NETWORK DESIGN AND IMPLEMENTATION

Table of Contents

Introduction

Rebuilding UKF's network infrastructure is a vital project that will improve security, availability, and performance for several trading floors and regional offices. The current structure has a red flag as it does not offer a future-proofing solution so that it can meet the needs of current demands and adapt to the tech trends that would keep changing. Also, the old hardware and cabling are holding back the operations. This broad measure is aimed at cutting the operating time of the dealers and the entire supporting staff, supporting the cross-device platform usability, and allowing maximum network traffic loading for operators. In view of the cutting-edge nature of the financial services business, effective techniques incorporating robust security measures and data transmission protocols will be deployed to ensure that UKF remains at the forefront. The span of these measures will build the base for a reliable and easy-to-grow network.

Implementation of the network topology

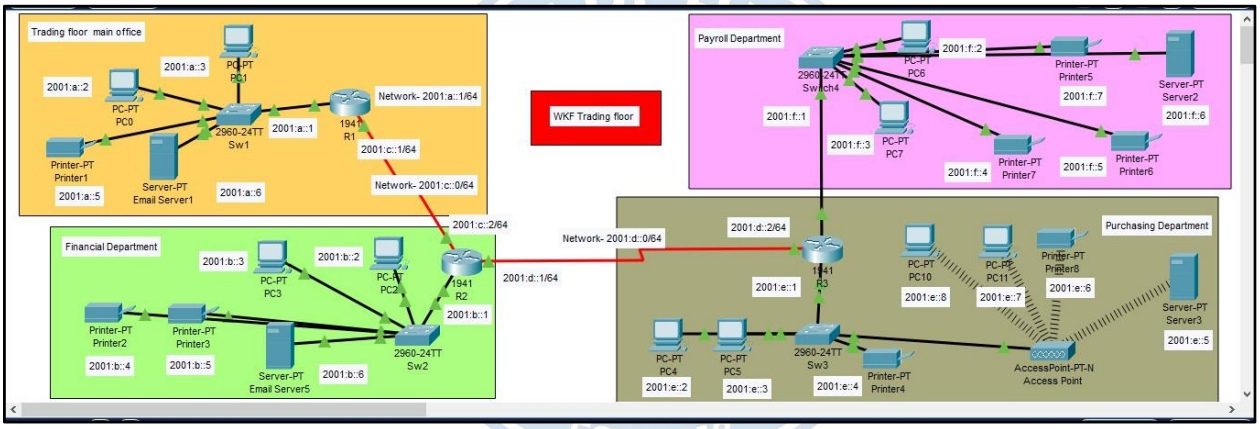

Figure 1: Network topology of UKF trading floor

The trading floor's network topology is shown in Figure 1, which highlights a strong infrastructure intended for high-performance trading activities. Routers (R1, R2) provide connectivity across various network segments, whilst switches (Sw1, Sw2, Sw3) control communication inside devices (Hou *et al.* 2021). Along with the email and financial applications, the traders and support personnel use servers like Server-PT, where they can access their workstations like PC-PT and PC1 through networks. Network masks and VLANs do better at the network's efficiency and security. Implementation of this structure ensures correct data passing fulfilling high demands to the financial market towards such critical aspects as speed and availability.

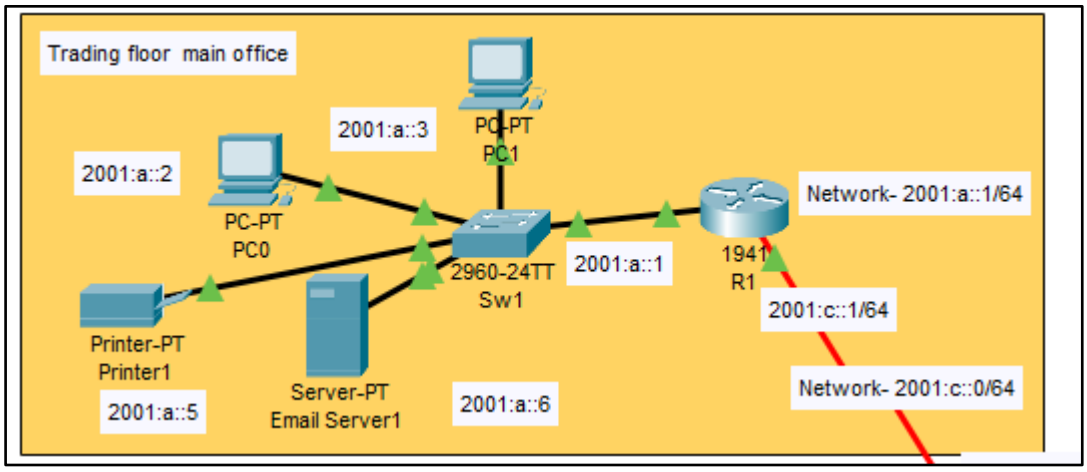

Figure 2: Trading floor main office network

The trading floor's main office's network configuration is shown in Figure 2, which includes all of the necessary parts for smooth operations (Umoga *et al.* 2024). To facilitate communication and data storage, workstations (PC-PT, PC1) are networked with printers (Printer-PT) and servers (Server-PT), including an email server. For effective data management, the network uses subnetting and VLAN segmentation (Network-2001). The trade floor area is guaranteed to have optimal performance and accessibility thanks to its simplified design.

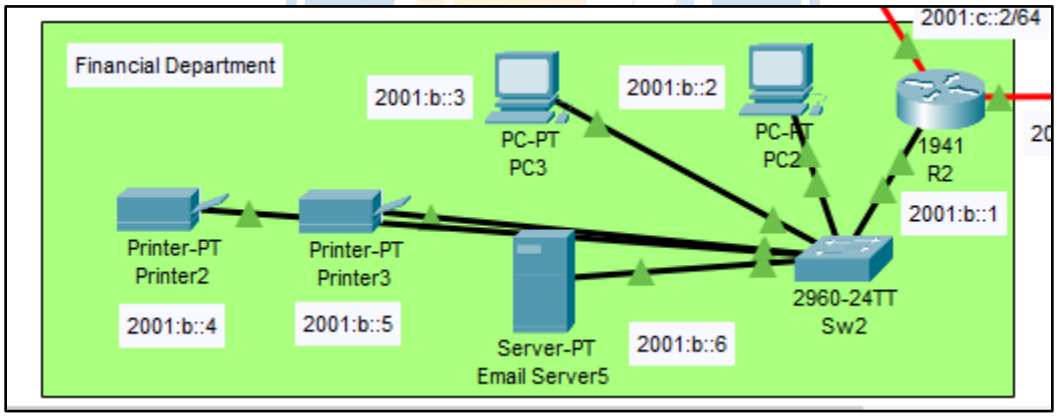

Figure 3: Financial department network

The network architecture of the Financial Department is in the figure below. This network supports a variety of critical financial processes. Printers (Printer1, Printer2, Printer3); those maintaining email and other vital services are linked with workstations (PC1, PC2, PC3). VLAN segmentation which is in relation to the year 2001 is of paramount importance when looking at security and network separation. The main switch (2980TT-24) of the department's network environment is the one that in addition to the configuration of the network, allows the exchange of data within the devices.

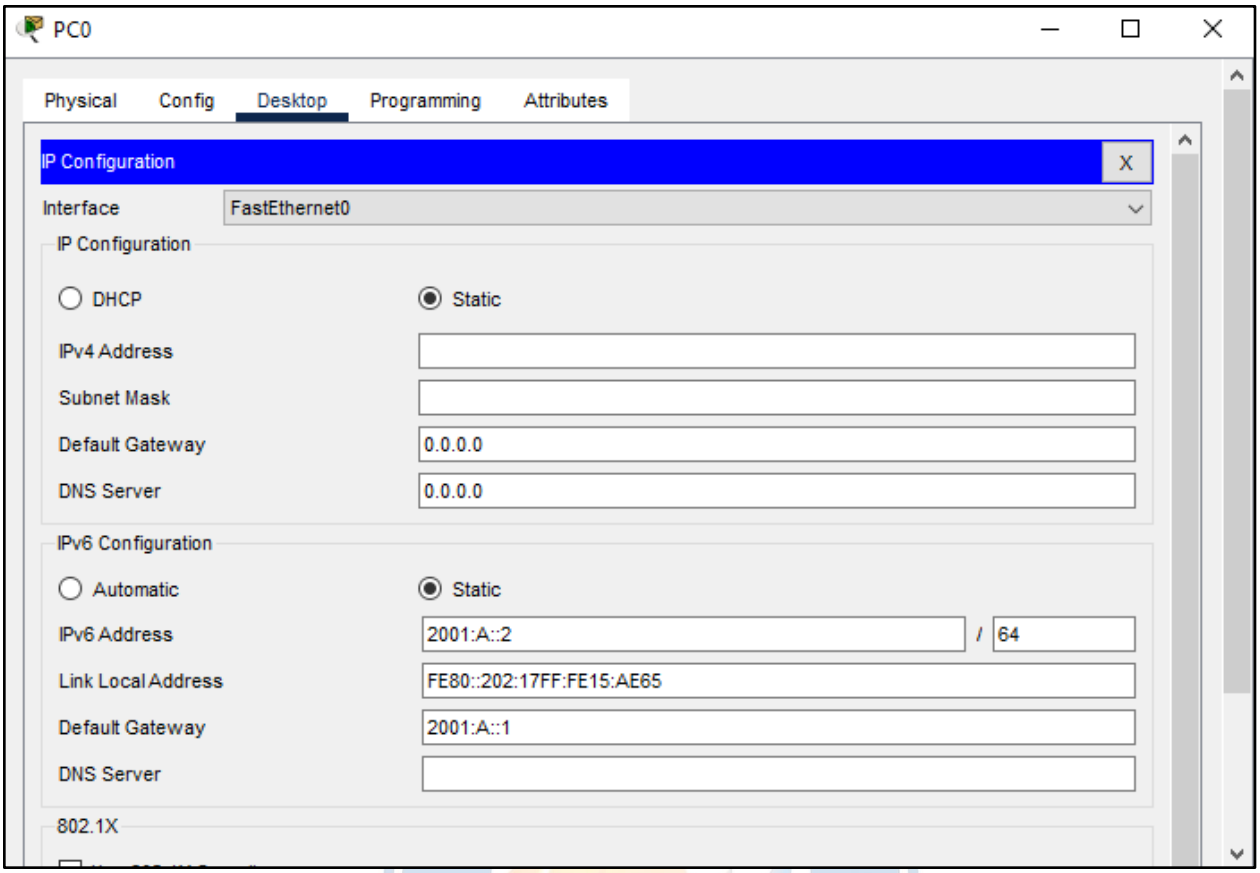

Figure 4: IPv6 configuration of PC

A PC's IPv6 setup settings are shown in Figure 4, which also includes link-local address assignment and automated address allocation. It also includes information on the DNS server, default gateway, and support for 802.1X authentication with static addressing.

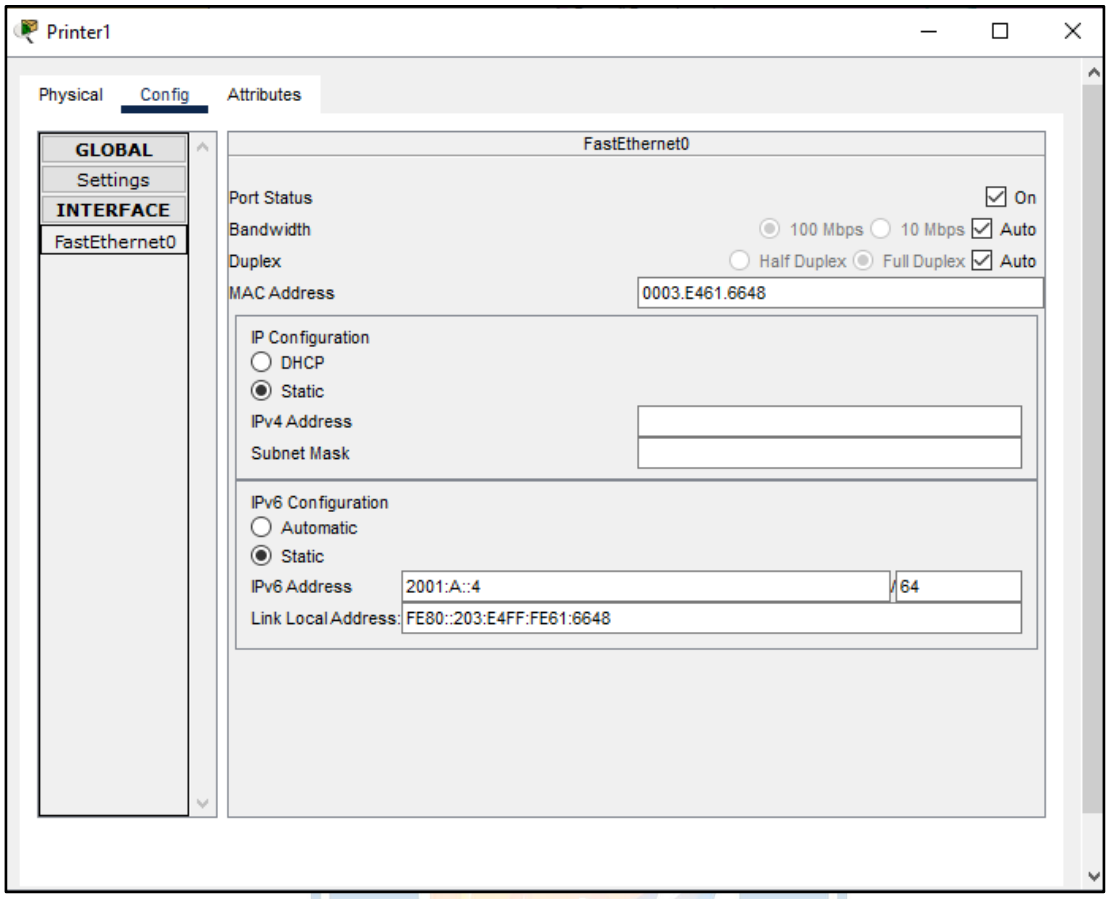

Figure 5: IPv6 configuration of printer

The printer's IPv6 setup, which allows for both automated and static address assignment, is shown in Figure 5. In order to provide local network access and communication, it also entails the assignment of an IPv8 address and a link-local address with a subnet prefix of 2001 and a prefix length of 64.

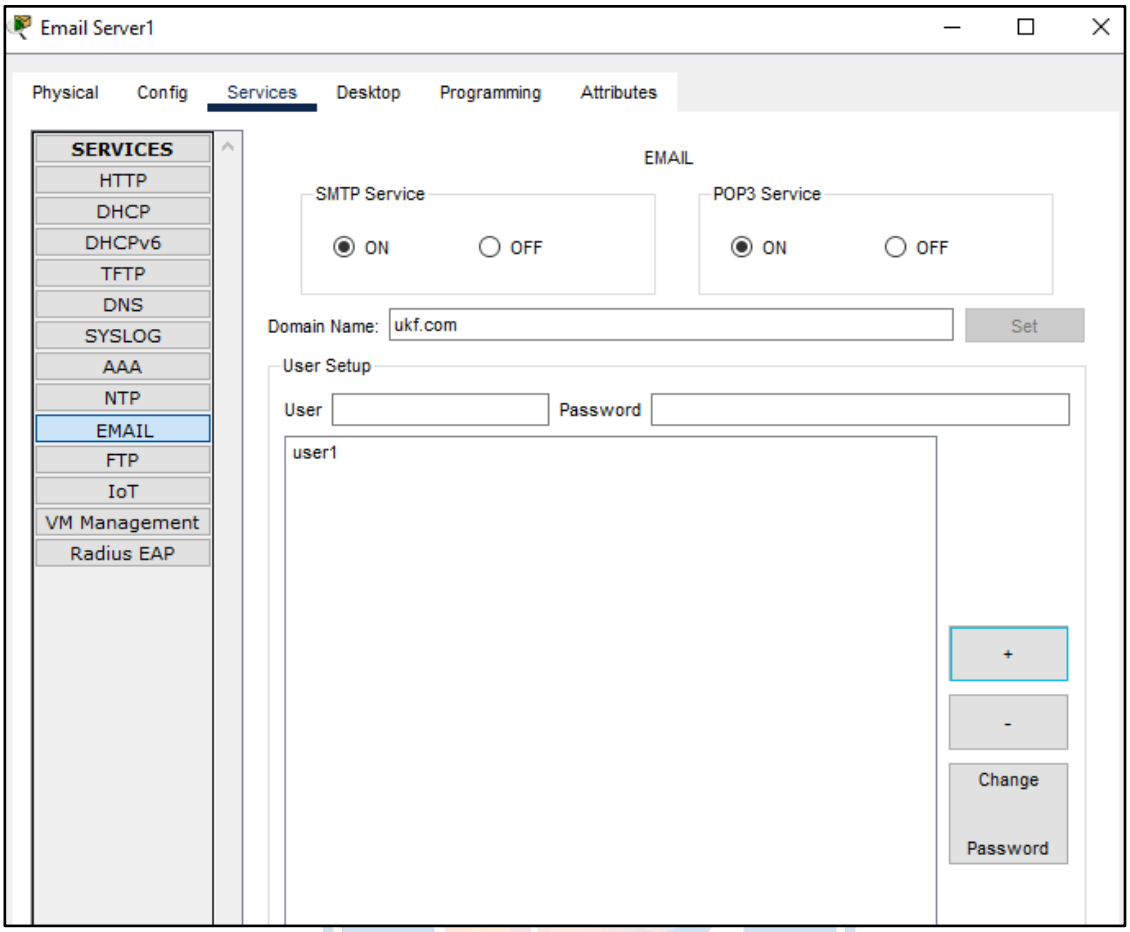

Figure 6: Email server configuration

Email server 1 arrangement is presented later. Inside, DHCPv6, SMTP, HTTO, and others protocols are listed as shown in Figure 6. The server also enables to read emails because it uses a POP3 network. With that feature, it is much easier to set up new users and passwords for their ukf.com email address and consider it as very secure and effective.

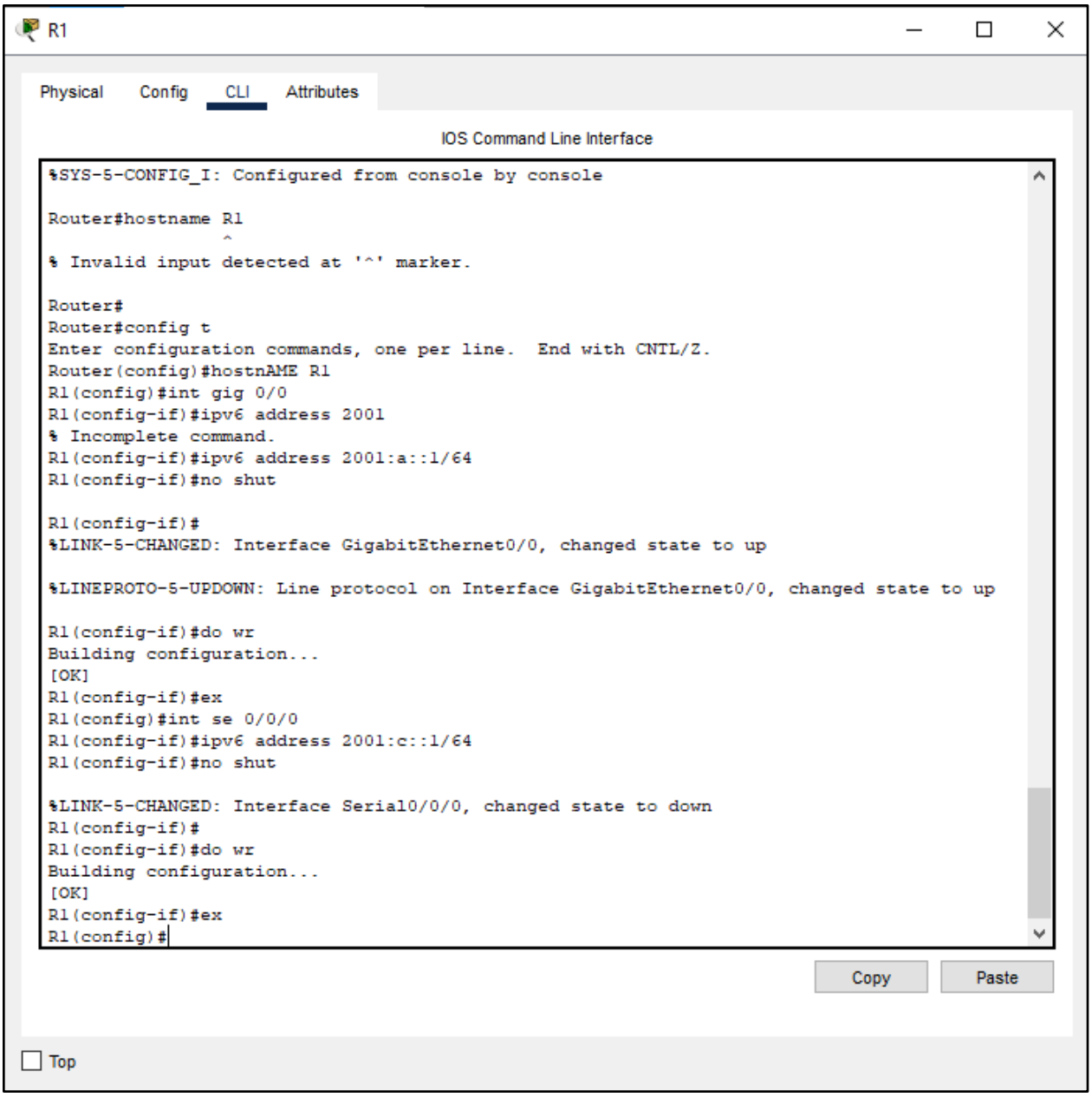

Figure 7: IPv6 configuration of Router 1

Router 1's IPv6 configuration procedure is shown in Figure 7. After configuring GigabitEthernet interface 0/0 with IPv6 address 2001:a::1/64, the interface is enabled and brought up. After that, the IPv6 address 2001:c::1/64 is assigned to Serial interface 0/0/0, and the interface is closed. The interface appears once the configuration modifications have been applied.

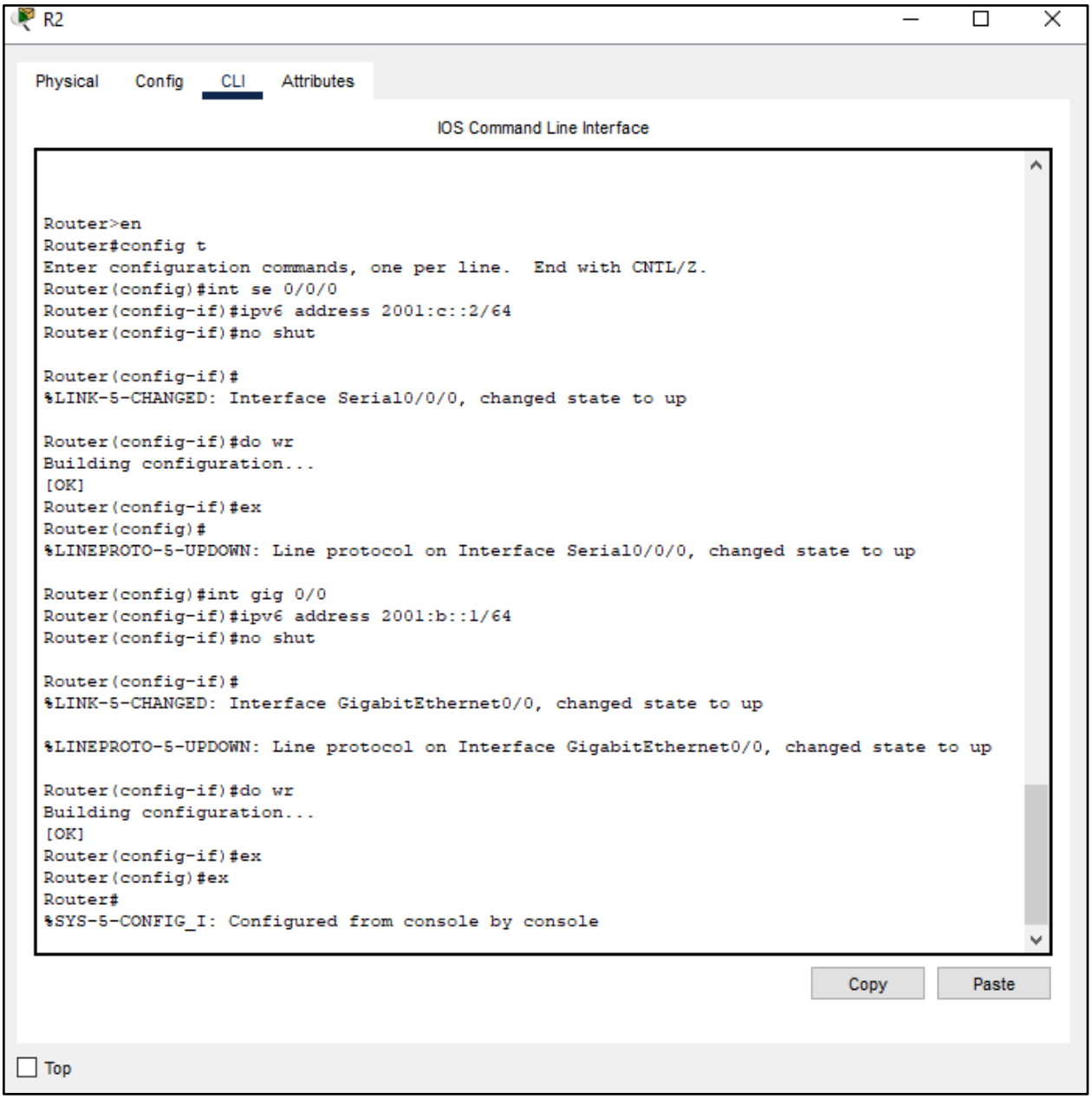

Figure 8: IPv6 configuration of Router 2

This figure shows a similar IPv6 configuration of router 2 in the Cisco packet tracer, where successfully implement the IPv6 addresses in each port.

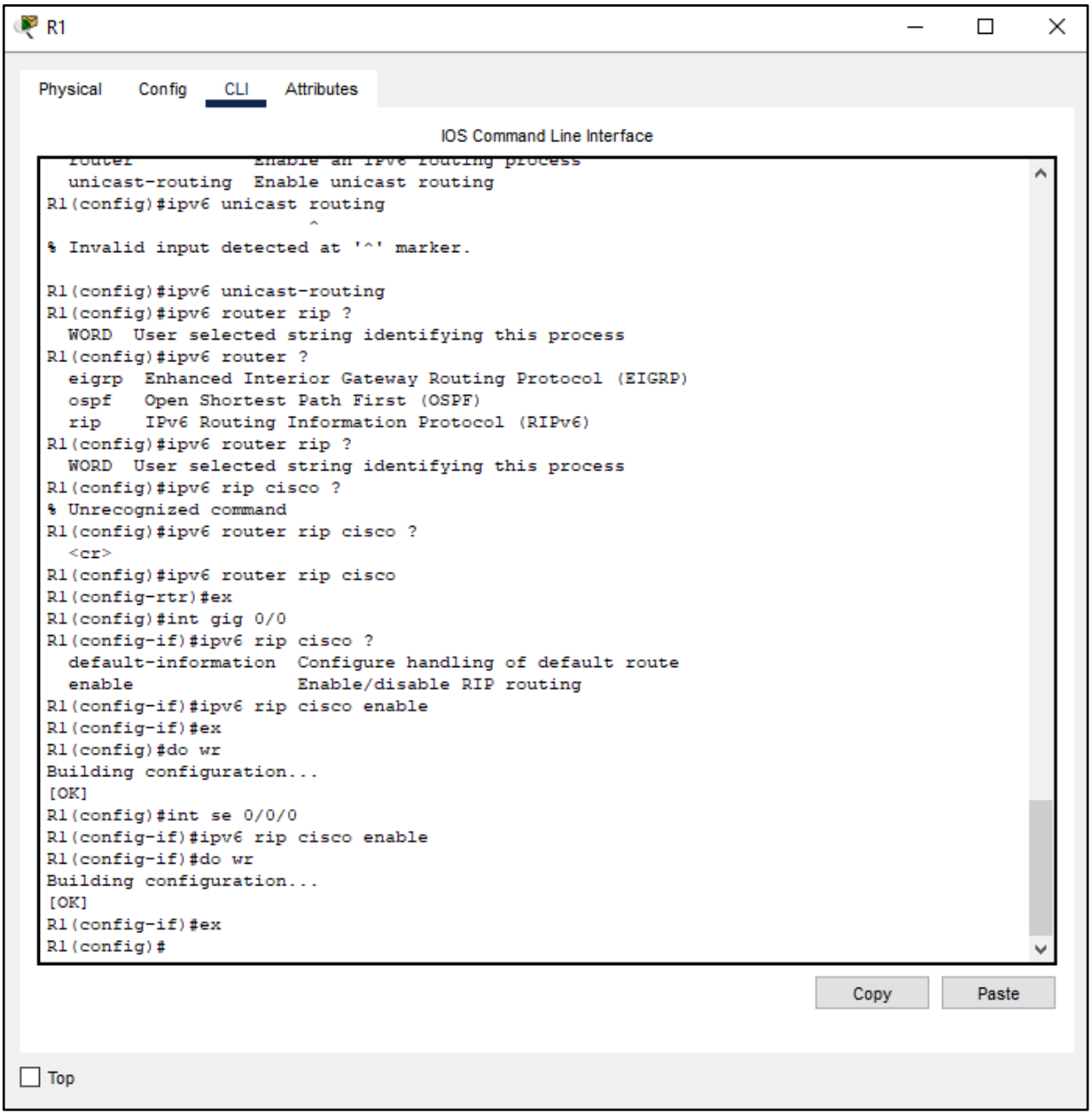

Figure 9: RIP configuration on network router

A network router's RIP (Routing Information Protocol) setup is shown in Figure 9. The router has IPv6 unicast routing enabled by default. Thereafter the configuration should start, for the setup needs both the Serial interface 0/0/0 and the Gigabit Ethernet interface 0/0/0 for the IPv6 RIP. Lastly, the configuration is kept, thus, it assures that the route of RIP for IPv6 correctly works on the router.

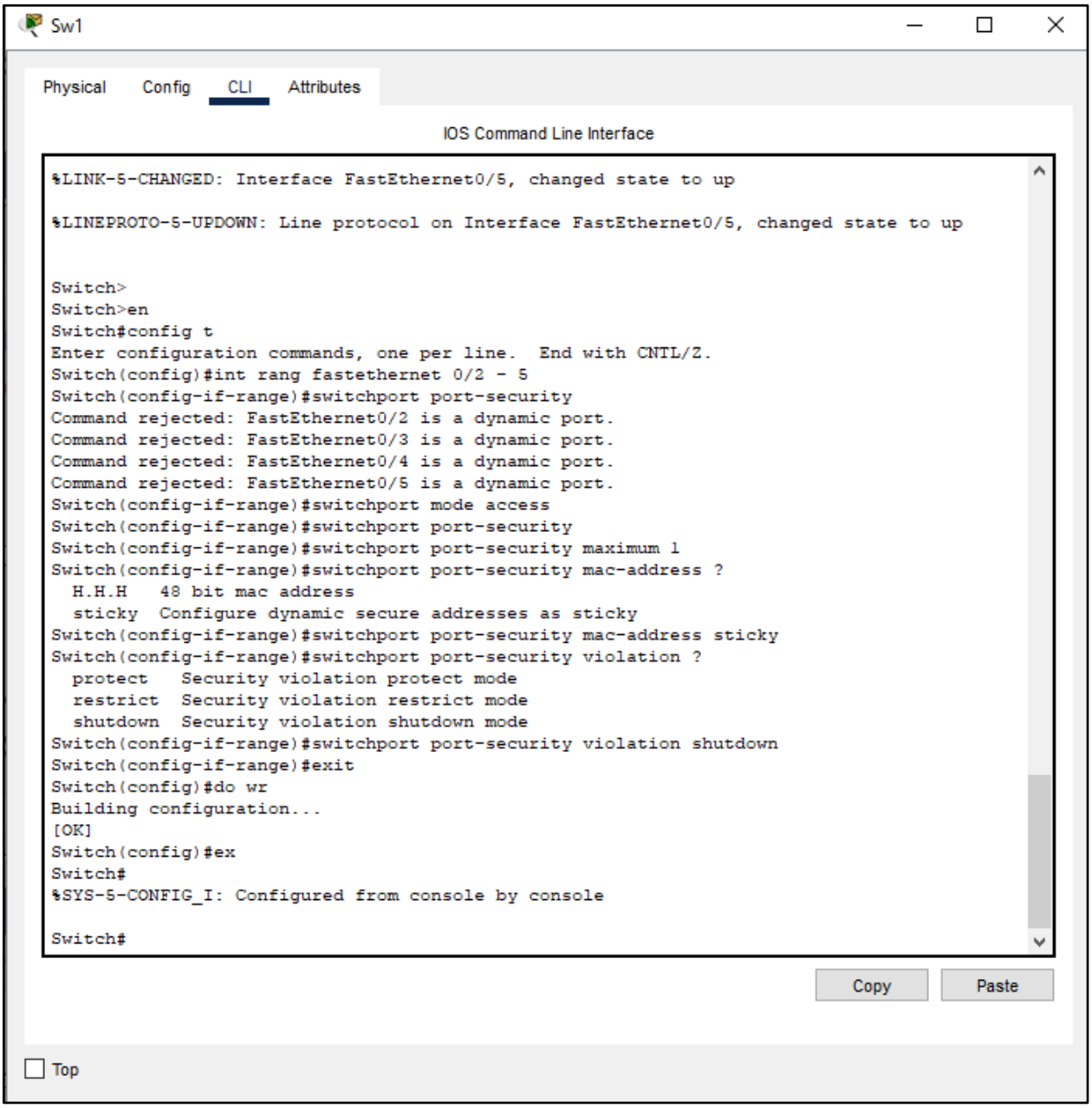

Figure 10: Port security implementation

The application of port security on a switch is shown in Figure 10. Only one MAC address is permitted per port on FastEthernet interfaces 0/2 through 0/5, which are set up as access ports with port security enabled. Also, specific kinds of threats for port security violation actions terminate. This increases the probability of response that attempts of security personnel arrest pirates. Modification to the setup is remembered for the coming instances.

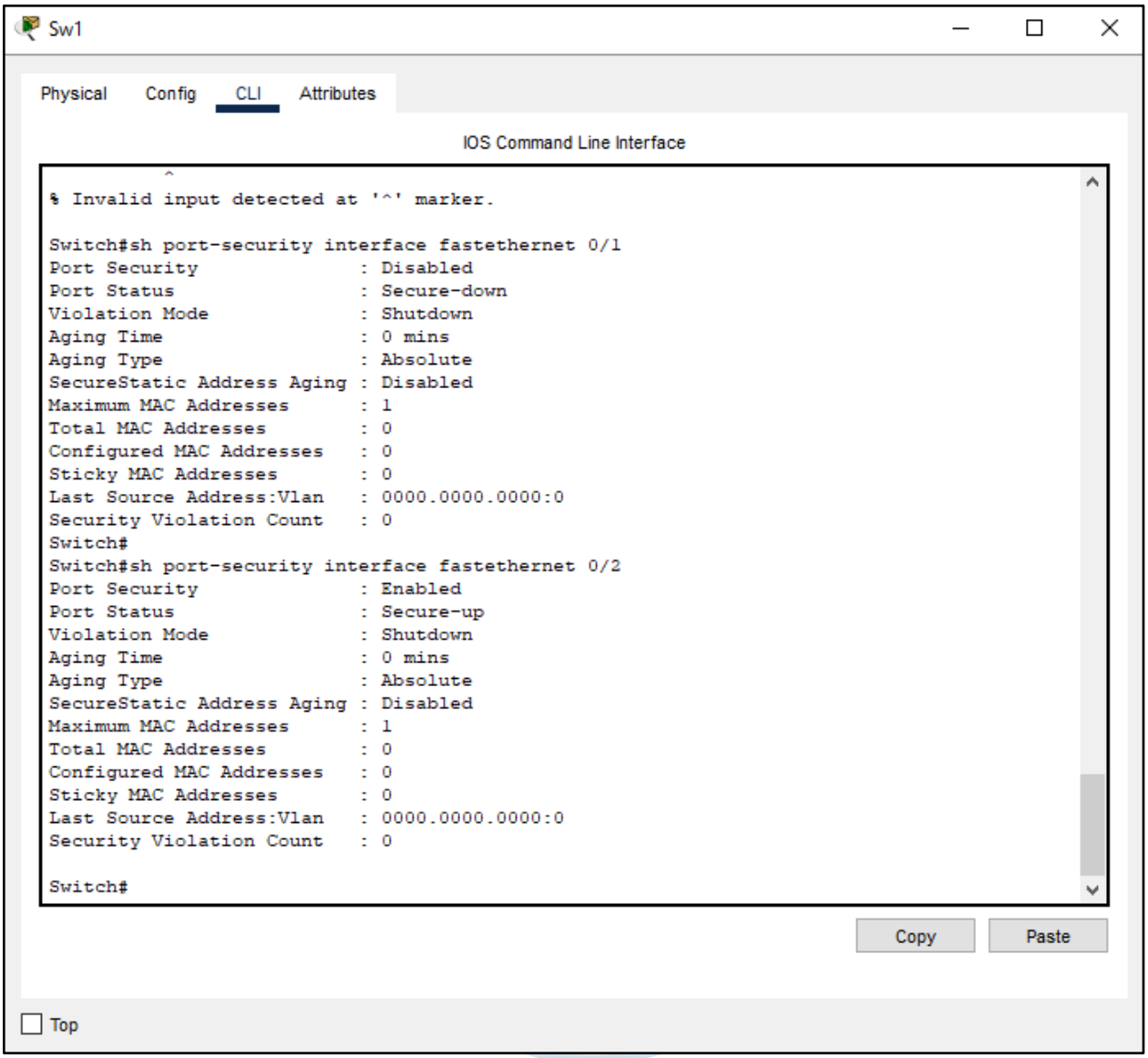

Figure 11: Displaying port security status

The port security state of the switch's FastEthernet interfaces 0/1 and 0/2 is shown in Figure 11. While interface 0/2 is secure-up and has port security enabled, interface 0/1 displays port security as deactivated and in a secure-down state. Strict security enforcement is ensured by the violation mode of shutdown on both interfaces.

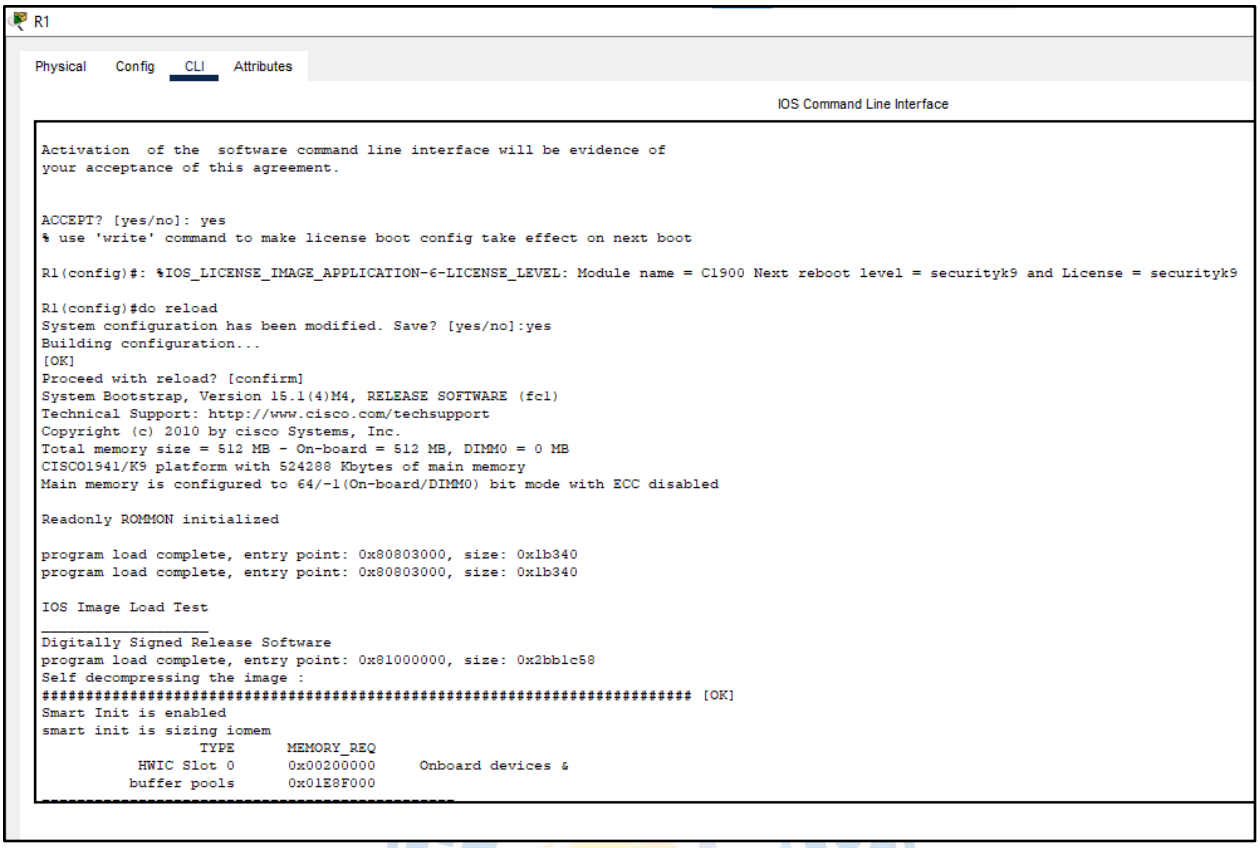

Figure 12: Technology-package securityk9 for IPS implementation

The use of the "securityk9" technology package for Intrusion Prevention System (IPS) capabilities is shown in Figure 12. This package improves the switch's security features, making it more capable of identifying and thwarting possible network attacks and providing strong network defence.

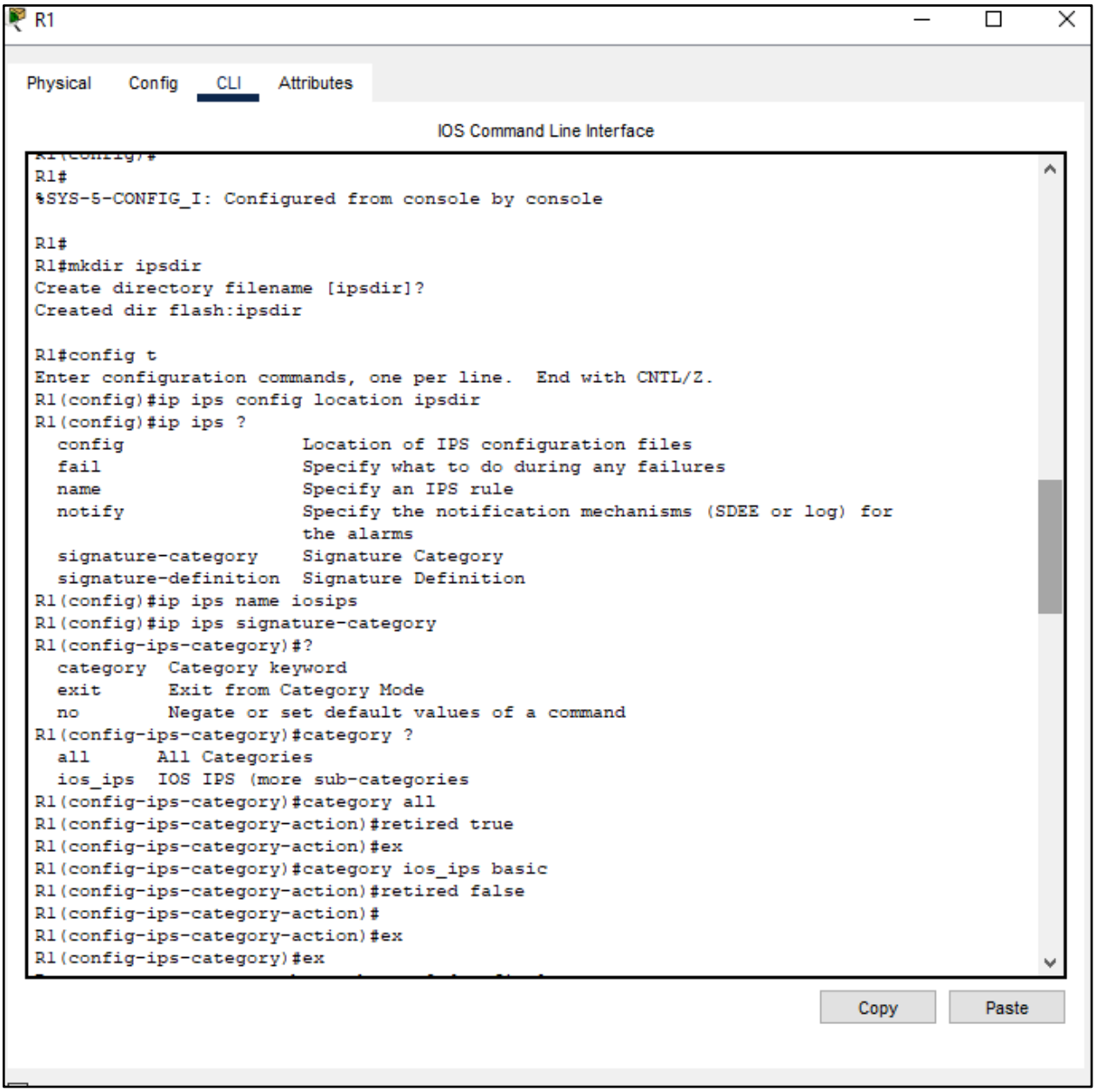

Figure 13: IPS implementation

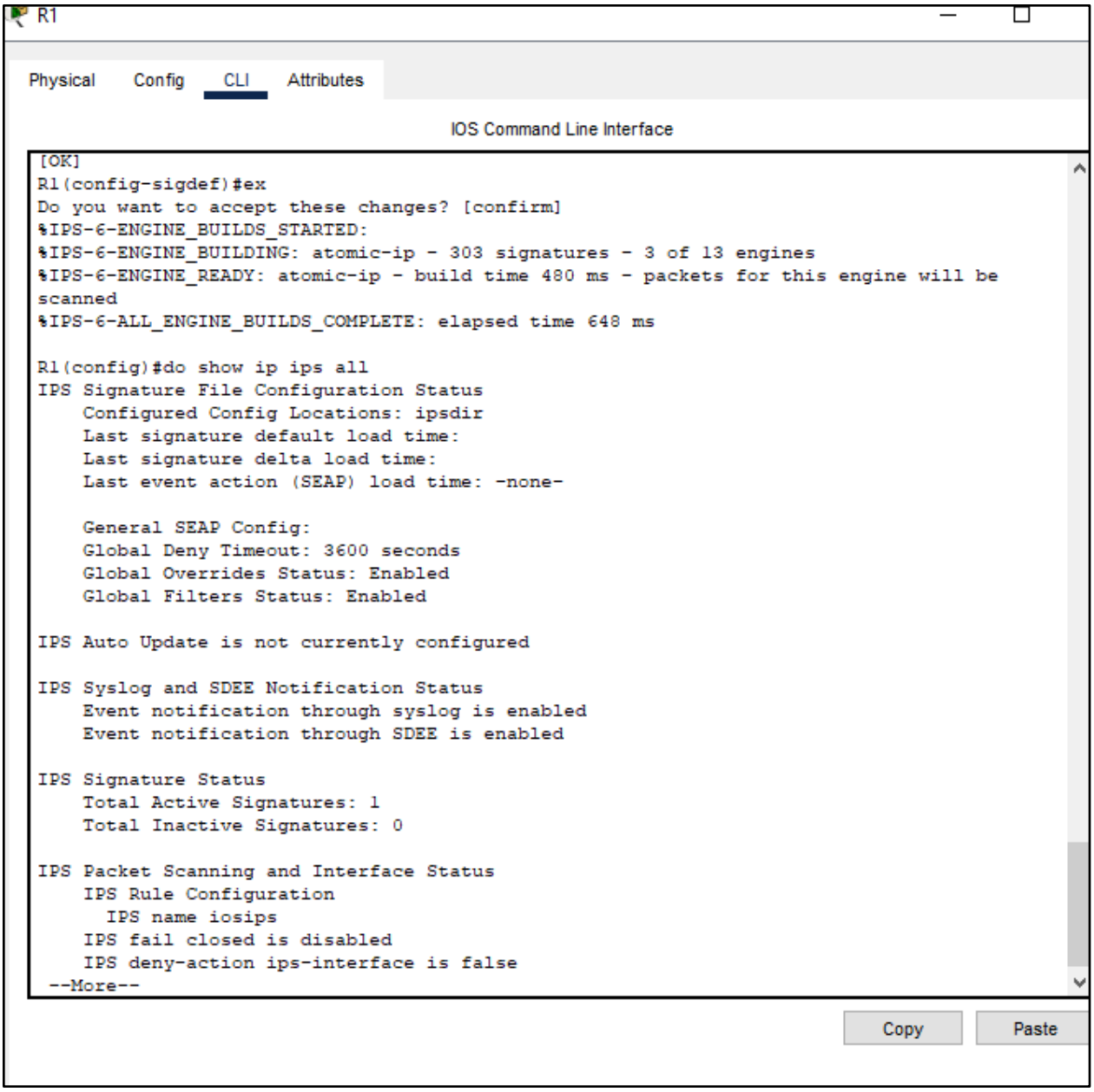

Figure 14: Displaying IPS status

The configuration of an Intrusion Prevention System (IPS) and its status on a router is shown in the above figures. In order to effectively manage network security, it entails establishing a directory called "ipsdiz" for IPS configuration files, configuring IPS location, defining IPS rules, defining alerting methods, and classifying IPS signatures.

Implementation of wireless network design

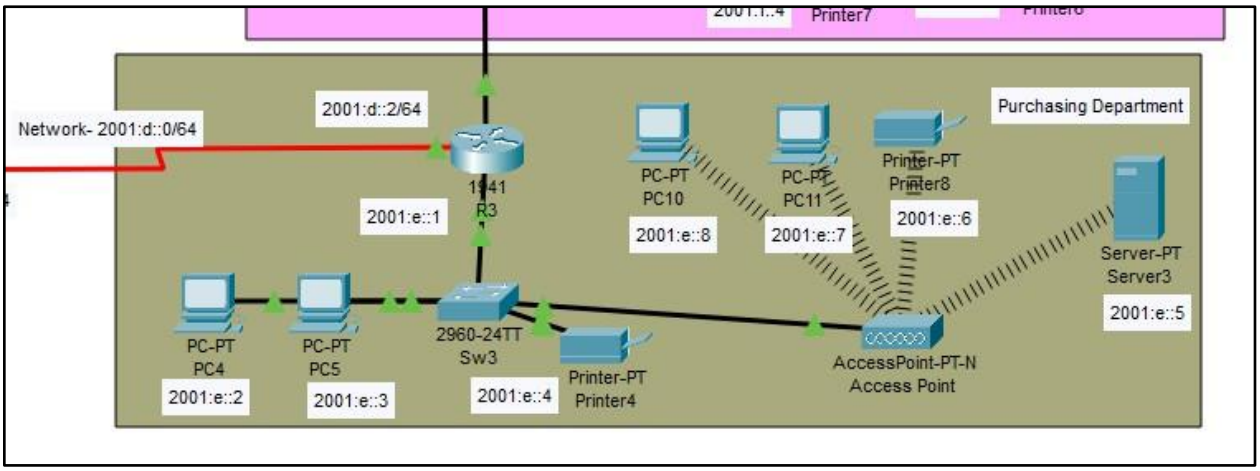

Figure 15: WSN implementation on the Purchasing department

The deployment of a Wireless Sensor Network (WSN) in the purchasing department is shown in Figure 15. It consists of IPv6-configured PCs, printers, servers, and access points, among other devices (Kumar *et al.* 2020). For network isolation, VLAN segmentation (2001) is used, and device connection is managed by a central switch (2980-247).

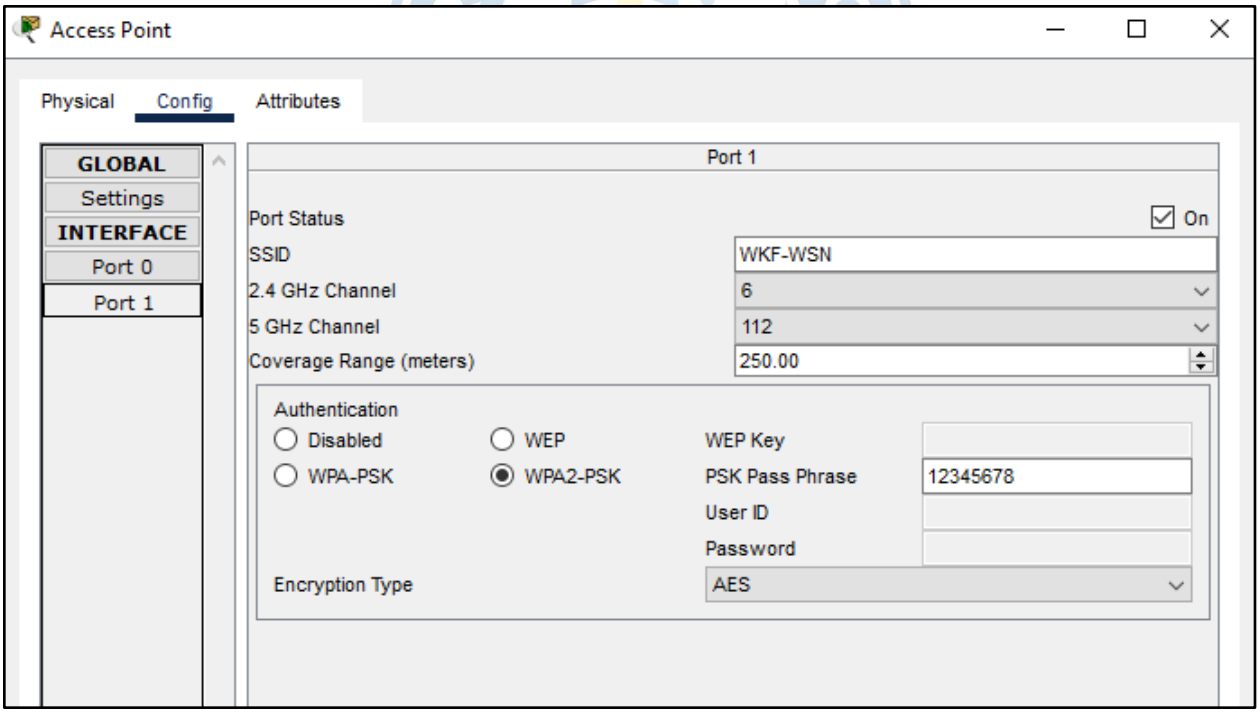

Figure 16: Access point configuration

Figure 16 describes an access point's setup settings in detail, including global parameters and Port 1 properties. The access point has a 250-meter coverage range and runs on both 2.4 GHz

and 5 GHz frequencies. It uses a PSK passphrase for authentication and WPA2-PSK encryption for secure wireless communication.

Figure 17: Wireless connectivity between PC and access point

Figure 17 below depicts the networking details between the Access Point and the PCIO device wirelessly. "HX" PCIO has provided the evolution of a Wireless-N Notebook Adapter to connect to a "WKF-WSN" network. A network is running in a number of wireless gateways as the adapter's MAC address is already there. Nay and the converter is now activated and good, and the wireless connection has been established.

Wireless Network Security issues and mitigation

There are multiple challenges to overcome when it comes to the security of wireless networks, especially in environments where essential information relating to finances is being transmitted. Measures of prevention gain so much power to find out and correct any detected weaknesses,

and prevent the network from any harm. Network intrusion, data hijacking, and unauthorized logins are the most common issues to security. Achieving a secure transmission of data over the wireless medium is the main reason for the use of powerful encryption algorithms such as WPA2-PSK. It would in turn cut off the chances of eavesdropping that leads to the stealing of sensitive information.

Also, VLAN technology is very useful in eliminating "security holes", which represent one of the causes of such malicious attacks, especially where are critical network areas. Certificate-based authentication in this way is considered as the strongest authentication mechanism to implement the granular level of access control and limit the unauthorized users away from the network. To strengthen network security posture, conducting routine security audits as well as monitoring network traffic patterns can also effectively identify and thwart security problems.

Discussion of the backbone network

Effective data transmission across the organization is made possible by the backbone network, which acts as the fundamental infrastructure linking different network segments (Dolgui *et al.* 2020). The intervening network is often deployed and is built of fibre optics or high-capacity switches for consistent communications and minimal latency control. In the existing condition the backbone network system serves as the spine that would connect the critical devices of servers, routers, switches, access points, etc. with different departments or trading floors. Efficient functioning of the business system, fast trading, and ensuring connectivity to the crucial internet services including email, banking system, and applications related to the trading floor of the exchange such as execution system, order booking application, or the one for stock positions stuffing mostly depends on them (Zhang *et al.* 2022). As such, capacity of an organization's productivity and management highly depends on excellent backbone which connect infrastructure components.

Discussion of WAN protocol

Regional offices and other geographically scattered sites are connected to the core network infrastructure using the Wide Area Network (WAN) protocol. London's trading floor along with the regional hubs in Birmingham, Manchester, and Edinburgh are apt in this case as they rely on WAN connections to share data and to keep in touch with each other (Nasir *et al.* 2020). It is crucial to select a safe and reliable protocol like MPLS or VPN to ensure traffic is secure from interception and performance levels are met for an increase in business and traffic. Additionally,

in the context of WAN efficiency and protecting really important data that is traveling on the network, factors such as allowing bandwidth, QoS, and encryption measures are also very important.

Discussion of Data Link layer and wireless protocols

Reliable data transfer between local network segments is ensured by the Data Link layer, which acts as a bridge between the network protocols and the physical network hardware (Mohammad *et al.* 2021). The Data Link layer as Protocols like Ethernet for wired connections and Wi-Fi for wireless connections involves regulating data structure, transmitting, as well as receiving the data inside the network that is being discussed. This can be accomplished through the inclusion of the standards of communication protocol for wireless communication function, which includes channel access, authentication, and security, alongside technologies like IEEE 802.11 protocol (Wi-Fi) which guarantees an efficient and secure transfer of data between devices (You *et al.* 2020). Provisioning standards for a handshake, synchronization as well as connection maintenance necessitate the use of Data Links and wireless protocols; this guarantees the optimum performance of all networks.

Testing and validation

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Pe
	Successful	PC0	Email Server1	ICMPv6		0.000	
	Successful	PC0	Printer1	ICMPv6		0.000	
	Successful	PC3	PC2	ICMPv6		0.000	
	Successful	PC1	PC4	ICMPv6		0.000	
	Successful	PC4	PC10	ICMPv6		0.000	
	Successful	PC4	Printer4	ICMPv6		0.000	
	Successful	PC7	Printer7	ICMPv6		0.000	
	Successful	PC7	PC6	ICMPv6		0.000	
	Successful	PC1	PC4	ICMPv6		0.000	
	Successful	PC1	PC3	ICMPv6		0.000	
	Successful	PC1	PC6	ICMPv6		0.000	
	Failed	PC6	PC11	ICMPv6		0.000	
	Successful	PC6	PC3	ICMPv6		0.000	
	Successful	PC6	PC10	ICMPv6		0.000	

Figure 18: PDU List

A PDU (Protocol Data Unit) list pane is shown in Figure 18, which describes network communication between several sources and destinations. Similarly to the time and the colour-designated statuses of execution, it would list the type of protocol (ICMPv6). Certainly, by using the list, can monitor traffic, to ensure the success and failure of the transmission, and also the diagnosis of connectivity problems.

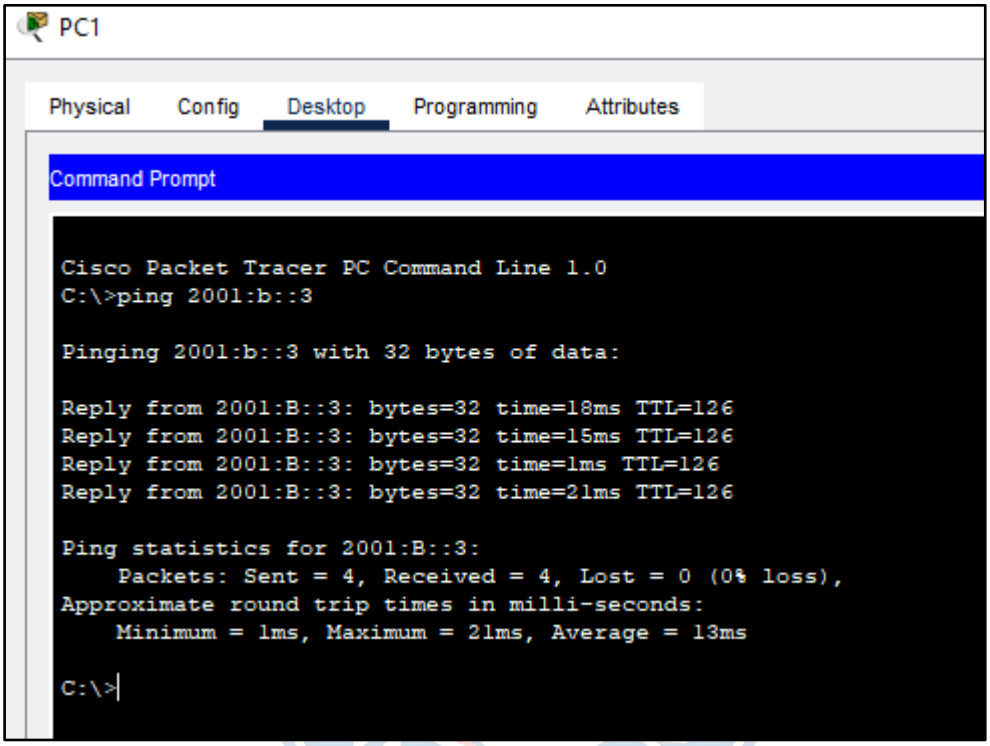

Figure 19: Ping test between the trading floor main office and the finance department

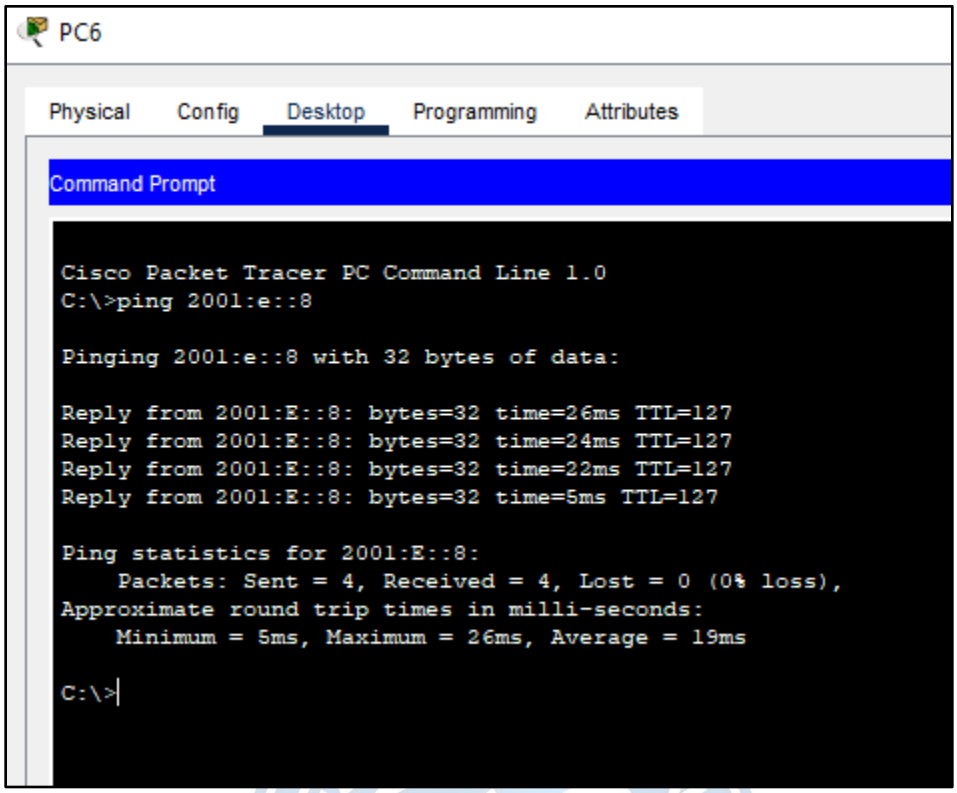

Figure 20: Ping test between Purchasing and payroll department

Ping tests between the finance department and the trading floor main office are shown in Figure 19, where the round-trip timings range from 1 to 26 Ms, suggesting little packet loss and effective communication. Also, it comes through that in Figure 20 ping tests between payroll and purchasing departments are successful, besides exhibiting steady round-trip speeds and a slight amount of packet loss suggesting communication continuity between different network segments.

Conclusion

UKF's network architecture and deployment demonstrate a strong infrastructure suited to high-performance trading environments' requirements. Integration of modern technologies ensures safe data transmission, strong network reliability, and proactive security managed by humans or machines. Illustrations of these technologies are bytecode level, IPv6 setting, and port security. Utilizing of WAN protocols and wireless network protection against security challenges, the organization becomes capable of transforming the network connection between the many departments and trading floors into a higher-level and more effective one. This process promotes the undistorted functioning of the economy as well as sustainable competition.

RESEARCHRYNO
INNOVATIONS
EST. 2018

References

Dolgui, A., Ivanov, D. and Sokolov, B., 2020. Reconfigurable supply chain: The X-network. International Journal of Production Research, 58(13), pp.4138-4163.

Hou, Q., Zhou, D. and Feng, J., 2021. Coordinate attention for efficient mobile network design. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 13713-13722).

Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V. and Hossain, E., 2020. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE access, 8, pp.118433-118471.

Mohammad, A.S.Y., Tahseen, A.J.A., Sotnik, S. and Lyashenko, V., 2021. Neural networks as a tool for pattern recognition of fasteners.

Nasir, S., Al-Qaraawi, S. and Croock, M., 2020. Design and implementation a network mobile application for plants shopping center using QR code. International Journal of Electrical & Computer Engineering (2088-8708), 10(6).

Umoga, U.J., Sodiya, E.O., Ugwuanyi, E.D., Jacks, B.S., Lottu, O.A., Daraojimba, O.D. and Obaigbena, A., 2024. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Scientia Advanced Research and Reviews, 10(1), pp.368-378.

You, J., Ying, Z. and Leskovec, J., 2020. Design space for graph neural networks. Advances in Neural Information Processing Systems, 33, pp.17009-17021.

Zhang, H., Wu, C., Zhang, Z., Zhu, Y., Lin, H., Zhang, Z., Sun, Y., He, T., Mueller, J., Manmatha, R. and Li, M., 2022. Resnest: Split-attention networks. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 2736-2746).