Project: Network Security Lab - VLAN Segmentation, DHCP & ACLs

Simulated enterprise LAN configuration in Cisco Packet Tracer

Author: Harrison Whitely

Date/Version: August 2025 - v1.0

Executive Summary

In this project, I designed and configured a secure LAN topology in Cisco Packet Tracer. The network included multiple VLANs, DHCP pools, and ACLs to restrict unauthorised access. I validated connectivity with test clients and confirmed that security policies were enforced. This demonstrates my ability to configure and troubleshoot networking features relevant to IT support and entry-level network administration roles.

Table of Contents

Network Topology & Design

The TMC LAN was designed in Cisco Packet Tracer to simulate a small enterprise environment with multiple VLANs, DHCP, and ACL-based network security. The network consists of routers, switches, servers, and client devices across four VLANS, connected via trunk and routed links.

VLANs & Subnets

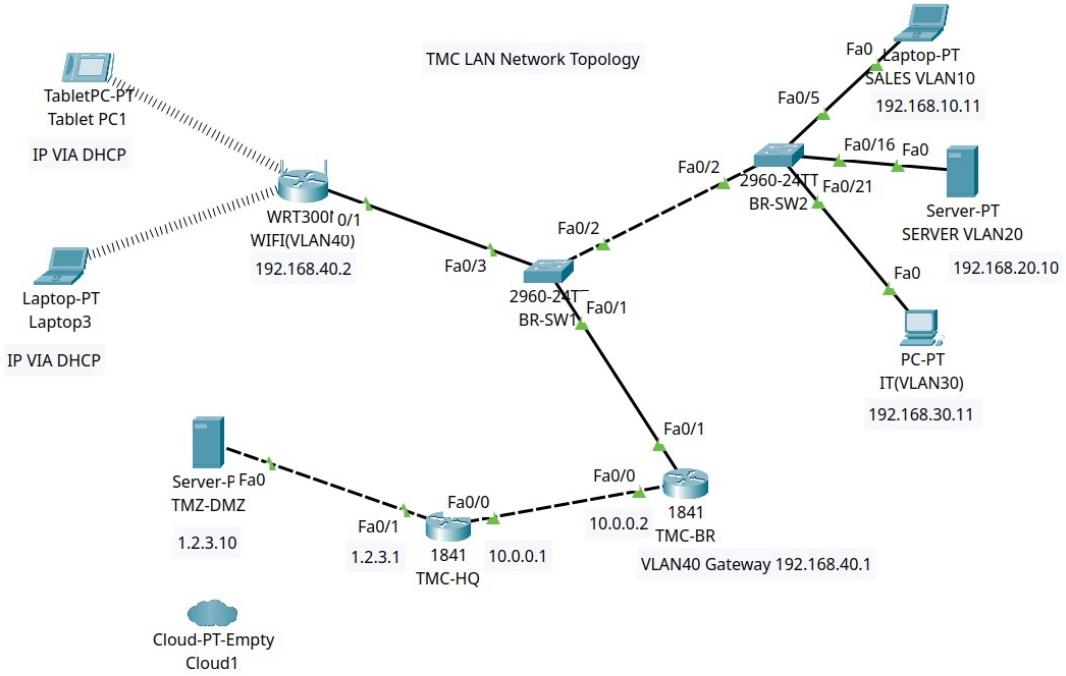
- **VLAN 10 - Sales**
  - Subnet: 192.168.10.0/24
  - Gateway 192.168.10.1
  - Devices: 1 laptop (Sales-PC, 192.168.10.11)
- **VLAN 20 - Servers**
  - Subnet: 192.168.20.0/24
  - Gateway: 192.168.20.1
  - Devices: 1 server (Server-PT, 192.168.20.10)
- **VLAN 30 - IT**
  - Subnet: 192.168.30.0/24
  - Gateway: 192.168.30.1
  - Devices: 1 IT workstation (PC-PT, 192.168.30.11)
- **VLAN 40 - Guest Wi-Fi**
  - Subnet: 192.168.40.0/24
  - Gateway: 192.168.40.1
  - Devices: 1 tablet and 1 laptop (both assigned via DHCP), wireless AP IP 192.168.40.2

Core Devices

- **Router TMC-HQ**
  - Interface Fa0/0 - DMZ link (1.2.3.1)
  - Interface Fa0/1 - WAN link (10.0.0.1)
  - Runs RIP v2 for branch routing.
- **Router TMC-BR**
  - Interface Fa0/0 - link to HQ (10.0.0.2)
  - Interface Fa0/1 - link to Switch BR-SW1 (VLAN trunk)

- Provides inter-VLAN routing

- **Switches BR-SW1 & BR-SW2**
  - Configured trunk ports for VLAN transport
  - Provide access for Sales, IT, Server, and Guest VLAN devices
- **WRT300N Wireless Router**
  - Acts as an access point for Guest VLAN40
  - Connected to Switch BR-SW1 (192.168.40.2)
- **Server-PT (DMZ)**
  - Located outside the LAN on subnet 1.2.3.9/24 (1.2.3.10)
  - Represents external-facing services
- **Cloud (TPG NBN)**
  - Simulates WAN/Internet connection



(Screenshot: **Figure 1** - *Updated Packet Tracer topology with four VLANs (Sales, Servers, IT, and Guest Wi-Fi) interconnected via BR-SW1/BR-SW2 and routed by TMC-HQ/TMC-BR)*

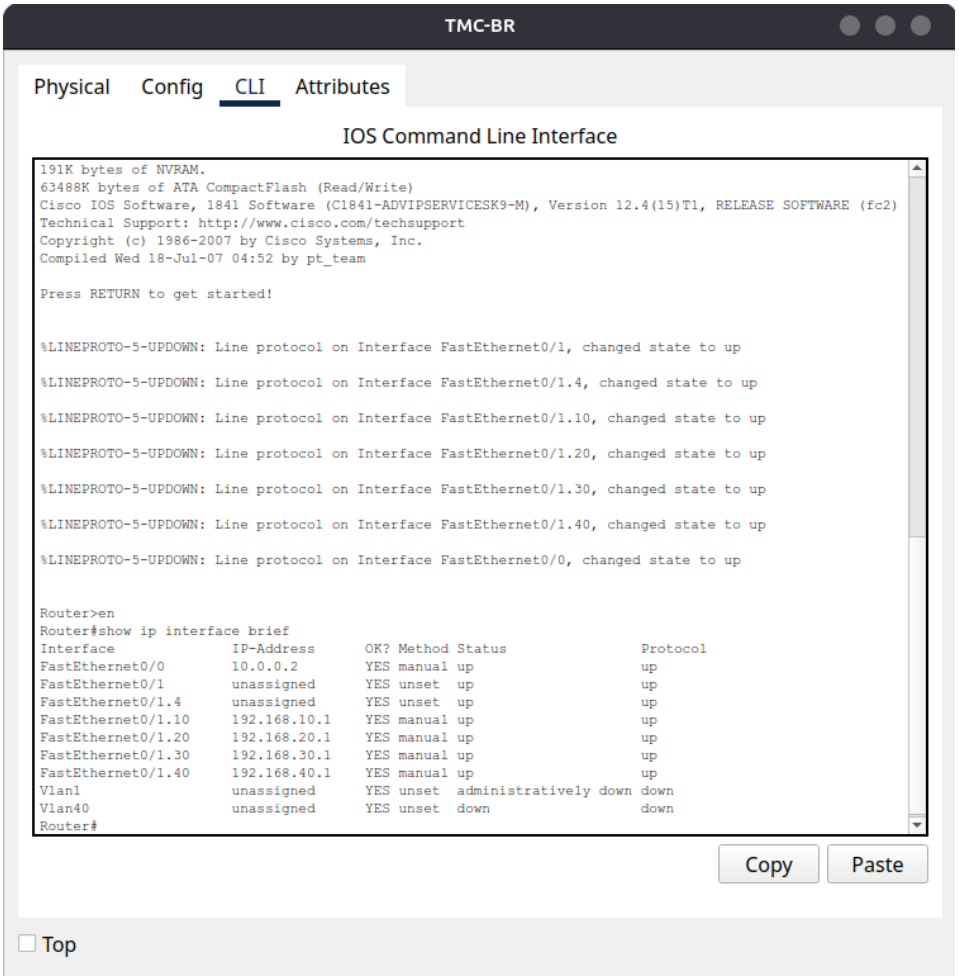
Configuration Steps

VLAN Setup

To segment the network into departments, I implemented a Router-on-a-Stick configuration on the TMC-BR router. A single FastEthernet interface (Fa0/1) was divided into four 802.1Q subinterfaces, each acting as the default gateway for its VLAN.

Subinterface Configuration

- VLAN 10 - Sales - 192.168.10.1/24
- VLAN 20 - Servers - 192.168.20.1/24
- VLAN 30 - IT - 192.168.30.1/24
- VLAN 40 - Guest Wi-Fi - 192.168.40.1/24



(Screenshot: **Figure 2** - *Subinterfaces configured for VLAN 10, 20, 30 and 40 with correct IP addresses)*

Configuration Snippet

```
TMC-BR(config)# interface fa0/1.10
TMC-BR(config-subif)# encapsulation dot1Q 10
TMC-BR(config-subif)# ip address 192.168.10.1 255.255.255.0

TMC-BR(config)# interface fa0/1.20
TMC-BR(config-subif)# encapsulation dot1Q 20
TMC-BR(config-subif)# ip address 192.168.20.1 255.255.255.0

TMC-BR(config)# interface fa0/1.30
TMC-BR(config-subif)# encapsulation dot1Q 30
TMC-BR(config-subif)# ip address 192.168.30.1 255.255.255.0

TMC-BR(config)# interface fa0/1.40
TMC-BR(config-subif)# encapsulation dot1Q 40
TMC-BR(config-subif)# ip address 192.168.40.1 255.255.255.0
```

Verification

Used the *show ip interface brief* command to confirm all VLAN subinterfaces were:

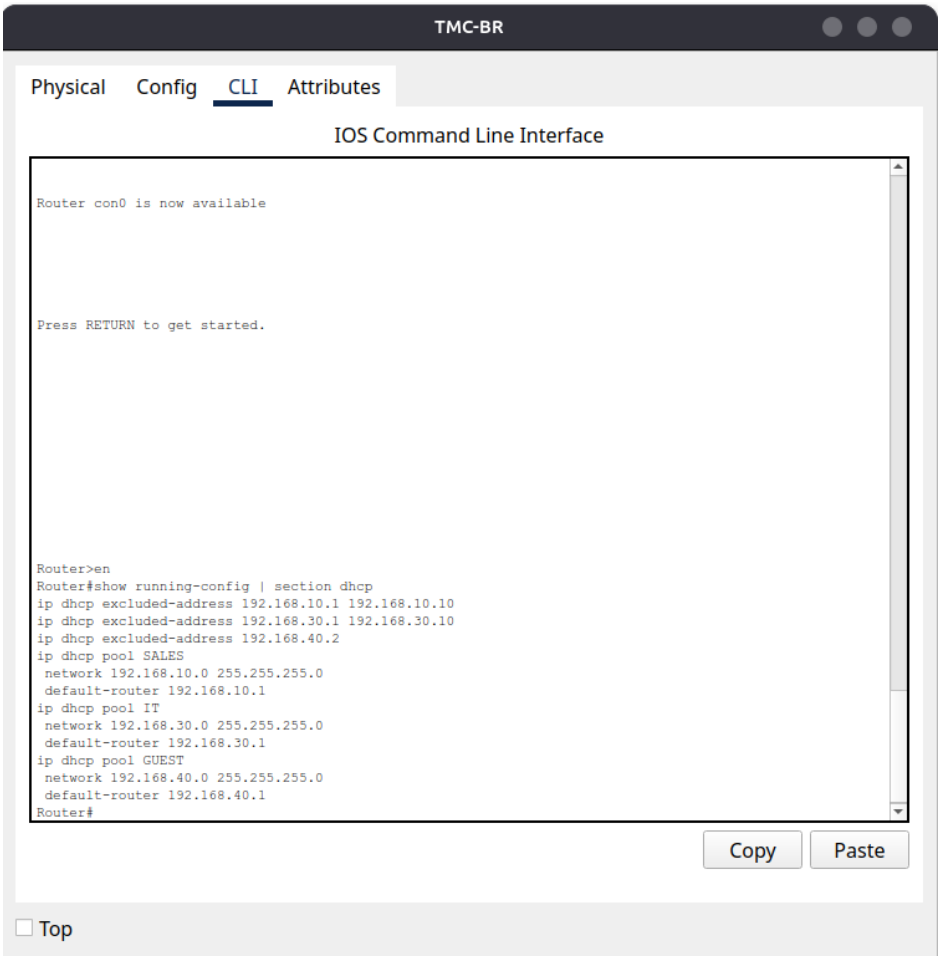
- Admin up
- Protocol up
- Assigned correct IP addresses

DHCP Setup

To simplify IP management, I configured DHCP pools on the TMC-BR router for all VLANs except the Server VLAN (VLAN 20), which used static addressing. Each DHCP pool was tied to its VLAN subnet, with default gateway and DNS settings provided automatically.

DHCP Pool Configuration

- **VLAN 10 – Sales**
  Network: 192.168.10.0/24
  Gateway: 192.168.10.1
  Pool Name: SALES
- **VLAN 30 – IT**
  Network: 192.168.30.0/24
  Gateway: 192.168.30.1
  Pool Name: IT
- **VLAN 40 - Guest Wi-Fi**
  Network: 192.168.40.0/24
  Gateway: 192.168.40.1
  Pool Name: GUEST



(Screenshot: **Figure 3** - *DHCP pools configured for VLAN 10, VLAN, 30, and VLAN 40)*

Configuration Snippet

TMC-BR(config)# ip dhcp pool SALES

TMC-BR(dhcp-config)# network 192.168.10.0 255.255.255.0

TMC-BR(dhcp-config)# default-router 192.168.10.1

TMC-BR(config)# ip dhcp pool IT

TMC-BR(dhcp-config)# network 192.168.30.0 255.255.255.0

TMC-BR(dhcp-config)# default-router 192.168.30.1

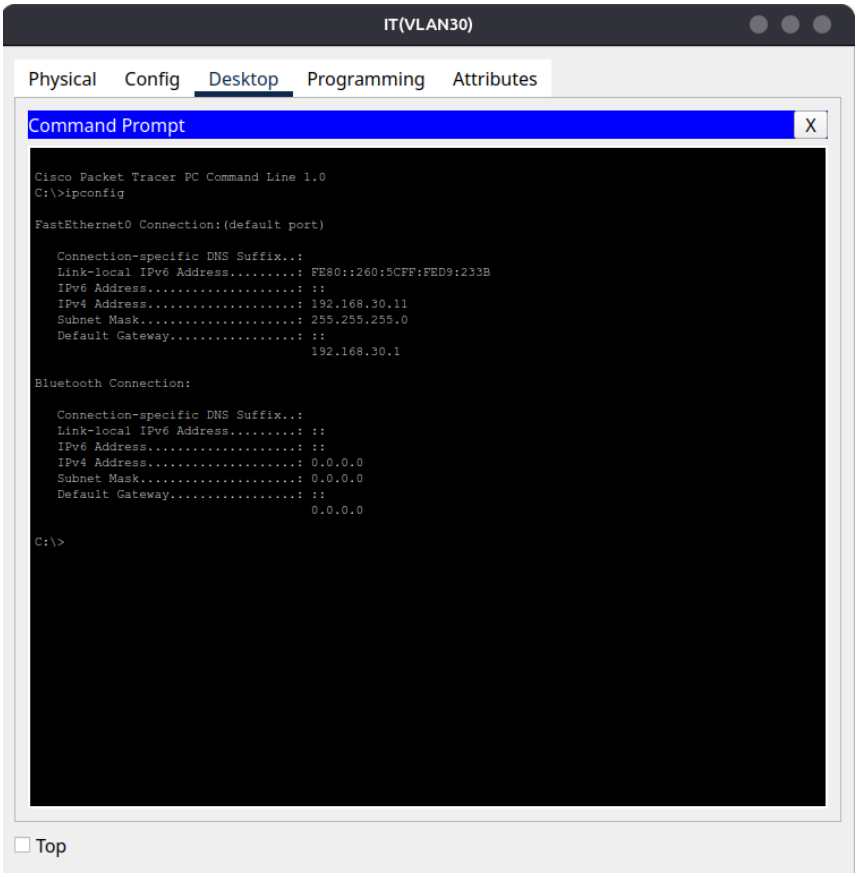
TMC-BR(config)# ip dhcp pool GUEST

TMC-BR(dhcp-config)# network 192.168.40.0 255.255.255.0

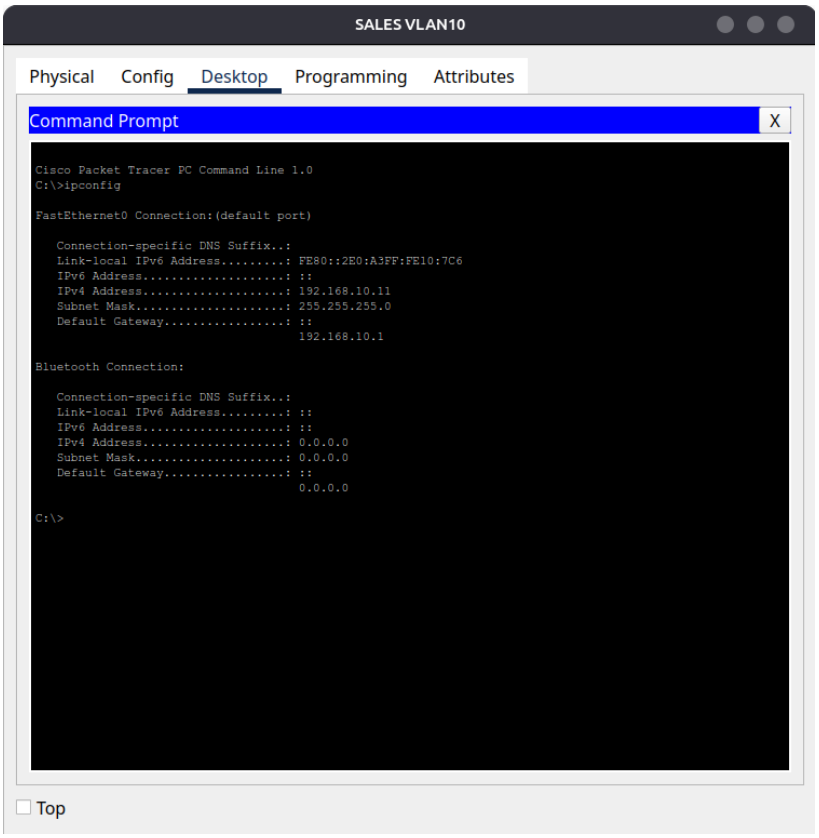
TMC-BR(dhcp-config)# default-router 192.168.40.1

Verification

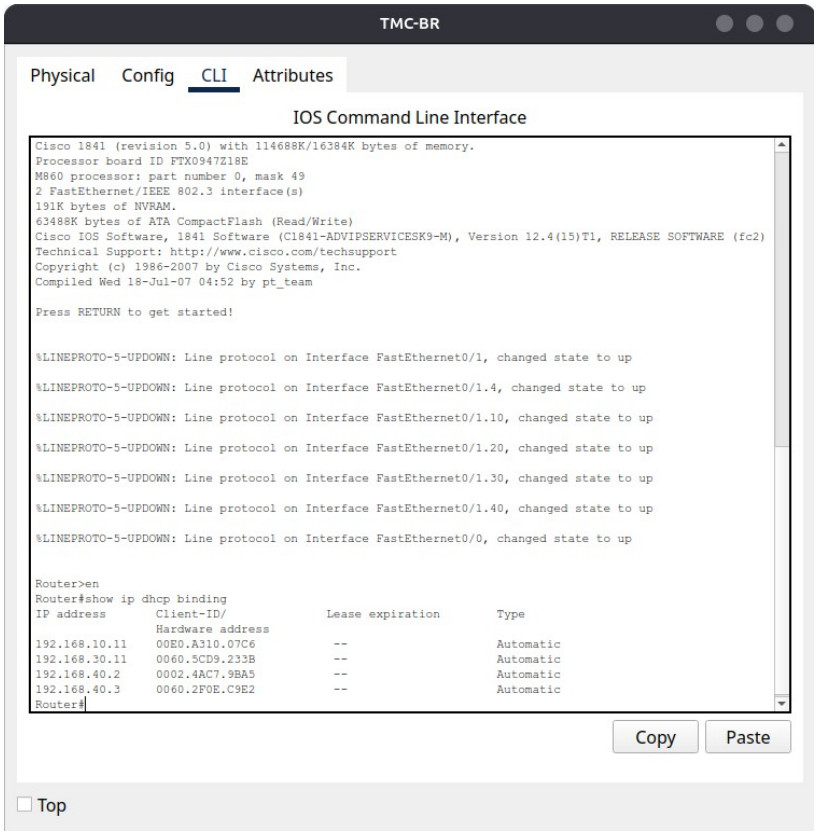
Clients on VLAN 10 and 30 successfully received addresses from the configured DHCP pools. Verified using both CLI and device configuration windows in Packet Tracer.



(Screenshot: **Figure 4** - *IT PC receiving IP address 192.168.30.11 from DHCP*)



(Screenshot: **Figure 5** - *SALES PC receiving IP address 192.168.10.11 from DHCP*)



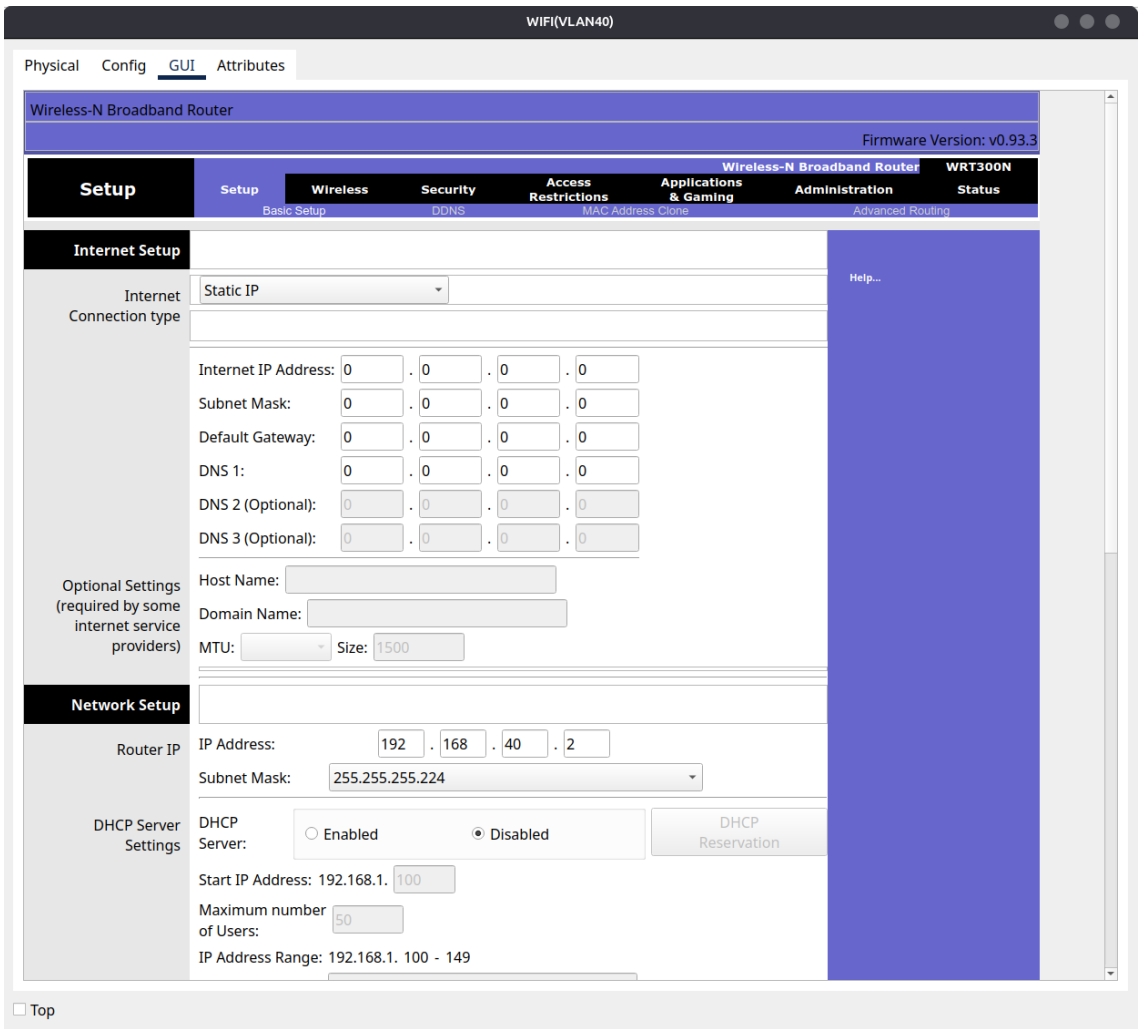
(Screenshot: **Figure 6** - *DHCP bindings showing dynamic addresses leased to clients on VLAN 10, 30, and 40*)

Wireless Access Point Configuration

To provide guest wireless connectivity on VLAN40 (Guest), the WRT300N was implemented in access point mode. DHCP services were disabled on the WRT300N, with all IP addressing handled centrally by the TMC-BR router.

WRT300N Basic Setup

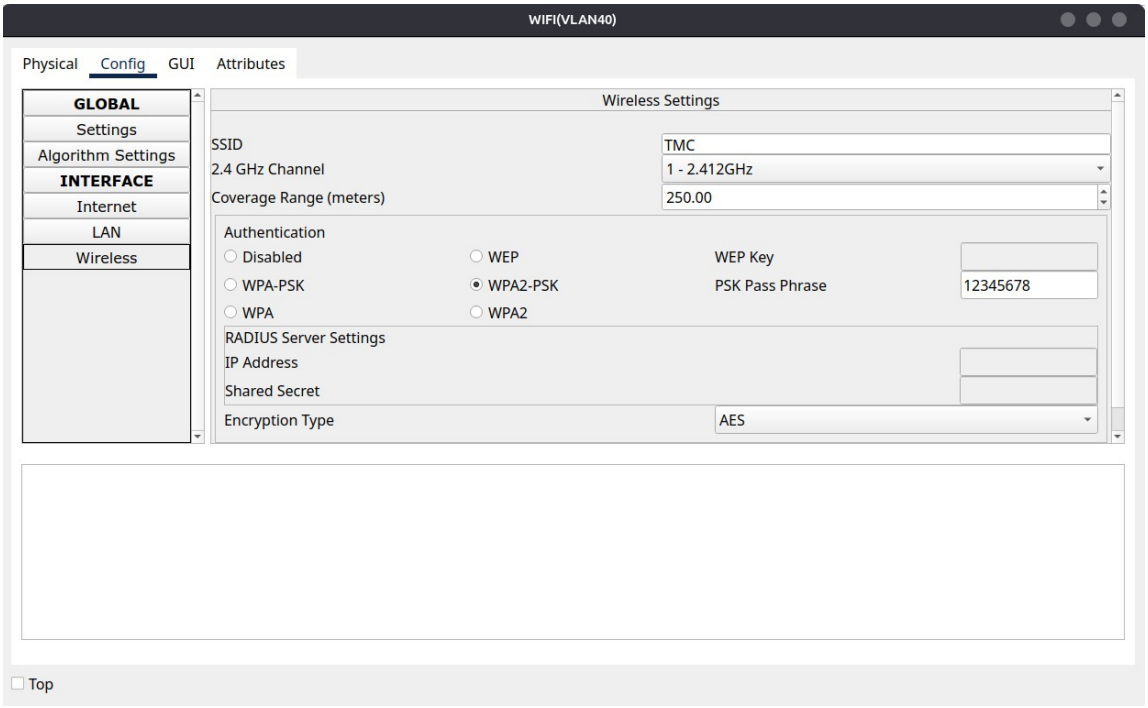
- **Router IP:** 192.168.40.2/24
- **DHCP Server:** Disabled
  - DHCP leases are provided by the TMC-BR router for consistency and centralised control



(Screenshot: **Figure 7** - *WRT300N Basic Setup with static IP 192.168.40.2 and DHCP disabled*)

Wireless Configuration

- **Network Name (SSID):** TMC
- **Security Mode:** WPA2-Personal
- **Encryption:** AES
- **Passphrase:** 12345678

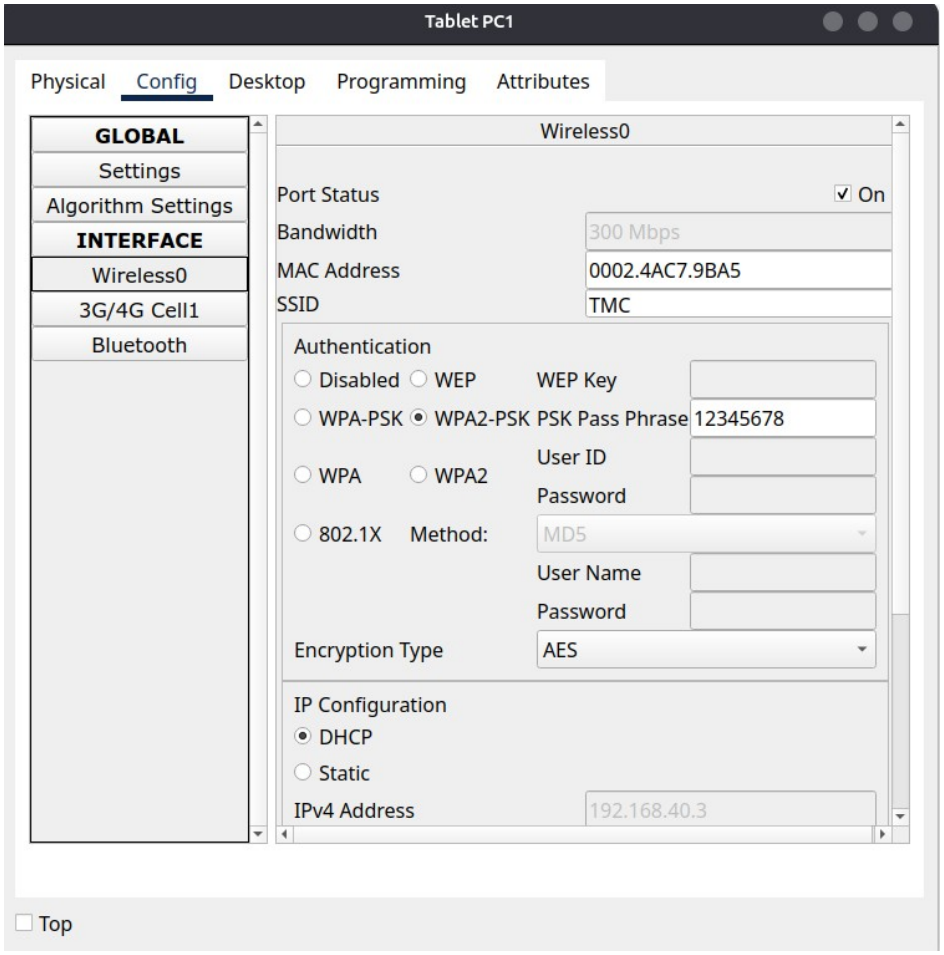


(Screenshot: **Figure 8** - *WRT300N Wireless setup with SSID "TMC" and security configuration showing WPA2-Personal with AES encryption*)

Wireless Client Configuration

The wireless end device was configured to connect to the SSID TMC using the WPA2 key.

- **Mode:** DHCP
- IP allocation via *TMC-BR router DHCP pool for VLAN40*



(Screenshot: **Figure 9** - *Wireless end device Wi-Fi settings connected to SSID TMC with WPA2 key and correct DHCP assigned IP address in the 192.168.40.x subnet*)

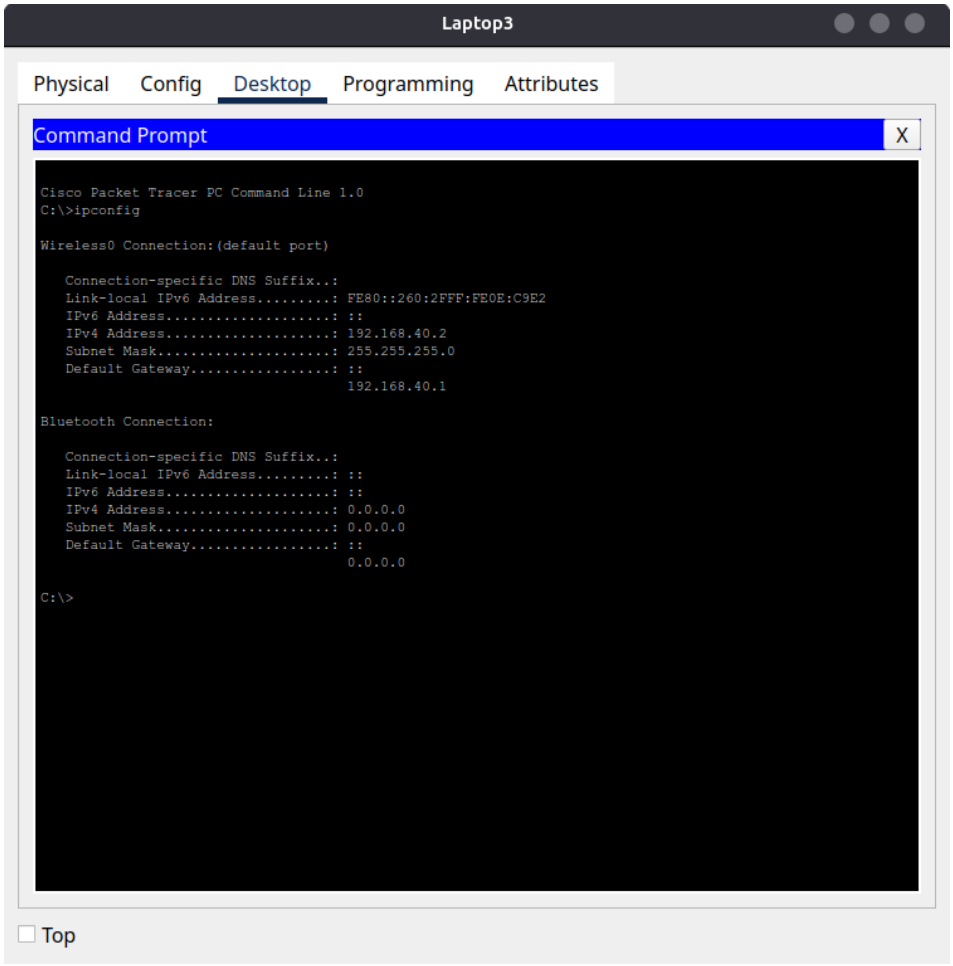
Verification & Troubleshooting

Connectivity was verified by:

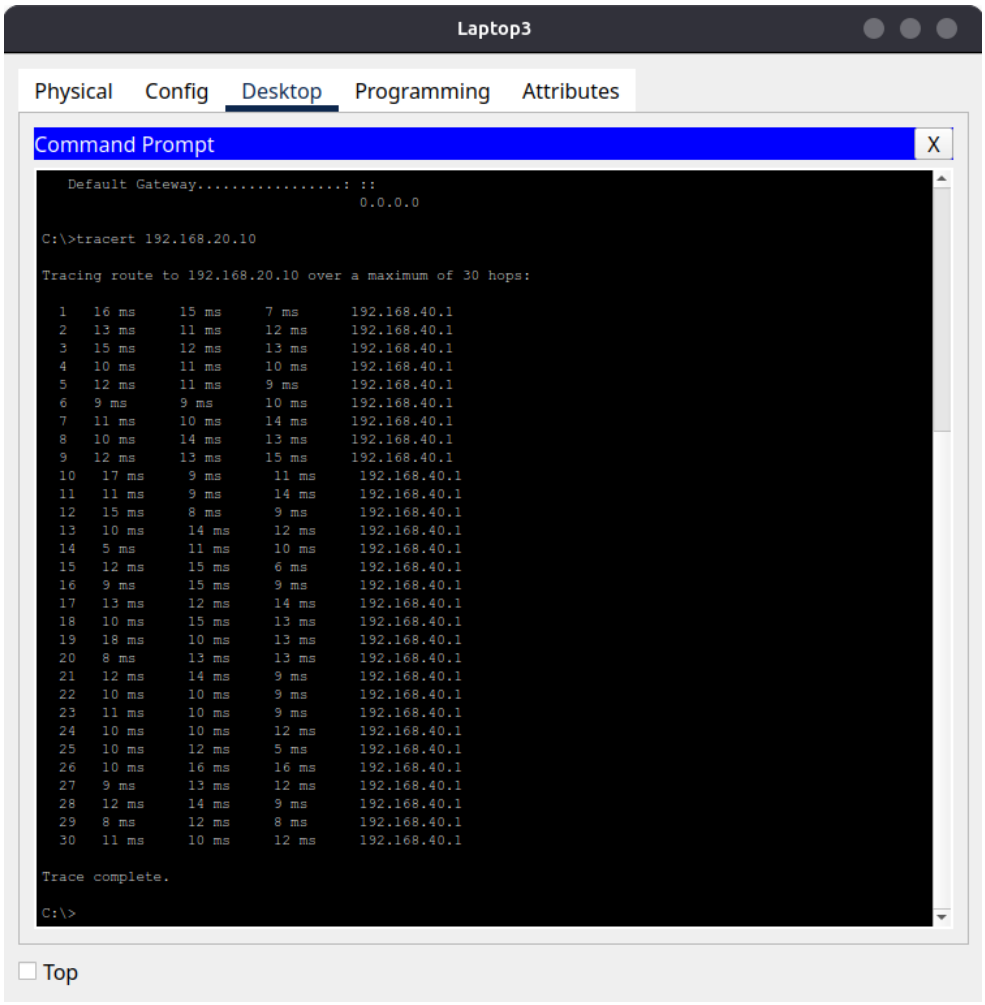
- Checking the client received an IP address from the router DHCP pool
- Running traceroute to devices in other VLANs

Expected results:

- Successful lease: 192.168.40.x with gateway 192.168.40.1
- Traceroute shows connectivity to the Server VLAN (192.168.20.x) and onward to DMZ/Internet



(Screenshot: **Figure 10** - *DHCP allocated IP shown on wireless end device*)



(Screenshot: **Figure 11** - *Traceroute output from guest client to Server VLAN*)

ACL Configuration

To enforce least-privilege access for the Guest VLAN (VLAN 40), an extended ACL (WIFI-RESTRICT) was configured on the router and applied inbound on the VLAN 40 subinterface (Fa0/1.40). The ACL ensures guests can only access services explicitly required for operation, while blocking sensitive internal resources.

Function and Operation

When a packet from 192.168.40.0/24 (Guest VLAN 40) enters the router on Fa0/1.40, the ACL inspects it against defined rules in order.

- **Permitted:**
  - DHCP (UDP ports 67/68) for address assignment
  - DNS queries (UDP/53) to the internal DNS server 192.168.20.10
  - HTTP traffic (TCP/80) to servers in VLAN 20 (192.168.20.0/24)
- **Denied:**
  - Any access from Guests to Sales (192.168.10.0/24)
  - Any access from Guests to IT (192.168.30.0/24)
  - Any non-HTTP traffic to VLAN 20 servers
- **Permitted:**
  - All other traffic (e.g. Internet/DMZ)

This order enforces business requirements while preventing Guests from reaching unauthorised internal resources.

Final ACL (WIFI-RESTRICT)

ip access-list extended WIFI-RESTRICT

DHCP for Guest VLAN clients

permit udp 192.168.40.0 0.0.0.255 any eq bootpc

permit udp any eq bootps 192.168.40.0 0.0.0.255

DNS to internal resolver

permit udp 192.168.40.0 0.0.0.255 host 192.168.20.10 eq domain

HTTP to Server VLAN (VLAN20) only

permit tcp 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 80

Deny Guest to other VLANs and services

deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255

deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255

deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255

Permit Guest to Internet/DMZ

permit ip 192.168.40.0 0.0.0.255 any

Applied inbound:

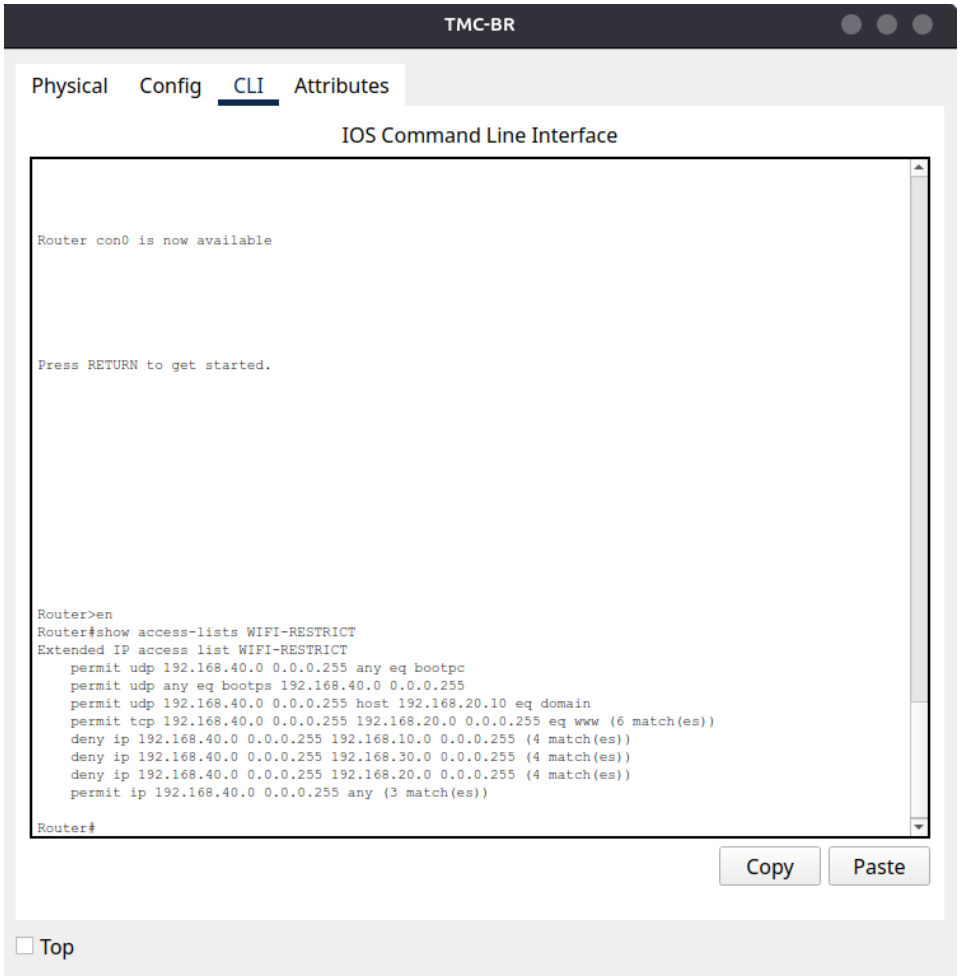
interface Fa0/1.40

ip access-group WIFI-RESTRICT in

Verification & Evidence

ACL Hit Counters

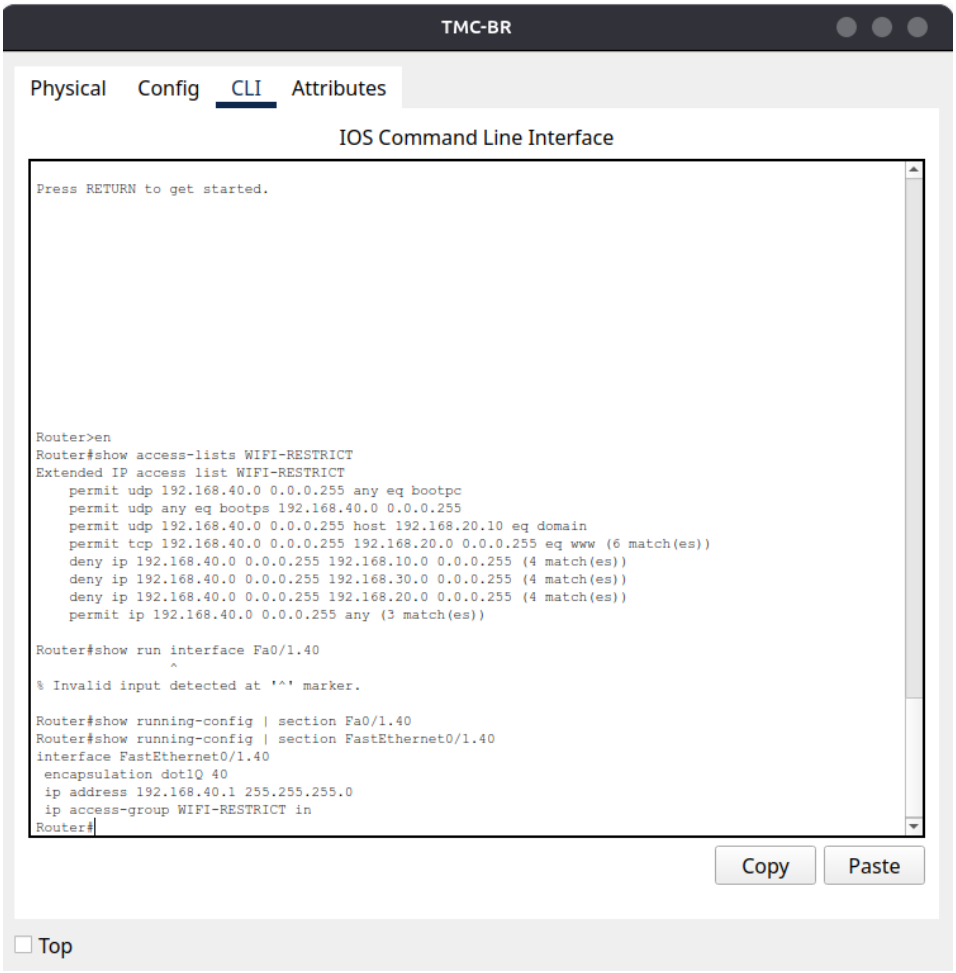
show access-lists WIFI-RESTRICT



(Screenshot: **Figure 12** - *ACL WIFI-RESTRICT with incrementing counters after test traffic*)

Interface Application

show running-config | section FastEthernet0/1.40



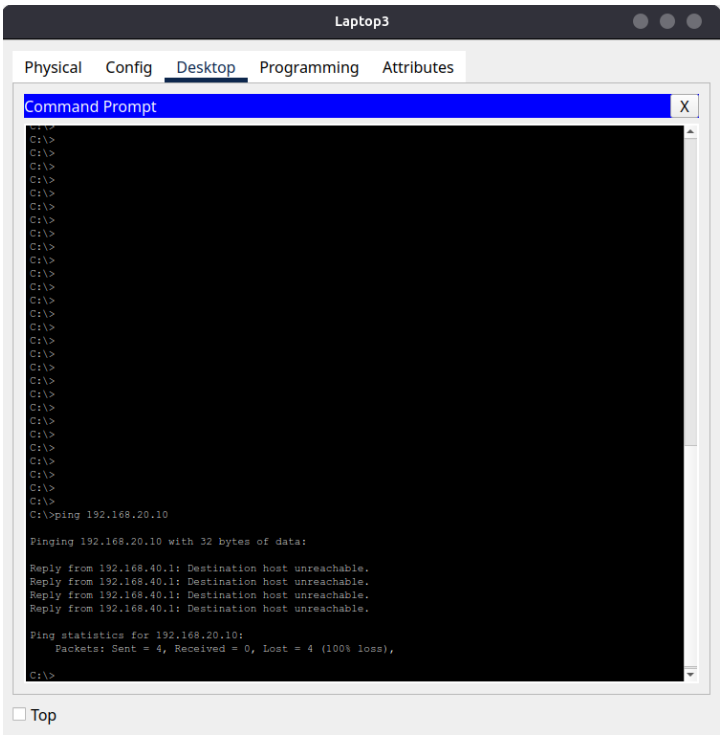
(Screenshot: **Figure 13** - *Fa0/1.40 with WIFI-RESTRICT applied inbound*)

Client Tests (Guest PC, VLAN 40)

http://192.168.20.10 = Success

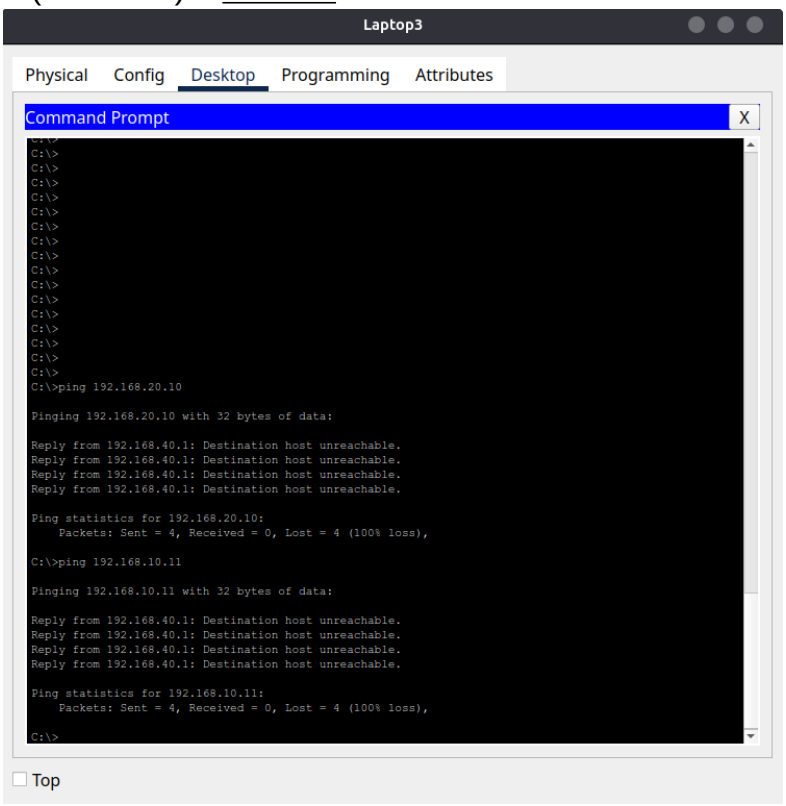
(Screenshot: **Figure 14.1** - *Guest client successfully accessing HTTP service on Server VLAN (192.168.20.10)*)

ping 192.168.20.10 = Blocked (non-HTTP not allowed)



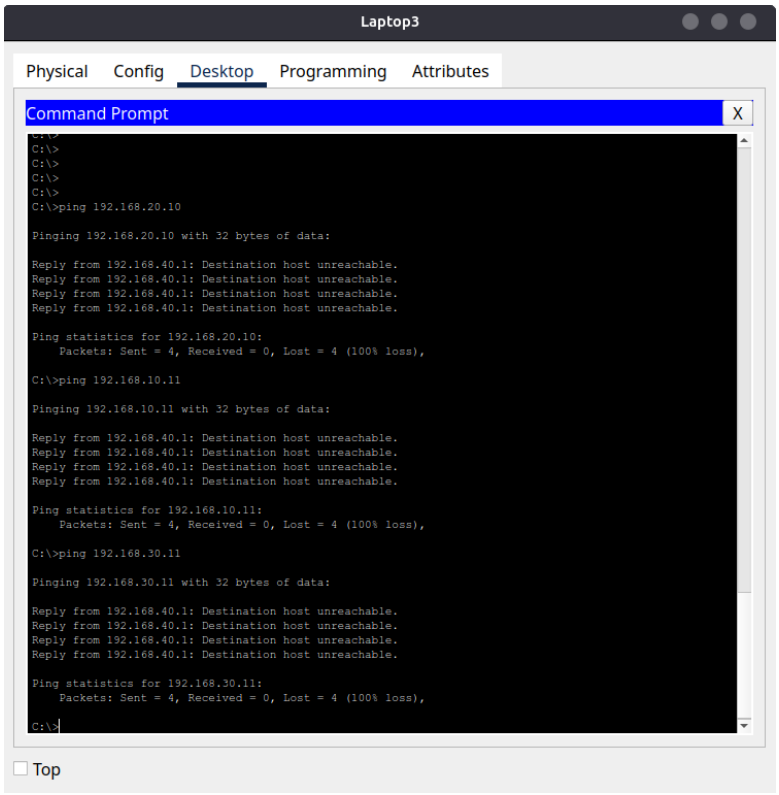
(Screenshot: **Figure 14.2** - *Guest client denied when attempting ICMP access to Server VLAN (192.168.20.10)*)

ping 192.168.10.11 (Sales PC) = Blocked



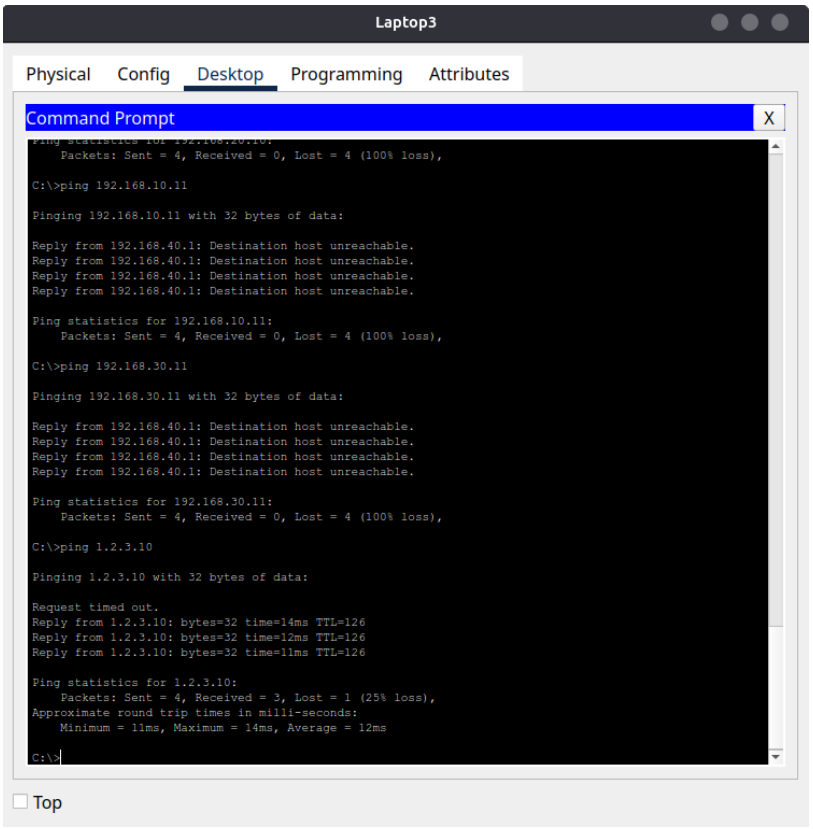
(Screenshot: **Figure 14.3** - *Guest client blocked from accessing Sales VLAN (192.168.10.11)*)

ping 192.168.30.11 (IT PC) = Blocked



(Screenshot: **Figure 14.4** - *Guest client blocked from accessing IT VLAN (192.168.30.11)*)

ping 1.2.3.10 (DMZ) = Success



(Screenshot: **Figure 14.5** - *Guest client permitted to access external/DMZ network resources*)

Final Validation & Results

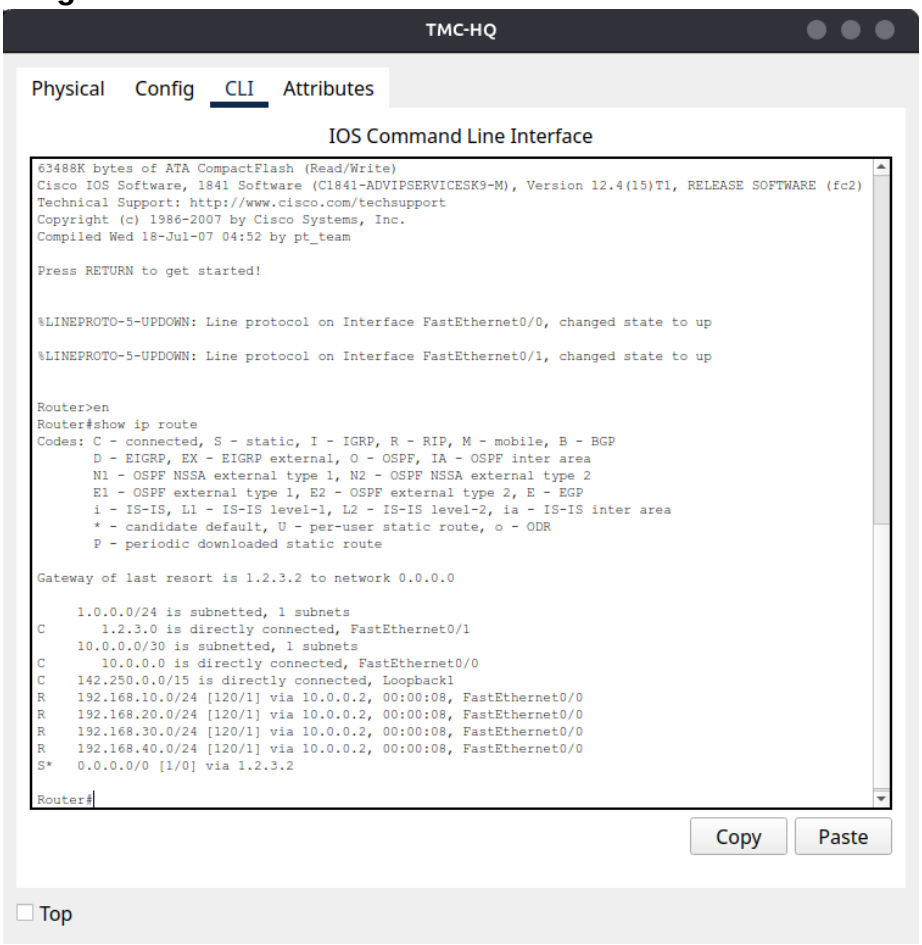
Routing Table Checks

The routing tables on TMC-BR and TMC-HQ confirm correct routing between VLANs and Internet/DMZ. Directly connected to networks appear with a *C* code, while routes learned from the RIP protocol are marked with *R*. The default route *(0.0.0.0/0)* is learned from TMC-HQ, ensuring Guest VLAN traffic can reach the DMZ/Internet.

TMC-BR Routing Table

(Screenshot: **Figure 15** - *TMC-BR routing table showing connected VLANs and RIP learned default route*)

TMC-HQ Routing Table



(Screenshot: **Figure 16** - *TMC-HQ routing table showing directly connected Internet/DMZ and RIP learned VLAN networks*)

Traceroute / Ping Tests

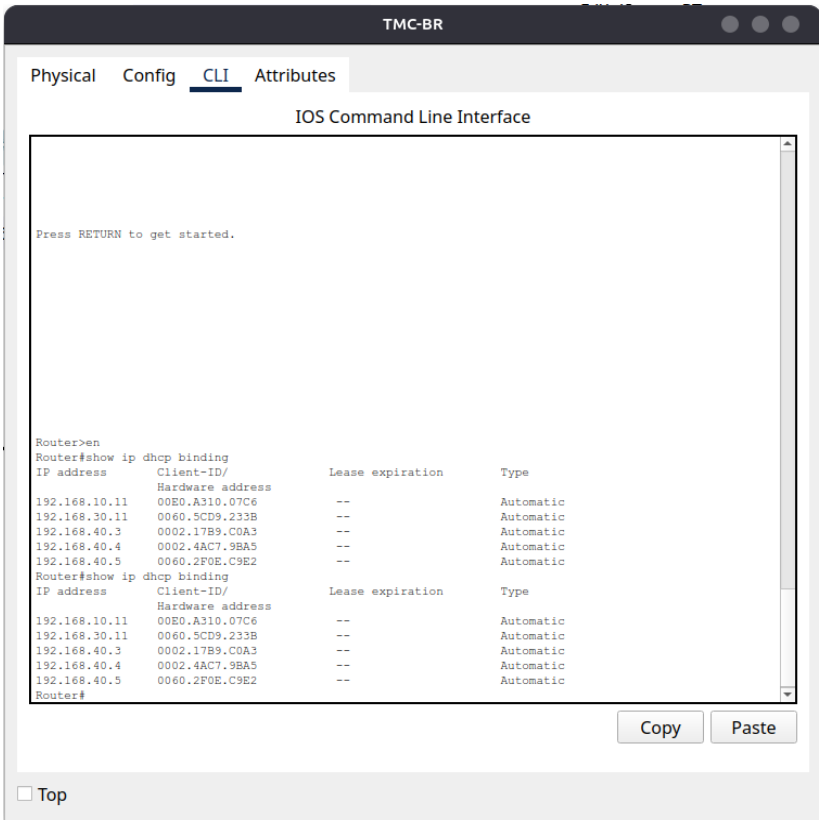
Connectivity from the Guest VLAN was already verified in the ACL configuration section. Tests confirmed that HTTP access to the Server VLAN was allowed, while ICMP and other services were blocked. Guest traffic to Sales and IT VLANs were denied, while DMZ/Internet access succeeded as expected. (See Figures 14-14.5).

(Screenshot: **Figure 17** - *Guest client successfully accessing HTTP service on DMZ/Internet*)

DHCP Bindings Proof

To confirm correct IP allocation across VLANs, the DHCP bindings were verified on the TMC-BR router. Each DHCP pool (Sales, IT, Guest) assigned IP addresses to clients, while the Server VLAN used static addressing as intended. This demonstrates that DHCP configuration is functioning as expected and VLAN clients are receiving valid addresses, gateways, and DNS settings.

Command Output



(Screenshot: **Figure 18** - *DHCP bindings showing dynamic allocations for Sales (192.168.10.x, IT (192.168.30.x), and Guest (192.168.40.x) clients*)

Interpretation

This confirms that:

- Each VLAN receives addresses only from its designated DHCP pool
- Server VLAN (192.168.20.0/24) is excluded from the DHCP and uses static assignment (192.168.20.10 for the internal DNS/web server)
- No address overlap occurs between VLANs
- The Guest VLAN is correctly integrated with DHCP after ACL restriction

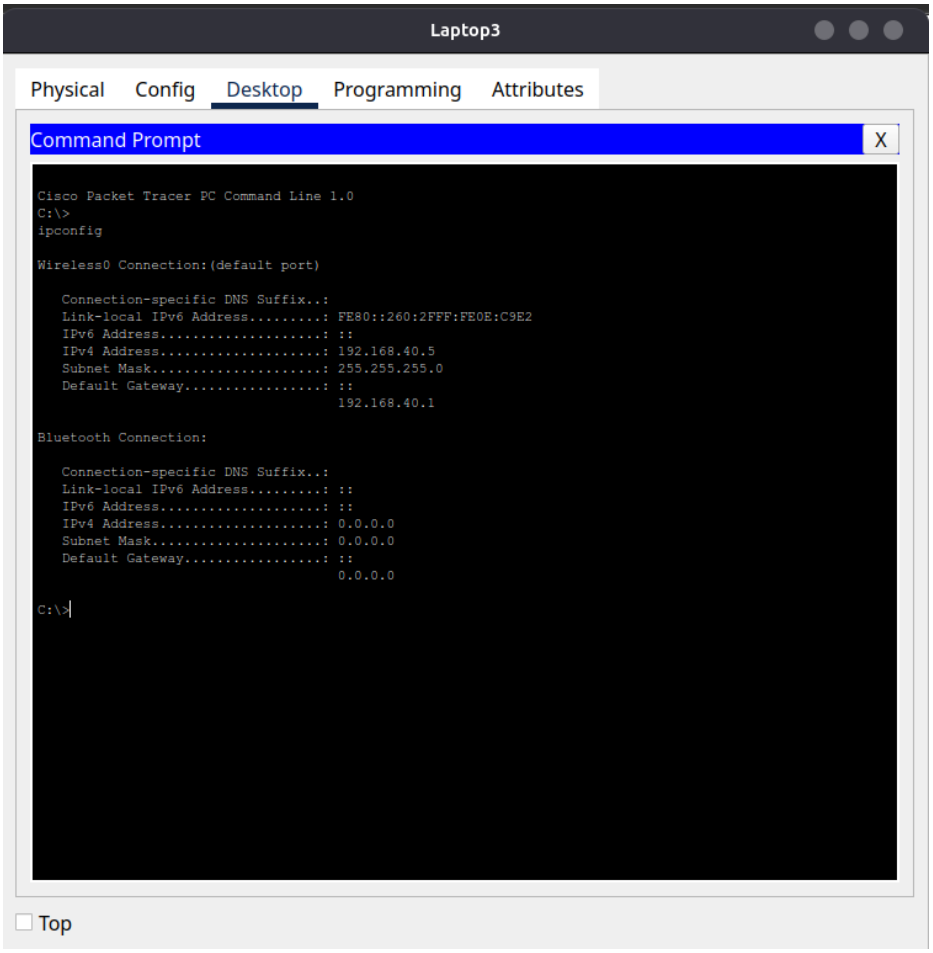
Wireless Client Test

To validate DHCP functionality and ACL restrictions from the perspective of a guest client, a laptop and tablet were connected to VLAN 40 (Wi-Fi/Guest VLAN). This will focus on one of the connected devices, Laptop 3.

DHCP Assignment

The client was configured to obtain its address dynamically via DHCP. It successfully received:

- IP Address: 192.168.40.5
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.40.1

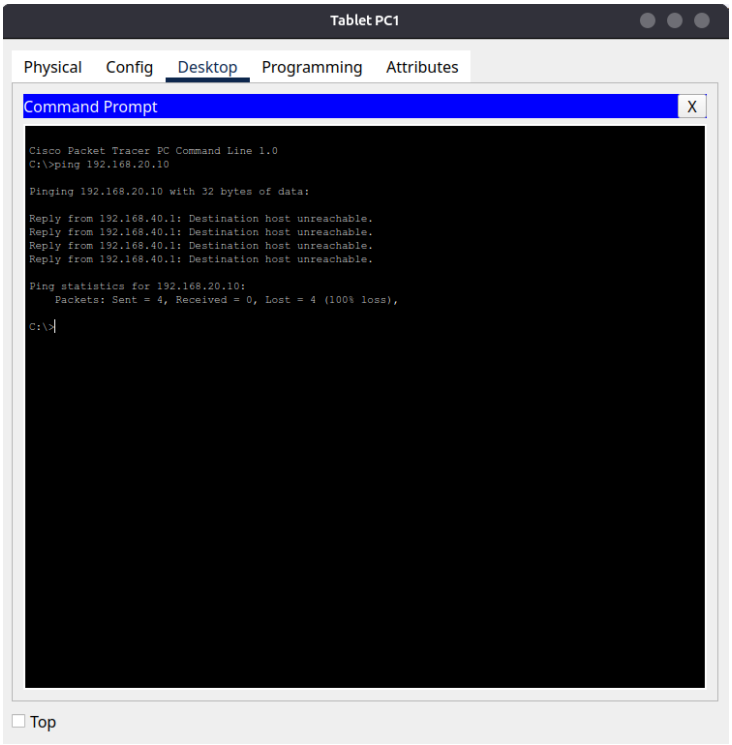


(Screenshot: **Figure 19** - *Guest client IP configuration showing DHCP assignment from VLAN 40*)

ACL Enforcement Tests

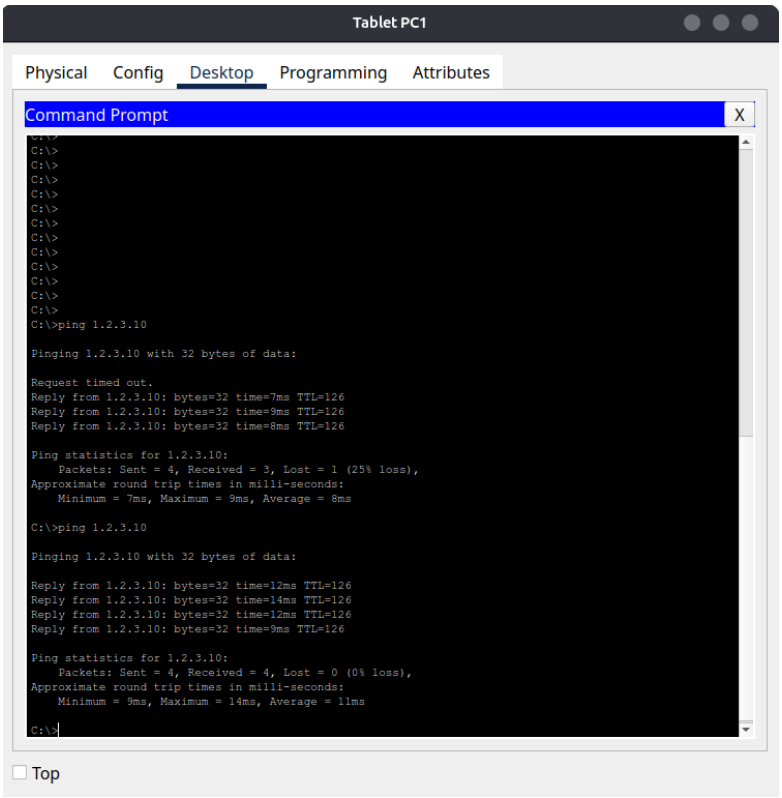
The following tests were conducted from the guest client (Tablet PC1):

- *ping 192.168.20.10* = Blocked (ICMP not permitted by ACL)
- *http://192.168.20.10* (web browser) = Allowed (HTTP explicitly permitted)
- *ping 1.2.3.10* (DMZ/Internet simulation) = Allowed



(Screenshot: **Figure 20.1** - *Blocked ping to 192.168.20.10 (Server VLAN)*)

(Screenshot: **Figure 20.2** - *Successful HTTP access to 192.168.20.10 via browser*)



(Screenshot: **Figure 20.3** - *Successful ping to 1.2.3.10 (DMZ/Internet*)

Professional Notes

Troubleshooting Challenges

During the implementation of this lab, several issues arose that required careful troubleshooting:

- **DHCP Lease Issues** - Guest clients on VLAN 40 initially failed to obtain addresses. This was traced to ACL rules blocking DHCP broadcast from 0.0.0.0 to 255.255.255.255. Rebuilding the ACL with DHCP permit rules at the top resolved the problem.
- **VLAN Membership Confusion** - At one stage, VLAN 40 did not appear in the DHCP bindings because end devices were incorrectly assigned to VLAN 1. Verifying with *show vlan brief* ensured devices were placed in the correct VLAN.
- **ACL Ordering** - Misconfigured access-lists (multiple overlapping ACLs applied to the same subinterface) led to conflicts. This was corrected by removing unused ACLs and ensuring only the final *WIFI-RESTRICT* ACL was bound to VLAN 40.

Lessons Learned

- Always check DHCP broadcast traffic when ACLs are applied, as it's easy to block unintentionally.
- Confirm VLAN assignments at the switchport level with *show interfaces switchport*.
- Sequence ACL rules carefully. Critical rules (DHCP, DNS) must appear first.
- Use simulation mode in Packet Tracer to watch the full DHCP -> OFFER -> REQUEST -> ACK handshake, it's an invaluable diagnostic tool.
- Denying VLAN 20 after the HTTP/DNS permit ensures Guests cannot exploit other services.
- This approach demonstrates network segmentation and least privilege enforcement, key principles in secure design.

Future Improvements

While this lab demonstrates successful inter-VLAN routing, DHCP assignment, and ACL enforcement, several enhancements could make the network design more realistic and enterprise ready:

- Dynamic Routing Upgrade - Replace RIP v2 with OSPF, which is more scalable and commonly used in modern enterprise environments.
- Wi-Fi Security - Implement WPA2-Enterprise with a RADIUS server for authentication, instead of WPA2-Personal, to better simulate corporate Wi-Fi security.

- High Availability - Add redundancy through protocols such as HSRP or VRRP, ensuring continuous gateway availability if one router fails.
- Firewall Logging - Enable logging on ACL deny statements to capture unauthorised access attempts, improving monitoring and auditing.
- Centralised DNS/DHCP Services - Move DHCP and DNS roles to a dedicated server for more realistic enterprise deployment.
- Monitoring & Alerts - Integrate SNMP or Syslog for proactive device and network health monitoring.

Conclusion

This lab demonstrated secure segmentation of an enterprise LAN using VLANs, DHCP, ACLs, and wireless integration. Final validation confirmed DHCP reliability, enforced ACL restrictions, and successful Guest Wi-Fi access to permitted resources while bloacking sensitive VLANs. The project highlights my ability to design, configure, troubleshoot, and document enterprise style networks, skills that are directly applicable to IT support and junior network/security roles.

References

- Cisco Systems. *Configuring DHCP on Cisco Routers.* Cisco IOS Documentation. https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
- Navin Reddy. *Configuring RIP (Routing Information Protocol) Packet Tracer | BScIT MCA Practical*. https://www.youtube.com/watch?v=krM9GprN6qA
- GeeksforGeeks (2023). *VLAN ACL (VACL)*. https://www.geeksforgeeks.org/vlan-acl-vacl/
- Firewall.cx (2025). *How To Configure Router-on-a-Stick - 802.1q Trunk to Cisco Router*. https://www.firewall.cx/cisco/cisco-routers/cisco-router-8021q-router-stick.html