always less than B. In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

4.3. Latency (Delay): The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time(=distance/propagation speed), transmission time (=data size/bandwidth), queuing time and processing delay.