**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#_Toc212502818)

[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#_Toc212502819)

[Phase 2: Network Device Setup & Addressing 4](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502820)

[PHASE 3: VLANS Configuration & Port Assignments 7](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502821)

[PHASE 4: Trunking and EtherChannel Configuration 9](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502822)

[PHASE 5: Server Configurations & Services 11](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502823)

[PHASE 6: Security Implementation 15](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502824)

[Connectivity verification 16](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502825)

[Challenges 18](file:///C:\Users\user\Documents\Auca\sem-3\CNet\MidTermExam\29061_Joseph_MUTANGANA_CNet-F25_MID-29061_BANK.docx#_Toc212502826)

# ****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**.

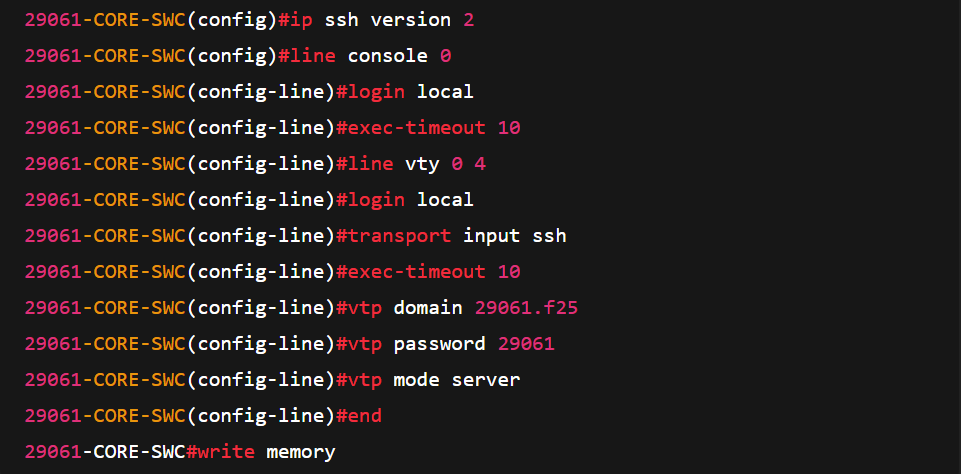
The project demonstrates practical knowledge in **enterprise networking,** emphasizing secure communication, logical segmentation, and centralized management of network devices.

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

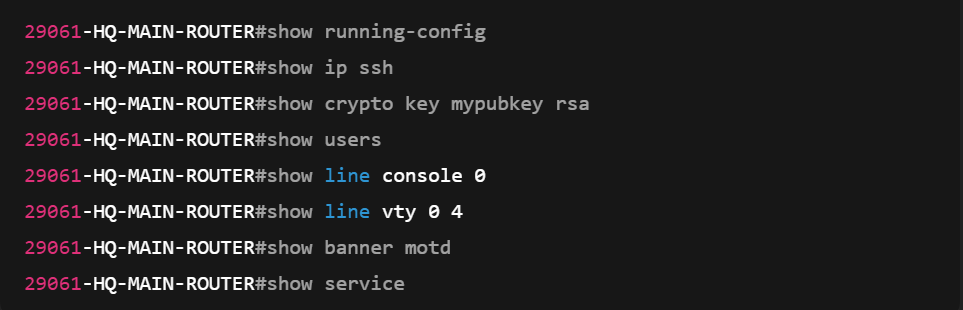
**DEVICE: HQ-MAIN-ROUTER**

**TABLE OF USED COMMANDS**



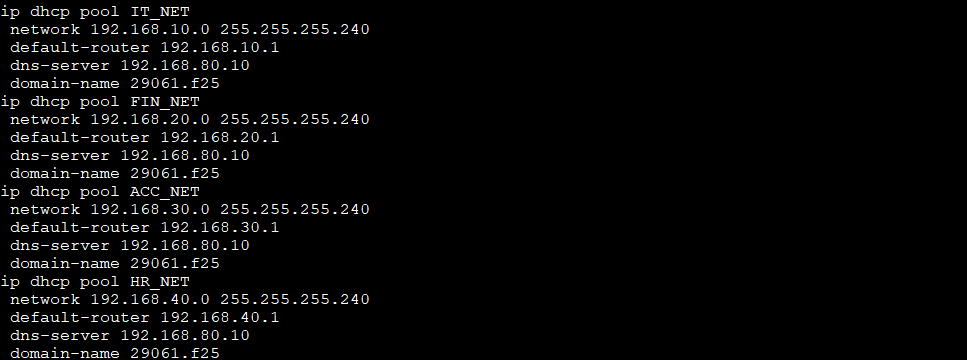


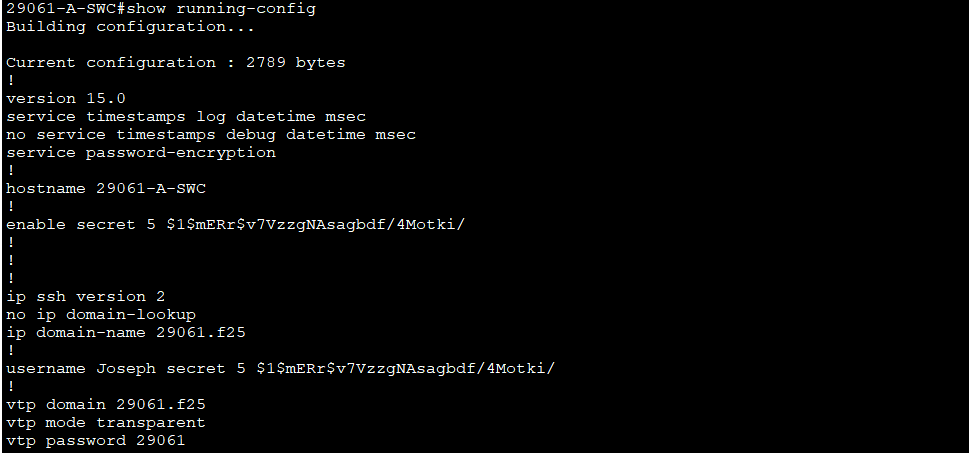
**TABLE OF VERIFICATION COMMANDS**



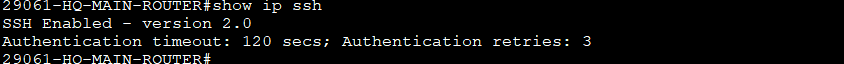


#show running-config

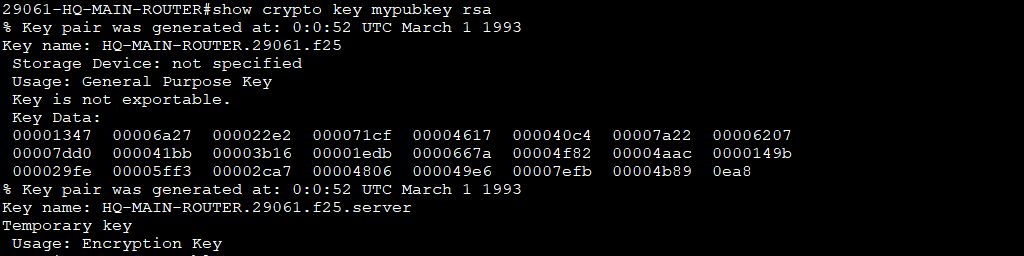




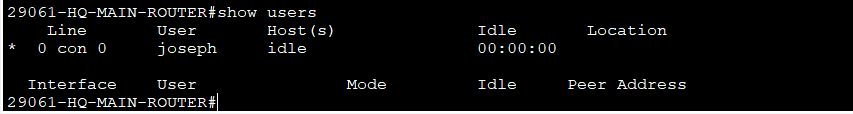
#show ip ssh



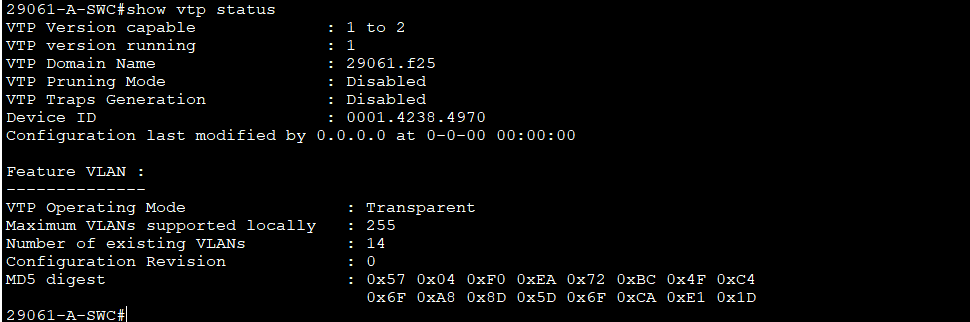
#show crypto key mypubkey rsa



#show users



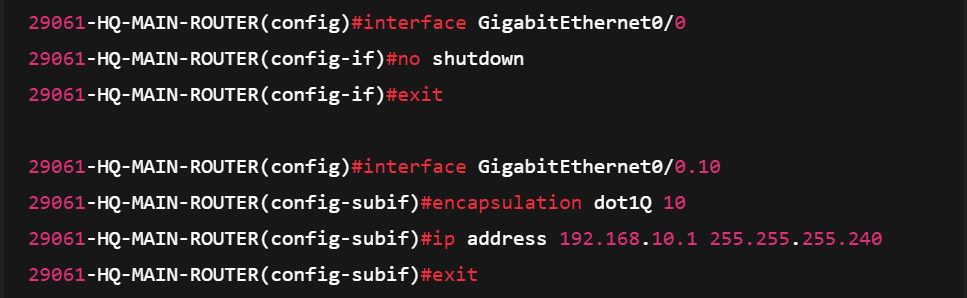
#show vtp status

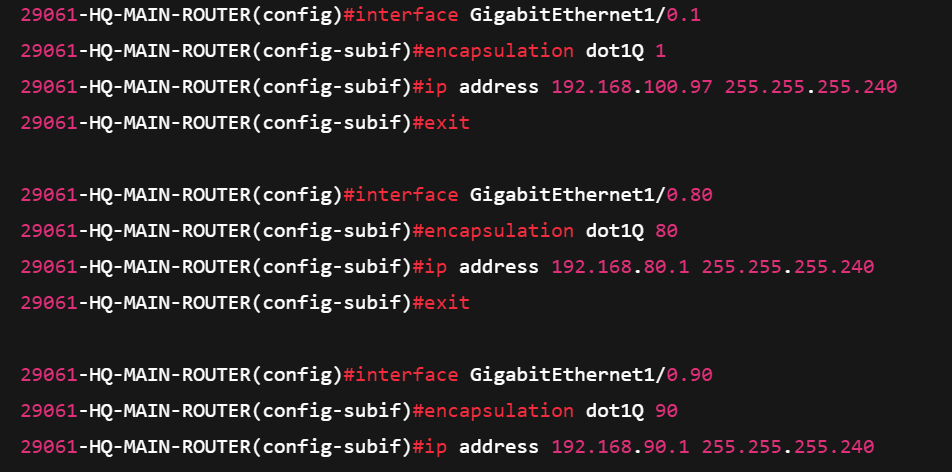
****

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

**TABLE OF USED COMMANDS**

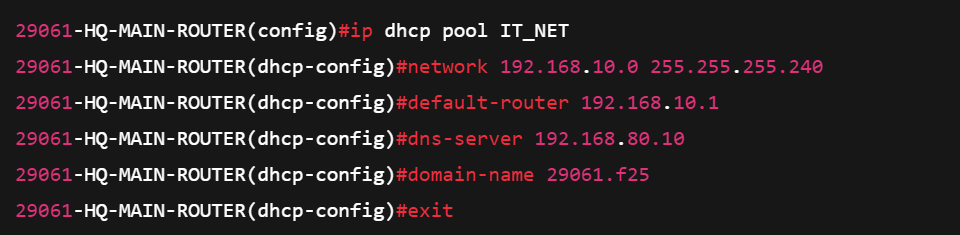
**DEVICE: HQ-MAIN-ROUTER CREATING SUB-INTERFACES AND ASSIGNING IP ADDRESS (ROUTER-ON-A-STICK)**

****

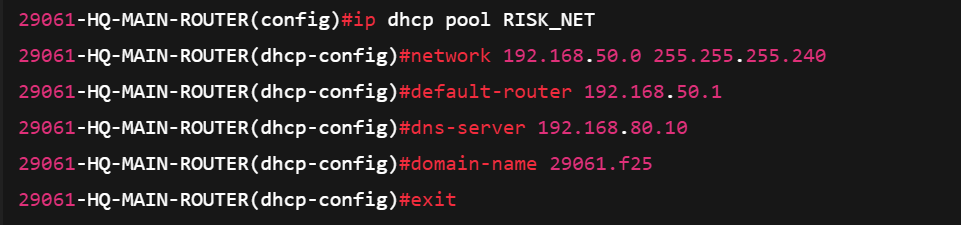
****

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

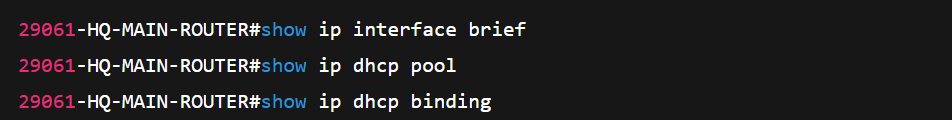
****

****

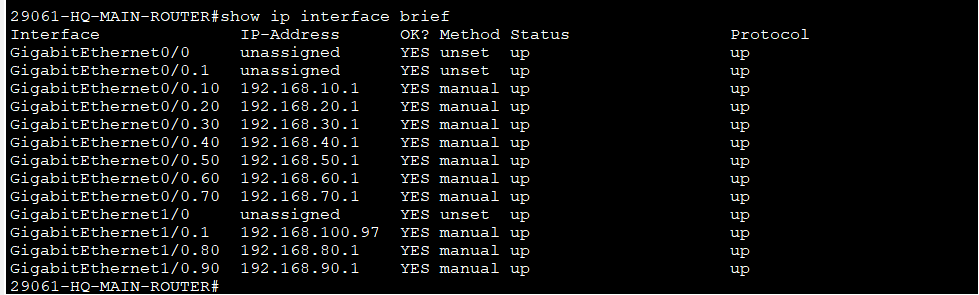
**DEVICE: HQ-MAIN-ROUTER DHCP POOL**

****

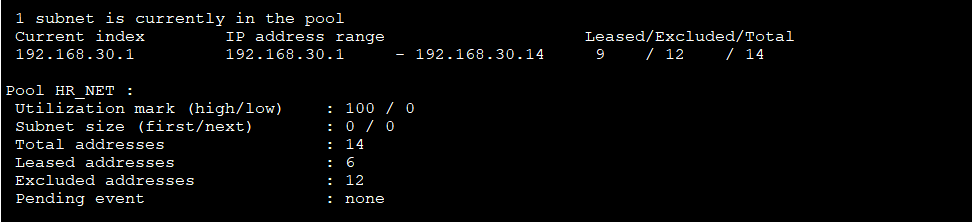
**TABLE OF VERIFICATION COMMANDS**

****

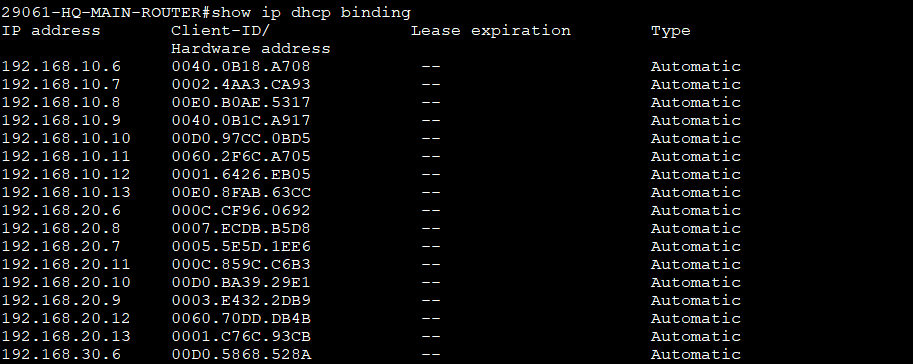
#show ip interface brief

****

#show ip dhcp pool

****

#show ip dhcp binding

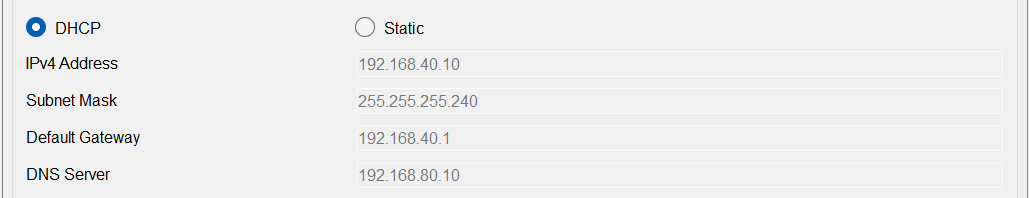
****

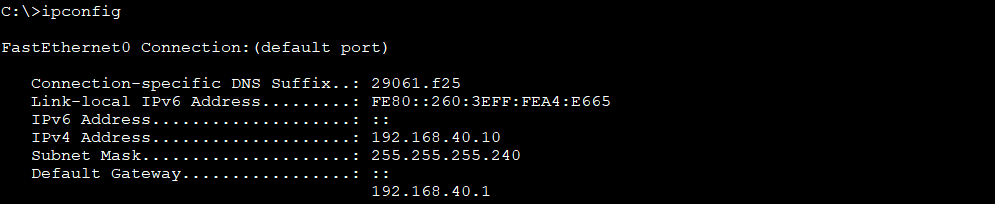
**On PCs and Laptops to get IP address Dynamic**

Step 1: Open PC/Laptop

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

Step 4: Select DHCP

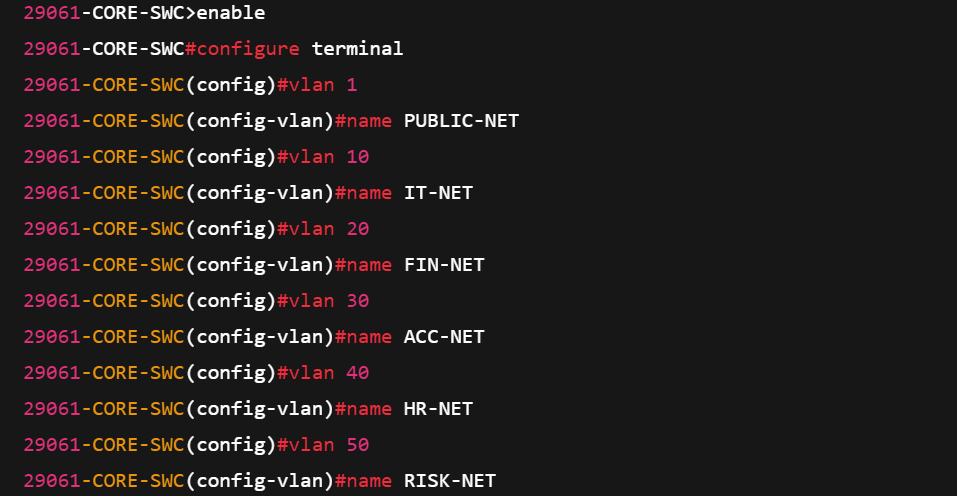


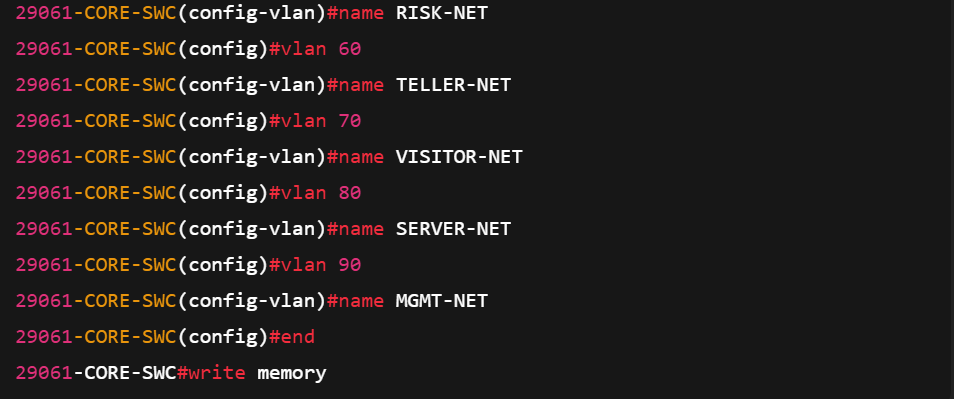


# PHASE 3: VLANS Configuration & Port Assignments

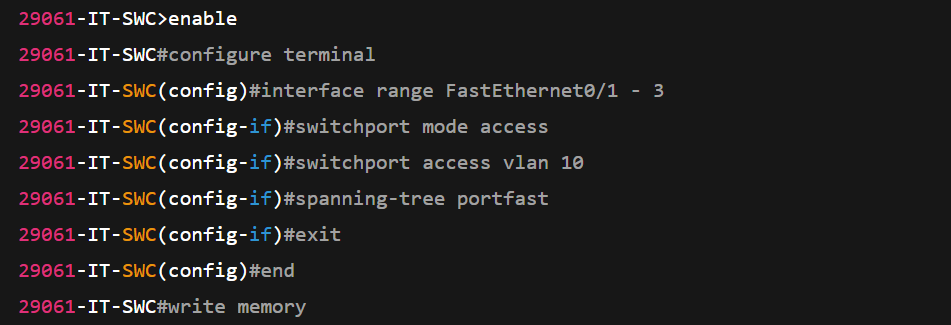
**TABLE OF USED COMMANDS**

**VLANs creation**

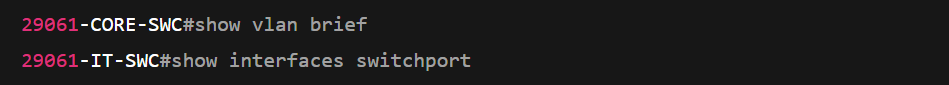
****

****

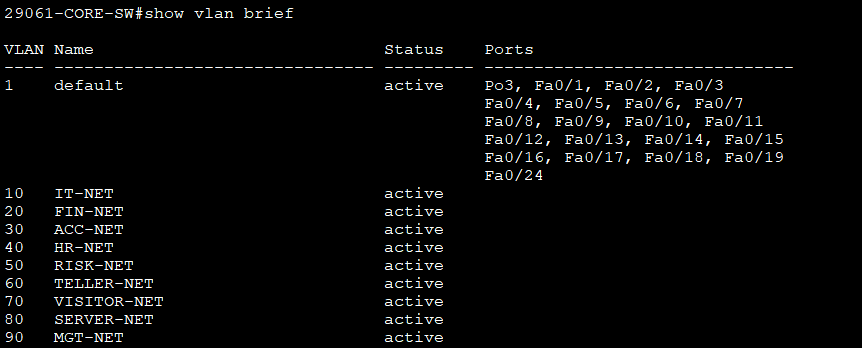
**ACCESS SWITCH VLAN ASSIGNMENTS**

****

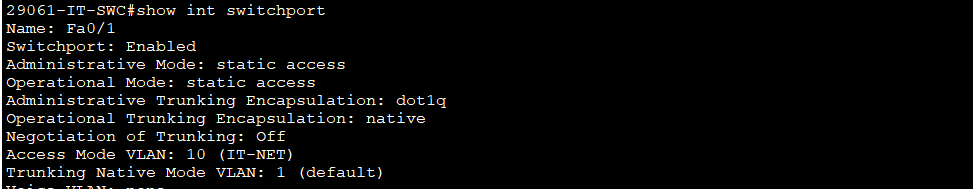
**TABLE OF VERIFICATION COMMANDS**

****

#show vlan brief

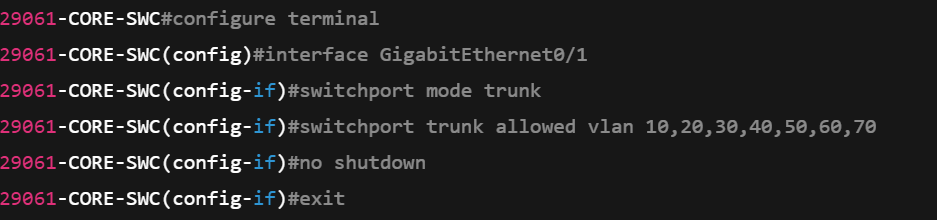
****

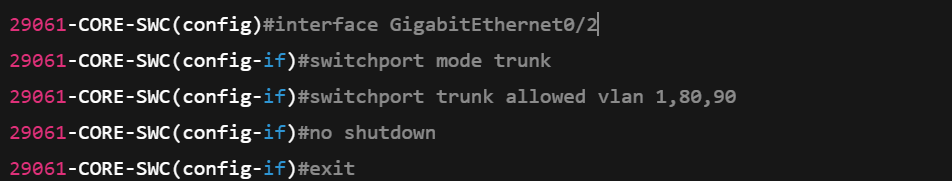
#show interface switchport

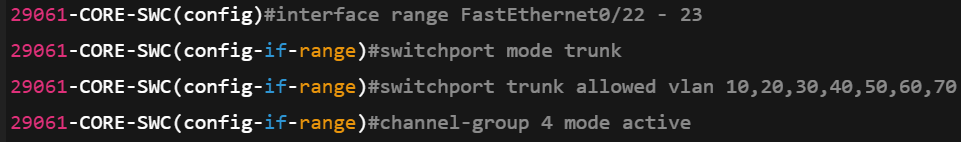
****

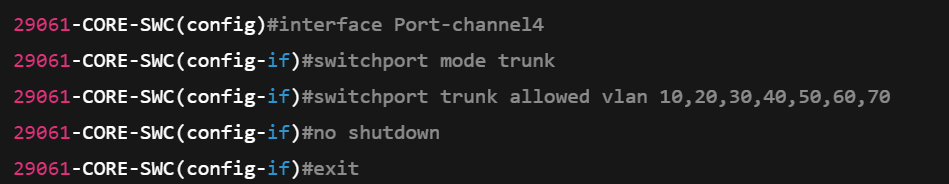
# PHASE 4: Trunking and EtherChannel Configuration

**TABLE OF USED COMMANDS**

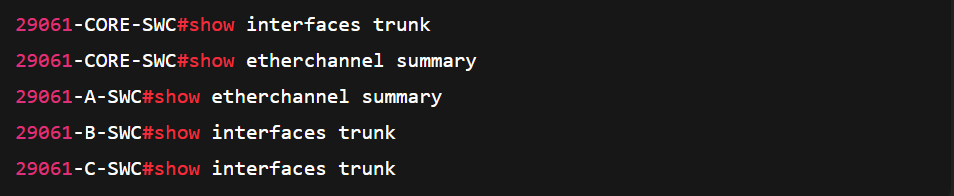




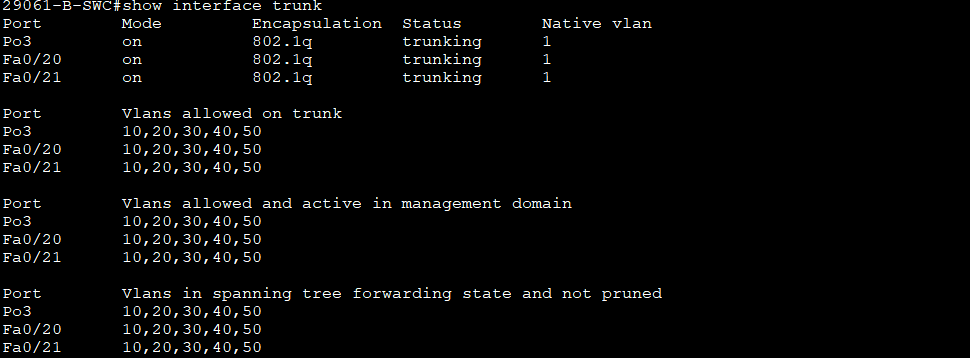


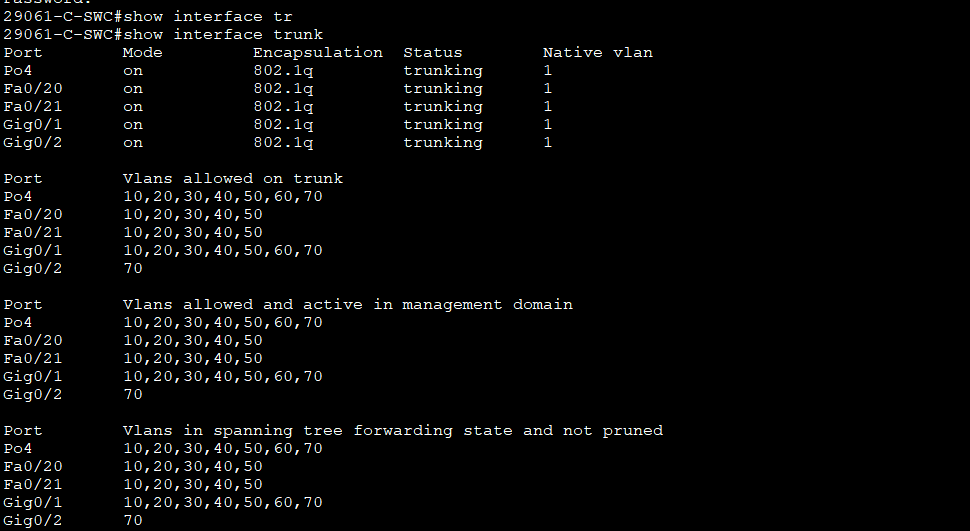


**TABLE OF VERIFICATION COMMANDS**

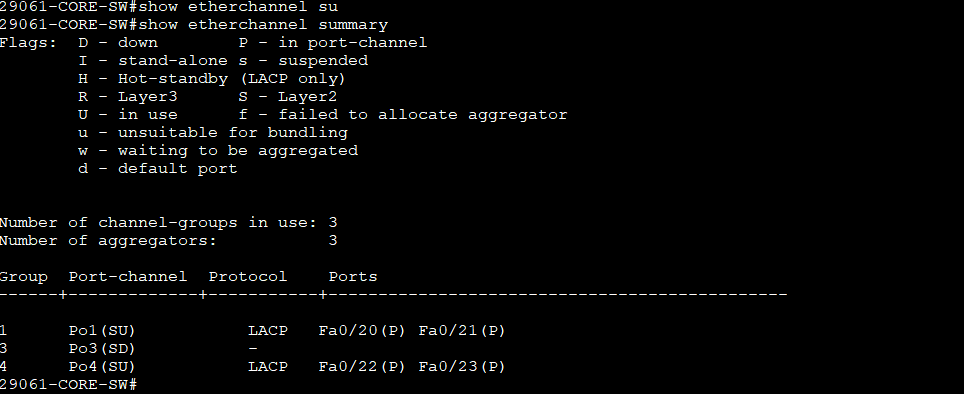


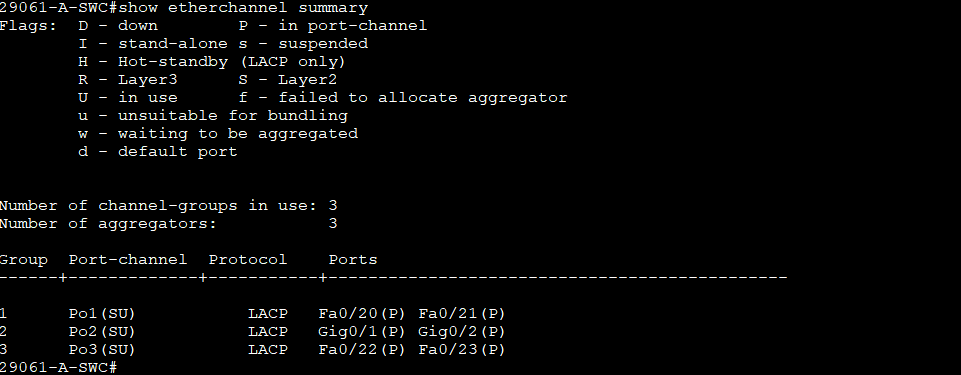
#show interface trunk





#show etherchannel summary





# PHASE 5: Server Configurations & Services

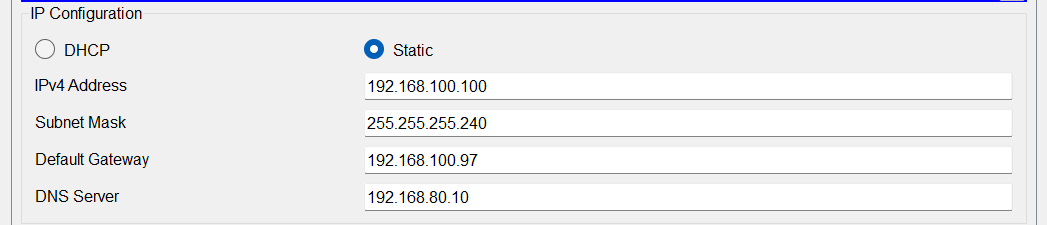
**STATIC IP ADDRESS ON WEB SERVER**

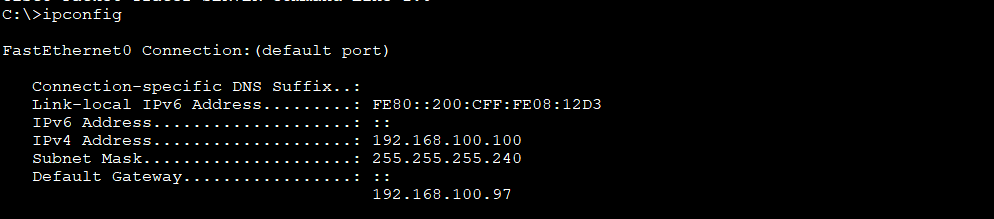
Step 1: Open Server

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

Step 4: Click on Static

Step 5: Fill required field

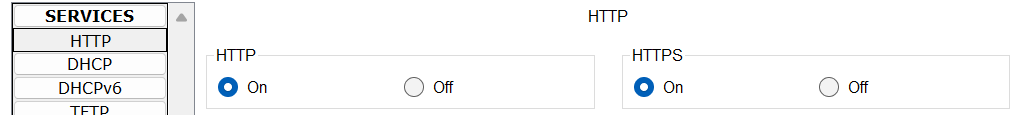




**SERVICE HTTP AND HTTPS ON WEB SERVER**

Step 1: Open Server

Step 2: Click Service Tab

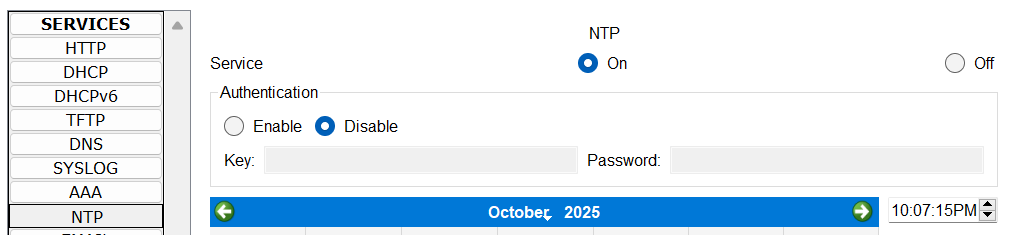
Step 3: Select HTTP on left side  
Step 4: Enable HTTP(ON) & HTTPS (ON) 

**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)

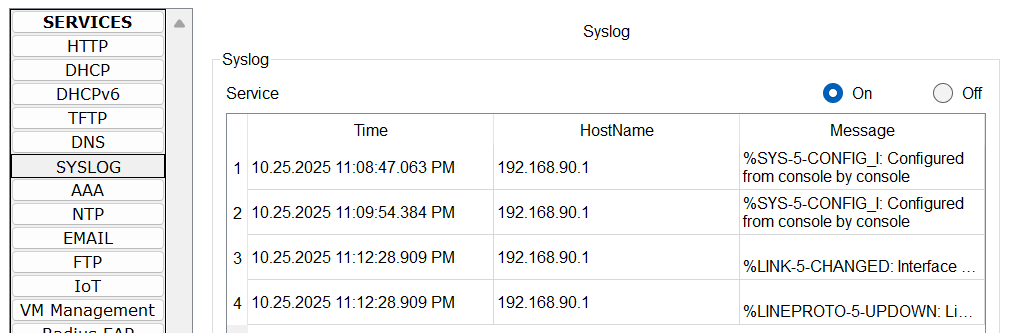
Step 5: Set time  


**SERVICE NTP ON SYLOG SERVER**

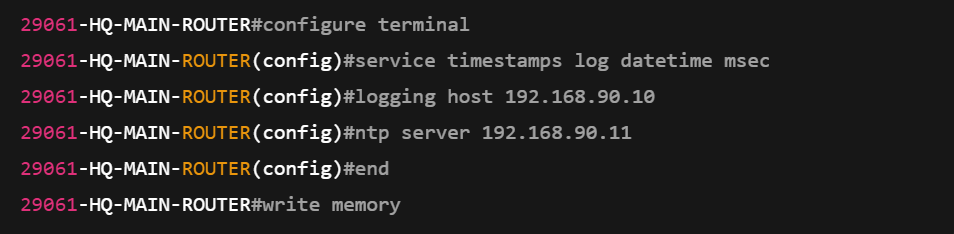
Step 1: Open Server

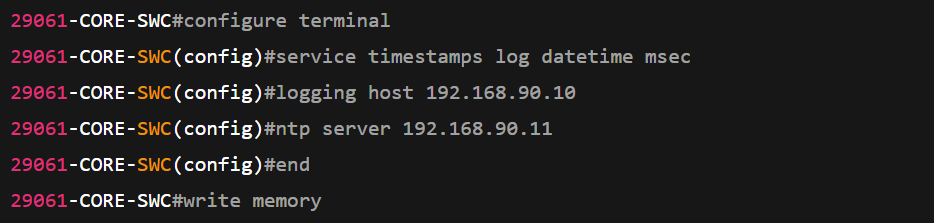
Step 2: Click Service Tab

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

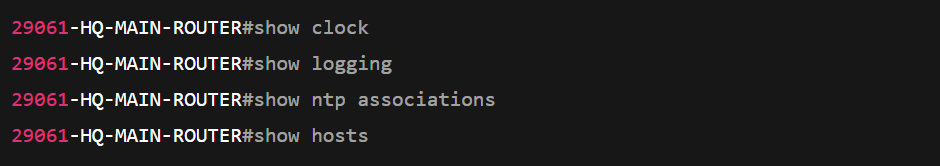


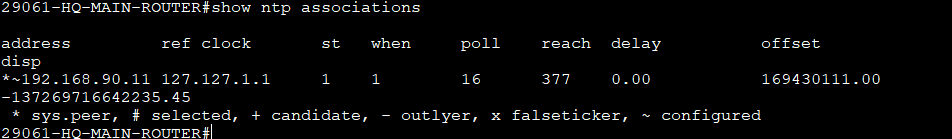
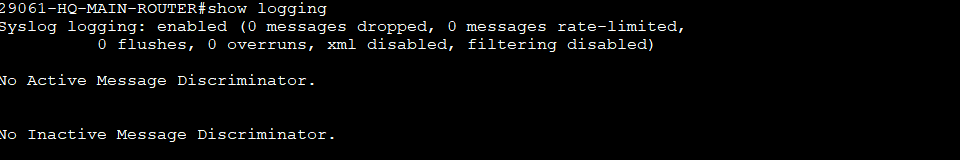
**TABLE OF USED COMMANDS ON BOTH SWITCH AND HQ-MAIN-ROUTER**





**TABLE OF VERIFICATION COMMANDS**



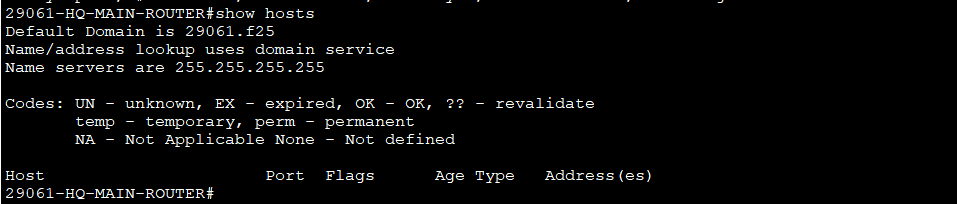


#show show clock

#show logging

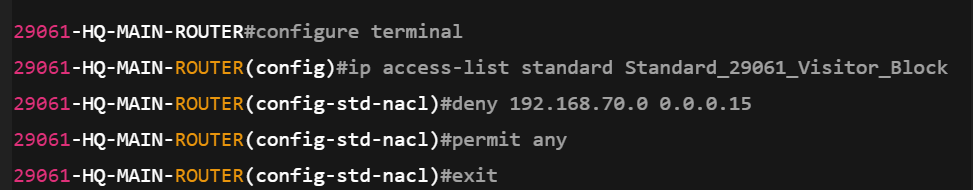
#show ntp association

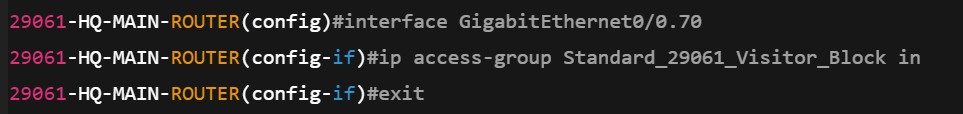
#show hosts



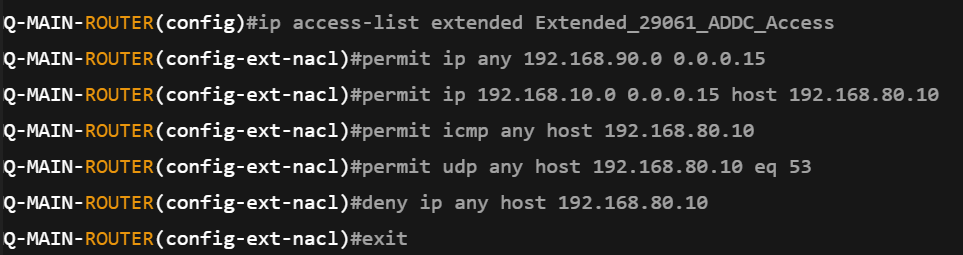
# PHASE 6: Security Implementation

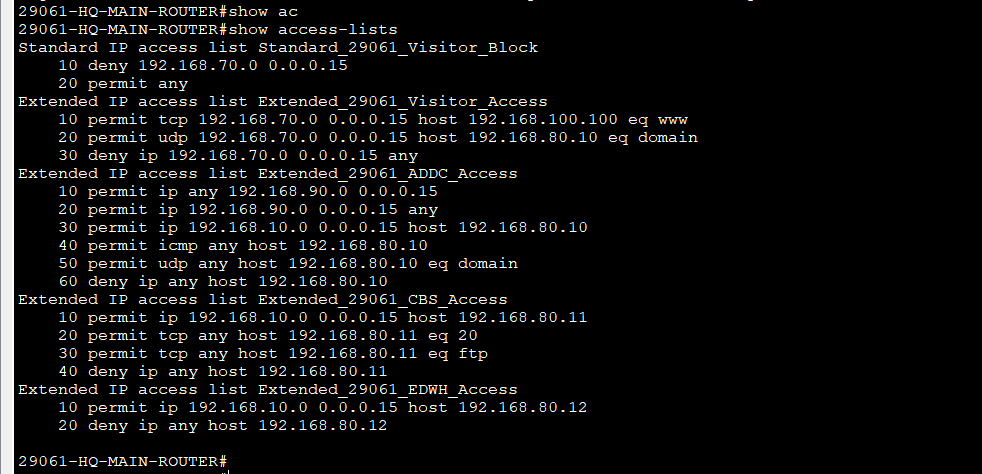
ACL 1 — Block Visitor VLAN (70) from accessing all internal networks



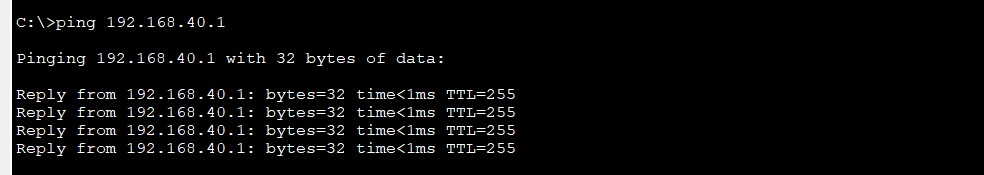


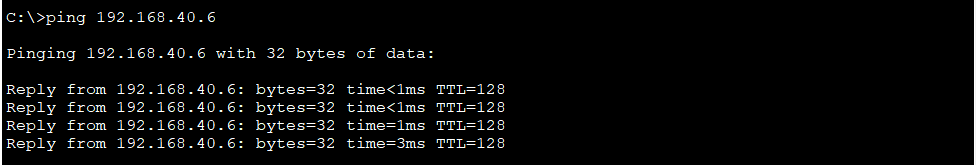
#### **ACL 3 — AD-DC (Full access for IT-NET, limited access for others)**

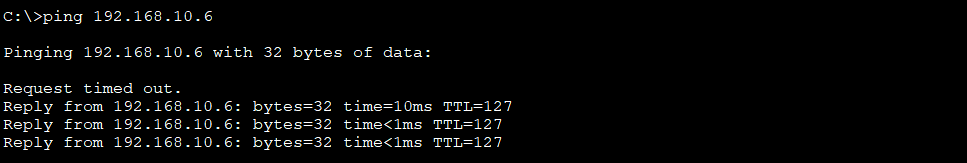


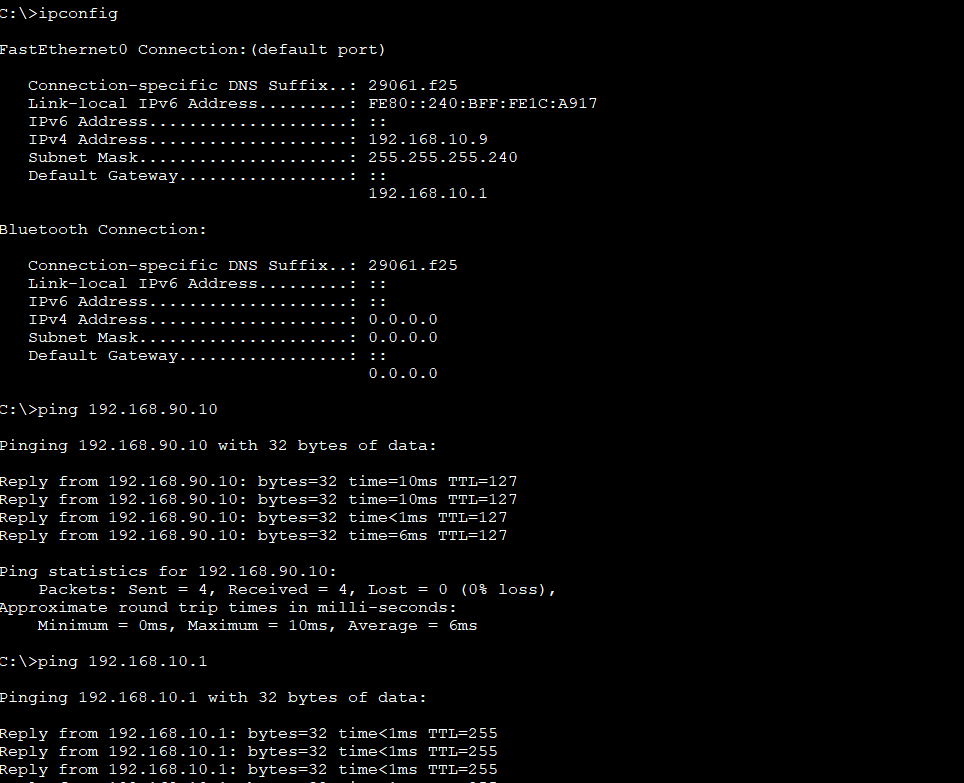


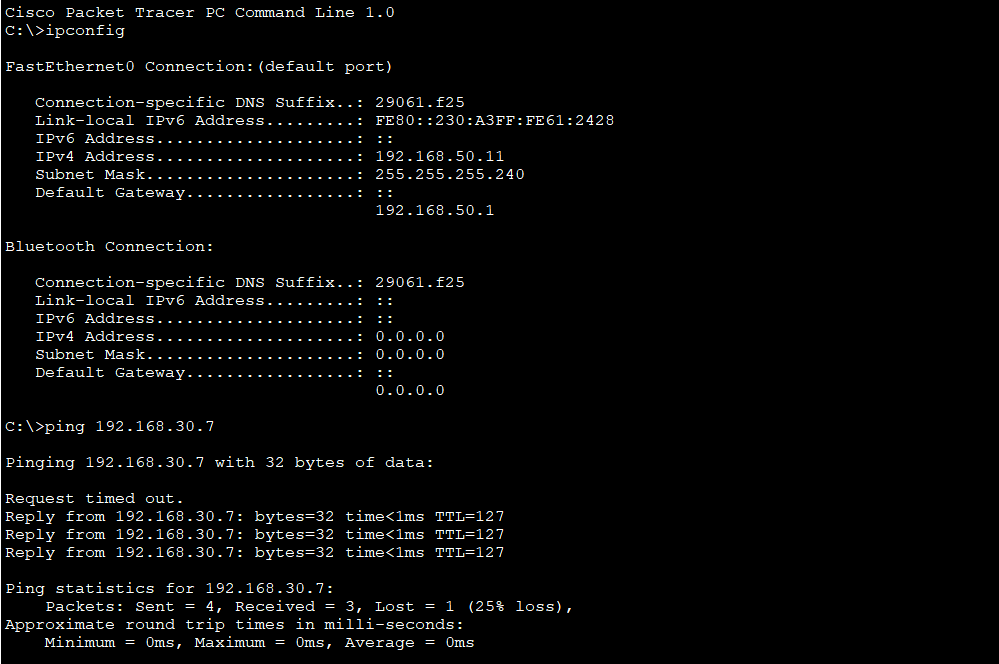
# Connectivity verification











# 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.