**EXAM PREPARATION**

**I, QUESTIONS:**

* **TCP/IP model**

Given a scenario, e.g. retrieving a web page or sending/receiving an email, then questions about TCP/IP model, the layers, protocols, etc. with respect to the given scenario.

**Definition of TCP/IP**

TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private computer network (an intranet or an extranet).

**TCP**

TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

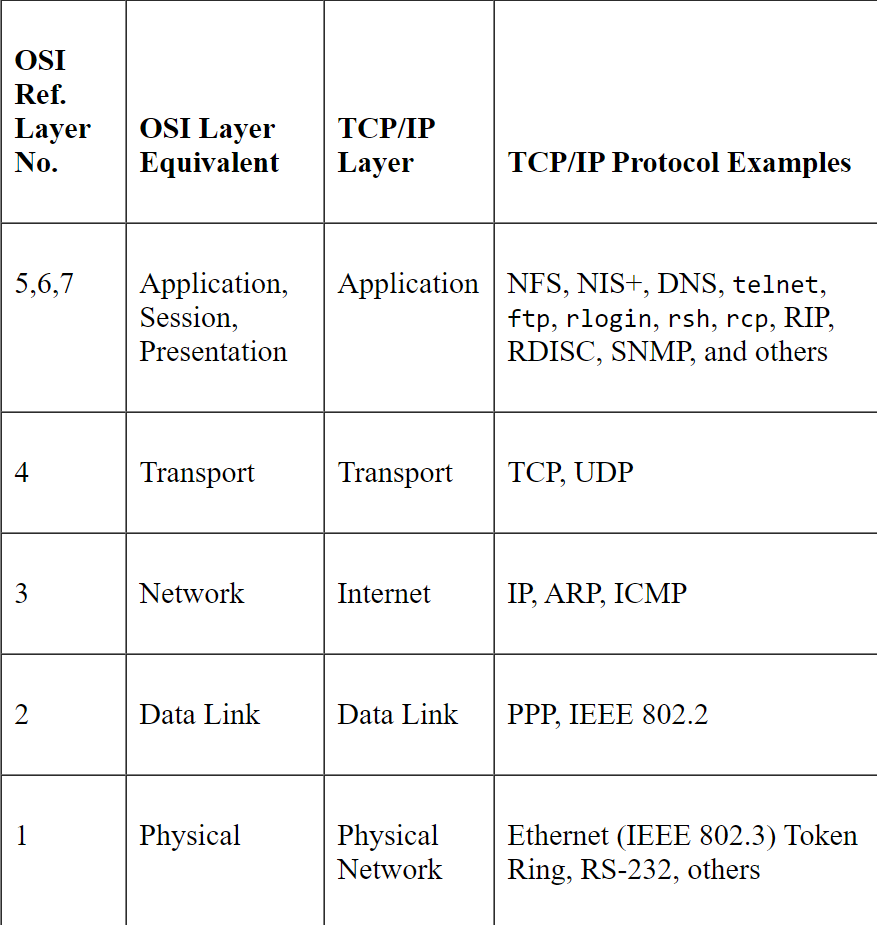
**IP**

IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

**IP is responsible for:**

* **IP addressing** - The IP addressing conventions are part of the IP protocol. (Chapter 5, Planning Your TCP/IP Network describes IPv4 addressing in detail and Chapter 14, Overview of IPv6 describes IPv6 addressing in detail.)
* **Host-to-host communications** - IP determines the path a packet must take, based on the receiving host's IP address.
* **Packet formatting** - IP assembles packets into units known as IP datagrams. Datagrams are fully described in "Internet Layer".
* **Fragmentation** - If a packet is too large for transmission over the network media, IP on the sending host breaks the packet into smaller fragments. IP on the receiving host then reconstructs the fragments into the original packet.

**Common protocols of TCP/IP:**



* **HTTP (Hyper Text Transfer Protocol)** handles the communication between a web server and a web browser.
* **HTTPS (Secure HTTP)** handles secure communication between a web server and a web browser.
* **FTP (File Transfer Protocol)** handles transmission of files between computers.

**TCP/IP model layers**

TCP/IP functionality is divided into **4 layers**, each of which include specific protocols:

* **The application layer** provides applications with standardized data exchange. Its protocols include the **HTTP, FTP, Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).** At the application layer, the payload is the actual application data.
  + **Secure Shell (SSH), File Transfer Protocol (FTP), Telnet**: For peer-to-peer file sharing, and, in Telnet's case, logging into another user's computer to access a file.
  + **Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP)**: For sending and receiving email
  + **HTTP**: For web access
  + **HTTP and HTTPS** – HTTP is used by the World Wide Web to manage communications between web browsers and servers. HTTPS is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
  + **SSH – SSH stands for Secure Shell**. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
* **NTP – NTP stands for Network Time Protocol**. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions.
* **FTP - File Transfer Protocol,** transfers files to and from a remote network.FTP enables a user to specify the name of the remote host and file transfer command options on the local host's command line.
* **Telnet** - The Telnet protocol enables terminals and terminal-oriented processes to communicate on a network running TCP/IP. Telnet provides a user interface through which two hosts can communicate on a character-by-character or line-by-line basis.
* **The transport layer** is responsible for maintaining **end-to-end**, **host-to-host** communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include **TCP and User Datagram Protocol (UDP),** which is sometimes used instead of TCP for special purposes.

**TCP Protocol**

* + TCP enables applications to communicate with each other as though connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discreet packets.
  + TCP attaches a header onto the transmitted data.
  + TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts.

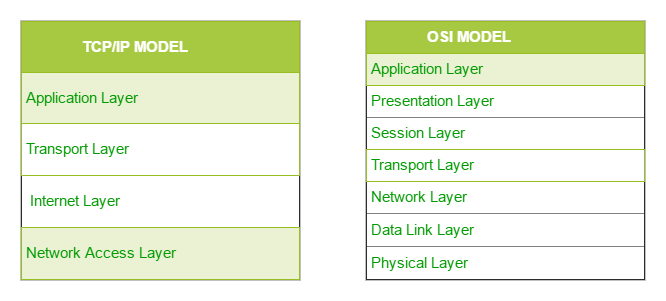
**UDP Protocol**

* UDP, the other transport layer protocol, provides datagram delivery service.
* It does not provide any means of verifying that connection was ever achieved between receiving and sending hosts.
* Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use it rather than TCP.
* **The network layer**, also called **the internet layer**, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the **IP and the Internet Control Message Protocol (ICMP), which is used for detecting network error conditions and reporting on them.**
* **The physical layer**, also known as **the network interface layer or data link layer, network access,** consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this lowest layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

**TCP services**

**Domain Name System - The Domain Name System (DNS)** provides host names to the IP address service. It also serves as a database for mail administration.

**Comparison with OSI (Open Systems Interconnection)**



**The similarities**

* They are both logical models.
* They define networking standards.
* They divide the network communication process in layers.
* They provide frameworks for creating and implementing networking standards and devices.
* They enable one manufacturer to make devices and network components that can coexist and work with the devices and components made by other manufacturers.

**The differences**

* **TCP/IP** uses just one layer (application) to define the functionalities of the upper layers, while the **OSI** model uses three layers (application, presentation and session).
* **TCP/IP** is more reliable than **OSI**
* The **TCP/IP** model uses one layer (link) to define the functionalities of the bottom layers, while the **OSI** uses two layers (physical and data link).
* The **TCP/IP** model use the internet layer to define the routing standards and protocols, while **OSI** uses the network layer.
* The **TCP/IP** header size is 20 bytes while the **OSI** header is 5 bytes.
* The **TCP/IP** model is a protocol-oriented standard, whereas the **OSI** model is a generic model based on the functionalities of each layer.
* **TCP/IP** follows a horizontal approach, while **OSI** follows a vertical approach.
* In the **TCP/IP** suite, the protocols were developed first, and then the model was developed. In **OSI**, the model was developed first, and then the protocols in each layer were developed.
* **TCP/IP** helps establish a connection between different types of computers, whereas the **OSI** model helps standardize routers, switches, motherboards and other hardware.
* **Ethernet switching**

Given a network, how a switch builds (self-learns) MAC address table, how it makes forwarding decisions …

* **Encapsulation and de-encapsulation**

What is it? How is it done?

* **ARP**

Given a network, how ARP works

The Address Resolution Protocol (ARP) conceptually exists between the data link and Internet layers. ARP assists IP in directing datagrams to the appropriate receiving host by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

* **IPv4 addresses**

Given an IPv4 address and the subnet mask, figure out relevant information about its network, e.g. network address, broadcast address, usable host addresses, number of hosts.

* **IPv4 address related question**

Questions related to key concepts such as subnet masks, number of hosts etc.

* **Identify configuration issues**

Given a network topology diagram and IPv4 address information for devices in the network, identify errors regarding the configuration, and provide solutions to fix the problems.

* **Functions of transport layer protocols and how they work, e.g. for tracking individual conversations etc.**

**II, ANSWERS:**

**TCP/IP Communication Process**

1. Web server prepares the HTML page as data to be sent

2.  The application protocol HTTP header is added to the front of the HTML data (header contains various information, including the HTTP version the server is using and a status code indicating it had information for the web client).

3.  The HTTP application layer protocol delivers the HTML to the transport layer. The TCP transport layer protocol is used to manage individual conversations.

4.  IP information is added to the front of the TCP information. IP assigns the appropriate source and destination IP addresses → known as IP packet

5.  Ethernet protocol adds information to both ends of the IP packet → known as data link frame. Frame is delivered to the nearest router along the path towards the web client. This router removes the Ethernet connection, analyses IP packet, determines the best path for the packet, inserts the packet into a new frame, and sends it to the next neighboring router towards the destination. Each router removes and adds new data link information before forwarding the packet.

6.  This data is now transported through the internetwork (media and intermediary devices)

7.  Client receives the data link frames that contain the data. Each protocol header is processed and then removed in the opposite order it was added. Ethernet information is processed and removed, followed by IP protocol information, the TCP information and finally the HTTP info.

 8.  The web page information is then passed on to the client’s web browser software.

**Well-known protocols and their purposes**

DNS → Domain Name System (or Service): Translates domain names into IP address

BOOTP → Bootstrap Protocol: Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. Is being superseded by DHCP

DHCP → Dynamic Host Configuration Protocol: Dynamically assigns IP addresses to client stations at start-up. Allows address to be re-used when no longer needed.

SMTP → Simple Mail Transfer Protocol: Enables clients to send email to a mail server. Enables servers to send email to other servers.

POP → Post Office Protocol version 3 (POP3): Enables clients to retrieve email from a mail server. Downloads email from the mail server to the desktop.

IMAP → Internet Message Access Protocol: Enables clients to access email stored on a mail server. Maintains email on the server.

FTP → File Transfer Protocol: Sets rules that enable a user on one host to access and transfer file to and from another host over a network. Reliable, connection-oriented, and acknowledged file delivery protocol.

TFTP → Trivial File Transfer Protocol: Simple, connectionless file transfer protocol. A best-effort, unacknowledged file delivery protocol. Utilizes less overhead then FTP.

HTTP → Hypertext Transfer Protocol: Set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the www. Transport Layer

UDP → User Datagram Protocol: Enables a process running on one host to send packets to a process running on another host. Does not confirm successful datagram transmission.

TCP → Transmission Control Protocol: Enables reliable communication between processes running on separate hosts. Reliable, acknowledged transmissions that confirm successful delivery. Internet Layer IP → Internet Protocol Receives message segments from the transport layer. Packages messages into packets. Addresses packets for end-to-end delivery over an Internetwork.

NAT → Network Address Translation: Translates IP addresses from a private network into globally unique public IP addresses

ICMP → Internet Control Message Protocol: Provides feedback from a destination host to a source host about errors in packet delivery

OSPF → Open Shortest Path First: Link-state routing protocol. Hierarchal design based on areas. Open standard interior routing protocol.

EIGRP → Enhanced Interior Gateway Routing Protocol: Cisco proprietary routing protocol. Uses composite metric based on bandwidth, delay, load and reliability.  Network Access Layer

ARP → Address Resolution Protocol: Provides dynamic address mapping between an IP address and a hardware address.

PPP → Point-to-Point Protocol: Provides a means of encapsulating packets for transmission over a serial link

Ethernet: Defines the rules for wiring and signaling standards of the network access layer Interface Drivers Provides instruction to a machine for the control of a specific interface on a network device.

**How an Ethernet switch works**

An Ethernet Switch is a Layer 2 device.

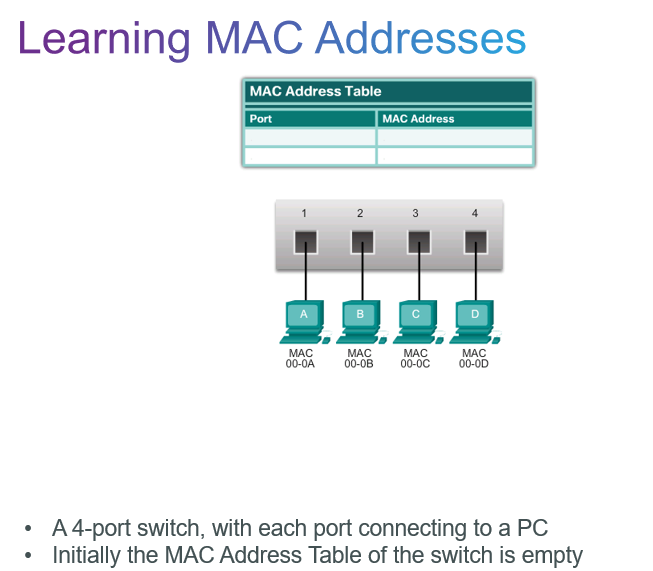
It uses MAC addresses to make forwarding decisions.

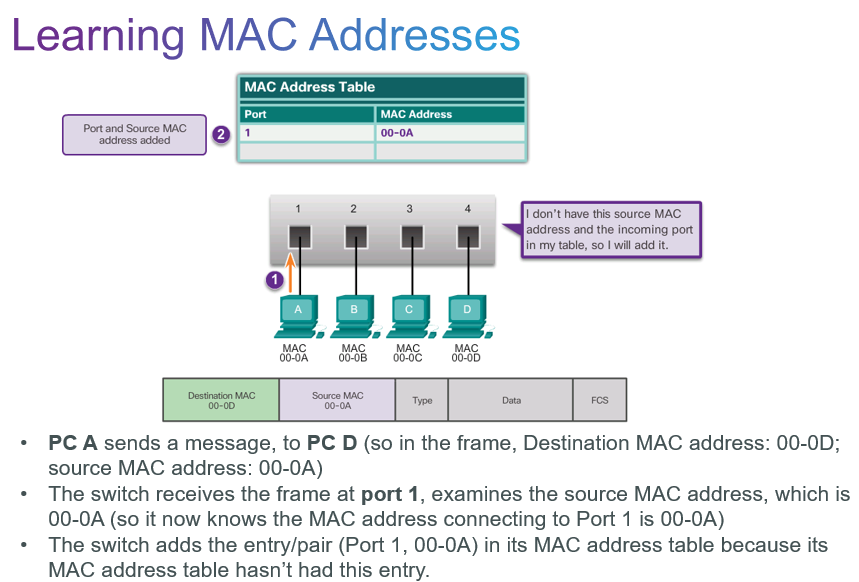
The MAC address table is sometimes referred to as a content addressable memory (CAM) table.

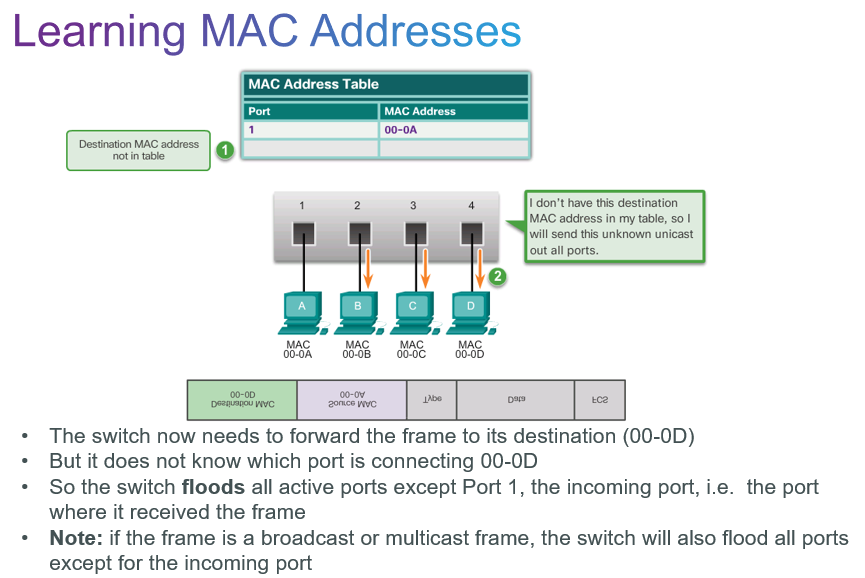
An Ethernet Switch creates its MAC address table through “self-learning”, by examining the source MAC address of the frames received on a port.

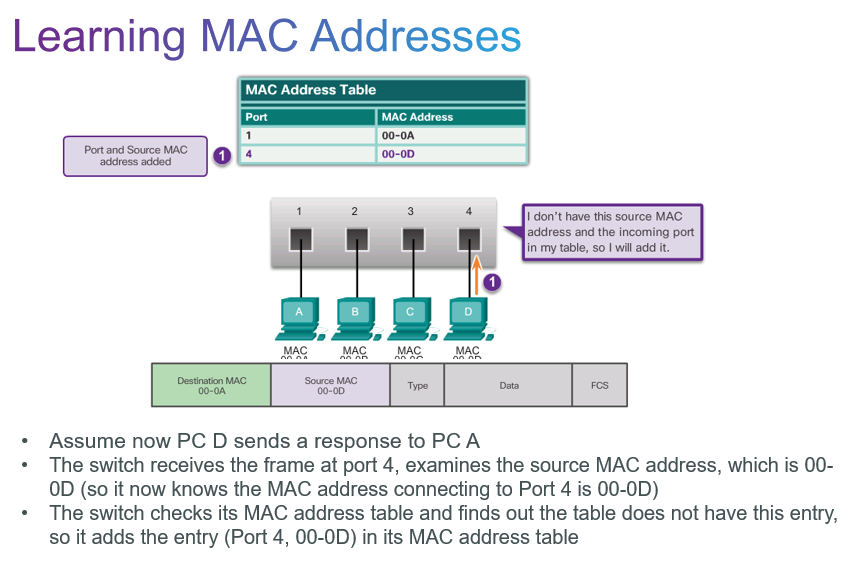
The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.

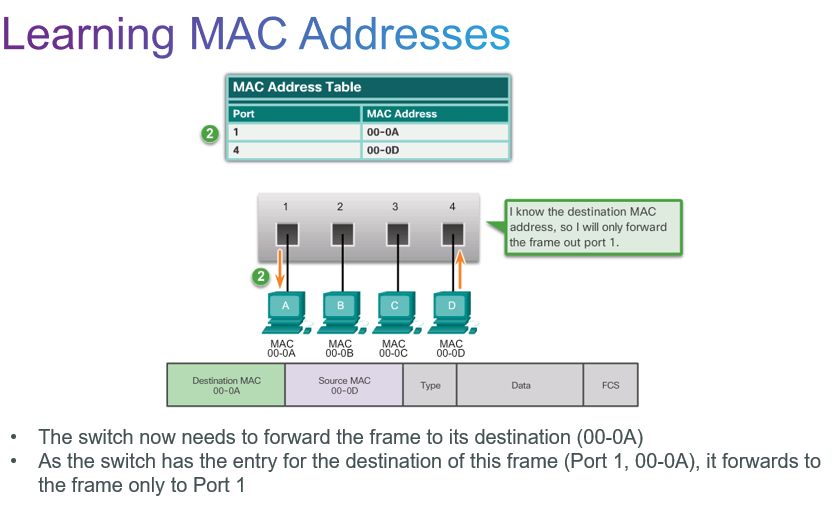
**Self-learning**

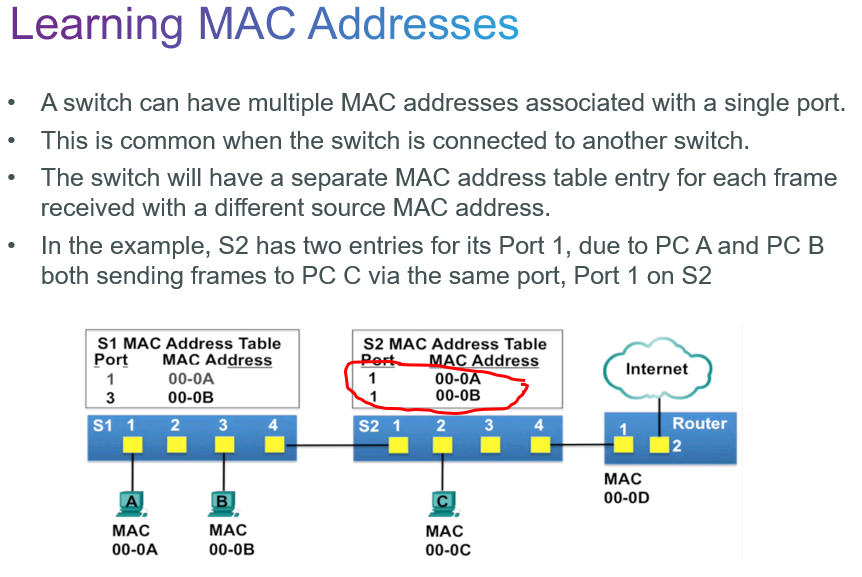












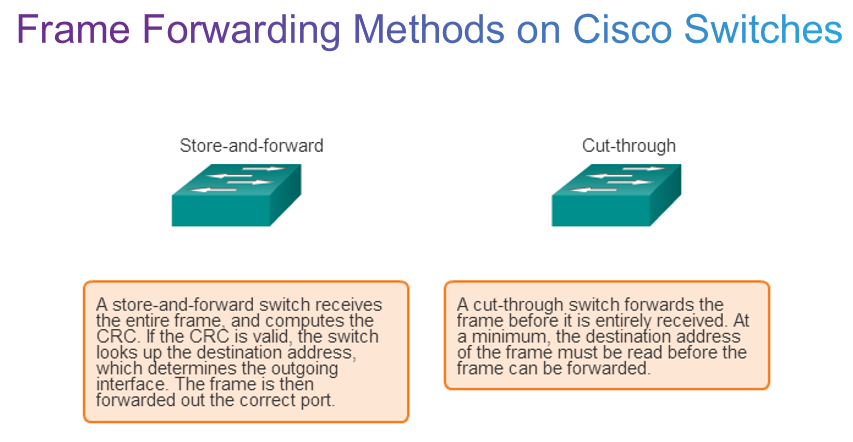
**Frame-forward decision**

Every frame that enters a switch is checked for new information to learn, by examining the frame’s source MAC address and the incoming port number.

* If the source MAC address does not exist in the table, it is added to the table along with the incoming port number.
* If the source MAC address does exist and the incoming port is the same, the switch keeps the entry and updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for 5 minutes.
* Note: If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address but with the more current port number.

To forward the received frame,

* When the switch’s MAC address table contains the destination MAC address, it will forward the frame out the specified port.
* When the switch MAC address table does not contain the destination MAC address, the switch will flood all ports except the incoming port.



Cut-through switching is the predominant switching method used on Cisco switches.

Two types of cut-through switching:

* Fast-forward switching: Lowest level of latency immediately forwards a packet after reading the destination address.
* Typical cut-through method of switching.

  Fragment-free switching:

* Switch stores the first 64 bytes of the frame before forwarding.
* Most network errors and collisions occur during the first 64 bytes.

**Memory Buffering**

