ADVENTIST UNIVERSITY OF CENTRAL AFRICA

FACULTY OF INFORMATION TECHNOLOGY

Date: 30th October 2025

COURSE NAME: COMPUTER NETWORK

INSTRUCTOR: JOASHUA IRADUKUNDA

STUDENT NAME: NDARUHUTSE MOISE

STUDENT ID: 28340

MID-TERM EXAM PROJECT: COMPREHENSIVE NETWORK CONFIGURATION GUIDE

Table of Contents

TOPIC 1. Project Overview & Network Topology

1.1 Project Overview

Computer Networking course is the course that help in IT career to solve main problem related on networking. There is the main Project Goal of this Mid-Term Project are:

- Build complete campus network following the provided topology diagram
- Implement VLAN segmentation and inter-VLAN routing on Main-Router
- Configure VTP modes (Server, Transparent, Client) as specified
- Deploy EtherChannel for link aggregation
- Implement comprehensive security controls
- Configure DHCP services for client networks
- Setup DNS and NTP services

1.2 Network Topology Description

This is a hierarchical enterprise network for "28340 _ BANK" with a centralized core architecture connecting multiple departmental networks across different physical locations (HQ blocks) and Main Router.

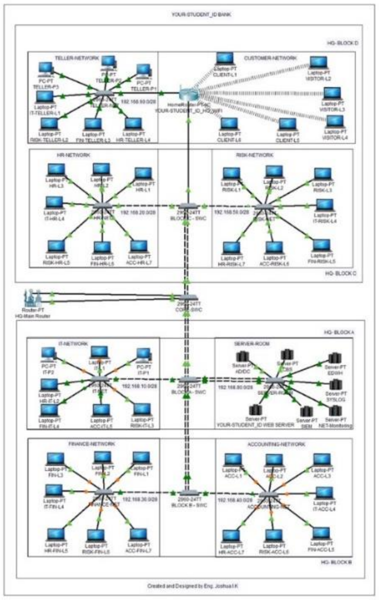


Figure1: Network Topology

TOPIC 2. Pre-Configuration Requirement

Pre-configuration requirements are critical to the success of any network implementation. Here's why they matter for a network topology like the bank system shown:

- Prevents Configuration Errors
- Ensures Security & Compliance
- Optimizes Network Performance
- Establishes Documentation Standards
- Facilitates Troubleshooting

2.1 Software & Equipment Requirement

- Cisco Packet Tracer v8.2.2.0400 or compatible
- Download file format: 28340_NDARUHUTSE MOISE_CNet-F25_MID - ID BANK.pka
- **Console Access:** Use console cable from IT computer to device console port
- **Router & Switch Terminals use Console cable**: To configure any network device (Routers, Switches), connect an IT Computer to the device using a Console cable.
- Lab notebook or digital log for command tracking

TOPIC 3. Naming and Credential Standards

Naming and credential standards are fundamental pillars of professional network management. They directly impact security, efficiency, and long-term maintainability of your network infrastructure. Here are some Key Important why naming and credential standards matter:

- **Security**: Protecting critical banking systems
- **Compliance**: Meeting regulatory requirements
- **Efficiency**: Reducing operational costs
- **Reliability**: Minimizing downtime
- **Scalability**: Supporting business growth
- **Professionalism**: Demonstrating competence

TOPIC 4. Network Device Set Up & Addressing

Every device needs a unique address (like IP addresses) to send and receive data correctly. Without proper addressing, devices can't communicate similar to how mail needs accurate addresses to reach the right destination, Proper addressing schemes (like subnetting) allow you to logically organize networks into manageable segments. This improves performance, security, and makes troubleshooting much easier.

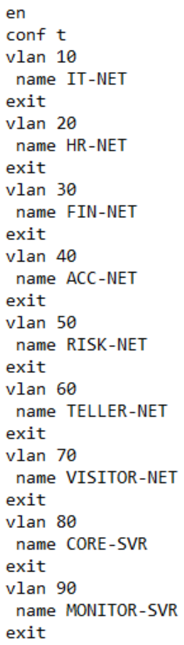
Without proper setup and addressing, you face issues like:

- IP address conflicts causing devices to drop offline
- Security vulnerabilities from default configurations
- Poor network performance and bottlenecks
- Difficulty troubleshooting problems
- Inability to implement network policies or monitoring

TOPIC 5. VLANs Configuration and Port Assignments

A VLAN (Virtual Local Area Network) is a logical grouping of devices on a network, regardless of their physical location. VLANs allow you to segment a single physical network into multiple isolated broadcast domains, creating separate "virtual" networks on the same physical infrastructure.

5.1 Basic of VLANs Configuration Example



```
en
conf t
vlan 10
 name IT-NET
exit
vlan 20
 name HR-NET
exit
vlan 30
 name FIN-NET
exit
vlan 40
 name ACC-NET
exit
vlan 50
 name RISK-NET
exit
vlan 60
 name TELLER-NET
exit
vlan 70
 name VISITOR-NET
exit
vlan 80
 name CORE-SVR
exit
vlan 90
 name MONITOR-SVR
exit
```

Figure 2: Manually VLAN Configuration.

5.2 Port Assignment Types

- **Access Mode**: Port belongs to one VLAN only. Used for end devices like computers, printers, phones.
- **Trunk Mode**: Port carries multiple VLANs. Used for switch-to-switch or switch-to-router connections.
- **Dynamic Mode**: Port can automatically negotiate to become access or trunk (less common in modern networks).

5.3 Importance of VLANs in Networking

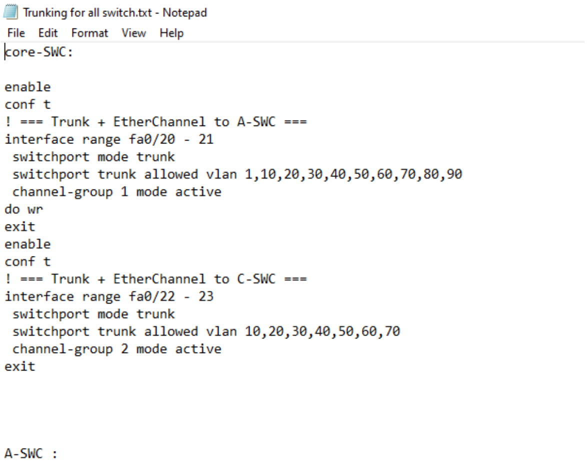
- **Enhanced Security:** VLANs isolate sensitive data by separating departments or functions. For example, your finance department's traffic never mixes with guest Wi-Fi traffic.
- **Improved Performance:** Each VLAN is its own broadcast domain. Broadcasts from one VLAN don't flood the entire network, reducing unnecessary traffic.
- **Simplified Network Management**: Group devices by function (Sales, HR, IT) rather than physical location, making the network structure match your organizational structure.
- **Better Traffic Management:** Easier to identify and troubleshoot issues when traffic is logically separated.
- **Cost Savings:** You don't need separate physical switches for each department - one switch can host multiple virtual networks, Easy to expand without major infrastructure investments.

TOPIC 6. Trunking and EtherChannel Configuration

6.1 Trunking

Trunking is a method of carrying traffic from multiple VLANs over a single physical network link between switches, routers, or other network devices. Instead of needing a separate cable for each VLAN, a trunk link uses VLAN tagging to identify which VLAN each frame belongs to, allowing all VLAN traffic to share the same connection.

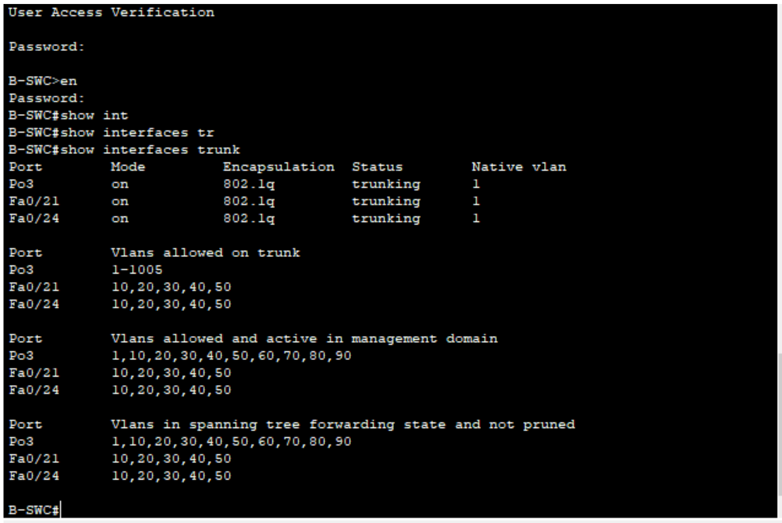
6.1.1 Basic Trunking Configuration Example (Cisco)


Trunking for all switch.txt - Notepad
File Edit Format View Help

```
core-SWC:

enable
conf t
! === Trunk + EtherChannel to A-SWC ===
interface range fa0/20 - 21
 switchport mode trunk
 switchport trunk allowed vlan 1,10,20,30,40,50,60,70,80,90
 channel-group 1 mode active
do wr
exit
enable
conf t
! === Trunk + EtherChannel to C-SWC ===
interface range fa0/22 - 23
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 channel-group 2 mode active
exit



A-SWC :
```

Figure 3: Basic Trunking Configuration

6.1.2 To Verify Trunking Configuration



```
User Access Verification

Password:

B-SWC>en
Password:
B-SWC#show int
B-SWC#show interfaces tr
B-SWC#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po3         on           802.1q         trunking      1
Fa0/21      on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po3         1-1005
Fa0/21      10,20,30,40,50
Fa0/24      10,20,30,40,50

Port        Vlans allowed and active in management domain
Po3         1,10,20,30,40,50,60,70,80,90
Fa0/21      10,20,30,40,50
Fa0/24      10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Po3         1,10,20,30,40,50,60,70,80,90
Fa0/21      10,20,30,40,50
Fa0/24      10,20,30,40,50

B-SWC#
```

Figure 4: Showing verification of Trunking.

6.2 EtherChannel Configuration

EtherChannel is a port link aggregation technology that bundles multiple physical Ethernet links into a single logical link. This creates a high-bandwidth connection between switches, or between a switch and a server/router. There are Three Ways to Configure EtherChannel:

1.PAgP (Port Aggregation Protocol):

- Cisco proprietary
- Modes: desirable (active) and auto (passive)

2.**LACP (Link Aggregation Control Protocol)**

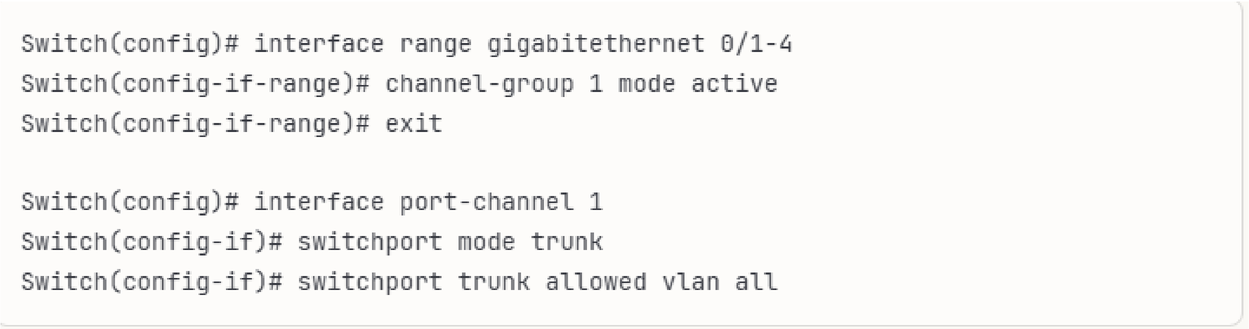
- IEEE 802.3ad standard (industry standard)
- Modes: active and passive
- Preferred for multi-vendor environments

3. **Static (Manual) Configuration**

- Mode: on
- No negotiation protocols

- Both sides must be manually configured

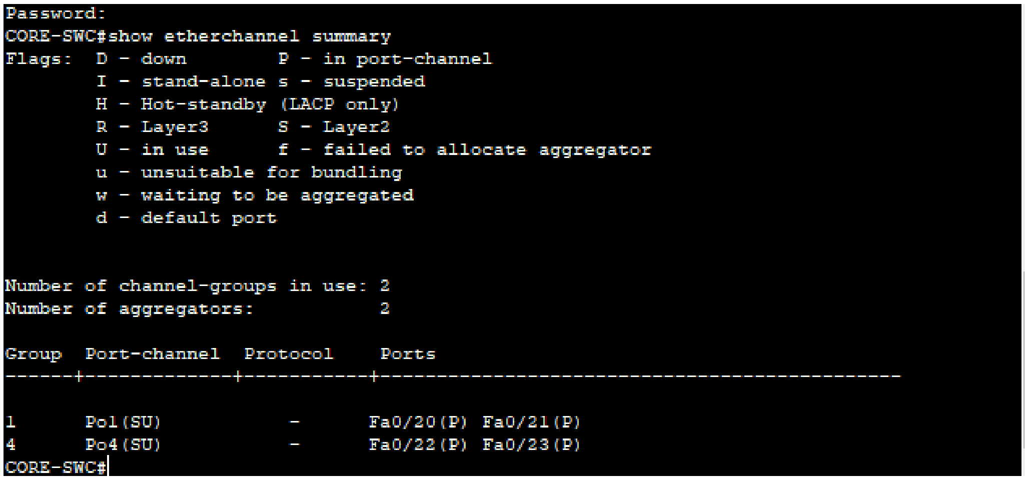
6.2.1 Basic EtherChannel Configuration (Cisco)



```
Switch(config)# interface range gigabitethernet 0/1-4
Switch(config-if-range)# channel-group 1 mode active
Switch(config-if-range)# exit

Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
```

Figure 5: Showing EtherChannel Configuration

6.2.2 To verify the EtherChannel Configuration



```
Password:
CORE-SWC#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------------

1      Po1(SU)           -      Fa0/20(P) Fa0/21(P)
4      Po4(SU)           -      Fa0/22(P) Fa0/23(P)
CORE-SWC#
```

Figure 6: Showing verification of EtherChannel configuration.

TOPIC 7. Server Configuration & Services

Server configuration refers to the process of setting up, optimizing, and managing server hardware and software to provide specific services to clients on a network. It involves installing operating systems, configuring network settings, implementing security measures, and deploying various services. In Our Project we have several different Server we are going to see their functionality in our project. We have Web-Server, AD/DC server, CBS server, EDWH server, Syslog server, NET-monitoring server and SIEM server.

- **Web-Server:** is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the internet or intranet. Its core job is to store, process, and deliver web pages and content to users.
- **AD/DC server:** is Microsoft's directory service that manages and organizes network resources in a Windows domain environment. It provides centralized authentication, authorization, and management of users, computers, and other network objects.
- **CBS server:** CBS is Windows' built-in servicing technology for managing system components, updates, and configurations.
- **EDWH server:** is a centralized repository that stores integrated data from multiple sources across an entire organization.
- **Syslog server:** is logging system that collects, stores, and manages log messages from network devices, servers, applications, and security systems across an IT infrastructure.
- **NET-monitoring server:** is system that continuously observes, tracks, and analyzes the performance, availability, and health of network infrastructure, devices, servers, and applications. It provides real-time visibility into network operations and alerts administrators to issues before they impact users.
- **SIEM server:** server is a comprehensive security platform that collects, aggregates, analyzes, and correlates security-related data from across an entire IT infrastructure in real-time.

7.1 Example of Web Server configured on this project

TOPIC 8. Security Implementation

Security implementation in networking means applying different security measures, tools, and configurations to protect network devices, data, and communication from unauthorized access, misuse, or attacks. It ensures that confidentiality, integrity, and availability of data are maintained throughout the network.

8.1 The Main Component of Security Implementation in Networking

1. **Device Security:** Protects routers, switches, and servers by controlling who can access or configure them.

Examples:

- Setting strong passwords
- Using SSH instead of Telnet for remote access
- Implementing AAA (Authentication, Authorization, Accounting)

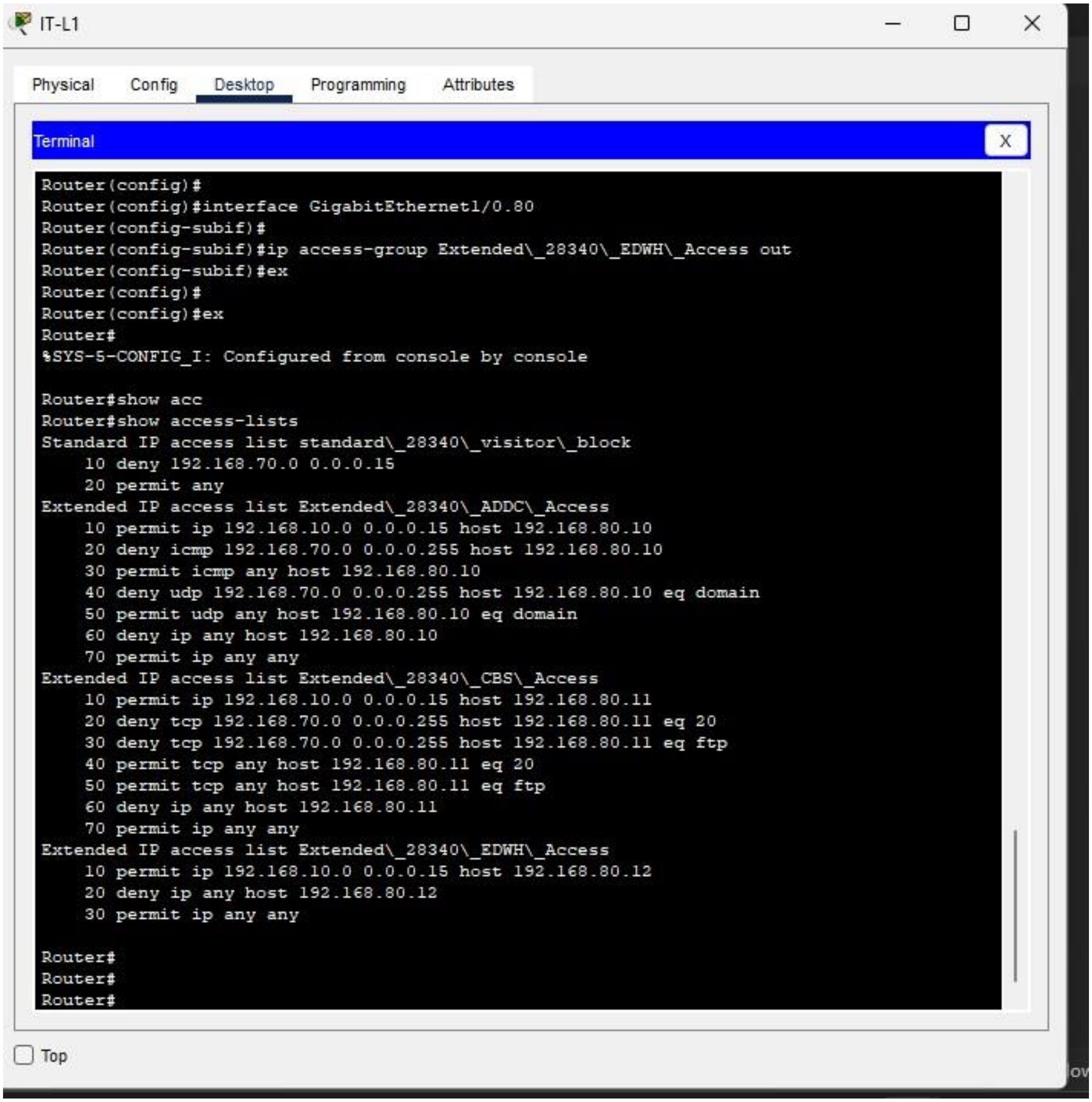
8.1.2 Device Security using SSH (Secure Shell) Configuration

2. **Network Access Control:** Restricts what users and devices can do once they're connected.

Examples:

- **Access Control Lists (ACLs)**: filter traffic by IP, port, or protocol
- **Port security**: limit which devices can connect to a switch port
- **802.1X authentication**: verify devices before granting access

8.1.3 Access Control list verification (ACL)



```
Router(config)#
Router(config)#interface GigabitEthernet1/0.80
Router(config-subif)#
Router(config-subif)#ip access-group Extended\_28340\_EDWH\_Access out
Router(config-subif)#ex
Router(config)#
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show acc
Router#show access-lists
Standard IP access list standard\_28340\_visitor\_block
    10 deny 192.168.70.0 0.0.0.15
    20 permit any
Extended IP access list Extended\_28340\_ADDC\_Access
    10 permit ip 192.168.10.0 0.0.0.15 host 192.168.80.10
    20 deny icmp 192.168.70.0 0.0.0.255 host 192.168.80.10
    30 permit icmp any host 192.168.80.10
    40 deny udp 192.168.70.0 0.0.0.255 host 192.168.80.10 eq domain
    50 permit udp any host 192.168.80.10 eq domain
    60 deny ip any host 192.168.80.10
    70 permit ip any any
Extended IP access list Extended\_28340\_CBS\_Access
    10 permit ip 192.168.10.0 0.0.0.15 host 192.168.80.11
    20 deny tcp 192.168.70.0 0.0.0.255 host 192.168.80.11 eq 20
    30 deny tcp 192.168.70.0 0.0.0.255 host 192.168.80.11 eq ftp
    40 permit tcp any host 192.168.80.11 eq 20
    50 permit tcp any host 192.168.80.11 eq ftp
    60 deny ip any host 192.168.80.11
    70 permit ip any any
Extended IP access list Extended\_28340\_EDWH\_Access
    10 permit ip 192.168.10.0 0.0.0.15 host 192.168.80.12
    20 deny ip any host 192.168.80.12
    30 permit ip any any

Router#
Router#
Router#
```

Figure 9: Showing Accessing Control List verification

3. Monitoring and Logging: Tracks and records network activity to detect unusual or malicious behavior.

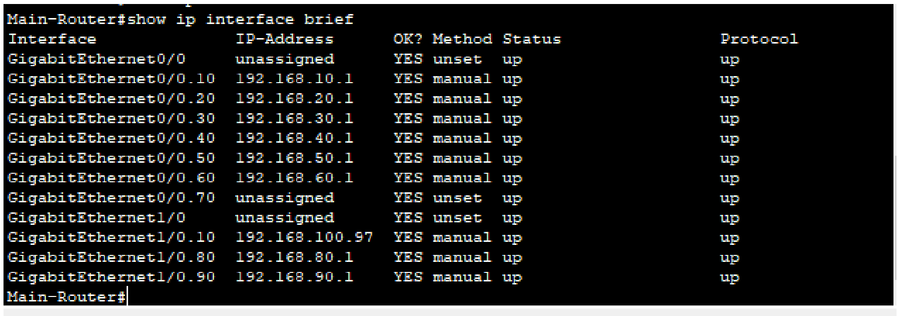
Examples:

- **Syslog servers**: store logs from routers/switches
- **SNMP monitoring**: track network performance and alerts
- **IDS/IPS logs**: detect security threats

TOPIC 9. Verification and Testing Procedures

9.1 Verification

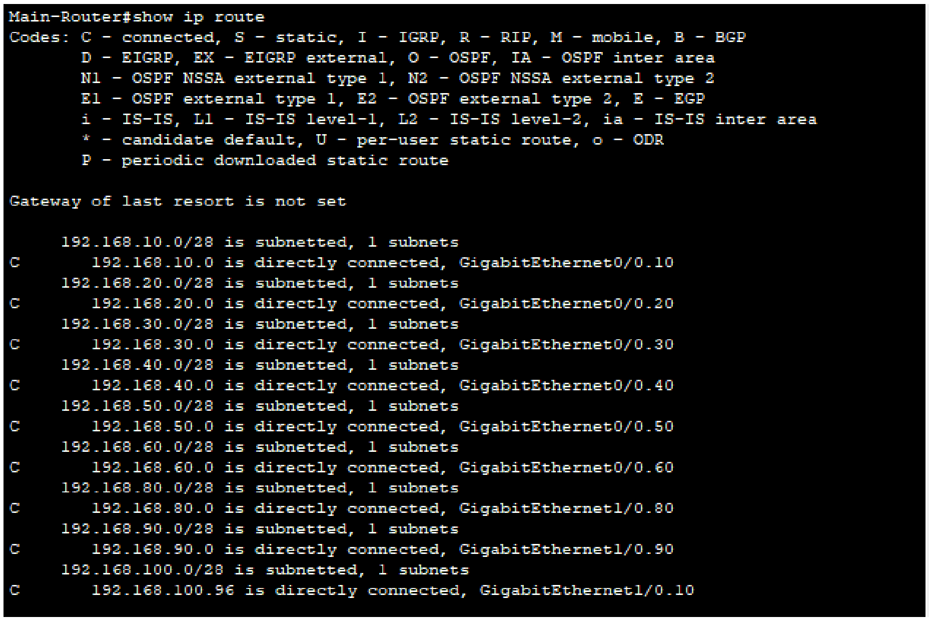
1. Show Ip Interfaces Brief



```
Main-Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
GigabitEthernet0/0.40  192.168.40.1    YES manual up                    up
GigabitEthernet0/0.50  192.168.50.1    YES manual up                    up
GigabitEthernet0/0.60  192.168.60.1    YES manual up                    up
GigabitEthernet0/0.70  unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  up                    up
GigabitEthernet1/0.10  192.168.100.97  YES manual up                    up
GigabitEthernet1/0.80  192.168.80.1    YES manual up                    up
GigabitEthernet1/0.90  192.168.90.1    YES manual up                    up
Main-Router#
```

Figure 11: Showing interface and their status on router.

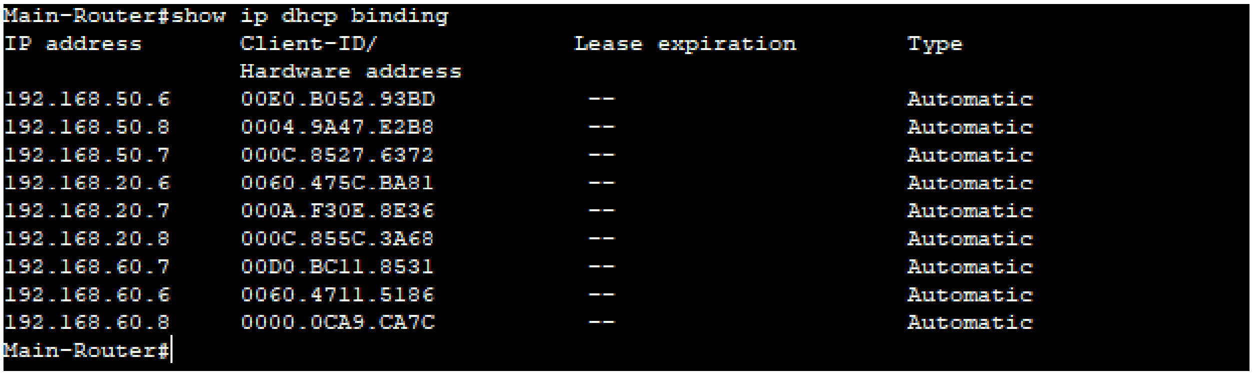
2. Show Ip Route



```
Main-Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/28 is subnetted, 1 subnets
C       192.168.10.0 is directly connected, GigabitEthernet0/0.10
     192.168.20.0/28 is subnetted, 1 subnets
C       192.168.20.0 is directly connected, GigabitEthernet0/0.20
     192.168.30.0/28 is subnetted, 1 subnets
C       192.168.30.0 is directly connected, GigabitEthernet0/0.30
     192.168.40.0/28 is subnetted, 1 subnets
C       192.168.40.0 is directly connected, GigabitEthernet0/0.40
     192.168.50.0/28 is subnetted, 1 subnets
C       192.168.50.0 is directly connected, GigabitEthernet0/0.50
     192.168.60.0/28 is subnetted, 1 subnets
C       192.168.60.0 is directly connected, GigabitEthernet0/0.60
     192.168.80.0/28 is subnetted, 1 subnets
C       192.168.80.0 is directly connected, GigabitEthernet1/0.80
     192.168.90.0/28 is subnetted, 1 subnets
C       192.168.90.0 is directly connected, GigabitEthernet1/0.90
     192.168.100.0/28 is subnetted, 1 subnets
C       192.168.100.96 is directly connected, GigabitEthernet1/0.10
```

Figure 12: Showing routing table.

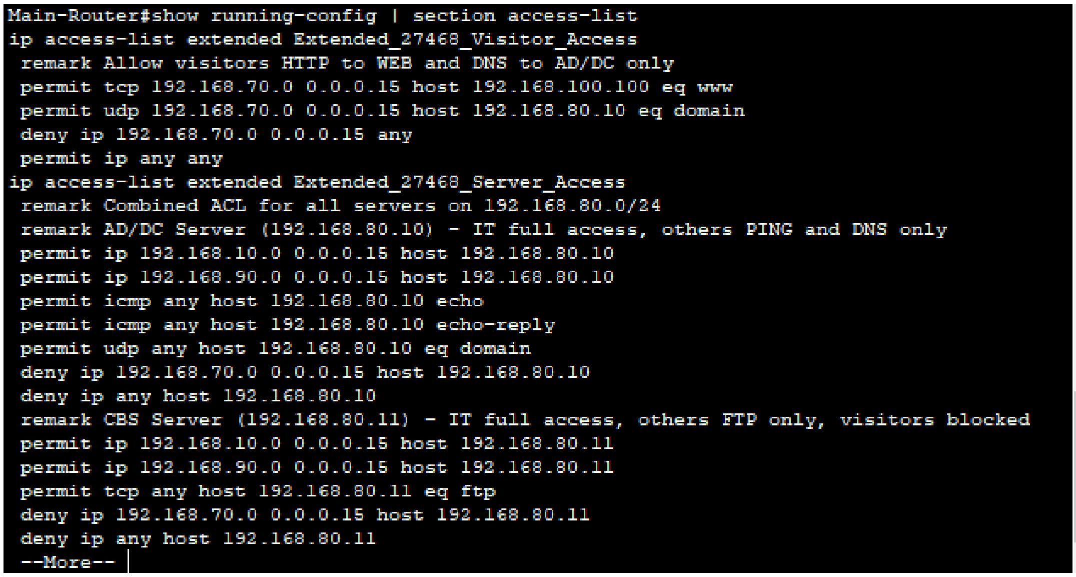
3. Show IP DHCP Binding



```
Main-Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.50.6     00E0.B052.93BD           --                     Automatic
192.168.50.8     0004.9A47.E2B8           --                     Automatic
192.168.50.7     000C.8527.6372           --                     Automatic
192.168.20.6     0060.475C.BA81           --                     Automatic
192.168.20.7     000A.F30E.8E36           --                     Automatic
192.168.20.8     000C.855C.3A68           --                     Automatic
192.168.60.7     00D0.BC11.8531           --                     Automatic
192.168.60.6     0060.4711.5186           --                     Automatic
192.168.60.8     0000.0CA9.CA7C           --                     Automatic
Main-Router#
```

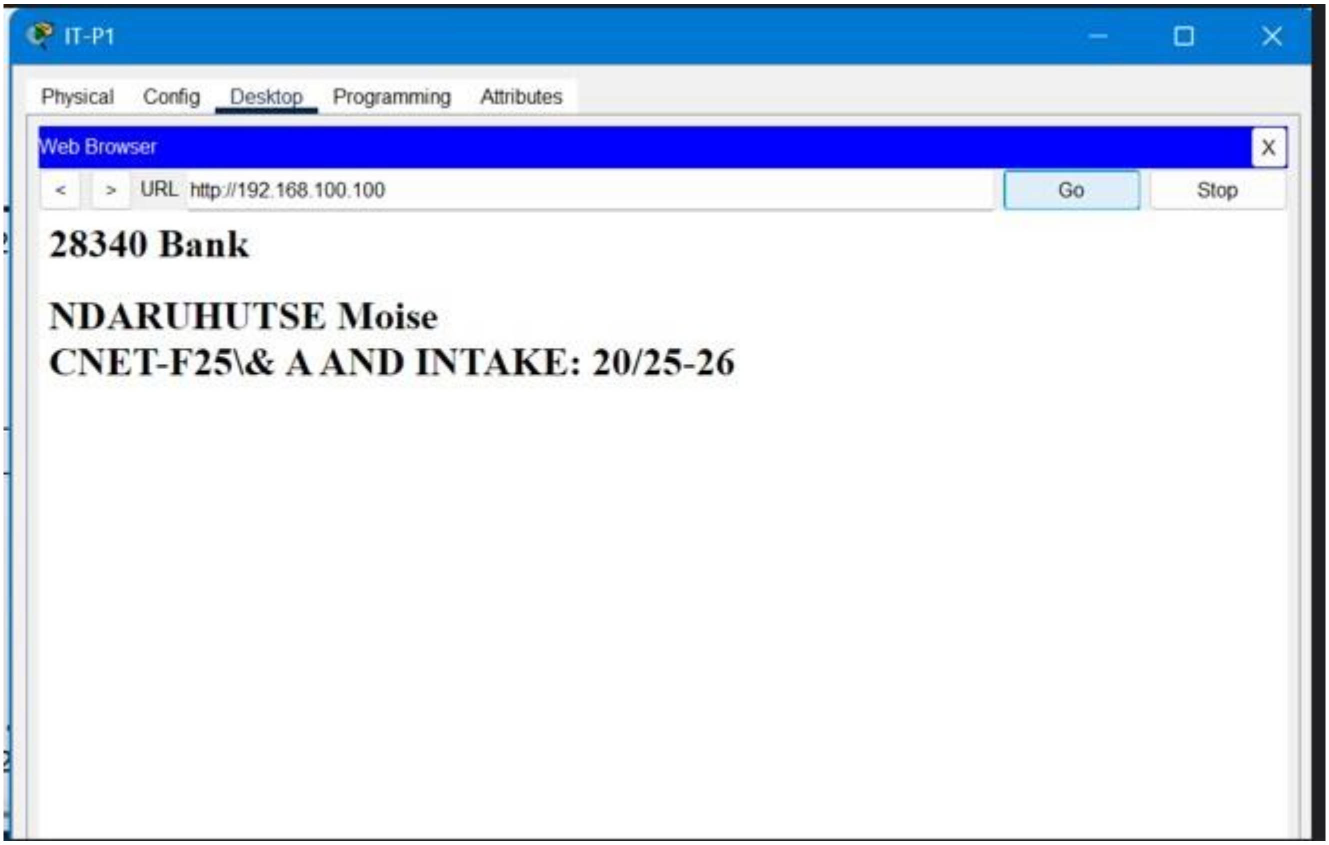
Figure 13: Showing binding DHCP in router.

4. show Ip access-lists Visitor Access



```
Main-Router#show running-config | section access-list
ip access-list extended Extended_27468_Visitor_Access
 remark Allow visitors HTTP to WEB and DNS to AD/DC only
 permit tcp 192.168.70.0 0.0.0.15 host 192.168.100.100 eq www
 permit udp 192.168.70.0 0.0.0.15 host 192.168.80.10 eq domain
 deny ip 192.168.70.0 0.0.0.15 any
 permit ip any any
ip access-list extended Extended_27468_Server_Access
 remark Combined ACL for all servers on 192.168.80.0/24
 remark AD/DC Server (192.168.80.10) - IT full access, others PING and DNS only
 permit ip 192.168.10.0 0.0.0.15 host 192.168.80.10
 permit ip 192.168.90.0 0.0.0.15 host 192.168.80.10
 permit icmp any host 192.168.80.10 echo
 permit icmp any host 192.168.80.10 echo-reply
 permit udp any host 192.168.80.10 eq domain
 deny ip 192.168.70.0 0.0.0.15 host 192.168.80.10
 deny ip any host 192.168.80.10
 remark CBS Server (192.168.80.11) - IT full access, others FTP only, visitors blocked
 permit ip 192.168.10.0 0.0.0.15 host 192.168.80.11
 permit ip 192.168.90.0 0.0.0.15 host 192.168.80.11
 permit tcp any host 192.168.80.11 eq ftp
 deny ip 192.168.70.0 0.0.0.15 host 192.168.80.11
 deny ip any host 192.168.80.11
 --More--
```

Web Access by IP and DNS Resolution



URL http://192.168.100.100

28340 Bank

NDARUHUTSE Moise
CNET-F25\& A AND INTAKE: 20/25-26

END