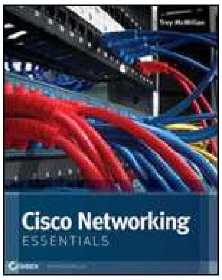


Cisco Networking Essentials

by Troy McMillan

Chapter 10: Network Devices

Various hardware devices can be deployed to connect a network. Knowledge of how they work and where to place them is critical to designing the network. A poorly designed network will be difficult to optimize, regardless of the quality of the equipment.

This chapter is dedicated to the understanding of the role played by each device and the principles that drive the positioning of each. Specifically, this chapter covers the following topics:

- Describing device functions
- Understanding device placement principles

Describing Device Functions

Infrastructure devices are those devices that connect sections of the network together, like road systems that connect cities and towns. Some of the devices create connections that operate like limited-access interstate highways connecting cities, while others create connections that are more like secondary highways that connect smaller towns and provide access to the interstate highway at specified entrance ramps. Finally, using the same analogy, some of the devices create connections that might be considered local roads, connecting neighborhoods to the secondary roads.

If you've ever driven in an area where the road system developed over time without a master plan and experienced the headaches that result from this, you can understand why proper network design in the front end is critical. Besides designing for the immediate performance of the network, you need to consider the ability of the network to absorb growth over time without sacrificing performance. Before you can properly design the network and place the devices, you must have an understanding of the functions of the devices, the concepts that guide their operation, and the interrelationships that exist.

One of the best ways to frame the discussion of each device is to map the device to the TCP/IP model. When we do this, it helps to make clear the layers at which the devices operate, and this in turn helps us understand which devices should create interstate highways and which should create secondary roads and so forth from a design perspective.

This section covers the major devices with respect to the following:

- The TCP/IP layers at which they operate
- The roles they can play in the Cisco three-layer model
- The position they occupy in the LAN hierarchy

Understanding Repeaters

Repeaters operate at the Network Access layer of the TCP/IP model, but to say they operate at that layer is really to overstate the intelligence of these devices. The Network Access layer includes both the Network Access layer technology (which in the case of a LAN is Ethernet using MAC addresses) and the physical implementation of that technology. A repeater operates on only the physical part of this layer, so it is sometimes referred to as a physical device.

A repeater simply takes the original signal and amplifies, or boosts, the signal. As you may remember from the discussion about cable length and attenuation in the preceding chapter, after the signal has traversed a certain length of cable, the signal strength is gradually weakened by the resistance in the cable (which is called *attenuation*). At some point (at the maximum cable length), the signal becomes so degraded that it cannot be understood when it arrives at the destination device. A repeater can be used to connect two lengths of cable that together would exceed the maximum length. It simply amplifies the signal and transmits it.

Repeaters really should be avoided in network design. You should plan the location of the access switches in such a way that no runs of cable over 100 meters are required. You should view repeaters as a solution to a network design problem that you inherited, not one you created. If a bad network design causes a repeater to be included in the network, this device would be considered to be operating on the Access layer of the Cisco three-layer model. This model is discussed in more detail at the end of the chapter.

Understanding Hubs

Hubs operate at the same layer as repeaters and are sometimes referred to as *multiport repeaters*. They have no intelligence. When a signal is received by a hub on one of its ports, it simply repeats the signal to all other ports. This is illustrated in Figure 10.1. A signal arriving in port 1 is simply sent out all other ports.

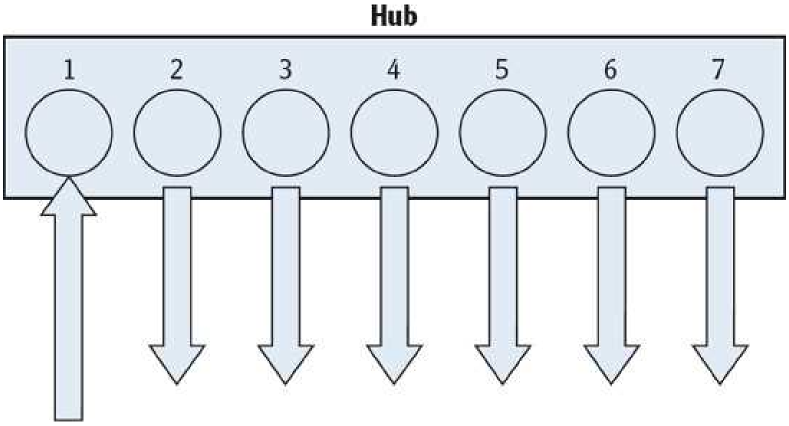


Figure 10.1: Hub operation

The problem with this operation is that all of the ports are on a shared network. They all exist in one collision domain. You will learn more about collision domains later in this chapter, but for now understand that when signals are regenerated to every port as with a hub, the frequency of collisions is greatly increased. As you learned, collisions lead to retransmissions, which lead to reduced data throughput (that is, a slow network).

Hubs should never be a planned piece in a network design. Over and above the performance problems they introduce, they also create security concerns. If a protocol analyzer or sniffer is connected to a port on the hub or is operating as software on a computer connected to the hub, traffic from all computers connected to the hub can be captured. As explained in the next section, switches segregate devices into separate collision domains (one for each port) and in the process make capturing packets from all devices impossible. If a sniffer is connected to a port on a switch or is running as software on a computer connected to a port on a switch, only the traffic between the sniffer or computer and the switch port can be captured. If a hub is included in the network, it would be considered to be operating on the Access layer of the Cisco three-layer model.

Note The Cisco three-layer model is discussed at the end of this chapter.

Understanding Bridges

Bridges operate on the Network Access layer of the TCP/IP model, but unlike repeaters and hubs, they go beyond the physical half of the layer and use Ethernet information (MAC addresses) to make forwarding decisions. When a bridge is first started, it acts as a hub does. It sends a frame out every port except for the one on which it arrived. However, in a very short period of time, it learns the MAC address of every device connected to every port. It stores these addresses in a table called the *MAC address table*. Then, when it receives a frame (these are frames, remember, because we are using information at the Network Access layer), it sends that frame only out the port where the destination MAC address is located, as shown in Figure 10.2. This process is called transparent bridging.

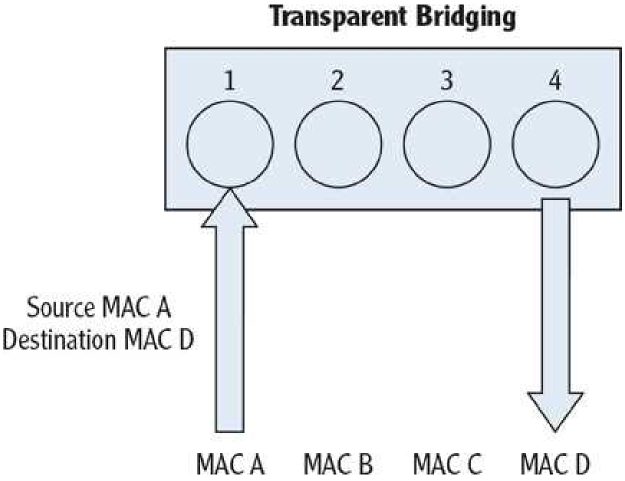


Figure 10.2: Bridging operation

The result of this is that each bridge port resides in its own *collision domain*. The traffic on each bridge port is *only* traffic destined for that device (or network). That greatly decreases the chance of collisions and in turn lowers the retransmission rate, which increases performance by leaps and bounds.

Bridges have typically been used in the past to connect network segments, rather than devices. So when bridges are used in this manner, each network segment is a collision domain, as shown in Figure 10.3.

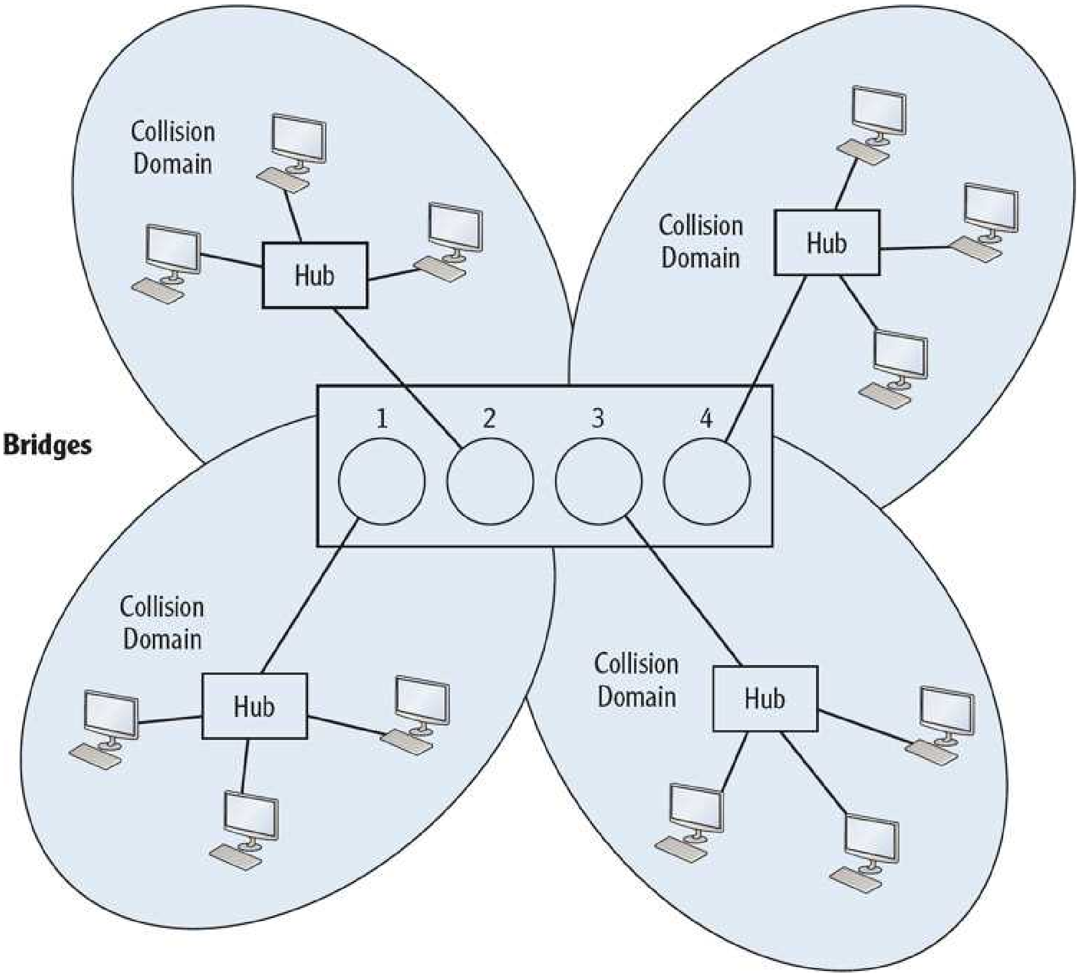


Figure 10.3: Bridges

Switches provide a port and a collision domain to each device, as shown in Figure 10.4.

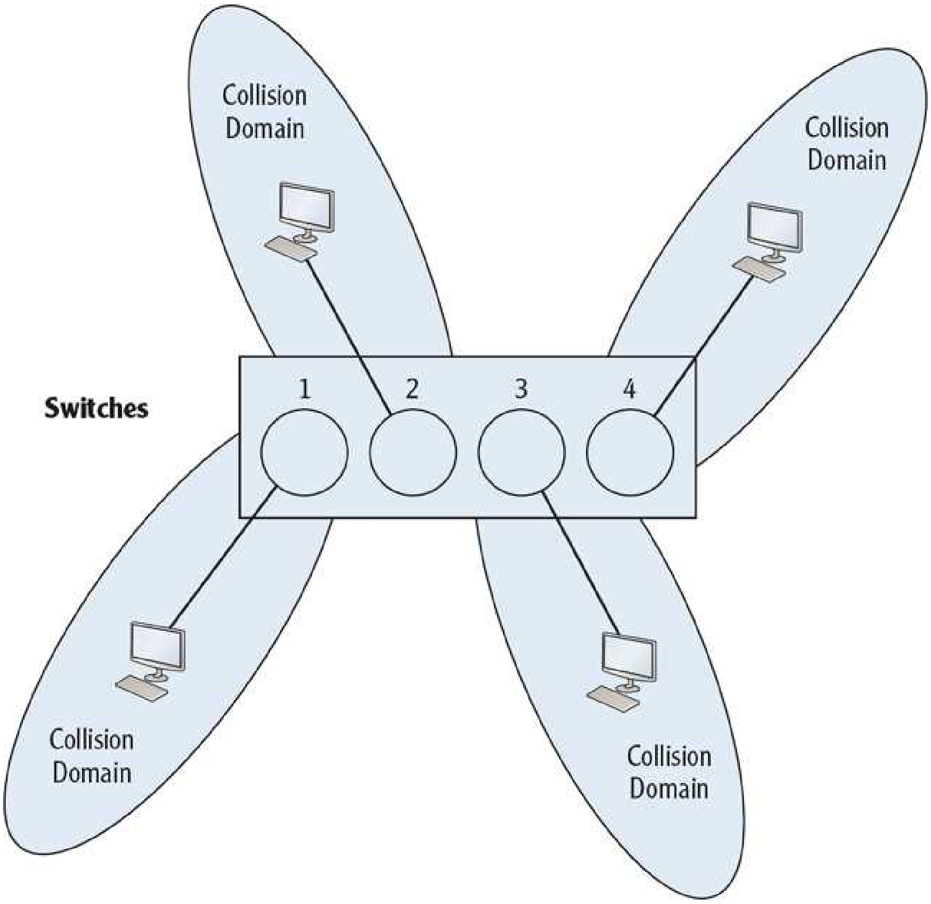


Figure 10.4: Switches

Bridges are rarely used anymore in networks because the same transparent bridging can be provided by switches, which have many advantages over bridges. These advantages are discussed in the next section. If a bridge is included in the network, it would be considered to be operating on the Access layer of the Cisco three-layer model.

Note The Cisco three-layer model is discussed at the end of this chapter.

Understanding Switches

Switches also operate on the Network Access layer of the TCP/IP model and use Ethernet information (MAC addresses) to make forwarding decisions. There are all sorts of functions that you can configure on a Cisco switch by connecting to it with a console cable and using the Cisco command-line interface (CLI). But even if you never touch this interface and use the switch as it comes straight out of the box, it will provide the same transparent bridging provided by an Ethernet bridge.

Advantages of Using Switches

The main advantages of a switch over a bridge are as follows:

- **Software vs. Hardware** Bridges perform the bridging function by using software. Switches, on the other hand, are hardware based. The switching is done using ASIC chips. When hardware is used for this function, the forwarding process is much quicker.

ASICs

Application-specific integrated circuits (ASICs) are those that are dedicated to a specific function, as opposed to a general-purpose integrated circuit. An example is a chip designed solely for a cell phone (you can use it for only that purpose). By using this customized circuitry for the switching function, rather than using the CPU or other more general-purpose circuitry in the switch, performance is greatly enhanced. This is sometimes referred to as switching in the hardware rather than switching in the software.

- **Port Density** Because bridges are designed to connect network segments, they tend to have fewer ports. Switches, on the other hand, normally come in 16-, 24-, and even 52-port models.

Note *Port density* simply refers to the number of ports. A device with 24 ports would exhibit more port density than one with 8 ports.

- **Spanning-Tree Instances** Bridges are limited to a single instance of Spanning Tree, while switches can have many. Spanning Tree Protocol (STP) is discussed in Chapter 14, "Configuring Switches." This protocol is used to prevent switching loops that can occur when switching path redundancy is present in the network.

Path Redundancy and Loops

If designing path redundancy creates switching loops, why would you include them in the design, anyway? The reason for this is fault tolerance. Just as multiple routing paths between two destinations allows for a backup route if one of the routes becomes unavailable, switching path redundancy provides the same benefit. It is such a beneficial design characteristic that the Spanning Tree Protocol (STP) was designed to prevent loops when switching path redundancy exists. Moreover, you don't even have to enable this; it operates automatically!

So as you can see, there are many reasons that switches are used rather than bridges even though they perform the same function.

Types of Switches

Switches come in two versions: those that operate at the Network Access layer only and those that are called multilayer switches. Multilayer switches operate at both the Network Access and the Internet layers, which means (as you will learn in the next section) they do switching and routing. The rest of this section presents the characteristics of both Network Access layer switches and multilayer switches.

- **Network Access Layer Switches** These switches make forwarding decisions based only on MAC addresses and do not use Internet layer information (IP addresses). They typically act as the connection point to the network for workstations, printers, and other devices on the LAN. A Network Access layer switch is shown in Figure 10.5.

Figure 10.5: Network Access layer switch

Because this is the case, these types of switches are said to be operating on the Access layer of the Cisco three-layer model. The functions of switches that operate at this layer are listed here:

Note The Cisco three-layer model is discussed at the end of this chapter.

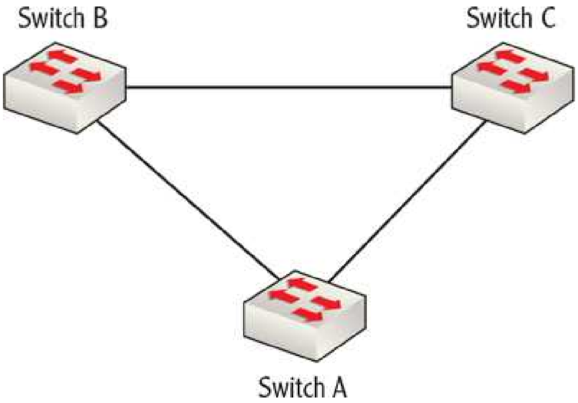
  - **MAC Address Learning** The switch identifies the source MAC address whenever a frame enters one of the ports and places this in its MAC address table.
  - **Forward/Filter Decisions** When a frame enters a port, the switch identifies the destination MAC address. If it finds that MAC address in its table, it sends the frame out the port listed for that MAC address *only*. If it doesn't find the MAC address listed in its table, it will flood the frame out every port except the one on which it arrived.

    Note *Port flooding* refers to the process of sending a frame out every port except the one on which it arrived.
  - **Loop Avoidance** If switch path redundancy exists in the network, it is the job of the switch to avoid loops. Loops occur when a frame doesn't find its destination and (because of loops that exist in the network for redundancy purposes) continues around the network over and over again. Loops are avoided by the switches communicating with one another using STP to close these loops. You will learn more about STP and its operations in Chapter 14.

Switch Path Redundancy

So what does switch path redundancy look like? The following graphic shows that because of the way switches A, B, and

C are connected, there is redundancy between A and C if the direct link between them fails. They can still have a switching path by going through switch B. By building in this fault tolerance, however, a potential switching loop is introduced around switches A, B, and C. STP is used to prevent these loops from causing problems, as you will learn in Chapter 14.



- **MLS Switches** Multilayer switches perform routing and switching, but what is most impressive is the way in which they combine these functions. To appreciate the operation of these devices, consider that when one device is sending data to another device, it is a not a transmission made up of a single packet. It can be made up of hundreds and even thousands of individual packets in the same transmission.

  Rather than simply routing each packet (which is what you would expect if this were simply a box containing both a router and a switch), it routes the first packet (routing is a much slower process than switching) and then by maintaining an awareness of that route, it switches all of the other packets in the transmission. This concept has come to be known in the Cisco world as *route one and switch many*. The result is an impressive increase in speed of the delivery of the entire transmission. Multilayer switches can operate on the Access layer of the Cisco three-layer model. However, in most cases they operate on the Distribution layer, where most routers operate, or on the Core layer of the model, where their speed is one of the main requirements of devices at that layer.

Note The Cisco three-layer model is discussed at the end of this chapter.

Understanding Routers

Routers operate at the Internet layer of the TCP/IP model and make routing decisions based on IP address information. A router is shown in Figure 10.6.

Figure 10.6: Router

The IP address information is stored in routing tables. Routing tables contain routes, or pathways, to networks (called *network routes*, usually maintained in the form of the network ID) and if configured as such, routes to specific devices (called host routes). They also can contain a type of route called a default route. The router uses the default route to send all traffic for which it has no route in its table. A default route can be thought of as the default gateway for the router because it uses that route much like a host uses its default gateway (that is, a host will send any traffic that is not in its local network to the default gateway). If a router is configured with a default route and you issue the command to show all routes (show ip route), this route is referred to as the gateway of last resort.

Routing tables of the routers can be populated in two ways. When an administrator connects to the router and manually uses commands to program the routes into the routing table, the router will be using *static routing*. When the router is configured to use a routing protocol, the router will be using *dynamic routing*. Each of these methods has advantages and disadvantages, which are discussed in the following sections.

Dynamic Routing

When a routing protocol is enabled on a router, it will exchange routing information with other routers that have been enabled with the same routing protocol. Before a router has learned any information from other routers, it will have only routes in its table to networks to which it is directly connected. In Figure 10.7, router R1 has routes in its table only to the 192.168.5.0/24 and 192.168.6.0/24 networks. This is because it is directly connected to only those networks. It does not, however, know about the 192.168.7.0/24 network because it is not directly connected to that network.

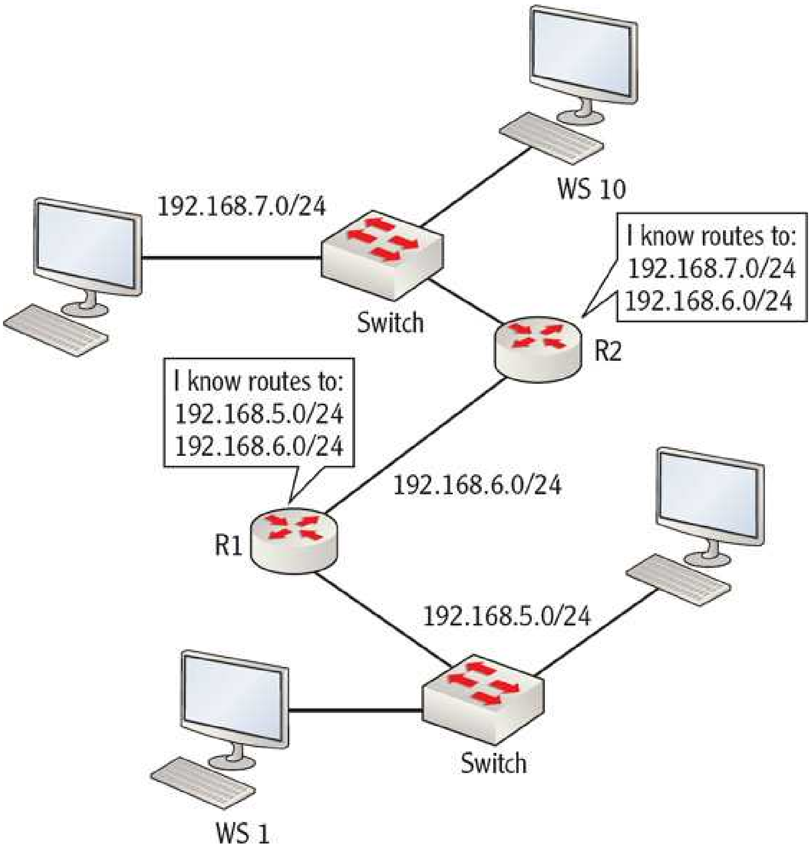

WS 10
192.168.7.0/24
I know routes to: 192.168.7.0/24 192.168.6.0/24
Switch
R2
I know routes to: 192.168.5.0/24 192.168.6.0/24
192.168.6.0/24
R1
192.168.5.0/24
Switch
WS 1

Figure 10.7: Directly connected routes

Likewise, before any routing information is exchanged between R1 and R2, router R2 will know about only the 192.168.6.0/24 and 192.168.7.0/24 networks, because those are the only networks to which it is directly connected. After the two routers have exchanged their routing tables, both routers will have all three routes in their tables, as shown in Figure 10.8, and *only then* will a packet from WS 1 destined for WS 10 be routed successfully.

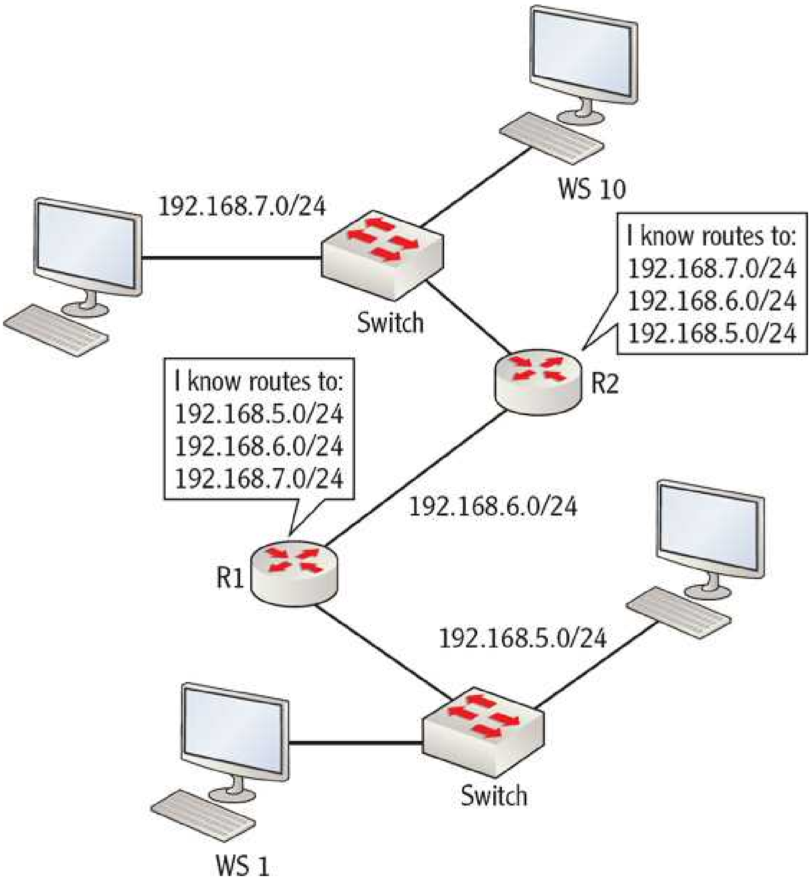


Figure 10.8: Routing tables updated

The advantages of dynamic routing are that the remote routes (the routes that are not directly connected) will not have to be entered manually but will be placed in the table automatically as the routers exchange information. The disadvantage is that for this to occur, the routers create traffic on the network called *routing update traffic*. In some cases, this traffic can be significant and competes with normal data traffic on the network.

Another advantage of dynamic routing is that if multiple paths exist to the same network, as shown in Figure 10.9, the router can use metrics to choose the best route. A *metric* is a value that is used to determine the best route that can be based on the number of routers on each path (called hops) or on more-sophisticated combinations of information such as hop count and bandwidth. The routers in Figure 10.9 are using hop count (number of routers on the path) as their metric, and so R1 will send any information from WS1 to WS10 through R4 because it's a shorter path in terms of hop count.

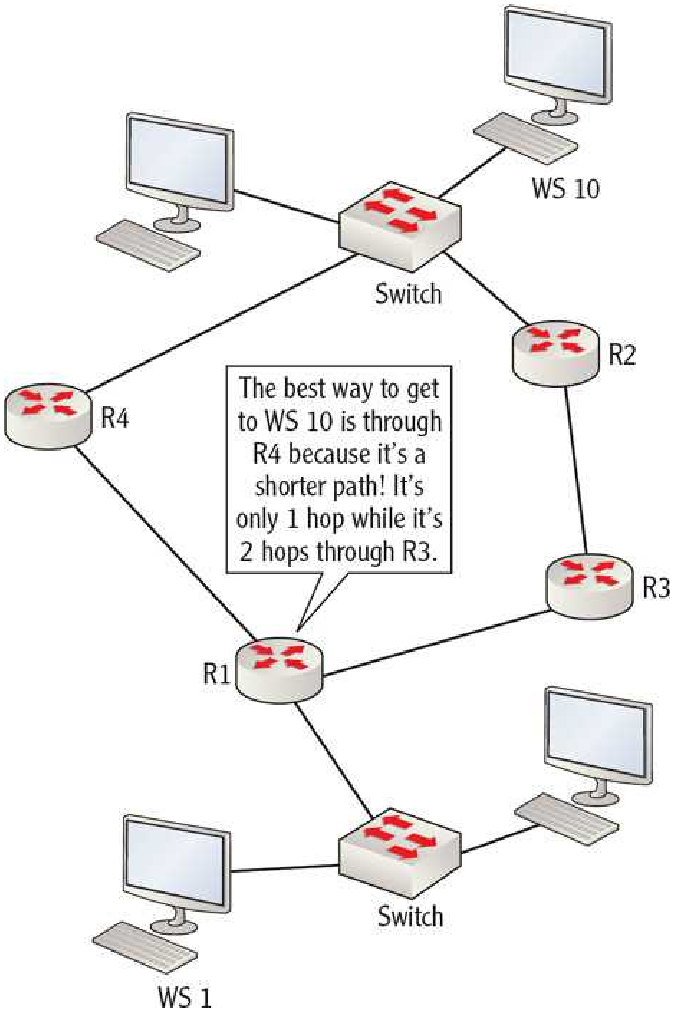

WS 10
Switch
R2
R4
The best way to get to WS 10 is through R4 because it's a shorter path! It's only 1 hop while it's 2 hops through R3.
R3
R1
Switch
WS 1

Figure 10.9: Multiple routes

Moreover, if the best route becomes unavailable (because of link outages, for example), the router can use the other route to still reach the remote network, as shown in Figure 10.10.

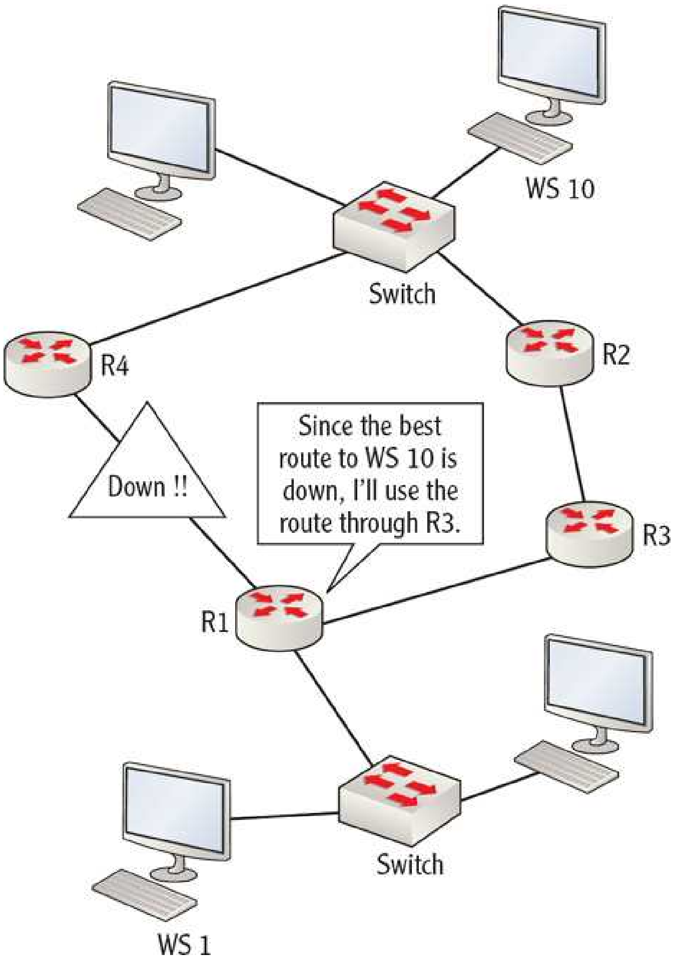

WS 10
Switch
R4
R2
Down !!
Since the best route to WS 10 is down, I'll use the route through R3.
R3
R1
Switch
WS 1

Figure 10.10: Route fault tolerance

Static Routing

The advantage of using static routing is that there is no routing update traffic created. In some situations where the network is very small and the equipment and connections are very reliable and stable, it may be the best choice. The disadvantages of static routing are as follows:.

- The routes must be entered manually.
- Any changes that occur from a link outage, from a change in design, or from the addition of devices must be made manually.
- The best route choice must be made by the administrator and manually configured.

Understanding Wireless Access Points and Wireless Routers

Wireless access points (APs) can be of two types. Some APs are simply switches that provide logical wireless ports to multiple wireless devices, while others are also routers. In an enterprise network, there is a role for both. Depending on the role of the AP and where it is located in the network, it may not be required for it to be a router, and wireless routers cost more than simple APs. In this section both are discussed.

Wireless APs

An AP that is not a router is acting as a switch. It doesn't look like a switch because it doesn't have physical switch ports that you can see and touch (although some models may include one or two of those). The ports are wireless and they are logical. When a device connects to an AP (which may or may not require authentication), it is said to be *associated* with the AP.

The AP maintains this information in an association table that is much like the MAC address table in a switch. If a wireless device needs to send traffic that goes through the AP and then on to the wired part of the network, the device will have to have an IP address that is on the same subnet as the network to which the AP is connected. This is the same concept that would apply if a wired device were connected to a switch. This process is shown in Figure 10.11. In this scenario, because AP 20 is operating as a switch and is *not* a router, laptop 1 will not be able to connect to the router R3 because its IP address is not in the same subnet as the interface on the connection from router R3 to the AP (which is the 192.168.5.0/24 network). The other laptops will not have that problem because their IP addresses are in the same subnet as the router.

Say That Again?

How do we know that router R3 and laptop 1 are not in the same subnet, and what is that 192.168.5.0/24 address all about? Laptops 2 and 3 and the router all have 24-bit subnet masks (255.255.255.0 or /24). That means that if the first three octets of their IP addresses match, they are in the same subnet. Because they all have 192.168.5 in the first three octets, they are all in the same network, which is the 192.168.5.0/24 network. Laptop 1 also has a 24-bit mask, but its first three octets are 192.168.56, so it is not in the same network as laptops 2 and 3 and the router.

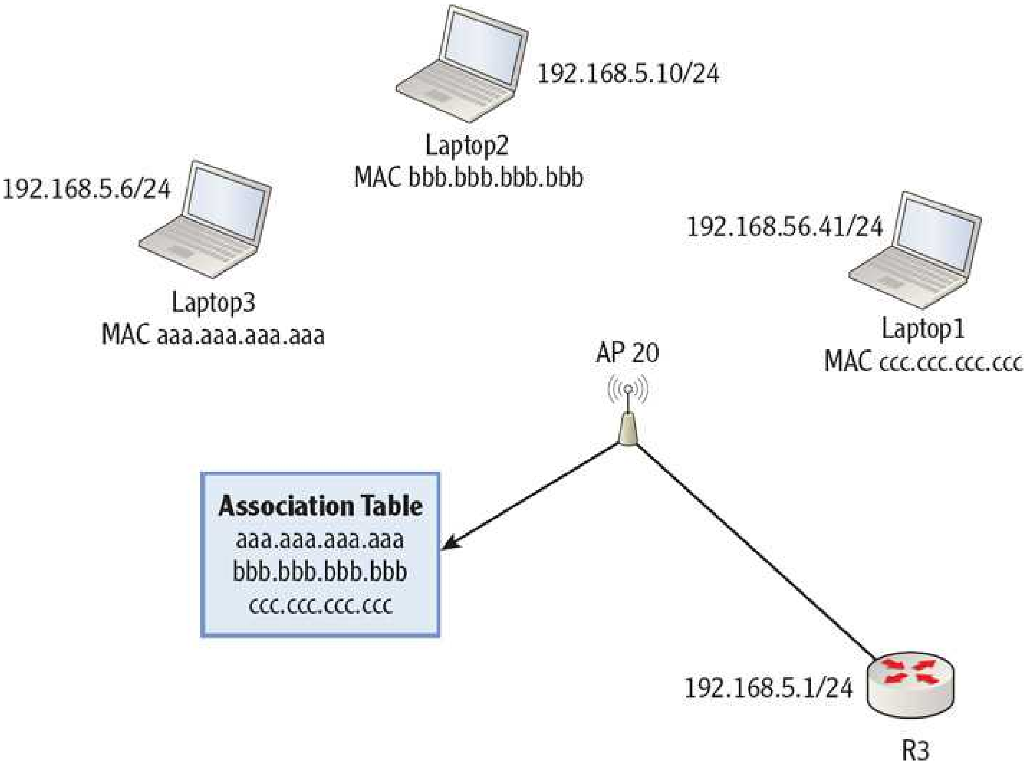


Figure 10.11: AP as a switch

When the AP is connected to a router that can provide routing, as shown in Figure 10.11, it is not necessary for the AP to be a router.

Wireless Routers

In some situations, it is beneficial or even required for the AP to also be a router. The best example of this is a wireless AP that provides access to the Internet in a home. In this situation, the wireless clients in the home will be using private IP addresses. Because these addresses cannot be used to access the Internet, those addresses must be converted to a public IP address using Network Address Translation. This is a function performed by a router.

Moreover, the AP in this situation will also probably be acting as a DHCP server for the wireless clients. Therefore, it will assign them a private IP address, maintain both the MAC address and the IP address in the association table, and when Internet access is required, it will convert the private IP address to a public IP address. This entire process is shown in Figure 10.12. When laptop 2 sends traffic to the Internet, the AP will convert the IP address 192.168.5.10/24 to the public IP address 202.62.31.9/24.

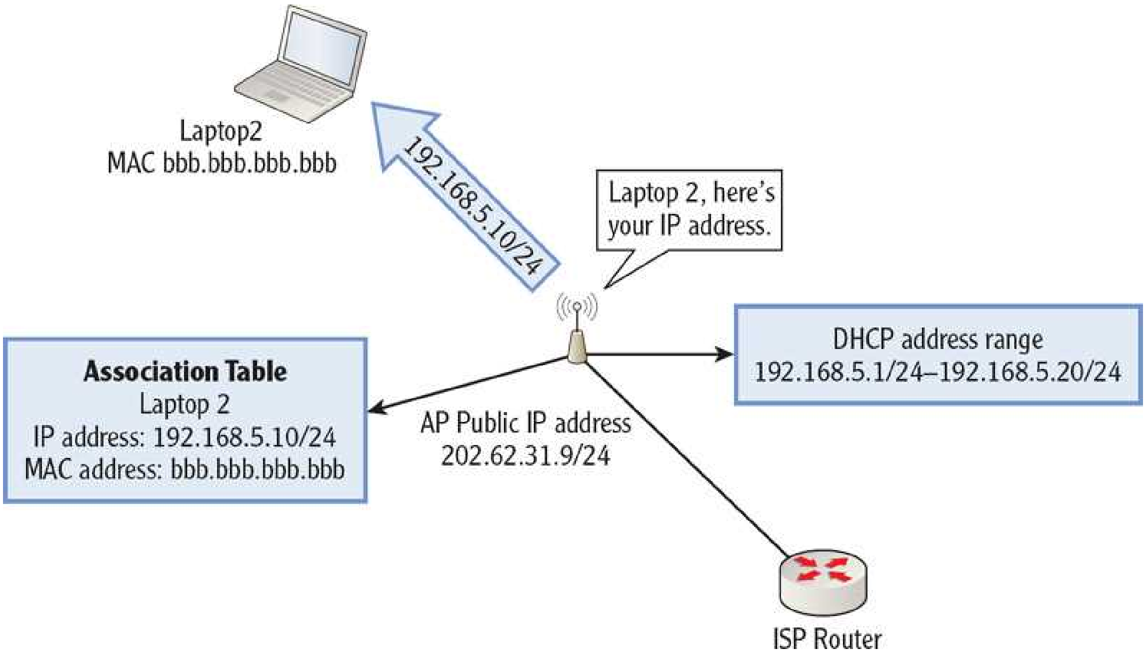


Figure 10.12: Wireless router

Regardless of whether the AP is acting as a switch only or as a wireless router, these devices are acting on the Access layer of the Cisco three-layer model.

Note The Cisco three-layer model is discussed at the end of this chapter.

Understanding Device Placement Principles

Once you understand the operations of the various devices and their roles in the network, it's time to put the pieces together. In this section, a review of collision and broadcast domains will be followed by a more complete description of the three-layer Cisco hierarchical model.

Defining Broadcast Domains

A *broadcast domain* is a set of devices that will receive one another's broadcast packets. If these devices have physical connectivity with one another and are in the same subnet, they are in the same broadcast domain. One of the main functions of routers is to separate or create broadcast domains. In Figure 10.13, the router has four interfaces, and each interface is a separate broadcast domain.

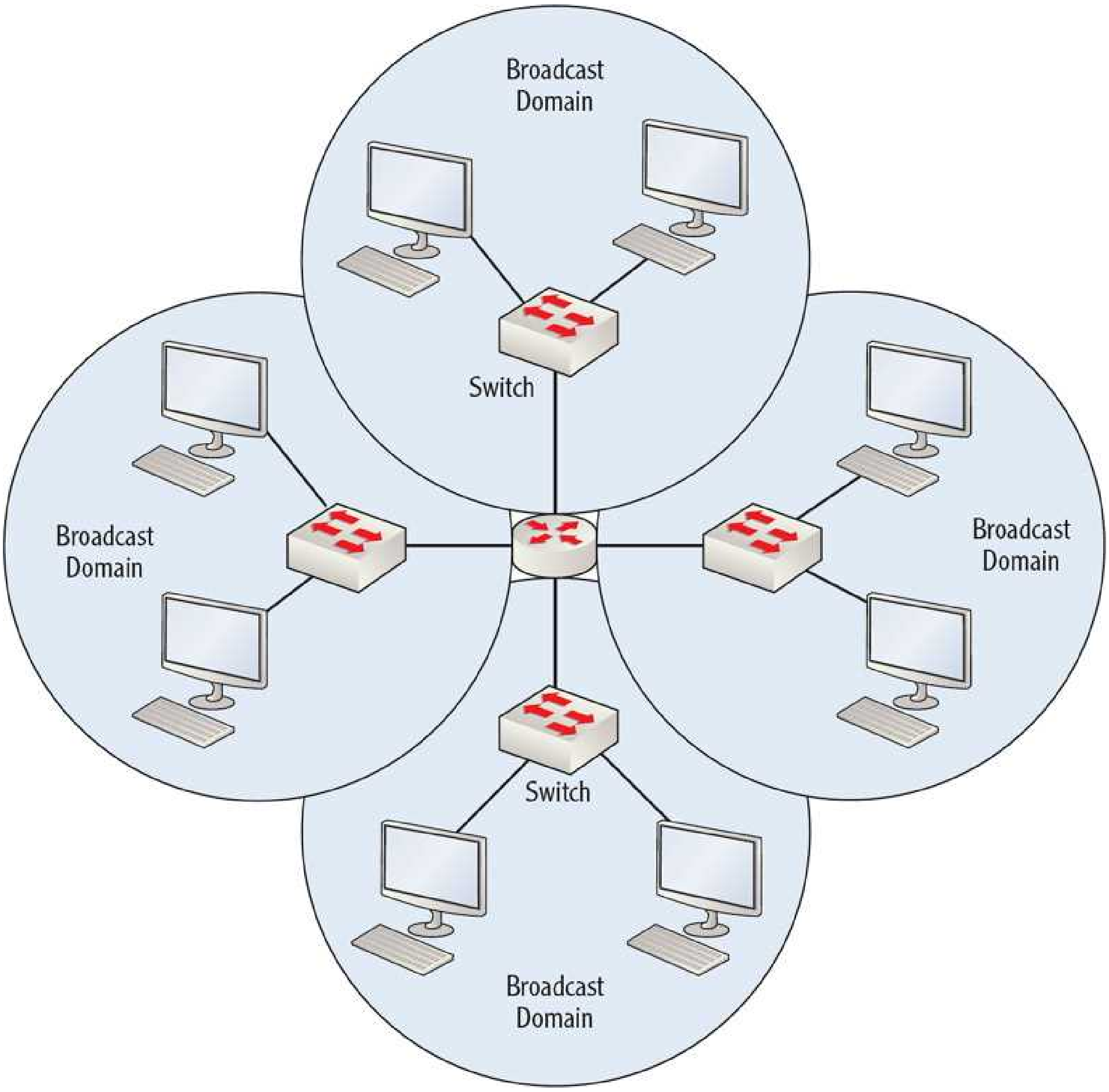


Figure 10.13: Broadcast domains

Creating broadcast domains is an integral part of the function of a router. If you attempt to put an IP address on a router interface that is in the same subnet as another interface on the same router, you will receive an error message. For example, if you tried to put an IP address on FastEthernet1 located in the same subnet as the IP address used on Fastethernet0/0, the error message would say `overlaps with FastEthernet0/0`. This basically means that you cannot do that. Each interface is supposed to host a different broadcast domain, which is not possible if they are in the same subnet. In Figure 10.13, hosts in one broadcast domain will never receive broadcast packets from other broadcast domains.

Defining Collision Domains

A *collision domain* is a set of devices whose packets could potentially collide with one another. By definition, devices that are in the same collision domain are also in the same broadcast domain. One of the purposes of a switch is to place each device in its own collision domain so that collisions are reduced. Because a hub cannot provide that, all devices connected to a hub are in the same collision domain. This relationship is illustrated in Figure 10.14.

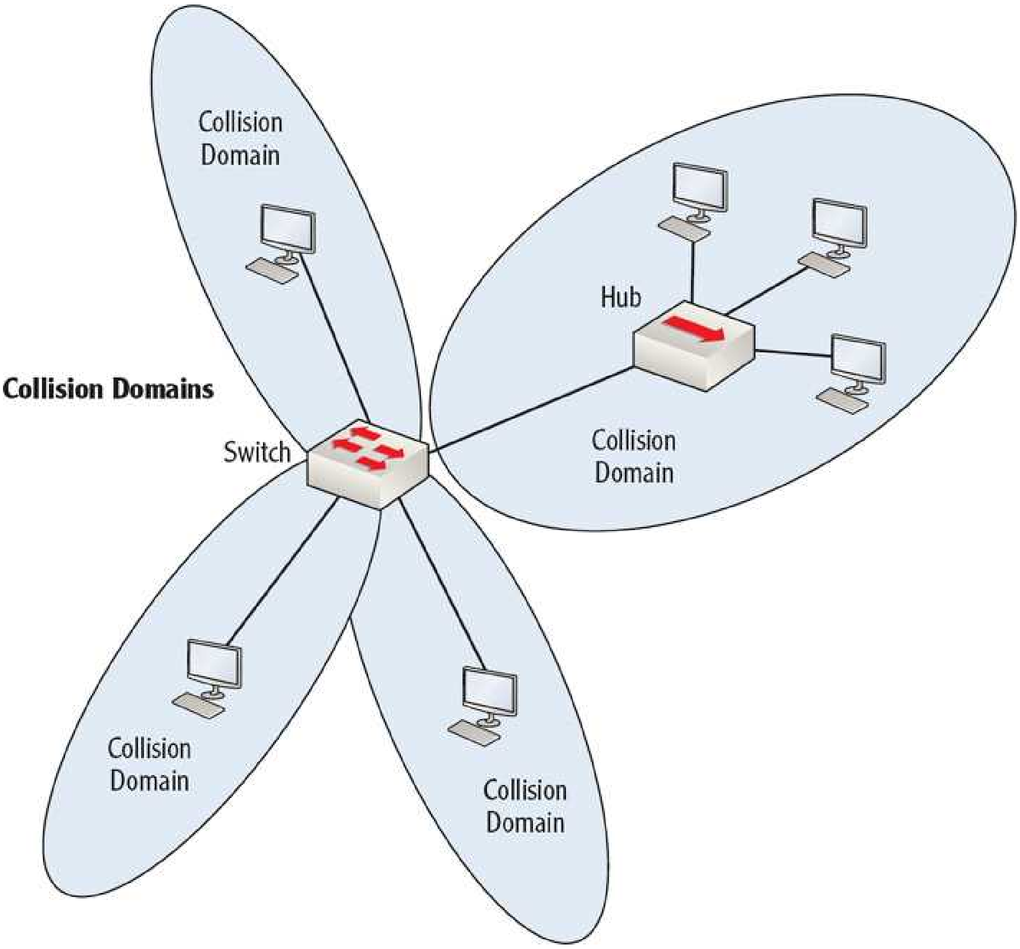


Figure 10.14: Collision domains

In this scenario, each switch port provides a collision domain. However, because a hub is connected into one switch port, and then three computers are connected into the hub, those three devices are forced to share the collision domain—in contrast to the other devices that have their own collision domains.

When we put the routers, switches, and hubs together in one network diagram, you can more easily grasp the relationship between collision and broadcast domains (see Figure 10.15).

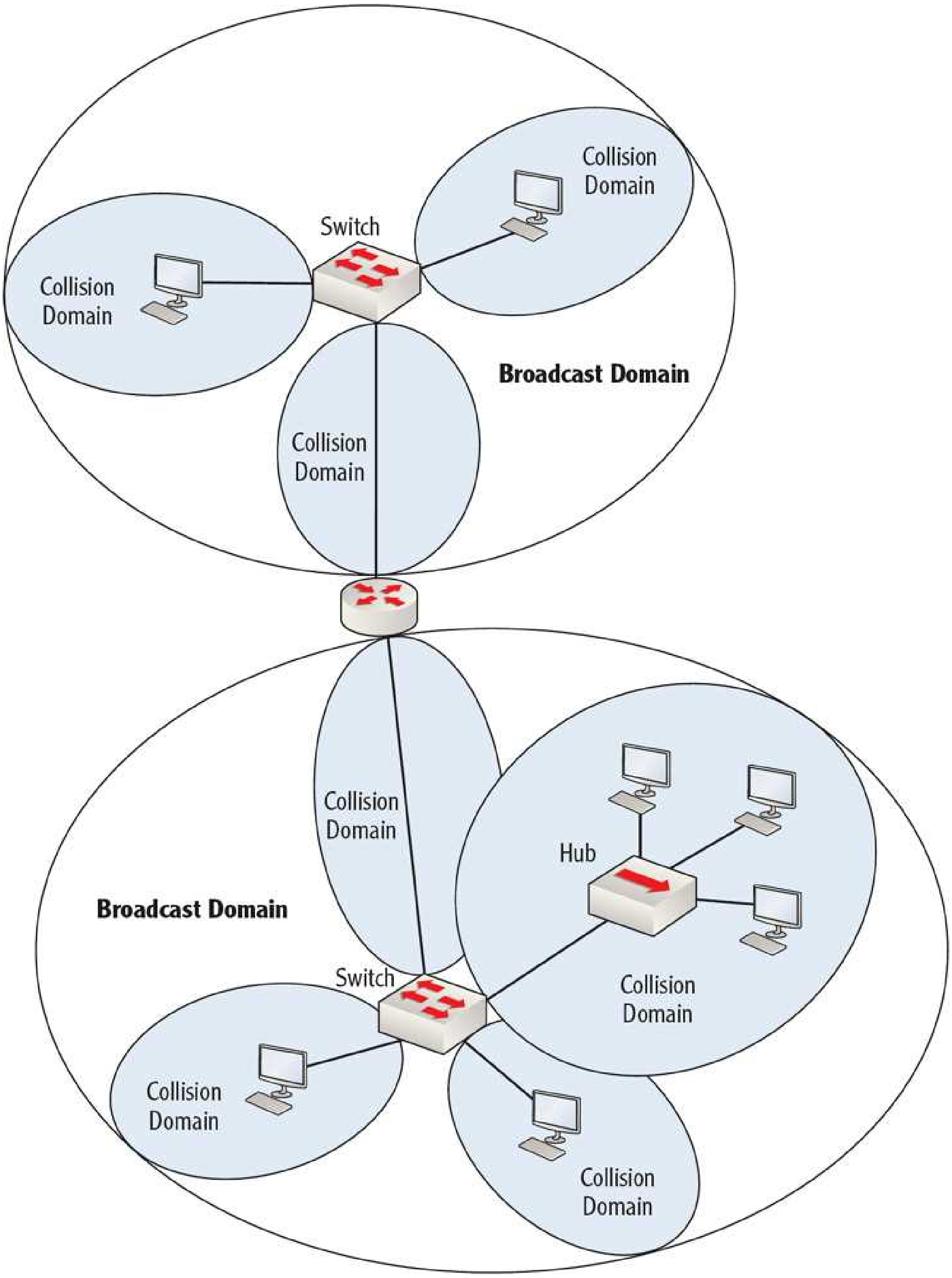


Figure 10.15: Collision and broadcast domains

Understanding the Cisco Three-Layer Model

The *Cisco three-layer model* is used to describe the way in which infrastructure devices such as routers and switches should be organized to maximize the performance and security of the network. Certain functions should be performed on certain levels, and certain devices should be placed on certain levels.

- **Access Layer** The access layer is the connection point for workstations, printers, wireless computers, and any other devices that operate on the network with an IP address. These devices usually make this connection via a switch, hub, and wireless AP or wireless router. This is also called the *network edge*.
- **Distribution Layer** This layer is where routers and multilayer switches connect the access switches together. This layer is typically where security is applied in the form of access control lists. It is also where the routing function takes place.

- **Core Layer** This is the backbone of the network, where the emphasis should be on speed. Functions that do anything to impede this goal, such as routing and security, should not be performed on this layer. Devices on this layer are usually high-speed multilayer switches. Fault tolerance is also important on this layer, because problems on this layer generally are felt across the entire network.

  The three layers and their relationships are shown in Figure 10.16.

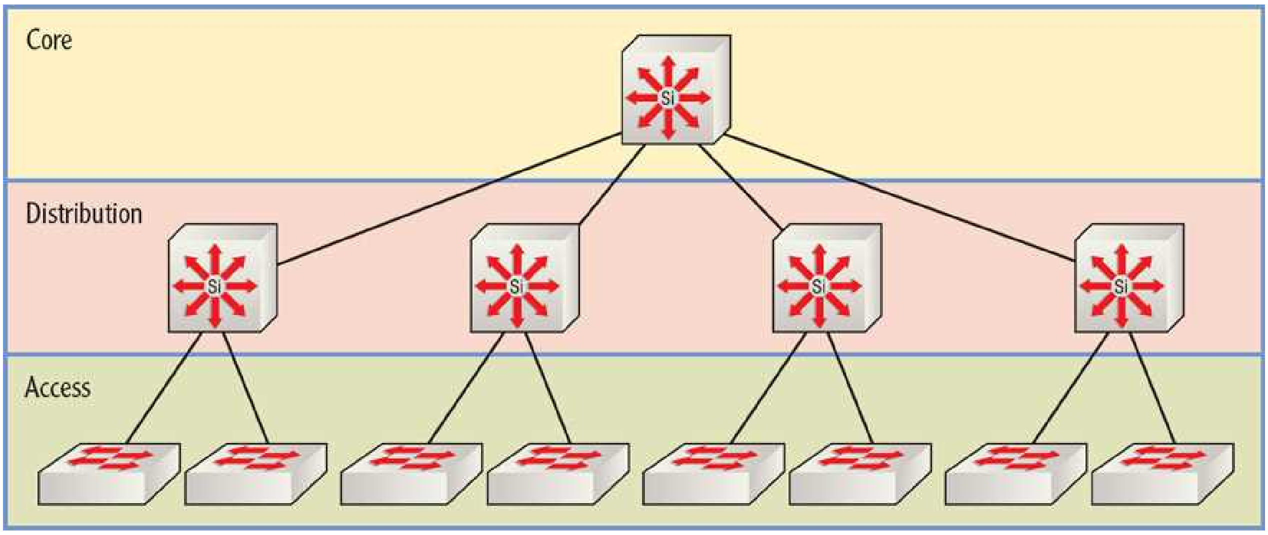


Figure 10.16: Three-layer model

The Essentials and beyond

Infrastructure devices are those devices that connect sections of the network together, such as repeater, hubs, bridges, and switches. Repeaters, hubs, and bridges operate at the Network Access layer. Repeaters amplify, or boost, the original signal. Hubs create a single collision domain for all ports. Bridges use MAC addresses to make forwarding decisions. Switches create a separate collision domain for each port. Multi-layer switches operate at both the Network Access and the Internet layers by performing routing and switching and can route the first packet and switch all of the other packets in the transmission. Routers operate at the Internet layer. Routers make routing decisions based on IP address information located in routing tables that can be populated either manually or by using dynamic routing protocols. Routers define broadcast domain borders at each interface of the router. Wireless access points can be either switches or routers, and depending on their function operate on the Network Access and Internet layers, respectively.

A broadcast domain is a set of devices that will receive one another's broadcast packet. A collision domain is a set of devices whose packets could potentially collide with one another. The Cisco three-layer model is used to describe the way in which infrastructure devices such as routers and switches should be organized to maximize the performance and security of the network. The model consists of an Access, Distribution, and Core layer.

Additional Exercises

1. Using Figure 10.17, determine the number of collision and broadcast domains in the network.

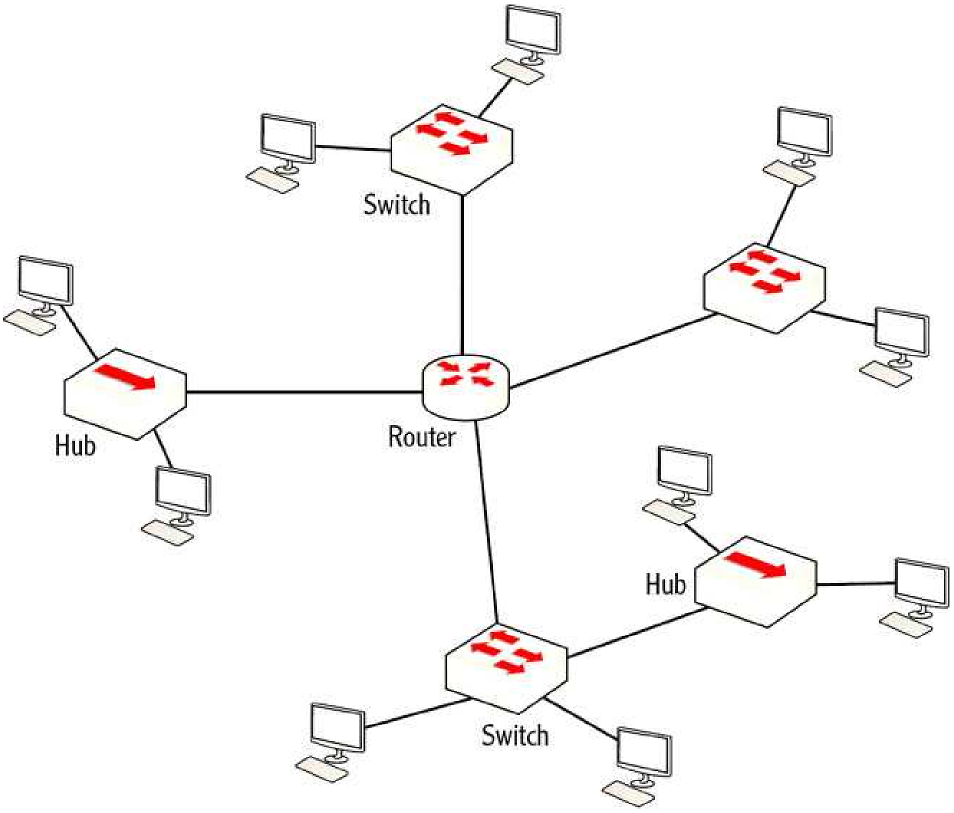


Figure 10.17: Domain exercise 1

2. Using Figure 10.18, label each of the seven domains as either collision or broadcast.

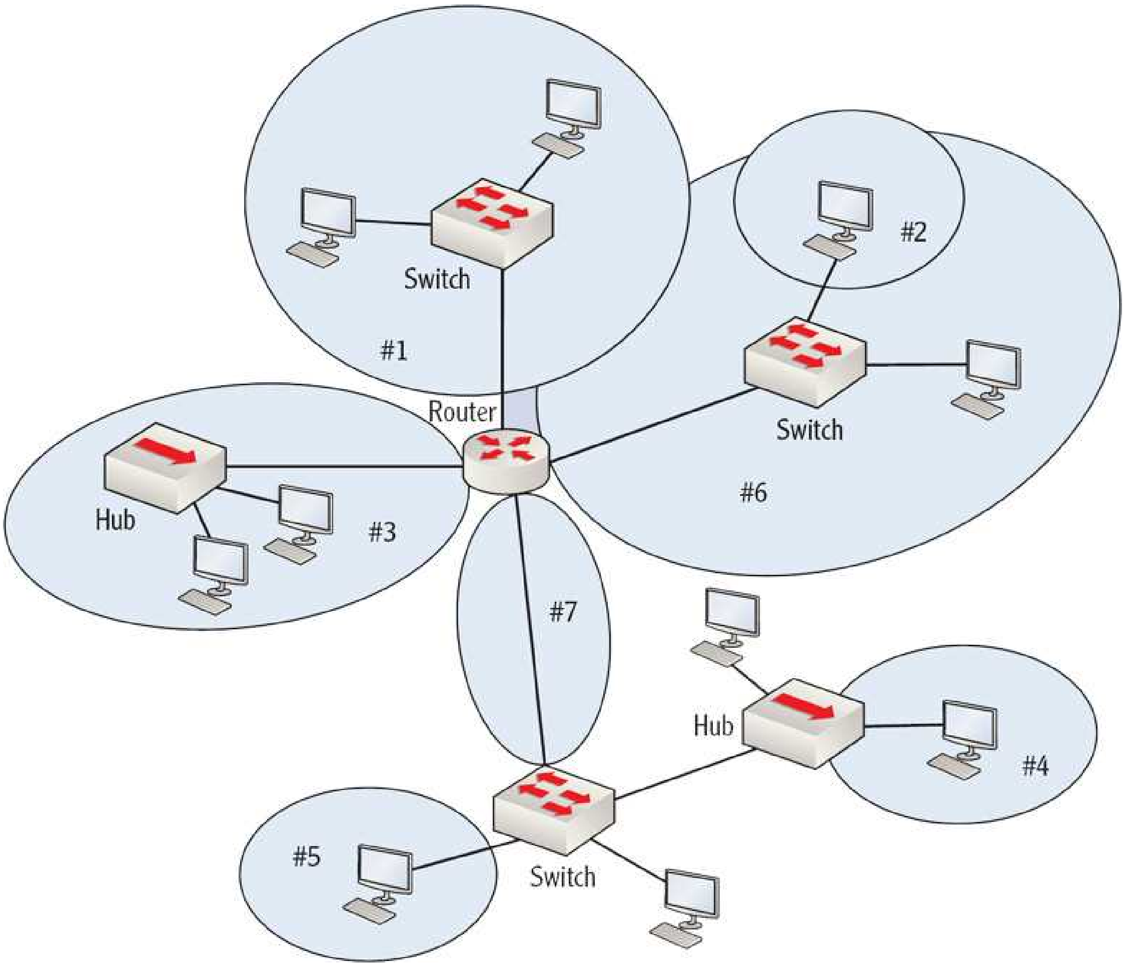


Figure 10.18: Domain exercise 2

Review Questions

1. Repeaters operate at which layer of the TCP/IP model?

   A. Internet

   B. Network Access

   C. Application

   D. Transport

2. What cable behavior are repeaters designed to mitigate?

   A. EMI

   B. RFI

   C. Crosstalk

   D. Attenuation

3. Which of the following devices operates on the Internet layer of the TCP/IP model?

   A. Repeater

   B. Hub

   C. Bridge

   D. Router

4. With which of the following devices are all of the ports in the same collision domain?

   A. Hub

   B. Bridge

   C. Switch

   D. Router

5. Which if the following is *not* an advantage of switches over bridges?

   A. MAC address learning

   B. Hardware bridging

   C. Port density

   D. More Spanning Tree instances

6. Which of the following is *not* a function of Network Access layer switches?

   A. IP address filtering

   B. MAC address learning

   C. Forward/filter decisions

   D. Loop avoidance

7. Which device operates on both the Network Access and the Internet layer?

   A. Switch

   B. Router

   C. MLS switch

   D. Bridge

8. Which of the following is *not* a type of route contained in a routing table?

A. Default

B. Multicast

C. Network

D. Host

9. What type of route is also known as the gateway of last resort?

A. Default

B. Multicast

C. Network

D. Host

10. Which of the following is *not* an advantage of using a dynamic routing protocol?

A. Less network traffic

B. Route fault tolerance

C. Best router selection

D. Automatic table population

Answers

1. **B** Repeaters operate at the Network Access layer.
2. **D** A repeater takes the original signal and amplifies, or boosts, the signal. After the signal has traversed a certain length of cable, the signal strength is gradually weakened by the resistance in the cable (which is called attenuation).
3. **D** Routers operate at the Internet layer of the TCP/IP model and make routing decisions based on IP address information.
4. **A** On hubs, all of the ports are on a shared network. They all exist in one collision domain.
5. **A** Both bridges and switches perform MAC address learning.
6. **A** Switches do not use IP address information for filtering.
7. **C** Multilayer switches perform routing and switching and thus operate on both the Network Access and the Internet layer.
8. **B** There are no multicast routes in a routing table.
9. **A** If a router is configured with a default route and you issue the command to show all routes (`show ip route`), this route will be referred to as the gateway of last resort.
10. **A** Dynamic routing protocols create more network traffic, because they send routing updates.