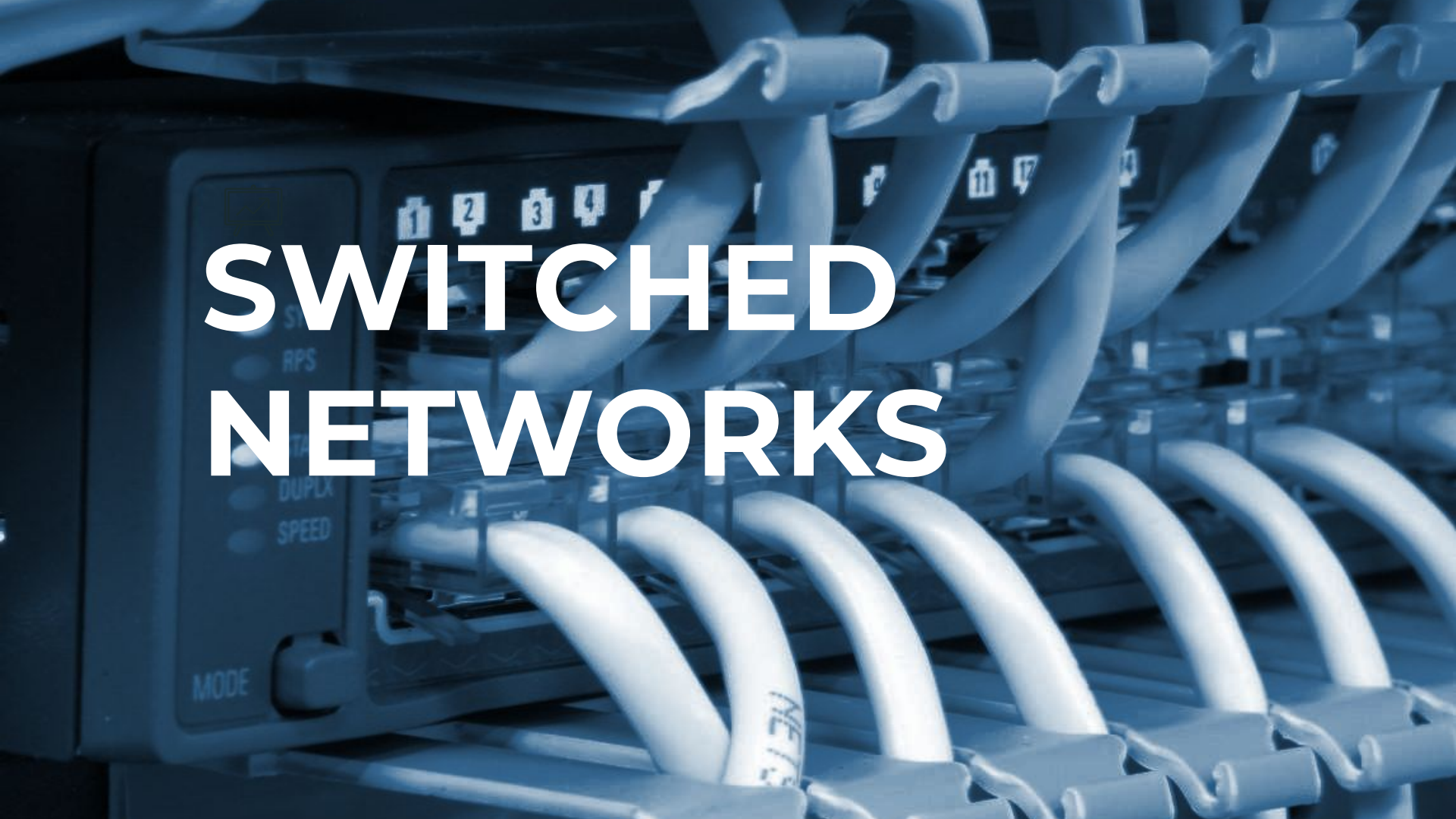
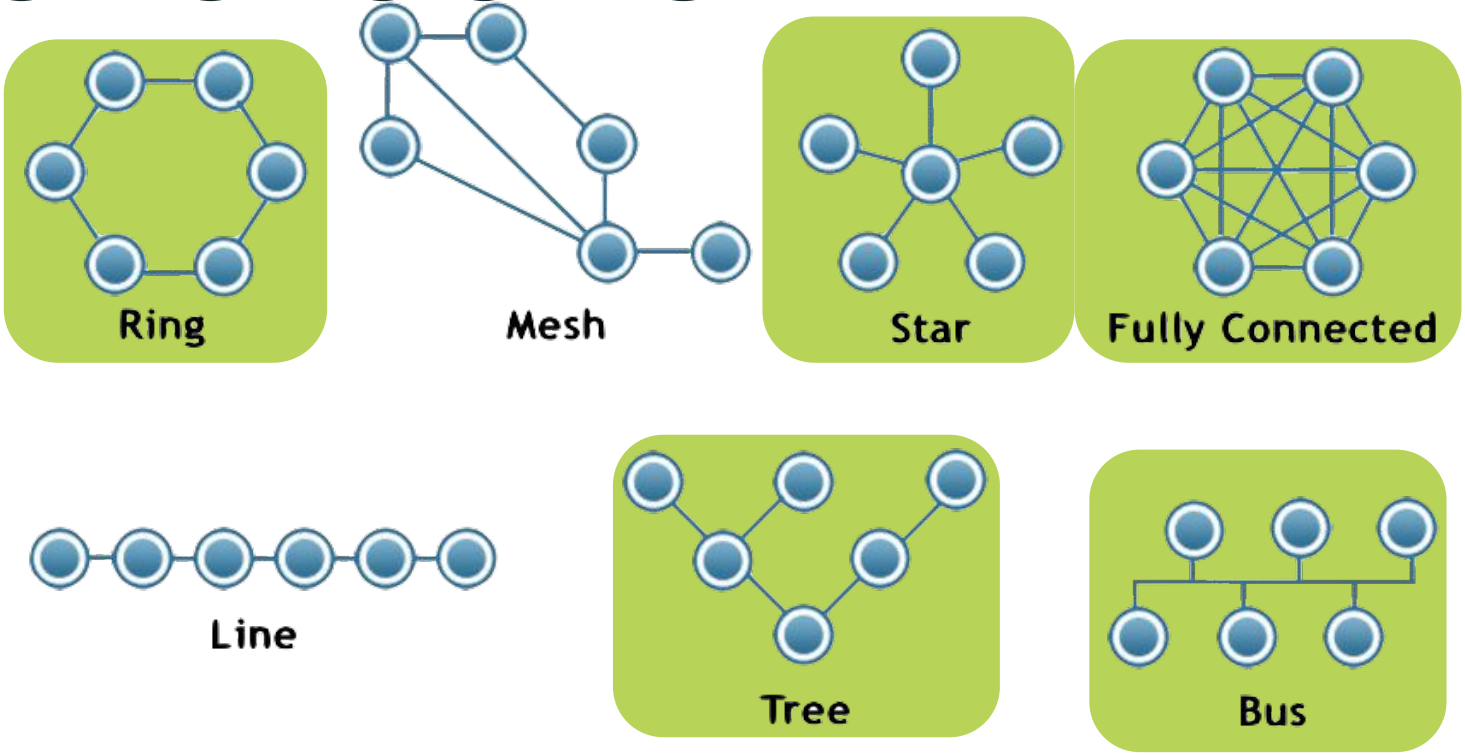


SWITCHED NETWORKS

Important Terms

- **Switch** – Layer 2 device used to connect end devices to routers
- **LAN** – Local Area Network; group of devices in an enclosed network
- **Legacy equipment** – devices no longer in production but are still in use
- **Converged network** – modern network that supports multiple functions (phone, web, video)
- **MAC address** – Layer 2 device identifier

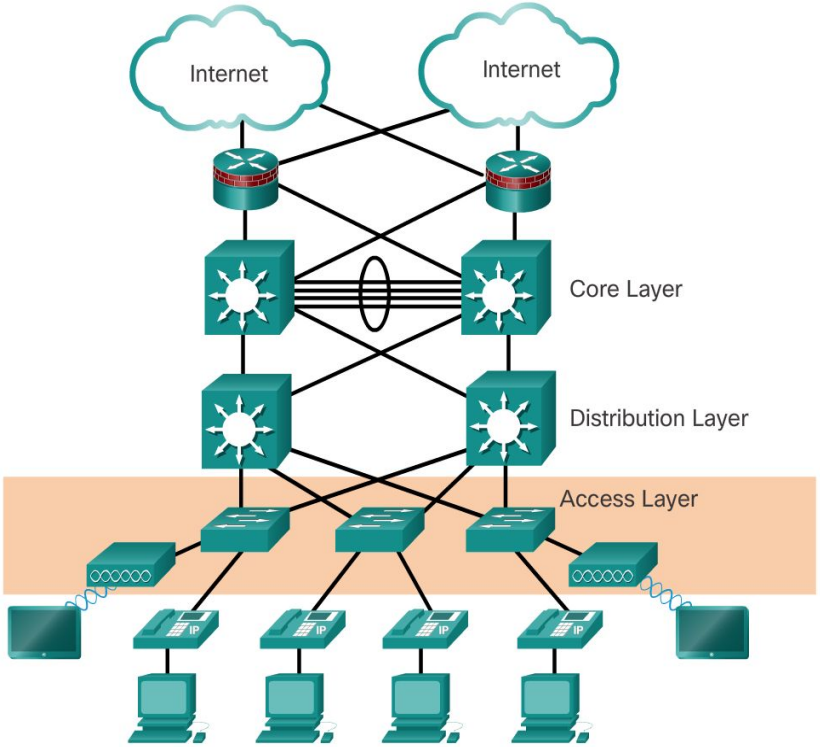
NETWORK TOPOLOGIES

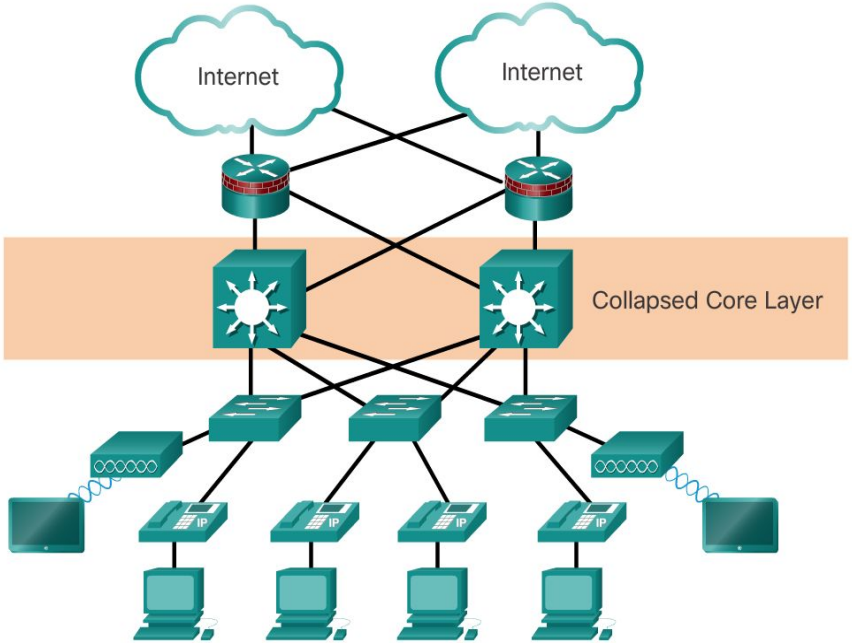


Principles of Switched Network Design

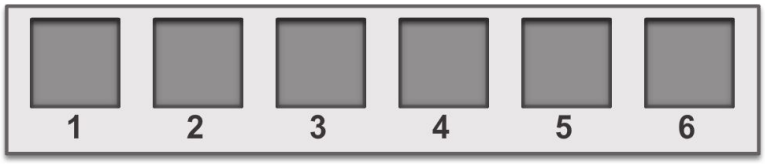
- **Hierarchical design –** tiered approach used to simplify deployment, operation, and management
- **Modularity –** allows for network expansion and adaptability
- **Resiliency –** network must always be accessible
- **Flexibility –** allows intelligent traffic load sharing by using all network resources

2 AND 3 TIER DESIGNS





Frame Processing



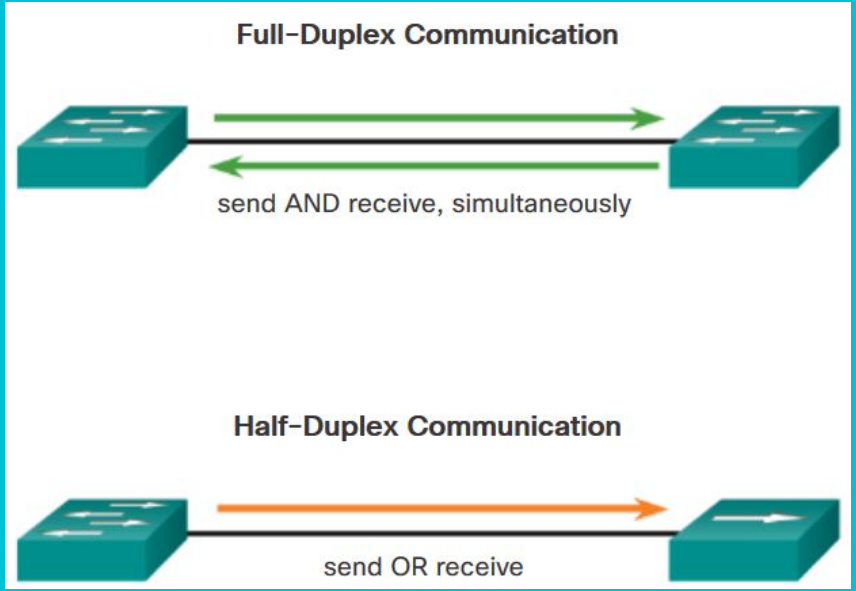
Port Table

Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

- Switch maintains a table of MAC addresses and their corresponding ports
- Ingress port is irrelevant
- If destination device is not in table, the frame is flooded to all ports and response is recorded
- Can use store-and-forward (layer 2 version of TCP), cut-through (layer 2 version of UDP), or fragment-free switching methods

Full- vs Half-Duplex

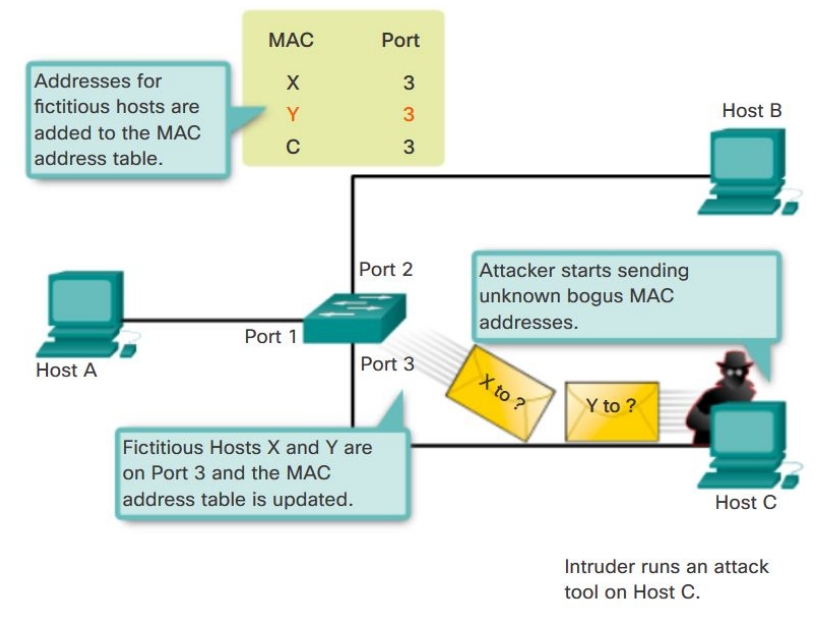
- Full-Duplex: Both devices on the connection can send and receive information at the same time
- Half-Duplex: Only one device can be sending data at a time



Cisco Switch IOS Commands

Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`

MAC Address Flooding



- MAC Address flooding happens when an attacker spams a switch with fictitious MAC addresses, filling its table with fake entries.
- Once the table is full, the switch acts like a hub.

Configuring Port Security

Step Description	Placement	Command	Category	Notes
set ports to access mode	switch interfaces leading to end devices	switchport mode access	requirement	sometimes pre-configured
enable port security	switch interface in access mode	switchport port-security	requirement	
set maximum MAC addresses allowed	switch interface	switchport port-security maximum [#]	optional	default is 1
set action in case of a violation	switch interface	switchport port-security violation [protect/restrict/shutdown]	optional	The modes: Protect: Drops frames from other MACs Restrict: Like protect, but logs violation Shutdown: Shuts down the port entirely
record MAC addresses as they are received	switch interface	switchport port-security mac-address sticky	optional	
manually add a secure MAC	switch interface	switchport port-security mac-address [MAC address]	optional	

SSH: Secure Shell

- SSH is a secure protocol for remotely logging into a device across a network.
- It can be used to configure a device without connecting via console cable.

SSH Configuration

Step Description	Placement	Command	Category	Notes
assign a hostname	router config	hostname [hostname]	requirement	hostname cannot be default
assign a domain name	router config	ip domain-name [domain name]	requirement	
generate RSA keys and enable SSH	router config	crypto key generate rsa	requirement	"crypto key zeroize rsa" to reverse the command; will be prompted to enter key size from 360-4096 after entering the command (1024+ recommended)
create at least one user account	router config	username [username] secret [password]	requirement	"privilege [0-15]" can be added after the username to set a privilege level; username is case-sensitive
only allow SSH on vty lines	all vty lines	transport input ssh	requirement	
require local authentication	all vty lines	login local	requirement	
turn on management VLAN	management VLAN	no shutdown	requirement	management VLAN must have an IP
set an enable password	router config	enable [password/secret] [password]	requirement	
set an SSH version	router config	ip ssh version [1/2]	optional	default supports versions 1 and 2
set a timeout for inactive connections	router config	ip ssh time-out [0-120]	optional	time is in seconds
set a limit for authentication retries	router config	ip ssh authentication [# of retries]	optional	

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash