Guide to Networking Essentials, 6th Edition

Chapter 7: Network Hardware in Depth

Objectives

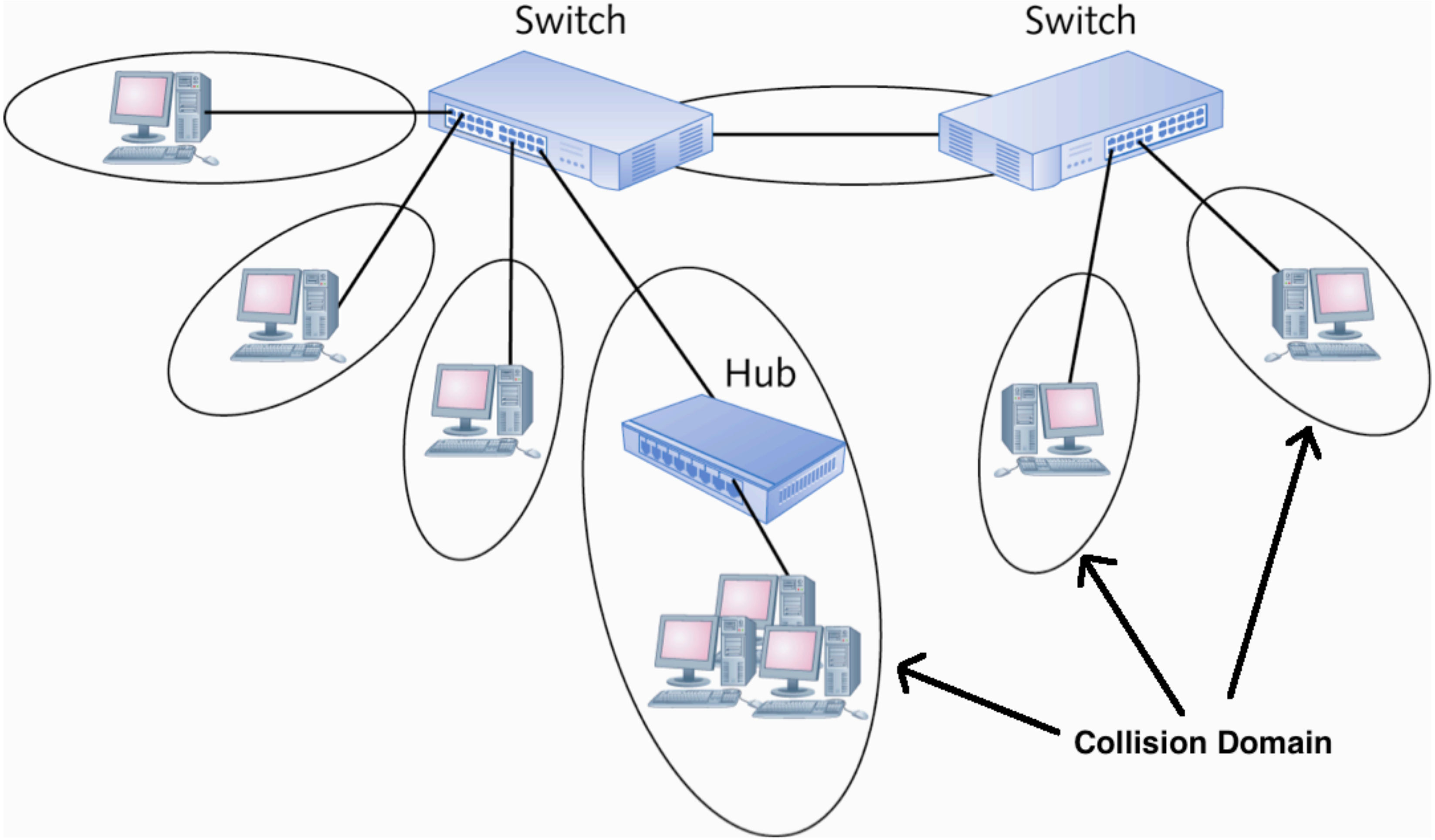
- Describe the advanced features and operation of network switches
- Describe routing table properties and discuss routing protocols
- Explain basic and advanced wireless access point features
- Select the most suitable NIC bus and features for a computer

Network Switches in Depth

Data Link Layer (2)
SLIP, PPP
802.2 SNAP
Ethernet II

- Switches work at the Data Link layer (Layer 2)
  - Receive frames on one port and forward them out the port where the destination device can be found
- Switches send broadcast frames out all ports
- Each switch port is considered a collision domain (see figure on next slide)
  - Switches do not forward collision information to any other ports
- Switch ports can operate in full-duplex mode
  - Allows connected devices to transmit and receive simultaneously, eliminating the possibility of a collision

Network Switches in Depth



Each switch port is a collision domain

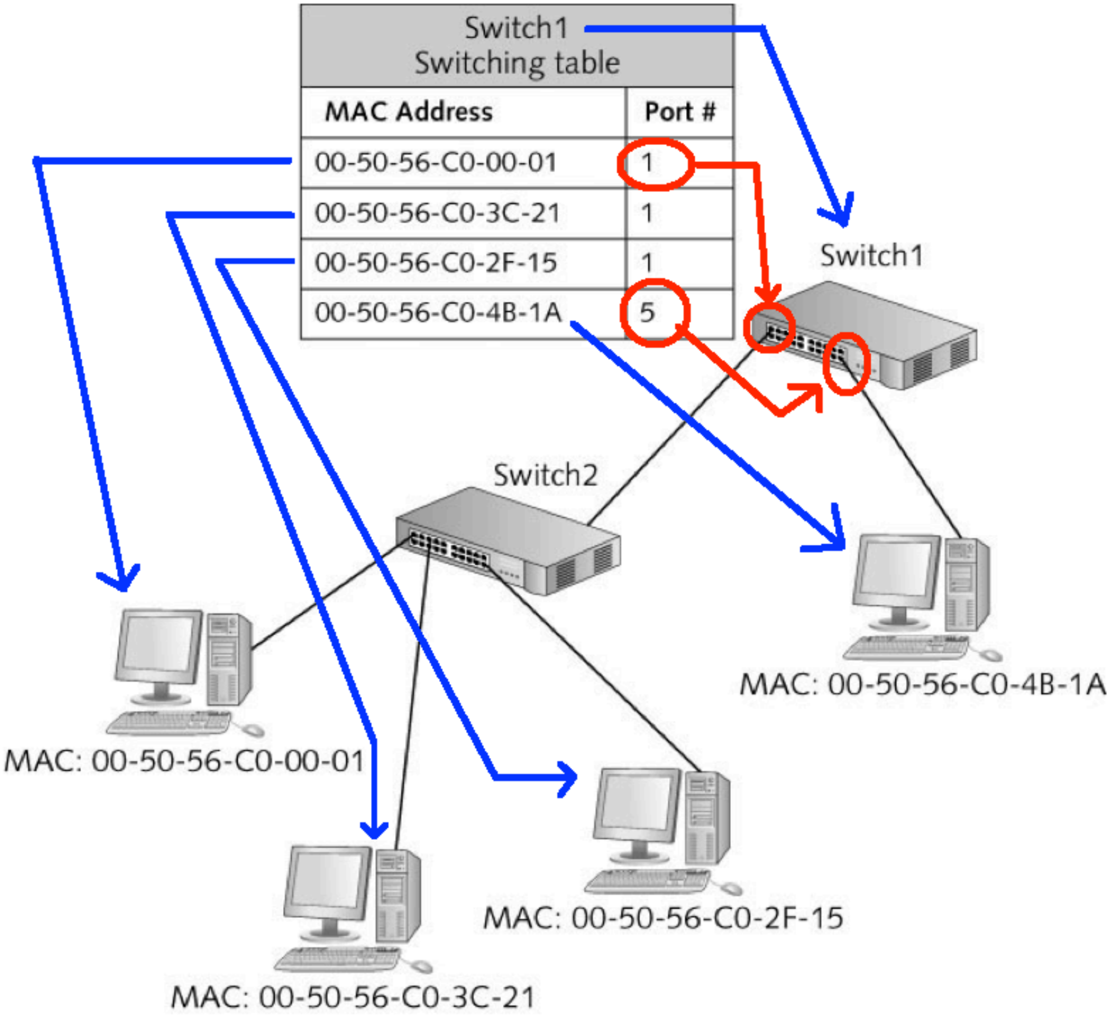
Switch Port Modes of Operation

- Ports on a typical 10/100 Mbps switch can usually operate in full-duplex:
  - Full-duplex - allows connected devices to transmit and receive simultaneously
    - 10 Mbps full-duplex
    - 100 Mbps full-duplex
- Most switches run in **auto-negotiate mode**, which means the switch sets the mode to the highest performance setting the connected device supports

Creating the Switching Table

- A switching table holds MAC address/port pairs that tell the switch where to forward a frame, based on the destination MAC address
- When a switch is first powered on, its table is empty
- As network devices send frames, the switch reads each frame' s source address and adds it to the table along with the port it was received from
- If a frame' s destination address isn' t found in the switching table, the switch forwards the frame out all ports

Creating the Switching Table



Switch1 Switching table	
MAC Address	**Port #**
00-50-56-C0-00-01	1
00-50-56-C0-3C-21	1
00-50-56-C0-2F-15	1
00-50-56-C0-4B-1A	5

Switching tables can contain multiple MAC addresses per port

Creating the Switching Table

- Most switches include a number that indicates the number of MAC addresses the switch can hold in its table (8K MAC addresses supported)
- Switching tables prevent stale entries by including a timestamp when an entry is created
  - When a switch receives a frame from a device already in its table, it updates the entry with a new timestamp
- The period of time a table keeps a MAC address is called the **aging time**
  - If the timestamp isn’t updated within the aging time, the entry expires and is removed from the table

Advanced Switch Features

- High-end switches, often referred to as “smart switches” and “managed switches,” can help make a network more efficient and reliable
- The following slides are an overview of the most common features found in “smart switches”

Advanced Switch Features

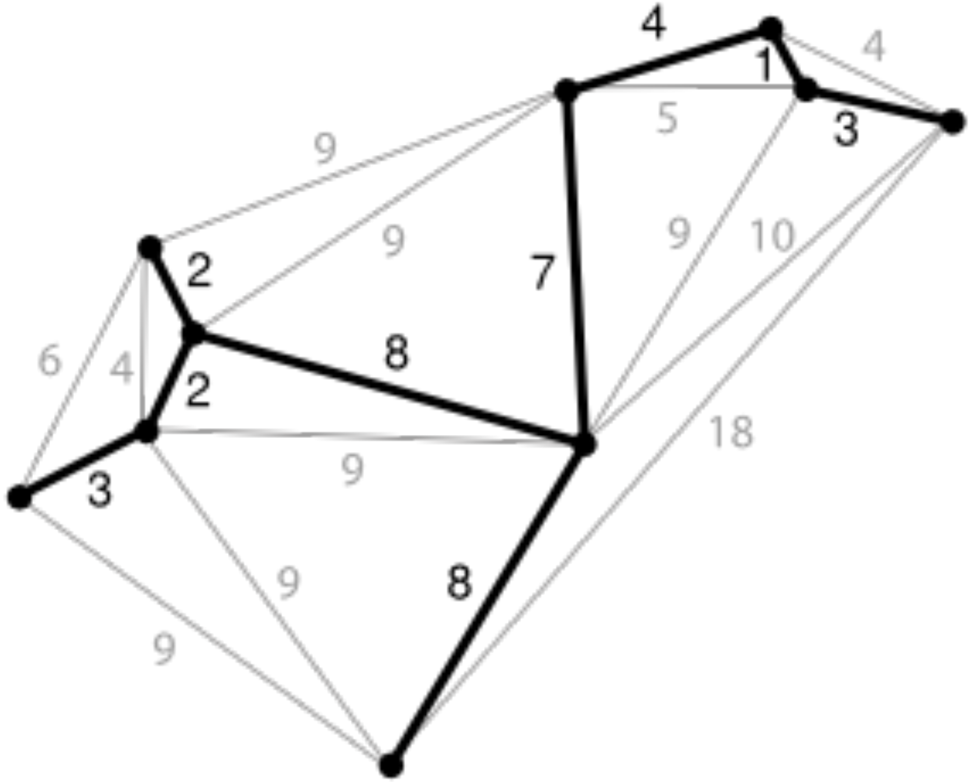
- **Multicast processing** – Switches process multicast frames in one of two ways
  - By treating them as broadcasts and sending them out all ports
    - Used by low-end switches or those that have not been configured for it
  - By forwarding the frames only to ports that have registered the multicast address
    - Used by switches that support Internet Group Management Protocol (IGMP)
    - Multicast MAC addresses always begin with 01:00:5E, leaving the rest of the address to identify a particular multicast application

Advanced Switch Features

- **Spanning Tree Protocol** – Enables switches to detect when there is a potential for a switching loop
- A loop occurs when a frame is forwarded from one switch to another in an infinite loop
  - When a possible loop is detected, one of the switch ports goes into blocking mode, preventing it from forwarding frames that would create a loop
  - If the loop configuration is broken, the switch that was in blocking mode resumes forwarding frames

- *Simulation 15 – STP prevents switching loops*

Spanning Tree



Points – represent switch in network
Numbers – represent cost to transmit to next switch
Switch – each switch has computers attached

Advanced Switch Features

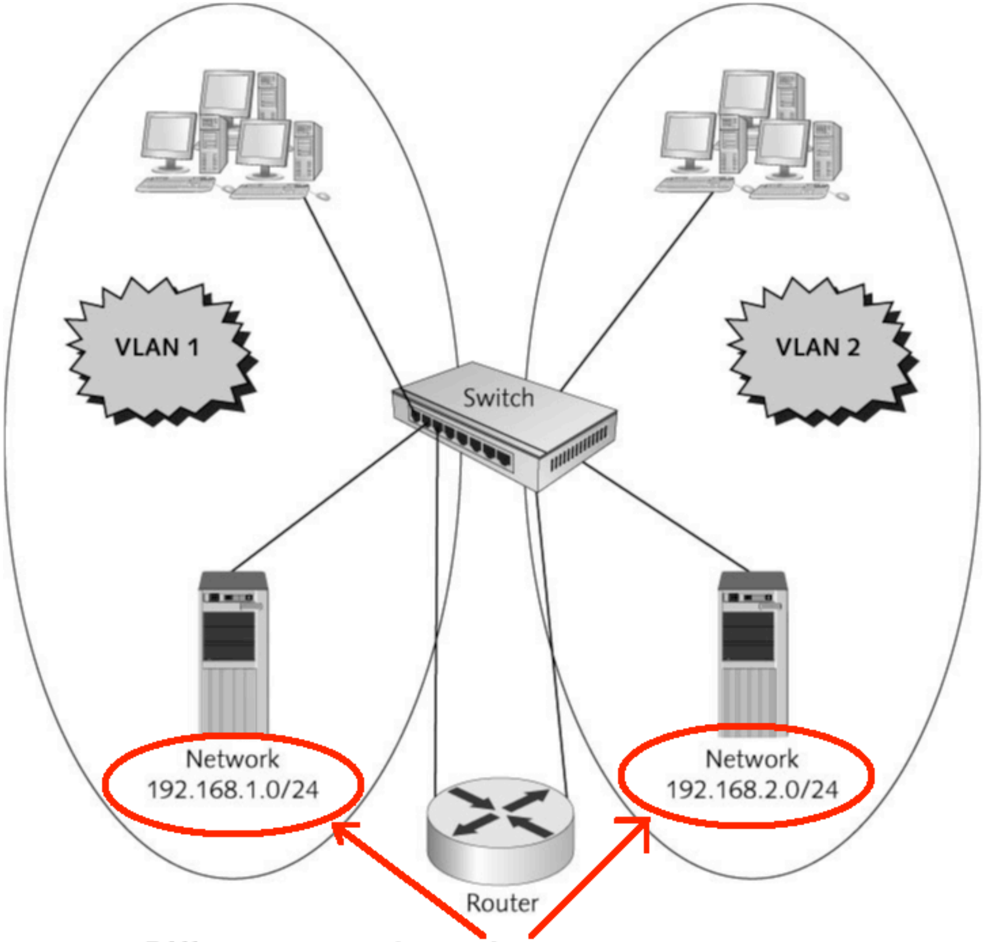
- **Virtual Local Area Networks (VLANS)** – enable you to configure one or more switch ports into separate broadcast domains
  - It's like separating a switch into two or more switches that aren't connected to one another
  - A router is needed to communicate between VLANs
  - Improves management and security of the network and gives more control of broadcast frames
  - Allows administrators to group users and resources logically instead of by physical location

Advanced Switch Features

VLANs logically group users and resources from different physical locations

A **trunk port** is a switch Port configured to carry Traffic from all VLANs to another switch or router

Simulation 16 – How switches use trunk ports with VLANs



Different network numbers means:
-- 2 different networks
-- router required to connect the 2 networks
-- only packets addressed to the other network get passed from 1 network to the other

Routers in Depth

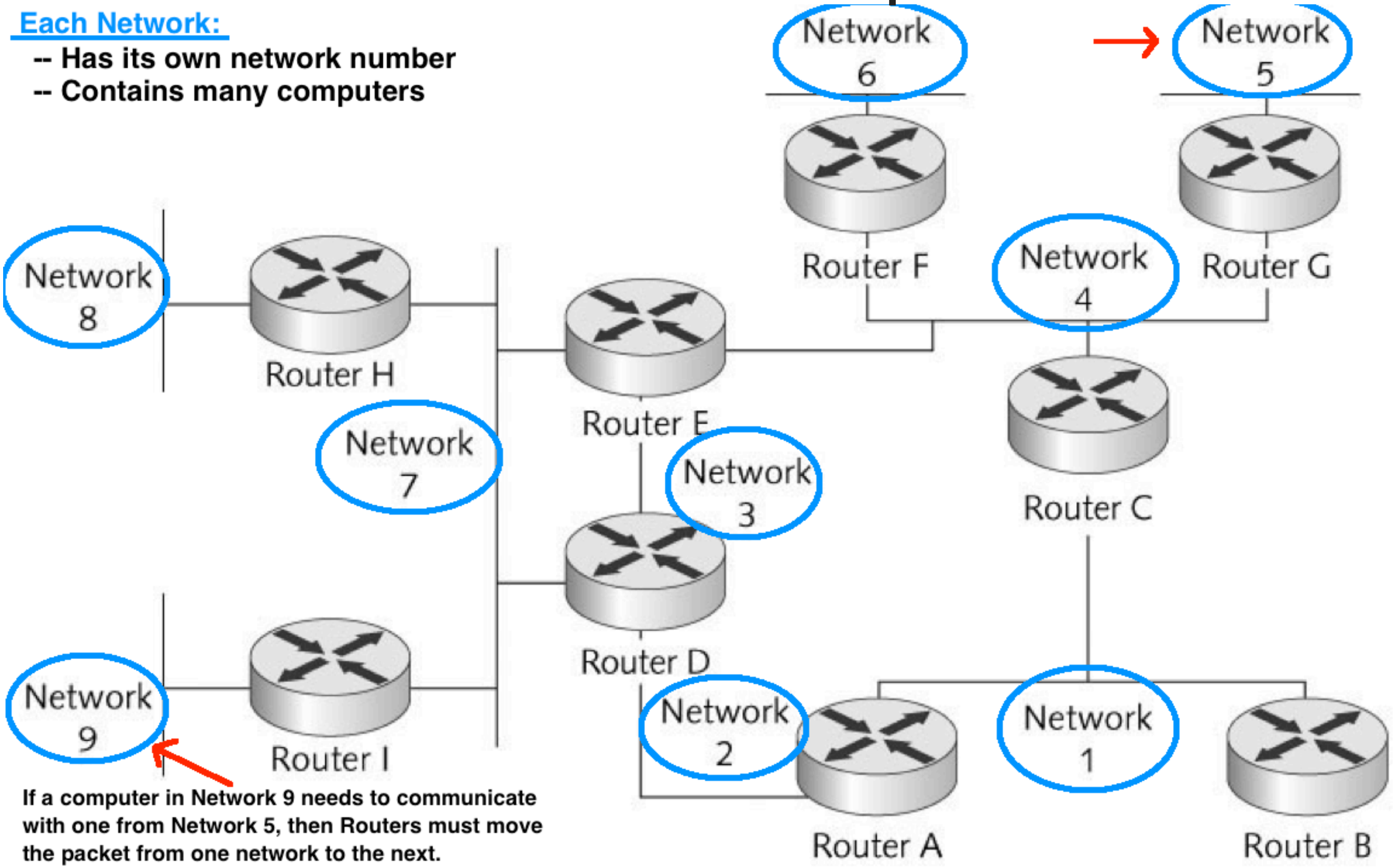
- Routers operate at the Network layer (Layer 3) and work with packets
  - Connect separate logical networks to form an internetwork
  - Broadcast frames are not forwarded to other router ports (other networks)
  - Routers can be used to create complex internetworks with multiple paths creating fault tolerance and load sharing
  - All processing done by routers depends on the following features found on most routers:
    - Router interfaces
    - Routing tables
    - Routing protocols
    - Access control lists

Network Layer (3)
Internet Protocol Version 6
Internet Protocol Version 4

Routers in Depth

Each Network:

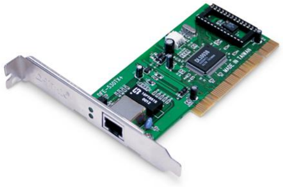
-- Has its own network number
-- Contains many computers

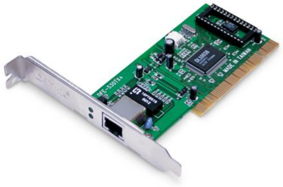


If a computer in Network 9 needs to communicate with one from Network 5, then Routers must move the packet from one network to the next.

Router Interfaces

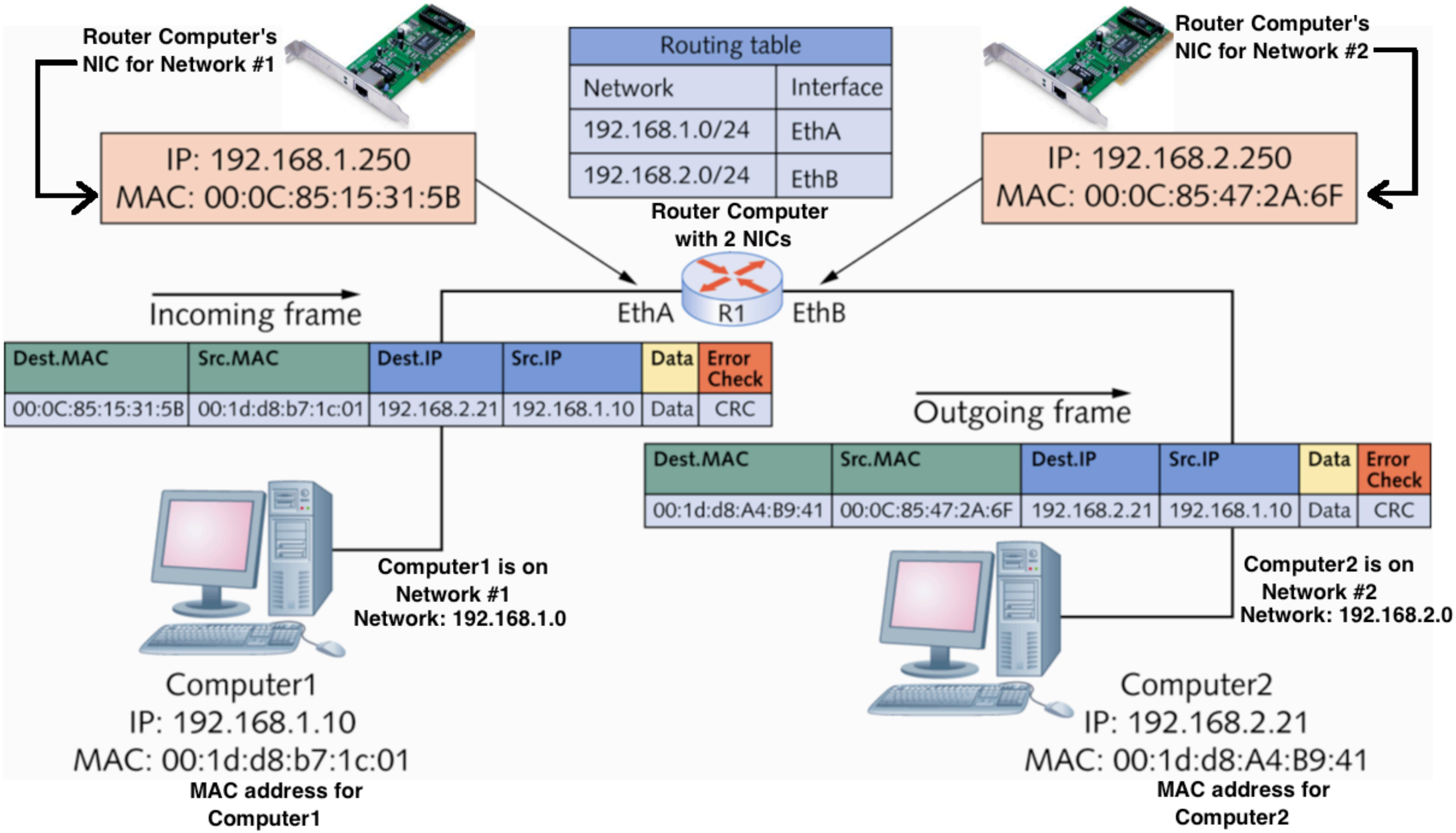
- Routers must have two or more interfaces (ports) in order to take packets coming from one network and forward them to another network -- that is, 2 NIC cards





- When a router interface receives a frame, it compares the destination MAC address with the interface's MAC address
  - If they match, the router strips the frame header and trailer and reads the packet's destination IP address
  - If the IP address matches it processes the packet
  - If the IP address does not match, the router consults its routing table to determine how to get the packet to the its destination
  - The process of moving a packet from the incoming interface to the outgoing interface is called **packet forwarding**

Router Interfaces



Router Computer's NIC for Network #1

IP: 192.168.1.250
MAC: 00:0C:85:15:31:5B

Routing table	
Network	Interface
192.168.1.0/24	EthA
192.168.2.0/24	EthB

Router Computer with 2 NICs

Router Computer's NIC for Network #2

IP: 192.168.2.250
MAC: 00:0C:85:47:2A:6F

EthA R1 EthB

Incoming frame

Dest.MAC	Src.MAC	Dest.IP	Src.IP	Data	Error Check
00:0C:85:15:31:5B	00:1d:d8:b7:1c:01	192.168.2.21	192.168.1.10	Data	CRC

Outgoing frame

Dest.MAC	Src.MAC	Dest.IP	Src.IP	Data	Error Check
00:1d:d8:A4:B9:41	00:0C:85:47:2A:6F	192.168.2.21	192.168.1.10	Data	CRC

Computer1 is on Network #1
Network: 192.168.1.0

Computer2 is on Network #2
Network: 192.168.2.0

Computer1
IP: 192.168.1.10
MAC: 00:1d:d8:b7:1c:01

MAC address for Computer1

Computer2
IP: 192.168.2.21
MAC: 00:1d:d8:A4:B9:41

MAC address for Computer2

Packets are forwarded from one network to another

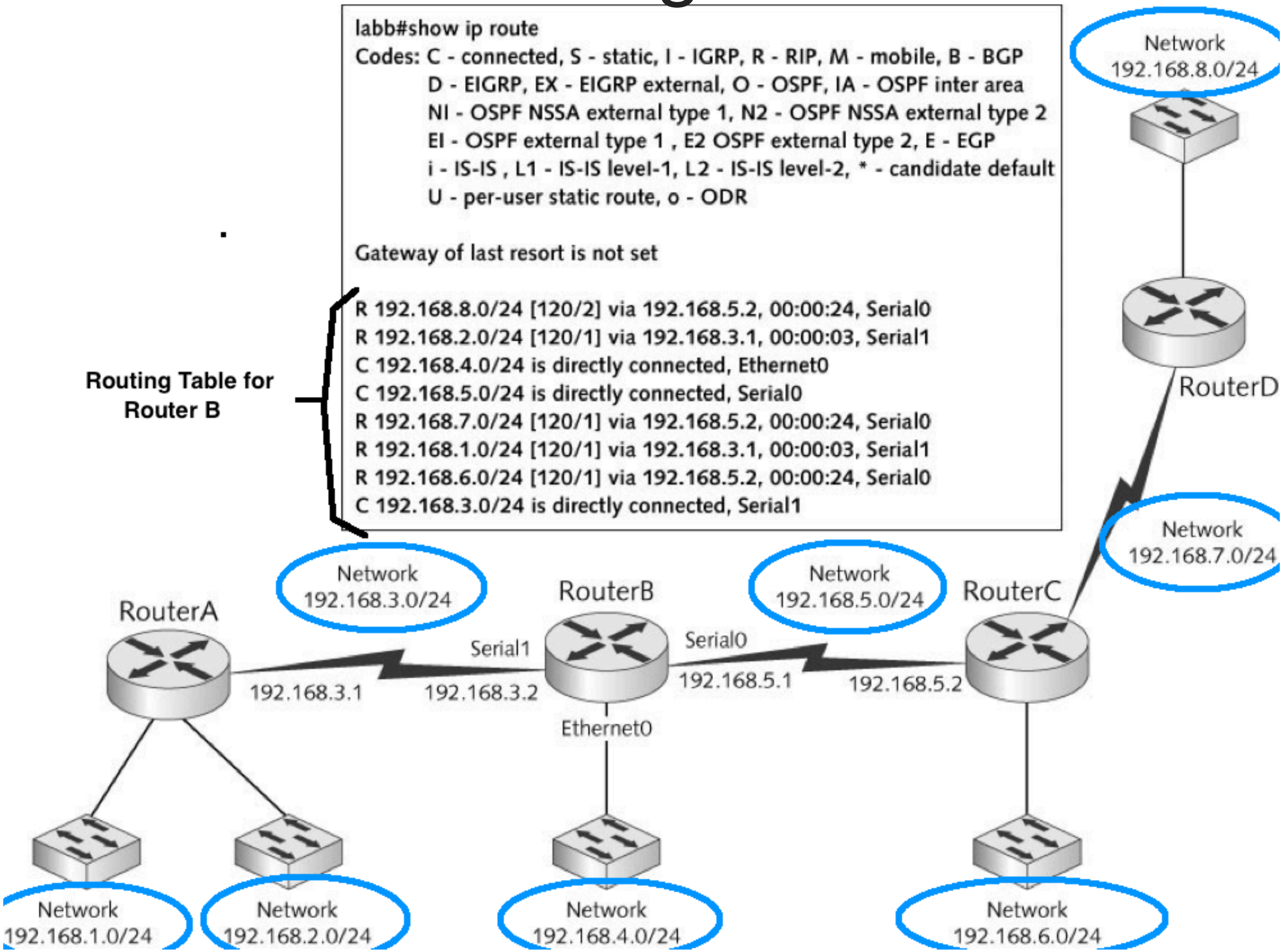
Routing Tables

- Routing tables are composed of network address and interface pairs that tell the router which interface a packet should be forwarded to
- Most routing tables contain the following for each entry:
  - Destination network: Usually expressed in CIDR notation such as 172.16.0.0/16
  - Next hop: The next hop indicates an interface name or the address of the next router in the path to the destination
    - Total number of routers a packet must travel through is called the hop count
  - Metric: Numeric value that tells the router how “far away” the destination network is (also called cost or distance)

Routing Tables

- Contents of routing tables (cont.):
  - How the route is derived: This field tells you how the route gets into the routing table (one of 3 ways)
    - Network is connected directly
    - Administrator enters the route information manually (called a static route)
    - Route information is entered dynamically, via a routing protocol
  - Timestamp: Tells the router how long it has been since the routing protocol updated the dynamic route
- *Simulation 17 – Routers use multiple paths in an internetwork*

Routing Tables



```
labb#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       NI - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       EI - OSPF external type 1 , E2 OSPF external type 2, E - EGP
       i - IS-IS , L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

R 192.168.8.0/24 [120/2] via 192.168.5.2, 00:00:24, Serial0
R 192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:03, Serial1
C 192.168.4.0/24 is directly connected, Ethernet0
C 192.168.5.0/24 is directly connected, Serial0
R 192.168.7.0/24 [120/1] via 192.168.5.2, 00:00:24, Serial0
R 192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:03, Serial1
R 192.168.6.0/24 [120/1] via 192.168.5.2, 00:00:24, Serial0
C 192.168.3.0/24 is directly connected, Serial1
```

Routing Protocols

- Routing protocol – A set of rules that routers use to exchange information so that all routers have accurate information about an internetwork to populate their routing tables
- Two main types of routing protocols
  - ***Distance-vector protocols*** share information about an internetwork's status by copying a router's routing table to other routers (routers sharing a network are called neighbors)
    - Routing Information Protocol (RIP) and RIPv2 are most common
  - ***Link-state protocols*** share information with other routers by sending the status of all their interface links to other routers
    - Open Shortest Path First (OSPF) is most common

Access Control Lists

- Access Control List (ACL) – A set of rules configured on a router's interface for specifying which addresses and which protocols can pass through an interface and to which destinations
- When an ACL blocks a packet it is called ***packet filtering***
- Usually configured to block traffic based on:
  - Source address
  - Destination address
  - Protocol
- Addresses can be specific IP addresses or network numbers and filtering can be done on either source or destination address or both

Wireless Access Points in Depth

- Basic wireless settings on most APs define the settings a client wireless device needs to connect to an AP:
  - Wireless network mode: allows you to choose which 802.11 standard the AP should operate under
  - Wireless network name (SSID): when an AP is shipped, the SSID is set to a default value – it is recommended that you change it upon setup
  - SSID broadcast status: by default
- Commonly purchased:
  - Wireless Router consisting of:
    - Wireless access point
    - Router
    - Switch

Wireless Security Options

- Most APs offer the following security options:
  - Encryption
  - Authentication
  - MAC filtering
  - AP isolation
- Encryption – all private networks should use this
  - Most common protocols are:
    - Wired Equivalent Privacy (WEP) - weakest
    - Wi-Fi Protected Access (WPA)
    - Wi-Fi Protected Access 2 (WPA2) - strongest
  - Use the highest level of security your systems support
    all devices must use the same protocol

Wireless Security Options

- Authentication – If used, users must enter a username and password to access the wireless network

- MAC filtering – enables you to restrict which devices can connect to your AP
  - Add the MAC addresses of the wireless devices allowed to access your network to a list on the AP

Network Interface Cards in Depth

- PC Bus Options – a bus makes the connections between a computer's vital components
  - The faster the bus, the faster data can be transferred between these components, which makes for a faster system
  - NICs are considered I/O devices and can be built into the motherboard or added as an expansion card
  - Peripheral Component Interconnect (PCI) bus became the *default bus standard*
    - Most implementations are 32-bit and operate at 33 MHz with a maximum data transfer rate of 133 MBps
    - First bus to accommodate the Microsoft Plug-and-Play architecture

Advanced Features of NICs

- If a NIC is slow, it can limit network performance
- When selecting a network adapter, first identify the physical characteristics the card must match (type of bus, type of network technology, type of connector needed to connect to media)
- Hardware-enhancement options:
  - *Shared adapter memory*: the adapter's buffers map directly to RAM on the computer
  - *Shared system memory*: a NIC's onboard processor selects a region of RAM on the computer and writes to it as though it were buffer space on the adapter

Advanced Features of NICs

- Hardware-enhancement options (continued):
  - RAM buffering: means a NIC includes additional memory to provide temporary storage for incoming and outgoing network data that arrives at the NIC faster than it can be sent out
  - Onboard co-processors: enable the card to process incoming and outgoing network data without requiring service from the CPU

Advanced Features of NICs

- Hardware-enhancement options (continued):
  - Improved fault tolerance by installing a second NIC
    - Failure of the primary NIC shifts network traffic to the second NIC
  - Advanced Configuration Power Management Interface (ACPI) offers wake-on LAN, which allows an administrator to power on a PC remotely by accessing the NIC through the network
  - Preboot Execution Environment (PXE) allow a computer to download an OS instead of booting it from a local hard drive
    - Used on diskless workstations ("thin clients") that do not store the OS locally
- Typical desktop computers with basic features are usually adequate.
- Servers do warrant some of these high-end features

Chapter Summary

- Network switches use auto-negotiate mode to determine the link speed and duplex mode
- Switching tables can hold many more MAC addresses than ports
- Switches forward frames by using a variety of methods: cut-through, fragment-free, and store-and-forward
- Advanced features, such as VLANs, STP, multicast support, and port security are found on smart switches
- Routing tables contain destination networks, next hop addresses, metrics, methods used to derive routes, and timestamps

Chapter Summary

- Routing protocols populate routing tables dynamically. The most common type of routing protocols are distance-vector and link-state
- Access points have the following basic settings: wireless mode, SSID, and wireless channel
- Higher-end APs can support advanced features, such as multiple SSIDs, adjustable transmit power, VLANs, QoS, and repeater and bridge modes
- NIC selection includes the PC bus
- Some advanced NIC features to consider include RAM buffering, onboard co-processors, automatic link aggregation, and multiple ports for fault tolerance