1)Try Test-Connection and nslookup commands for below websites

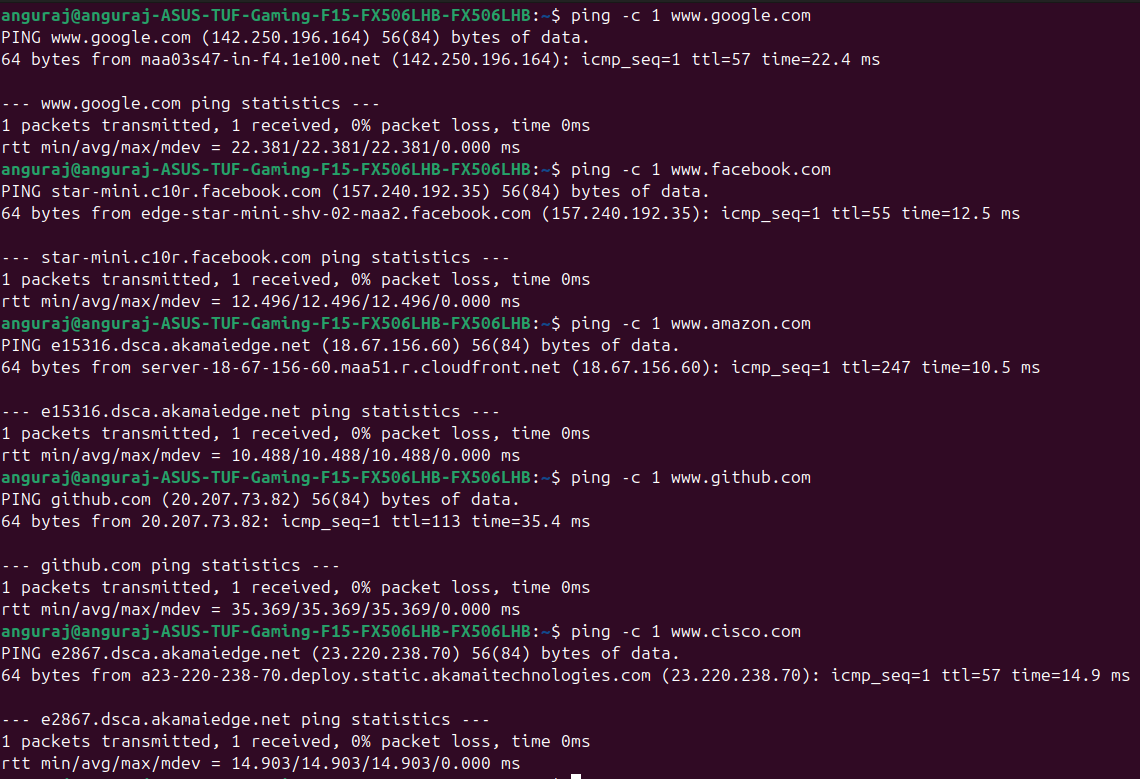
www.google.com

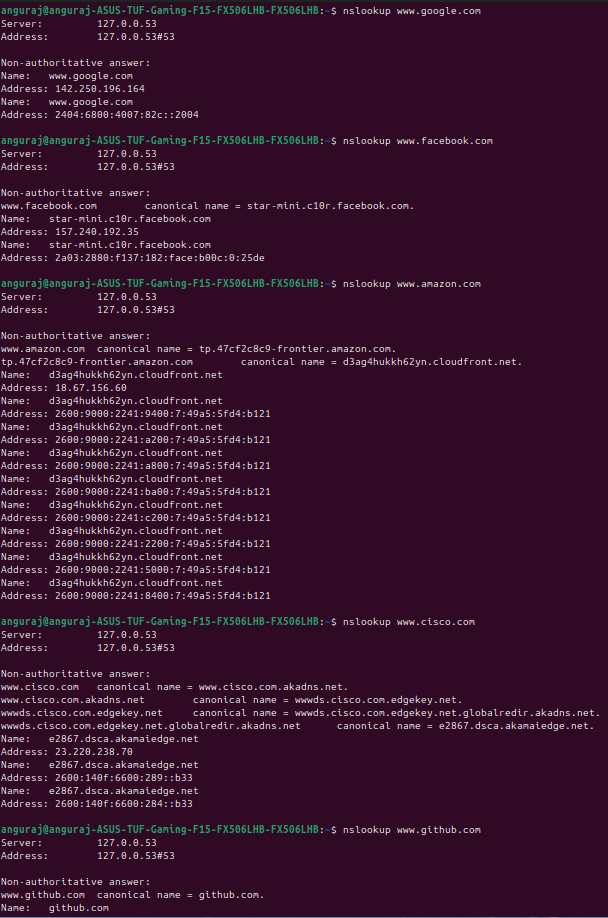
www.facebook.com

www.amazon.com

www.github.com

www.cisco.com





2.Use Wireshark to capture and analyze DNS, TCP, UDP traffic and packet header, packet flow, options and flags

**DNS**: Resolves domain names to IPs.

**TCP**: Connection-oriented, reliable communication with flags and sequence numbers.

**UDP**: Connectionless, faster but less reliable.  
  
**DNS Traffic Analysis**

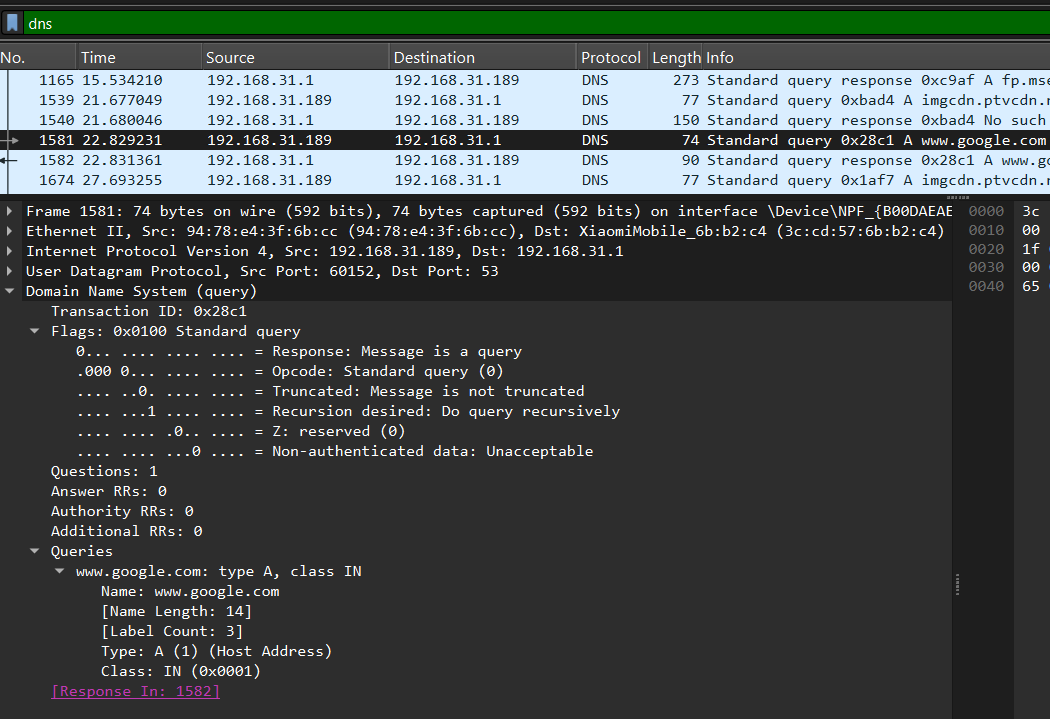
#### **Filter DNS Packets:** dns

#### **Key Fields to Analyze:**

* **Transaction ID**: Unique identifier for each query.
* **Flags**: Identifies query (0x0000) or response (0x8000).
* **Queries & Responses**: Shows domain resolution process.
* **Record Type**: A (IPv4), AAAA (IPv6), CNAME, MX.

#### **Example DNS Query Analysis:**

* A client requests www.google.com → Wireshark shows a query to a DNS server.
* The DNS server responds with an IP address.



### **TCP Traffic Analysis**

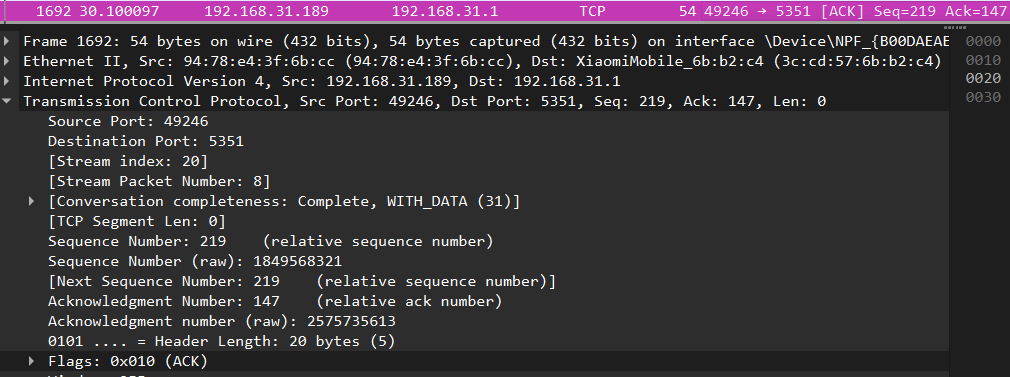
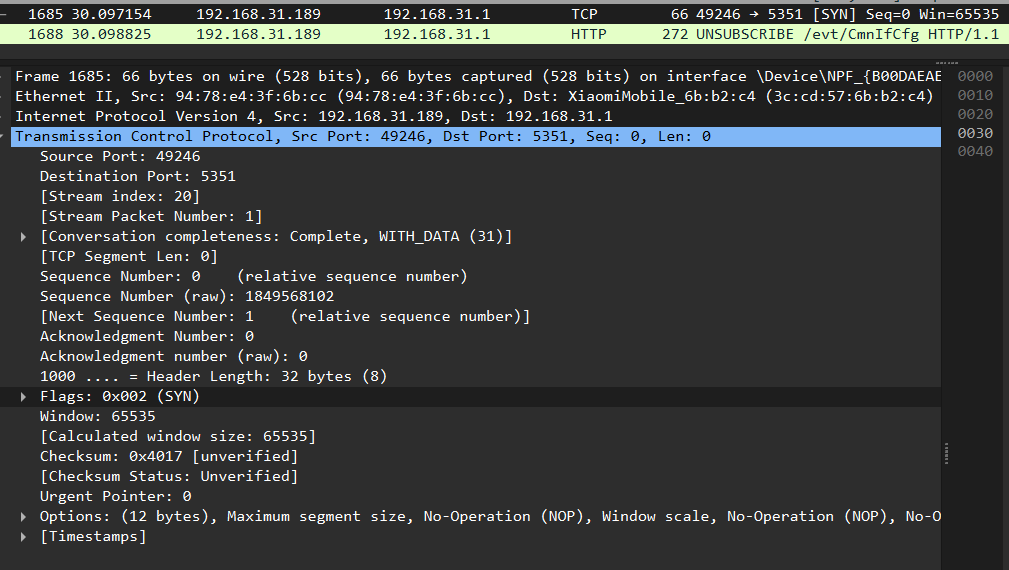
#### **Filter TCP Packets:** tcp

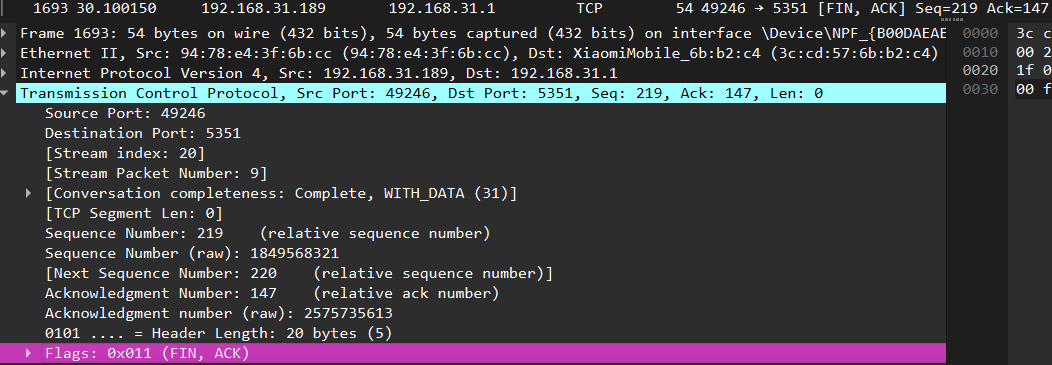
#### **Key Fields to Analyze:**

* **Source & Destination Ports**: Identifies the service (80, 443, 22).
* **Sequence & Acknowledgment Numbers**: Tracks communication flow.
* **TCP Flags:**
  + **SYN** (0x02) - Connection initiation.
  + **ACK** (0x10) - Acknowledgment.
  + **FIN** (0x01) - Connection termination.
  + **RST** (0x04) - Reset connection.

#### **Example TCP 3-Way Handshake Analysis:**

1. **SYN**: Client sends SYN to initiate connection.
2. **SYN-ACK**: Server responds with SYN-ACK.
3. **ACK**: Client sends final ACK, establishing a connection.





### **UDP Traffic Analysis**

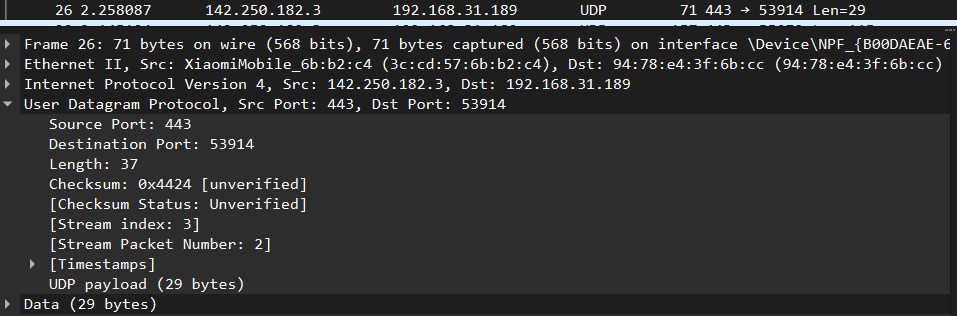
#### **Filter UDP Packets:** udp

#### **Key Fields to Analyze:**

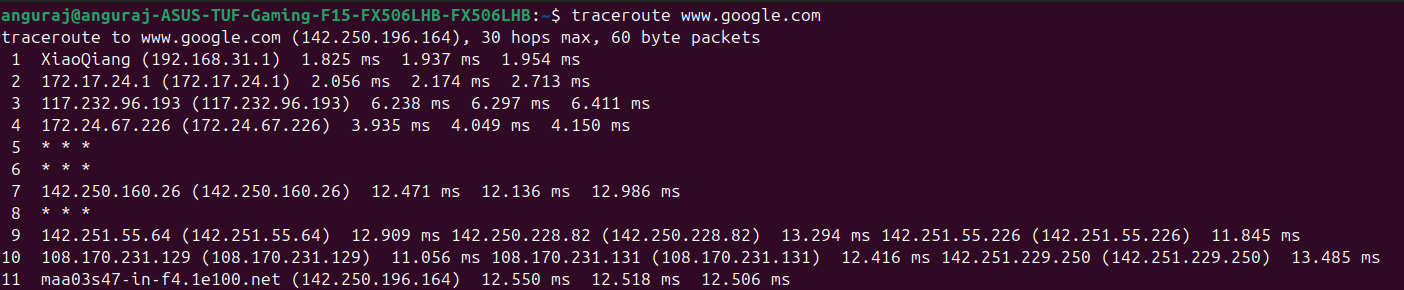
* **Source & Destination Ports**: Example - 53 (DNS), 67-68 (DHCP).
* **Length**: Size of the UDP payload.
* **Checksum**: Validates packet integrity.

#### **Example UDP Analysis:**

* DNS requests typically use UDP.



3.Explore traceroute/tracert for different websites eg:google.com and analyse the parameters in the output and explore different options for traceroute command



### **Columns Explanation**

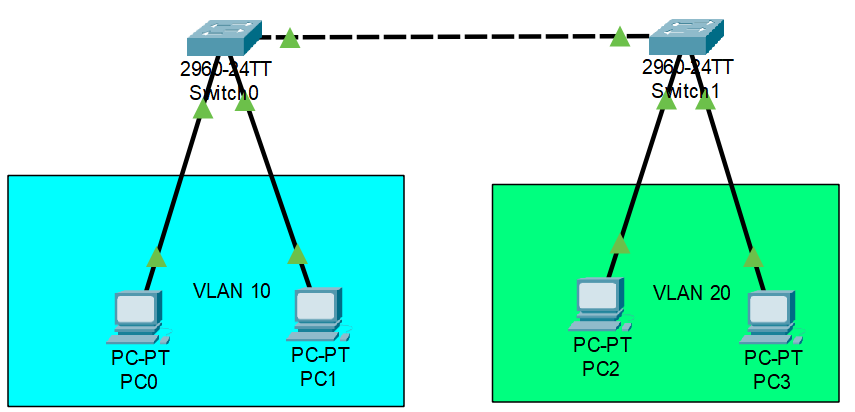
* **Hop Number**: Numbered list showing each router in the path.
* **IP Address / Hostname**: IP or resolved domain name of the router.
* **RTT (Round Trip Time) in ms**: Three response times indicate how long it took for a packet to reach the router and return.

### **Key Observations**

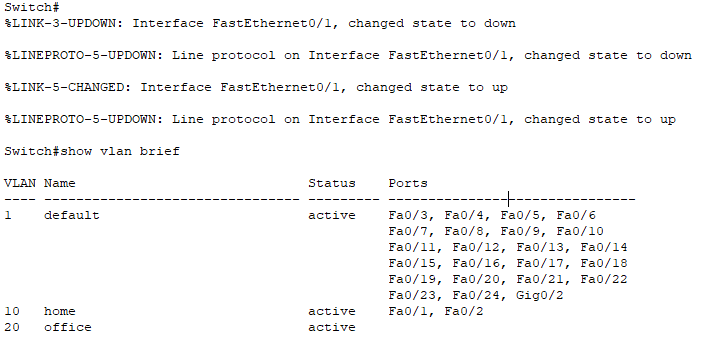
* \* \* \*: Indicates a timeout or a firewall blocking ICMP packets.
* Increasing latencies (ms values): Can indicate network congestion or distance.
* Private IPs (192.168.x.x / 10.x.x.x): Represent internal networks.

**Use Cisco packet tracer for the below**

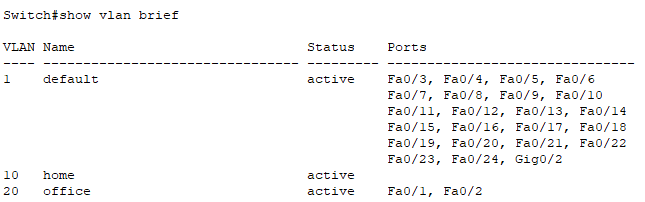
**Q4. Set up trunk ports between switches and try ping between different VLANS**

****

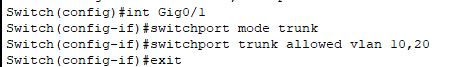
**Configuration in switch 0 (VLAN 10):**

****

**Configuration in switch 1 (VLAN 20):**

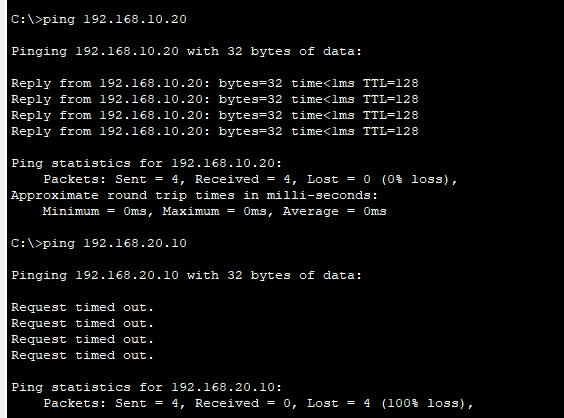


**Configuration for Trunk port between Switch 0 and switch 1 :**

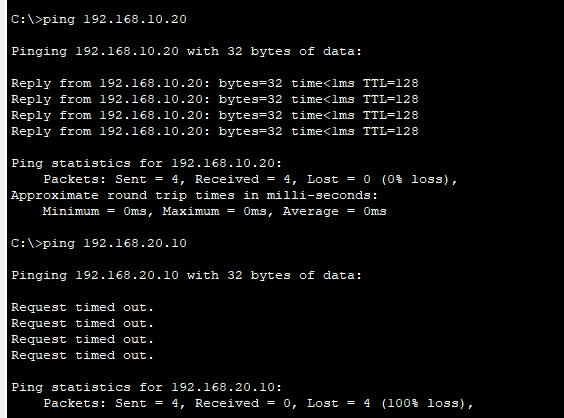
****

****

**Ping from PC0 to PC1 (same VLAN):**

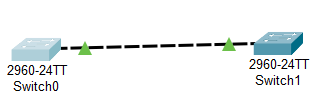
****

**Ping from PC0 to PC2 (different VLAN):**

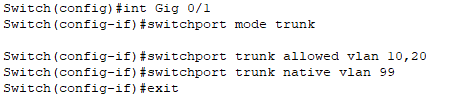
****

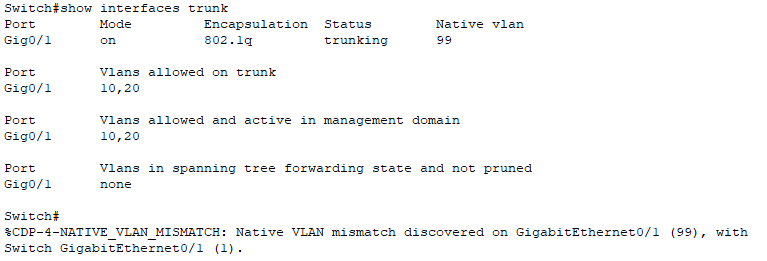
**Q5. Change the native VLAN on a trunk port. Test for VLAN mismatches and troubleshoot.**

**Two switches 0 and 1 connected with Crossover cable**

****

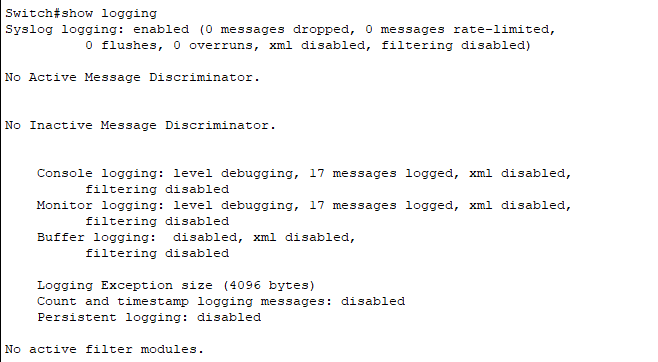
**Native VLAN configuration in switch 0:**

****

**Native VLAN mismatch issue:  
  
**

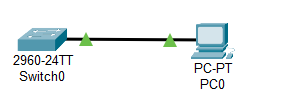
**Fix the mismatch in switch 1 :**

****

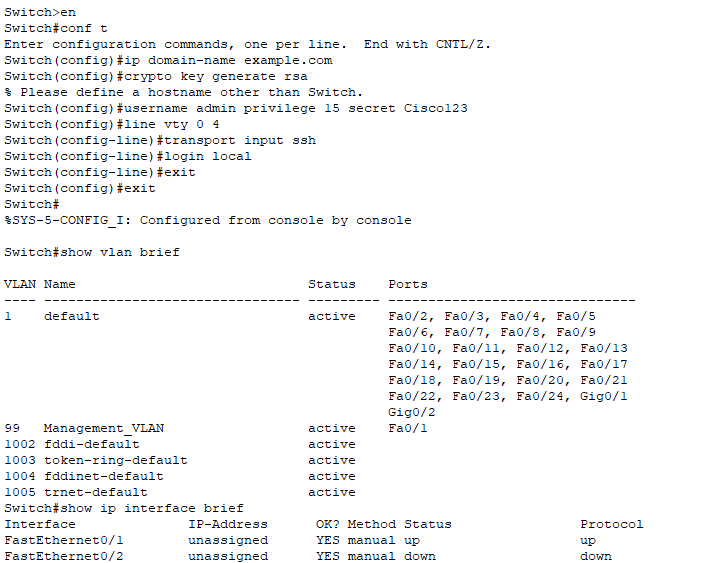
****

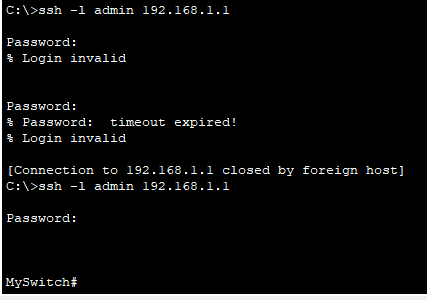
**Q6 .Configure a management VLAN and assign an IP address for remote access.**

**Test SSH or Telnet access to the switch.**

****

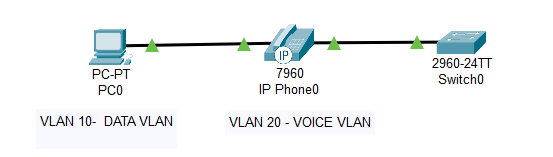
**Switch Configuration**

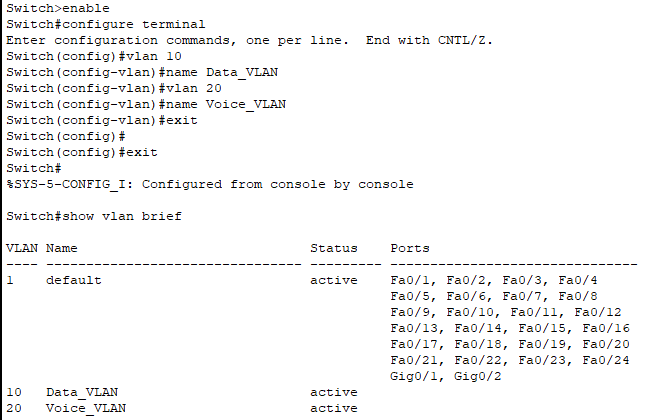
****

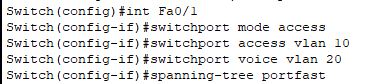
**SSH test at PC:  
  
**

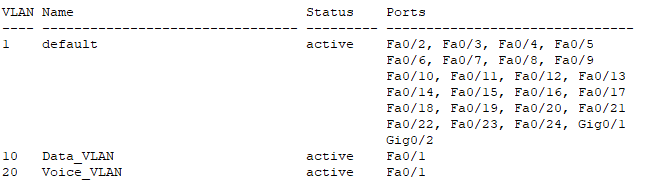
**Q7. You have a Cisco switch and a VoIP phone that needs to be placed in a voice VLAN (VLAN 20).**

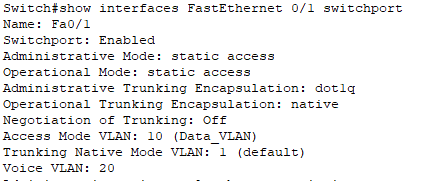
**The data for the PC should remain in a separate VLAN (VLAN 10). Configure the switch port to support both voice and data traffic.**

****

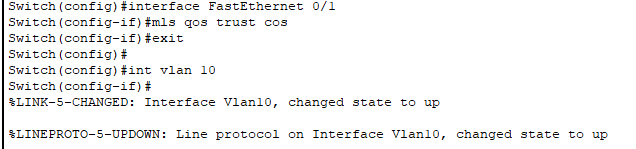
**Creating VLANs  
**

****

****

****

**Enable QoS ( for Voice Traffic)**

****