جامعة الحمدانية
كلية التربية
قسم علوم الحاسوب

Networking Devices

المرحلة الرابعة
د.م.نورس يونس السليم
المحاضرة الثامنة

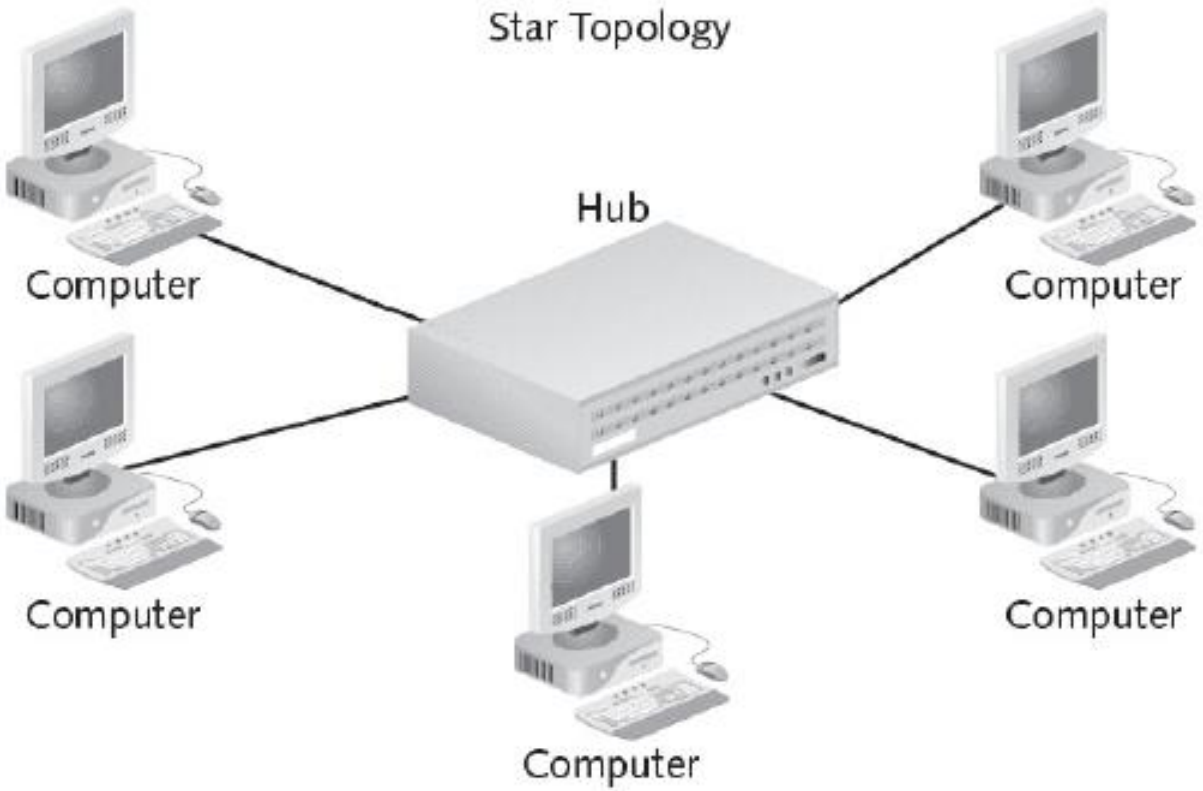
Networking Devices

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and requirements for a Network.

Hubs

At the bottom of the networking food chain, so to speak, are hubs. Hubs are used in networks that use twisted-pair cabling to connect devices. Hubs can also be joined together to create larger networks. *Hubs* are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device.

Hubs


Star Topology
Hub
Computer
Computer
Computer
Computer
Computer

- There is two type of hub

1.The ***passive hub*** does nothing except provide a pathway for the electrical signals to travel along.

2.The ***active*** **hub** providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices.

- A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes:

- Small hubs with five or eight connection ports are commonly referred to as *workgroup hubs*.

- Others can accommodate larger numbers of devices (normally up to 32). These are referred to as *high-density devices*.

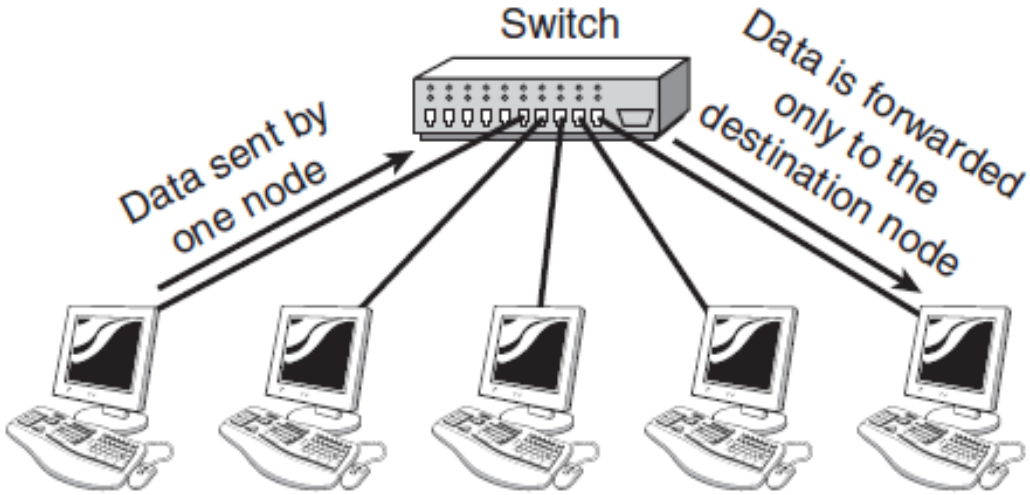
Switches

Switches are the connectivity points of an Ethernet network.

Devices connect to switches via twisted-pair cabling, one cable for each device.

The difference between hubs and switches is in how the devices deal with the data that they receive. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device.

It does this by *learning* the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives.



By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode.

The method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:

➤ **Cut-through**—In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast, but creates the possibility of errors being propagated through the network, as there is no error checking.

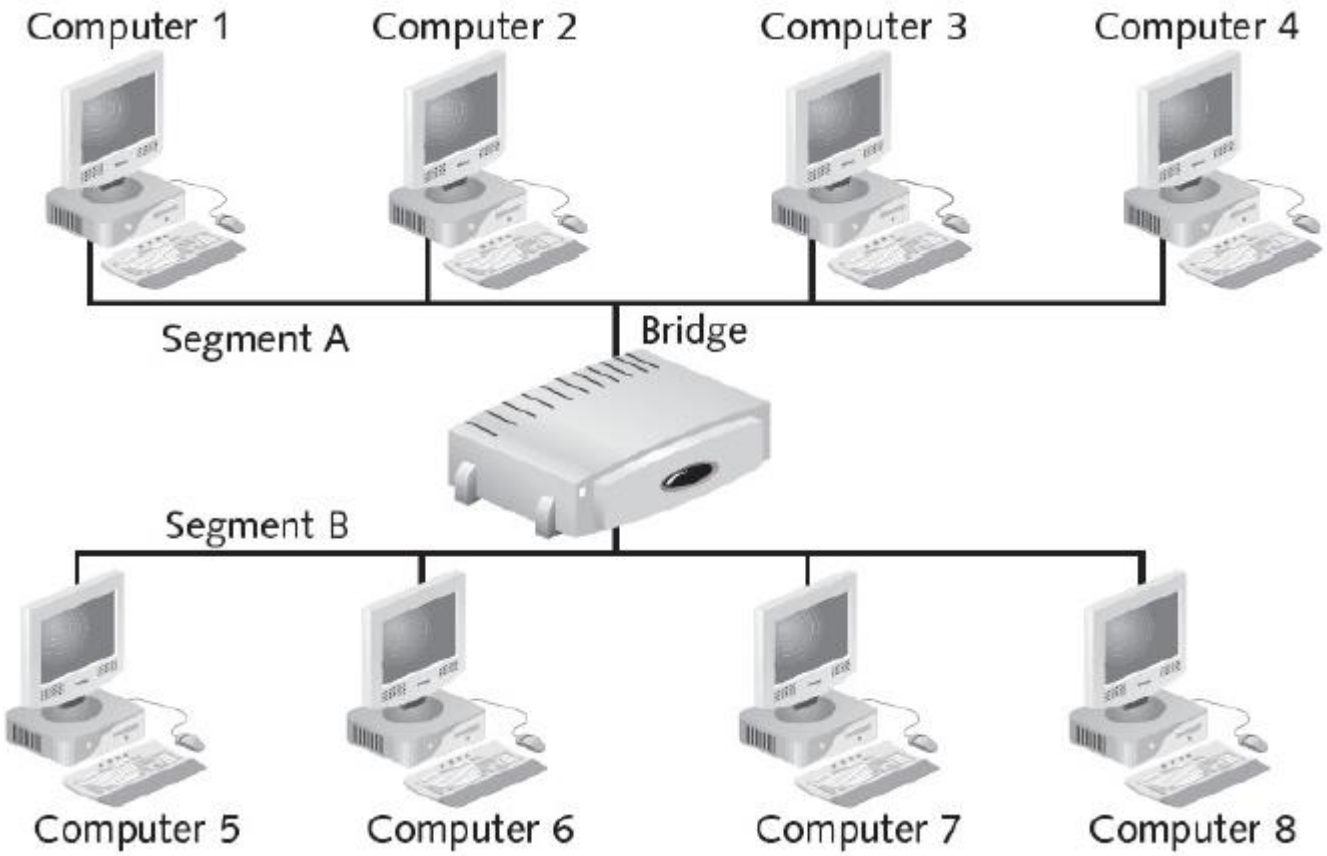
➤ **Store-and-forward**—Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.

Bridges

Bridges are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came).

When bridges were introduced, the MAC addresses of the devices on the connected networks had to be entered manually, a time-consuming process that had plenty of opportunity for error. Today, almost all bridges can build a list of the MAC addresses on an interface by watching the traffic on the network.

Such devices are called *learning bridges* because of this functionality.


Computer 1
Computer 2
Computer 3
Computer 4
Segment A
Bridge
Segment B
Computer 5
Computer 6
Computer 7
Computer 8

Bridge Placement and Bridging Loops

There are two issues that you must consider when using bridges. The first is the bridge placement, and the other is the elimination of bridging loops:

➤ **Placement**—Bridges should be positioned in the network using the 80/20 rule. This rule dictates that 80% of the data should be local and that the other 20% should be destined for devices on the other side of the bridge.

➤ **Bridging loops**—Bridging loops can occur when more than one bridge is implemented on the network. In this scenario, the bridges can confuse e each other by leading one another to believe that a device is located on a certain segment when it is not. To combat the bridging loop problem, the IEEE 802.1d Spanning Tree protocol enables bridge interfaces to be assigned a value that is then used to control the bridge-learning process.

Types of Bridges

Three types of bridges are used in networks:

1.**Transparent bridge.**

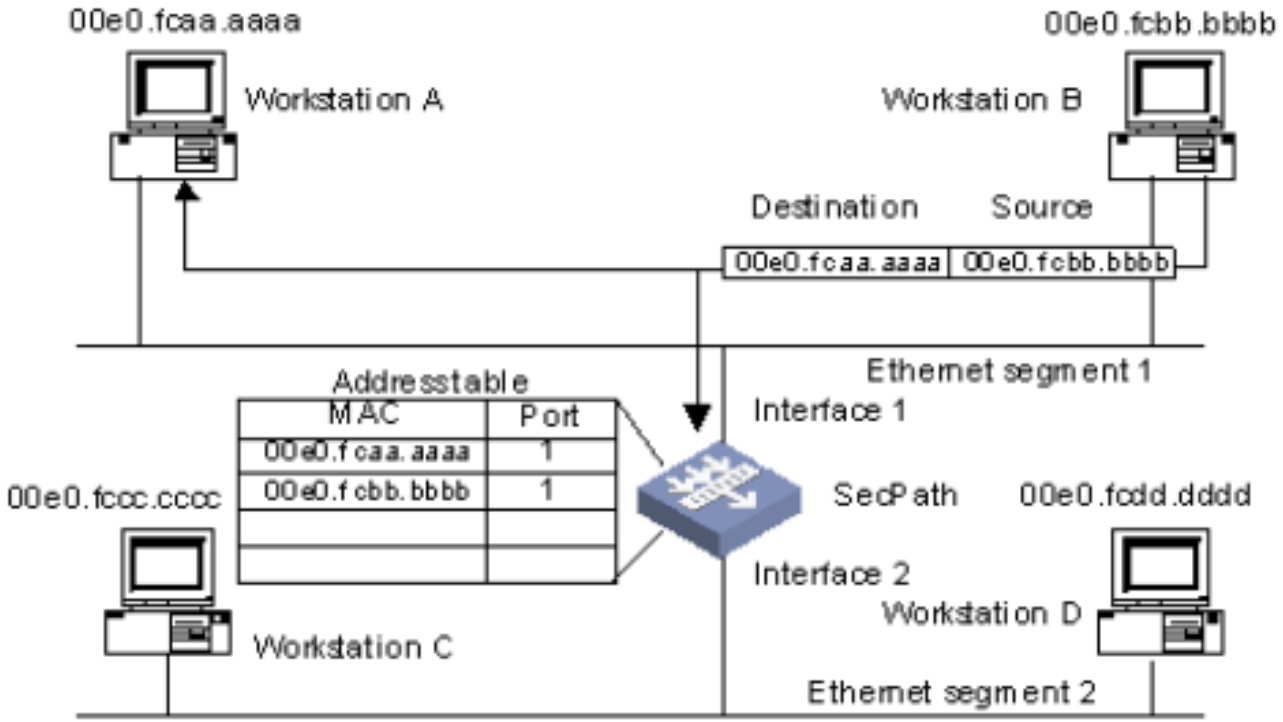
2. **Source route bridge.**

3.**Translational bridge**.

Transparent Bridges

Transparent bridge—Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.

- Also called learning bridges Because they build a table of MAC addresses as they receive frames. They “learn” which addresses are on which segments
- The bridge uses the source MAC addresses to determine which addresses are on which segments.



Transparent Bridges

Source-Routing Bridges

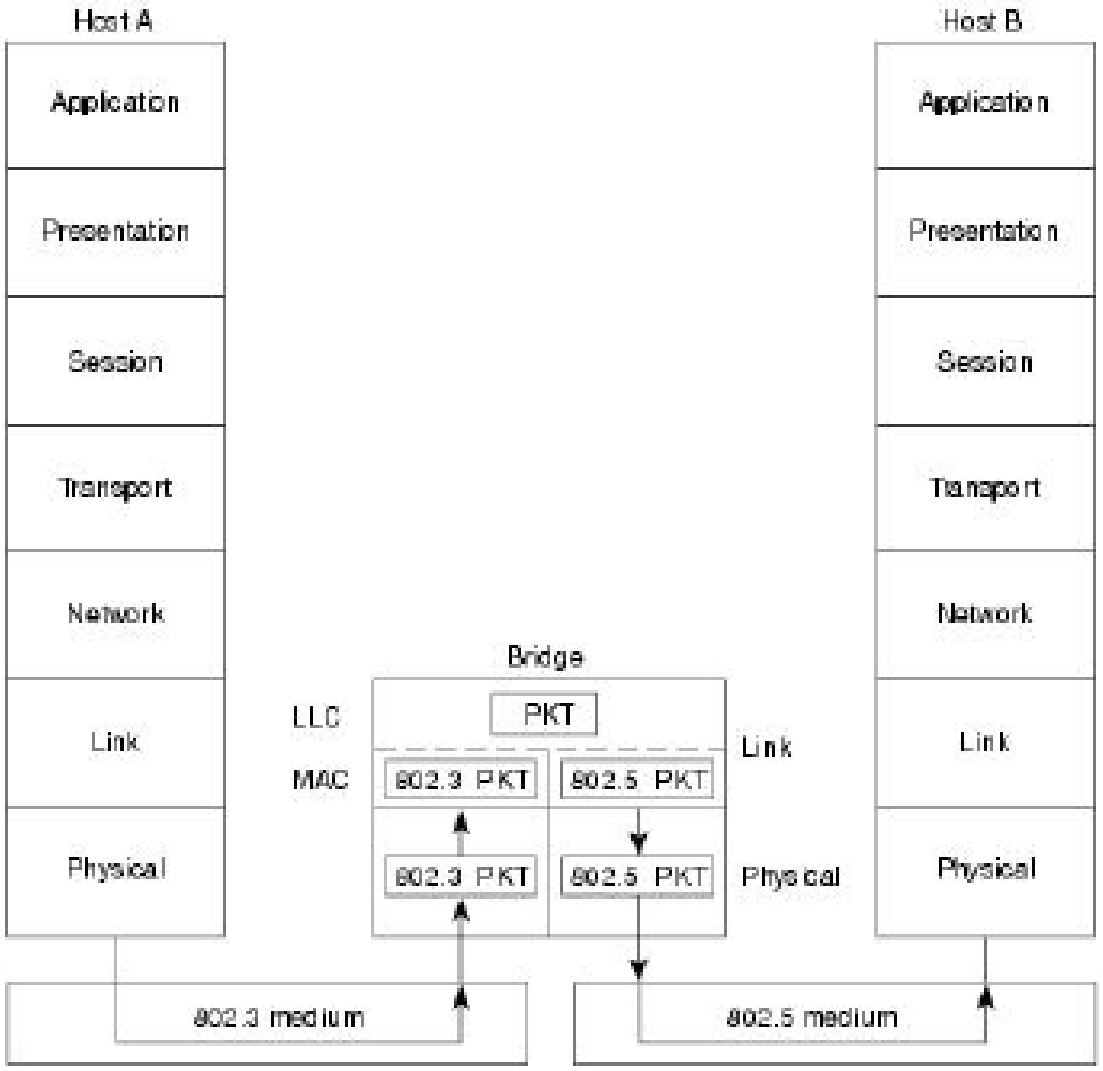
- Rely on the source of the frame transmission to provide the routing information The source computer determines the best path by sending out explorer frames.
- The source includes the routing information returned by its ***explorer frames*** in the frame sent across the network
- The bridge uses this information to build its table

Translation Bridges

- Can connect networks with different architectures, such as Ethernet and Token Ring
- These bridges appear as:

1.Transparent bridges to an Ethernet host

2.Source-routing bridges to a Token Ring host


Host A
Application
Presentation
Session
Transport
Network
Link
Physical
Host B
Application
Presentation
Session
Transport
Network
Link
Physical
Bridge
LLC
MAC
PKT
Link
802.3 PKT
802.5 PKT
802.3 PKT
802.5 PKT
Physical
802.3 medium
802.5 medium

Advantages and Disadvantages of Bridges

Advantages

1.Can extend a network by acting as a repeater

2.Can reduce network traffic on a segment by subdividing network communications.

3. Increase the available bandwidth to individual nodes.

because fewer nodes share a collision domain.

4. Reduce collisions.

5.Some bridges connect networks using different media types and architectures.

Disadvantages

1. Slower than repeaters and hubs.
2. Extra processing by viewing MAC addresses.
3. More expensive than repeaters and hubs.

Routers

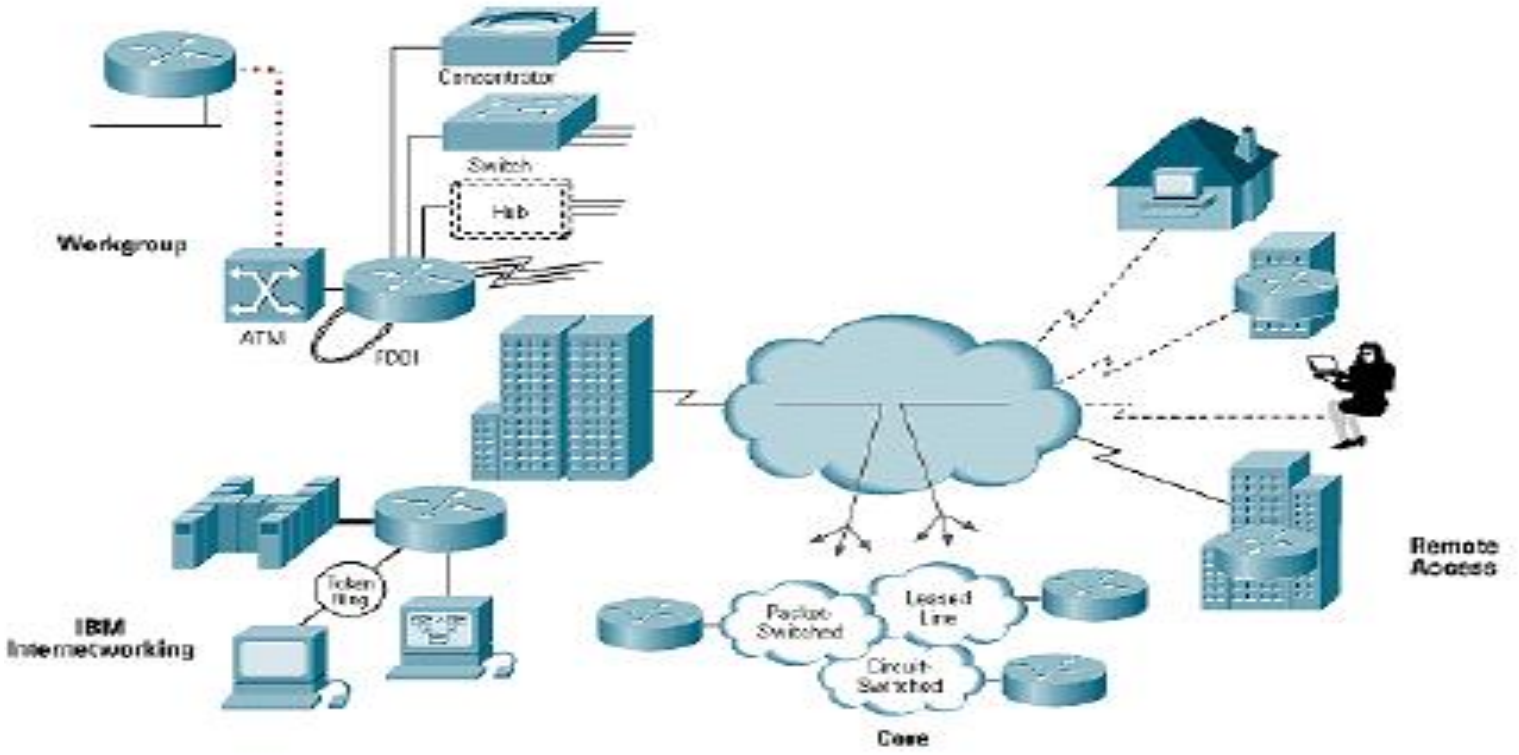
routers are used to create larger networks by joining two network segments. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software. All modern network operating systems include the functionality to act as a router.

– Operate at the Network layer of the OSI model

– Provide filtering and network traffic control on LANs and WANs.

– Can connect multiple segments and multiple networks.

- **Internetworks:** Networks connected by multiple routers.
- Similar to switches and bridges in that they segment a network and filter traffic
- Routers use the logical address



How work router

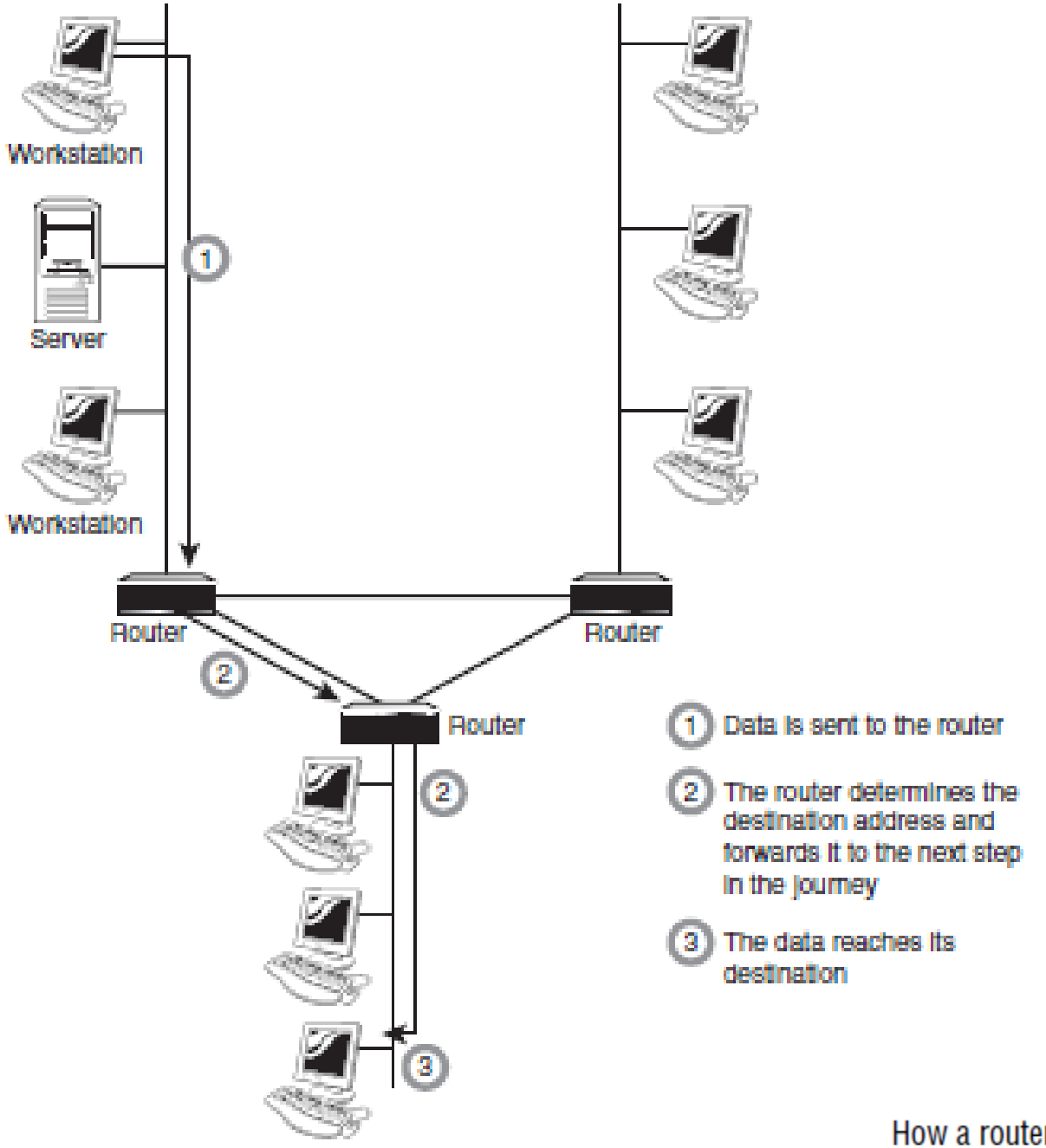
- A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its ***routing table*** to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router.

- There are two ways that the router can get the information for the routing table through ***static routing*** or ***dynamic*** routing.

1-**Static Routing**

In environments that use *static routing*, routes and route information are entered into the routing tables manually.

when there is a change in the layout, or topology, of the network, statically configured routers must be manually updated with the changes.



How a router works.

2.Dynamic Routing

In a *dynamic routing* environment, routers use special routing protocols to communicate. The purpose of these protocols is simple; they enable routers to pass on information about themselves to other routers so that other routers can build routing tables.