Switching Services

by Sophia

WHAT'S COVERED

In this lesson, you will learn about Layer 2 switch functions.

Specifically, this lesson will cover the following:

BEFORE YOU START

As, we have previously covered, Layer 2 switching is the process of forwarding frames using the hardware MAC addresses of devices on a LAN. We are now going to explore a more in-depth explanation of Layer 2 switching and how it works.

As discussed previously, a collision domain is a network segment sharing the same bandwidth, and switching breaks up large collision domains into smaller ones. Each port on a switch is its own collision domain, so you can create a much better Ethernet LAN by simply replacing legacy hubs with switches.

Switches truly have changed the way networks are designed and implemented. If a pure switched design is properly implemented, it will result in a high-performance, cost-effective, and resilient network.

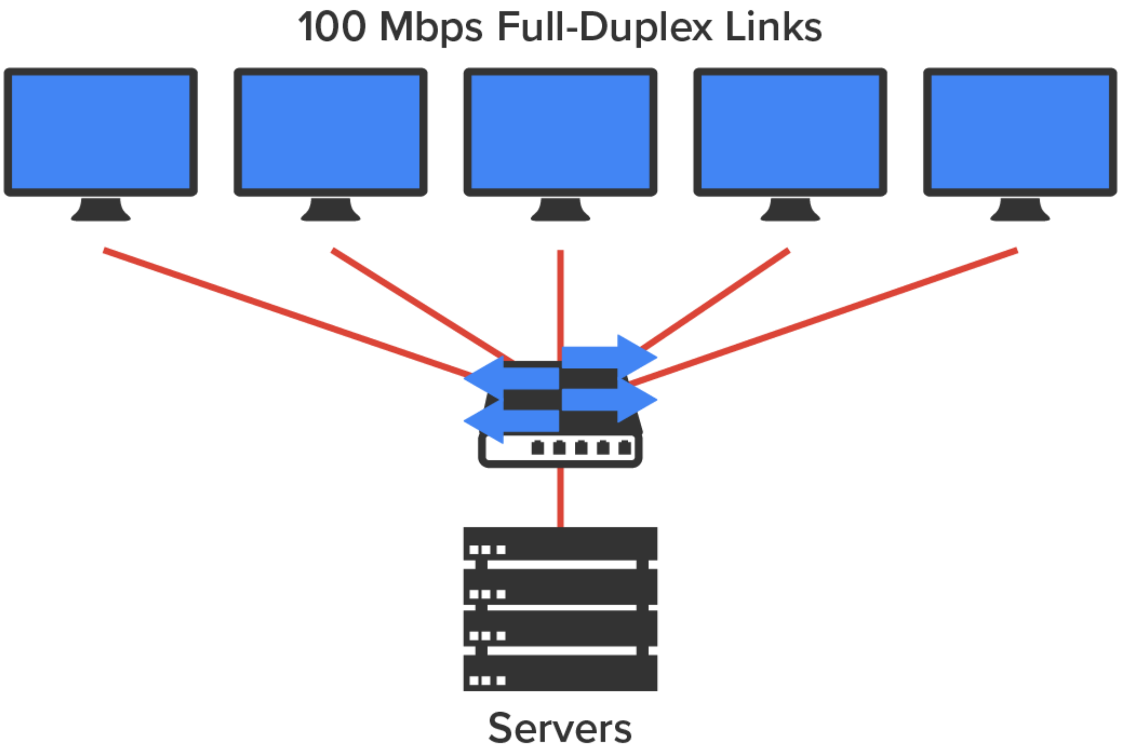
1. Switching Services

A Layer 2 switch is essentially a multiport bridge because its basic functions of forwarding frames based on MAC address and of breaking up collision domains are the same as those of a bridge. However, the mechanism for doing so differs. Legacy bridges use software to create and manage a filter table. In contrast, switches use **application-specific integrated circuits (ASICs)** to create and manage filter tables. An ASIC is an integrated circuit (IC) chip customized for a particular use.

KEY CONCEPT

Layer 2 switches and bridges are faster than routers because they don't take up time to look at the Layer 3 (network) header information. Instead, they look at the frame's hardware MAC addresses before deciding to forward, flood, or drop the frame.

Switches create private, dedicated collision domains and provide independent bandwidth on each port, unlike hubs. The diagram below shows five hosts connected to a switch. Unlike with a hub, each host has full-duplex, 100 Mbps of dedicated communication to the server.



KEY CONCEPT

Layer 2 switching provides the following benefits:

- Hardware-based bridging using ASICs
- Wire speed
- Low latency
- Low cost

What makes Layer 2 switching so efficient is that no modification to the data packet takes place. The device reads only the frame encapsulating the packet, which makes the switching process considerably faster and less error-prone than Layer 3 routing processes.

Layer 2 switching increases the bandwidth for each user because each port on the switch is its own collision domain.

TERM TO KNOW

Application-Specific Integrated Circuits (ASICs)

An integrated circuit (IC) chip customized for a particular use, rather than being intended for general-purpose use.

1a. Limitations of Layer 2 Switching

Switched networks break up collision domains, but remember that the network is really still one big broadcast domain. Neither Layer 2 switches nor bridges break up broadcast domains, which not only limits your network's size and growth potential but can also reduce its overall performance!

Broadcasts and multicasts along with the slow convergence time of spanning trees—network protocols that build a loop-free logical topology for Ethernet networks—can impact performance as your network grows. These are the major reasons Layer 2 switched networks need Layer 3 routers to facilitate connectivity between different networks.

1b. Three Switching Functions at Layer 2

KEY CONCEPT

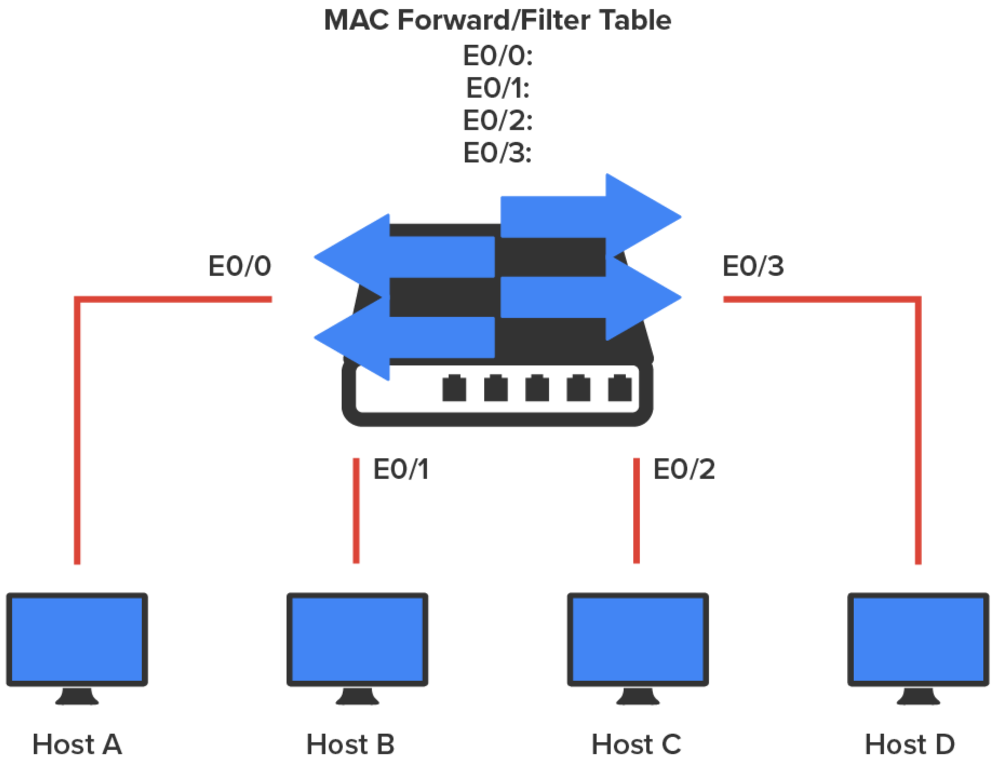
There are three distinct functions of Layer 2 switching:

- Address learning
- Forward/filter decisions
- Loop avoidance

We will discuss address learning and forward/filter decisions in this tutorial.

Address Learning

Layer 2 switches and bridges are capable of **address learning**; that is, they remember the source hardware address of each frame received on an interface (switch port) and enter this information into a MAC database known as a **forward/filter table**. When a switch is initially powered on, the MAC forward/filter table is empty, as shown in the diagram below.

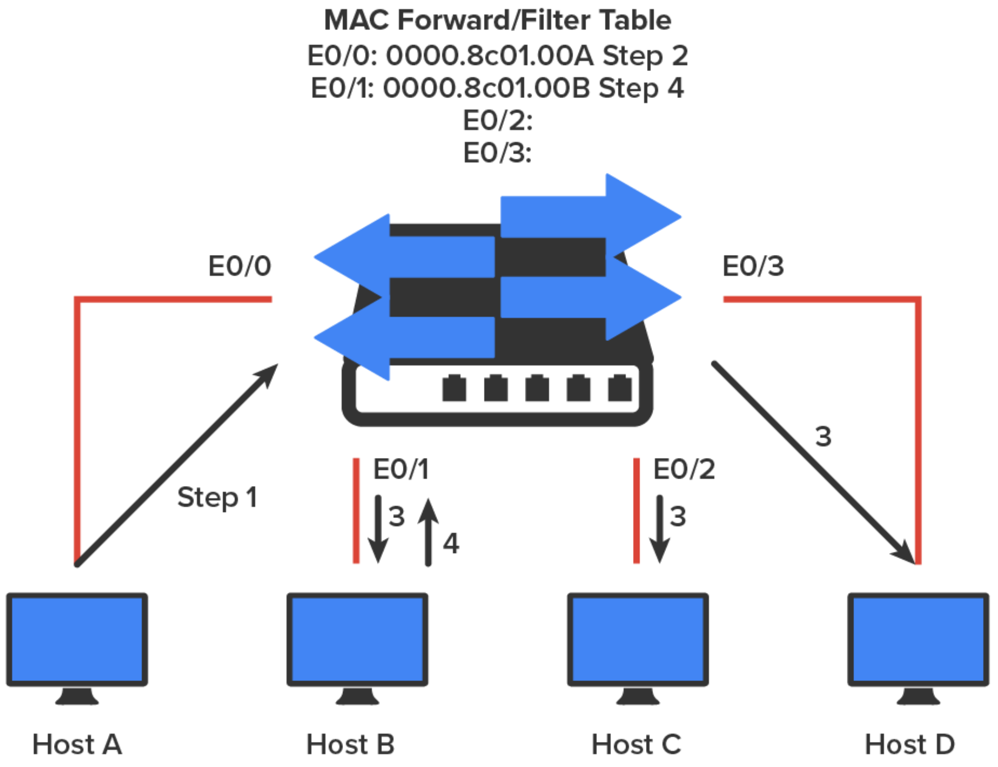


When a device transmits and an interface receives a frame, the switch places the frame’s source address in the MAC forward/filter table, which allows it to remember the interface on which the sending device is located. The switch then has no choice but to **flood** the network with this frame out of every port except the source port because it has no idea where the destination device is actually located.

If a device answers this flooded frame and sends a frame back, then the switch will take the source address from that frame and place that MAC address in its database as well, thereby associating the newly discovered address with the interface that received the frame.

Because the switch now has both of the relevant MAC addresses in its filtering table, the two devices can make a point-to-point connection. The switch doesn’t need to flood the frame as it did the first time because, now, the frames can and will be forwarded only between the two devices recorded in the table. This is exactly the thing that makes Layer 2 switches better than hubs because, in a hub network, all frames are forwarded out of all ports every time. The diagram below shows the processes involved in building a MAC database.

> EXAMPLE In the figure below, you can see four hosts attached to a switch. When the switch is powered on, it has nothing in its MAC address forward/filter table. However, when the hosts start communicating, the switch places the source hardware address of each frame in the table along with the port that the frame’s address corresponds to.



STEP BY STEP

Here is a step-by-step example of how a forward/filter table becomes populated:

1. Host A sends a frame to Host B. Host A's MAC address is 0000.8c01.000A, and Host B's MAC address is 0000.8c01.000B.
2. The switch receives the frame on the E0/0 interface and places the source address in the MAC address table, associating it with the port it came in on.
3. Because the destination address is not in the MAC database, the frame is forwarded (flooded) out of all interfaces except the source port.
4. Host B receives the frame and responds to Host A. The switch receives this frame on interface E0/1 and places the source hardware address in the MAC database, associating it with the port it came in on.
5. Host A and Host B can now make a point-to-point connection, and only the two devices will receive the frames. Hosts C and D will not see the frames, nor are their MAC addresses found in the database, because they haven't yet sent a frame to the switch.

If Host A and Host B do not communicate to the switch again within a certain amount of time, the switch will flush their entries from the database to keep it as current as possible.

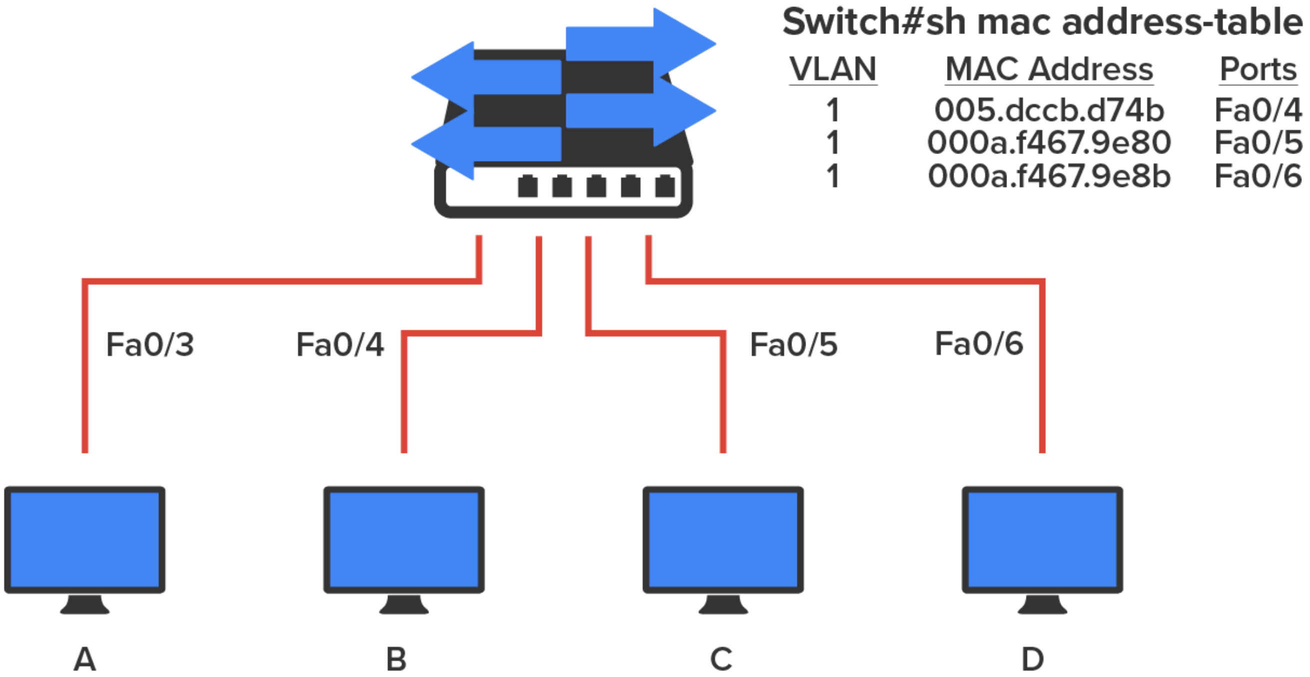
Forward/Filter Decisions

When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database, and the switch makes a forward/filter decision. In other words, if the destination hardware address is known (listed in the database), the frame is only sent out to the specified exit interface. The switch will not transmit the frame out of any interface except the destination interface. Not transmitting the frame preserves bandwidth on the other network segments and is called **frame filtering**.

HINT

> As mentioned earlier, if the destination hardware address isn’t listed in the MAC database, then the frame is flooded out to all active interfaces except the interface on which the frame was received. If a device answers the flooded frame, the MAC database is updated with the device’s location.
>
> So by default, if a host or server sends a broadcast on the LAN, the switch will flood the frame out of all active ports except the source port. Remember, the switch creates smaller collision domains, but it’s still one large broadcast domain by default.

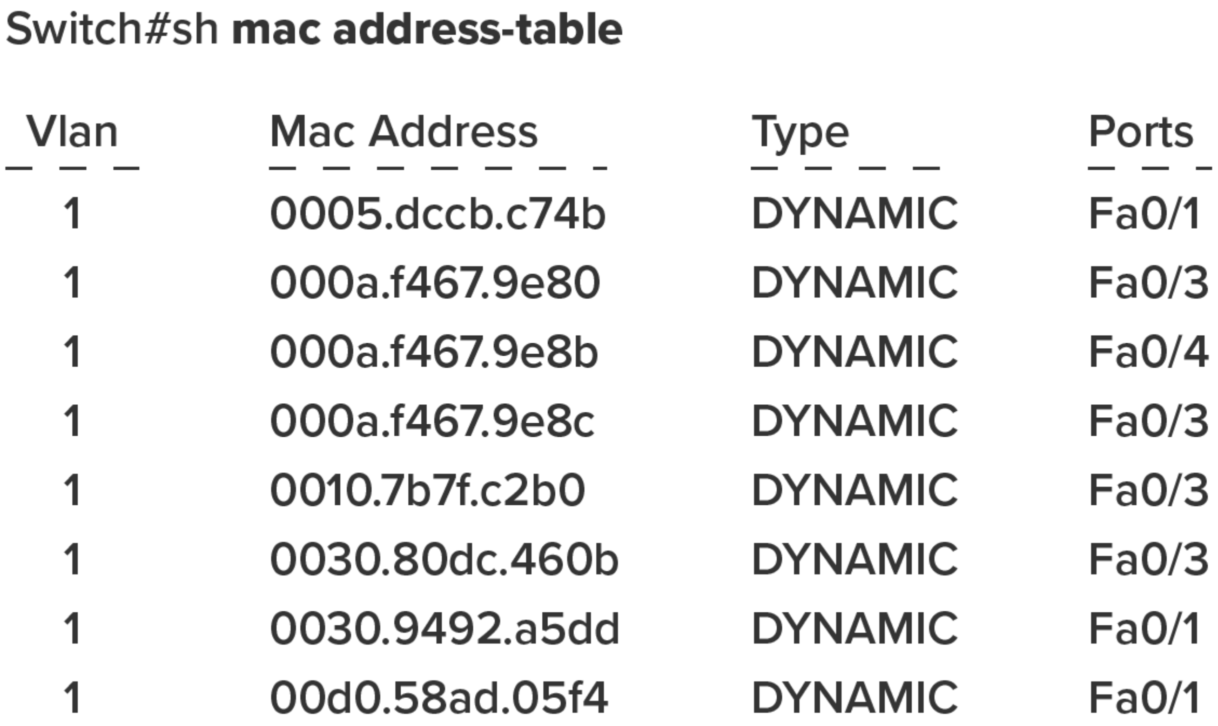
In the diagram below, you can see Host A sending a data frame to Host D. What will the switch do when it receives the frame from Host A?



```
Switch#sh mac address-table
VLAN     MAC Address        Ports
  1      005.dccb.d74b      Fa0/4
  1      000a.f467.9e80     Fa0/5
  1      000a.f467.9e8b     Fa0/6
```

If you answered that because Host A’s MAC address is not in the forward/filter table, the switch will add the source address and port to the MAC address table and then forward the frame to Host D, you’re halfway there. If you also came back with, “If Host D’s MAC address were not in the forward/filter table, the switch would have flooded the frame out of all ports except for port Fa0/3,” then congratulations—you nailed it!

Let’s take a look at the output of a “show mac address-table” command as seen from a Cisco Catalyst switch. (The MAC address table works pretty much exactly the same on all brands of switches.)



```
Switch#sh mac address-table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  1     0005.dccb.c74b    DYNAMIC     Fa0/1
  1     000a.f467.9e80    DYNAMIC     Fa0/3
  1     000a.f467.9e8b    DYNAMIC     Fa0/4
  1     000a.f467.9e8c    DYNAMIC     Fa0/3
  1     0010.7b7f.c2b0    DYNAMIC     Fa0/3
  1     0030.80dc.460b    DYNAMIC     Fa0/3
  1     0030.9492.a5dd    DYNAMIC     Fa0/1
  1     00d0.58ad.05f4    DYNAMIC     Fa0/1
```

Now, suppose the preceding switch received a frame with the following MAC addresses:

```
Source MAC: 0005.dccb.d74b
Destination MAC: 000a.f467.9e8c
```

THINK ABOUT IT

How will the switch handle this frame? The right answer is that the destination MAC address will be found in the MAC address table and the frame will be forwarded out of Fa0/3 only. Remember that if the destination MAC address is not found in the forward/filter table, it will forward the frame out of all ports of the switch looking for the destination device.

Now that you can see the MAC address table and how switches add hosts' addresses to the forward/filter table, how do you stop switching loops if you have multiple links between switches? Let's talk about this possible problem in more detail.

TERMS TO KNOW

Address Learning

The process of a switch storing the source hardware MAC address of each frame received on an interface (switch port) in a forward/filter table.

Forward/Filter Table

A dynamic table that maps MAC addresses to switch ports.

Flood

The transmission of a frame out of every port except the source port when the location of the destination device is unknown.

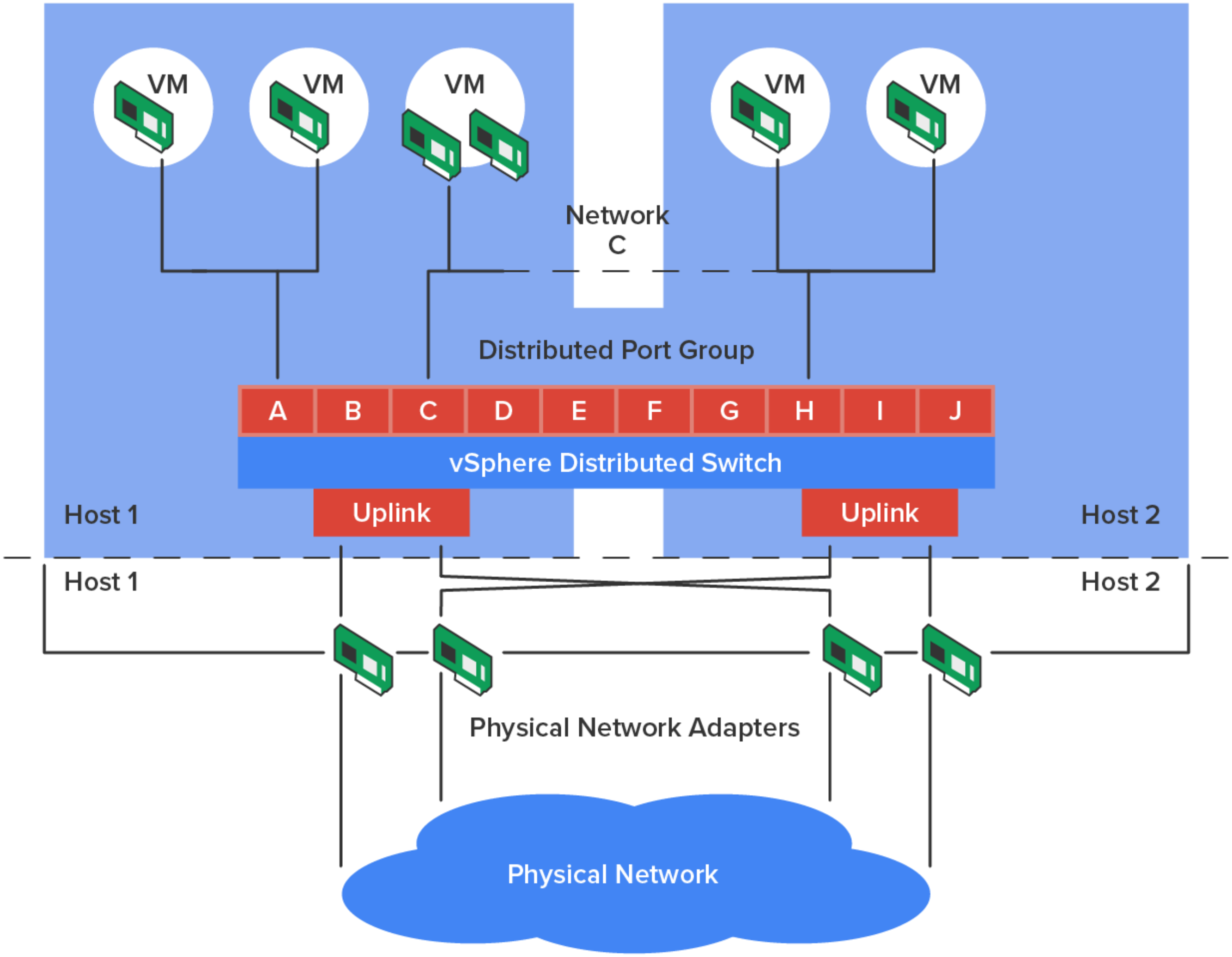
Frame Filtering

The forwarding of a frame to a single switch port where the destination device resides.

1c. Distributed Switching

In a virtual environment such as those you might find in many of today's data centers, not only are virtual servers used in place of physical servers, but virtual switches (software based) are used to provide connectivity between the virtual systems. These virtual servers reside on physical servers that are called hosts (but in a different context from network hosts). The virtual switches can be connected to a physical switch to enable access to the virtual servers from the outside world.

One of the unique features of these virtual switches is the ability of the switches to span multiple physical hosts. When this is done, the switch is called a **distributed switch**. This provides connectivity between virtual servers that are located on different hosts, as shown in the diagram below.



TERM TO KNOW

Distributed Switch

A switch that provides connectivity between virtual servers that are located on different hosts.

SUMMARY

In this lesson, you learned about Layer 2 switch functions, including **switching services**; some **limitations of Layer 2 switching**; and the **three switching functions**, including address learning and forward/filter decisions. You were also introduced to the concept of **distributed switching**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Address Learning

The process of a switch storing the source hardware MAC address of each frame received on an interface (switch port) in a forward/filter table.

Application-Specific Integrated Circuits (ASICs)

An integrated circuit (IC) chip customized for a particular use, rather than being intended for general-purpose use.

Distributed Switch

A switch that provides connectivity between virtual servers that are located on different hosts.

Flood

The transmission of a frame out of every port except the source port when the location of the destination device is unknown.

Forward/Filter Table

A dynamic table that maps MAC addresses to switch ports.

Frame Filtering

The forwarding of a frame to a single switch port where the destination device resides.