

BN 303 Wireless NETWORK AND SECURITY

Design and implementation of secure enterprise wireless network



**Prepared by:**

**Bibek Lamichhane (MIT213769)**

**Sweta Manandhar (MIT213695)**

**Mission Thapa (MIT213624)**

**Gyanendra Gautam (MIT220162)**

**Submitted to:**

**Anuj Nepal**

**Lecturer and Tutor**

Table of Contents

[Introduction 2](#_Toc168263766)

[Ethical implications 2](#_Toc168263767)

[Network design and simulation 4](#_Toc168263768)

[Subnetting 4](#_Toc168263769)

[Determining the Range of Subnetted Networks 4](#_Toc168263770)

[List of IP addresses of routers 5](#_Toc168263771)

[List of IP addresses assigned to East Sydney: 6](#_Toc168263772)

[List of IP addresses assigned to West Sydney: 7](#_Toc168263773)

[Network Schematic 7](#_Toc168263774)

[Analysis of secure enterprise wireless network 8](#_Toc168263775)

[WPA2: 9](#_Toc168263776)

[Radius server: 9](#_Toc168263777)

[Implementation of secure enterprise wireless network (WPA2 and Radius server) 10](#_Toc168263778)

[Testing 12](#_Toc168263779)

[Configuration of East Sydney Switch 14](#_Toc168263780)

[Configuration on WLC of East Sydney 16](#_Toc168263781)

[Configuration on West Sydney Router 18](#_Toc168263782)

[Configuration on West Sydney WLC 21](#_Toc168263783)

[IP Routing 24](#_Toc168263784)

[Verification of END-Devices (Clients) 26](#_Toc168263785)

[Authentication: 28](#_Toc168263786)

[Association: 30](#_Toc168263787)

[Dissociation: 30](#_Toc168263788)

[Testing users and IOT devices. 32](#_Toc168263789)

[Pinging users and IoT devices: 37](#_Toc168263790)

[Conclusion 38](#_Toc168263791)

[References 39](#_Toc168263792)

# 

# Introduction

Wireless networks, which are common in homes, offices, and telecommunications, are computer networks that use Radio Frequency (RF) connections between nodes. They make Wi-Fi extensible in settings with high user coverage by enabling many Wi-Fi devices to connect to a network using an identical Access Point (AP).

They are used to connect users in different locations, including public areas, workplaces, and industrial settings. They serve as the foundation for all contemporary communication systems, enabling anything from small-scale business apps to private correspondence.

There are various technologies using wireless communications for specified ranges.

Wi-Fi Technology: Without the need for cable connections, Wi-Fi technology has become an essential component of modern living, providing flexible and convenient internet access. This widespread utilization has contributed to the development of numerous wireless products and services, enhancing interaction, efficiency, and entertainment in private homes, businesses, and public areas.

Bluetooth Technology: With Bluetooth technology, electronic devices can connect wirelessly to one another over a short distance—typically 10 meters for data transfer and the construction of wireless networks for a variety of applications including smart home automation and wireless audio transmission. Most likely, we frequently use Bluetooth technology to listen to music in the car or to pair wireless headphones with our phone. With the growing popularity of Bluetooth, it is now possible to connect a wide range of devices—including speakers, headphones, computers, tablets, and smartphones—smoothly and conveniently.

Infrared Technology: The television remote control is the most frequent application of infrared communication, but it can also be used for short-range line-of-sight communication between devices that include infrared transmitters and receivers. Even with its limited coverage and line-of-sight constraints infrared communication is still a straightforward and efficient way to send data wirelessly, especially over short distances [1].

# Ethical implications

Design and Implementation of a Secure Enterprise Wireless Network: Ethical Considerations

Multiple ethical issues are involved in the design and implementation of a secure business wireless network. These factors include user privacy, data security, adherence to legal requirements, and wider effects on the environment and society. Investigating these ethical ramifications, this paper identifies major areas of concern and suggests the best methods for resolving them [2].

1. Confidentiality and privacy

User data protection: It is crucial to make sure that private and sensitive data is sufficiently shielded from unwanted access. This entails putting strong access restrictions and encryption technologies in place.

Monitoring and surveillance: Although keeping an eye on network traffic is crucial for security, the right to privacy must be taken into consideration. Notifying users about monitoring procedures and, where necessary, seeking permission are among the ethical issues.

2. Security measures

Data integrity and availability: one of the most important ethical duties is to make sure that data is not altered and is accessible when required. Maintaining trust is aided using robust authentication techniques and redundant systems.

Stopping Unauthorized Access: It’s crucial to use intrusion detection systems, firewalls, and other security measures to stop unauthorized access. But using these technologies ethically means protecting user privacy and making sure that the measures don’t encroach too much.

3. Respect for the Laws and Regulations

Regulatory Compliance: Complying with data protection laws like GDPR, HIPAA, and others is not only required by law but also by morality. Ensuring compliance guarantees the preservation and observation of user rights.

Industry Standards: Maintaining a high degree of security and trust may be achieved by adhering to industry best practices and standards for wireless security, such as WPA3 for Wi-Fi [2].

4. Accountability and Transparency

Clear Communication: It is crucial to inform users of any data gathering procedures and security measures in place in a transparent manner. Providing data gathering procedures and security measures in place in a transparent manner. Providing explicit terms of service and privacy policies is part of this.

Accountability and measured: Ensuring that the network is handled properly and ethically requires the establishment of accountability measures, such as frequent security audits and a point of contact for security-related issues.

5. Effects on Workers and Users

User Education: it is essential to teach and educate staff members on safe procedures and moral network resource use. Users are now better equipped to safeguard their own data and see the value of security precautions.

Employee surveillance: Managing employee surveillance ethically entails striking a balance between the requirement for security and individual privacy. Key factors to consider are minimum intervention and transparent procedures.

# Network design and simulation

# Subnetting

In networking, subnetting is the process of partitioning a big network into more manageable and smaller subnetworks in order to increase security and enhance performance. Subnet masks are used to identify the network and host components of an IP address, making routing and addressing systems more effective. By limiting broadcast domains and separating network traffic, subnetting improves network performance and improves fault isolation and resource usage. In general, subnetting is an essential technique in network architecture that helps to create scalable, secure, and effective network designs.

## Determining the Range of Subnetted Networks

Let us consider the range of the provided network i.e. 10.10.128.0/20.

Here /20 denotes the CIDR notation.

Note: CIDR (Classless Inter-Domain Routing): A simplified technique to represent a subnet mask which identifies the number of binary bits set to a 1 or 0 in a subnet mask.

Considering this network, it doesn’t change the class of the address, so the IP address has Class A network address, however a Class B subnet mask is used [3].

Converting this network into binary:

IP address: 00001010.00001010.10000000.00000000

Subnet Mask: 11111111.11111111.11110000.00000000

In 32 bits, 20 bits are used by network bits so we can only use 12 bits for host networks,

Applying 2^n-2 rule,

Range of IP address: 2^12-2=4094 IP addresses

The first and last IP addresses are used for default network and broadcast network.

Note: All the host bits use 0 bit while network bits use 1 bit.

According to this, the available range of IP addresses are:

IP Address: 10.10.128.0 -10.10.143.255

According to the case study provided,

For 75 users, the number of IP addresses has been reduced to 128 by breaking it into /25 subnets.

## List of IP addresses of routers

|  |  |  |
| --- | --- | --- |
| Routers | IP address and Subnet Masks | Rip protocol |
| ISP | Se0/1/0 - 172.16.72.1  255.255.0.0  Se0/1/1 – 192.168.72.1  255.255.25.0 | 20.0.0.0  192.168.72.0  172.16.72.0 |
| East Sydney | Se0/1/0 – 20.0.0.5  255.255.255.128  Se0/1/1 – 192.168.72.8  255.255.255.0 | 20.0.0.0  192.168.72.0  172.16.72.0 |
| West Sydney | Se0/1/0 – 172.16.72.3  255.255.0.0  Se0/1/1 – 20.0.0.3  255.255.255.128 | 20.0.0.0  192.168.72.0  172.16.72.0 |

### List of IP addresses assigned to East Sydney:

Network address: 10.10.128.0/25.

Subnet Mask: 255.255.255.128

|  |  |  |  |
| --- | --- | --- | --- |
| Departments | Network address | VLAN Assigned | Usable IPs(encapsulated) |
| Radius & IoT Server | 10.10.128.3/25 | N/A | - |
| Eswlc (WLAN controller) | 10.10.128.2/25 | N/A | - |
| Mgmt-PC | 10.10.128.5/25 | 10 | - |
| Admin2 | 10.10.128.11/25 | 20 | 10.10.128.128 -10.10.128.255 |
| Finance2 | 10.10.128.13/25 | 30 | 10.10.129.1 - 10.10.129.128 |
| ARdepartment2 | 10.10.128.12/25 | 40 | 10.10.129.129 - 10.10.129.255 |

### List of IP addresses assigned to West Sydney:

Network address: 20.20.128.0/25.

Subnet Mask: 255.255.255.128

|  |  |  |  |
| --- | --- | --- | --- |
| Departments | Network Address | VLAN Assigned | Usable IPs(encapsulated) |
| Radius & IoT Server 2 | 20.20.128.3/25 | N/A | - |
| Wswlc (WLAN controller) | 20.20.128.2/25 | N/A | - |
| Mgmt-PC2 | 20.20.128.5/25 | 10 | - |
| Admin | 20.20.128.13/25 | 20 | 20.20.128.128 - 20.20.128.255 |
| Finance | 20.20.128.12/25 | 30 | 20.20.129.1 - 20.20.129.128 |
| ARdepartment | 20.20.128.10/25 | 40 | 20.20.129.129 - 20.20.129.255 |

## Network Schematic

Network design was created using Cisco Packet Tracer which consists of all the wired and wireless devices to build a wireless enterprise network.

Devices used:

2 x WLC for East and West Sydney

3 x Routers - ISP, East Router and West Router

2 x Server each for East and West Sydney

2x Switch each for East and West Sydney

2x Management PCs East and West Sydney

6 x Access Point (LAP) 3 each for East and West Sydney

End devices as required.

IOT devices as required.

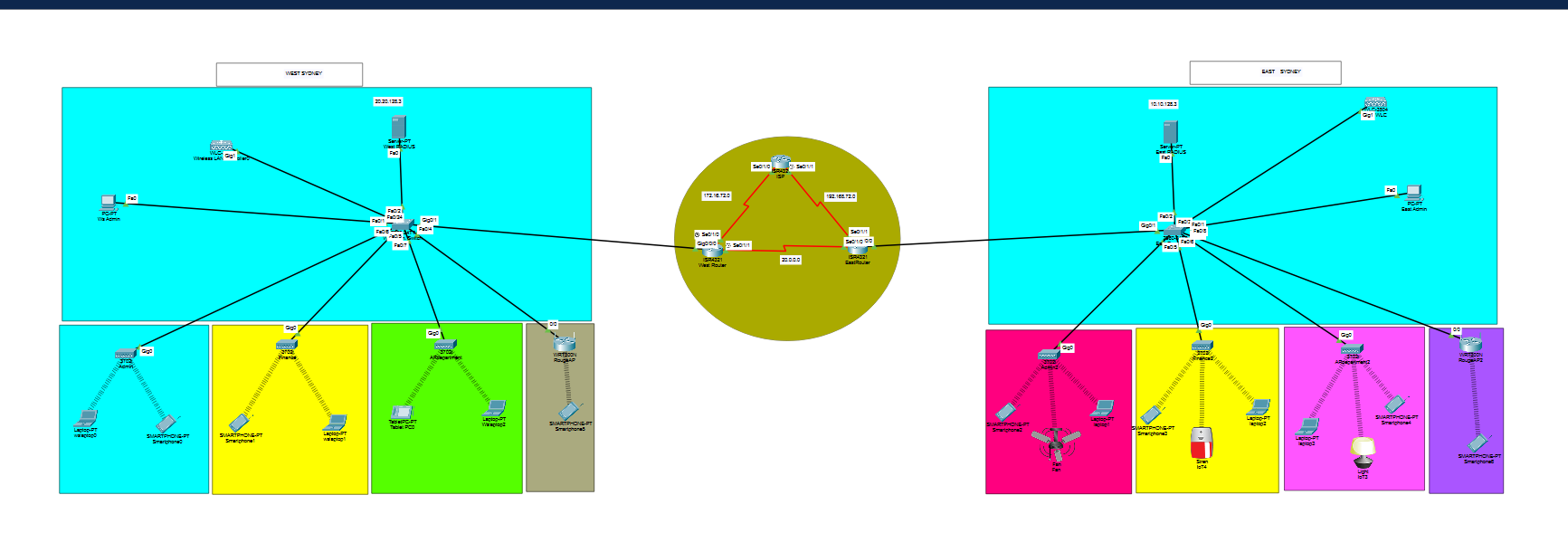


Figure 1: Network design

To design a wireless Network Design for Albert’s School consisting of two branches East and West Sydney, a Packet tracer has been used. After that we added all the devices as per requirements which is mentioned above and can be clearly identified from the given figure. To get connected to each other along with the different branch’s configuration has been done on WLC, Management PC, Routers and Switches.

Finally, the Radius Authentication Server to provide an extra layer of security for the Username and Password has been added and is provided to end devices (clients) and IOT devices for wireless connection. To provide remote access, an IOT account has been created in regards with Radius Authentication Server IP Address. Those credentials are registered into the Remote access of each IOT device. Then the created credentials are logged in from the browser of the clients. After this user can have remote access to the IOT devices and control accordingly.

By following all these methods a wireless enterprise secure network for Albert’s School was created.

# Analysis of secure enterprise wireless network

Considering the CIAAA triad or components, now let's examine the security aspects of a WPA2 and RADIUS server-based secure business wireless network in our network diagram.

## WPA2:

WPA2(Wi-Fi Protected Access2) is a robust security protocol designed to address several aspects of wireless network security. One of the primary features of WPA2 is its commitment to maintaining the secrecy of transmitted data, that is confidentiality. As WPA2 employs strong encryption techniques like advanced encryption standard (AES), sensitive data is shielded from unauthorized access and kept private. Additionally, the protocol employs measures like the message integrity check (MIC), which identifies and prevents unauthorized changes or tampering during transmission, to preserve data integrity. WPA2’s primary concerns are secrecy and integrity, but by limiting unauthorized access to the network and guaranteeing that approved users may still access it, it also indirectly addresses availability [4].

A crucial part of WPA2’s security architecture is its authentication procedure, which offers two options: Enterprise mode using pre-shared key (PSK) and Extensible Authentication Protocol (EAP). While PSK uses a shared passphrase for enhanced authentication, enterprise mode makes use of a RADIUS server. This strong authentication system greatly improves overall security by guaranteeing that only authorized users may access the wireless network Furthermore, by including a RADIUS server to control user access restrictions and choose which resources users may access after authentication, WPA2 goes beyond authentication. By ensuring that verified users have the proper rights, this extra layer of control and protection strengthens the security posture of the wireless network.

## Radius server:

An essential component in improving the security of commercial wireless networks is RADIUS, which complies with the CIAAA (confidentiality, integrity, availability, authentication, and authorization) standards. While authorization and authentication are the main goals of RADIUS, it also helps maintain confidentiality by limiting access to authorized users and protecting private data from unauthorized access. RADIUS exhibits its dedication to integrity management by using secure authentication procedures that thwart efforts at tampering and forgery. To put it simply, RADIUS acts as a vigilant and conscientious security guard, making sure that only authorized users get access to the wireless network and protecting the authentication process using safe protocols [5].

RADIUS improves network availability by centralizing authentication and authorization procedures, reduces the likelihood of unwanted access while guaranteeing that authorized users continuously access network resources. Authentication, which uses a variety of techniques, including EAP, to confirm user identities, is an essential component of RADIUS. Concurrently, the authorization features of RADIUS create access controls, limiting the resources and services that users may interact with. These security protocols, when combined with WPA2, provide a strong foundation that complies with CIAAA guidelines, providing corporate networks with a safe and dependable wireless communication environment.

# Implementation of secure enterprise wireless network (WPA2 and Radius server)

We first created an admin account for WLC using Mgmt-pc.

Using login credentials, we can then configure Wireless LANs.

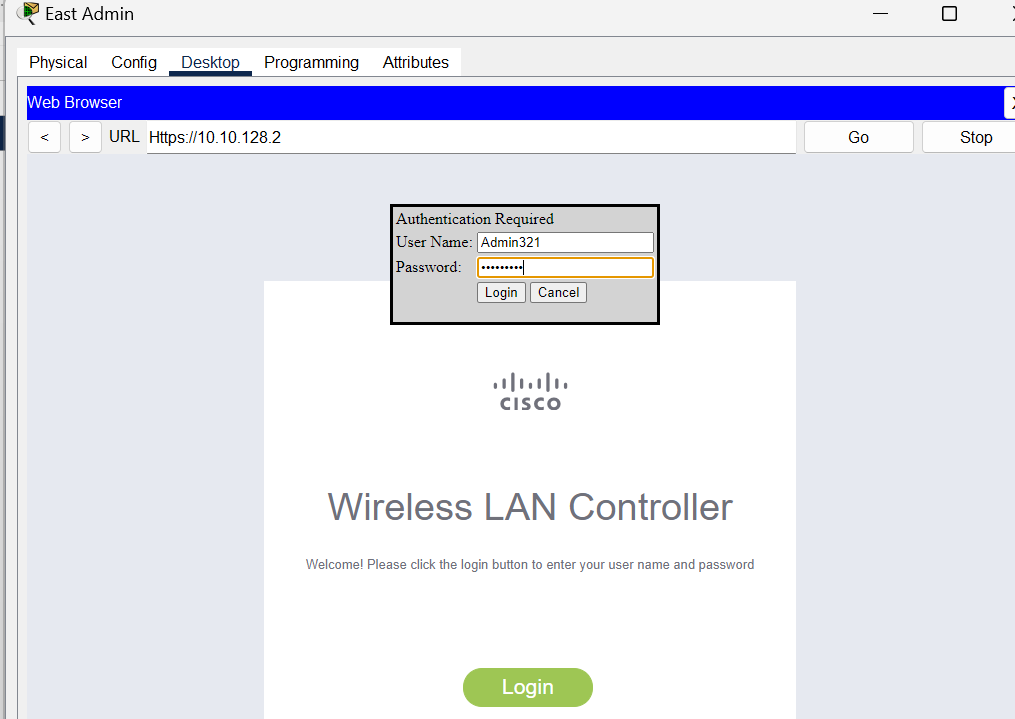


Figure 2: Logging into WLAN

To add a Radius authentication server, we need to go to security, add server IP address and put port number and shared key the same as that of AAA in the server.

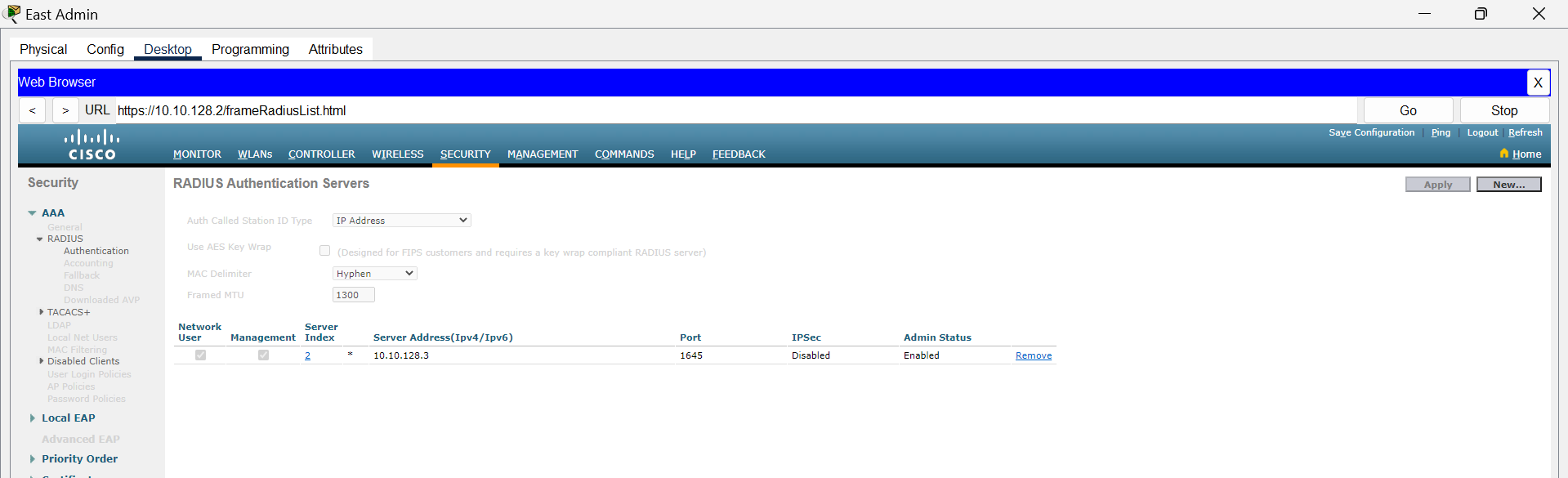


Figure 3: Radius server.

Then from Wlan tab, go to security>layer 2> and select WPA+WPA2, WPA2 policy, WPA2 encryption and 802.1X

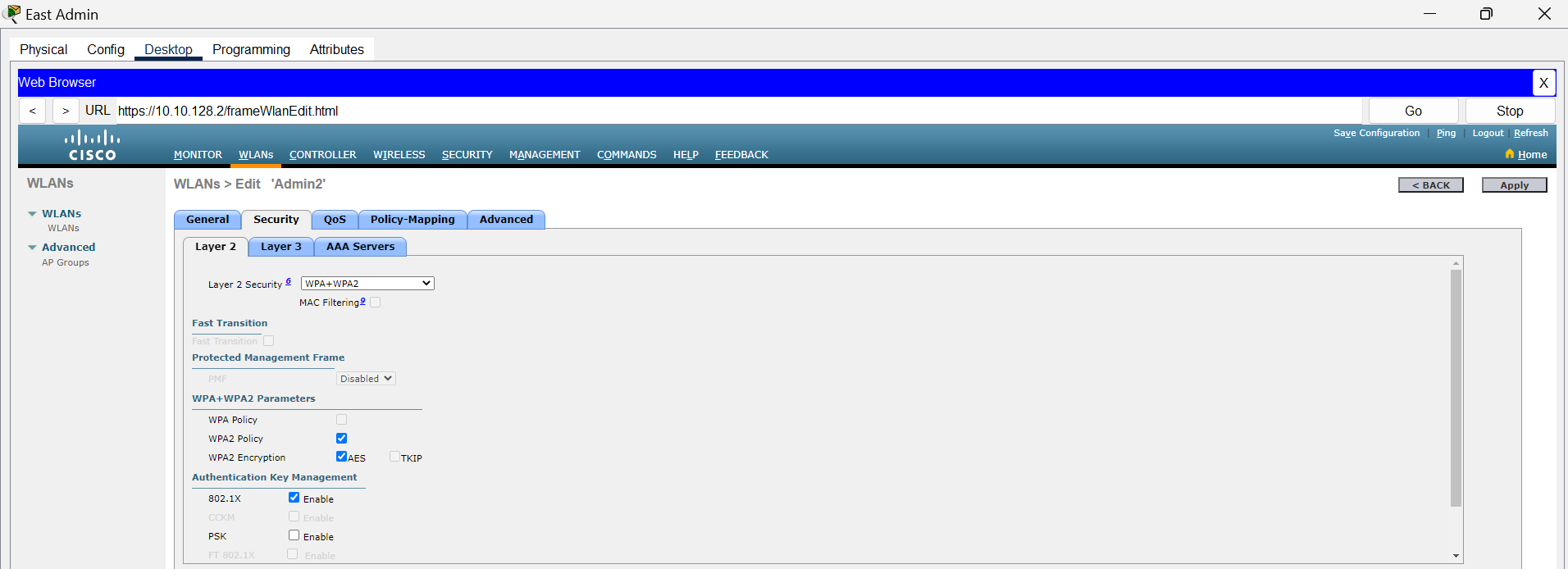


Figure 4: Configuring WLAN security

Then, select the <server ip> option AAA server tab.

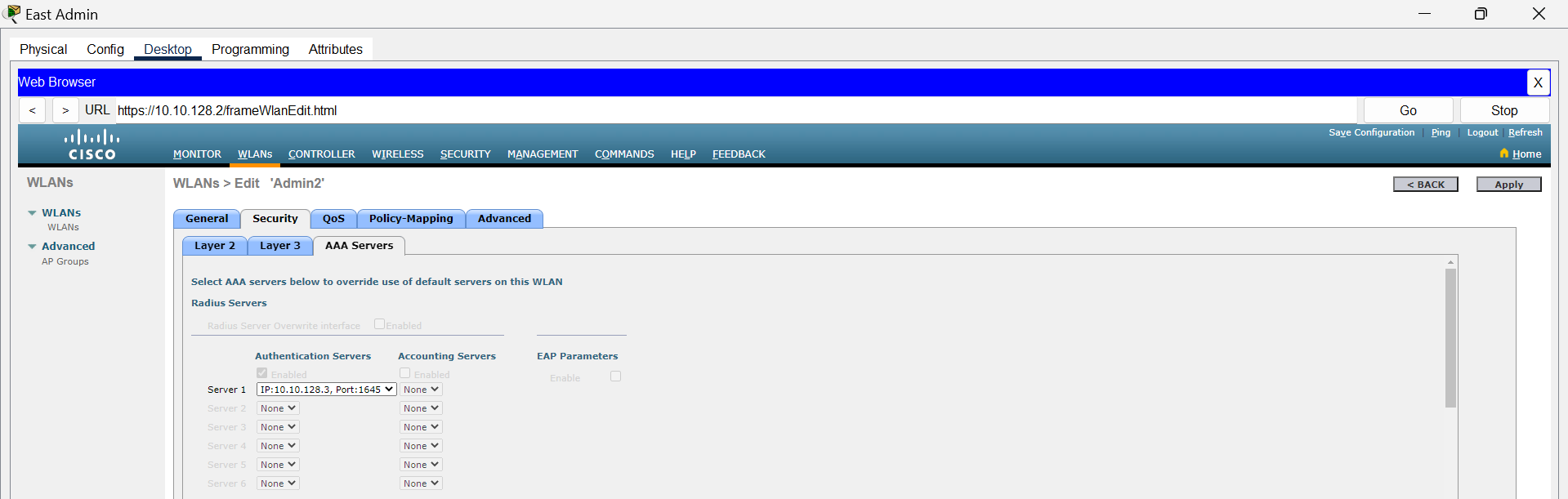


Figure 5: Selecting Radius server and port in AAA server of WLAN

Doing all these make the Radius Authentication Server, WLAN and APs to be used by the users.

# Testing

Configuration Of East Sydney Router

(Assigning IP Address to East Sydney Router)

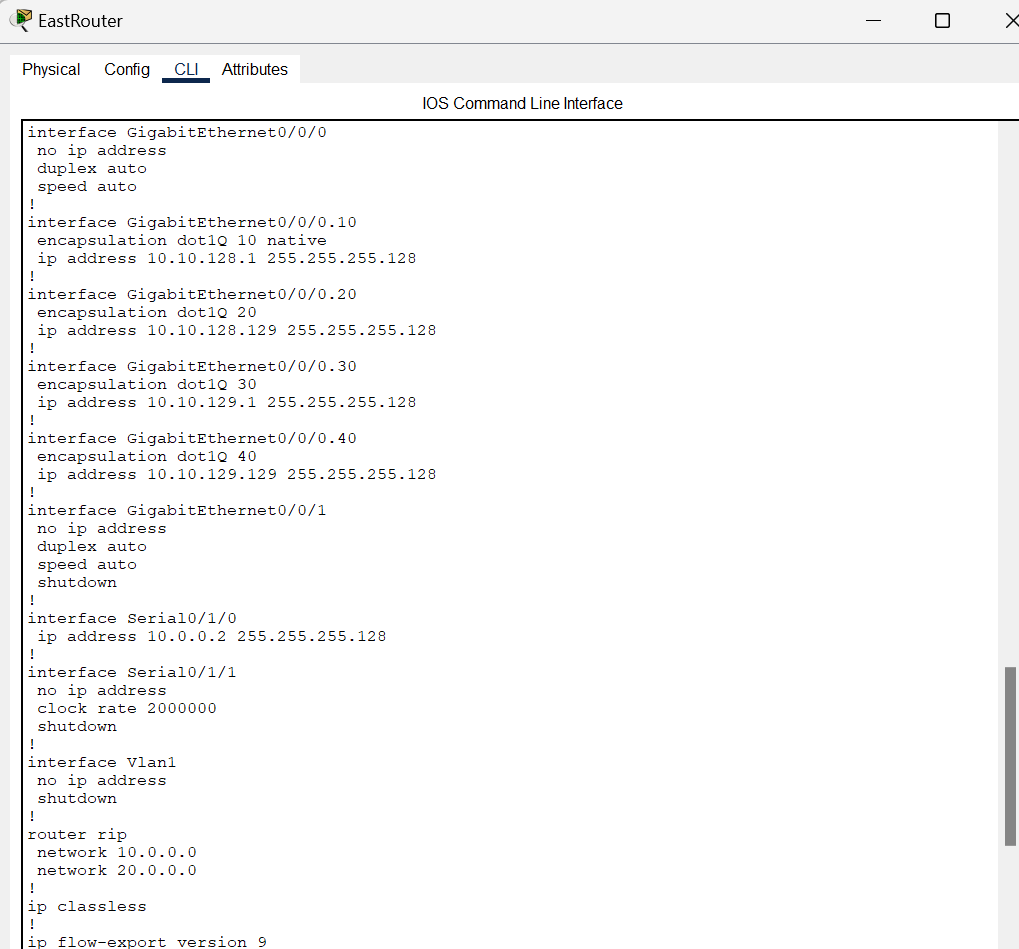


Figure 6: Encapsulating VLANs

Creating IP DHCP Pool for East Sydney

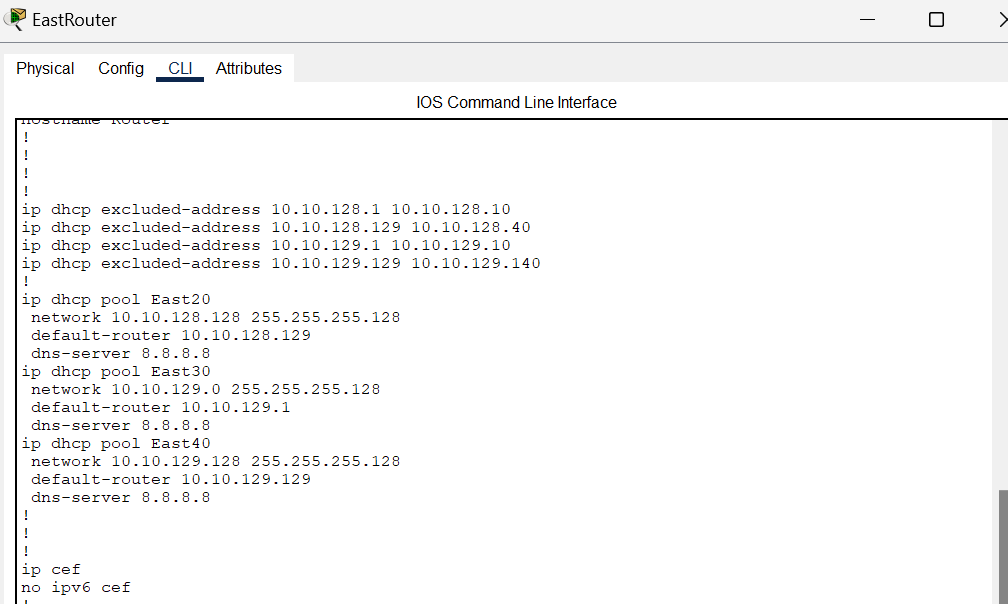


Figure 7: Adding DHCP pool and excluding addresses

## Configuration of East Sydney Switch

Assigning VLANS

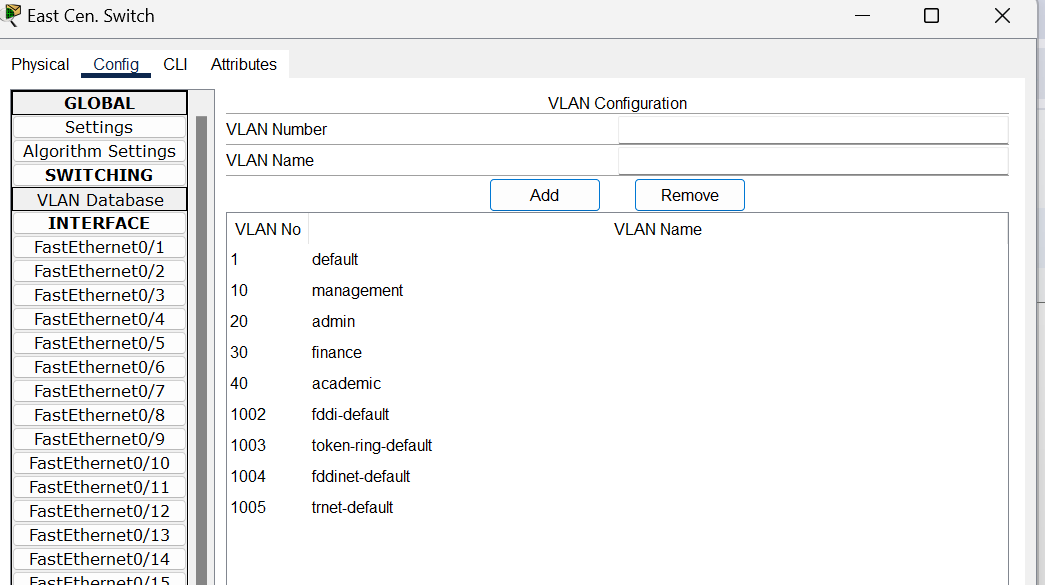


Figure 8: VLANs.

Switchport Trunk in East Sydney

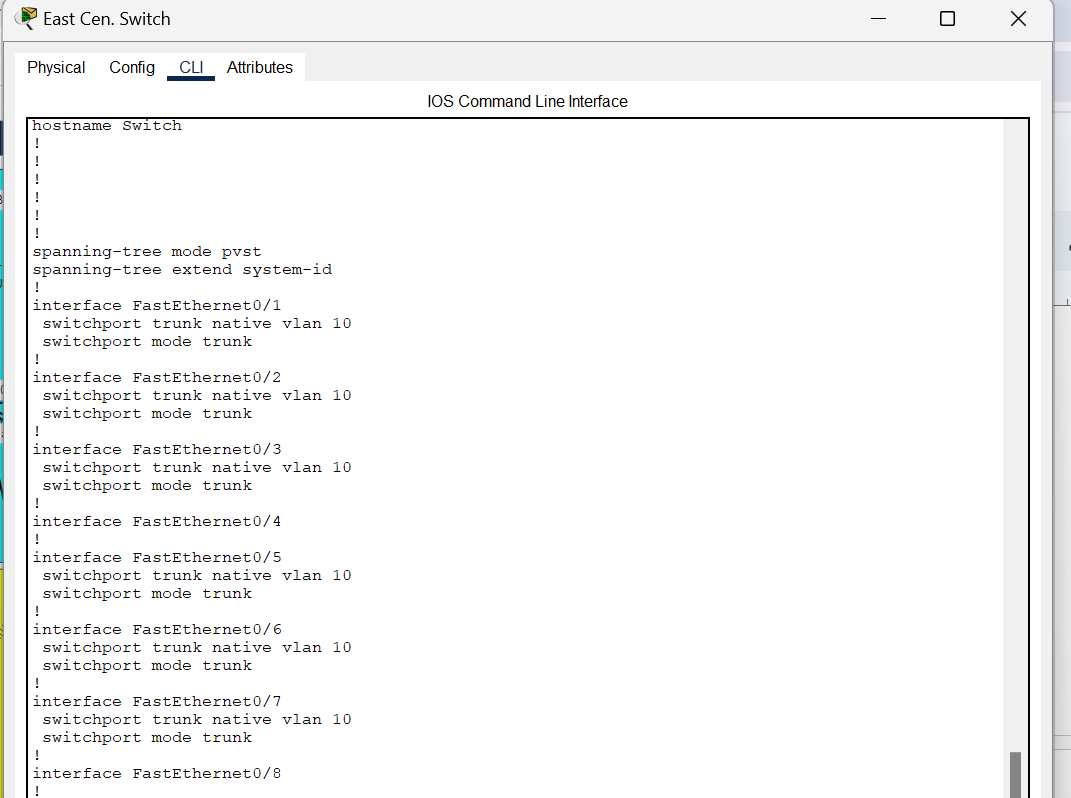


Figure 9:Enabling switchport trunk.

## Configuration on WLC of East Sydney

Setting up WLC Profile for East Sydney

IP Address: 10.10.128.2

Username = Admin321, Password = Password2 of WLC

Creating VLAN Interface in East Sydney WLC

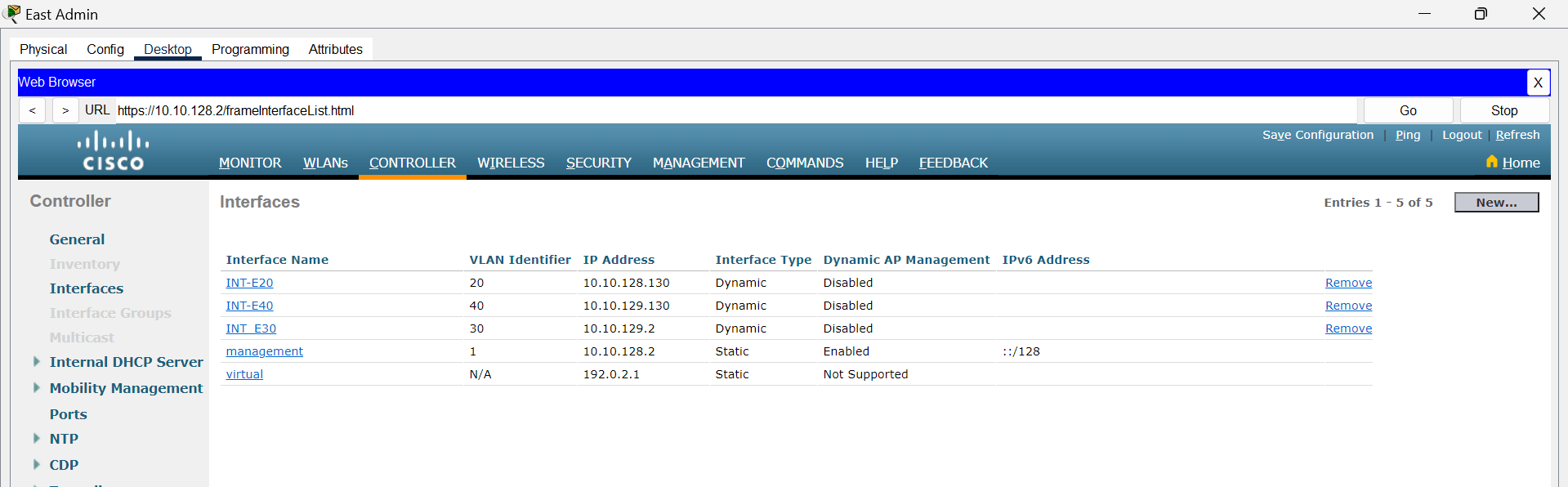


Figure 10: VLAN interfaces.

Creating WLANs and APs on East Sydney WLC respectively.

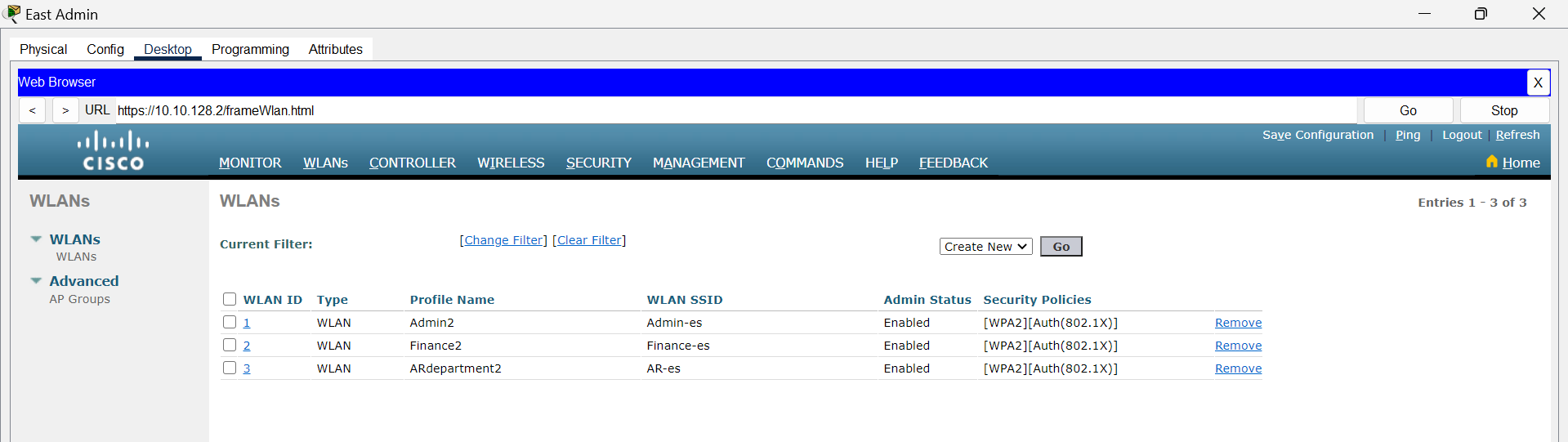


Figure 11: WLAN created in East Sydney

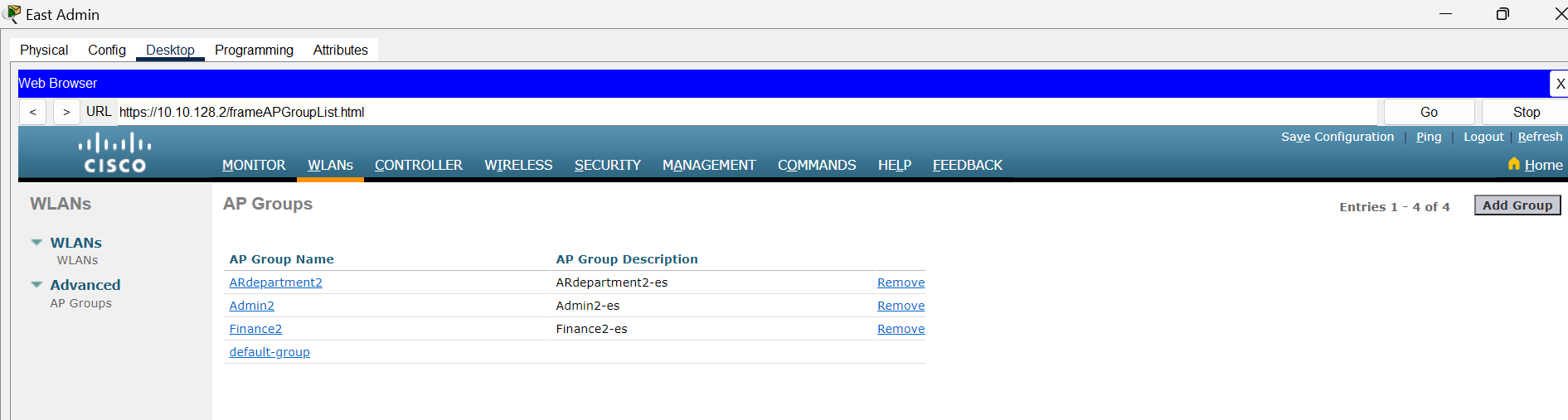


Figure 12: APs created in East Sydney

Creating DHCP Server in East Sydney WLC

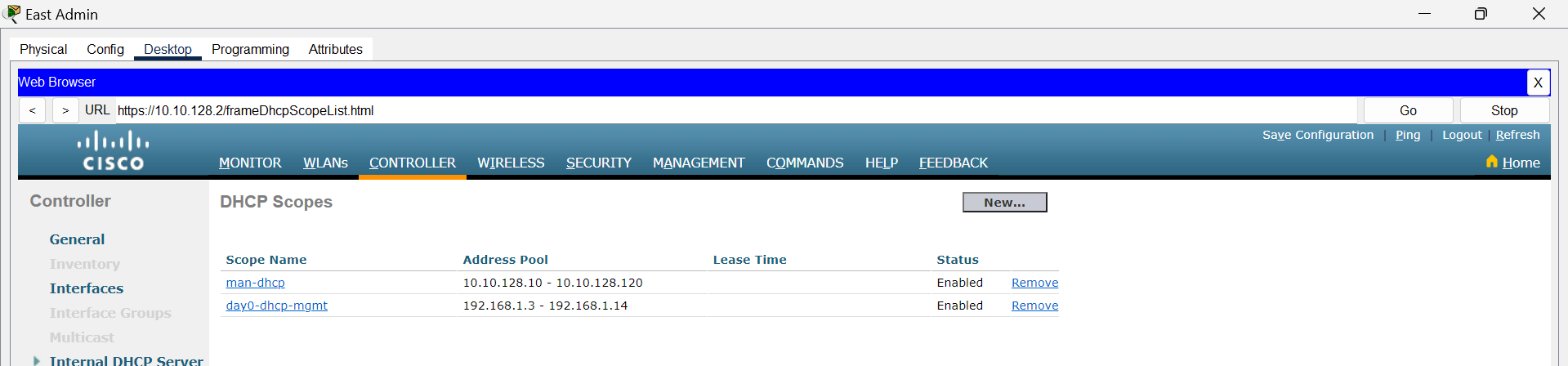


Figure 13: DHCP server.

Assigning DHCP Server to each VLAN

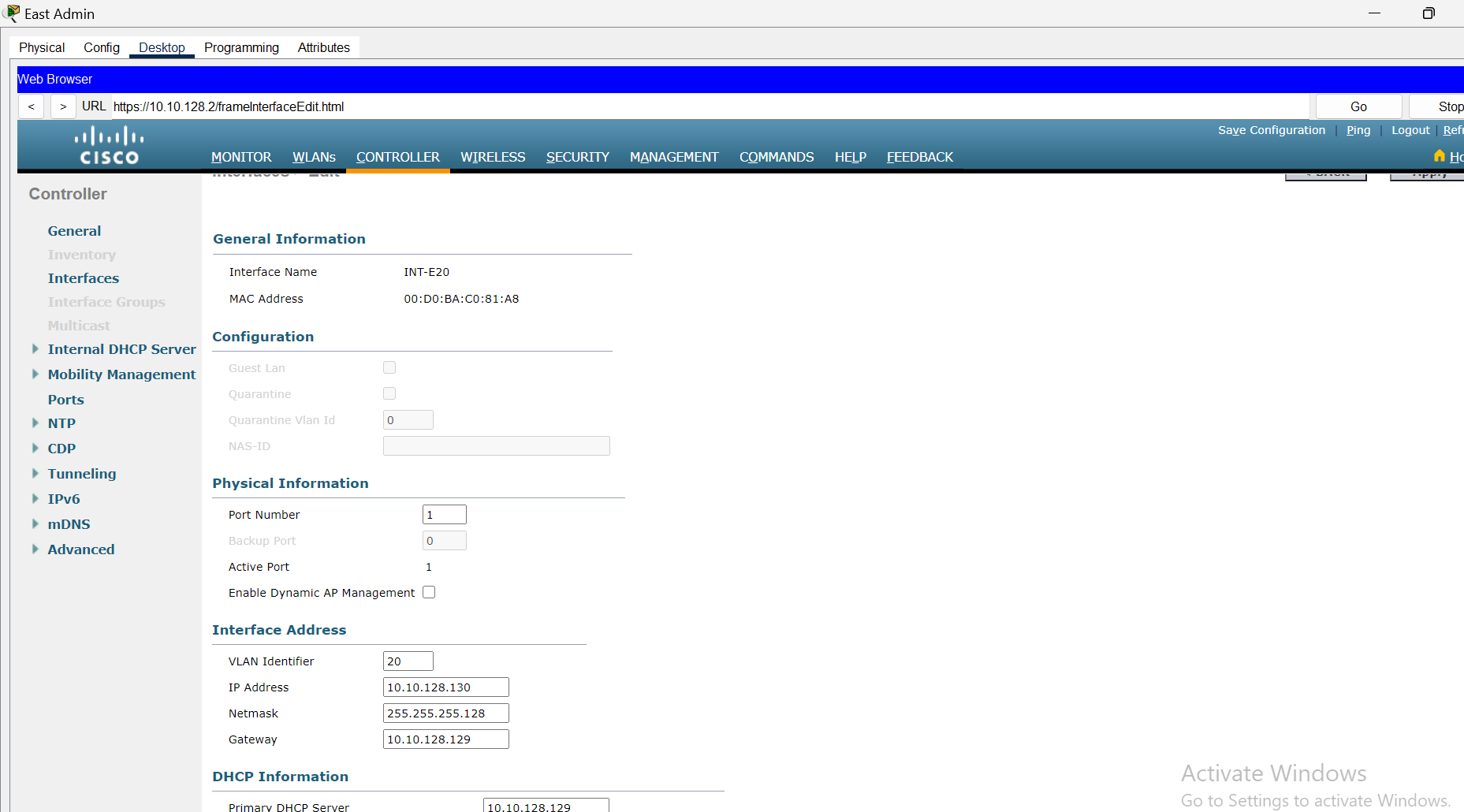


Figure 14: Assigning DHCP

## Configuration on West Sydney Router

Assigning IP Address to West Sydney router

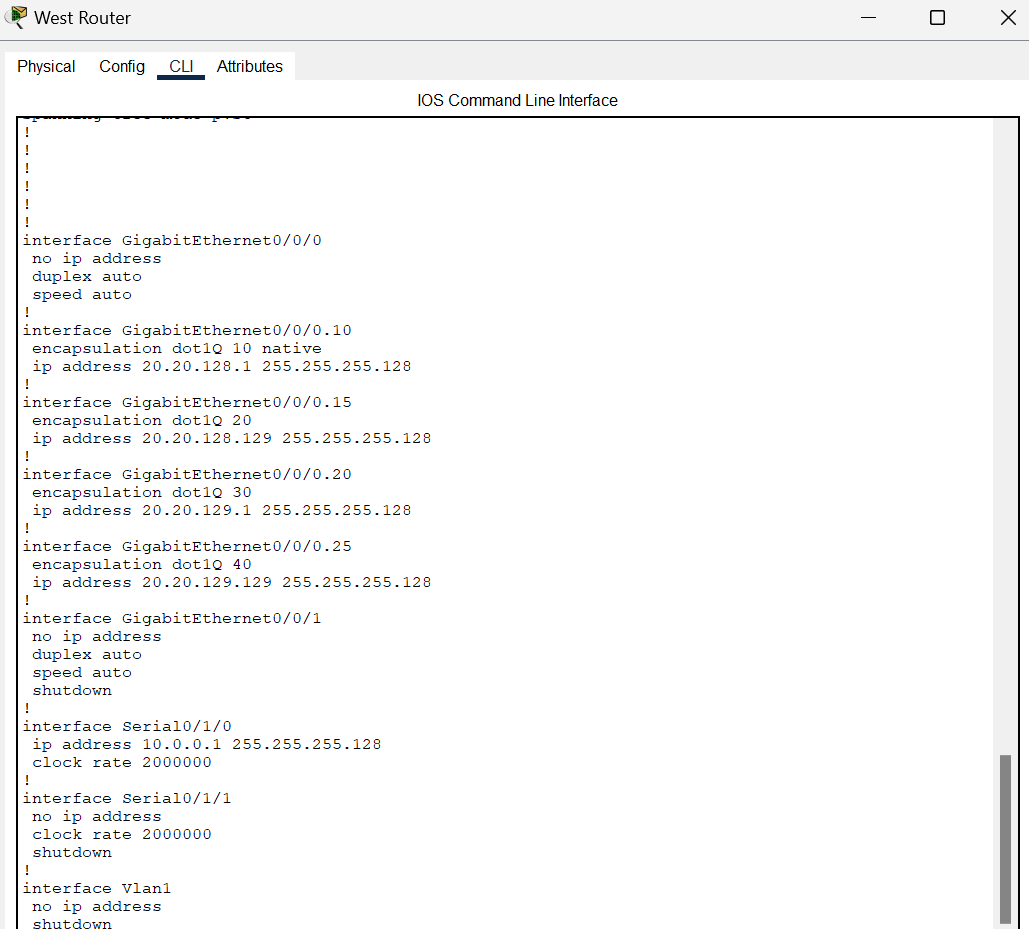


Figure 1: IP address of west Sydney

Creating DHCP Pool and excluded Ip Address for West Sydney Router

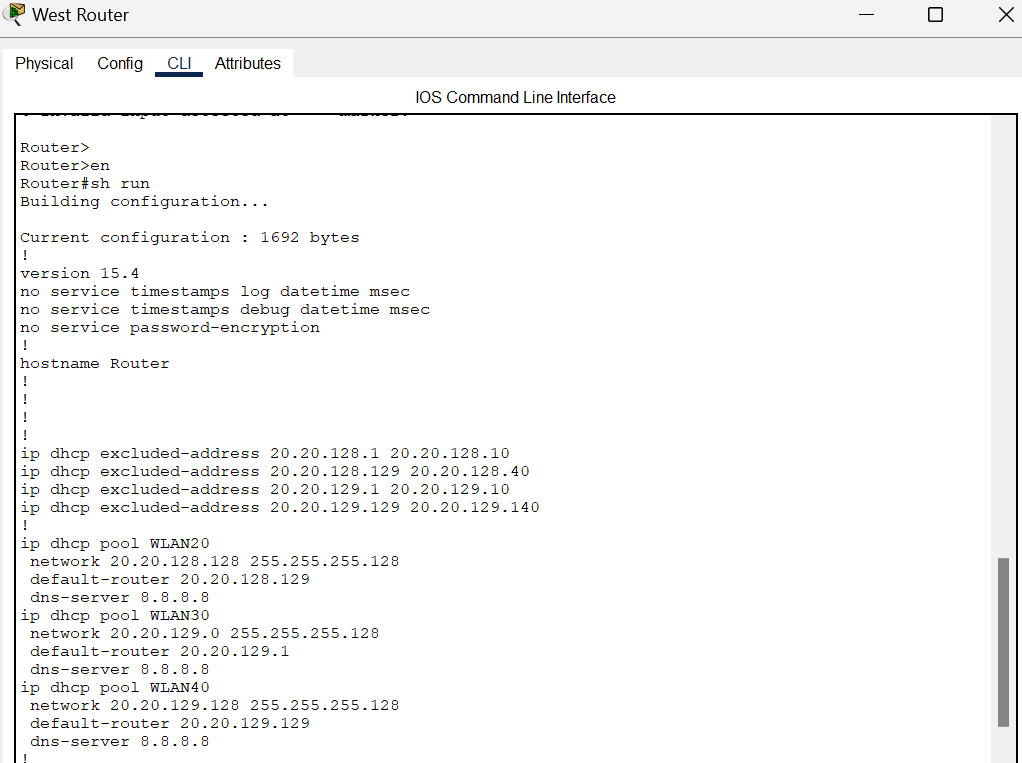


Figure 2: DHCP pool and IP exclusion in router

West Sydney Switch Configuration

Creating trunk on West Sydney

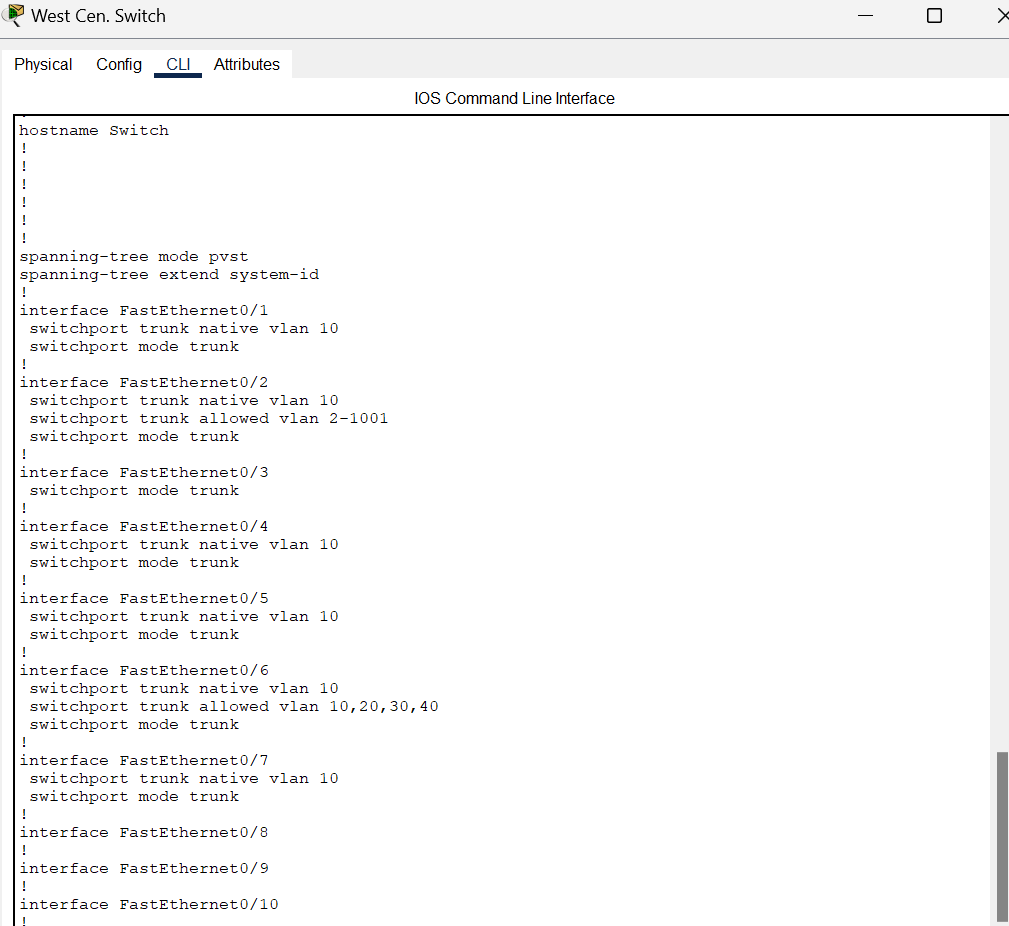


Figure 3:Switchport mode trunk on switch

Created VLAN on West Sydney Switch

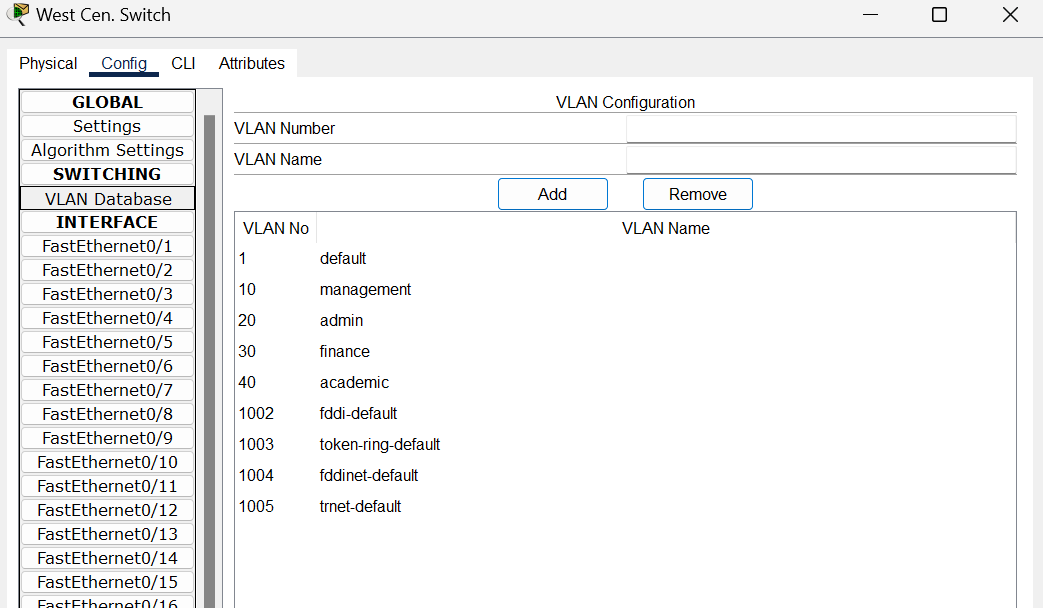


Figure 4: VLAN on Switch

## Configuration on West Sydney WLC

Setting up WLC Profile for West Sydney

IP Address: 20.20.128.2

Username = Admin123 , Password = Password1 of WLC



Figure 5: Login Credentials of West WLC

Creating VLAN Interface in East Sydney WLC

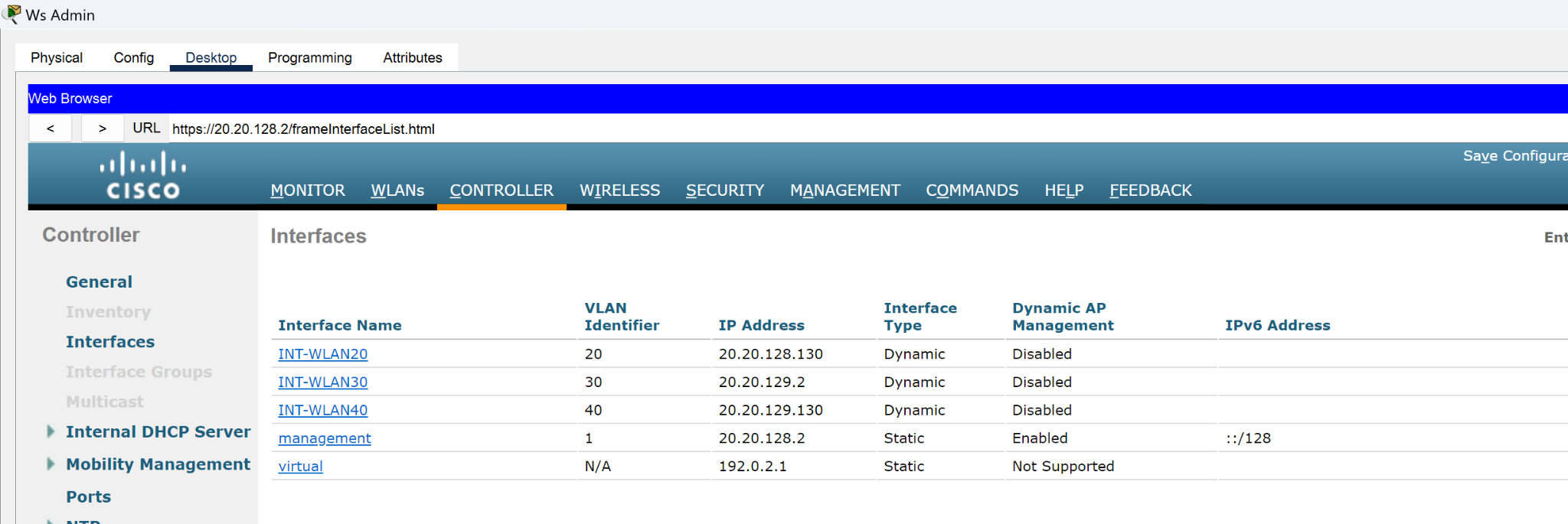


Figure 6: Interfaces of each department on WLC controller

Creating WLANs and APs on West Sydney WLC respectively

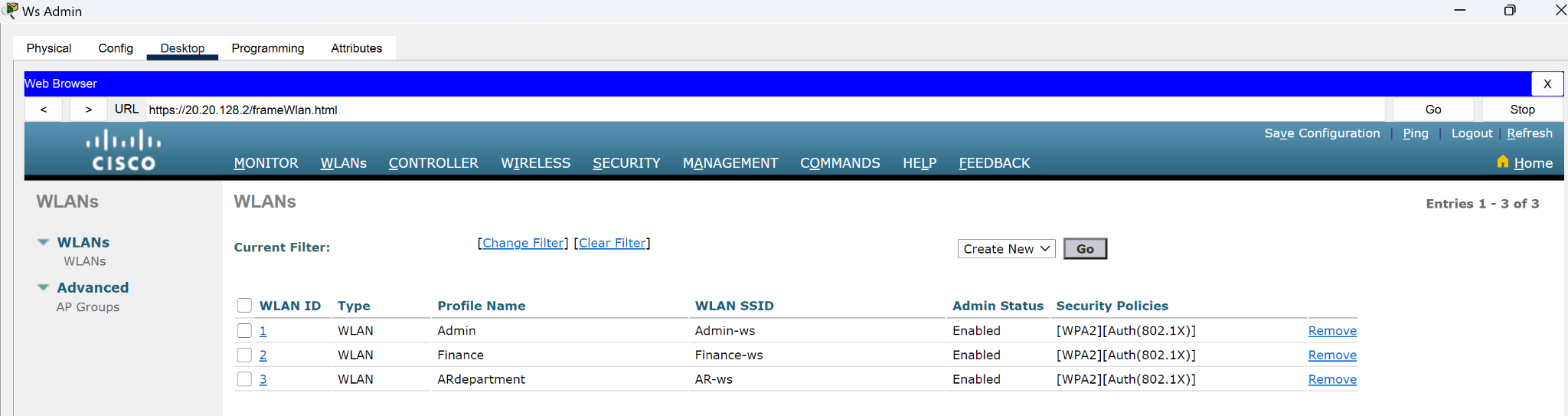


Figure 7: WLANS created in WLC

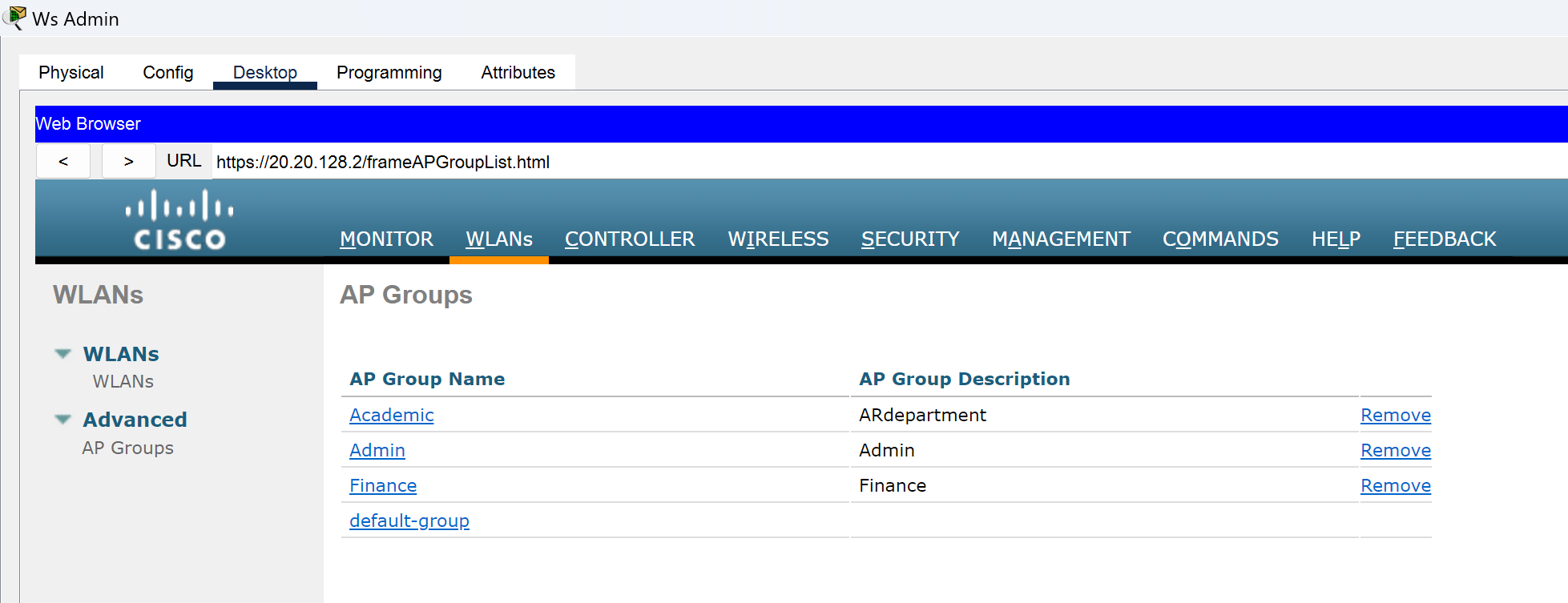


Figure 8: APS of West Albert Branch

Creating DHCP Server in West Sydney WLC

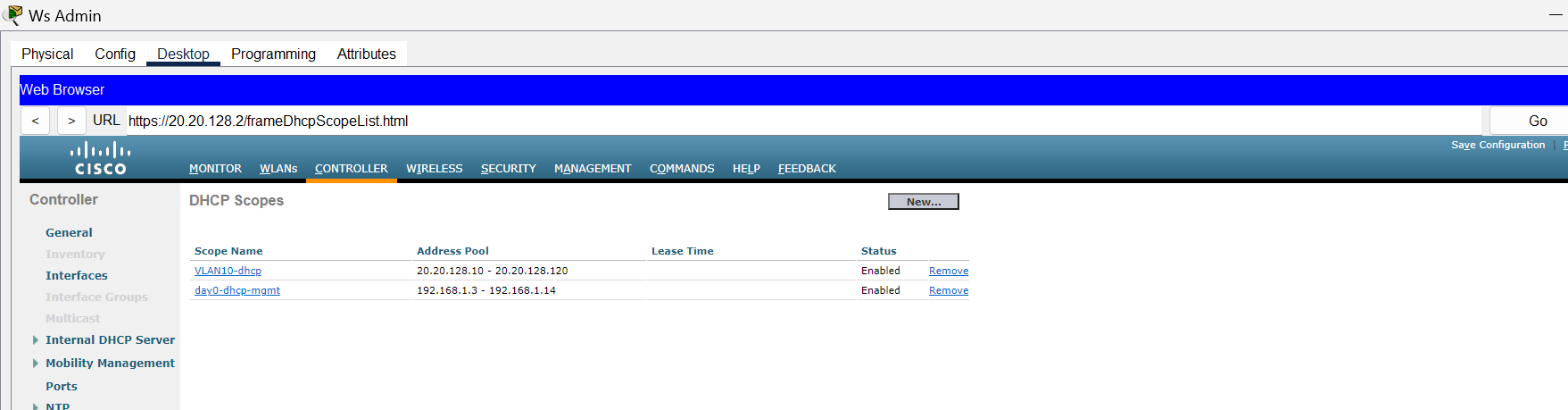


Figure 9: DHCP scope in WLC

Assigning DHCP Server to each VLAN

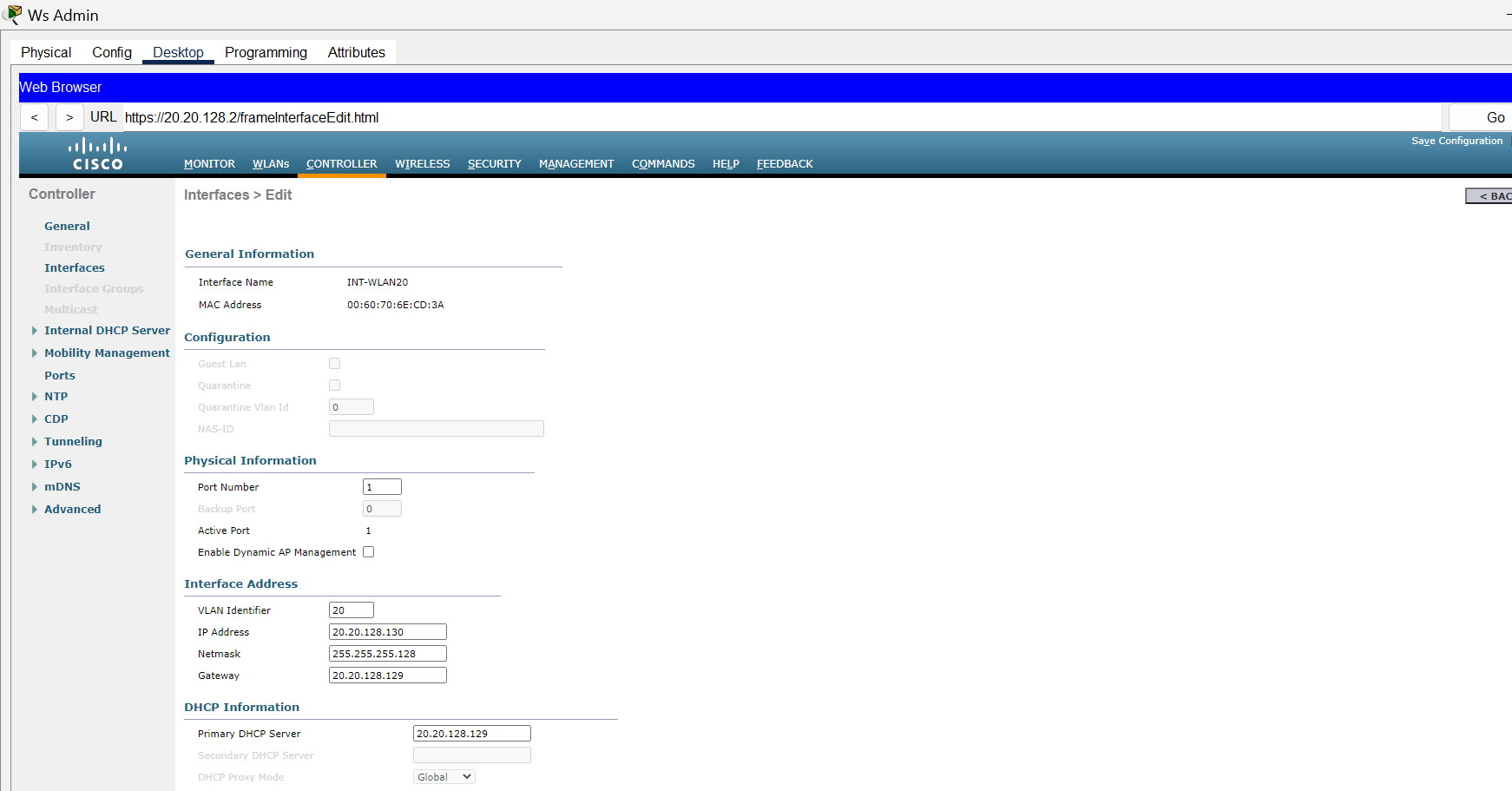


Figure 10:DHCP service pool to each VLAN

## IP Routing

Here, we have used RIP routing as a routing protocol to exchange information and packets among users. RIP is a distance vector protocol which specifies how routers should exchange data while transferring traffic between a network of linked local area networks. Users can employ the router RIP command to instruct the router to enable RIP after IP addresses have been issued to the appropriate computers and router interfaces. Users can then utilize the network command to specify the networks they wish to work with. It is only necessary to specify the networks that are directly connected to the router [6].

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 11: RIP routing on east and west Sydney Routers

## Verification of END-Devices (Clients)

Pinging within the east branch (Admin department to ARdepartment)

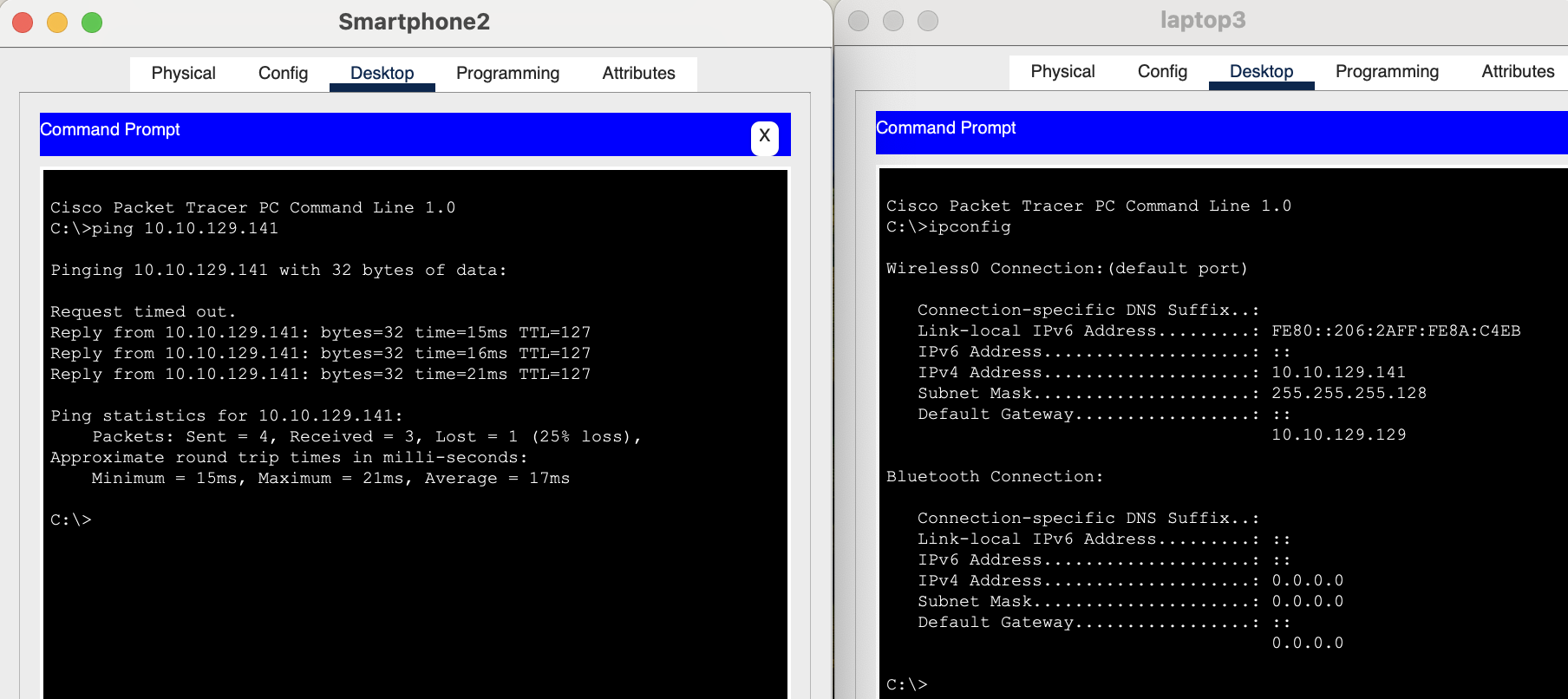


Figure 12: Successful pinging of end device on same branch

Pinging between two branches (east admin to west admin)

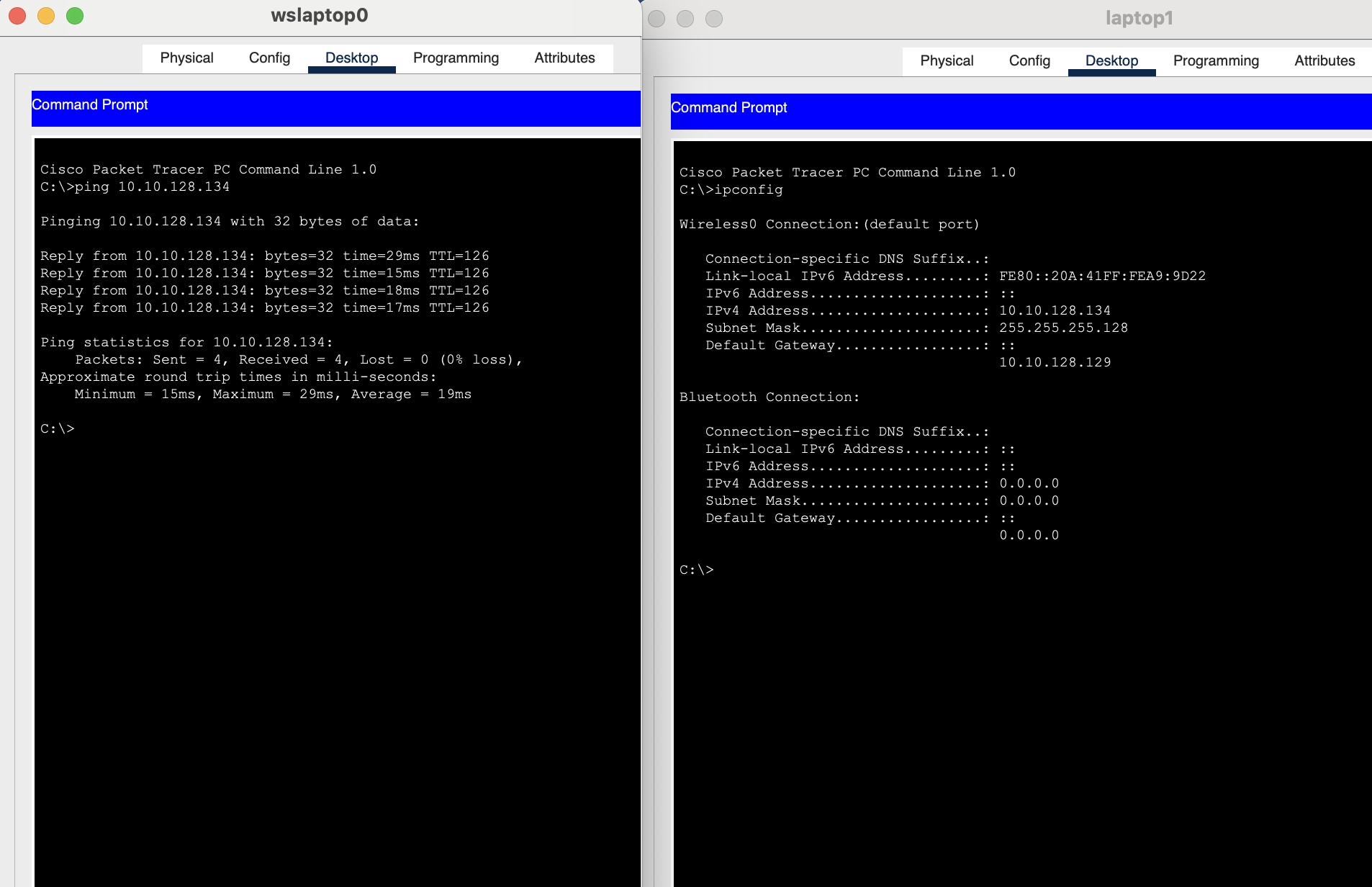


Figure 13: Successful pinging of east Sydney from West Sydney

## Authentication:

For authentication of the user, WPA2 protocol has been used.

Here users can connect to the AP only by knowing SSID, user ID and password.

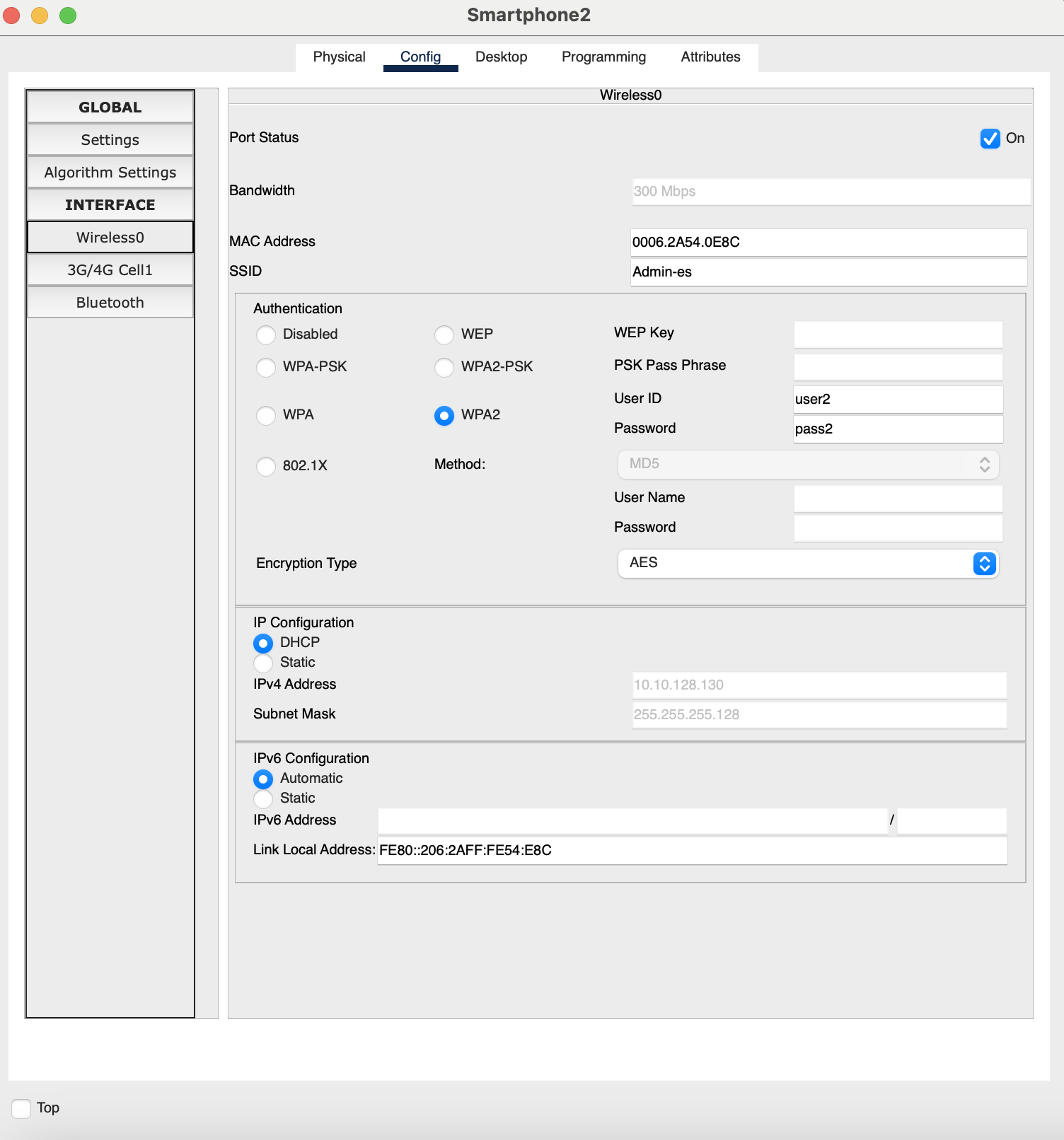


Figure 14: User Authentication through SSID and WPA2

## Association:

Association simply implies with connecting devices through a wireless network.

Here, the clients have been associated with the APs in the west branch.

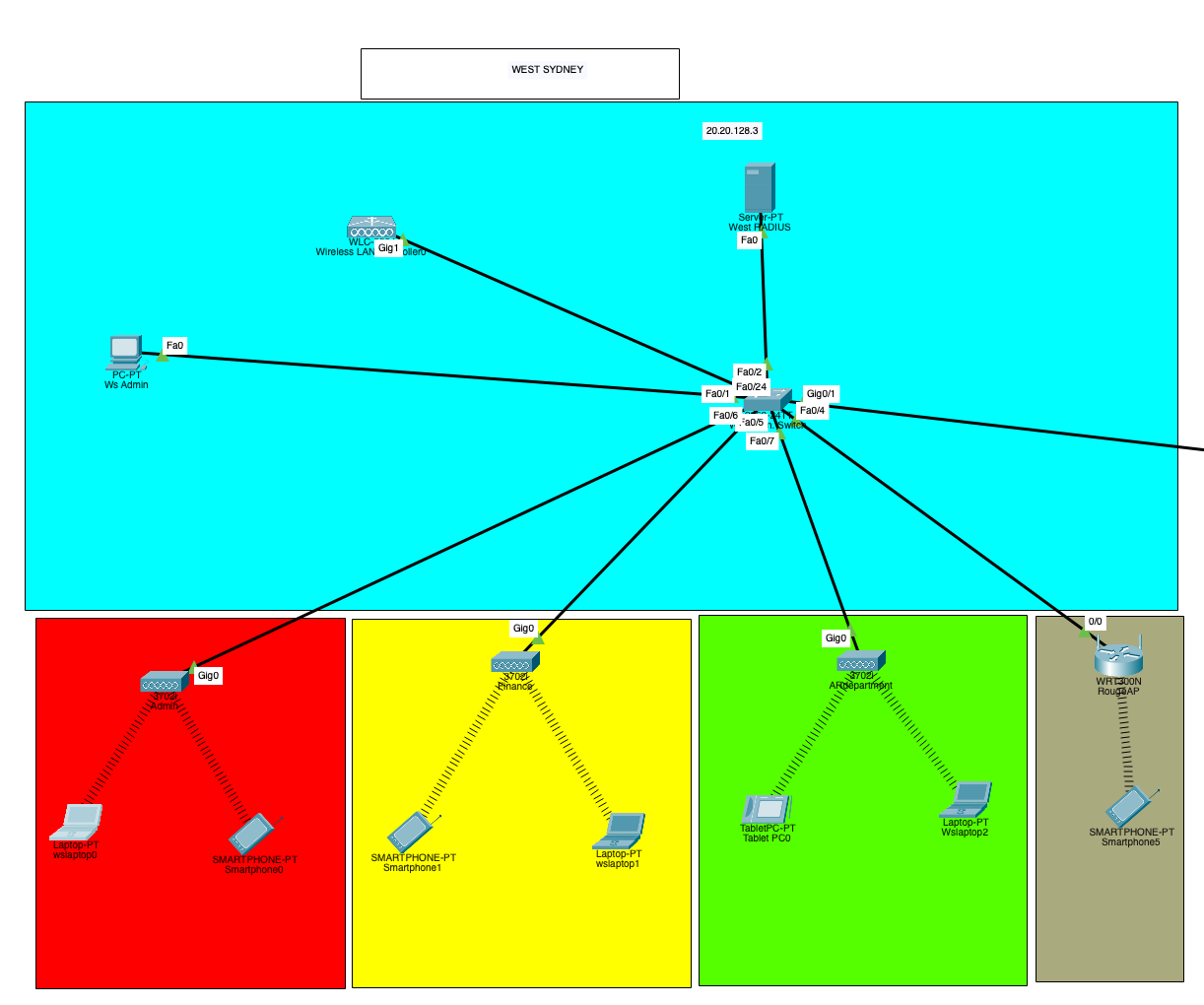


Figure 15:Wireless Connectivity on end devices-Association

## Dissociation:

This implies disconnecting devices from wireless network with incorrect SSID and login credentials i.e username password or incorrect passphrase.

After changing the SSID in the laptop, i.e. Admin instead of “Admin-ws” the connection from the laptop is disassociated from the wireless network.

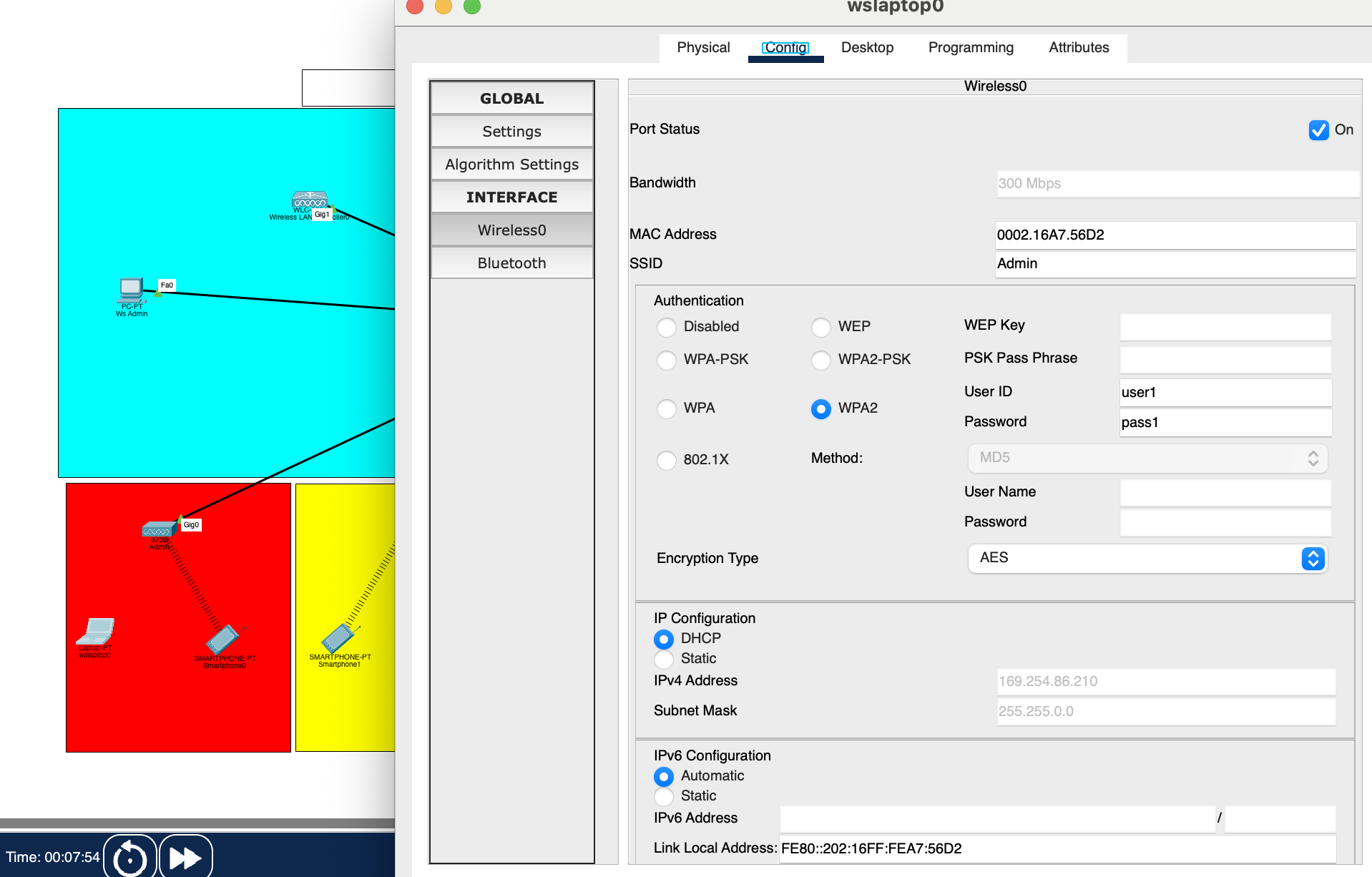


Figure 16: Dissociation of wireless network of Laptop from Admin

## Testing users and IOT devices.

**Configuration of IOT service in Server**

Each department in East Sydney is embedded with IoT systems and technologies. IoT monitoring and control is implemented using Server as follows:

Install all the IoT devices and provide authentication using the same SSID and WPA2 password of respective departments for the wireless connection in IoT systems.

On Server>Services>IoT>Enable the IoT service “on”.

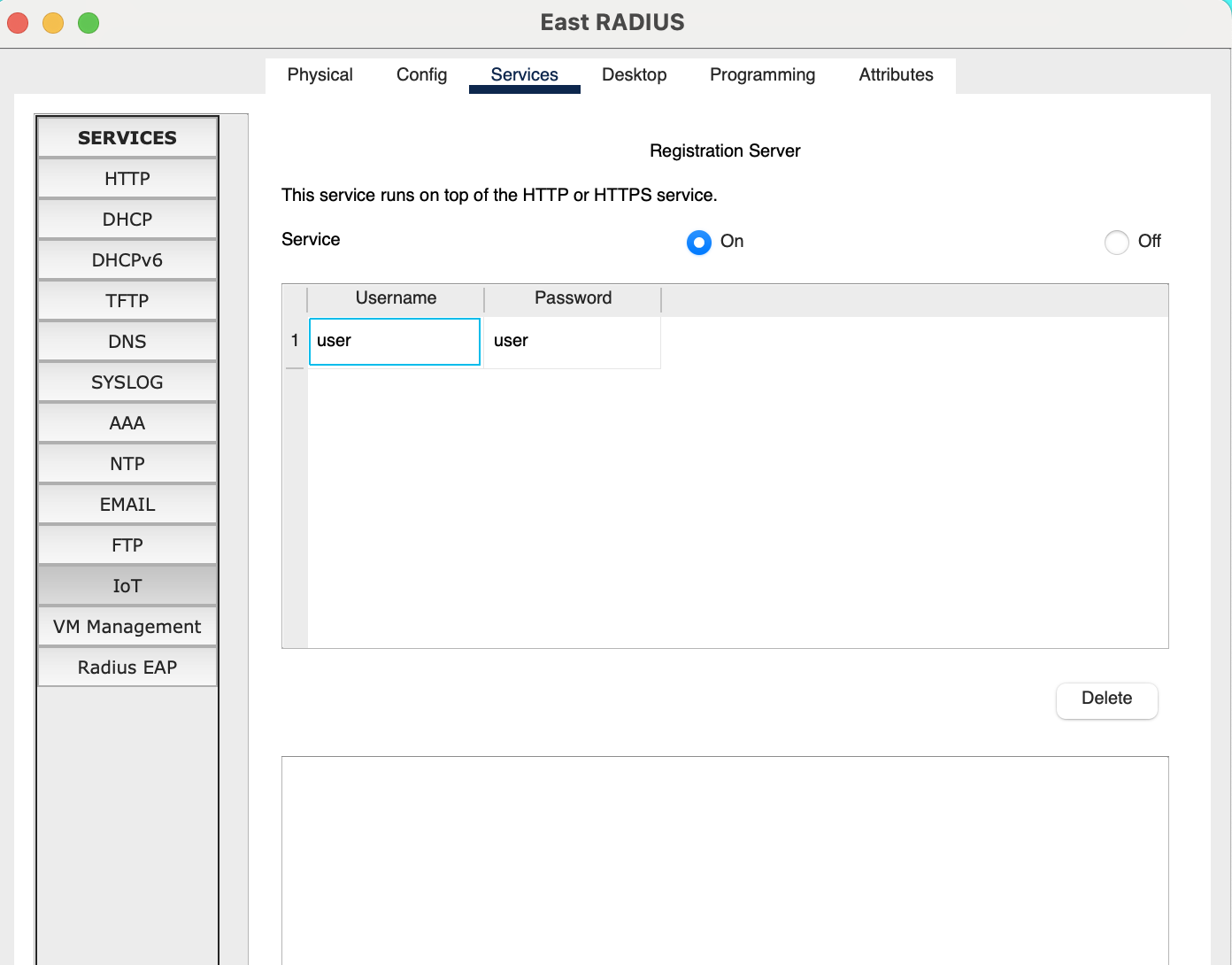


Figure 17:IoT service on Server

From a client from any branch of east Sydney, browse the IP of the server using the default Web Browser.

Register and sign up for user credentials to configure the IoT services on Server.

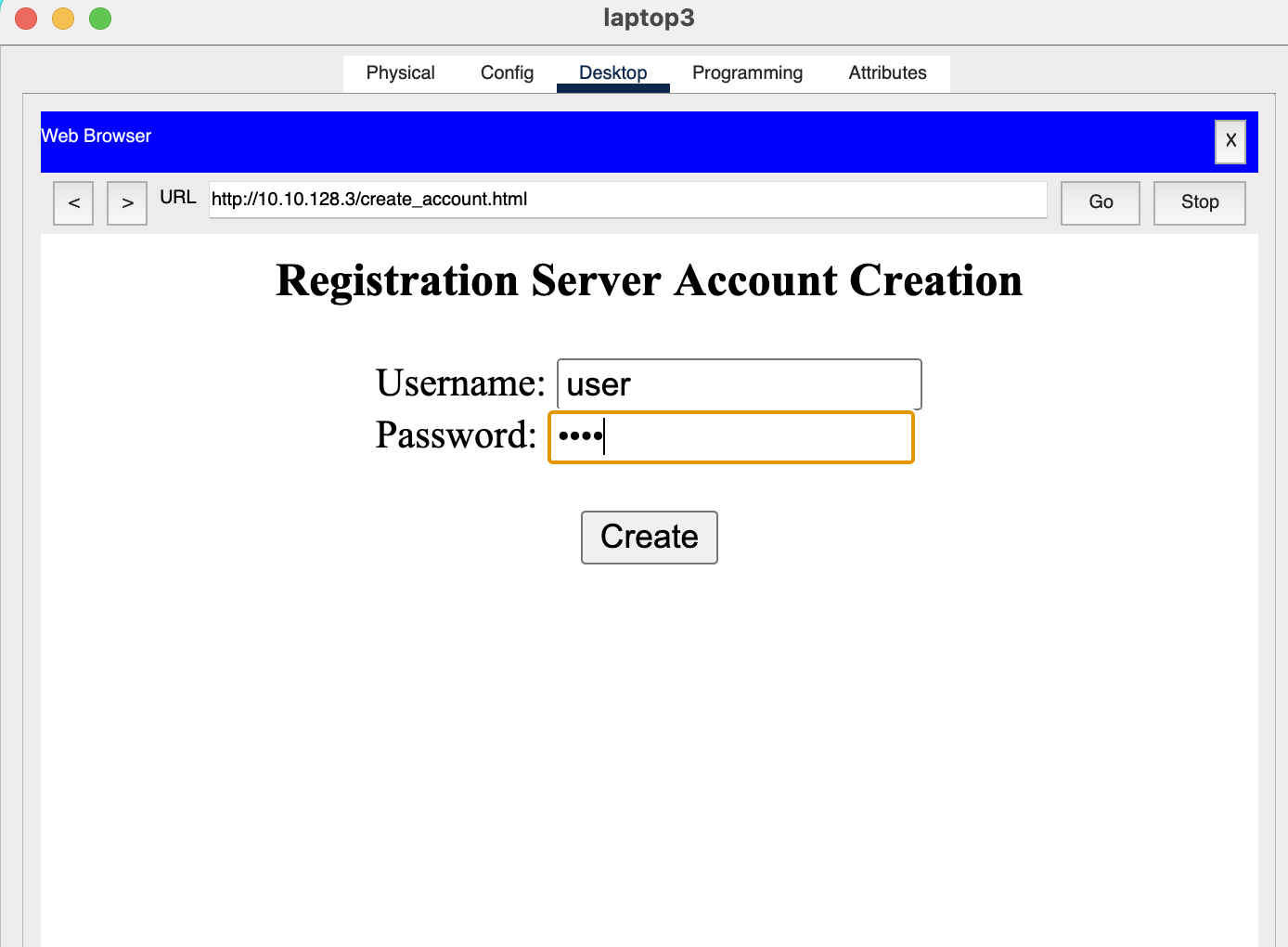


Figure 18: IoT user account registration

Go to config>Iot server >select Remote server to put the IoT username and password and server Ip address.

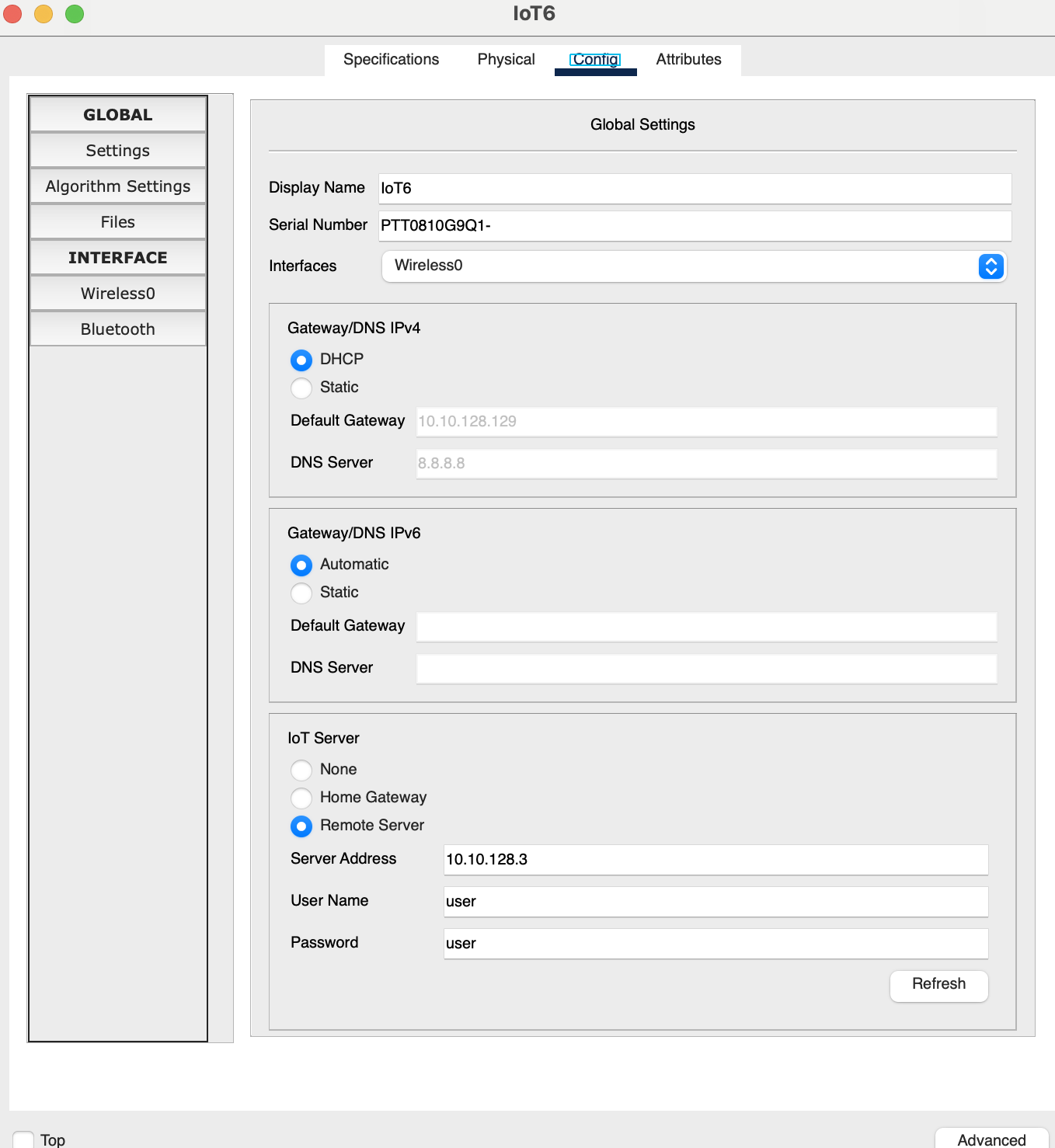


Figure 19:Remote server access on IoT

IoT monitoring and control through the same client browser as provided in the snapshot.

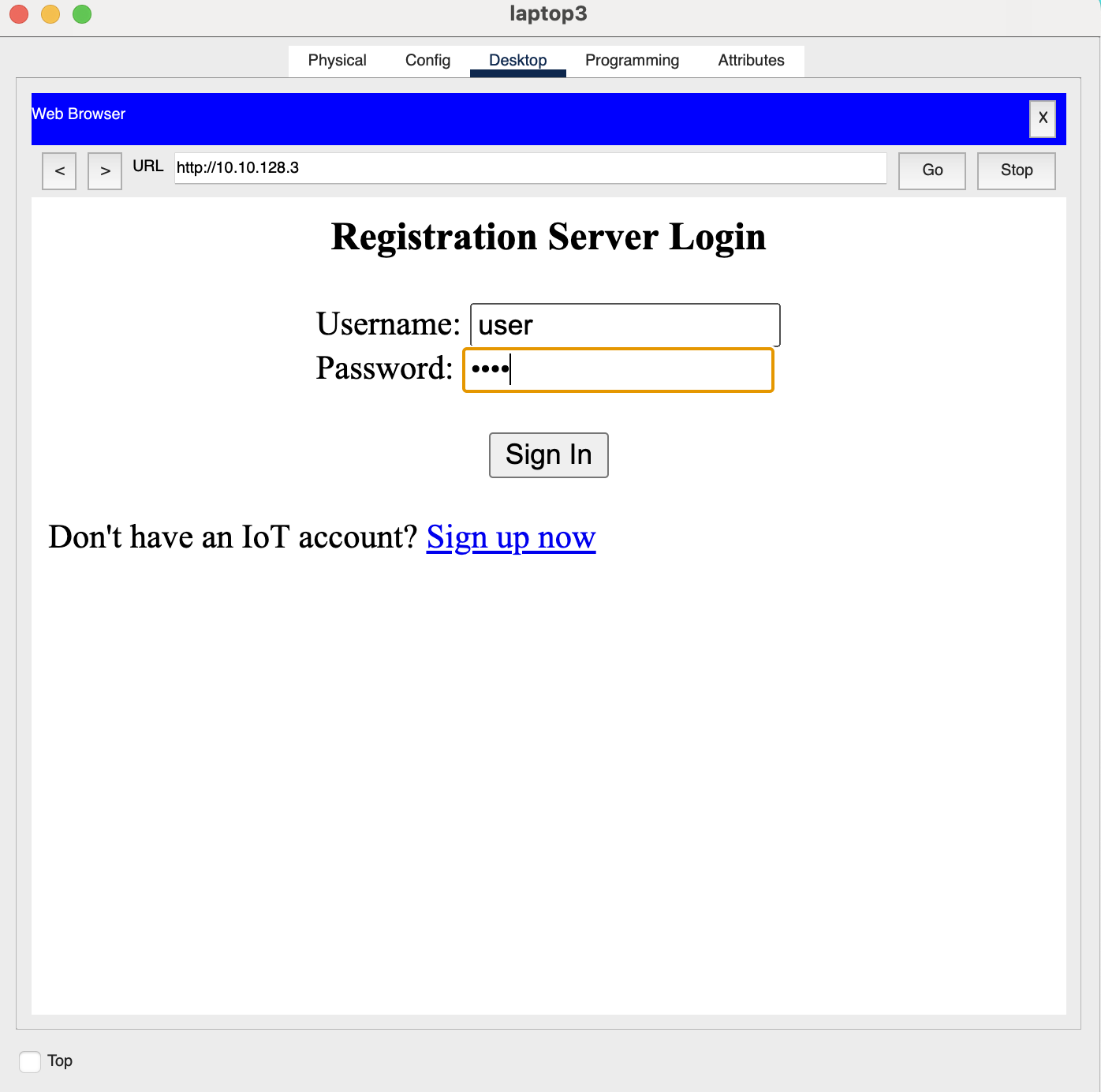


Figure 20:Server Login for access control IoT

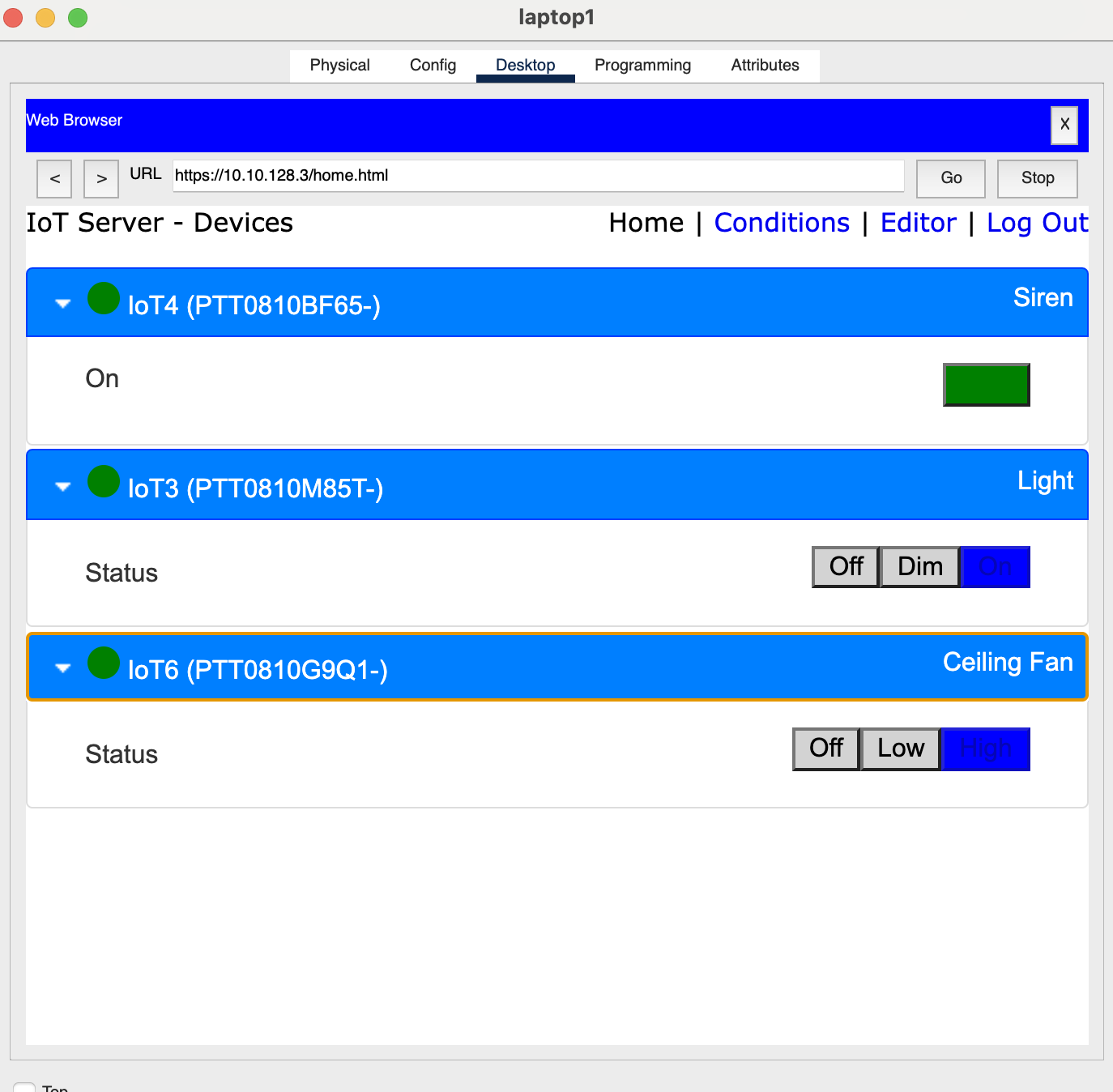


Figure 21: IoT Monitoring and Control through Laptop

## Pinging users and IoT devices:

IP of one of the IoT devices to be pinged.

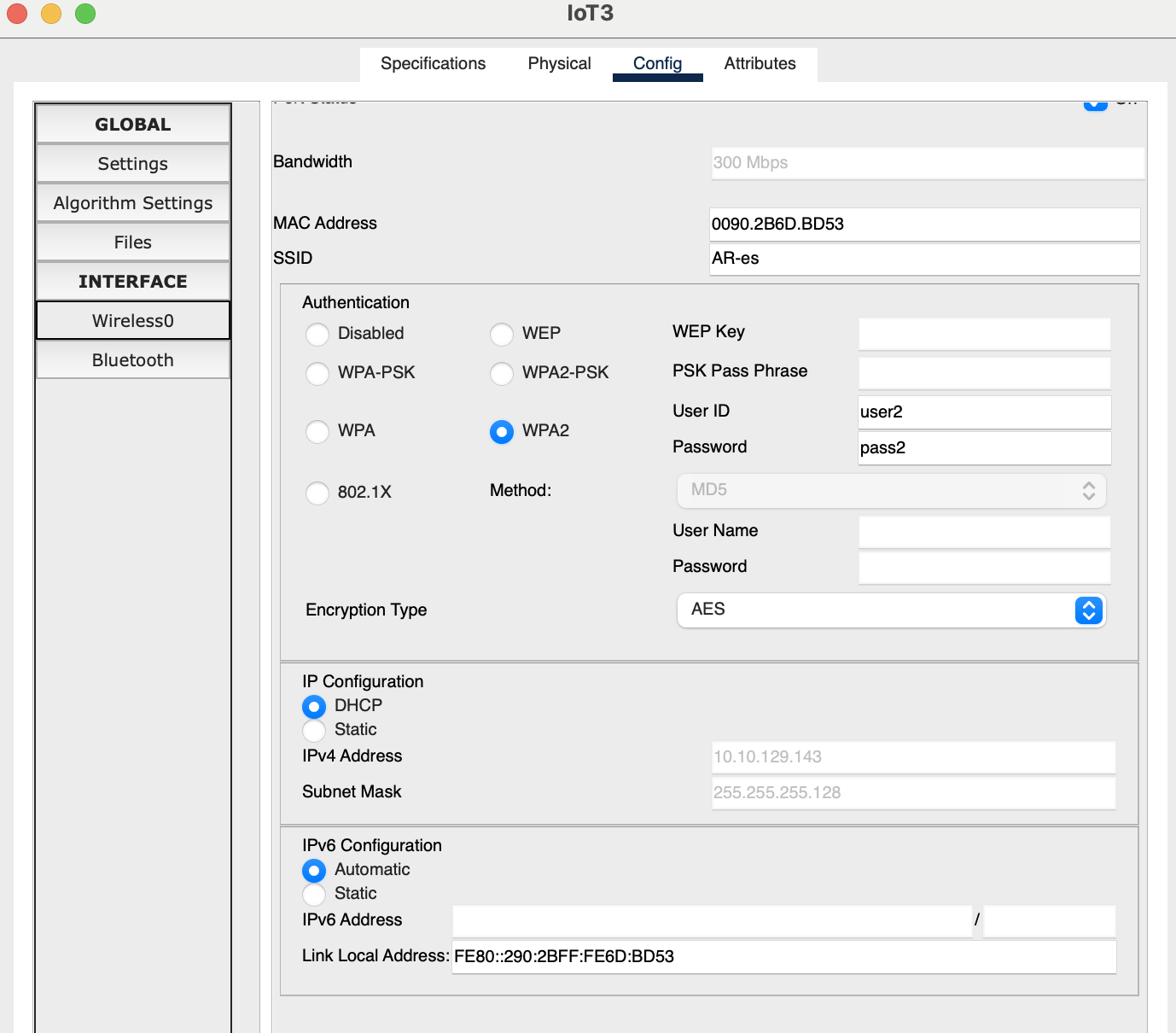


Figure 22: IP address of the IoT system

Pinging IoT from client

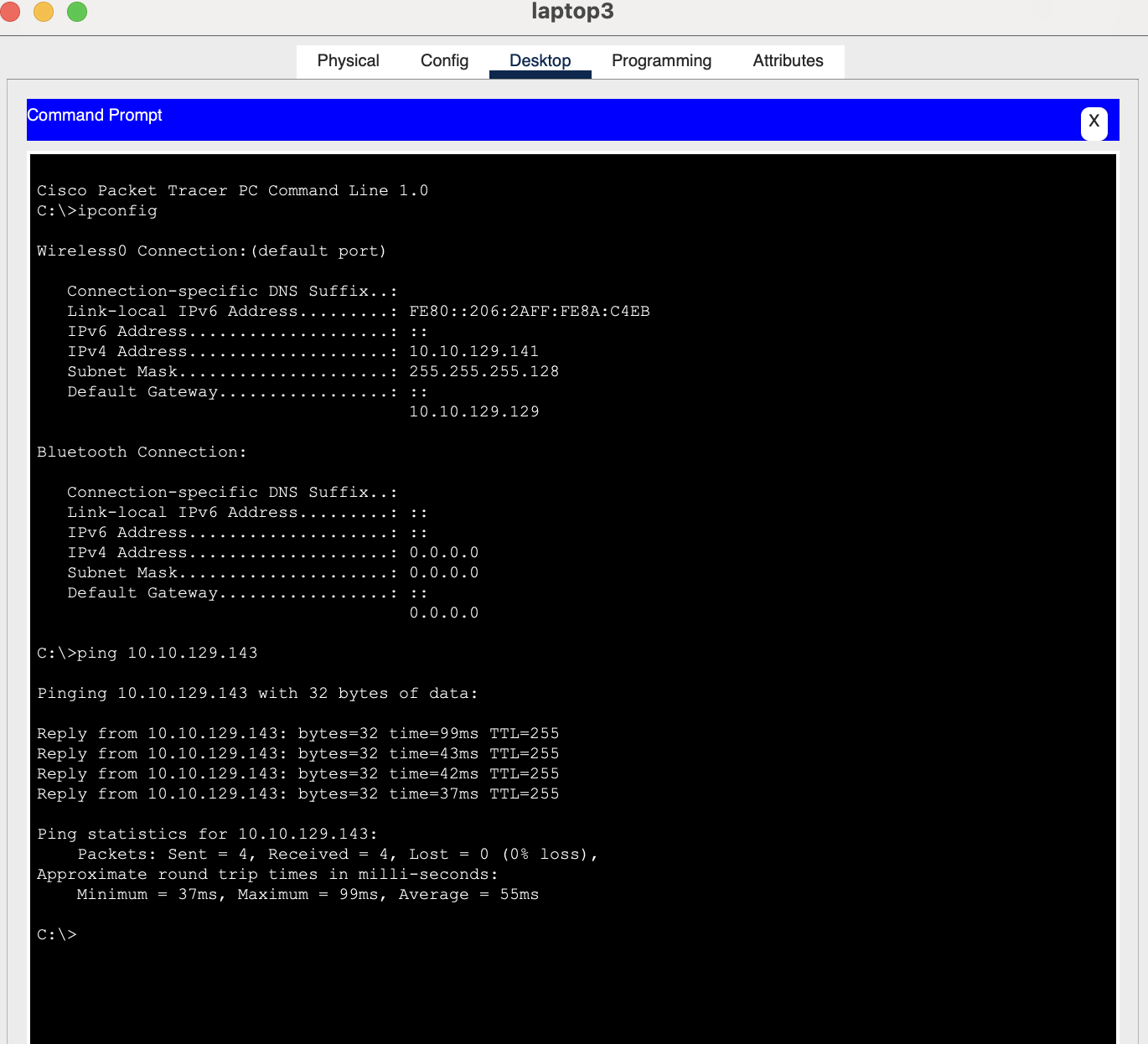


Figure 23: Successful pinging of IoT from user(laptop)

# Conclusion

This report provides a secure network design for Albert school addressing the need for the users, budget and reliability on wireless access. The proposed wireless network design for Albert School addresses the need for secure, cost-effective, and reliable wireless access. To facilitate effective communication and data interchange, it focuses on integrating Internet of Things (IoT) devices, establishing distinct VLANs, and putting access control policies. The design incorporates robust security measures, supports seamless inter-branch connectivity, and integrates IoT devices efficiently. The budgetary constraints of Albert School have been considered in the design to maximize the cost-effectiveness. Cisco Packet Tracer has guaranteed performance and durability as a reasonable networking system and equipment. The use of Cisco Packet Tracer for simulation ensures that the network configuration is practical and functional before deployment. In this way, a secure and high-performing network infrastructure that meets the school's operational needs and requirements has been implemented for effective communication between two branches.

# References

[1] F. S. Samui, “Wireless local area network (s) security: a case study on some business centers in Lusaka central district (Doctoral dissertation).,” *The University of Zambia*, 2020.

[2] L. e. a. Dhirani, “Ethical dilemmas and privacy issues in emerging technologies,” *A Review Sensors*, vol. 23, no. 3, p. 1151, 2023.

[3] D. A. K. Singh, “Internet Protocol (IP) Address–Subnetting and Supernetting*.,” Int. J. Emerg. Trends Technol. Comput. Sci*., vol. 4, no. 5(2), pp. 87-90, 2015.

[4] K. A. Adbeib, “Comprehensive Study on Wi-Fi Security Protocols by Analyzing WEP, WPA, and WPA2.,” *African Journal of Advanced Pure and Applied Sciences (AJAPAS),* 385-402., vol. 2, no. 4, pp. 385-402, 2023.

[5] A. S. S. &. C.-P. A. Rizzardi, “Analysis on functionalities and security features of Internet of Things related protocols.,” *Wireless Networks*, vol. 28, no. 7, pp. 2857-2887, 2022.

[6] J. Macfarlane, Network routing basics: Understanding IP routing in Cisco Systems*. Indiana: Wiley Publishing, Inc*, 2007.