Introduction to Switched Networks

Routing And Switching
Converged Networks
Growing Complexity of Networks

- Our digital world is changing
- Information must be accessed from anywhere in the world
- Networks must be secure, reliable, and highly available
Converged Networks

Elements Of A Converged Network

- Collaboration is a requirement
- To support collaboration, networks employ converged solutions
- Data services such as voice systems, IP phones, voice gateways, video support, and video conferencing
- Call control, voice messaging, mobility and automated attendant are also common features
Converged Networks

Elements Of A Converged Network

- Benefits of Converged Networks include:
  - Multiple types of traffic; Only one network to manage
  - Substantial savings over installation and management of separate voice, video and data networks
  - Integrates IT management
Borderless switched network design guidelines are built upon the following principles:

- Hierarchical
- Modularity
- Resiliency
- Flexibility
Converged Networks
Core, Distribution, Access

Building B - Marketing and Sales
Access
Distribution
Core

Building C - Engineering

Building A - Management

Building D - Research and Development
Access
Distribution

Building E - Information Technology

Building F - Data Center

www.ncp.edu.pk
Switched Networks
Role of Switched Networks

- The role of switched networks has evolved
- A switched LAN allows more flexibility, traffic management
- It also support features such as quality of service, additional security, support for wireless, support for IP telephony and mobility services
Switched Networks
Form Factor

- Fixed
- Modular
- Stackable

Features and options are limited to those that originally come with the switch.
The chassis accepts line cards that contain the ports.
Stackable switches, connected by a special cable, effectively operate as one large switch.
Frame Forwarding

Switching as a General Concept

- A Switch makes a decision based on ingress and destination port.
- A LAN switch keeps a table that it uses to determine how to forward traffic through the switch.
- LAN switches forward Ethernet frames based on the destination MAC address of the frames.
Frame Forwarding
Dynamically Populating a Switch MAC Address Table

- A switch must first learn which devices exist on each port before it can transmit a frame.
- It builds a table called a MAC address, or content addressable memory (CAM) table.
- The mapping device <-> port is stored in the CAM table.
- CAM is a special type of memory used in high-speed searching applications.
- The information in the MAC address table is used to send frames.
- When a switch receives an incoming frame with a MAC address that is not found in the CAM table, it floods it to all ports but the one that received the frame.
Frame Forwarding

Switch Forwarding Methods

Store-and-Forward

A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

Cut-Through

A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.
Frame Forwarding

Store-and-Forward Switching

- Store-and-Forwarding allows the switch to:
  - Check for errors (via FCS check)
  - Perform Automatic Buffering
- Slower forwarding

Store-and-forward switching entails receipt of the entire frame (up to about 9,200 bytes for jumbo frames) before a forwarding decision is made.

www.ncp.edu.pk
Frame Forwarding

**Cut-Through Switching**

- Cut-Through allows the switch to start forwarding in about 10 microseconds
- No FCS check
- No Automatic Buffering

Frames can begin to be forwarded as soon as the Destination MAC is received.

www.ncp.edu.pk
Switching Domains

Collision Domains

- Collision domain is the segment where devices must compete to communicate
- All ports of a hub belong to the same collision domain
- Every port of a switch is a collision domain on its own
- A switch break the segment into smaller collision domains, easing device competition.
Switching Domains

Broadcast Domains

- Broadcast domain is the extend of the network where a broadcast frame can be heard.

- Switches forward broadcast frames to all ports. Therefore switches don’t break broadcast domains.

- All ports of a switch (with its default configuration) belong to the same broadcast domain.

- If two or more switches are connected, broadcasts will be forward to all ports of all switches (except for the port that originally received the broadcast).
Switching Domains

Alleviating Network Congestion

Switches help alleviating network congestion by:

- facilitating the segmentation of a LAN into separate collision domains
- providing full-duplex communication between devices
- taking advantage of their high port density
- buffering large frames
- employing high speed ports
- taking advantage of their fast internal switching process
- having a low per-port cost
Basic Switch Configuration

Switch Boot Sequence

1. POST (Power On Self Test)
2. Run boot loader software
3. Boot loader does low-level CPU initialization
4. Boot loader initializes the flash filesystem
5. Boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.
Basic Switch Configuration

Switch Boot Sequence

In order to find a suitable IOS image, the switch goes through the following steps:

1. It attempts to automatically boot by using information in the BOOT environment variable

2. If this variable is not set, the switch performs a top-to-bottom search through the flash file system. It will load and execute the first executable file, if it can.

3. The IOS operating system then initializes the interfaces using the IOS commands found in the configuration file, startup configuration, which is stored in NVRAM.

Note: the command `boot system` can be used to set the BOOT environment variable.
Basic Switch Configuration

Preparing for Basic Switch Management

- In order to remotely manage a switch, it needs to be configured to access the network
- An IP address and a subnet mask must be configured
- If managing the switch from a remote network, a default gateway must also be configured
- The IP information (address, subnet mask, gateway) is to be assigned to a switch SVI (switch virtual interface)
- Although these IP settings allow remote management and remote access to the switch, they do not allow the switch to route Layer 3 packets.
## Basic Switch Configuration
### Preparing for Basic Switch Management

<table>
<thead>
<tr>
<th><strong>Cisco Switch IOS Commands</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration mode.</td>
<td>S1# configure terminal</td>
</tr>
<tr>
<td>Enter interface configuration mode for the SVI.</td>
<td>S1(config)# interface vlan99</td>
</tr>
<tr>
<td>Configure the management interface IP address.</td>
<td>S1(config-if)# ip address 172.17.99.11</td>
</tr>
<tr>
<td>Enable the management interface.</td>
<td>S1(config-if)# no shutdown</td>
</tr>
<tr>
<td>Return to the privileged EXEC mode.</td>
<td>S1(config-if)# end</td>
</tr>
<tr>
<td>Save the running config to the startup config.</td>
<td>S1# copy running-config startup-config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Cisco Switch IOS Commands</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration mode.</td>
<td>S1# configure terminal</td>
</tr>
<tr>
<td>Configure the default gateway for the switch.</td>
<td>S1(config)# ip default-gateway 172.17.99.</td>
</tr>
<tr>
<td>Return to the privileged EXEC mode.</td>
<td>S1(config-if)# end</td>
</tr>
<tr>
<td>Save the running config to the startup config.</td>
<td>S1# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configure Switch Ports

Configure Switch Ports at the Physical Layer

Configure Duplex and Speed

Cisco Switch IOS Commands

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration mode.</td>
<td><code>S1# configure terminal</code></td>
</tr>
<tr>
<td>Enter interface configuration mode.</td>
<td><code>S1(config)# interface fastethernet 0/1</code></td>
</tr>
<tr>
<td>Configure the interface duplex.</td>
<td><code>S1(config-if)# duplex full</code></td>
</tr>
<tr>
<td>Configure the interface speed.</td>
<td><code>S1(config-if)# speed 100</code></td>
</tr>
<tr>
<td>Return to the privileged EXEC mode.</td>
<td><code>S1(config-if)# end</code></td>
</tr>
<tr>
<td>Save the running config to the startup config.</td>
<td><code>S1# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
Configure Switch Ports

MDIX Auto Feature

- Certain cable types (straight-through or crossover) were required when connecting devices.
- The automatic medium-dependent interface crossover (auto-MDIX) feature eliminates this problem.
- When auto-MDIX is enabled, the interface automatically detects and configures the connection appropriately.
- When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto**.
**Configure Switch Ports**

**MDIX Auto Feature**

---

**Enable auto-MDIX**

- **PC1** connected to **S1**
- **S1** connected to **S2**
- **S2** connected to **PC2**

---

### Cisco Switch IOS Commands

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration mode.</td>
<td>S1# configure terminal</td>
</tr>
<tr>
<td>Enter interface configuration mode.</td>
<td>S1(config)# interface fastethernet 0/1</td>
</tr>
<tr>
<td>Configure the interface to autonegotiate duplex with the connected device.</td>
<td>S1(config-if)# duplex auto</td>
</tr>
<tr>
<td>Configure the interface to autonegotiate speed with the connected device.</td>
<td>S1(config-if)# speed auto</td>
</tr>
<tr>
<td>Enable auto-MDIX on the interface.</td>
<td>S1(config-if)# mdix auto</td>
</tr>
<tr>
<td>Return to the privileged EXEC mode.</td>
<td>S1(config-if)# end</td>
</tr>
<tr>
<td>Save the running config to the startup config.</td>
<td>S1#copy running-config startup-config</td>
</tr>
</tbody>
</table>
## Configure Switch Ports

### Verifying Switch Port Configuration

#### Verification Commands

<table>
<thead>
<tr>
<th>Cisco Switch IOS Commands</th>
<th>Verification Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display interface status and configuration.</td>
<td>S1# show interfaces [interface-id]</td>
</tr>
<tr>
<td>Display current startup configuration.</td>
<td>S1# show startup-config</td>
</tr>
<tr>
<td>Display current operating config.</td>
<td>S1# show running-config</td>
</tr>
<tr>
<td>Displays info about flash filesystem.</td>
<td>S1# show flash</td>
</tr>
<tr>
<td>Displays system hardware &amp; software status.</td>
<td>S1# show version</td>
</tr>
<tr>
<td>Display history of commands entered.</td>
<td>S1# show history</td>
</tr>
<tr>
<td>Display IP information about an interface.</td>
<td>S1# show ip [interface-id]</td>
</tr>
<tr>
<td>Display the MAC address table.</td>
<td>S1# show mac-address-table</td>
</tr>
</tbody>
</table>

[Image of a logo or emblem]
Security Concerns in LANs

MAC Address Flooding

- Attacker flooding the CAM table with bogus entries

<table>
<thead>
<tr>
<th>MAC</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>3</td>
</tr>
<tr>
<td>Y</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
</tbody>
</table>

Bogus addresses are added to the MAC address table.

X and Y are on Port 3 and the MAC address table is updated.

Attacker starts sending unknown bogus MAC addresses.

Intruder runs an attack tool on MAC C.
Security Concerns in LANs
MAC Address Flooding

- The switch now behaves as a hub
Security Concerns in LANs

DHCP Spoofing

- DHCP is a network protocol used to assign IP info automatically

- Two types of DHCP attacks are:
  - DHCP spoofing
  - DHCP starvation

- In DHCP spoofing attacks, a fake DHCP server is placed in the network to issue DHCP addresses to clients.

- DHCP starvation is often used before a DHCP spoofing attack to deny service to the legitimate DHCP server.
Security Concerns in LANs

DHCP Spoofing

- DHCP Spoof Attack

1) An attacker activates a DHCP server on a network segment.
2) The client broadcasts a request for DHCP configuration information.
3) The rogue DHCP server responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
4) Host packets are redirected to the attacker’s address as it emulates a default gateway for the erroneous DHCP address provided to the client.
Security Best Practices

Network Security Tools: Options

- Network Security Tools are very important to network administrators
- Such tools allow an administrator to test the strength of the security measures implemented
- An administrator can launch an attack against the network and analyze the results
- This is also to determine how to adjust security policies to mitigate those types of attacks
- Security auditing and penetration testing are two basic functions that network security tools perform
Network Security Tools: Audits

- Network Security Tools can be used to audit the network.

- By monitoring the network, an administrator can assess what type of information an attacker would be able to gather.

- For example, by attacking and flooding the CAM table of a switch, an administrator would learn which switch ports are vulnerable to MAC flooding and correct the issue.

- Network Security Tools can also be used as penetration test tools.
Security Best Practices

Network Security Tools: Audits

- Penetration testing is a simulated attack
- It helps to determine how vulnerable the network is when under a real attack.
- Weaknesses within the configuration of networking devices can be identified based on pen test results
- Changes can be made to make the devices more resilient to attacks
- Such tests can damage the network and should be carried out under very controlled conditions
- An off-line test bed network that mimics the actual production network is the ideal.
Switch Port Security

Secure Unused Ports

- Disable Unused Ports is a simple yet efficient security guideline

Disable unused ports using the shutdown command.

S1# show run
Building configuration...
...
version 15.0
hostname S1
...
interface FastEthernet0/4
  shutdown
!
interface FastEthernet0/5
  shutdown
!
interface FastEthernet0/6
description web server
!
interface FastEthernet0/7
  shutdown
!
...
Switch Port Security

DHCP Snooping

- DHCP Snooping specifies which switch ports can respond to DHCP requests

- DHCP snooping allows the configuration of ports as trusted or untrusted.
  - Trusted ports can send DHCP requests and acknowledgements.
  - Untrusted ports can forward only DHCP requests.
- DHCP Snooping enables the switch to build a DHCP binding table that maps a client MAC address, IP address, VLAN, and port ID.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```
Port Security: Operation

- Port security limits the number of valid MAC addresses allowed on a port.
- The MAC addresses of legitimate devices are allowed access, while other MAC addresses are denied.
- Any additional attempts to connect by unknown MAC addresses will generate a security violation.
- Secure MAC addresses can be configured in a number of ways:
  - Static secure MAC addresses
  - Dynamic secure MAC addresses
  - Sticky secure MAC addresses
Switch Port Security

Port Security: Violation Modes

- IOS considers a security violation when either of these situations occurs:
  - The maximum number of secure MAC addresses for that interface have been added to the CAM, and a station whose MAC address is not in the address table attempts to access the interface.
  - An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

- There are three possible action to be taken when a violation is detected:
  - Protect
  - Restrict
  - Shutdown
## Switch Port Security

### Port Security: Configuring

- Dynamic Port Security Defaults

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port security</td>
<td>Disabled on a port.</td>
</tr>
<tr>
<td>Maximum number of secure MAC addresses</td>
<td>1</td>
</tr>
<tr>
<td>Violation mode</td>
<td>Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.</td>
</tr>
<tr>
<td>Sticky address learning</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
Switch Port Security

Port Security: Configuring

- Configuring Dynamic Port Security

### Cisco IOS CLI Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1(config)#interface fastethernet 0/18</td>
<td>Specify the interface to be configured for port security.</td>
</tr>
<tr>
<td>S1(config-if)#switchport mode access</td>
<td>Set the interface mode to access.</td>
</tr>
<tr>
<td>S1(config-if)#switchport port-security</td>
<td>Enable port security on the interface.</td>
</tr>
</tbody>
</table>
Switch Port Security

Port Security: Configuring

- Configuring Port Security Sticky

Cisco IOS CLI Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1(config)#interface fastethernet 0/18</td>
<td>Specify the interface to be configured for port security.</td>
</tr>
<tr>
<td>S1(config-if)#switchport mode access</td>
<td>Set the interface mode to access.</td>
</tr>
<tr>
<td>S1(config-if)#switchport port-security</td>
<td>Enable port security on the interface.</td>
</tr>
<tr>
<td>S1(config-if)#switchport port-security max</td>
<td>Set the maximum number of secure addresses allowed on the port.</td>
</tr>
<tr>
<td>S1(config-if)#switchport port-security mac-address sticky</td>
<td>Enable sticky learning.</td>
</tr>
</tbody>
</table>
Switch Port Security

Port Security: Verifying

- Verifying Port Security Sticky

```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```
Switch Port Security

Port Security: Verifying

- Verifying Port Security Sticky – Running Config

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
  switchport mode access
  switchport port-security maximum 50
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0025.83e6.4b02
```
Switch Port Security

Ports In Error Disabled State

- A port security violation can put a switch in error disabled state
- A port in error disabled is effectively shut down
- The switch will communicate these events through console messages

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```
Switch Port Security

Ports In Error Disabled State

- The show interface command also reveals a switch port on error disabled state

```
S1# show interface fa0/18 status
Port Name  Status   Vlan  Duplex  Speed  Type
Fa0/18      err-disabled  1     auto  auto  10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security       : Enabled
Port Status          : Secure-shutdown
Violation Mode       : Shutdown
Aging Time           : 0 mins
Aging Type           : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses: 1
Total MAC Addresses  : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 000c.292b.4c75:1
Security Violation Count : 1
```
Switch Port Security

Ports In Error Disabled State

- A shutdown/no shutdown interface command must be issued to re-enable the port

```
S1(config )#interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
```
Spanning-Tree Protocol

- How is reliability in a network achieved and downtime reduced?

  by using reliable equipment

  by designing networks that are tolerant to failures and faults

- Networks should be designed to re-converge rapidly so that a fault is bypassed

  Fault tolerance is achieved by redundancy
Spanning-Tree Protocol

Redundant Switched Topologies

- Redundant topologies *eliminate single points of failure*
- If a path or device fails, the redundant path or device can take over the tasks of the failed path or device.

A Simple Redundant Switched Topology
Switches flood traffic out all ports when the traffic is sent to a destination that is *not yet known*

Broadcast and multicast traffic is forwarded out every port, except the port on which the traffic arrived

This traffic can be caught in a loop
Spanning-Tree Protocol
Avoiding Switching Loops

- The *Spanning-Tree Protocol* is used in switched networks to create a *loop free logical topology* from a physical topology that has loops.

- “Given a connected, undirected graph, a *spanning tree* of that graph is a subgraph which is a tree and connects all the vertices together”.

- A single graph can have many different spanning trees.
Spanning-Tree Protocol

Intro to Spanning-Tree Protocol (STP)

- IEEE 802.1D Spanning-Tree Protocol
  
  Used by Ethernet bridges and switches to construct a loop free shortest path network using the *spanning-tree algorithm*

- Shortest path is based on *cumulative link costs*

  Link costs are based on the **speed** of the link

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>Cost (Revised IEEE Spec)</th>
<th>Cost (Previous IEEE Spec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Gbps</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>19</td>
<td>10</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

www.ncp.edu.pk
The Spanning-Tree Protocol establishes a root node, called the root bridge.

STP constructs a topology that has one path for reaching every network node.

The resulting tree originates from the root bridge.

Redundant links that are not part of the shortest path tree are blocked.

Data frames received on blocked links are dropped.

Because certain paths are blocked, a loop free topology is possible.
The Spanning-Tree Protocol requires network devices to exchange messages to help form a loop-free logical topology.

These messages are called *Bridge Protocol Data Units (BPDUs)*.

Links that will cause a loop are put into a *blocking state*.

*BPDUs continue to be received on blocked ports* (ensures that if an active path or device fails, a new spanning tree can be calculated).
More on BPDUs…

- BPDUs help switches do the following:
  - Select a **single switch** that will act as the **root** of the spanning tree
  - Calculate the shortest path from itself to the root switch
  - Designate one of the switches as the closest one to the root, for each LAN segment. This bridge is called the “**designated switch**”
    - The designated switch handles all communication from that LAN towards the root bridge.
  - Choose one of its ports as a **root port** (if it is a **non-root switch**)
    - This is the interface that gives the best path to root switch.
  - Select ports that are part of the spanning tree, called **designated ports**
  - Non-designated ports are **blocked**
Root Ports, Designated Ports, & Non-Designated Ports

[Diagram showing network topology with Root Bridge, Cat-A, Cat-B, and Cat-C, indicating Root Ports, Designated Ports, and Non-Designated Ports with costs and IP addresses.]
Information Contained in BPDUs

- **Root BID**: Who is the root bridge?
- **Root Path Cost**: How far away is the root bridge?
- **Sender BID**: What is the BID of the bridge that sent this BPU?
- **Port ID**: What port on the sending bridge does this BPDU come from?
Spanning-Tree Operation

- When the network has stabilized, it has converged and there is one spanning tree per network.

- For every switched network the following elements exist:
  - One root bridge per network
  - One root port per non root bridge
  - One designated port per segment
  - Unused, non-designated ports

- Root ports and designated ports forward data traffic.

- Non-designated ports discard data traffic. These ports are called blocking or discarding ports.
Selecting the Root Bridge

- The first decision that all switches in the network make, is to identify the root bridge using the spanning-tree algorithm.

  the bridge with the smallest Bridge ID (BID) value will be the root bridge.

- BPDUs are sent out with the Bridge ID (BID).

  The BID consists of a bridge priority (that defaults to 32768) and the switch base MAC address.

  By default BPDUs are sent every two seconds.

  All switches see the BIDs sent.
Selecting the Root Bridge Cont’d

- When a switch first starts up, it assumes it is the root switch and sends “inferior” BPDUs.
  
  These BPDUs contain the bridge priority and switch MAC address in both the root and sender BID.

- As a switch receives a BPDU with a lower root BID it replaces that in the subsequent BPDUs it sends out.

- A network administrator can influence the decision by setting the switch priority to a smaller value than the default (which will make the BID smaller).
  
  Should only be implemented when the traffic flow on the network is well understood.
Four Stages of Spanning-Tree Port States

- A port can also be in a disabled state which occurs when an administrator shuts down the port or the port fails.
Four Stages of Spanning-Tree Port States

- **Blocking State**
  
  Ports can only receive BPDUs.
  
  Data frames are discarded and no addresses can be learned.
  
  It may take up to 20 seconds to change from this state.

- **Listening State**
  
  Switches determine if there are any other paths to the root bridge.
  
  The path that is not the least cost path to the root bridge goes back to the blocked state.
  
  BPDUs are still processed.
  
  User data is not being forwarded and MAC addresses are not being learned.
  
  The listening period is called the forward delay and lasts for 15 seconds.
Four Stages of Spanning-Tree Port States

- **Learning State**
  
  user data is not forwarded, but MAC addresses are learned from any traffic that is seen

  The learning state lasts for 15 seconds and is also called the forward delay

  BPDUs are still processed

- **Forwarding state**

  user data is forwarded and MAC addresses continue to be learned

  BPDUs are still processed

- **Disabled State (Fifth State)**

  can occur when an administrator shuts down the port or the port fails
Spanning-Tree Recalculation

- A switched internetwork has converged when all the switch and bridge ports are in either the *forwarding or blocked state*
  
  Forwarding ports send and receive data traffic and BPDUs
  
  Blocked ports will only receive BPDUs

- When the network topology changes, switches and bridges recompute the Spanning Tree causing a disruption of user traffic.

- Convergence on a new spanning-tree topology using the IEEE 802.1D standard can take up to *50 seconds*
Link Aggregation

- Also known as *port bundling, link bundling, Etherchannel*
- You can use multiple links in parallel as a single, logical link
  - For increased capacity
  - For redundancy (fault tolerance)
- LACP (Link Aggregation Control Protocol) is a standardized method of negotiating these bundled links between switches using LACPDUs
- PAgP is Cisco’s proprietary Port Aggregation Protocol.
Link Aggregation

- Two switches connected via multiple links will send control packets to form a single logical link.

- **active**: Enable LACP unconditionally
- **passive**: Enable LACP only if a LACP device is detected
- **auto**: Enable PAgP only if a PAgP device is detected
- **desirable**: Enable PAgP unconditionally
- **on**: Enable Etherchannel only

---

**Will an EtherChannel Form?**

<table>
<thead>
<tr>
<th>LACP</th>
<th>PAgP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td><strong>Desirable</strong></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Passive</th>
<th><strong>Auto</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

www.ncp.edu.pk
LACP Operation

- Two switches are connected to each other using two sets of Fast Ethernet ports. LACP is enabled and the ports are turned on.

- Switches start sending LACPDUs, then negotiate how to set up the aggregation.

- The result is an aggregated 200 Mbps logical link which is fault tolerant.
VLANs

Routing And Switching
Overview Of VLANs

VLAN Definitions

- VLAN (virtual LAN) is a logical partition of a layer 2 network
- Multiple partition can be created, allowing for multiple VLANs to co-exist
- Each VLAN is a broadcast domain, usually with its own IP network
- VLANS are mutually isolated and packets can only pass between them through a router
- The partitioning of the layer 2 network takes inside a layer 2 device, usually a switch.
- The hosts grouped within a VLAN are unaware of the VLAN’s existence
Overview Of VLANs

VLAN Definitions

Third Floor

Second Floor

First Floor

VLAN2 IT 10.0.2.0/24

VLAN3 HR 10.0.3.0/24

VLAN4 Sales 10.0.4.0/24
Overview Of VLANs

Benefits of VLANs

- Security
- Cost reduction
- Better performance
- Shrink broadcast domains
- Improved IT staff efficiency
- Simpler project and application management
Overview Of VLANs

Types of VLANs

- Data VLAN
- Default VLAN
- Native VLAN
- Management VLAN
- Private VLAN
Overview Of VLANs

Types of VLANs

VLAN 1

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/5, Fa0/6, Fa0/7, Fa0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/9, Fa0/10, Fa0/11, Fa0/12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/13, Fa0/14, Fa0/15, Fa0/16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/17, Fa0/18, Fa0/19, Fa0/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fa0/21, Fa0/22, Fa0/23, Fa0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gi0/1, Gi0/2</td>
</tr>
</tbody>
</table>

1002 fddi-default  act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default    act/unsup

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.
VLANs in a Multi-Switched Environment

VLAN Trunks

- A VLAN trunk carries more than one VLAN
- Usually established between switches so same-VLAN devices can communicate even if physically connected to different switches
- A VLAN trunk is not associated to any VLANs.
- Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol
VLANs in a Multi-Switched Environment

**VLAN Trunks**

- VLAN 10 Faculty/Staff - 172.17.10.0/24
- VLAN 20 Students - 172.17.20.0/24
- VLAN 30 Guest - 172.17.30.0/24
- VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.

VLAN trunks configured to support: VLAN 10, 20, 30 and VLAN 99.
VLANs in a Multi-Switched Environment

Controlling Broadcast Domains with VLANs

- VLANs can be used to limit the reach of broadcast frames
- A VLAN is a broadcast domain of its own
- Therefore, a broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- This help controlling the reach of broadcast frames and their impact in the network
- Unicast and multicast frames are forwarded within the originating VLAN as well
Frame tagging is used to properly transmit multiple VLAN frames through a trunk link.

Switches will tag frames to identify the VLAN they belong. Different tagging protocols exist, with IEEE 802.1q being a very popular one.

The protocol defines the structure of the tagging header added to the frame.

Switches will add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports.

Once properly tagged, the frames can traverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.
VLANs in a Multi-Switched Environment
Tagging Ethernet Frames for VLAN Identification
VLANs in a Multi-Switched Environment
Native VLANs and 802.1q Tagging

- A frame that belongs to the native VLAN will not be tagged.
- A frame that is received untagged will remain untagged and placed in the native VLAN when forwarded.
- If there are no ports associated to the native VLAN and no other trunk links, an untagged frame will be dropped.
- In Cisco switches, the native VLAN is VLAN 1 by default.
VLANs in a Multi-Switched Environment

Voice VLAN Tagging

Switch port configured to support voice traffic:
- Instructs phone to tag voice frames with VLAN 150
- Prioritizes voice frames
- Forwards data frames on VLAN 20

Configured to tag voice traffic frames with VLAN 150.

Configured to send untagged data traffic.

Configured to send untagged data traffic.
VLAN Assignment

VLAN Ranges On Catalyst Switches

- The Catalyst 2960 and 3560 Series switches support over 4,000 VLANs

- These VLANs are split into 2 categories:

  - Normal Range VLANs
    - VLAN numbers from 1 through 1005
    - Configurations stored in the vlan.dat (in the flash)
    - VTP can only learn and store normal range VLANs

  - Extended Range VLANs
    - VLAN numbers from 1006 through 4096
    - Configurations stored in the running-config (in the NVRAM)
    - VTP does not learn extended range VLANs
### VLAN Assignment

#### Creating a VLAN

<table>
<thead>
<tr>
<th>Cisco Switch IOS Commands</th>
<th>Example Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration mode.</td>
<td>S1# configure terminal</td>
</tr>
<tr>
<td>Create a VLAN with a valid id number.</td>
<td>S1(config)# vlan vlan_id</td>
</tr>
<tr>
<td>Specify a unique name to identify the VLAN.</td>
<td>S1(config)# name vlan_name</td>
</tr>
<tr>
<td>Return to the privileged EXEC mode.</td>
<td>S1(config)# end</td>
</tr>
</tbody>
</table>

www.ncp.edu.pk
VLAN Assignment
Assigning Ports To VLANs

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```
VLAN Assignment
Deleting VLANs

S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/5, Fa0/6, Fa0/7, Fa0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/9, Fa0/10, Fa0/12, Fa0/13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/14, Fa0/15, Fa0/16, Fa0/17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/18, Fa0/19, Fa0/20, Fa0/21</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/22, Fa0/23, Fa0/24, Gi0/1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gi0/2</td>
</tr>
<tr>
<td>1002</td>
<td>fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004</td>
<td>fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>
S1#
### VLAN Assignment

#### Verifying VLAN Information

```plaintext
S1# show vlan name student

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>active</td>
<td>Fa0/11, Fa0/18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN Type</th>
<th>SAID</th>
<th>MTU</th>
<th>Parent</th>
<th>RingNo</th>
<th>BridgeNo</th>
<th>Stp</th>
<th>BrdgMode</th>
<th>Trans1</th>
<th>Trans2</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>enet</td>
<td>100020</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Remote SPAN VLAN
-----------------
Disabled

Primary Secondary Type | Ports
----------------------|---------

S1# show vlan summary

<table>
<thead>
<tr>
<th>Number of existing VLANs</th>
<th>: 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of existing VTP VLANs</td>
<td>: 7</td>
</tr>
<tr>
<td>Number of existing extended VLANS</td>
<td>: 0</td>
</tr>
</tbody>
</table>
```

S1#
VLAN Assignment

Configuring IEEE 802.1q Trunk Links

<table>
<thead>
<tr>
<th>Cisco Switch IOS Commands</th>
<th>Example Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration mode.</td>
<td><code>S1# configure terminal</code></td>
</tr>
<tr>
<td>Enter interface configuration mode for the SVI.</td>
<td><code>S1(config)# interface interface_id</code></td>
</tr>
<tr>
<td>Force the link to be a trunk link.</td>
<td><code>S1(config)# switchport mode trunk</code></td>
</tr>
<tr>
<td>Specify a native VLAN for untagged 802.1Q trunks.</td>
<td><code>S1(config-if)# switchport trunk native vlan vlan_id</code></td>
</tr>
<tr>
<td>Specify the list of VLANs to be allowed on the trunk link.</td>
<td><code>S1(config-if)# switchport trunk allowed vlan vlan-list</code></td>
</tr>
<tr>
<td>Return to the privileged EXEC mode.</td>
<td><code>S1(config-if)# end</code></td>
</tr>
</tbody>
</table>

```plaintext
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```
VLAN Assignment

Resetting the Trunk To Default State

Resetting Trunk Link Example

```
S1(config)#  interface f0/1
S1(config-if)#  no switchport trunk allowed vlan
S1(config-if)#  no switchport trunk native vlan
S1(config-if)#  end
S1#  show interfaces f0/1 switchport
Name:  Fa0/1
Switchport:  Enabled
Administrative Mode:  trunk
Operational Mode:  trunk
Administrative Trunking Encapsulation:  dot1q
Operational Trunking Encapsulation:  dot1q
Negotiation of Trunking:  On
Access Mode VLAN:  1 (default)
Trunking Native Mode VLAN:  1 (default)
Administrative Native VLAN tagging:  enabled
<output omitted>
Administrative private-vlan trunk mappings:  none
Operational private-vlan:  none
Trunking VLANs Enabled:  ALL
Pruning VLANs Enabled:  2-1001
<output omitted>
```
VLAN Assignment
Resetting the Trunk To Default State

Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```
VLAN Assignment

Verifying Trunk Configuration

Verifying Trunk Configuration

S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport

Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none

Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
VLAN Trunking Protocol (VTP)
VLAN Management Challenge (1)

It is not difficult to add new VLAN for a small network
VLAN Management Challenge (2)

The VLAN Management Challenge

Existing VLANs: 10, 20, 99

VLAN Management Task: Add VLAN 30

It is not easy to add a new VLAN to all of switches
What is VTP?

- VTP allows a network manager to configure a switch so that it will propagate VLAN configurations to other switches in the network.

- The switch can be configured in the role of a VTP server or a VTP client. VTP server distributes and synchronizes VLAN information to VTP-enabled switches throughout the switched network.

- VTP only learns about normal-range VLANs (VLAN IDs 1 to 1005).

- Extended-range VLANs (IDs greater than 1005) are not supported by VTP.
## VTP benefits

### VTP Benefits
- VLAN configuration consistency across the network
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs across a network
- Dynamic trunk configuration when VLANs are added to the network

---

### What is VTP?

1. **VLAN30**
   - **S1**: VTP Server
   - **F0/1**, **F0/3**: Ports
   - **VLAN30**
   - **S2**: VTP Enabled Switches
   - **S3**: VTP Enabled Switches

---

[Image: Diagram of VTP configuration]

www.ncp.edu.pk
VTP Components

- **VTP Domain**: consists of one or more interconnected switches.
- All switches in a domain share VLAN configuration details using VTP advertisements.
- A router or Layer 3 switch defines the boundary of each domain.
- **VTP Advertisements**: VTP uses a hierarchy of advertisements to distribute and synchronize VLAN configurations across the network.
- **VTP Modes**: A switch can be configured in one of three modes: server, client, or transparent.
- **VTP Pruning**: VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices.
Dynamic Trunking Protocol
Introduction to DTP

- Switch ports can be manually configured to form trunks
- Switch ports can also be configured to negotiate and establish a trunk link with a connected peer
- Dynamic Trunking Protocol (DTP) is a protocol to manage trunk negotiation
- DTP is a Cisco proprietary protocol and is enabled by default in Cisco Catalyst 2960 and 3560 switches
- If the port on the neighbor switch is configured in a trunk mode that supports DTP, it manages the negotiation
- The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto
Dynamic Trunking Protocol

Negotiated Interface Modes

- Cisco Catalyst 2960 and 3560 support the following trunk modes:
  - switchport mode dynamic auto
  - switchport mode dynamic desirable
  - switchport mode trunk
  - switchport nonegotiate
Routing Concepts

Routing Protocols
Functions of a Router

Why Routing?

- The router is responsible for the routing of traffic between networks.

Cisco IOS command line interface (CLI) can be used to view the route table.
Functions of a Router

Routers Interconnect Networks

- Routers can connect multiple networks.
- Routers have multiple interfaces, each on a different IP network.
Functions of a Router

Routers Choose Best Paths

- Determine the best path to send packets
  
  Uses its routing table to determine path

- Forward packets toward their destination
  
  Forwards packet to interface indicated in routing table.
  Encapsulates the packet and forwards out toward destination.

- Routers use static routes and dynamic routing protocols to learn about remote networks and build their routing tables.
Functions of a Router

Packet Forwarding Methods

- **Process switching** – An older packet forwarding mechanism still available for Cisco routers.

- **Fast switching** – A common packet forwarding mechanism which uses a fast-switching cache to store next hop information.

- **Cisco Express Forwarding (CEF)** – The most recent, fastest, and preferred Cisco IOS packet-forwarding mechanism. Table entries are not packet-triggered like fast switching but change-triggered.
Connect Devices

Default Gateways

To enable network access devices must be configured with the following IP address information:

- **IP address** - Identifies a unique host on a local network.

- **Subnet mask** - Identifies the host’s network subnet.

- **Default gateway** - Identifies the router a packet is sent to when the destination is not on the same local network subnet.

<table>
<thead>
<tr>
<th>Destination MAC Address</th>
<th>Source MAC Address</th>
<th>Source IP Address</th>
<th>Destination MAC Address</th>
</tr>
</thead>
</table>
Network Documentation should include at least the following in a topology diagram and addressing table:

- Device names
- Interfaces
- IP addresses and subnet mask
- Default gateways
Connect Devices

Enable IP on a Host

- **Statically Assigned IP address** – host is manually assigned the IP address, subnet mask and default gateway. DNS server IP address can also be assigned.
  
  Used to identify specific network resources such as network servers and printers
  
  Can be used in very small networks with few hosts.

- **Dynamically Assigned IP Address** – IP Address information is dynamically assigned by a server using Dynamic Host Configuration Protocol (DHCP)
  
  Most hosts acquire their IP address information through DHCP
Connect Devices

Enable IP on a Switch

- Network infrastructure devices require IP addresses to enable remote management.
- On a switch the management IP address is assigned on a virtual interface.

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.10.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#
S1(config)#ip default-gateway 192.168.10.1
S1(config)#
```
Basic Settings on a Router

Configure Basic Router Settings

Basics tasks that should be first configured on a Cisco Router and Cisco Switch:

- **Name the device** – Distinguishes it from other routers

- **Secure management access** – Secures privileged EXEC, user EXEC, and Telnet access, and encrypts passwords to their highest level

- **Configure a banner** – Provides legal notification of unauthorized access.

```plaintext
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#
```
Basic Settings on a Router

Configure Router Interfaces

To be available a router interface must be:

- **Configured with an address and subnet mask**.
- **Activated** – by default LAN and WAN interfaces are not activated. Must be activated using no shutdown command.
- Other parameters - serial cable end labeled DCE must be configured with the **clock rate** command.
- Optional description can be included.

```bash
R1(config)#interface gigabitethernet 0/0
R1(config-if)#description Link to LAN 1
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

*Jan 30 22:04:47.551: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down

```bash
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

R1(config)#
Basic Settings on a Router

Configure a Loopback Interface

- Loopback interface is a logical interface internal to the router.
- It is not assigned to a physical port, it is considered a software interface that is automatically in an UP state.
- Useful for testing and important in the OSPF routing process.

```
R2(config)#interface loopback 0
R2(config-if)#ip address 10.0.0.1 255.255.255.0
R2(config-if)#exit
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface loopback0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface loopback0, changed state to up
```
Verify Connectivity of Directly Connected Networks

Verify Interface Settings

Show commands to verify operation and configuration of interface.

- `show ip interfaces brief`
- `show ip route`
- `show running-config`

Show commands to gather more detailed interface information.

- `show interfaces`
- `show ip interfaces`

Verify the Routing Table

View the output of `show ip route` command.

Gateway of last resort is not set

```
192.168.10.0/24 is variably subnets, 2 subnets, 2 max hops
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
```

```
192.168.11.0/24 is variably subnets, 2 subnets, 2 max hops
C 192.168.11.0/24 is directly connected, GigabitEthernet0/0
L 192.168.11.1/32 is directly connected, GigabitEthernet0/0
```

```
209.165.200.0/24 is variably subnets, 2 subnets, 2 max hops
C 209.165.200.0/24 is directly connected, GigabitEthernet0/0
L 209.165.200.1/32 is directly connected, GigabitEthernet0/0
```
Switching Packets between Networks

Router Switching Functions

Encapsulating and De-Encapsulating Packets
Switching Packets between Networks

Send a Packet

PC1 Sends a Packet to PC2

Because PC2 is on different network, I will encapsulate the packet and send it to the router on MY network. Let me find that MAC address....

Layer 2 Data Link Frame

<table>
<thead>
<tr>
<th>Dest. MAC</th>
<th>Source MAC</th>
<th>Type</th>
<th>Packet's Layer 3 data</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-10</td>
<td>0A-10</td>
<td>800</td>
<td>Source IP 192.168.1.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dest. IP 192.168.4.10</td>
</tr>
</tbody>
</table>

PC1's ARP Cache for R1

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>00-10</td>
</tr>
</tbody>
</table>
Switching Packets between Networks
Forward to the Next Hop

R3 Forwards the Packet to PC2

Layer 2 Data Link Frame

<table>
<thead>
<tr>
<th>Dest. MAC</th>
<th>Source MAC</th>
<th>Type</th>
<th>Source IP</th>
<th>Dest. IP</th>
<th>IP fields</th>
<th>Data</th>
<th>Trailer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0B-31</td>
<td>00-20</td>
<td>800</td>
<td>192.168.1.10</td>
<td>192.168.4.10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

R1’s Routing Table

<table>
<thead>
<tr>
<th>Network</th>
<th>Hops</th>
<th>Next-hop-IP</th>
<th>Exit Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td>0</td>
<td>Dir. Connect.</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>192.168.2.0/24</td>
<td>0</td>
<td>Dir. Connect.</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>1</td>
<td>192.168.2.2</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>2</td>
<td>192.168.2.2</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>
Switching Packets between Networks
Packet Routing

R2 Forwards the Packet to R3

Layer 2 Data Link Frame

Packet’s Layer 3 data

R2’s Routing Table

<table>
<thead>
<tr>
<th>Network</th>
<th>Hops</th>
<th>Next-hop-IP</th>
<th>Exit Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td>1</td>
<td>192.168.3.1</td>
<td>Fa/0/0</td>
</tr>
<tr>
<td>192.168.2.0/24</td>
<td>0</td>
<td>Dir. Connect.</td>
<td>Fa/0/0</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>0</td>
<td>Dir. Connect.</td>
<td>S0/0/0</td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>1</td>
<td>192.162.3.2</td>
<td>S0/0/0</td>
</tr>
</tbody>
</table>
Switching Packets between Networks

Reach the Destination

R3 Forwards the Packet to PC2

My ARP table tells me that PC2 uses MAC address 0B-20.

Layer 2 Data Link Frame

<table>
<thead>
<tr>
<th>Layer 2 Data Link Frame</th>
<th>Packet’s Layer 3 data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest. MAC 0B-20</td>
<td>Source MAC 0C-22</td>
</tr>
<tr>
<td>Source IP 192.168.1.10</td>
<td>Dest. IP 192.168.4.10</td>
</tr>
<tr>
<td>IP fields</td>
<td>Data</td>
</tr>
<tr>
<td>Trailer</td>
<td></td>
</tr>
</tbody>
</table>

R3’s ARP Cache

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.4.10</td>
<td>0B-20</td>
</tr>
</tbody>
</table>

R3’s Routing Table

<table>
<thead>
<tr>
<th>Network</th>
<th>Hops</th>
<th>Next-hop-IP</th>
<th>Exit Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td>2</td>
<td>192.168.3.1</td>
<td>S0/0/0</td>
</tr>
<tr>
<td>192.168.2.0/24</td>
<td>1</td>
<td>192.168.3.1</td>
<td>S0/0/0</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>0</td>
<td>Dir. Connect.</td>
<td>S0/0/0</td>
</tr>
<tr>
<td>192.168.4.0/24</td>
<td>0</td>
<td>Dir. Connect.</td>
<td>Fa0/0</td>
</tr>
</tbody>
</table>
Path Determination
Routing Decisions

Packet Forwarding Decision Process

Packet arrives on interface.

Router searches the routing table for a match.

Does the destination IP address match the subnet of a…

Directly Connected Interface?

Yes

Check ARP cache (ARP if necessary) and forward to host on local subnet.

No

Remote network?

Yes

Encapsulate the frame and forward out of the exit interface to the next hop.

No

Is there a gateway of last resort available?

Drop the packet and send an ICMP message back to the source IP address.

Yes

Encapsulate the frame and forward out of the exit interface to the next hop.
Path Determination

**Best Path**

- Best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network.

- A metric is the value used to measure the distance to a given network.

- Best path to a network is the path with the lowest metric.

- Dynamic routing protocols use their own rules and metrics to build and update routing tables for example:
  
  **Routing Information Protocol (RIP)** - Hop count

  **Open Shortest Path First (OSPF)** - Cost based on cumulative bandwidth from source to destination

  **Enhanced Interior Gateway Routing Protocol (EIGRP)** - Bandwidth, delay, load, reliability
Path Determination

Load Balancing

- When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally.
Path Determination of the route

Administrative Distance

- If multiple paths to a destination are configured on a router, the path installed in the routing table is the one with the best (lowest) Administrative Distance (AD).

- Administrative Distance is the “trustworthiness” of the route.

- The Lower the AD the more trustworthy the route.

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Administrative Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>0</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>IS-IS</td>
<td>115</td>
</tr>
<tr>
<td>External EIGRP</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
</tbody>
</table>
The Routing Table

Routing Table is a file stored in RAM that contains information about:

- Directly Connected Routes
- Remote Routes
- Network or Next hop Associations
The Routing Table
Routing Table Sources

- Show ip route command is used to display the contents of the routing table

- Directly connected interfaces - Added to the routing table when an interface is configured and active.

- Static routes - Added when a route is manually configured and the exit interface is active.

- Dynamic routing protocol - Added when EIGRP or OSPF are implemented and networks are identified.
The Routing Table

Routing Table Sources

Routing Table of R1

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D  10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
```
The Routing Table

Remote Network Routing Entries

- Interpreting the entries in the routing table.
Directly Connected Routes

**Directly Connected Interfaces**

- A newly deployed router, without any configured interfaces, has an empty routing table.

- An active, configured directly connected interface creates two routing table entries Link Local (L) and Directly Connected (C)

---

**Directly Connected Network Entry Identifiers**

**Legend**

- Identifies how the network was learned by the router.
- Identifies the destination network and how it is connected.
- Identifies the interface on the router connected to the destination network.
Directly Connected Routes

Directly Connected Interfaces

- A newly deployed router, without any configured interfaces, has an empty routing table.

- An active, configured directly connected interface creates two routing table entries Link Local (L) and Directly Connected (C).
Statically Learned Routes

Static Routes

- Manually configured
- Define an explicit path between two networking devices.
- Must be manually updated if the topology changes.
- Benefits include improved security and control of resources.

- Static route to a specific network.
  \[
  \text{ip route} \text{networkmask} \{\text{next-hop-ip} \mid \text{exit-intf}\}
  \]

- Default Static Route used when the routing table does not contain a path for a destination network.
  \[
  \text{ip route} 0.0.0.0 0.0.0.0 \{\text{exit-intf} \mid \text{next-hop-ip}\}
  \]
Statically Learned Routes

Static Routes Example
Dynamic Routing Protocols

Dynamic Routing

- Used by routers to share information about the reachability and status of remote networks.
- Performs network discovery and maintaining routing tables.
Dynamic Routing Protocols

IPv4 Routing Protocols

- Cisco ISR routers can support a variety of dynamic IPv4 routing protocols including:
  - **EIGRP** – Enhanced Interior Gateway Routing Protocol
  - **OSPF** – Open Shortest Path First
  - **IS-IS** – Intermediate System-to-Intermediate System
  - **RIP** – Routing Information Protocol
Dynamic Routing Protocols
IPv4 Routing Protocols

```
R1# show ip route
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

D*EX 0.0.0.0/0 [170/2297856] via 209.165.200.226, 00:07:29, Serial0/0/0
    10.0.0.0/24 is subnetted, 2 subnets
    D  10.1.1.0 [90/2172416] via 209.165.200.226, 00:07:29, Serial0/0/0
    D  10.1.2.0 [90/2172416] via 209.165.200.226, 00:07:29, Serial0/0/0

    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
    C  192.168.10.0/24 is directly connected, GigabitEthernet0/0
    L  192.168.10.1/32 is directly connected, GigabitEthernet0/0

    192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
    C  192.168.11.0/24 is directly connected, GigabitEthernet0/1
    L  192.168.11.1/32 is directly connected, GigabitEthernet0/1

    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
    C  209.165.200.224/30 is directly connected, Serial0/0/0
    L  209.165.200.225/32 is directly connected, Serial0/0/0

R1#
```
Inter-VLAN Routing

Routing And Switching
Inter-VLAN Routing Operation

What is Inter-VLAN Routing?

- Layer 2 switches can’t forward traffic between VLANs without the assistance of a router
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another using a router
The so-called router-on-a-stick approach uses a different path to route between VLANs.

One of the router’s physical interfaces is configured as a 802.1Q trunk port. Now that interface can understand VLAN tags.

Logical sub-interfaces are then created. One sub-interface per VLAN.

Each sub-interface is configured with an IP address from the VLAN it represents.

VLAN members (hosts) are configured to use the sub-interface address as a default gateway.

Only one of the router’s physical interface is used.
Multilayer Switch Inter-VLAN Routing

- Multilayer switches can perform Layer 2 and Layer 3 functions. Routers are not required anymore.
- Each VLAN existent in the switch is a SVI.
- SVI are seen as layer 3 interfaces.
- The switch understands network layer PDUs and therefore, it can route between its SVIs just as a router routes between its interfaces.
- With a multilayer switch, traffic is routed internal to the switch device.
- Very scalable solution.
Configure Router-On-A-Stick

Preparation

- An alternative to legacy inter-VLAN routing is to use VLAN trunking and sub-interfaces
- VLAN trunking allows a single physical router interface to route traffic for multiple VLANs
- The physical interface of the router must be connected to a trunk link on the adjacent switch
- On the router, sub-interfaces are created for each unique VLAN on the network
- Each sub-interface is assigned an IP address specific to its subnet/VLAN and is also configured to tag frames for that VLAN
Configure Router-On-A-Stick
Switch Configuration

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```
Configure Router-On-A-Stick

Router Interface Configuration

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
```

* Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
* Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
* Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on changed state to down
* Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
* Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Configure Router-On-A-Stick

Verifying Sub-interfaces

```
R1# show vlans
<output omitted>
Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/0.10

Protocols Configured: Address: Received: Transmitted:
IP 172.17.10.1 11 18
<output omitted>

Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/0.30

Protocols Configured: Address: Received: Transmitted:
IP 172.17.30.1 11 8
<output omitted>
```
Configure Router-On-A-Stick

Verifying Sub-interfaces

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
       type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       O - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
    C 172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
    L 172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
    C 172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
    L 172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```


**Configure Router-On-A-Stick**

**Verifying Routing**

- Access to devices on remote VLANs can be tested using the **ping** command.
- The **ping** command sends an ICMP echo request to the destination address.
- When a host receives an ICMP echo request, it responds with an ICMP echo reply.
- Tracert is a useful utility for confirming the routed path taken between two devices.
Layer 3 switching usually have packet-switching throughputs in the millions of packets per second (pps).

All Catalyst switches support two types of Layer 3 interfaces:
  - Routed Port
  - SVI

High-performance switches, such as the Catalyst 6500 and Catalyst 4500, are able to perform most of the router’s functions.

But several models of Catalyst switches require enhanced software for specific routing protocol feature.
Inter-VLAN Routing with SVIs

- Today routing has become faster and cheaper and can be performed at hardware speed.
- It can be transferred to core and distribution devices with little to no impact on network performance.
- Many users are in separate VLANs, and each VLAN is usually a separate subnet.
- This implies that each distribution switch must have IP addresses matching each access switch VLAN.
- Layer 3 (routed) ports are normally implemented between the distribution and the core layer.
By default, an SVI is created for the default VLAN (VLAN1). This allows for remote switch administration.

Any additional SVIs must be created by the admin.

SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI.

The `interface vlan 10` entered by the first time creates an SVI named VLAN 10.

The VLAN number used corresponds to the VLAN tag associated with data frames on an 802.1Q encapsulated trunk.

Whenever the SVI is created, ensure that particular VLAN is present in the VLAN database.
SVIs advantages include:

- It is much faster than router-on-a-stick, because everything is hardware switched and routed.
- No need for external links from the switch to the router for routing.
- Not limited to one link. Layer 2 EtherChannels can be used between the switches to get more bandwidth.
- Latency is much lower, because it does not need to leave the switch.
Troubleshooting Layer 3 Switching

Layer 3 Switching Configuration Issues

- To troubleshoot Layer 3 switching issues, check the following items for accuracy:

  - **VLANs**
    - VLANs must be defined across all the switches
    - VLANs must be enabled on the trunk ports
    - Ports must be in the right VLANs

  - **SVIs**
    - SVI must have the correct IP address or subnet mask
    - SVI must be up
    - SVI must match with the VLAN number
To troubleshoot Layer 3 switching issues, check the following items for accuracy (cont):

- **Routing**
  - Routing must be enabled
  - Each interface or network should be added to the routing protocol

- **Hosts**
  - Hosts must have the correct IP address or subnet mask
  - Hosts must have a default gateway associated with an SVI or routed port