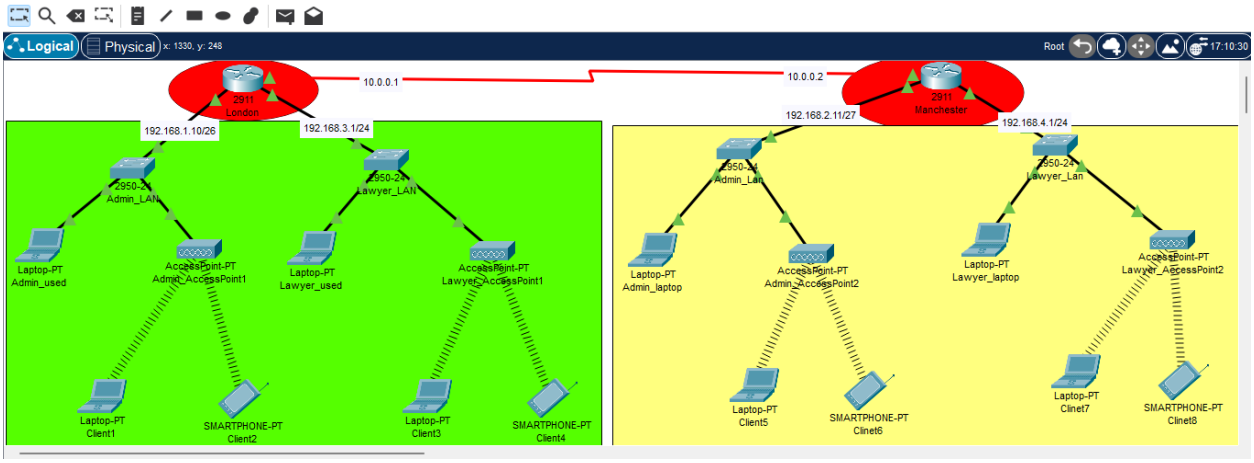
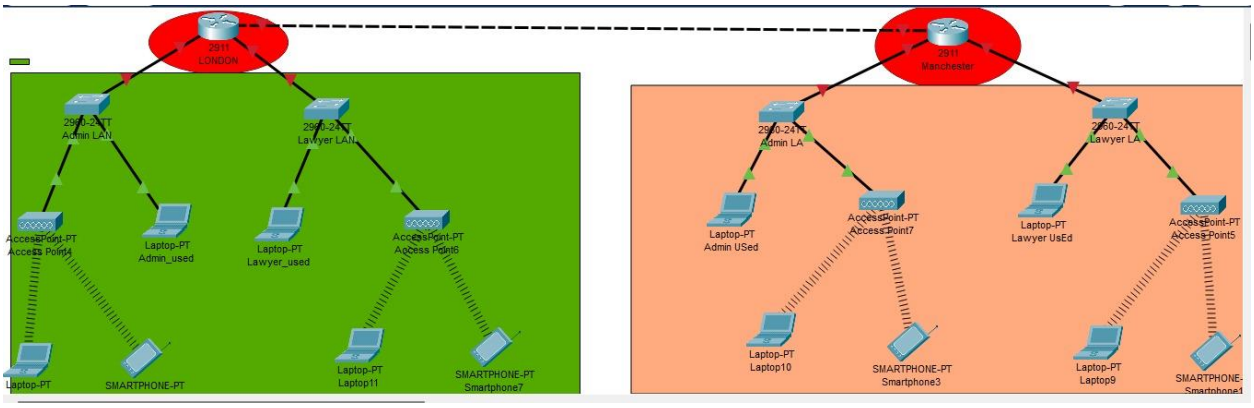
Network Topology



Task 1a- Network Design and Physical Prototype in Packet Tracer:

initial design:



Rationale and Justification for Equipment Choices:

Routers:

Type: Cisco 2911 Router.

Justification: The Cisco 2911 Router is a reliable and widely used model known for its robustness and versatility. It offers advanced security features such as firewall, VPN, and intrusion prevention, which are essential for protecting sensitive legal data. Additionally, the 2911 router provides sufficient performance and scalability to support the interconnection of subnets between the London and Manchester offices.

Switches:

Type: Cisco Catalyst 2960-24 Switch.

Justification: The Cisco Catalyst 2960-24 Switch is a reliable and cost-effective choice for small to medium-sized businesses like AP Finance. It provides 24 Ethernet ports, which are suitable for connecting the various devices within each office, including computers, printers, and VoIP phones. The 2960-24 switch also supports VLANs, allowing for efficient network segmentation and management.

Access Points:

Type: Cisco Aironet Access Point.

Justification: Cisco Aironet Access Points are known for their high performance, reliability, and security features. They offer fast wireless connectivity and support for multiple SSIDs, allowing for separate networks for staff and guest users. This helps ensure network security and efficiency by segregating traffic and providing appropriate access controls. Additionally, Cisco Aironet Access Points are easy to deploy and manage, making them a suitable choice for AP Finance's network infrastructure needs.

Factors:

Routers:

Cisco 2911 Router:

Performance: The Cisco 2911 Router offers high-performance routing capabilities, ensuring fast and reliable interoffice communication.

Scalability: With support for various interface types and expansion modules, the 2911 router can scale to accommodate future growth in network traffic and connectivity requirements.

Features: It comes with advanced security features such as firewall, VPN, and intrusion prevention, ensuring the confidentiality, integrity, and availability of data transmitted across the network.

Switches:

Cisco Catalyst 2960-24 Switch:

Performance: The Catalyst 2960-24 Switch delivers high-performance Ethernet connectivity, ensuring low latency and high throughput for network traffic.

Scalability: With 24 Ethernet ports, the switch provides scalability to accommodate additional devices and users as the law firm grows.

Features: It supports VLAN segmentation, enabling efficient traffic management and enhanced security by isolating different types of network traffic. Additionally, features like Quality of Service (QoS) ensure prioritization of critical traffic.

Access Points:

Cisco Aironet Access Point:

Performance: Cisco Aironet Access Points offer high-speed wireless connectivity, ensuring fast and reliable Wi-Fi access for staff and clients.

Scalability: With support for multiple SSIDs and high client capacity, these access points can scale to accommodate a large number of wireless devices while maintaining performance.

Features: They come with advanced security features such as WPA3 encryption and rogue access point detection, ensuring the security of wireless communications. Additionally, features like band steering and airtime fairness optimize the use of wireless spectrum and improve overall network performance.

Task 1b-Choice of WAN Technology and Bandwidth:

Bandwidth Requirement for WAN Connection:

For LC Solicitors' needs, a dedicated symmetrical bandwidth of 100 Mbps for the WAN connection would be ideal. This ensures fast and reliable communication between the London and Manchester offices, supporting efficient file sharing and resource accessibility.

This bandwidth allocation ensures sufficient capacity to support simultaneous communication, file transfers, and access to centralized resources between the two offices without experiencing congestion or performance degradation. Additionally, a symmetrical connection with equal upload and download speeds is preferred to ensure balanced traffic flow and consistent performance for both office locations.

Investigate WAN Choices pros and cons:

MPLS (Multiprotocol Label Switching):

Pros:

Reliability: MPLS networks offer high reliability and uptime, ensuring consistent connectivity between offices.

Security: MPLS provides inherent security features, making it suitable for transmitting sensitive legal data.

Quality of Service (QoS): MPLS supports QoS mechanisms, allowing prioritization of critical applications.

Cons:

Cost: MPLS connections can be expensive, particularly for smaller organizations.

Complexity: MPLS implementation and management require specialized expertise.

LC Solicitors' Needs

MPLS offers high reliability, security, and QoS, aligning well with LC Solicitors' need for secure and efficient connectivity between offices.

Leased Lines:

Pros:

Dedicated Bandwidth: Leased lines provide dedicated, symmetrical bandwidth, ensuring consistent performance.

Reliability: Leased lines offer high reliability and uptime, backed by SLAs.

Security: Leased lines operate on private connections, providing inherent security.

Cons:

Cost: Leased lines can be costly, particularly for higher bandwidth options.

Scalability: Upgrading leased lines may involve additional costs and lead times.

LC Solicitors' Needs:

Leased lines offer reliability, security, and dedicated bandwidth, making them suitable for LC Solicitors' requirements.

Broadband Connections:

Pros:

Cost-Effective: Broadband connections are more affordable than MPLS or leased lines.

Availability: Broadband connections are widely available and easy to provide.

Cons:

Performance: Variability: Broadband connections may experience performance fluctuations.

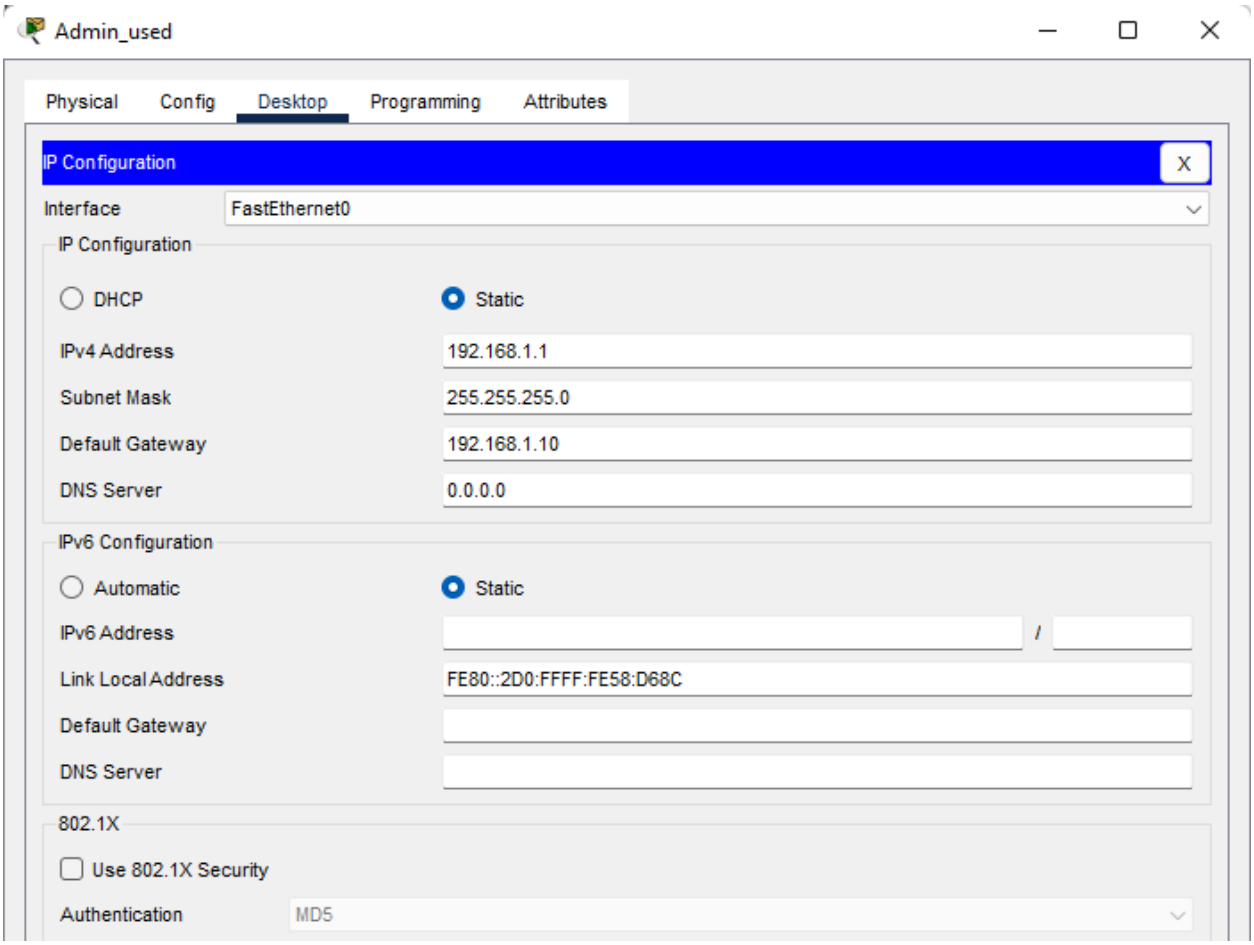
Security: Broadband connections may not offer the same level of security as MPLS or leased lines.

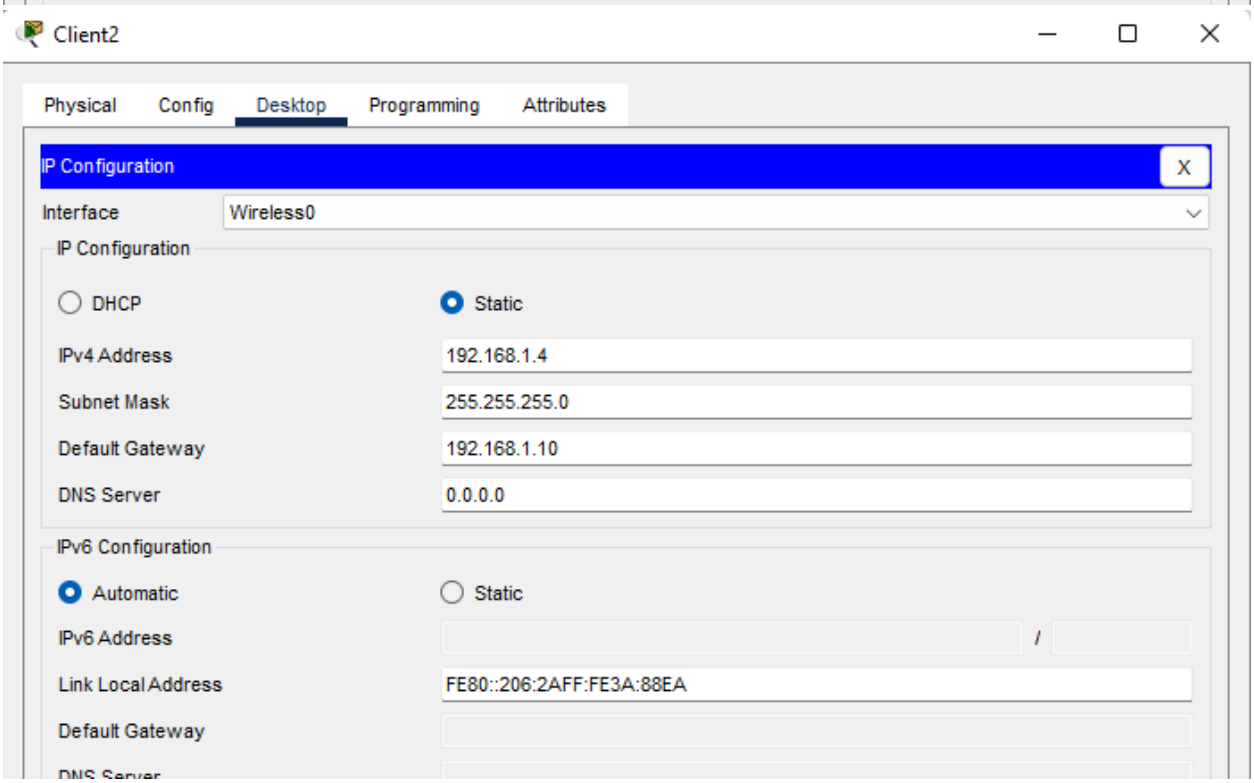
LC Solicitors' Needs:

Broadband connections offer cost-effectiveness but may lack the reliability and security required for transmitting sensitive legal data.

Task 1c- Network Configuration and Full Connectivity: IP Addressing Scheme:

1) Assign the IP of All devices in the network:

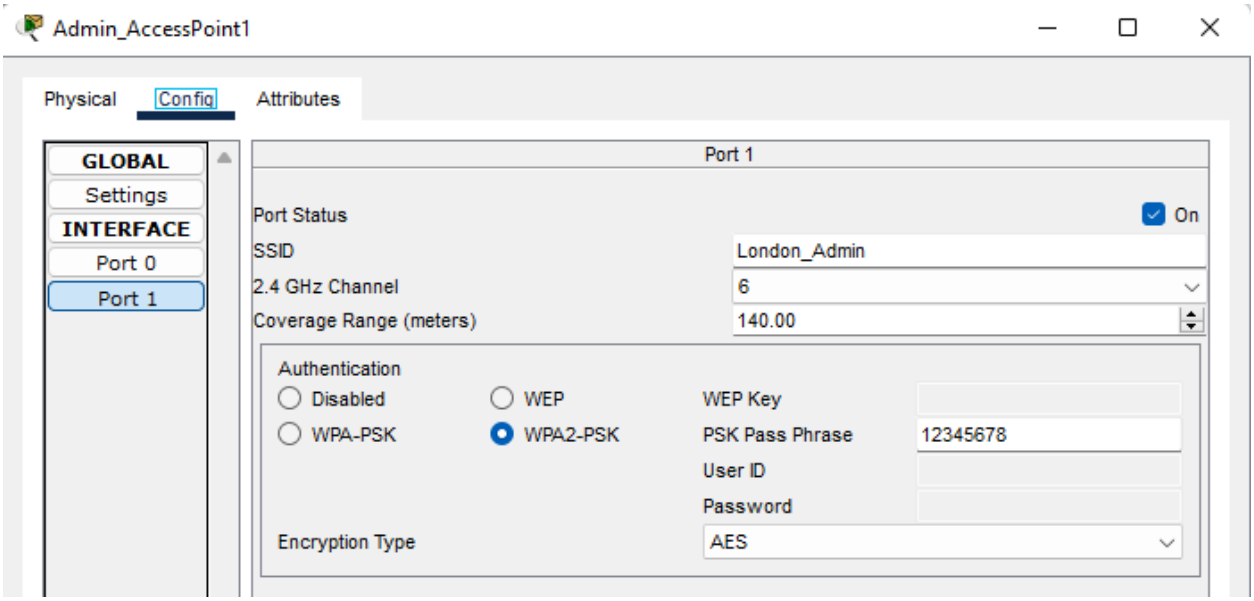

Admin_used
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:FFFF:FE58:D68C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5


Client2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
Wireless0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.10
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::206:2AFF:FE3A:88EA
Default Gateway
DNS Server

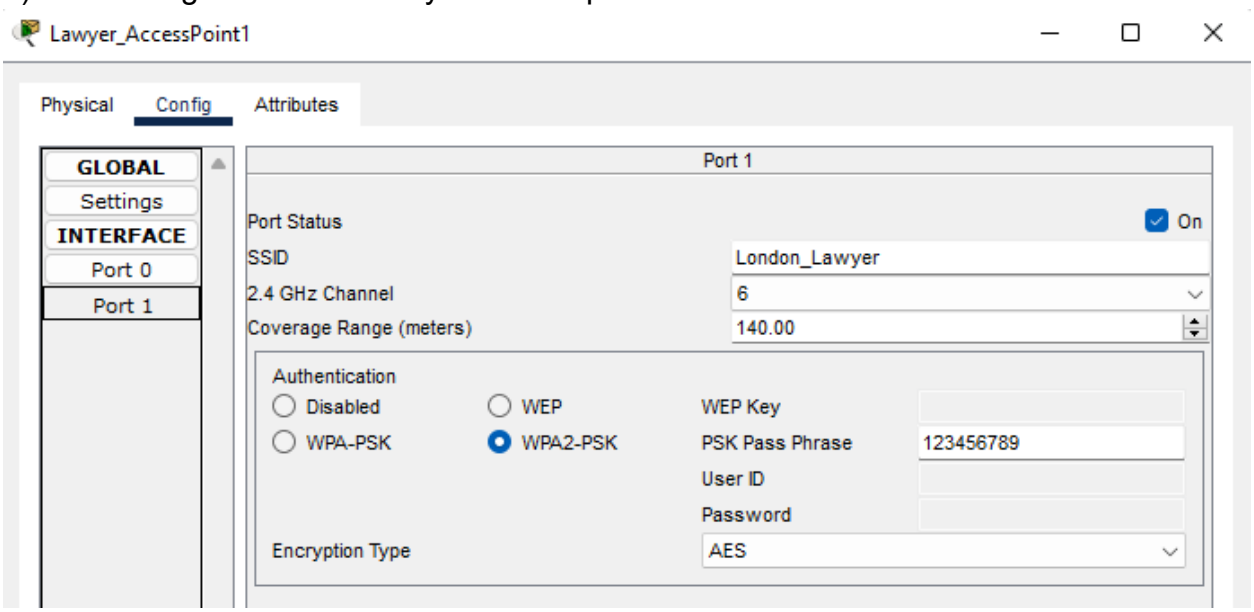
2) Do same process for the rest of devices:

Routers and switches and access point Configuration:

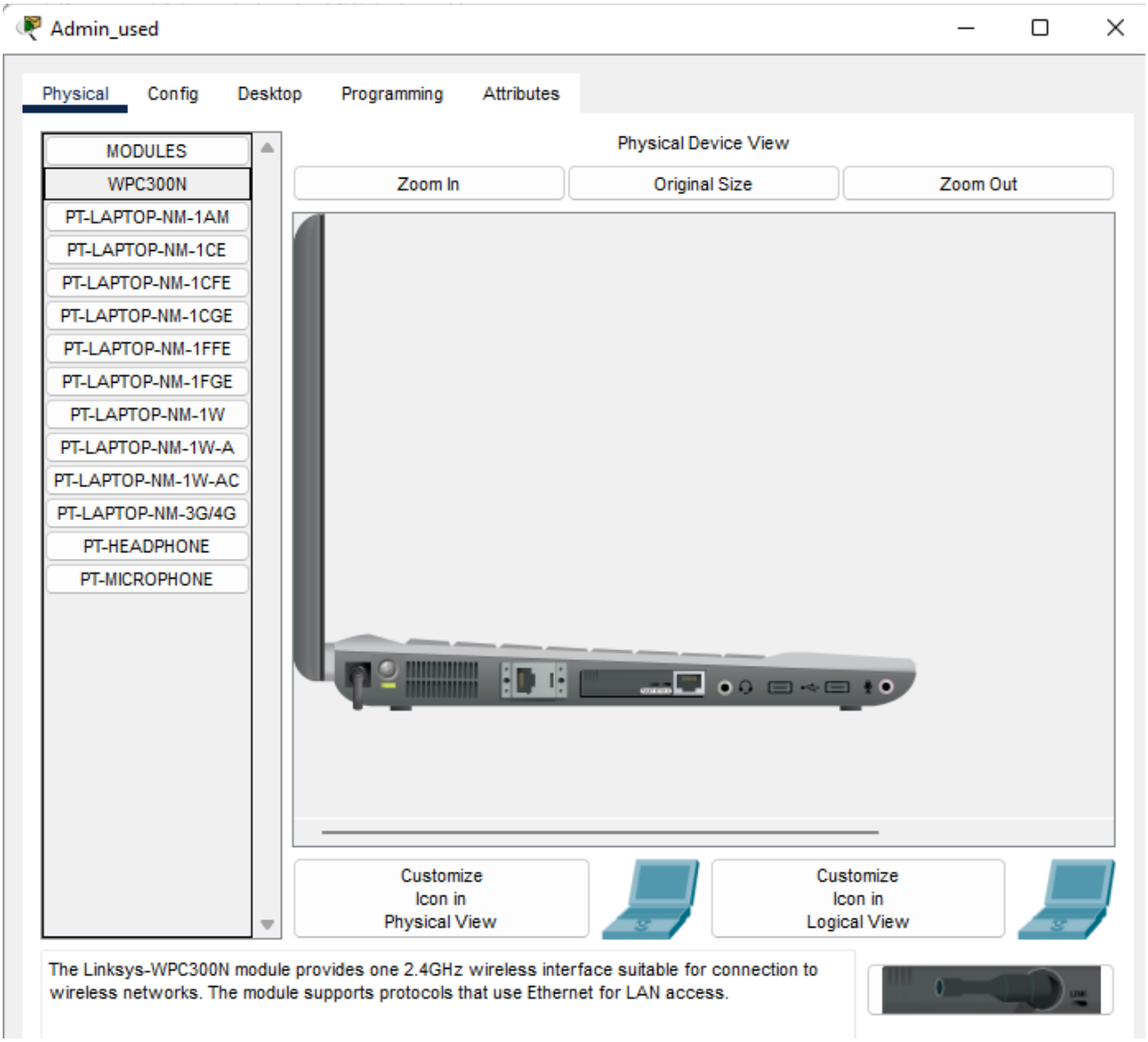
1) Configure the London access point and implement some protocols like AES, and WPA2-PSK:



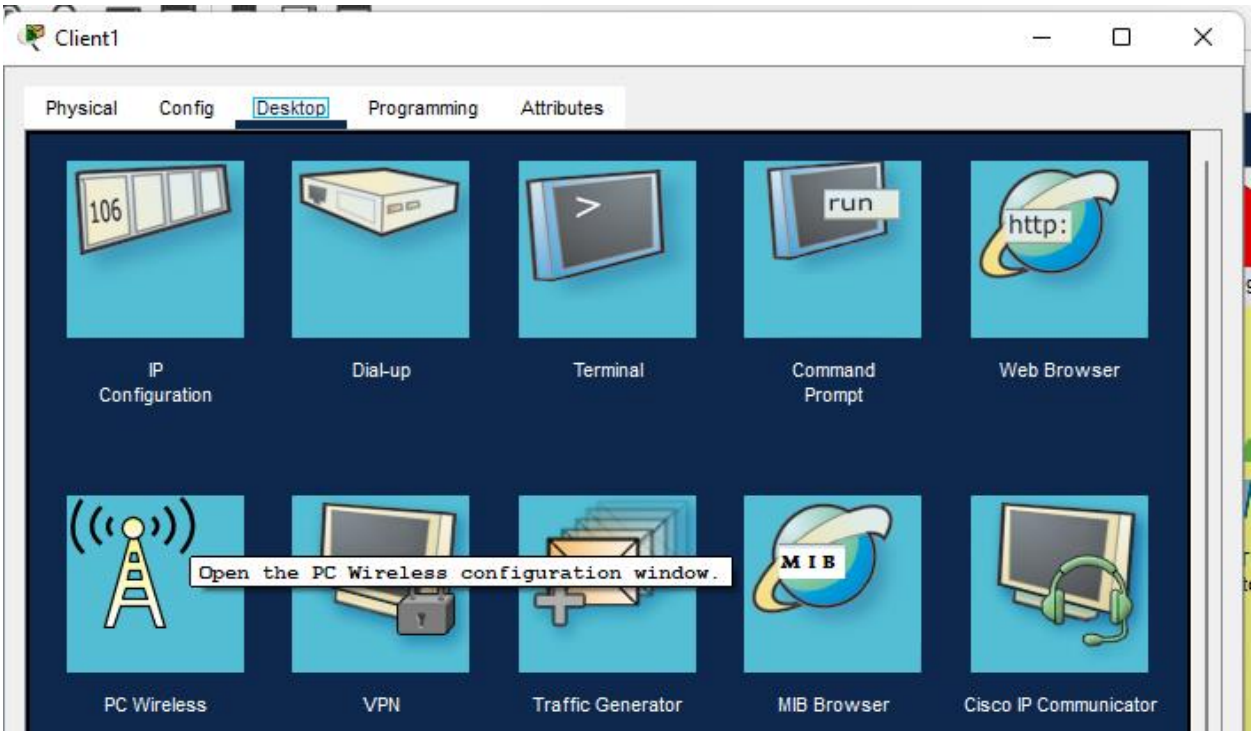
2)Then configure second Lawyer access point same as above:



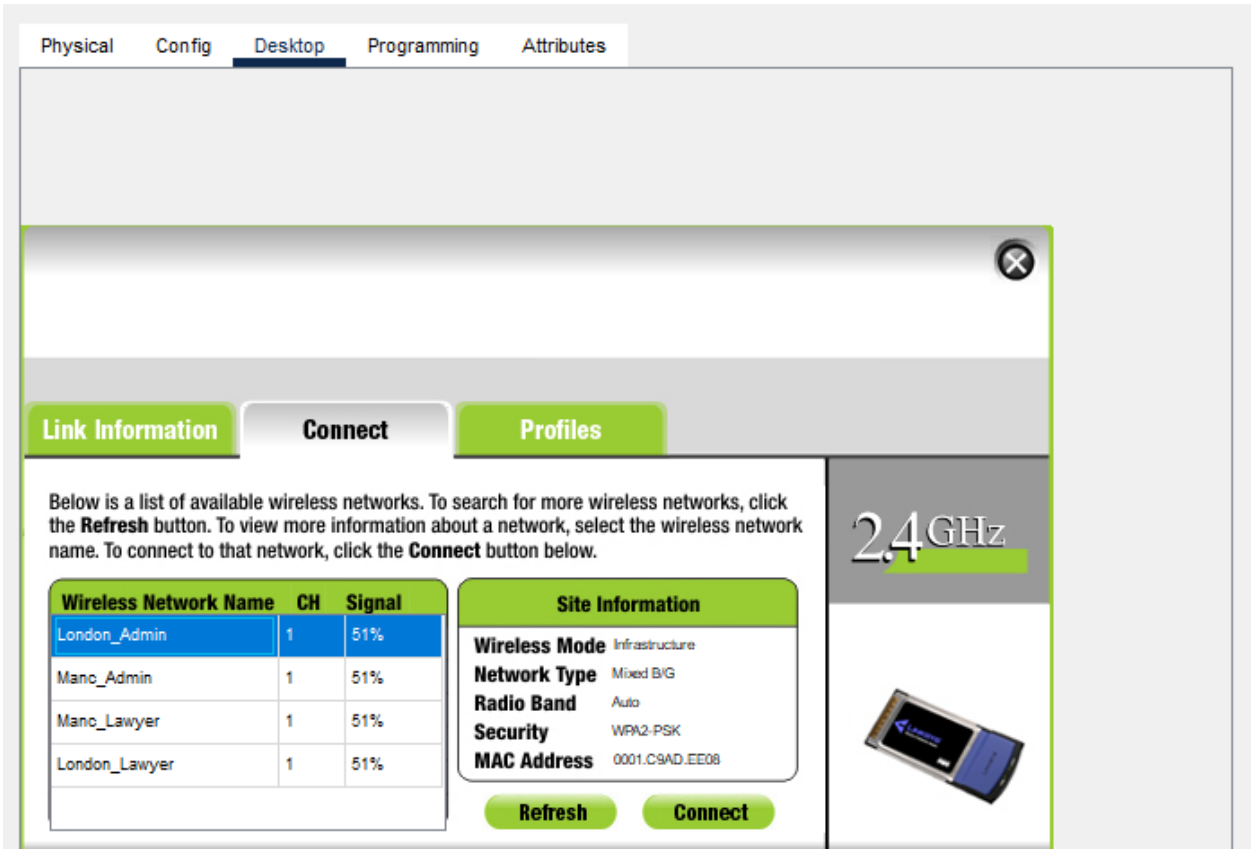
3) First Change the Ethernet cable and used WPC300N:



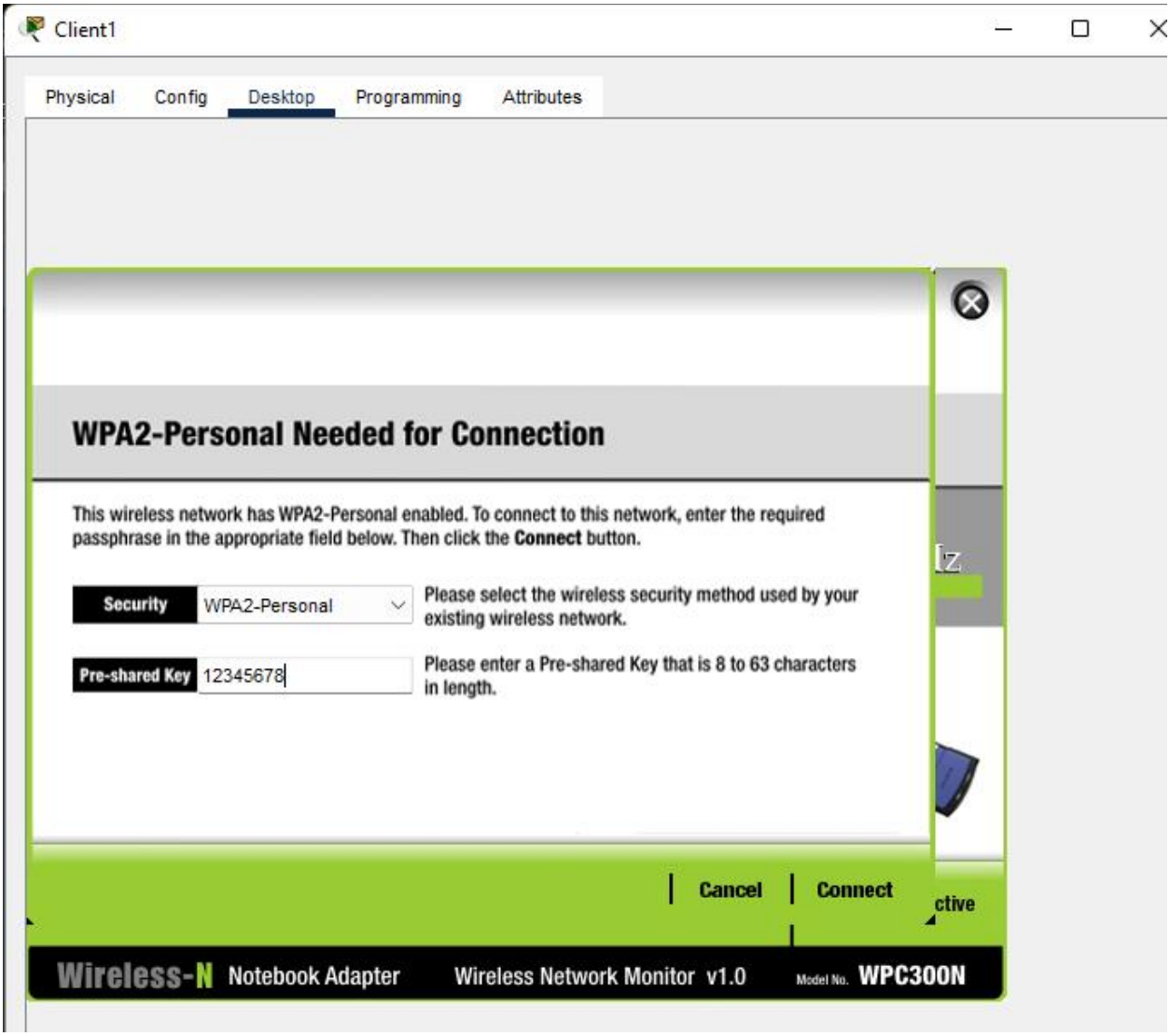
4) Then go the Wireless device which can be connected to the access point (Click the Client PC and Open the PC Wireless):



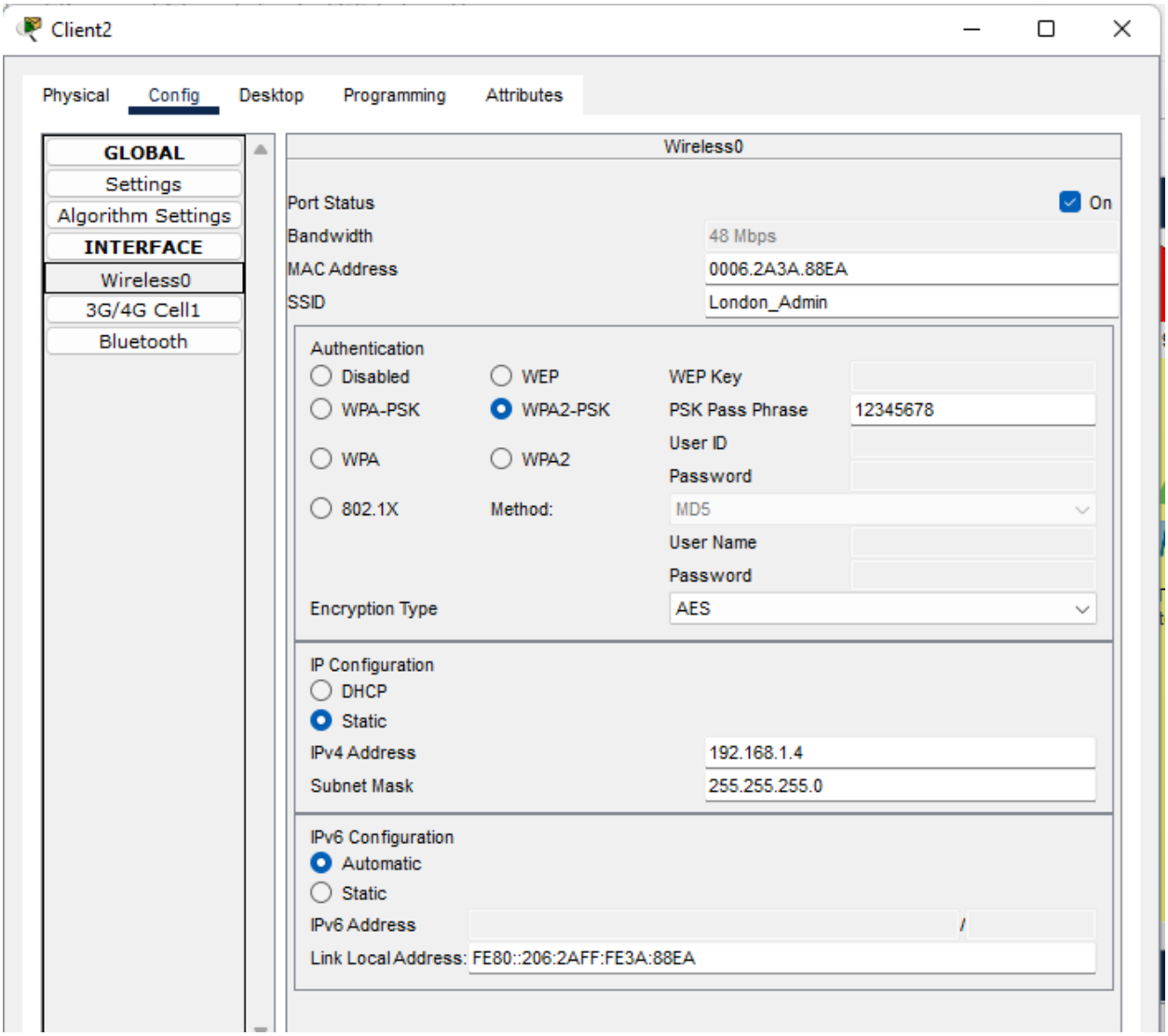
5) Go to the Connect Tab and Refresh it After Showing the name of the access point then Click to connect:



6) After Give the Pre-Shared key of the Access Point:



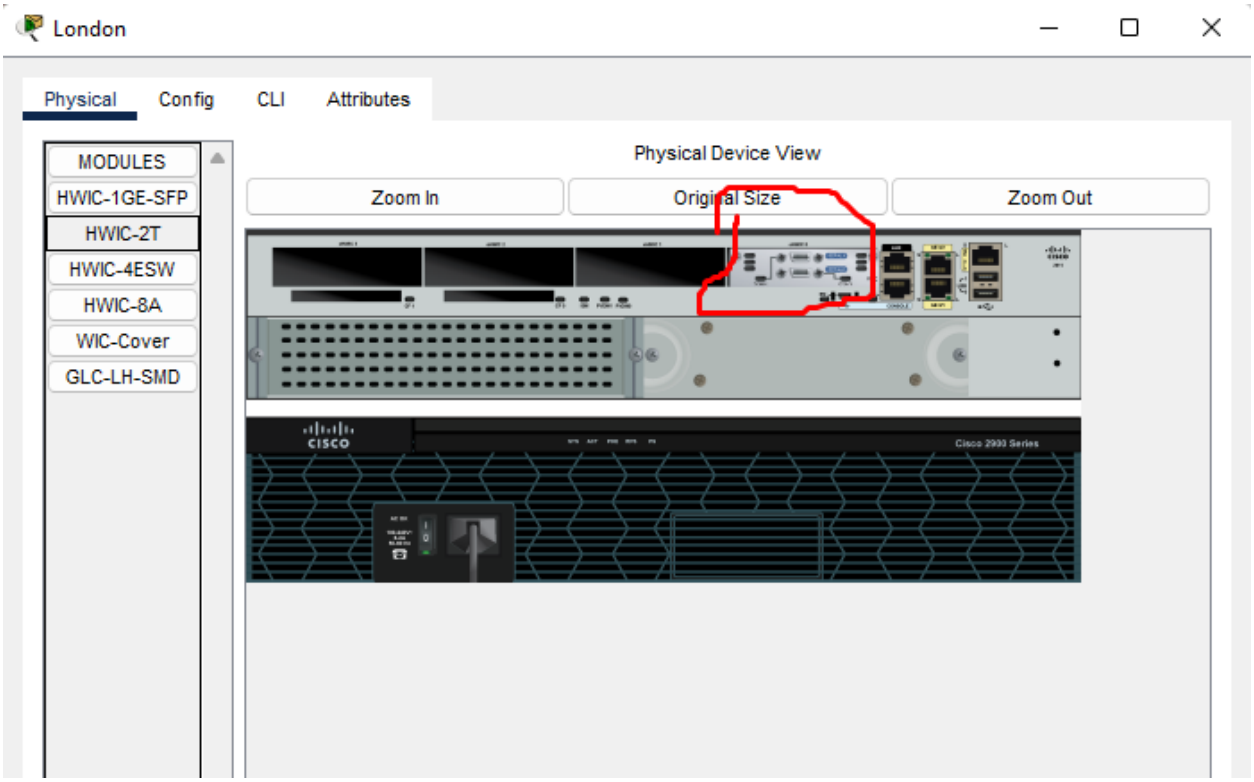
7) For Mobile Wireless configuration:



8) Same Configuration for the Rest of all wireless Client:

9) Then configure a router:

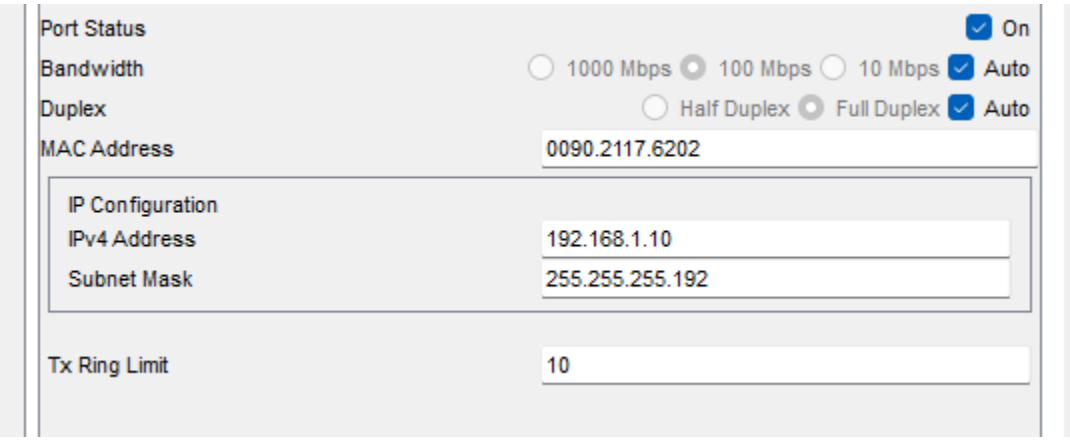
10) Click on the London Router and on physical First off the switch and then add the serial port in it (clock signals for synchronization) and then On it :



12) For London office subnet should support a minimum of 50 IP addresses:

192.168.1.10/26 (CIDR)

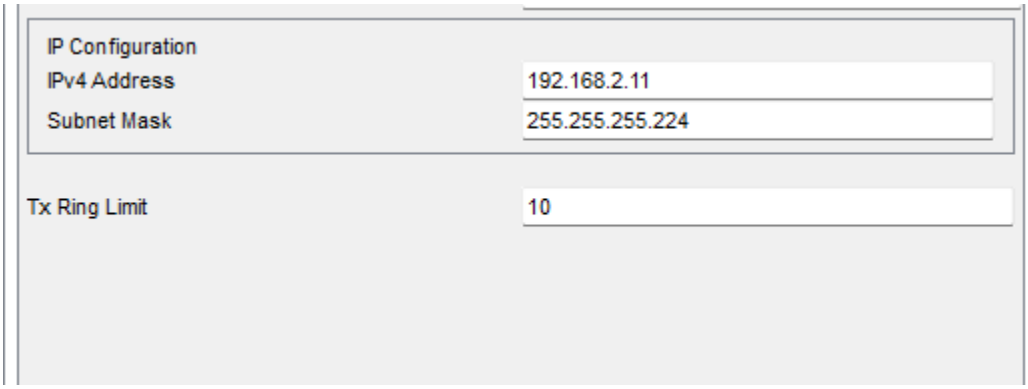
255.255.255.192 (Subnet mask)



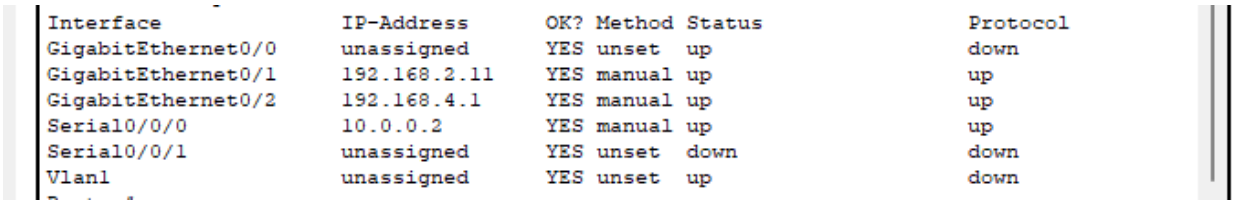
13) Manchester office subnet should support a minimum of 24 IP addresses:

192.168.2.11/27 (CIDR notation).

255.255.255.224 (subnet mask)



14) Give the IP That Given in the Diagram and on it:



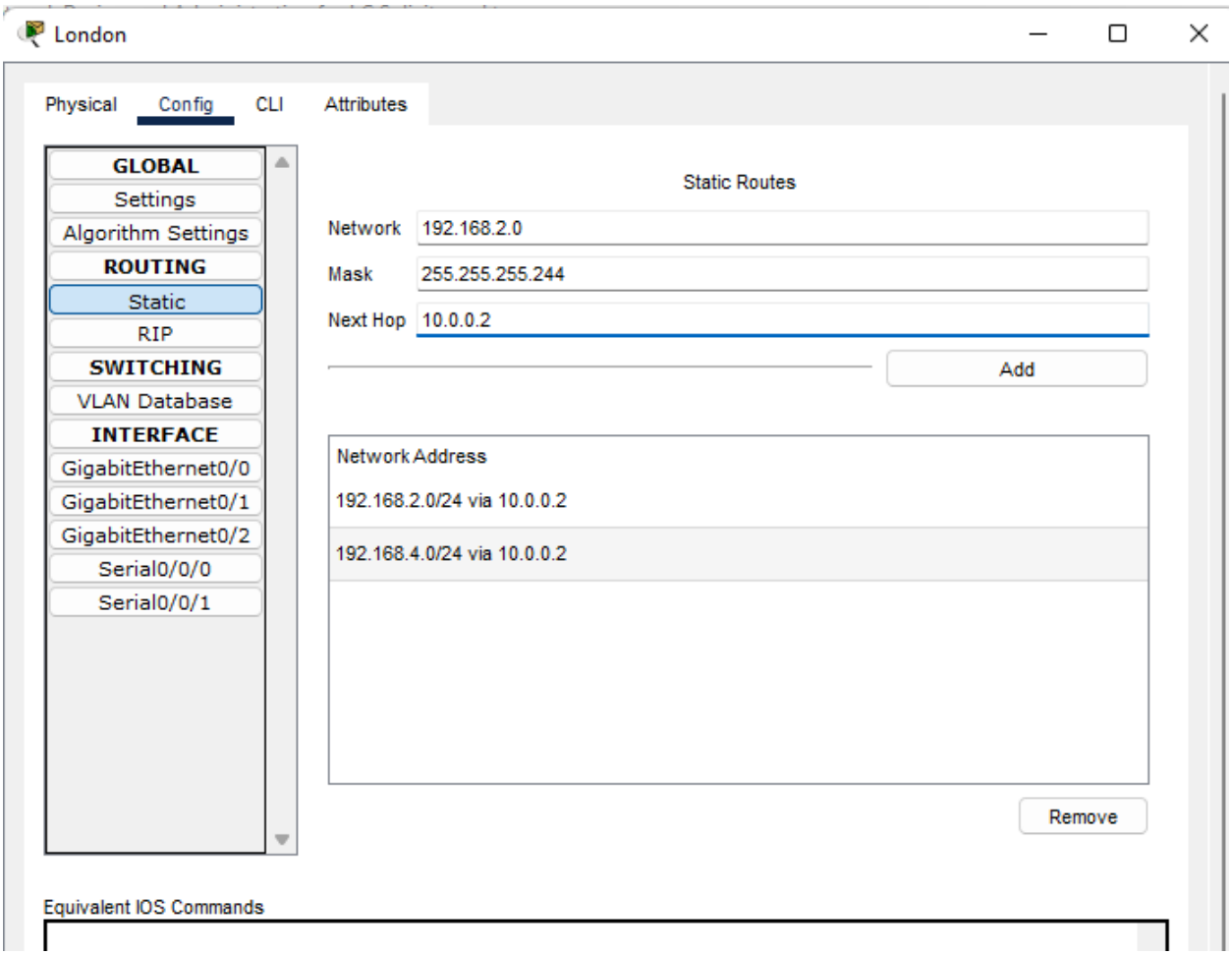
```
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    down
GigabitEthernet0/1     192.168.2.11    YES manual up                    up
GigabitEthernet0/2     192.168.4.1     YES manual up                    up
Serial0/0/0            10.0.0.2        YES manual up                    up
Serial0/0/1            unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  up                    down
```

15) Or Through CLI:

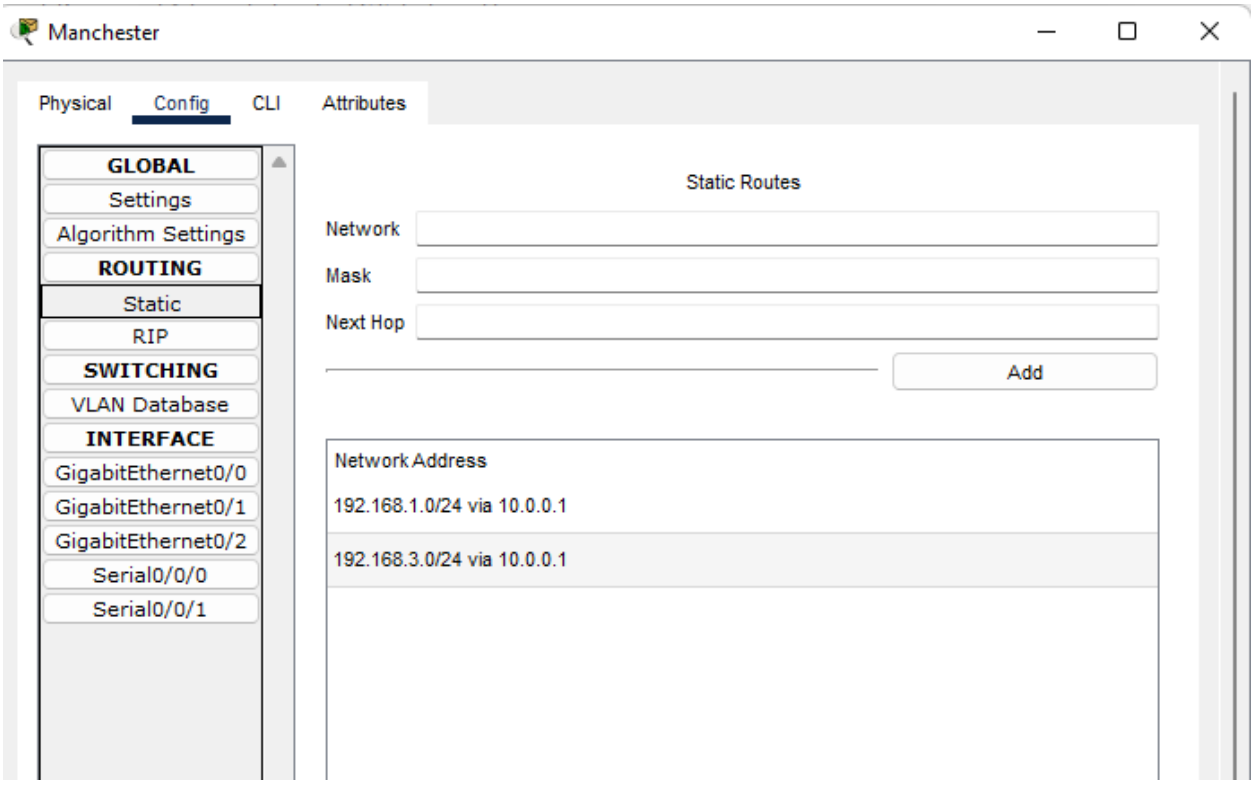
```
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.2.11 255.255.255.224
Router(config-if)#ip address 192.168.2.11 255.255.255.224
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/2
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
```

16) Same Configuration for the Manchester office:

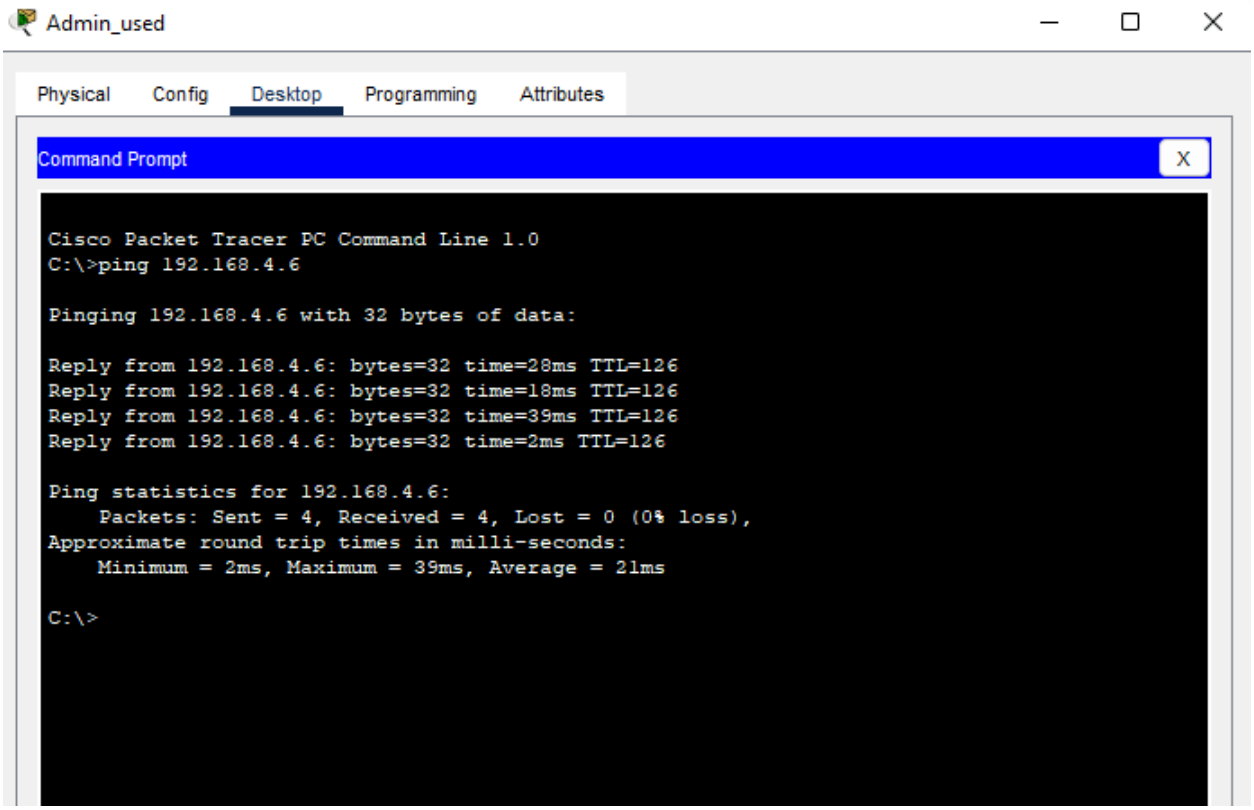
17) Also Configuration of the Next near router:



18) Same Configuration for the Manchester Router:



19) Now test the Network through ping and traceroute Command (Admin PC To Client 7):



Task 1d- Network Performance Measurement:

1) Identify and explore tools that can be used to measure network performance?

Network Analyzers: Network analyzers, such as Wireshark, provide in-depth analysis of network traffic. They capture and analyze packets flowing through a network interface, allowing administrators to identify performance bottlenecks, packet loss, and abnormal traffic patterns.

SNMP (Simple Network Management Protocol) Monitoring: SNMP monitoring tools, like Nagios or Zabbix, gather performance data from network devices such as routers, switches, and servers.

Traceroute: Traceroute is another command-line tool that traces the route packets take from the source to the destination. It displays the IP addresses of the routers along the path and measures the time taken for each hop.

Ping: Ping is a basic tool that sends ICMP (Internet Control Message Protocol) echo requests to a target device and measures the response time

2) Research both hardware and software tools that are commonly employed for this purpose.?

Hardware Tools:

Network Taps: These devices are placed in line with network connections to passively monitor traffic.

Network Probes: Network probes capture and analyze traffic at specific points in the network.

Software Tools:

Wireshark: Wireshark is a popular open-source packet analyzer that captures and analyzes network traffic in real-time.

Nagios: Nagios is a widely used open-source network monitoring tool that provides comprehensive monitoring of network devices, services, and applications.

3) Consider metrics such as latency, bandwidth, packet loss, and jitter?

Latency:

Hardware Tools: Network probes and performance monitoring appliances can measure latency by capturing packets at various points in the network and analyzing the time it takes for packets to travel from source to destination.

Software Tools: Tools like Wireshark and network monitoring software provide insights into latency by analyzing packet timestamps and calculating round-trip times (RTT) between network devices.

Bandwidth:

Hardware Tools: Network performance monitoring appliances and packet brokers can measure bandwidth utilization by monitoring traffic volume passing through network interfaces in real-time.

Software Tools: Network monitoring software, such as PRTG and SolarWinds NPM, provides bandwidth utilization reports and dashboards to visualize traffic patterns and identify bandwidth-intensive applications or services

Packet Loss:

Hardware Tools: Network probes and packet brokers can detect packet loss by analyzing captured packets and identifying missing or out-of-sequence packets.

Software Tools: Packet analyzers like Wireshark can identify packet loss by analyzing packet headers and payload contents, flagging packets with checksum errors or retransmissions.

Jitter:

Hardware Tools: Network probes and performance monitoring appliances can measure jitter by analyzing variations in packet arrival times over a period.

Software Tools: Network monitoring software often includes features to measure jitter by tracking changes in latency over time and calculating variance in packet arrival times

4)Justify the importance of monitoring and evaluating network performance for LC Solicitors?

Keeps operations smooth

Ensures client satisfaction

Enhances security

Saves money

Ensures compliance

5) Explain how regular performance assessments contribute to efficient network operations and user satisfaction.

Regular performance assessments play a critical role in maintaining efficient network operations and enhancing user satisfaction by identifying issues early, optimizing resource allocation, facilitating capacity planning, improving service levels, and enhancing the overall user experience

Task 1e: Dual Implementation and IPv6 Scheme Explanation:

1)Explain the concept of dual-stack implementation, which allows the simultaneous use of both IPv4 and IPv6 in the network?

In LC Solicitors' network, using both IPv4 and IPv6 simultaneously is like that every device gets two addresses: one IPv4 and one IPv6. This way, no matter which protocol someone is using, they can still talk to each other without any language barriers.

Sample of IPv6 : London office gets the subnet 2001:db8:abcd:1::/64 and vice versa.

2) Explain the benefits and reasons for adopting a dual-stack approach?

LC Solicitors the benefits of compatibility, futureproofing, improved performance, compliance, and global reach. By embracing both IPv4 and IPv6 protocols, LC Solicitors can ensure seamless connectivity, scalability, and readiness for the future of networking.

3) Address compatibility and coexistence challenges between IPv4 and IPv6?

Tunneling: Tunneling mechanisms enable IPv6 packets to travel over IPv4 networks and vice versa. LC Solicitors can use tunneling to bridge the gap between IPv4 and IPv6 networks, ensuring that devices can communicate regardless of the protocol they use.

Application Readiness: LC Solicitors should ensure that their applications and services are compatible with IPv6. By updating or modifying existing applications and deploying IPv6-compatible solutions, they can minimize compatibility issues and ensure smooth operation in a mixed IPv4/IPv6 environment.

NAT64: To facilitate communication between IPv6-only and IPv4-only devices, LC Solicitors can deploy NAT64, which translates IPv6 addresses to IPv4 and vice versa. This translation allows for smooth communication between devices using different protocols

4) Design a comprehensive IPv6 addressing scheme for both the London and Manchester offices for Admin, Lawyers, and wireless networks.?

London Office:

Office Subnet: 2001:db8:1:0::/64

Admin LAN: 2001:db8:1:1::/64

Lawyers LAN: 2001:db8:1:2::/64

Wireless LAN: 2001:db8:1:3::/64

Manchester Office:

Office Subnet: 2001:db8:2:0::/64

Admin LAN: 2001:db8:2:1::/64

Lawyers LAN: 2001:db8:2:2::/64

Wireless LAN: 2001:db8:2:3::/64