Switching:

- learn the source mac address.
- forward according to destination mac address.

How Switching Works:

- **Packet Forwarding:** When a switch receives a data packet, it examines the destination MAC address in the packet header.
- **MAC Address Table:** The switch maintains a MAC address table, also known as a forwarding table or CAM table, which maps MAC addresses to the ports on the switch.
- **Forwarding Decision:** Based on the destination MAC address, the switch determines the outgoing port for the packet and forwards it only to that port.
- **Address Learning:** If the source MAC address of the packet is not already in the MAC address table, the switch learns the source MAC address and the port it arrived on by updating the table.

*Frame Forwarding Method

- Switching methods determine how network switches forward data packets within a network. These methods vary in terms of latency, error checking, and efficiency. Here's an overview of common switching methods:

1. Store-and-Forward Switching:

- **Operation:** In store-and-forward switching, the switch receives the entire data packet before forwarding it to the destination.
- **Processing:** The switch performs error checking on the entire packet, including cyclic redundancy check (CRC) verification to detect errors.
- **Advantages:**
    - Comprehensive error checking ensures packet integrity.
    - Suitable for networks where data integrity is critical.
- **Disadvantages:**
    - Higher latency compared to cut-through switching due to packet buffering and error checking.
    - Can limit switch performance in high-speed networks.

2. Cut-Through Switching:

- **Operation:** In cut-through switching, the switch starts forwarding the packet as soon as it reads the destination MAC address in the packet header.
- **Processing:** The switch forwards the packet before it has been fully received, without waiting for the entire packet to arrive.
- **Advantages:**
    - Lower latency compared to store-and-forward switching, as packets are forwarded as soon as the destination address is identified.
    - Suitable for low-latency applications such as real-time communication and video streaming.
- **Disadvantages:**
    - Limited error checking since the entire packet has not been received, which may result in corrupted data being forwarded.

    - Unsuitable for networks where data integrity is critical or where packet errors are common.

3. Modified Cut-Through Switching:

- **Operation:** Modified cut-through switching is a variation of cut-through switching where the switch waits for a predefined portion of the packet to arrive before forwarding it.
- **Processing:** The switch waits for a specific number of bytes or bits to arrive (e.g., the first 64 bytes of an Ethernet frame) before forwarding the packet.
- **Advantages:**
    - Provides a compromise between low latency (similar to cut-through switching) and error detection (similar to store-and-forward switching).
    - Helps mitigate the risk of forwarding corrupted or incomplete packets.
- **Disadvantages:**
    - May introduce slightly higher latency compared to traditional cut-through switching due to the wait time for the predefined portion of the packet.

Considerations:

- **Latency:** Cut-through switching typically offers the lowest latency, making it suitable for low-latency applications. Store-and-forward switching has higher latency due to error checking.
- **Error Checking:** Store-and-forward switching provides comprehensive error checking, while cut-through switching sacrifices error checking for lower latency.
- **Network Environment:** The choice of switching method depends on factors such as network speed, error rate, and application requirements.
- ***Frame Forwarding Method**
- 1. Store and Forward Mechanism
    - It's slow but reliable
    - latency depends on store size
- 2. Cut Thorugh
    - It's fast but not reliable.
    - no delay in cut through mechanism
    - if next frame is damaged, it still forward.
- 3. Modified Cut Through/ Fragment Free Method
    - recives first 64 bytes then it forward it
    - 99.99% is reliable.
    - and fast.

> These above method are implemented according to Switch model Generally Store and Forward method is implemented on Switch.

Old consideration configuration of switch:

- K - command line.
- I - IP configuration.
- M - Menu Based.

Switch commands

```
switch> en
switch# config t
switch(config)# int vlan 1
switch(config-if)# no shutdown
switch(config-if)# ip address 172.16.10.100 255.255.255.0
switch(config-if)# exit
switch(config)# ip default-gateway 172.16.10.1
```

> all the port of switch they belongs to vlan 1

Port securtiy

- **Description:** Port security limits the number of MAC addresses allowed on a switch port, preventing unauthorized devices from connecting to the network.
- **Configuration:** Configure port security using the following steps:
  - Enable port security on the interface: 'switchport port-security'.
  - Define the action to be taken when the maximum MAC addresses are exceeded (e.g., shutdown the port): 'switchport port-security violation '.

commands:

```
switch(config)# int range fa1/0-7
switch(config)# switchport port-security mac-address sticky
```

sticky - what ever the mac address leart on this port it will be permanant.

```
switch(config)# switchport port-security violation shutdown
```

> if some one else try to connect these port it will be shutdown.

STP(Spannig Tree Protocol)

- The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology within a bridged or switched network. It prevents loops from forming by dynamically shutting down redundant paths between switches, thereby ensuring that there is only one active path between any two network devices. Here's an overview of Spanning Tree Protocol:

> BPDU (Bridge Protocol Data Unit) it sends packets every 2 sec.

Purpose:

- STP prevents network loops in Ethernet networks by logically blocking redundant paths, ensuring a loop-free topology.

Operation:

- STP operates by selecting a single root bridge from which all other bridges (switches) are reachable.
- Each switch in the network participates in the STP algorithm to determine the shortest path to the root bridge.
- STP identifies redundant paths and blocks them to prevent loops, ensuring that there is only one active path between any two devices.

Root Select (IEEE STP Cost):

| Bandwidth | Cost | | 10 Mbps | 100 | | 100 Mbps | 19 | | 1 Gbps | 4 | | 10 Gbps | 2 |

> Root switch selected criteria is lowest bandwidth cost.

Port Roles:

- **Root Port:** The port on each non-root switch that provides the shortest path to the root bridge.
- **Designated Port:** The port on each network segment with the lowest path cost to the root bridge.
- **Non-Designated Port/Blocked Port:** Redundant ports that are placed in a blocking state to prevent loops.

STP States:

- **Blocking:** Ports are in a listening state and do not forward data frames. They receive and process Bridge Protocol Data Units (BPDUs) to determine the network topology.
- **Listening:** Ports prepare to participate in the active topology by learning about neighboring switches and ports.
- **Learning:** Ports start to populate their MAC address tables by forwarding data frames but do not forward data yet.
- **Forwarding:** Ports are fully operational and forward data frames between devices.

Benefits:

- **Loop Prevention:** STP prevents network loops from forming by dynamically blocking redundant paths.
- **Redundancy:** Despite blocking redundant paths, STP ensures that backup paths are available in case of link failures, providing network redundancy.
- **Reliability:** By maintaining a loop-free topology, STP enhances network stability and reliability.

Root Port Selection Criteria:

Cost to Root:

- The cost to reach the root bridge is a measure of the overall distance (in terms of network topology) from a switch to the root bridge.
- It is calculated based on the cumulative cost of all the links (ports) in the path from the switch to the root bridge.
- The cost of a link is determined by the bandwidth of the link. For example, a faster link (higher bandwidth) will have a lower cost.

Neighbor Switch ID:

- The neighbor switch ID refers to the Bridge ID of the neighboring switch connected to a particular port on a switch.
- Each switch maintains a database of neighboring switches and their Bridge IDs, which is used to calculate the shortest path to the root bridge.

Port ID:

- The port ID uniquely identifies each port on a switch within the context of the STP topology.
- It consists of a combination of the port number and the switch's Bridge ID.
- The port ID is used to determine which port on a switch should be designated as the root port or a designated port.

Selection of Non-Designated Ports:

- Non-designated ports are ports on switches that are neither root ports nor designated ports. They are put into a blocking state to prevent loops.
- The selection of non-designated ports is primarily based on the following criteria:
    - Path cost to the root bridge: Ports with higher path costs are more likely to be put into a blocking state.
    - Bridge ID: In case of tiebreakers between ports with the same path cost, the Bridge ID (consisting of Bridge Priority and MAC address) is used to determine the port that remains in the forwarding state.
    - Port ID: Ports with lower Port ID values are given higher priority.

Root Cost of the Switches:

- The root cost represents the cumulative cost of the path from a switch to the root bridge, including the cost of the switch's ports and the links leading to the root bridge.
- Each switch calculates its root cost based on the path cost of its ports and the received Bridge Protocol Data Units (BPDUs) from neighboring switches.
- Switches with lower root costs are closer to the root bridge and have higher priority in the STP topology.

Switch ID (Bridge ID):

- The Switch ID, also known as the Bridge ID, uniquely identifies each switch in the network.
- It consists of a combination of Bridge Priority (configured on the switch) and MAC address.
- In case of tiebreakers between switches with the same root cost, the Switch ID is used to determine the switch that becomes the root bridge.
- Switches with lower Switch IDs have higher priority and are more likely to become the root bridge.

> In CISCO new device connected to port and connection on it shows orange(Umber) color port for 50 sec. In 50 sec every ports goes form following stages:
>
> 1. Blocking ---------> 2. Listening ----------> 3. Learning --------> 4. Forwarding

STP sequence:

1. **Common Spanning Tree (CST):**
    - CST is the original implementation of STP standardized by IEEE 802.1D.

- It creates a single spanning tree instance for the entire network, regardless of VLANs.
- CST treats all VLANs as a single broadcast domain and blocks redundant paths for the entire network.

2. **Per-VLAN Spanning Tree (PVST):**

   - PVST extends STP to support VLAN-based spanning trees.
   - It creates a separate spanning tree instance for each VLAN in the network.
   - PVST allows for finer control over spanning tree configuration on a per-VLAN basis, optimizing network performance and resilience for each VLAN independently.

3. **Per-VLAN Spanning Tree Plus (PVST+):**

   - PVST+ is an enhancement of PVST that adds support for Cisco proprietary features.
   - It is backward compatible with PVST and inter-operates with standard STP (CST).
   - PVST+ incorporates additional features such as BackboneFast and UplinkFast to improve convergence time and resiliency in Cisco network environments.

4. **Multiple Spanning Tree (MST):**

   - MST is a standardized version of STP introduced in IEEE 802.1s.
   - It allows multiple VLANs to be mapped to the same spanning tree instance, reducing the number of spanning tree instances required in large networks.
   - MST simplifies spanning tree configuration and reduces overhead by grouping VLANs into regions, each with its own spanning tree instance.

5. **Rapid Spanning Tree Protocol (RSTP):**

   - RSTP, defined by IEEE 802.1w, is an enhancement of STP that reduces convergence time and improves network performance.
   - It introduces new port states (discarding, learning, and forwarding) and mechanisms (port roles and port types) to achieve faster convergence.
   - RSTP converges much faster than STP, typically in a few seconds, making it suitable for modern networks with rapid link changes.

VLAN commands:

VLANs (Virtual Local Area Networks) are logical network segments created within a physical network infrastructure to improve network efficiency, security, and scalability. While VLANs are commonly associated with switches, they can also be implemented in routers to extend VLAN functionality across multiple network segments or to route traffic between VLANs. Here's how VLANs can be configured and utilized in routers:

Configuration of VLANs in Routers:

1. **VLAN Interfaces:**

   - Routers can create virtual VLAN interfaces, allowing them to communicate with devices within each VLAN.
   - Each VLAN interface is configured with an IP address and subnet mask, enabling routing between VLANs.

2. **Subinterfaces:**
    - In environments where routers are connected to VLAN-aware switches, routers can use subinterfaces to route traffic between multiple VLANs over a single physical interface.
    - Subinterfaces are virtual interfaces configured with VLAN IDs, encapsulating VLAN-tagged traffic for transmission between the router and the switch.

Utilization of VLANs in Routers:

1. **Inter-VLAN Routing:**
    - Routers with VLAN support can route traffic between different VLANs, allowing communication between devices in separate VLANs while maintaining network segmentation.
    - This facilitates the implementation of network policies, access control, and security measures between VLANs.

2. **Router-on-a-Stick (RoAS):**
    - Router-on-a-Stick is a configuration method where a single router interface is used to route traffic between multiple VLANs connected to a switch.
    - The router interface is configured as a trunk port, allowing it to receive VLAN-tagged traffic from multiple VLANs over a single physical connection.

commands:

```
switch(config)# vlan 2
switch(config-vlan)# name Sales
switch(config-vlan)# exit

switch(config)# vlan 3
switch(config-vlan)# name Purchase
switch(config-vlan)# exit

switch(config)# int fa 0/1
switch(config-if)# switchport access vlan 2
switch(config-if)# exit

switch(config)# int fa 1/1
switch(config-if)# switchport access vlan 2
switch(config-if)# exit

switch(config)# int range fa 2/1-2
switch(config-if)# switchport access vlan 3
```

VTP (VLAN Trunking Protocol)

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used for managing VLAN configurations across a switched network. It simplifies VLAN administration by allowing VLAN information to be automatically propagated to all switches within the network domain. Here's an overview of VTP:

1. **VLAN Management:**
    - VTP facilitates centralized management of VLAN configurations by automatically synchronizing VLAN information across switches within the same VTP domain.
    - It eliminates the need to manually configure VLANs on each switch, reducing administrative overhead and the potential for configuration errors.
2. **Domain-Based Configuration:**
    - Switches participating in VTP are organized into VTP domains, which define a logical boundary for VLAN configuration synchronization.
    - All switches within the same VTP domain share VLAN information, while switches in different domains maintain separate VLAN configurations.
3. **VTP Modes:**
    - **Server Mode:** Switches in Server mode can create, modify, and delete VLANs, and their changes are propagated to other switches in the VTP domain.
    - **Client Mode:** Switches in Client mode receive and synchronize VLAN information from VTP server switches but cannot make changes to VLAN configurations.
    - **Transparent Mode:** Switches in Transparent mode do not participate in VTP domain-wide VLAN configuration synchronization. They forward VTP advertisements but do not process them, allowing VLANs to be manually configured on a per-switch basis.

Benefits:

- **Simplified VLAN Management:** VTP streamlines VLAN administration by automatically distributing VLAN configurations, reducing manual configuration efforts and the risk of inconsistencies.
- **Consistency and Scalability:** VTP ensures consistency of VLAN configurations across the network, making it easier to scale and manage large switched environments.
- **Time Efficiency:** Changes made to VLAN configurations on one VTP server switch are automatically propagated to all other switches in the domain, saving time and effort.

Inter VLAN

Inter-VLAN routing refers to the process of forwarding traffic between different VLANs within a network. VLANs (Virtual Local Area Networks) are logical network segments that segregate network traffic, providing improved security, manageability, and performance. Inter-VLAN routing allows communication between devices residing on different VLANs, enabling them to exchange data and access resources across the network. Here's how inter-VLAN routing works and how it can be implemented:

How Inter-VLAN Routing Works:

1. **Layer 3 Routing:**
    - Inter-VLAN routing operates at the network layer (Layer 3) of the OSI model, where routers forward traffic between VLANs based on their IP addresses.
    - Routers examine the destination IP address of incoming packets and determine the appropriate VLAN for forwarding based on routing table entries.

2. **Router Configuration:**
    - To enable inter-VLAN routing, a router must have interfaces configured with IP addresses for each VLAN it needs to communicate with.
    - Each VLAN is assigned a unique IP subnet, and the router's interfaces are configured with IP addresses belonging to these subnets.
    - The router acts as a gateway for devices in each VLAN, forwarding traffic between VLANs based on the destination IP address.
3. **Trunk Links:**
    - To connect switches and routers for inter-VLAN routing, trunk links are used. Trunk links carry traffic for multiple VLANs over a single physical connection.
    - Trunk links encapsulate VLAN-tagged packets using protocols such as IEEE 802.1Q, allowing routers to distinguish between traffic belonging to different VLANs.
4. **Routing Decisions:**
    - When a device in one VLAN sends traffic to a device in another VLAN, the source device forwards the traffic to its default gateway (the router).
    - The router receives the packet, examines the destination IP address, and forwards it to the appropriate VLAN interface based on its routing table.

Inter-VLAN Routing Methods:

1. **Router-on-a-Stick (RoAS):**
    - In this method, a single router interface is configured with subinterfaces, each representing a different VLAN.
    - The subinterfaces are configured with VLAN IDs and IP addresses corresponding to the VLANs they represent.
    - Traffic for multiple VLANs is sent over the same physical interface, with each VLAN identified by its VLAN tag.
2. **Layer 3 Switching:**
    - Layer 3 switches have routing capabilities built into the switch hardware.
    - They can perform inter-VLAN routing at wire-speed, allowing for high-performance routing between VLANs directly within the switch.

Benefits of Inter-VLAN Routing:

- **Improved Network Segmentation:** VLANs provide logical segmentation of network traffic, enhancing security and manageability.
- **Efficient Resource Access:** Inter-VLAN routing allows devices in different VLANs to access shared resources, such as servers and printers, without compromising network security.
- **Scalability:** Inter-VLAN routing enables the creation of large and complex networks by facilitating communication between diverse VLANs.

Considerations:

- **Performance:** The routing capacity of the router or layer 3 switch should be sufficient to handle the inter-VLAN traffic load without introducing bottlenecks.
- **Configuration Complexity:** Configuring and managing inter-VLAN routing requires careful planning and configuration to ensure proper functionality and security.