




A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a dark blue background, resembling a circuit board or a network diagram.

NETWORKING FUNDAMENTALS

WEEK 2

INTRODUCTION TO WIRELESS NETWORKING

- Uses radio waves over specific frequencies to transfer data
 - Frequency – number of times a specific event occurs in a specified period of time
 - Page 116-117
- 1 cycle per second is 1 Hz
 - 1,000 Hz = 1 Kilohertz (KHz)
 - 1,000 KHz = 1 Megahertz (MHz)
 - 1,000 MHz = 1 Gigahertz (GHz)

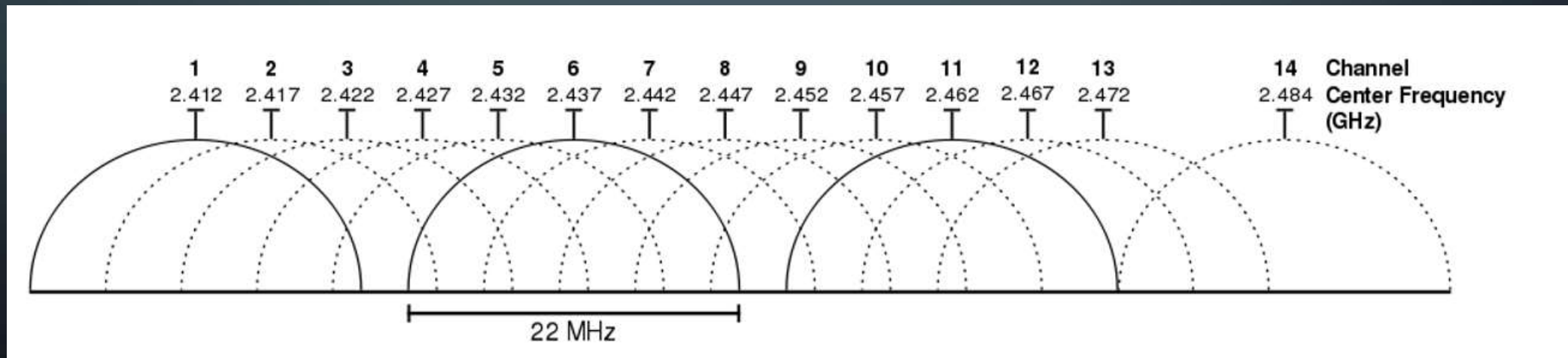
	$f = 0.5 \text{ Hz}$ $T = 2.0 \text{ s}$
	$f = 1.0 \text{ Hz}$ $T = 1.0 \text{ s}$
	$f = 2.0 \text{ Hz}$ $T = 0.5 \text{ s}$

2,4/5GHZ

- Both 2,4GHz and 5GHz are unlicensed frequencies
 - You are able to use them without special permits
- The both 2,4 and 5GHz range is split into several channels
- 5GHz can provide 23 Channels “non-overlapping” 20MHz each

2,4GHZ

- 14 Channels, each 22MHz. Channel Center Frequencies are 5Mhz apart
- Because of this, there is a lot of overlapping.



IEEE 802.11 STANDARDS

IEEE 802.11 Standard	Data Transfer Rate	Frequency
802.11a	54Mbps	5GHz
802.11b	11Mbps	2,4GHz
802.11g	54Mbps	2,4GHz
802.11n «WiFi 4»	600Mbps	Both 2,4 and 5GHz
802.11ac «WiFi 5»	1,3Gbps	5GHz

WIRELESS TOPOLOGIES

- Ad hoc – basically just peer-to-peer
 - Devices talk directly to each other without the need for a wireless access point
- Infrastructure mode
 - All communication goes through a wireless access point
 - May contain one or more WAPs
 - These WAPs can share the same SSID (Extended Service Set, Mesh)

Point-to-Point Wireless Bridge

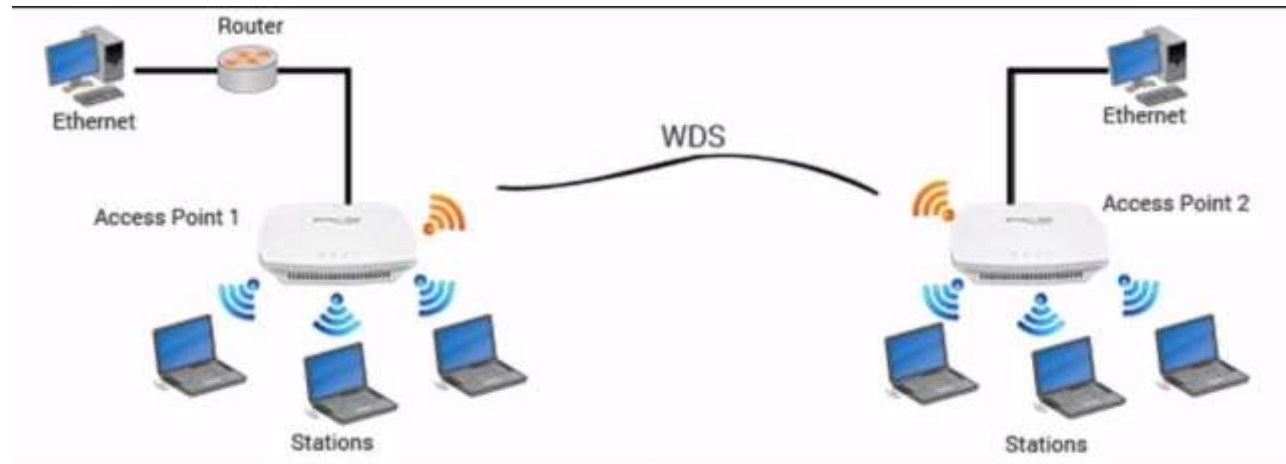
- Extend LAN across town or across campus—up to 15 miles away
- LWE200A-KIT includes a pair of radios pre-configured for plug-and-play deployments



POINT-TO-POINT WIRELESS BRIDGE

- Up to 15km range
- Requires line of sight
- Uses unidirectional antennas

WIRELESS DISTRIBUTION SYSTEM



- Wireless “Switching”
- Main base station – WAP that connects to the wired network.
- Remote base station – WAP that accepts connections from clients and relays that information to the main base station.
- Must use the same channel



WIRELESS SECURITY

CONFIDENTIALITY


Protecting data so that only the people who are authorized can see it

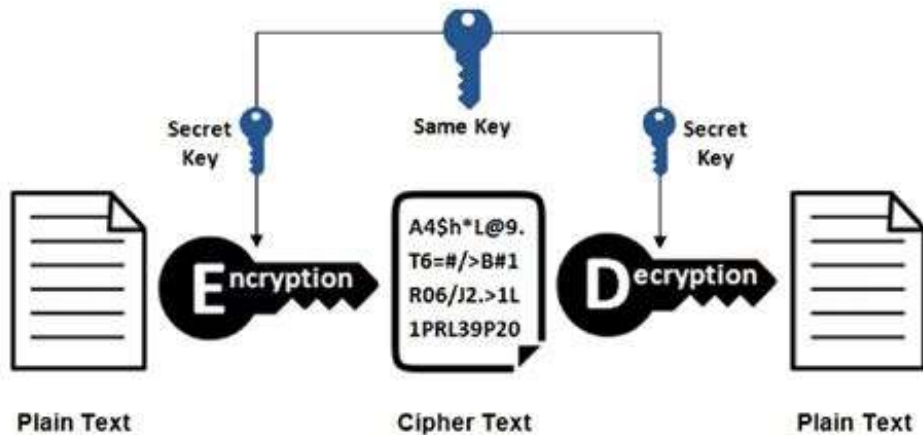
INTEGRITY

Can you trust the data, has it been changed.

AVAILABILITY

Ensures the data is available and ready to be used





ENCRYPTION

- Taking readable data (clear text) and putting it through a mathematical calculation (algorithm) to produce data that is not readable (cipher text)
- Symmetric encryption uses the same key to encrypt and decrypt.
- Asymmetrical encryption uses one key to encrypt, and a different key to decrypt.

WIRED EQUIVALENT PRIVACY

- First form of wireless encryption
- Uses a pre-configured password on the WAP to connect.
- Very outdated
- Do not use
- Can be cracked in 30 seconds

WIRELESS PROTECTED ACCESS

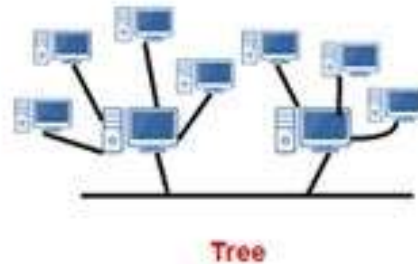
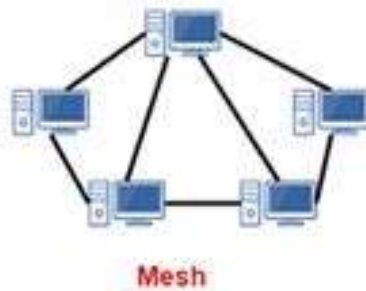
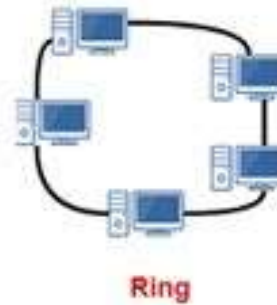
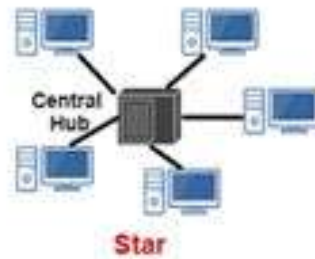
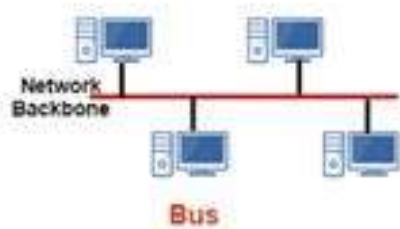
- More secure than WEP
- WPA has different versions, WPA, WPA2, WPA3
 - Usually more secure for each version
- Two formats, WPA-Personal and WPA-Enterprise
 - Personal uses a passphrase similar to WEP
 - Enterprise uses user credentials

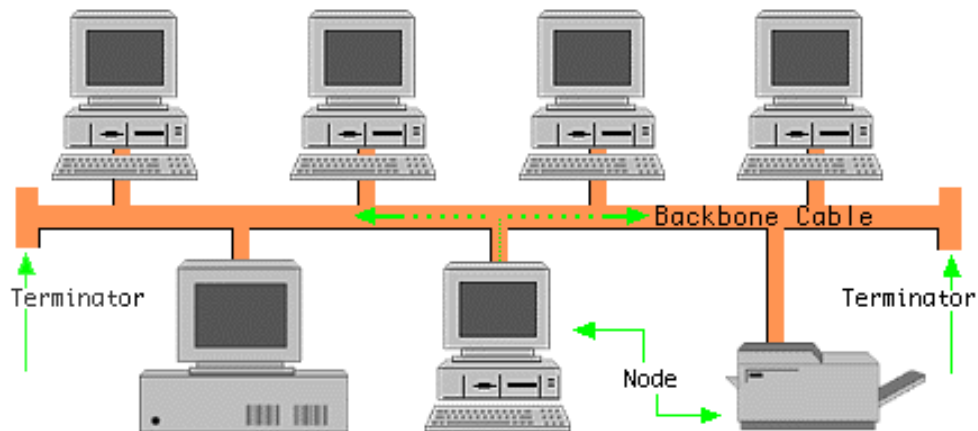
OTHER WIRELESS SECURITY TECHNIQUES

- Disable SSID Broadcast
- MAC-Filtering
- Disable WPS
- Reduce transmission power
- Change default username/password
- Segment your networks
- Scan for rogue WAPs

NETWORK TOPOLOGIES

- A map of the network
- Shows how clients and networking devices are connected together.



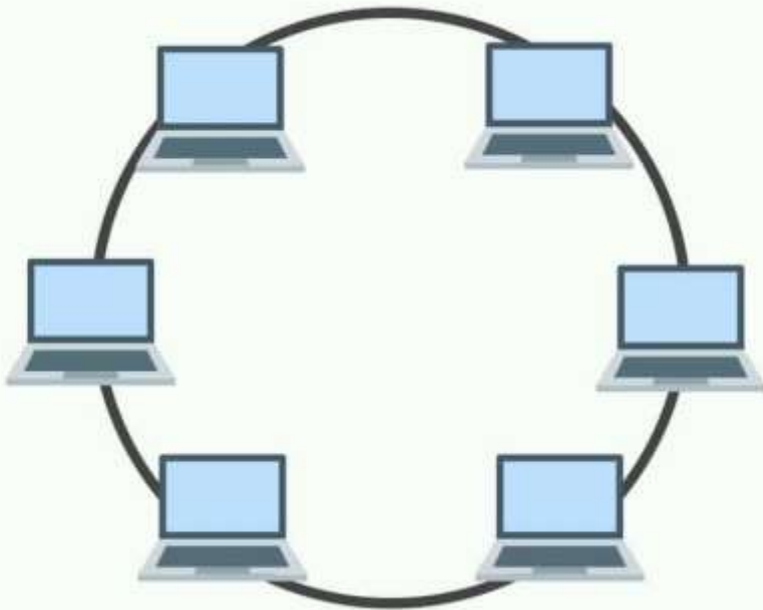


BUS TOPOLOGY

- All devices are connected to a backbone cable
- The Backbone cable has a terminator in both ends to prevent signals to bounce
- Functions like a hub, sends traffic to all devices
- Half-Duplex

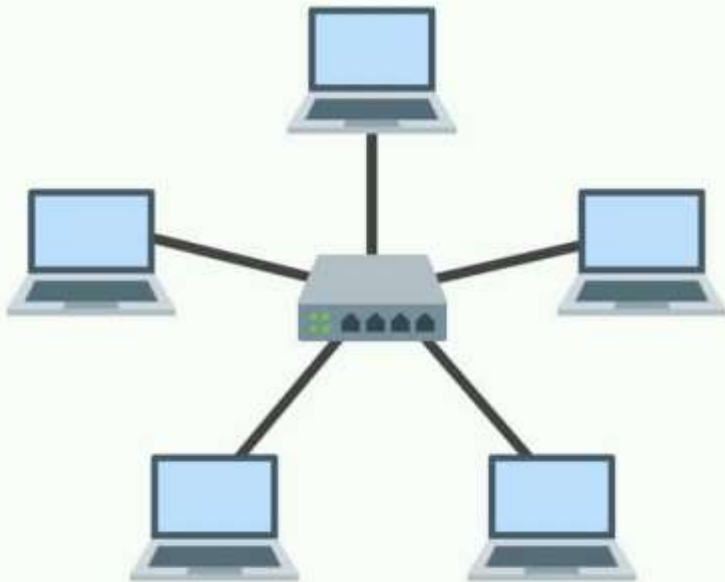
CSMA/CD

- Carrier Sense Multiple Access / Collision detection
 1. Listens if the medium (cable) is idle
 2. Sends traffic if idle, if there is another transmission it sets a random back off timer
 3. If a collision occurs, a jamming signal is sent out, telling all parties to stop sending traffic
 4. All devices then sets a random back off timer before they try to send traffic again



RING TOPOLOGY

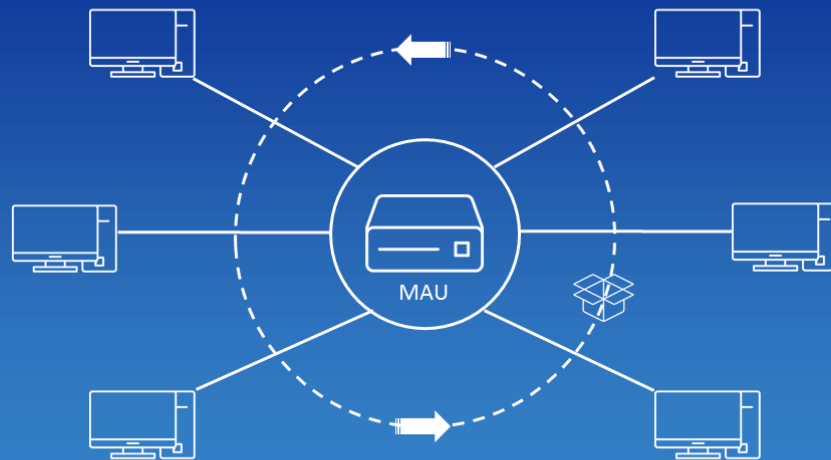
- Each devices is connected to two devices.
- Easy to troubleshoot, and there are no collisions on the network
- Can't add new devices without breaking up the network



STAR TOPOLOGY

- All devices are connected to a central point.
- Most common topology
- Easy to add new devices
- If the central device dies, so does your whole network

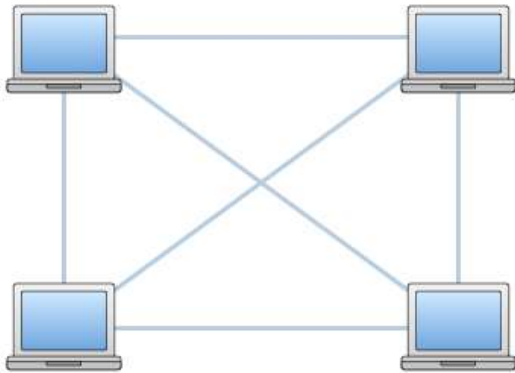
Token Ring



TOKEN RING

- Star topology, all devices are connected to central device (MAU)
 - Media access unit
- Devices can only talk when in possession of the token

MESH TOPOLOGY



- All devices are connected to every other device
- Very redundant/fault tolerant
- Requires a lot of interfaces and cables



SWITCHES AND SWITCHING

Forwarding traffic on a Local Network

SWITCH VS HUBS

SWITCH

- Breaks up collision domains
- Can be managed (change config)
- Can store MAC-addresses to make forwarding decisions

HUB

- 1 single collision domain
- Sends all traffic out all ports, other than receiving port

FRAME FORWARDING – 2 OPTIONS

CUT-THROUGH SWITCHING

- As soon as a switch has received the destination MAC address, it starts forwarding the frame
 - This is very fast, but can cause issue due to not checking for errors

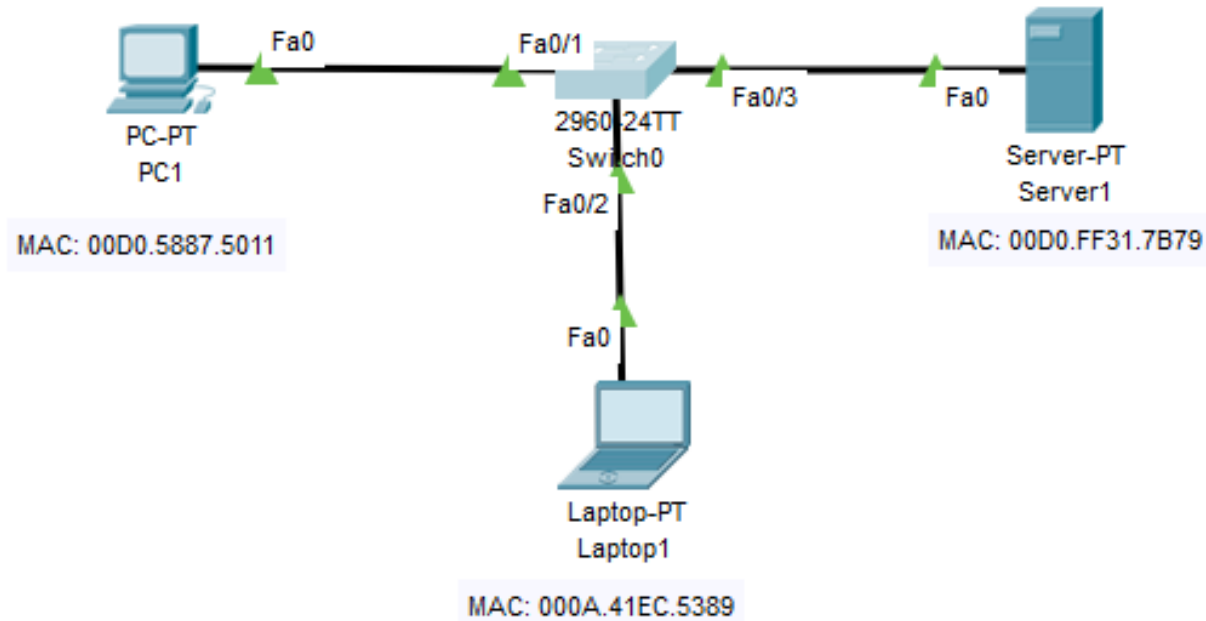
STORE AND FORWARD

- Forwards the frame only after the whole frame has been received, and an error check has been performed
 - Slower than Cut-through, but often considered better because of the error checking.

FRAME FORWARDING PROCESS

When a switch receives data:

1. It checks to see if the source MAC address is in the MAC table
 - If it isn't, the switch updates the table by specifying which interface the sender's MAC is on
2. Then it checks the same Table for an entry for the destination MAC
 - If there is, the frame is forwarded out said interface
 - If there isn't, the switch broadcasts the frame from all its interfaces, except the interface that received the frame (Similar to a Hub)
3. Hopefully the intended recipient will receive the frame and respond
4. The switch then repeats this process for returning traffic, but now it should know where the source and destination MAC is located



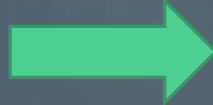
EXAMPLE: PC1 SENDS DATA TO SERVER1

1. PC1 sends data to the switch
2. The switch receives data and checks MAC table for an entry for PC1 (there is not)
3. Since no entry, the switch updates the table with the relevant information

```
Switch>show mac-address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
------	-------------	------	-------

```
Switch>
```



```
Switch>show mac-address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	00d0.5887.5011	DYNAMIC	Fa0/1

```
Switch>
```



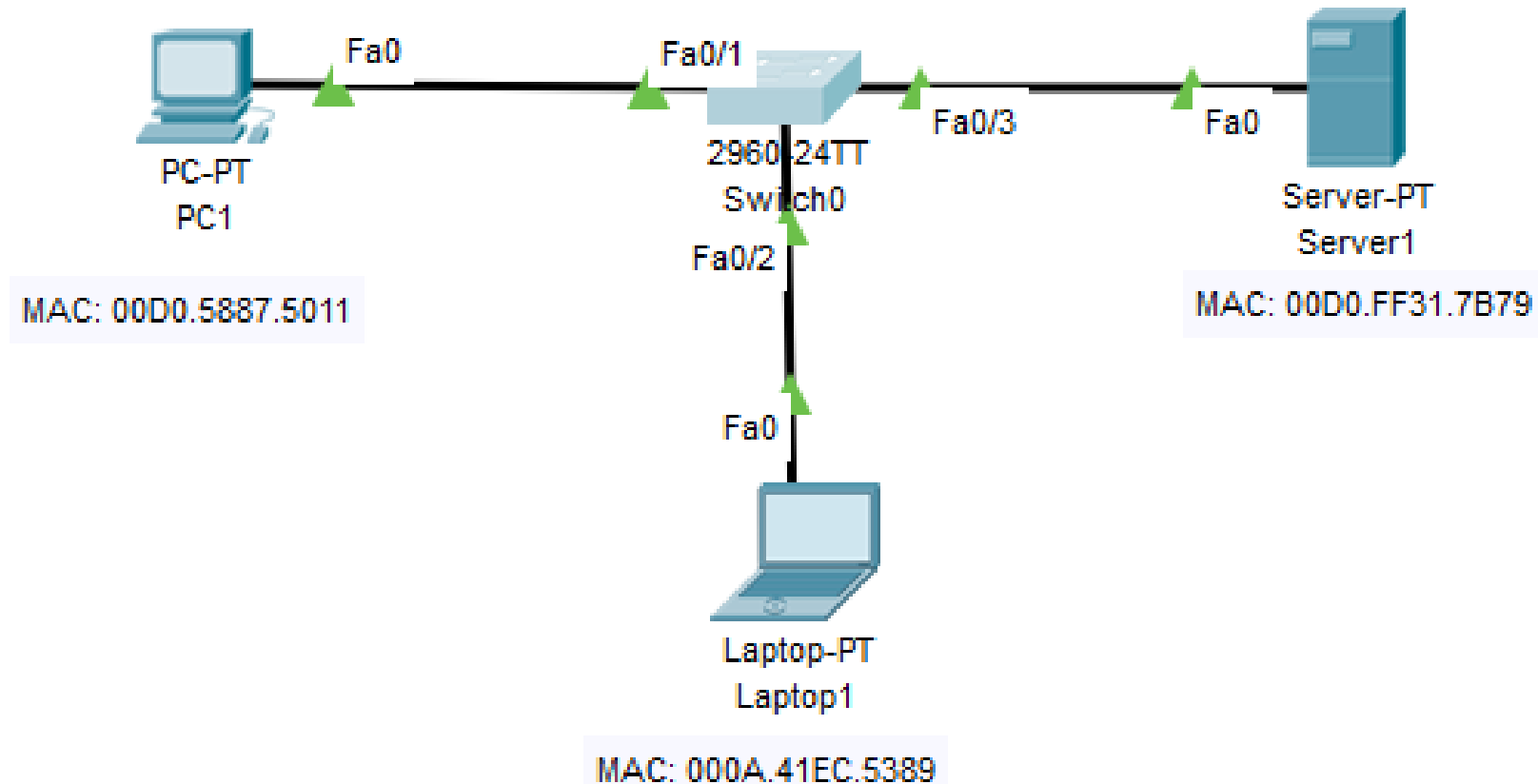
```
Switch>show mac-address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	00d0.5887.5011	DYNAMIC	Fa0/1
1	00d0.ff31.7b79	DYNAMIC	Fa0/3

```
Switch>
```

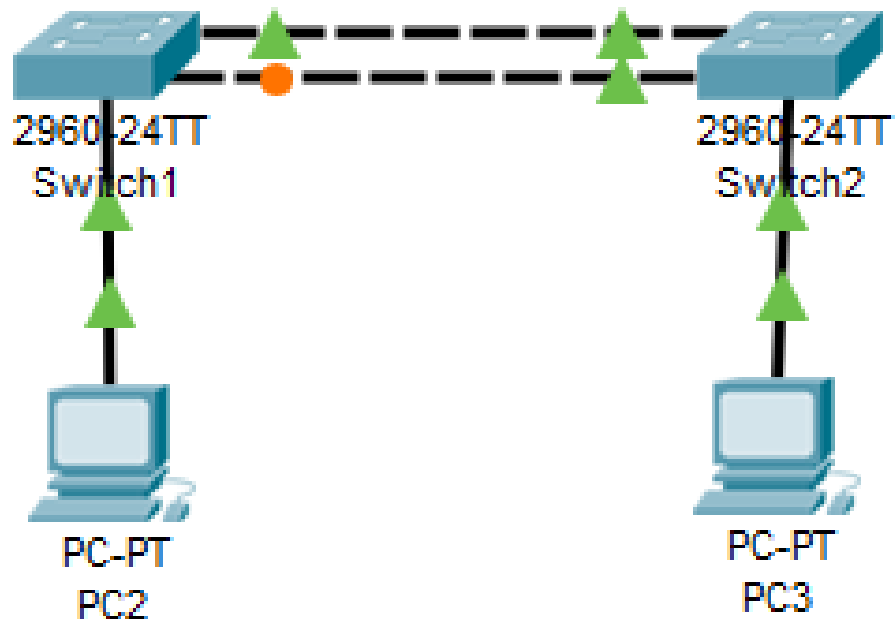
4. Switch checks MAC table for Destination MAC
5. Since missing, the frame is being sent out all interfaces (except fa0/1)
6. Both Laptop1 and Server1 will get the frame, Laptop1 ignores the frame as it's MAC does not match the destination MAC in the frame
7. Server1 will process the frame, and send a response
8. Switch receives frame, checks table for Source MAC
9. Since no entry in table, switch updates table with Server1's MAC address
10. The switch then checks table for an entry for the destination MAC (PC1)
11. Since this is already in the table, the frame gets forwarded

SUMMARY FRAME FORWARDING PROCESS



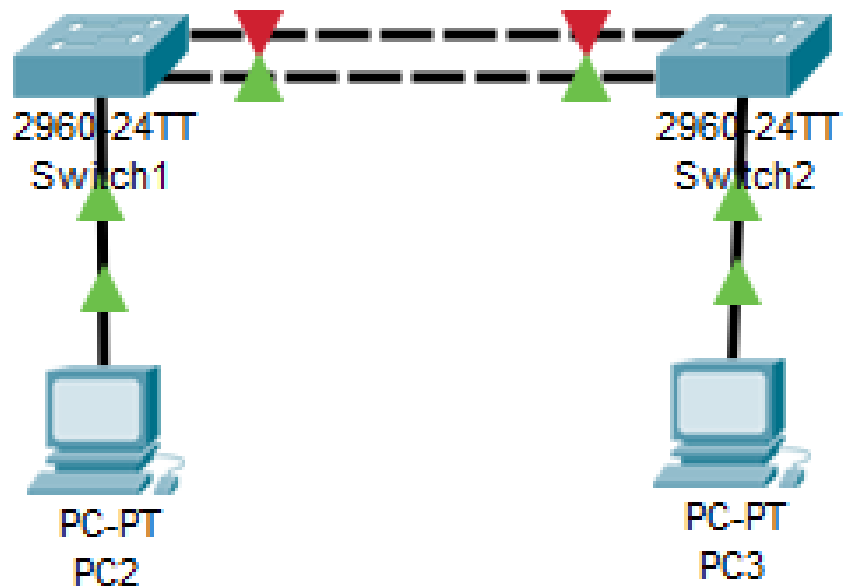
SPANNING TREE PROTOCOL

- STP is used to prevent loops (broadcast storms) when redundant links are implemented
- Switches has this enabled by default
- To identify a link being deactivated by STP, look for an orange colour on the port (both IRL and Packet Tracer)



SPANNING TREE PROTOCOL

- If one of the redundant links fails, or gets removed, the port blocked by STP will automatically get unblocked
 - With default settings, this takes 30 seconds.



MANAGED AND UNMANAGED SWITCHES

UNMANAGED

Comes preconfigured with default factory settings, cannot be changed.

MANAGED

Also comes preconfigured, ready to plug and play, but you can do so much more.

On a managed switch you can configure VLANS, port speeds, duplex settings etc.

To change config you often have to connect via console cable with a terminal emulator

SWITCH PORTS

AMOUNT

- Most standard managed switches has either 12, 24 or 48 ports
- Unmanaged switches usually has fewer ports

SPEEEEEEDS

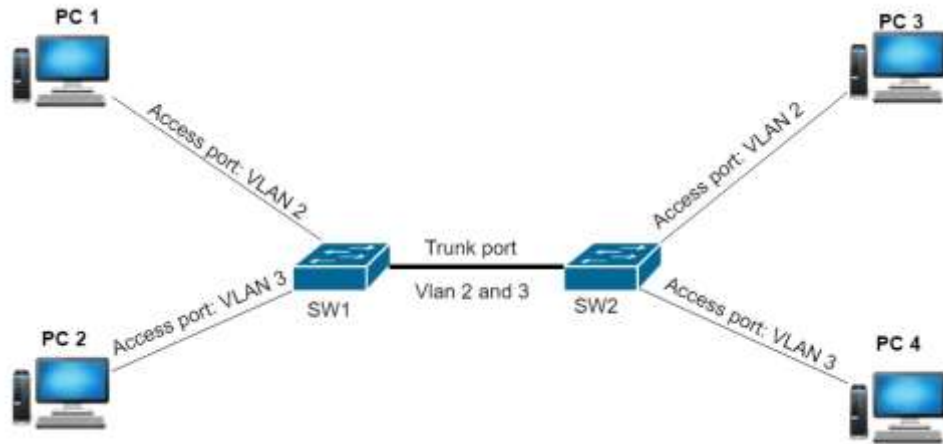
Switch port speeds vary by quite a lot

- Fast Ethernet – 10/100 Mbps
- Gigabit Ethernet – 10/100/1000 Mbps
- Ten Gigabit – 10/100/1000/10000 Mbps

LAYER 3 SWITCHES

- Some switches can also make forwarding decisions based on IP along with MAC addresses, these are called Layer 3 switches
- These switches can also route traffic, either by routing protocols or static routes

MORE VLANS



- Used to separate networks
- Needs a layer 3 switch or router to route traffic between different VLANS
- VLAN config is mostly done on switches
- You have 2 options for VLAN port settings
 - Access – Used to assign VLAN to ports
 - Trunk – Used to allow multiple VLANS to cross the same link.