**MID-TERM EXAM PROJECT NETWORK CONFIGURATION**

**29061 BANK**

**COMPUTER NETWORKS**

**NAME:** Joseph MUTANGANA

**STUDENT ID:** 29061

**COURSE NAME:** Computer Networks

**INSTRUCTOR NAME:** Eng. Joshua IRADUKUNDA

**TITLE:** MidTerm Exam

**DATE:** Nov-03-2025

**Contents**

[Introduction ii](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563562)

[PHASE 1: Naming and Credential Standards 1](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563563)

[Phase 2: Network Device Setup & Addressing 5](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563564)

[PHASE 3: VLANS Configuration & Port Assignments 11](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563565)

[PHASE 4: Trunking and EtherChannel Configuration 14](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563566)

[PHASE 5: Server IPs Configurations & Services 18](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563567)

[PHASE 6: Security Implementation 23](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563568)

[Connectivity verification 27](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563569)

[Challenges 28](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212563570)

# ****Introduction****

The Mid-Term Examination project, focuses on building a fully functional and secure enterprise network named **29061 Bank Network Deployment.**  
This configuration was implemented using **Cisco Packet Tracer (v8.2.2.0400)** as part of the **Computer Networks** course under the **Faculty of Information Technology.**

The project’s objective was to design, configure, and test a multi-departmental network that integrates key enterprise technologies such **as Inter-VLAN Routing, VTP, EtherChannel,** **Spanning Tree Protocol (RSTP), Port Security, Access Control Lists (ACLs),** and essential **server services** including **DHCP, DNS,** and **NTP.**

Each device in the topology—including routers, core, distribution, and access switches—was configured following institutional naming and credential standards. The setup ensured interconnectivity between all VLANs and secure network access for departments such as **IT, HR, Finance, Accounting, Risk, Teller,** and **Visitors,** while maintaining strong security and access control policies through **ACLs** and **Port Security**.

The project demonstrates practical knowledge in **enterprise networking,** emphasizing secure communication, logical segmentation, and centralized management of network devices.

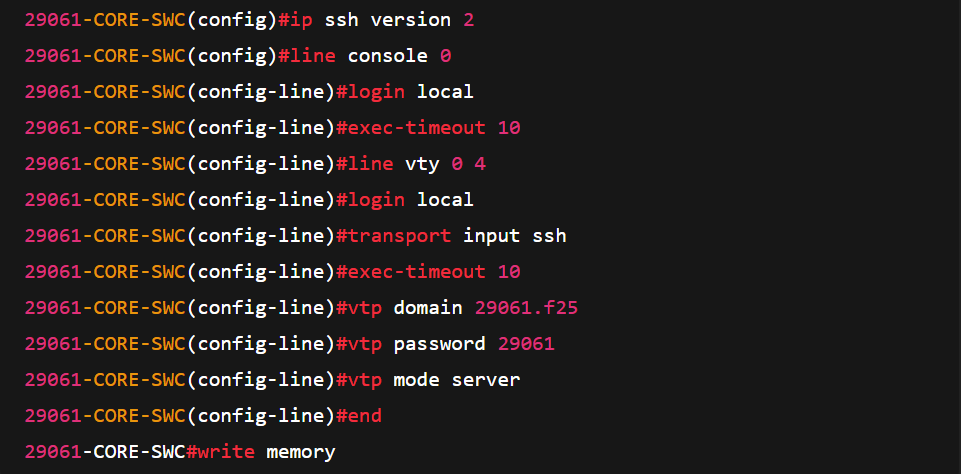
# ****PHASE 1: Naming and Credential Standards****

**DEVICE: HQ-MAIN-ROUTER**

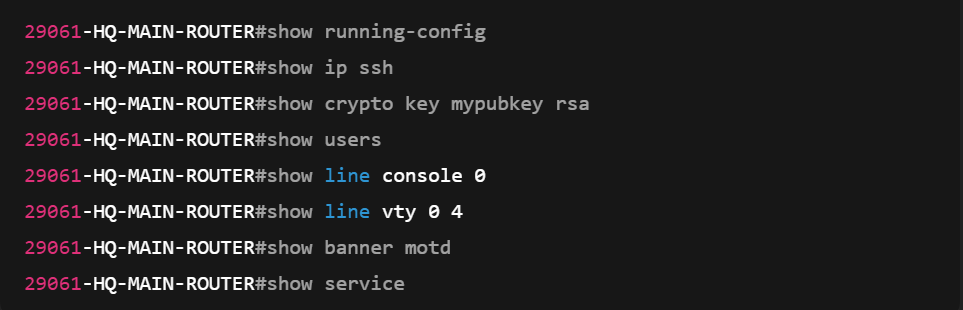
**TABLE OF USED COMMANDS**



**DEVICE: SWITCHES**

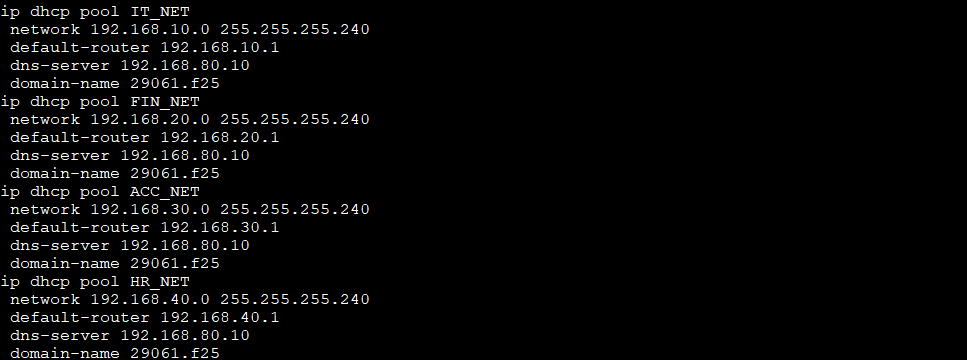


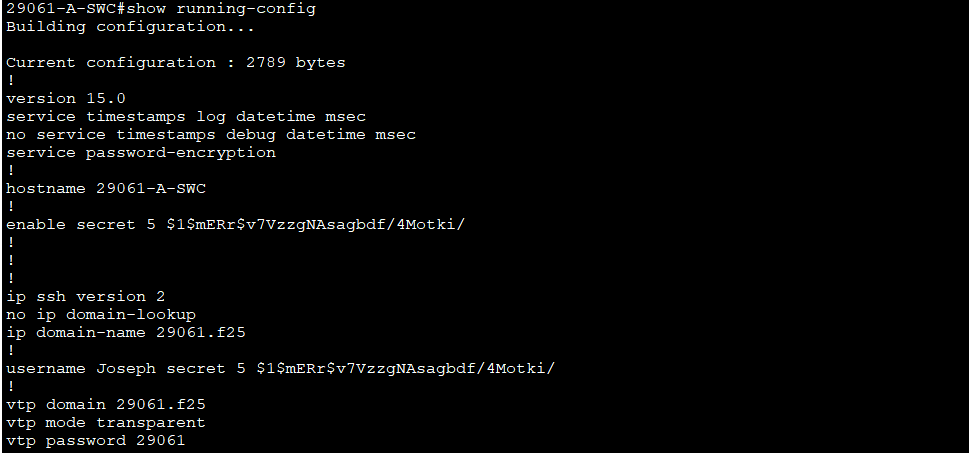
**TABLE OF VERIFICATION COMMANDS**



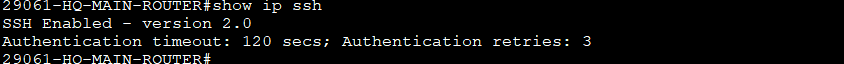


#show running-config

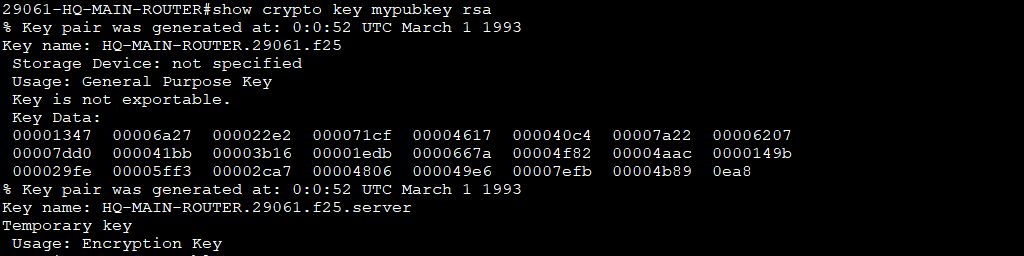




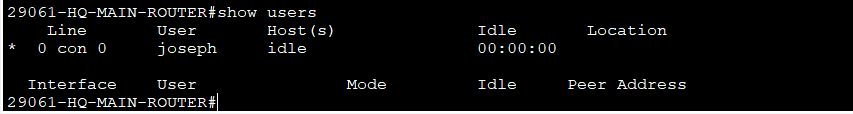
#show ip ssh



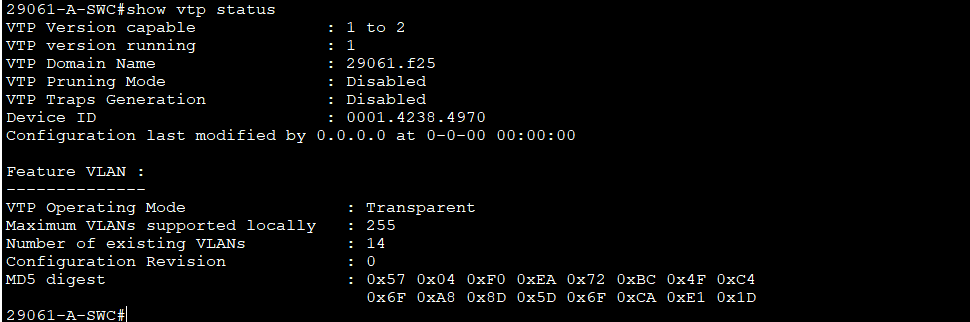
#show crypto key mypubkey rsa



#show users



#show vtp status

****

**Explanation of commands used in Phase 1**

**enable**  
→ Enters privileged EXEC mode (allows advanced commands).

**configure terminal**  
→ Enters global configuration mode to change settings.

**hostname HQ-MAIN-ROUTER**  
→ Sets the device’s name to “HQ-MAIN-ROUTER.”

**no ip domain-lookup**  
→ Disables DNS lookups when a command is mistyped.

**ip domain-name 29061.f25**  
→ Sets the device’s domain name (needed for SSH key generation).

**username Joseph privilege 15 secret 29061**  
→ Creates user “Joseph” with full admin rights and encrypted password “29061.”

**enable secret 29061**  
→ Sets an encrypted password for privileged (enable) mode.

**service password-encryption**  
→ Encrypts all plaintext passwords in the configuration.

**banner motd # Authorized Access Only - 29061 BANK #**  
→ Displays a login message warning unauthorized users.

**crypto key generate rsa**  
→ Generates RSA keys for SSH encryption.

**1024**  
→ Specifies the RSA key size (1024 bits).

**ip ssh version 2**  
→ Enables secure SSH version 2.

**line console 0**  
→ Enters console line configuration mode.

**login local**  
→ Uses local usernames and passwords for login.

**exec-timeout 10**  
→ Logs out inactive sessions after 10 minutes.

**line vty 0 4**  
→ Configures virtual terminal lines for remote access.

**login local**  
→ Uses local login for remote sessions.

**transport input ssh**  
→ Allows only SSH connections (disables Telnet).

**exec-timeout 10**  
→ Sets 10-minute timeout for SSH/Telnet sessions.

**end**  
→ Exits configuration mode.

**write memory**  
→ Saves the running configuration to startup memory.

**vtp domain 29061.f25**  
→ Sets the VTP domain name so switches can share VLAN info.

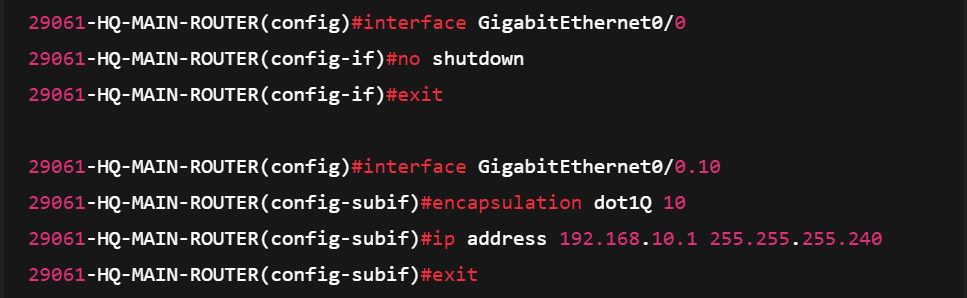
**vtp password 29061**  
→ Sets the VTP authentication password for domain members.

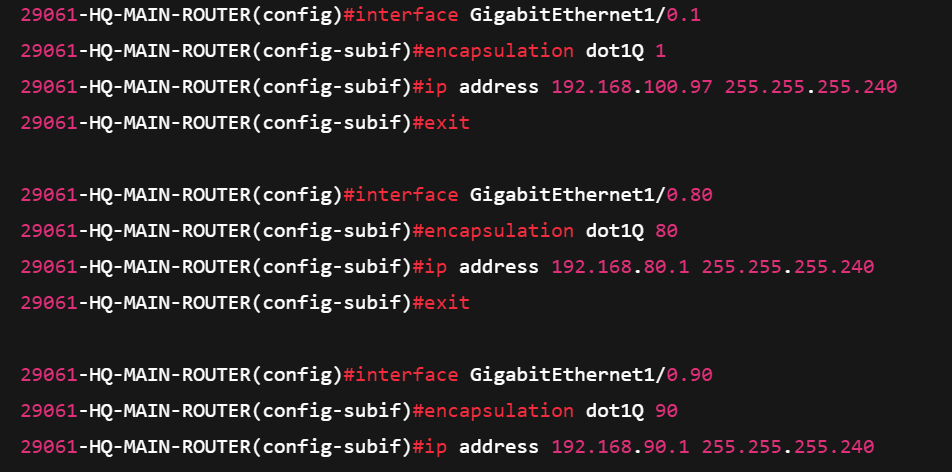
**vtp mode server**  
→ Sets the switch to *server mode* (can create and manage VLANs).

# Phase 2: Network Device Setup ****& Addressing****

**TABLE OF USED COMMANDS**

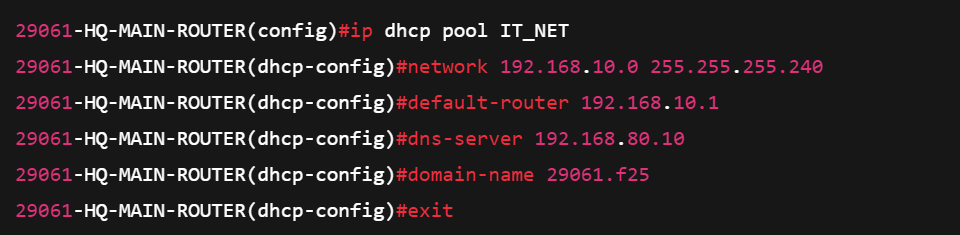
**DEVICE: HQ-MAIN-ROUTER CREATING SUB-INTERFACES AND ASSIGNING IP ADDRESS (ROUTER-ON-A-STICK)**

****

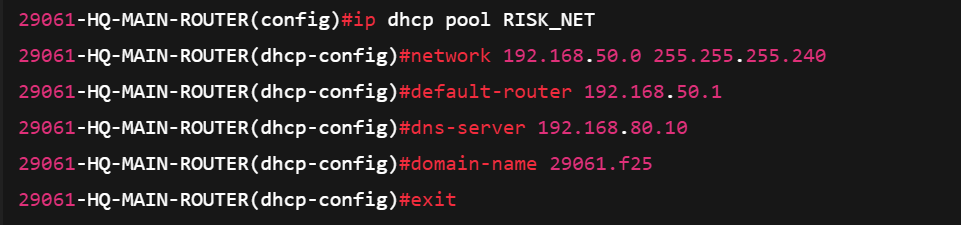
****

**DEVICE: HQ-MAIN-ROUTER DHCP EXCLUDING IP ADDRES**

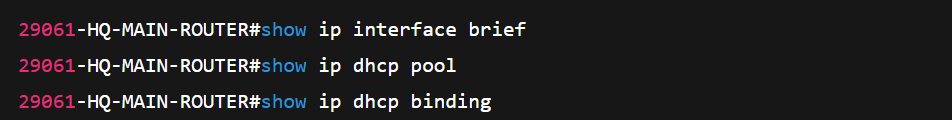
****

****

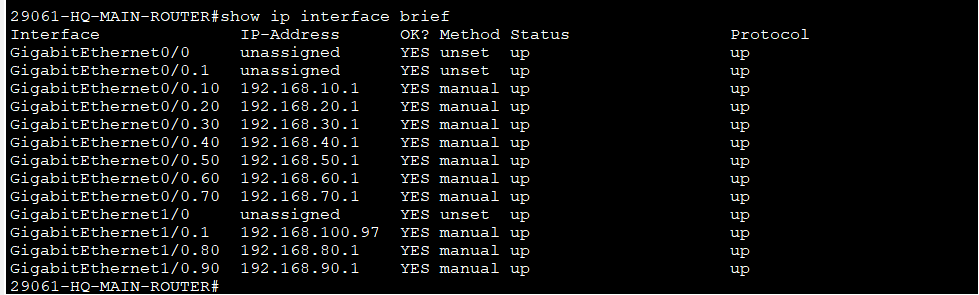
**DEVICE: HQ-MAIN-ROUTER DHCP POOL**

****

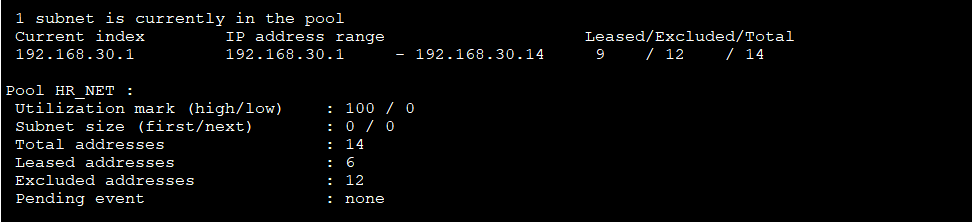
**TABLE OF VERIFICATION COMMANDS**

****

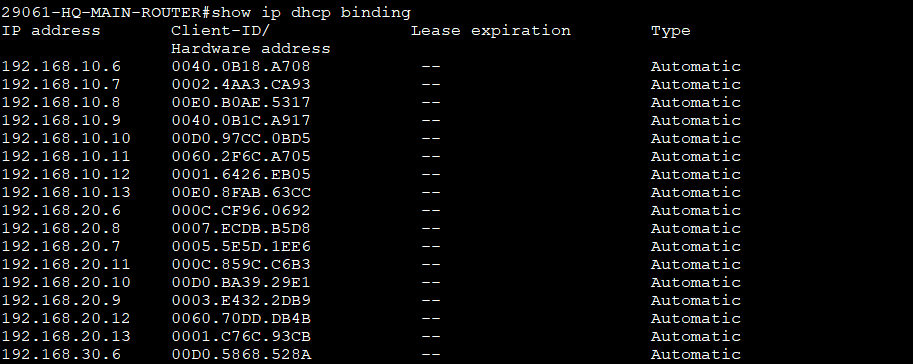
#show ip interface brief

****

#show ip dhcp pool

****

#show ip dhcp binding

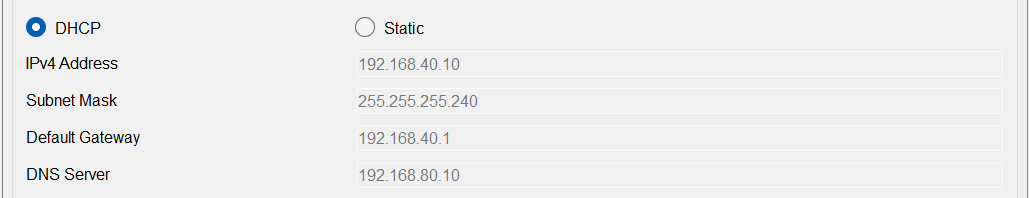
****

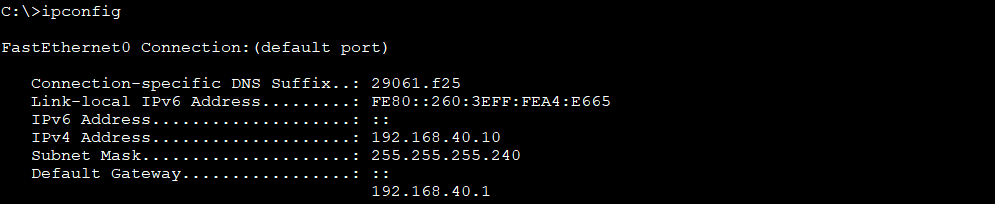
**On PCs and Laptops to get IP address Dynamic**

Step 1: Open PC/Laptop

Step 2: Click Desktop Tab  
Step 3: Choose IP Configuration

Step 4: Select DHCP





**Explanation of commands used in Phase 2**

**These are some from many subinterfaces for VLAN routing I had to configure**

**interface GigabitEthernet0/0**  
→ Enters config mode for the main physical interface (G0/0).

**no shutdown**  
→ Activates the interface (brings it up).

**exit**  
→ Leaves interface configuration mode.

**interface GigabitEthernet0/0.1**  
→ Creates subinterface for VLAN 1.

**encapsulation dot1Q 1**  
→ Assigns VLAN 1 to this subinterface using 802.1Q tagging.

**ip address 192.168.100.97 255.255.255.240**  
→ Sets IP address and subnet mask for VLAN 1’s gateway.

**exit**  
→ Returns to global configuration mode.

**interface GigabitEthernet0/0.10**  
→ Creates subinterface for VLAN 10.

**encapsulation dot1Q 10**  
→ Assigns VLAN 10 to this subinterface.

**ip address 192.168.10.1 255.255.255.240**  
→ Sets IP address and subnet mask for VLAN 10’s gateway.

**interface GigabitEthernet1/0.90**  
→ Creates subinterface for VLAN 90.

**encapsulation dot1Q 90**  
→ Assigns VLAN 90 to this subinterface.

**ip address 192.168.90.1 255.255.255.240**  
→ Sets IP address and subnet mask for VLAN 90’s gateway.

**ip dhcp excluded-address 192.168.10.1 192.168.10.5**  
→ Reserves these IPs (1–5) so DHCP won’t assign them to clients in VLAN 10.

**ip dhcp excluded-address 192.168.20.1 192.168.20.5**  
→ Reserves these IPs (1–5) so DHCP won’t assign them to clients in VLAN 20.

**ip dhcp pool IT\_NET**  
→ Creates a DHCP pool named *IT\_NET*.

**network 192.168.10.0 255.255.255.240**  
→ Defines the network range for this pool (VLAN 10).

**default-router 192.168.10.1**  
→ Sets the gateway for DHCP clients in this pool.

**dns-server 192.168.80.10**  
→ Assigns a DNS server address for this network.

**domain-name 29061.f25**  
→ Sets the domain name given to DHCP clients.

**ip dhcp pool FIN\_NET**  
→ Creates a DHCP pool named *FIN\_NET*.

**network 192.168.20.0 255.255.255.240**  
→ Defines the network range for this pool (VLAN 20).

**default-router 192.168.20.1**  
→ Sets the gateway for DHCP clients in this pool.

**dns-server 192.168.80.10**  
→ Assigns the DNS server for this network.

**domain-name 29061.f25**  
→ Sets the domain name given to DHCP clients.

**ip dhcp pool ACC\_NET**  
→ Creates a DHCP pool named *ACC\_NET*.

**network 192.168.30.0 255.255.255.240**  
→ Defines the network range for this pool (VLAN 30).

**default-router 192.168.30.1**  
→ Sets the gateway for DHCP clients in this pool.

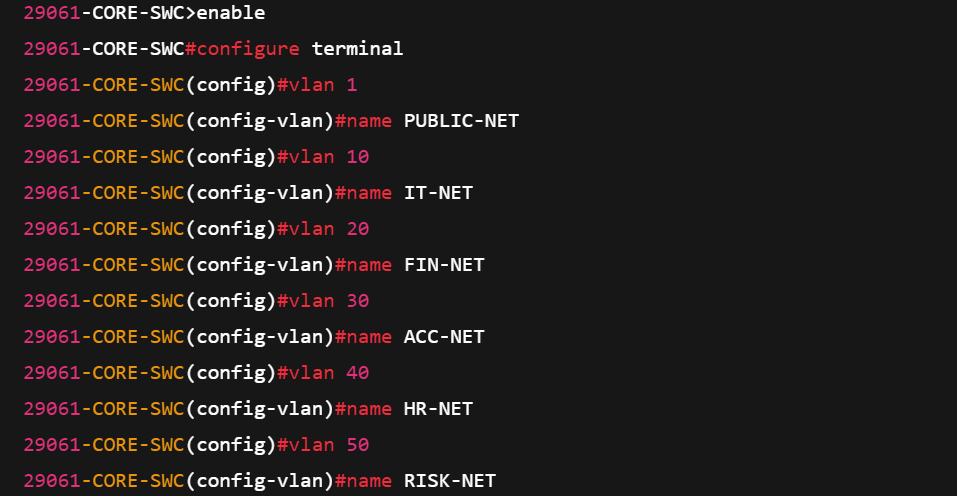
**dns-server 192.168.80.10**  
→ Assigns the DNS server for this network.

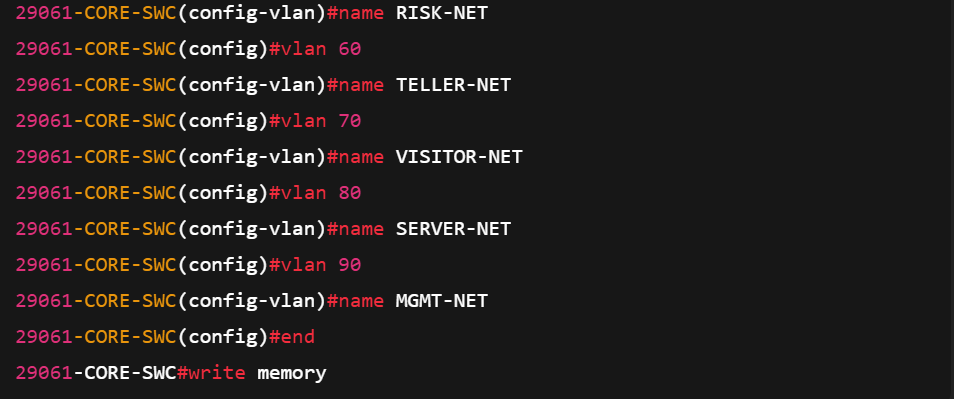
**domain-name 29061.f25**  
→ Sets the domain name given to DHCP clients.

# PHASE 3: VLANS Configuration & Port Assignments

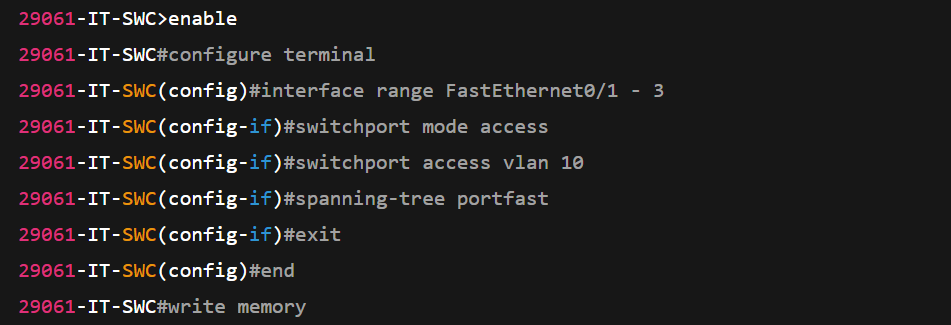
**TABLE OF USED COMMANDS**

**VLANs creation**

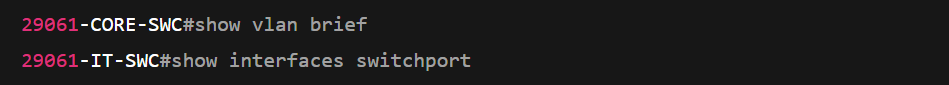
****

****

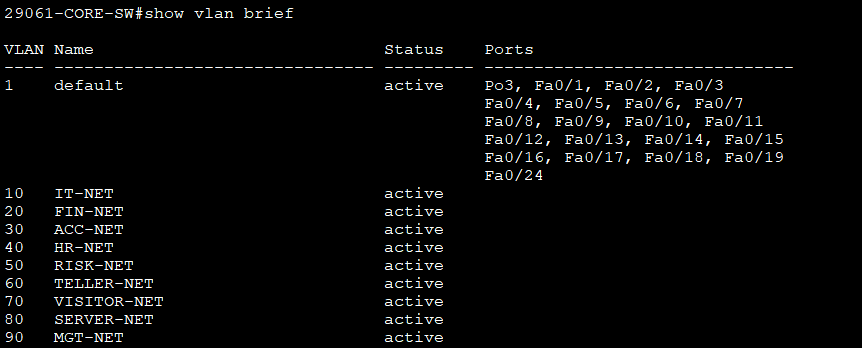
**ACCESS SWITCH VLAN ASSIGNMENTS**

****

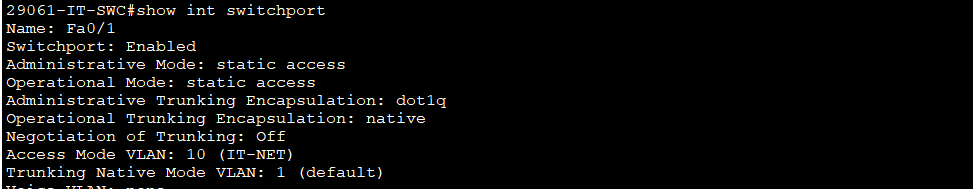
**TABLE OF VERIFICATION COMMANDS**

****

#show vlan brief

****

#show interface switchport

****

**Explanation of commands used in Phase 3 VLAN creation and assigned ports**

**enable**  
→ Enters privileged EXEC mode.

**configure terminal**  
→ Enters global configuration mode.

**vlan 1**  
→ Creates or enters VLAN 1 configuration mode.

**name PUBLIC-NET**  
→ Names VLAN 1 as “PUBLIC-NET.”

**vlan 10**  
→ Creates or enters VLAN 10 configuration mode.

**name IT-NET**  
→ Names VLAN 10 as “IT-NET.”

**vlan 20**  
→ Creates or enters VLAN 20 configuration mode.

**name FIN-NET**  
→ Names VLAN 20 as “FIN-NET.”

**interface range FastEthernet0/1 - 3**  
→ Selects interfaces F0/1 through F0/3 to configure together.

**switchport mode access**  
→ Sets ports as access ports (for end devices, not trunks).

**switchport access vlan 10**  
→ Assigns these ports to VLAN 10 (IT-NET).

**switchport port-security**  
→ Enables port security on the interfaces.

**switchport port-security maximum 1**  
→ Allows only one MAC address per port.

**switchport port-security violation shutdown**  
→ Shuts down the port if a security violation occurs.

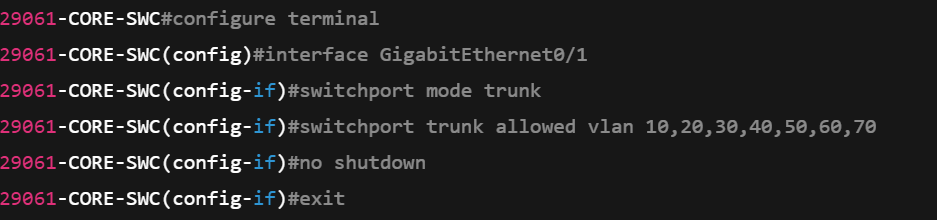
**spanning-tree portfast**  
→ Enables immediate forwarding state for end-device ports (bypasses STP learning).

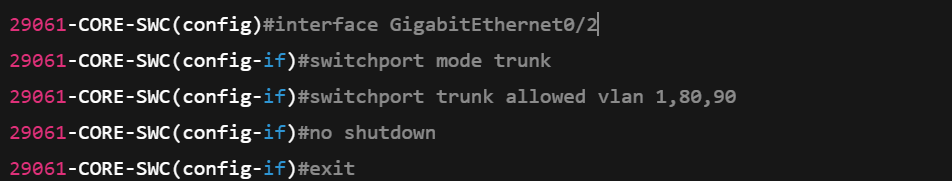
**spanning-tree bpduguard enable**  
→ Disables the port if a BPDU (Spanning Tree message) is received — protects against loops.

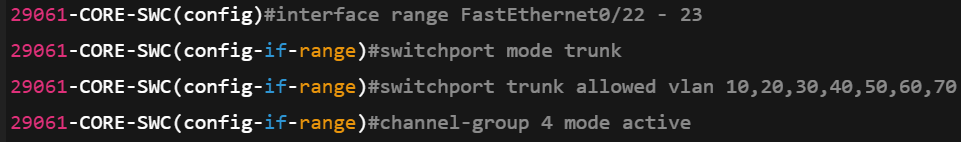
**no shutdown**  
→ Activates the interfaces.

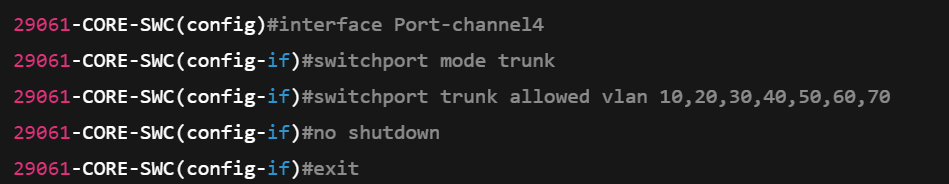
# PHASE 4: Trunking and EtherChannel Configuration

**TABLE OF USED COMMANDS**

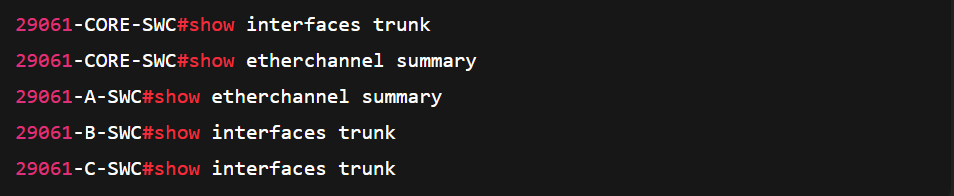




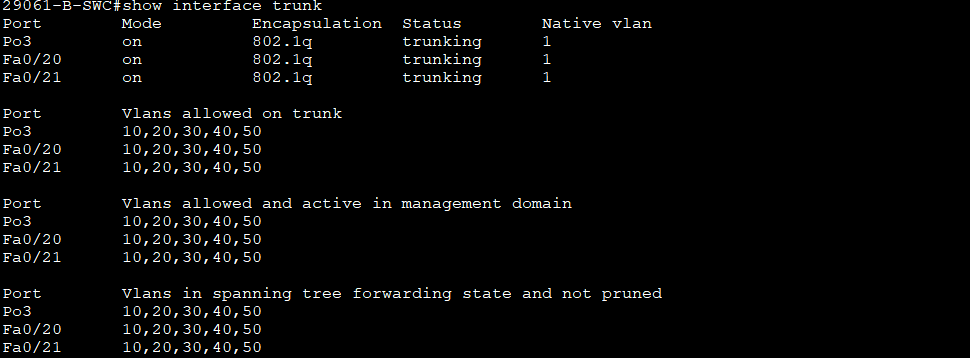


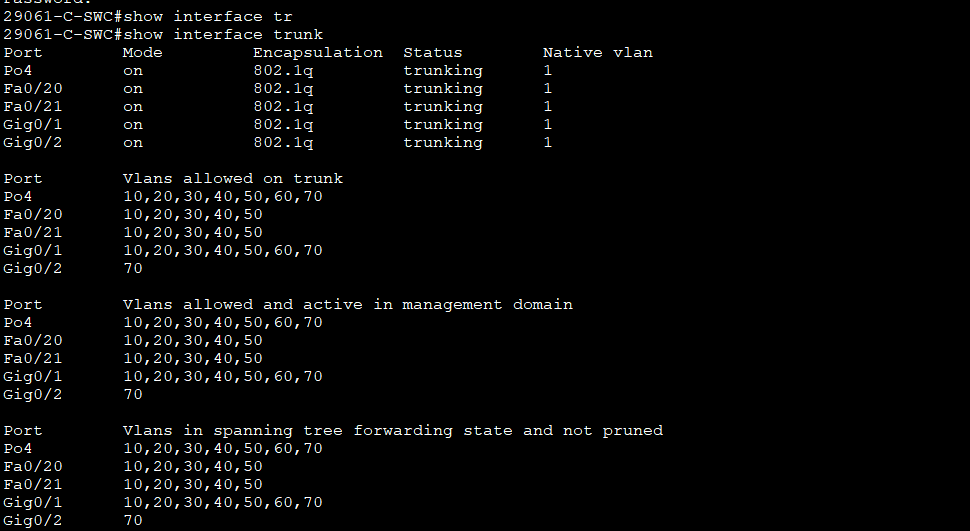


**TABLE OF VERIFICATION COMMANDS**

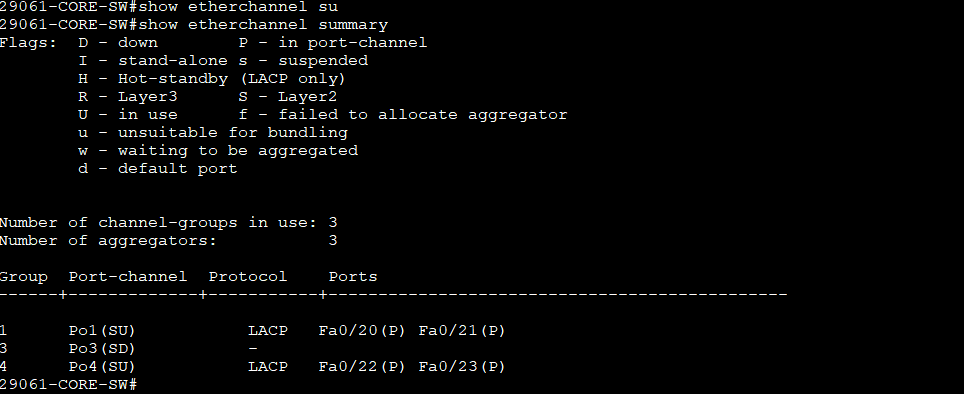


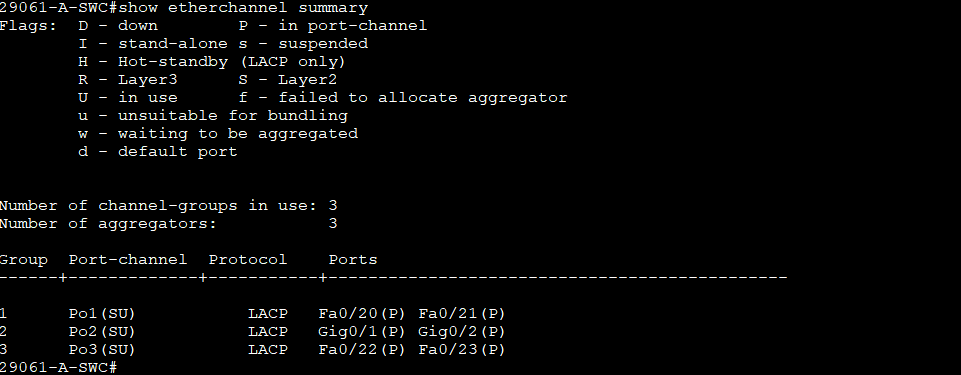
#show interface trunk





#show etherchannel summary





**Explanation of commands used in Phase 4, Trunking and EtherChannel**

**interface GigabitEthernet0/1**  
→ Enters configuration mode for interface G0/1.

**switchport mode trunk**  
→ Sets the port to trunk mode (carries multiple VLANs).

**switchport trunk allowed vlan 10,20,30,40,50,60,70**  
→ Allows only listed VLANs on this trunk link.

**no shutdown**  
→ Activates the interface.

**! Trunk to HQ-MAIN-ROUTER Gi0/2**  
→ Notes that interface Gi0/2 is another trunk link to HQ-MAIN-ROUTER.

**interface GigabitEthernet0/2**  
→ Enters configuration mode for interface G0/2.

**switchport mode trunk**  
→ Sets the port to trunk mode.

**switchport trunk allowed vlan 1,80,90**  
→ Allows VLANs 1, 80, and 90 across this trunk.

**no shutdown**  
→ Enables the interface.

**EtherChannel CORE <-> A-SWC**  
→ Defines EtherChannel connection between CORE switch and A-SWC.

**interface range FastEthernet0/20 - 21**  
→ Selects interfaces F0/20 and F0/21 to configure together.

**switchport mode trunk**  
→ Sets both ports to trunk mode.

**switchport trunk allowed vlan 1,10,20,30,40,50,60,70,80,90**  
→ Allows all listed VLANs on these trunks.

**channel-group 1 mode active**  
→ Bundles ports into EtherChannel group 1 using LACP (active mode).

**no shutdown**  
→ Enables the interfaces.

**interface Port-channel1**  
→ Configures the logical EtherChannel interface.

**switchport mode trunk**  
→ Sets Port-channel1 as a trunk.

**switchport trunk allowed vlan 1,10,20,30,40,50,60,70,80,90**  
→ Allows all listed VLANs on this Port-channel.

**no shutdown**  
→ Activates the EtherChannel interface.

# PHASE 5: Server IPs Configurations & Services

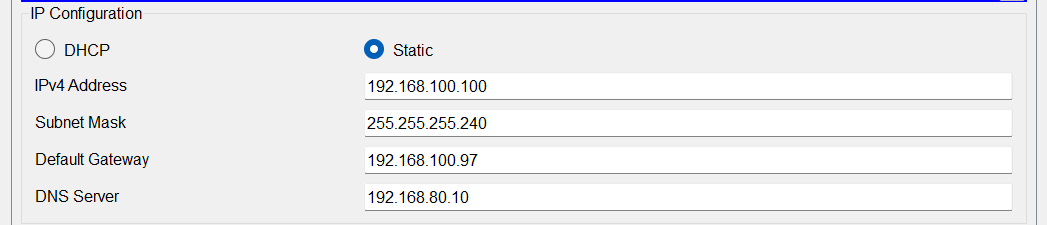
**STATIC IP ADDRESS ON WEB SERVER**

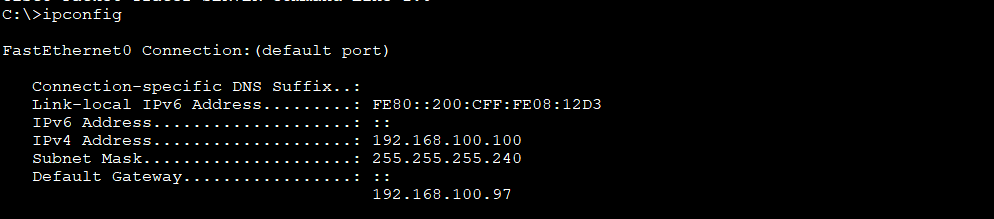
Step 1: Open Server

Step 2: Click Desktop Tab  
Step 3: Choose IP Configuration

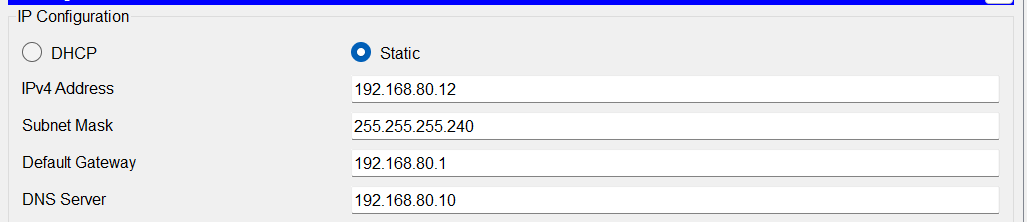
Step 4: Click on Static

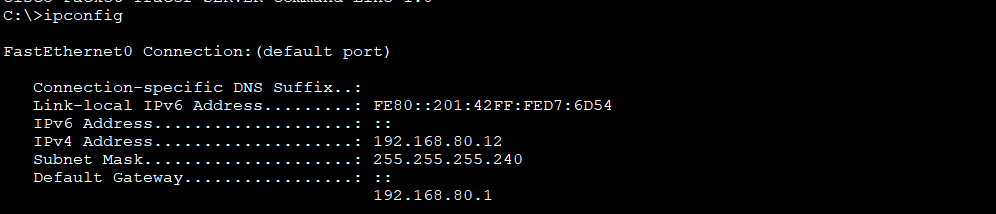
Step 5: Fill required field



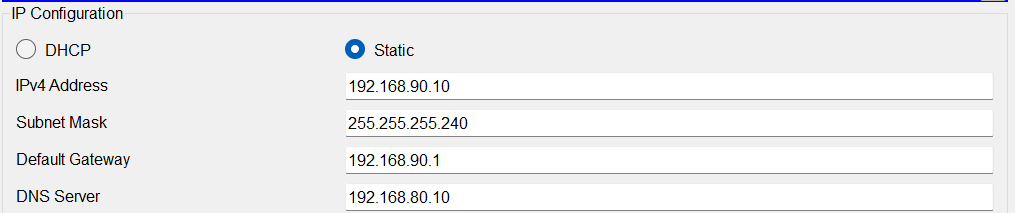


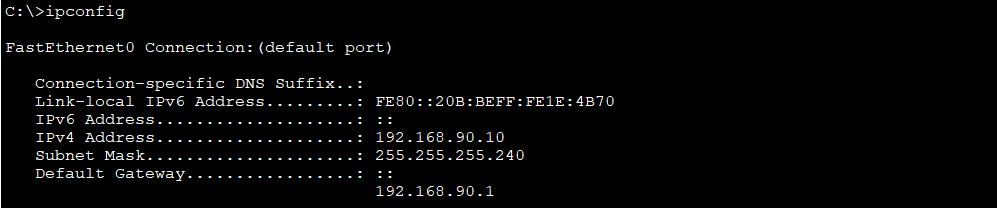
**STATIC IP ADDRESS ON EDWH SERVER**





**STATIC IP ADDRESS ON SYSLOG**

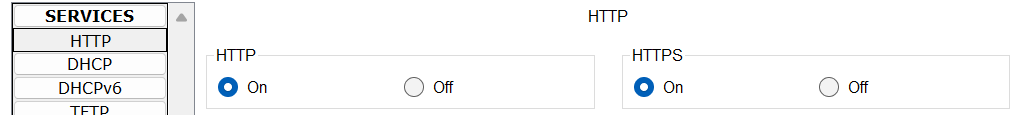




**SERVICE HTTP AND HTTPS ON WEB SERVER**

Step 1: Open Server

Step 2: Click Service Tab

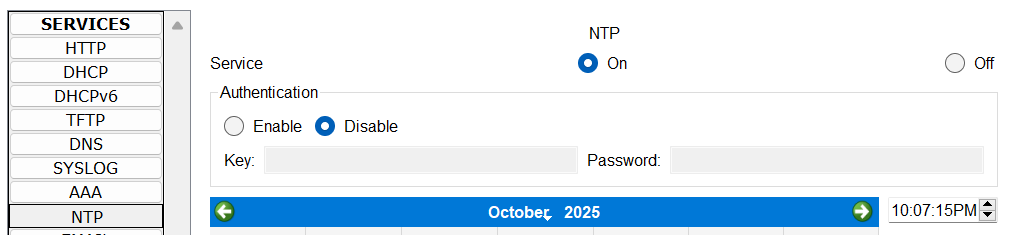
Step 3: Select HTTP on left side  
Step 4: Enable HTTP(ON) & HTTPS (ON) 

**SERVICE NTP ON NET-MONITORING SERVER**

Step 1: Open Server

Step 2: Click Service Tab

Step 3: Select NTP on the left side  
Step 4: Enable NTP (ON)

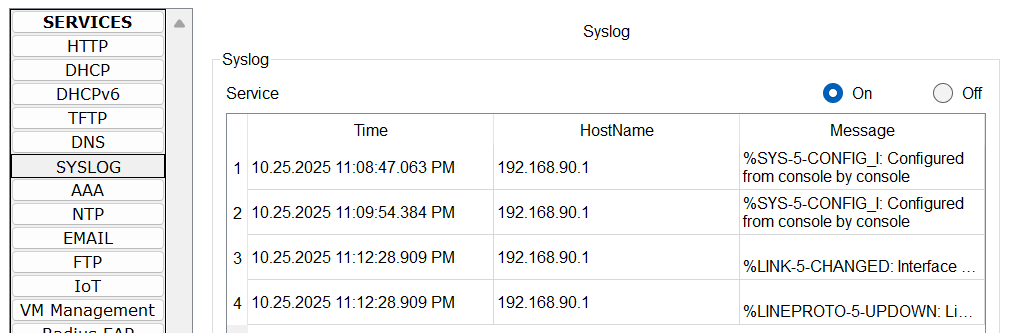
Step 5: Set time  


**SERVICE NTP ON SYLOG SERVER**

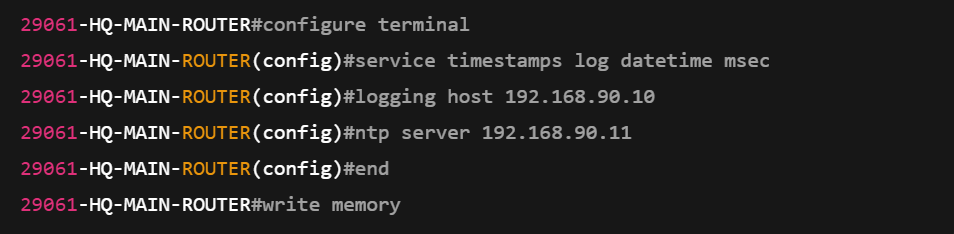
Step 1: Open Server

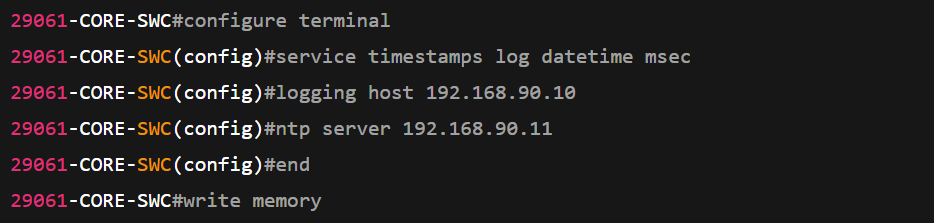
Step 2: Click Service Tab

Step 3: Select SYSLOG on the left side  
Step 4: Enable SYSLOG (ON)

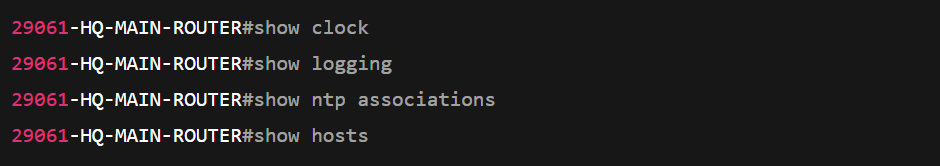


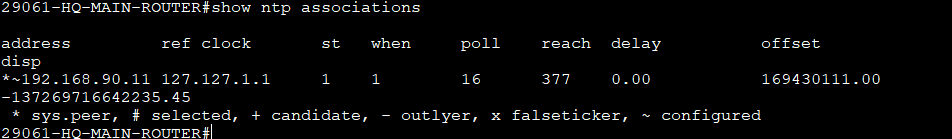
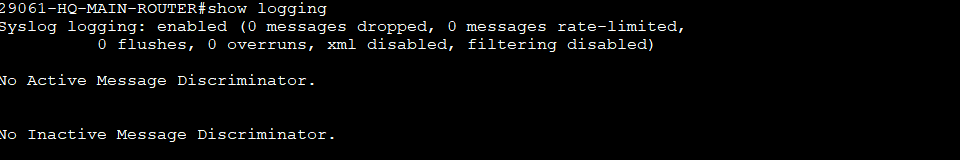
**TABLE OF USED COMMANDS ON BOTH SWITCH AND HQ-MAIN-ROUTER**





**TABLE OF VERIFICATION COMMANDS**



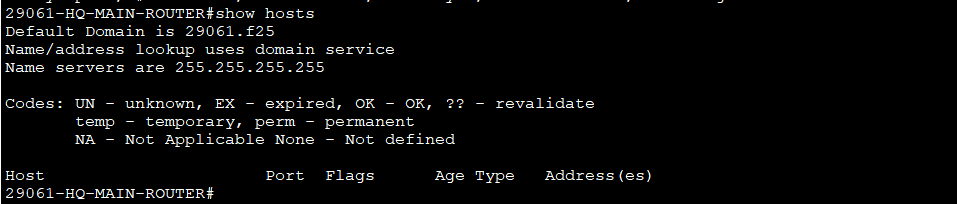


#show show clock

#show logging

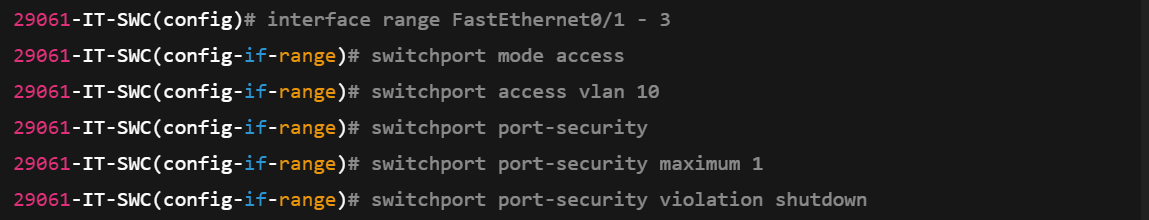
#show ntp association

#show hosts

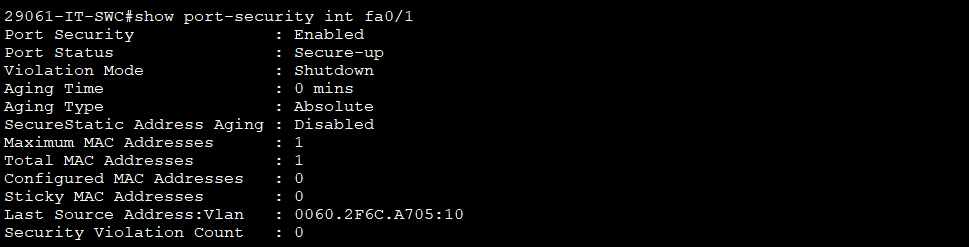


# PHASE 6: Security Implementation

**Port Security Commands**

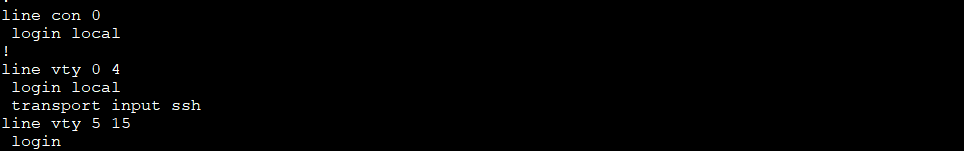


**Port Security Verification Commands**

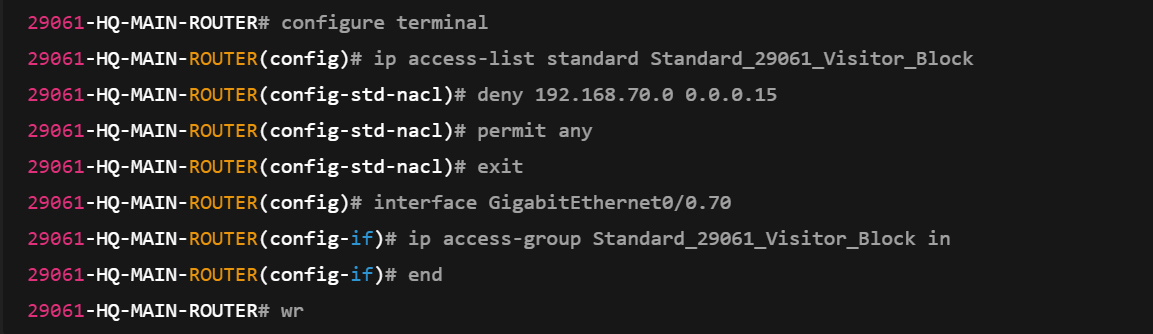


**SSH**

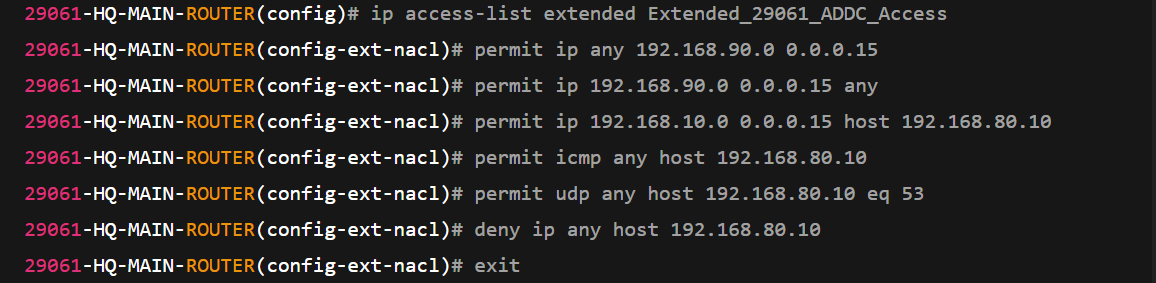


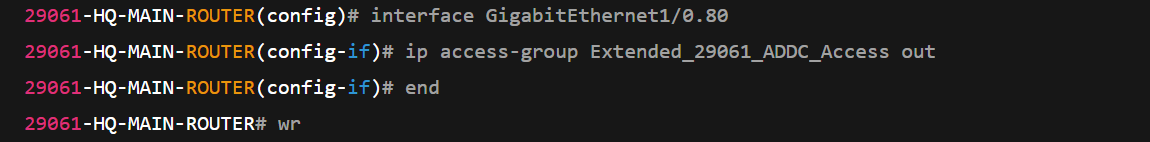


**ACL 1 — Block Visitor VLAN (70) from accessing all internal networks**

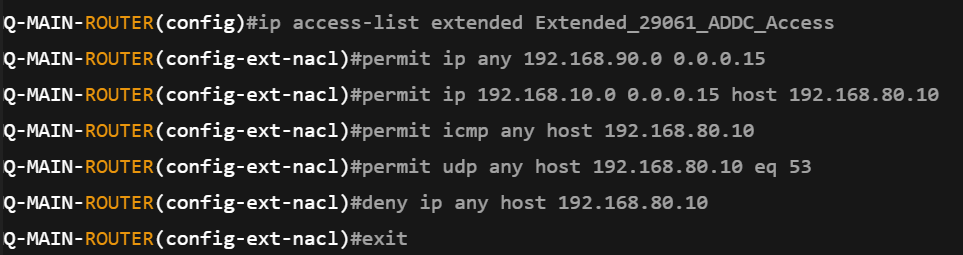


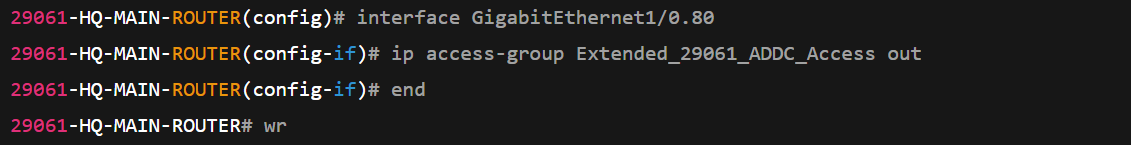
**ACL 2 — Allow VLAN 70 (Visitors) Only HTTP & DNS Access**



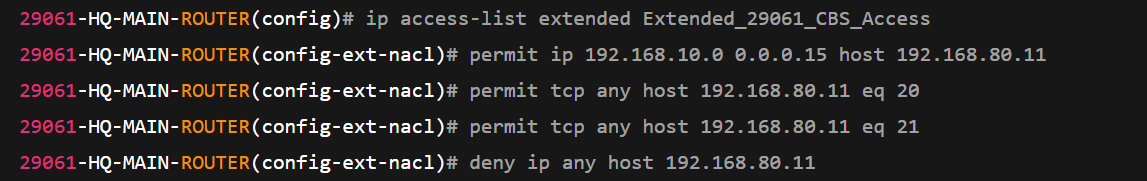


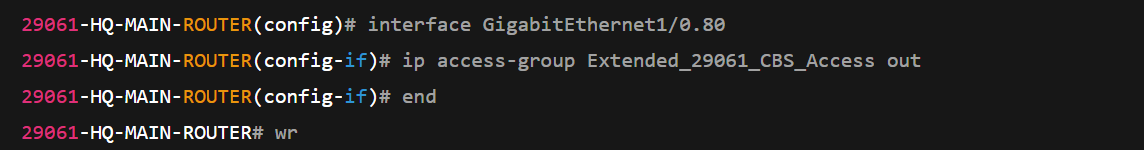
**ACL 3 — AD-DC Server Access (IT Full, Others Limited)**



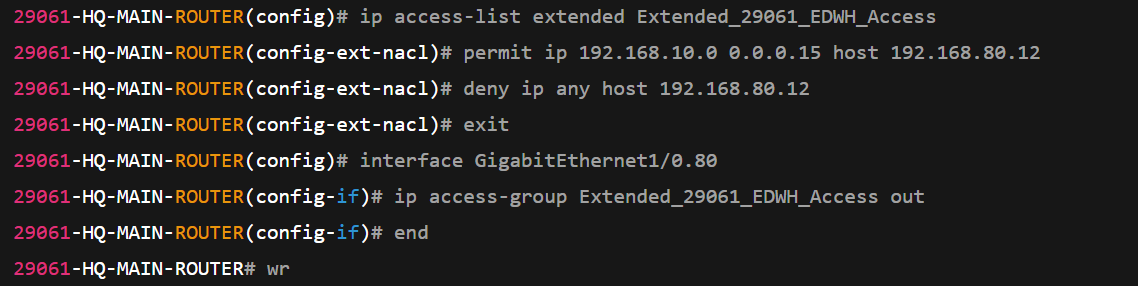


**ACL 4 — CBS Server Access (FTP Only for Non-IT VLANs**

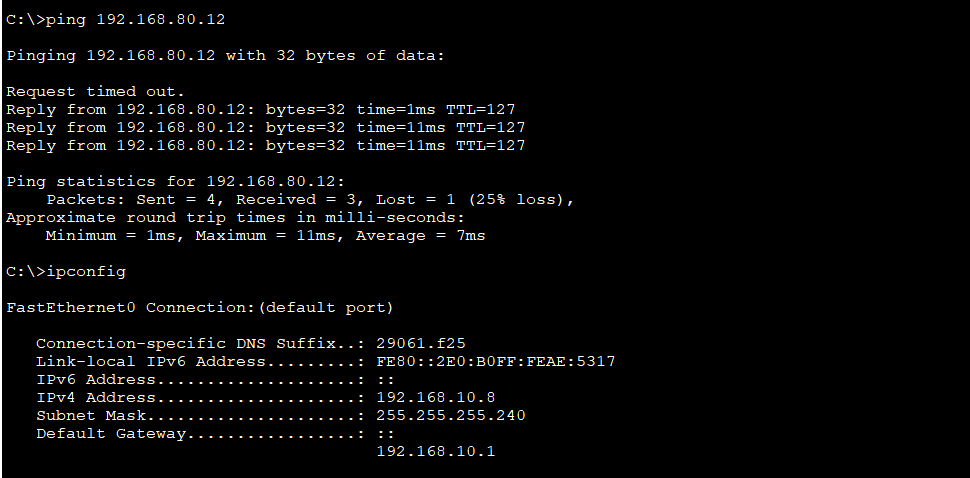




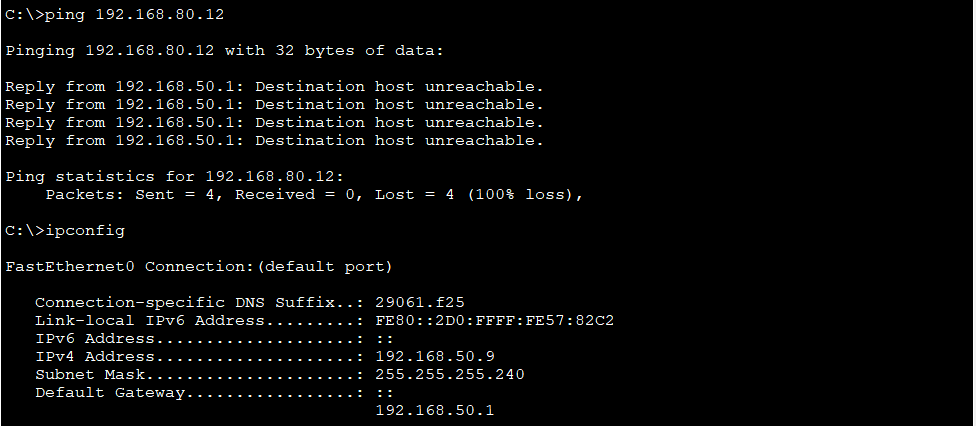
**ACL 5 — EDWH Server Access (Only IT-NET Allowed)VLANs**



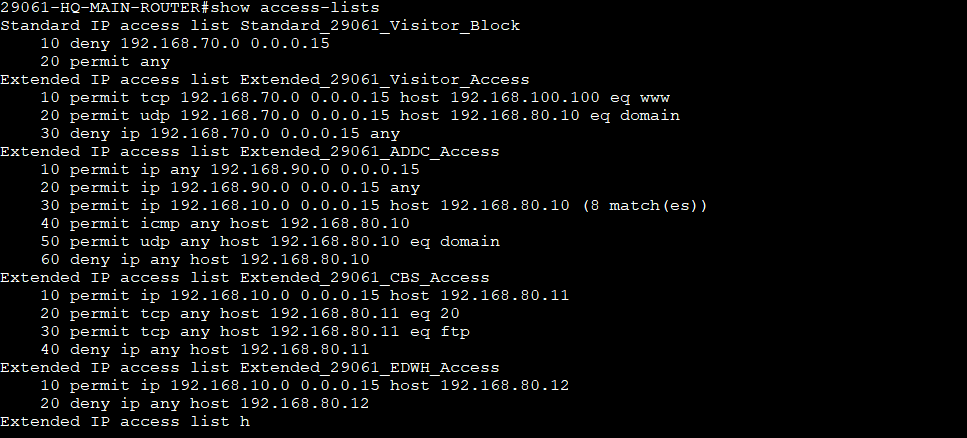
**ACL 5 — Verification1 IT-NET ping EDWH Server**



**ACL 5 — Verification 2 Other-NET can’t ping EDWH Server**

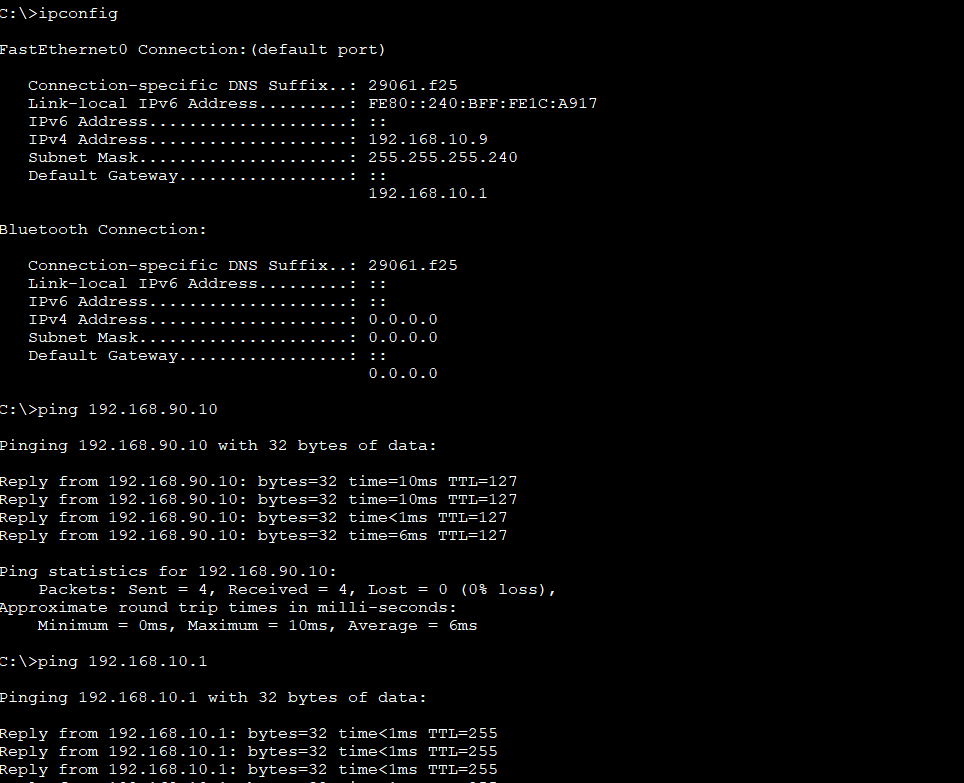


**PHASE 6 ACL LIST VERIFICATION**

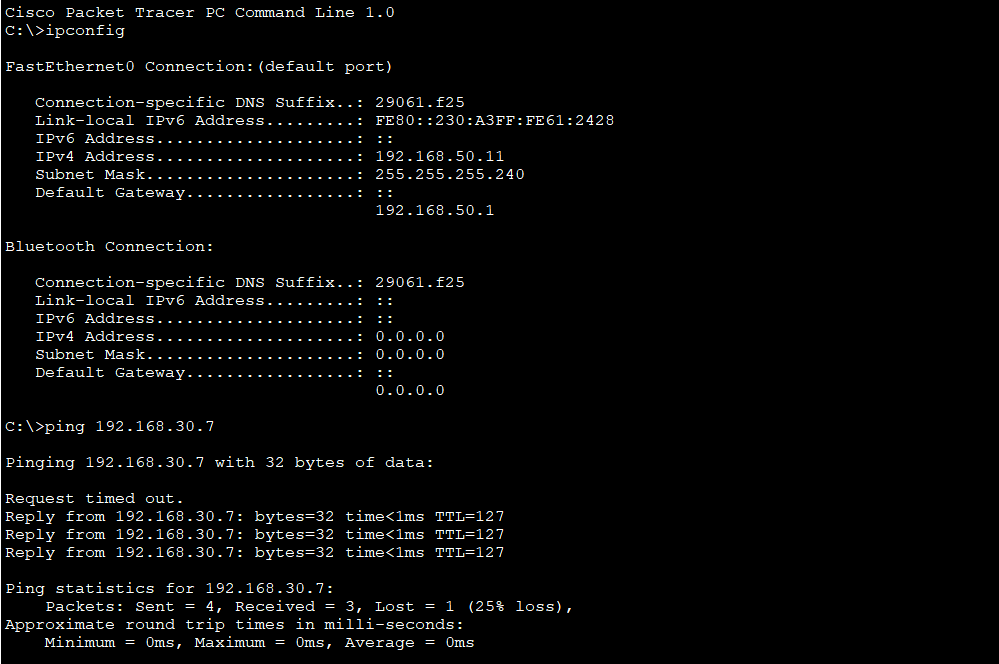


# Connectivity verification

**IT-NET PINGs OTHER NETs**



**HR-NET PINGs OTHER NETs**



# Challenges

During the configuration and testing of the **29061 Bank Network Deployment**, several practical issues were encountered:

1. **Wireless VLAN Integration (HomeRouter Configuration)**  
   A major challenge occurred when configuring the HomeRouter (Wireless Router) connected to the C-SWC.  
   Since the wireless router connects through a single interface while needing to serve multiple VLANs (for example, the Visitor and Teller networks), it was unclear how the router could receive multiple VLANs from the switch trunk link.  
   The limitation arose because most wireless home routers in Packet Tracer do not support trunk encapsulation (802.1Q).  
   This made it difficult to properly assign VLAN-based IPs and caused connection issues for wireless clients.  
   The issue was analyzed and documented, but a complete VLAN-aware configuration on the HomeRouter was not achievable within the default Packet Tracer device constraints.
2. **Teller VLAN Access Through HomeRouter**  
   The TELLER-SWC was connected to the same HomeRouter, creating a dependency on the router for network access.  
   Because the HomeRouter interface operates as an access port rather than a trunk, the Teller VLAN could not properly tag its traffic.  
   As a workaround, VLAN 60 (Teller) was maintained through the C-SWC trunk link, but full connectivity for hosts behind the HomeRouter remained limited.
3. Public / Web Server Connectivity Failure  
   Another challenge involved the Public-NET / WEB-SERVER VLAN (VLAN 1).  
   All other networks could successfully ping their gateways and communicate across VLANs, but the Web Server could neither send nor receive pings.

Despite these challenges, all remaining VLANs and services—such as DHCP, NTP, andSyslog—were verified to operate correctly, and inter-VLAN communication among internal departments worked as expected.