AIMS AND OBJECTIVES.

To design and implement a fully functional network in Cisco Packet Tracer incorporating routers, switches, VLANs, DHCP, NAT, and wireless access points. The network aims to provide secure, scalable, and seamless communication across wired and wireless clients, with proper segmentation, dynamic IP allocation, internet access, and wireless optimization.

RESOURCES USED.

.Cisco packet tracer(software)

- 5 pcs
- 3 laptops
- 4 access points
- 2 switch
- 3 routers
- 1 IP phone
- Server

STEPS FOLLOWED.

1. **Network Layout Design**:
    - Developed a structure with a router connected to two switches and a wireless access point.
    - Subnets were assigned based on departmental separation.
2. **Router Configuration**:
    - Interfaces were assigned appropriate IP addresses.
    - Routing was activated to support communication between VLANs.
    - NAT was configured to allow internal hosts to access external networks.
3. **Switch Setup**:
    - VLANs were created and associated with different departments.
    - Trunk ports were set to carry multiple VLANs between devices.
4. **DHCP and IP Assignment**:
    - The server was configured with DHCP pools.
    - IP ranges were defined to match each VLAN's subnet.
5. **Wireless Access Configuration:**
    - SSIDs were created for different user groups.
    - Wireless security settings and VLAN tagging were applied.
    - Roaming functionality was tested by moving devices between WAP zones
6. **SOHO Configuration:**
    - Simulated a basic SOHO setup with firewall and VPN support.
    - Enabled MAC filtering and wireless encryption for added security.
7. **Testing and Validation:**
    - Devices were tested for IP allocation, connectivity across VLANs, internet access, and wireless performance.

Theory

This project integrates core and advanced networking concepts essential for establishing secure, efficient, and scalable enterprise and SOHO (Small Office/Home Office) networks. Each configured element plays a critical role in ensuring reliable data transmission and network control.

- **VLANs (Virtual Local Area Networks)**

VLANs divide a physical network into multiple logical segments, creating distinct broadcast domains. This improves network organization, performance, and security by isolating traffic based on functions or departments (e.g., Admin, Guest, Staff). Devices within the same VLAN can communicate as if connected to the same switch, even when they are physically dispersed. This also minimizes broadcast traffic and enables the implementation of tailored network policies.

- **Inter-VLAN Routing**

Since VLANs are isolated by nature, communication between them requires a Layer 3 device. This setup uses the router-on-a-stick method, where a single router interface is divided into multiple sub-interfaces, each handling traffic for a specific VLAN. This allows secure communication across VLANs. The ip routing command activates Layer 3 functionality on the router to support this process.

- **DHCP (Dynamic Host Configuration Protocol)**

DHCP simplifies IP address management by dynamically assigning IP addresses, subnet masks, default gateways, and DNS server information to devices. This reduces manual errors and enhances scalability. Separate DHCP pools are created for each VLAN/subnet to ensure clients in different departments get addresses from the correct range. DHCP options like lease duration and reservations help ensure consistent connectivity for critical systems.

- **NAT (Network Address Translation)**

NAT allows internal private IP addresses to be translated into a single or a few public IPs, facilitating internet access for multiple internal devices. This setup uses PAT (Port Address Translation), which maps many internal addresses to one public IP using unique port numbers. PAT enhances security and conserves IPv4 address space by masking internal addresses from the public internet.

- **SSIDs and Wireless VLAN Association**

Different SSIDs (e.g., Admin_WiFi, Guest_WiFi) are configured to separate wireless user groups. Each SSID is linked to a specific VLAN, ensuring that wireless traffic is logically segmented just like wired traffic. VLAN tagging on access points and switch trunk ports ensures that traffic is correctly identified and routed.

- **Roaming and Wireless Optimization**

Wireless roaming allows users to move between access point zones without losing connectivity. Access point power levels, channels, and overlapping coverage were optimized to ensure smooth handoffs and consistent signal strength. This is vital in environments where users frequently move across rooms or floors.

- **DNS (Domain Name System)**

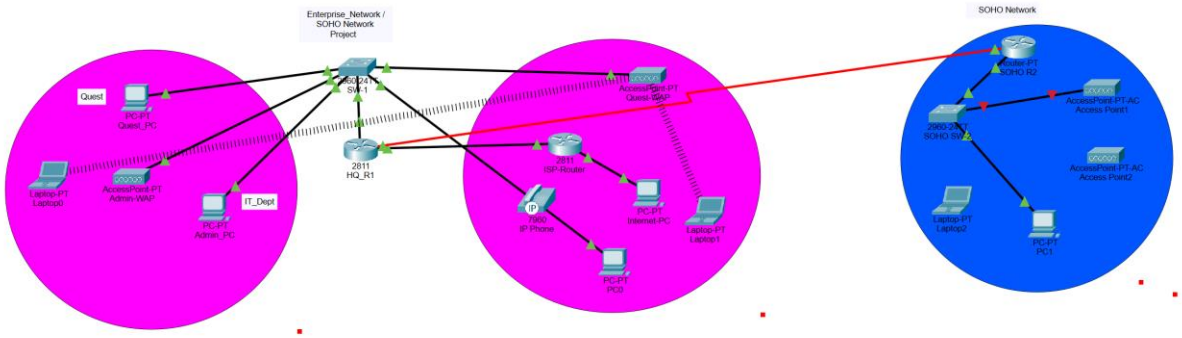
DNS servers resolve domain names into IP addresses, allowing users to access resources using human-friendly names instead of numeric IPs. In this project, the DNS service is hosted internally, and client devices are configured via DHCP to use it. This speeds up access to internal and external resources while simplifying navigation.

- **SOHO Network Design Aspects**

SOHO networks focus on ease of deployment and cost-effective security. Basic firewall configurations were used to block unauthorized traffic. Wireless encryption (WPA2) and MAC filtering were implemented to prevent unauthorized Wi-Fi access. Additionally, a VPN simulation demonstrated secure remote access, which is essential for businesses supporting remote workers.

RESULTS AND DISCUSSION.

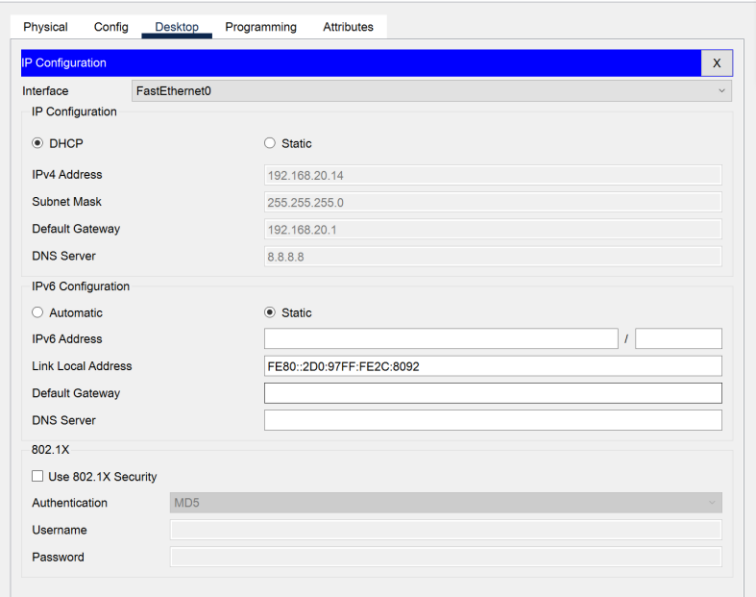
Finally, we have combined all the steps as mentioned in steps followed and implemented a fully functional SOHO network. We have the complete network that enables secure, organized, and seamless communication across different departments and user type**s** both wired and wireless while also allowing access to external services like the internet.



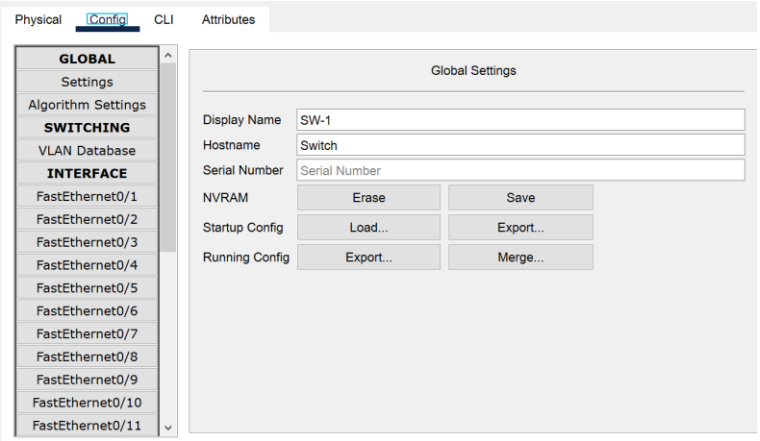
The complete diagram of the SOHO network created in packet tracer environment.

- **Configuring IP Addresses**

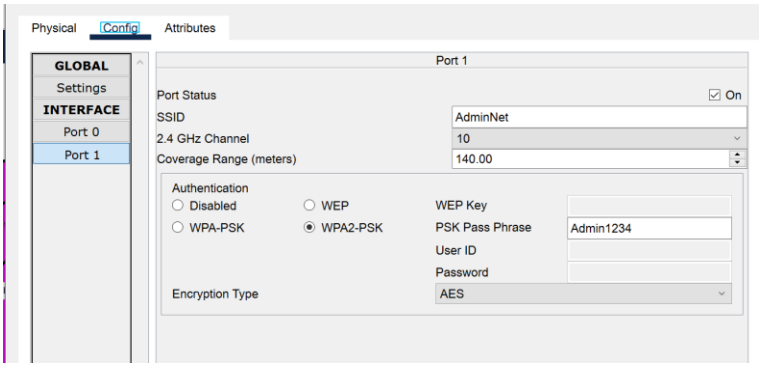
We have attached the screenshots of all the IP configuration below:



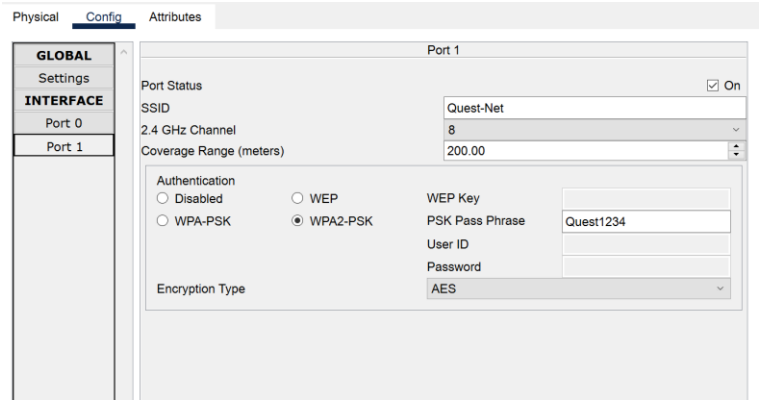
PC-PT configuration



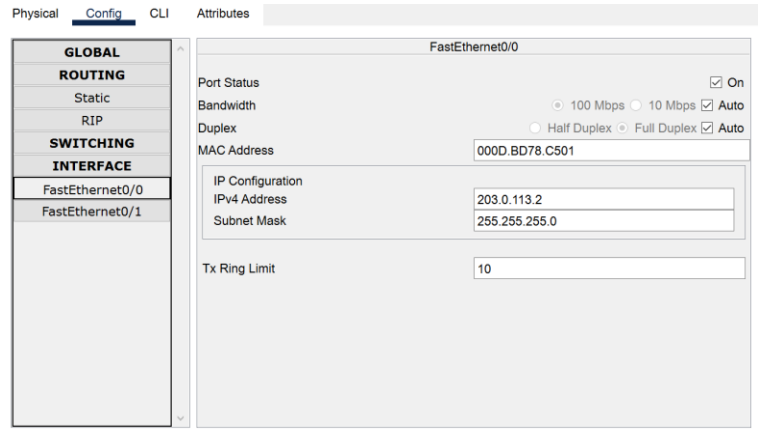
Main switch configuration



Access point admin-WAP configuration



Access point Quest-WAP Configuration



ISP Router configuration

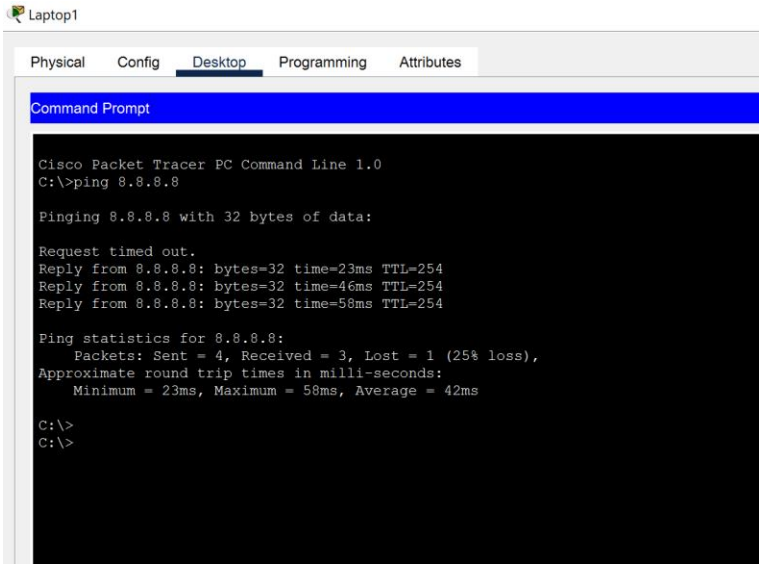
```
C:\>nslookup www.example.com

Server: [8.8.8.8]
Address:  8.8.8.8
DNS request timed out.
            timeout was 15000 milli seconds.
DNS request timed out.
            timeout was 15000 milli seconds.
```

DNS CONFIGURATION

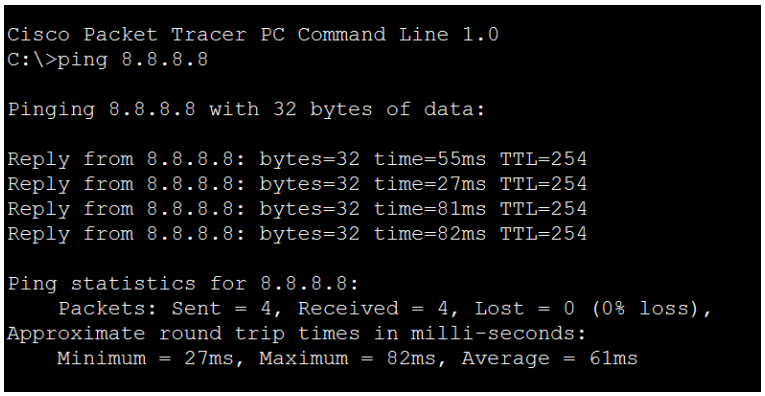
- **<u>Final Simulation</u>**

In Simulation Mode, you can watch your network run at a slower pace, observing the paths that packets take and inspecting them in detail. The proposed architecture, when simulated on Cisco Packet Tracer, produced results which are demonstrated as follows:

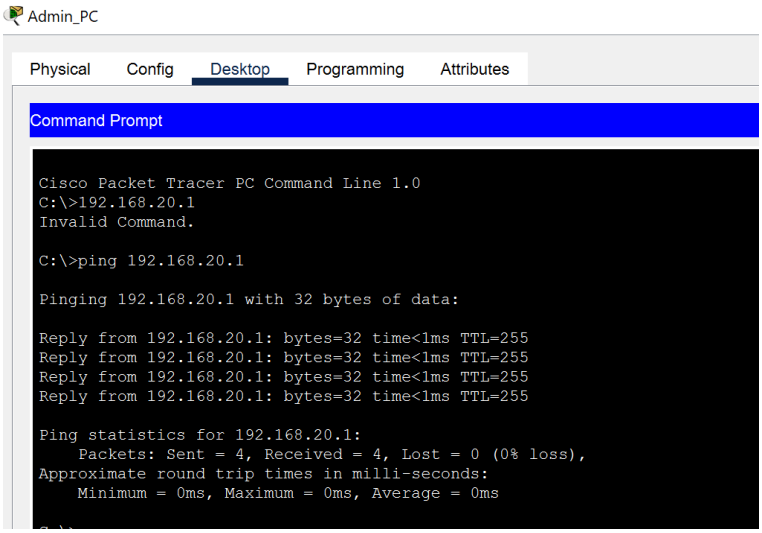
Ping Test: Network connectivity and communication can be tested using the ping command, followed by the domain name or the IP address of the device (equipment) whose connectivity one wishes to verify.



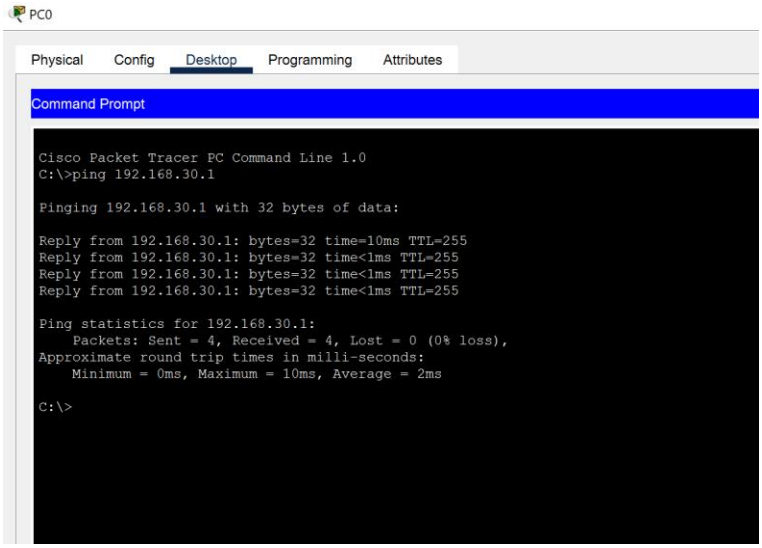
Ping test for laptop 1 to the internet



Subsequent ping test for laptop 1 to the internet



Ping tests for 2 PCs (different VLAN)



Ping test for pc to router

DISCUSSION

Ping tests were conducted between various devices to verify IP connectivity, VLAN configuration, inter-VLAN routing, DHCP functionality, and NAT-enabled internet access.

Pinging between PCs within the same VLAN returned successful replies, indicating that local connectivity was properly established. PCs in different VLANs were also able to communicate, confirming that inter-VLAN routing on the router was correctly configured

All PCs were able to ping their respective default gateway interfaces on the router, such as 192.168.10.1 and 192.168.20.1. This confirmed that the router interfaces were up and correctly configured.

Initial pings to external addresses such as 8.8.8.8 showed 25% packet loss. This was expected due to the NAT table initializing and the simulation environment processing delays. Subsequent pings returned with 0% loss, confirming stable connectivity.

Sources of Errors

Challenge Faced	***Action Taken***
VLANs not communicating	Enabled routing and verified trunk settings
DHCP not leasing IPs	Rechecked pool bindings and interface settings
Internet not reachable	Corrected NAT access-list and interface configuration
Wireless clients isolated	Mapped SSIDs to VLANs and confirmed trunk mode
DNS issues	Assigned static IP and enabled DNS services on server

Recommendations

- Document Configurations: Keep a record of all setup steps and commands used.
- Security Enhancements: Upgrade to stronger wireless security protocols like WPA3 if available.
- Monitor Network Health: Incorporate monitoring tools to catch issues early.
- Prepare for Growth: Plan for additional VLANs or users in advance to maintain scalability.
- Routine Backups: Save configuration files regularly to prevent data loss.

Conclusion

The project successfully achieved a structured, secure, and scalable network setup within a simulated environment. Through clear planning and proper implementation of essential networking protocols, a reliable infrastructure was created to support departmental segmentation, dynamic addressing, internet connectivity, and wireless access. The network is now fully operational and well-aligned with real-world standards expected in both enterprise and small office setups.