

Topic 04 Network Devices

RECAP SUMMARY



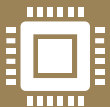
Network Repeaters and Hubs



A repeater receives bit signals generated by NICs and other devices, strengthens them, and then “repeats” them to other parts of the network



A repeater enables you to connect computers whose distance from one another would make communication impossible



A traditional repeater has two ports or connections that you can use to extend your network

Multiport Repeaters and Hubs



Referred as **Hub**



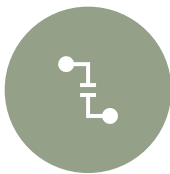
Receives bit signals generated from a connected computer's NIC on one of its ports



Cleans the signal by filtering out electrical noise



Regenerates the signal to full strength



Transmits the regenerated signal to all other ports where a computer (or other network device) is connected to

Hub



Hub

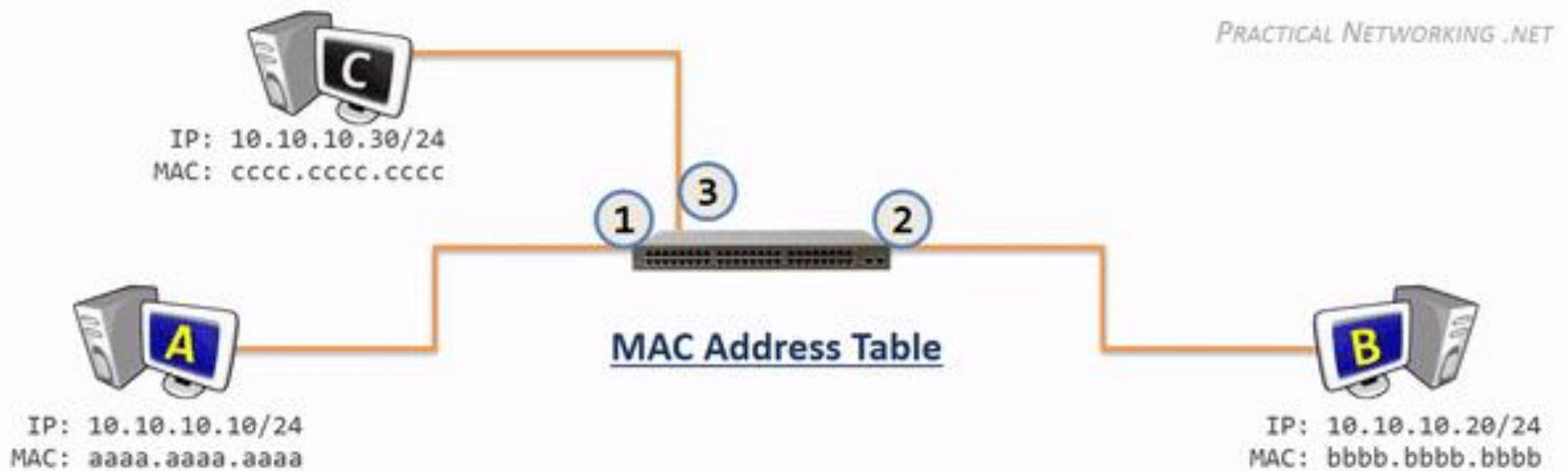
In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times

Network Switches

Looks just like a **hub**

- But a switch actually reads data in the message, determines which port the destination device is connected to, and forward the message to only that port
- Basic Switch Operation
 - Data is sent onto the medium one frame at a time
 - Each frame has the destination and source MAC addresses
 - Switch reads the addresses:
 - Use the source MAC address of frame to keep a record of which computer is on which port (switching table)
 - Forwards the frame to the port where the destination MAC can be found

How Network Switch Works



Steps of switch operation

1. The switch receives a frame.
2. The switch reads the source and destination MAC addresses.
3. The switch looks up the destination MAC address in its switching table.
4. The switch forwards the frame to the port where the computer owning the MAC address is found.
5. The switching table is updated with the source MAC address and port information.

Steps of switch operation

1. The switch receives a frame.
2. The switch reads the source and destination MAC addresses.
3. The switch looks up the destination MAC address in its switching table.
4. The switch forwards the frame to the port where the computer owning the MAC address is found.
5. The switching table is updated with the source MAC address and port information.

Switches and Network Bandwidth

Each port gets **dedicated bandwidth**

- Instead of having to share bandwidth with all ports

Multiple conversations can occur simultaneously

Can operate in **full-duplex mode** (hub only provides half-duplex mode)

- Can send and receive data simultaneously

Switches are the preferred device because of these advantages

Switch



Switches and Network Bandwidth

A switch, keeps a record of the MAC (Media Access Control) addresses of all the devices connected to it. With this information, a switch can identify which system is sitting on which port. So when a frame is received, it knows exactly which port to send it to, without significantly increasing network response times. In addition, unlike a hub, a 10/100Mbps switch will allocate a full 10/100Mbps to each of its ports. So regardless of the number of PCs transmitting, users will always have access to the maximum amount of bandwidth. It's for these reasons a switch is considered to be a much better choice than a hub.

Wireless Access Points



The heart of a wireless network is the wireless access point (AP)



APs operate similarly to a hub without wires



All communication passes through the AP



Most small business and home networks use a device typically called a wireless router that combines the functions of an AP, a switch, and a router



Wireless LANs are usually attached to wired networks

Network Interface Card (NIC)

The tasks a NIC and its driver perform:

- Provide a connection from computer to medium
- Incoming messages: Receives bit signals and assembles them into frames
 - Verifies the destination address
 - Removes frame header and sends the resulting packet to the network protocol
- Outgoing messages: receive packets from network protocol
 - Creates frames by adding MAC addresses/error check
- Converts frame into bit signals suitable for the medium and transmits them

NICs and MAC address

NIC manufacturers ensure that every NIC produced has a unique address

- Networks won't function correctly if duplicate MAC addresses exist

MAC address is stored in read-only memory (ROM) on the NIC

Two 24-bit hexadecimal numbers

- 24-bit manufacturer ID called **OUI**
- 24-bit serial number **assigned by the manufacturer**

48-bit address expressed in 12 hexadecimal digits:

- **04-40-31-5B-1A-C4**

NIC as Gatekeeper

When a frame arrives at a NIC, the NIC checks the frame's destination MAC address to see whether it matches its built-in MAC address

NIC only permits inbound communications if the destination MAC:

- Matches the NIC's burned-in address
- Is a broadcast address (ff-ff-ff-ff-ff-ff)
- NIC is in a special mode called promiscuous

When the destination MAC address matches the MAC burned-in address (BIA), or the physical address of a NIC, it's a unicast frame

- Intended for a single computer

NIC as Gatekeeper

When the destination is the broadcast address, it's a **broadcast frame**

- Broadcast frames are intended to be processed by all computers on the network

Promiscuous mode – turns off the gatekeeper functions and enables the NIC to process all frames it sees

- Used by software called a protocol analyzer or packet sniffer

Wireless NICs

Wireless NICs must be chosen according to type of wireless AP being used

Typical are Wireless-n, 802.11ac or 802.11 a/b/g/n

- The letter a,b,g, n, and ac refer to the wireless networking standard the device supports

Wireless NICs connect to network using service set identifier (SSID)

- SSID is the name assigned to the wireless network

You may also need to enter a security key or a username and password, depending on the network's security configuration

Routers

Most complex device

Connect LANs together to create an internetwork (Network of Networks)

Routers are devices that **enable multiple LANs to communicate with one another** by **forwarding packets** from one LAN to another

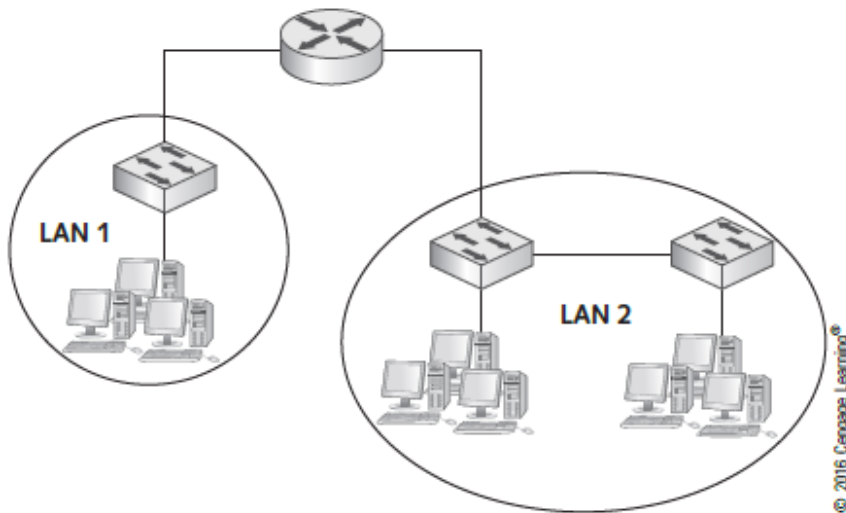


Figure 2-15 Two LANs connected by a router to make an internetwork

Differences between routers and switches

Routers connect LANs, switches connect computers to form LANs

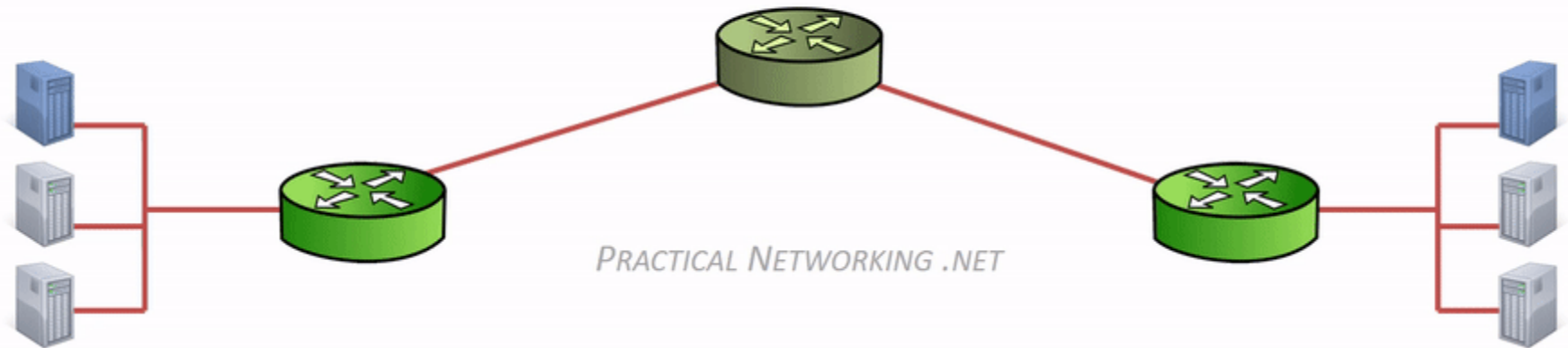
Routers work with logical (IP) addresses, switches work with physical (MAC) addresses

Routers work with packets, switches with frames

Routers don't forward broadcasts, switches do

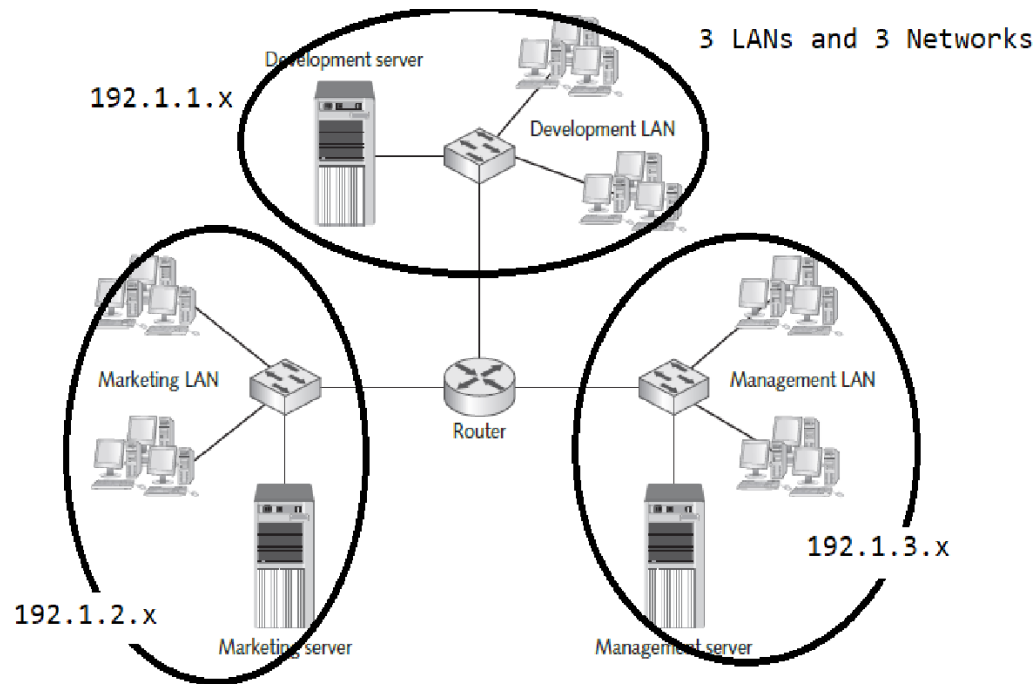
Routers use routing tables, switches use switching tables

How routers forward packet



Notice between each Router, the MAC address header is stripped and regenerated to get it to the next hop. The IP header generated by the first computer is only stripped off by the final computer, hence the **IP header handled the “end to end” delivery**, and each of the **four different MAC headers** involved in this animation **handled the “hop to hop” delivery**.

Routers Connect LAN

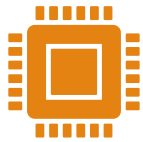


The router is used to **connect 3 separate LANs** in order to contain broadcast traffic and facilitate more effective communication in each department LAN

Difference between Hub, Switch and Router



Routers Work with IP Addresses and Routing Tables



Default route

Where to send a packet when the router doesn't have an entry in its routing table



Network unreachable

Message sent when the network can't be found and no default route



Default gateway

In a computer's IP address configuration – the IP address of the computer's router