**EE-424 Data Communication and Networking**

Lab Project

Title: Enhanced switch security and routing using IPv4/IPv6.

Instructor: Dr Moiz Anis

RA: Ahmed Bilal

**Group Members:**

Arsalan Ahmed

Mariyah Yousuf Hussain

Yousuf Moiz

Zeeshan Karim

**Objective:**

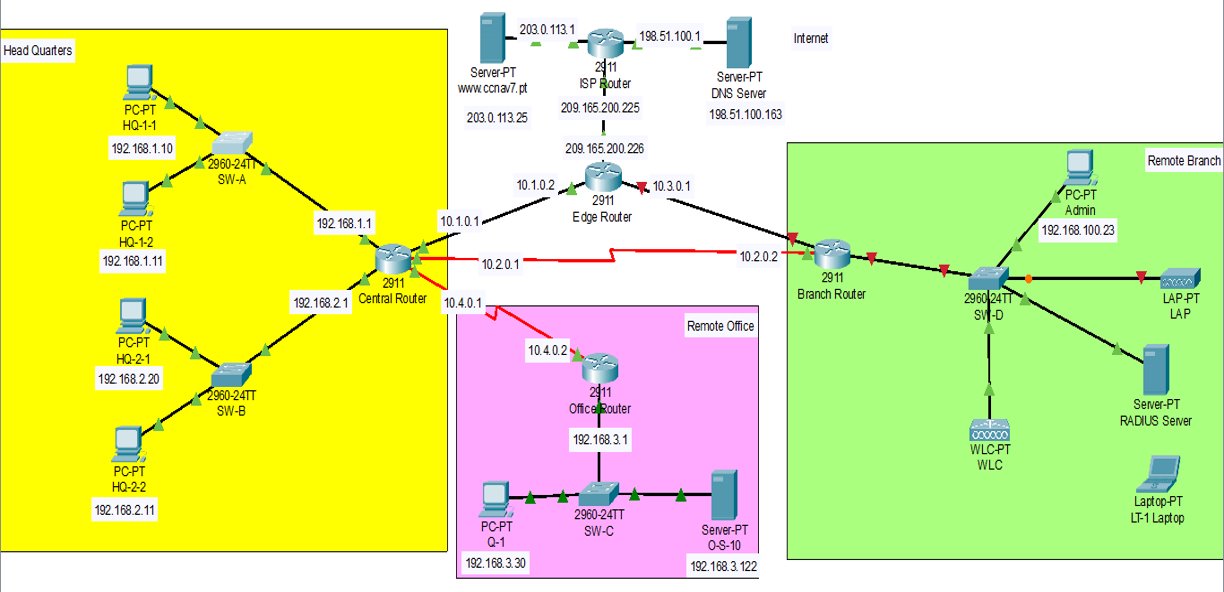
The project objectives include:

1. Floating static and default routes in IPv4 and IPv6.
2. Host routes in IPv4 and IPv6.
3. DHCP pools and scopes.
4. Switch security including port security.
5. Enhanced LAN security with DHCP snooping, dynamic ARP inspection, PortFast, and BPDU guard.
6. Wireless LAN Controller-based wireless LAN with enterprise authentication.

**Background/Motivation:**

In order to achieve the aforementioned objectives, we have created a scenario in which there is an organization with a central office, a north office branch and a south office branch. The organization has decided to rework their network. We have been asked to prototype the network in Packet Tracer for evaluation by senior network staff.

**Topology:**



**Theory of the Concepts involved:**

* **Static Routing:**

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. Static routing is used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information and since in our project there are only 5 routers with at max three routes per router, we preferred using static routing. Moreover, Static routing is often used as a complement to dynamic routing to provide a failsafe backup in the event that a dynamic route is unavailable.

* **DHCP Snooping:**

DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.

* **Dynamic ARP Inspection:**

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. ARP Poisoning is a type of cyberattack carried out over a LAN that involves sending malicious ARP packets. Dynamic ARP Inspection (DAI) validates ARP packets in a network based on valid IP-to-MAC address bindings stored in a trusted database.​

* **PortFast:**

Enabling the PortFast feature causes a switch or a trunk port to enter the STP forwarding-state immediately or upon a linkup event, thus bypassing the listening and learning states. ​

* **BPDU Guard:**

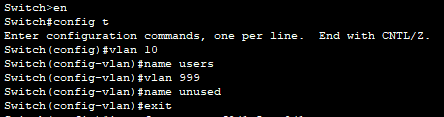
BPDU guard prevents a port from receiving BPDUs. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure.​

**Configurational Setup**

**Part 1: Configure Switch Security**

1. Configuring VLAN’s

* a. Configure VLAN 10 with name users.
* b. Configure VLAN 999 with the name unused.

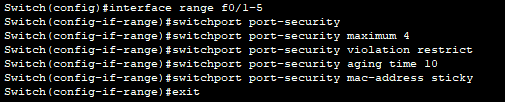


1. Configure active switch ports.

* Configure the ports Fast Ethernet 01 through 05 and port Gigabit Ethernet 0/1 as static access ports in VLAN 10.

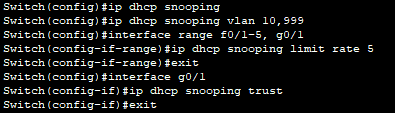


* Activate port security on the ports.





* Protect against DHCP snooping



* Guard against ARP attacks by implementing DAI.



* Secure STP by configuring PortFast and BPDUguard
* Mitigate STP attacks by configuring BPDUguard and PortFast on the active ports.





1. Secure unused switch ports.

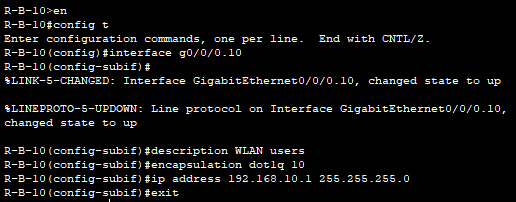
* Move all unused switch ports to VLAN 999.
* Configure all unused switch ports as static access ports.
* Deactivate all unused switch ports.



**Part 2: Configure Addressing and DHCP**

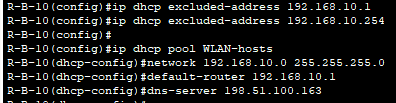
1. Configure and address a sub-interface for the WLAN user network.

* Configure sub-interface 10 on the router interface that is connected to the switch S4-1.
* The router should provide router-on-a-stick routing to VLAN 10.
* Configure the sub-interface with the address from the Addressing Table.

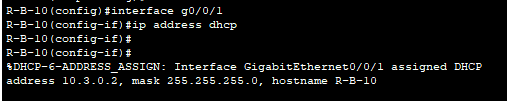


1. Configure a DHCP pool for WLAN user network.

* Exclude the router interface address and the management address of the WLC.
* Configure a DHCP pool that will be used by hosts that are connecting to the WLAN.



1. Configure an interface as a DHCP Client.

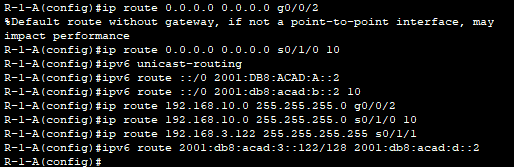


**Part 3: Configure Static Routes**

In this part, we configured static, default, floating static, and host routes in both IPv4 and IPv6. We will configure the Central and Branch-101 routers. The company has decided that it wants to use static routing between all its networks. In addition, the company wants to use the Ethernet links between routers for most data traffic and reserve serial link between Central and Branch-101 for backup purposes in case one of the Ethernet links becomes unavailable. We will be configuring floating static and default routes.

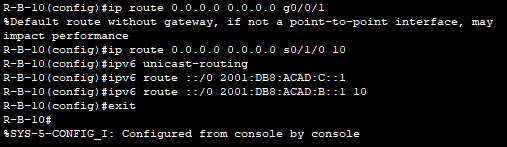
1. Configure static routes on Central.

* Configure IPv4 default routes to the cloud using the Ethernet link as the preferred link and the serial link as the backup. Use an administrative distance of 10 for the backup route. These routes should be directly connected. Note: Ethernet interfaces will give a warning when configured without a next-hop address. In this configuration, the interface is point-to point, so the warning can be ignored.
* Configure IPv6 default routes to the cloud. Use the Ethernet link as the primary route, and the serial link as backup. Use an administrative distance of 10 for the backup route. These routes should specify the next hop interface address.
* Configure IPv4 static routes to the Remote Office LAN WLAN user network following the same guidelines as above for type of route and administrative distance.
* Configure IPv4 and IPv6 host routes on Central to the Server-01 on the Remote Office LAN. Create a directly connected route for IPv4 and a next-hop route for IPv6.



1. Configure static routes on Branch 101.

* Branch-101 is configured with static routes to the other three networks in the Netacad PLC network. It will require floating static and default routes in IPv4 and IPv6 following the same guidelines as were used for the Central static routes.
* Configured IPv4 default routes to the cloud using the Ethernet link as the preferred link and the serial link as the backup.
* Configured IPv6 default routes to the cloud. Use the Ethernet link as the primary route, and the serial link as backup. Use an administrative distance of 10 for the backup route. These routes should specify the next hop interface address.

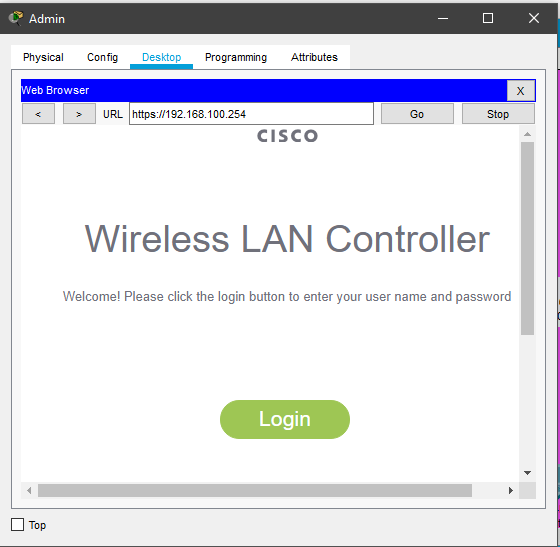


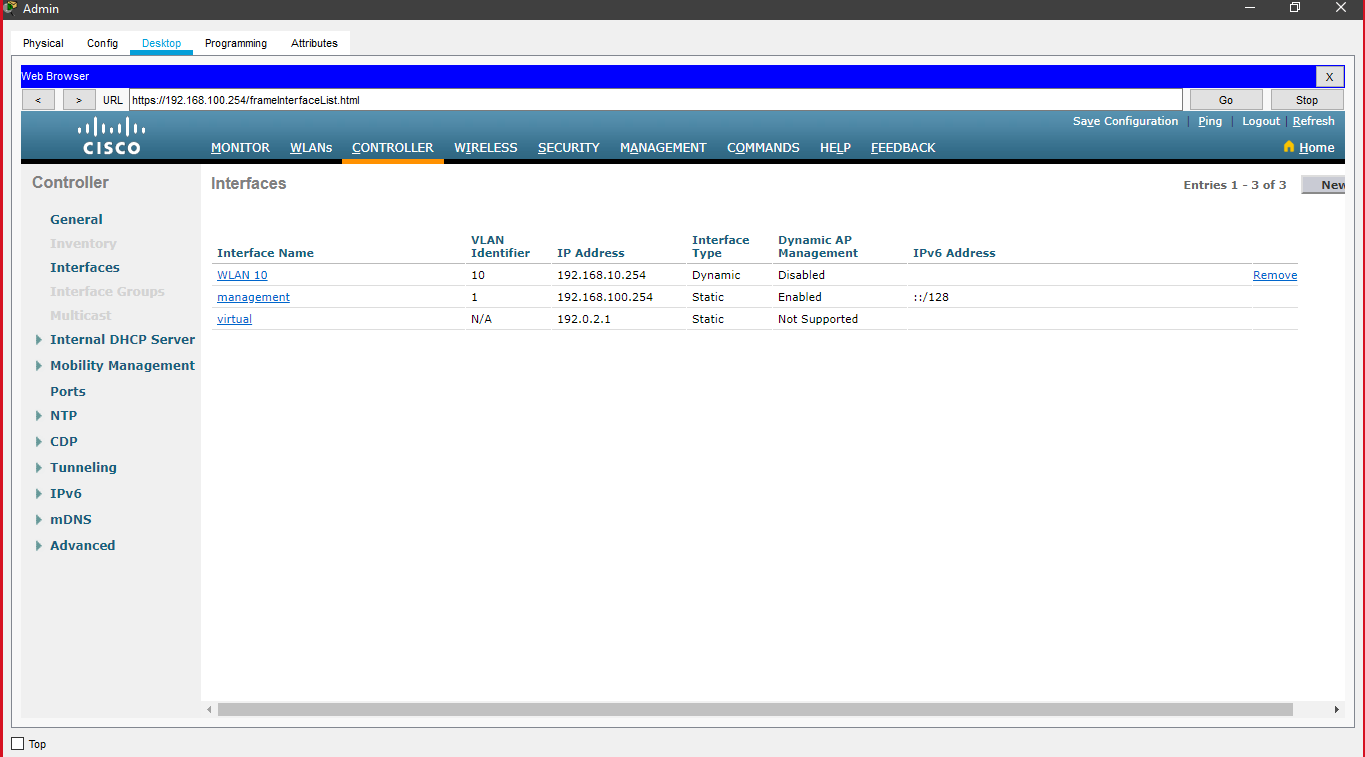
**Part 4: Configure a Wireless LAN using a Wireless LAN Controller**

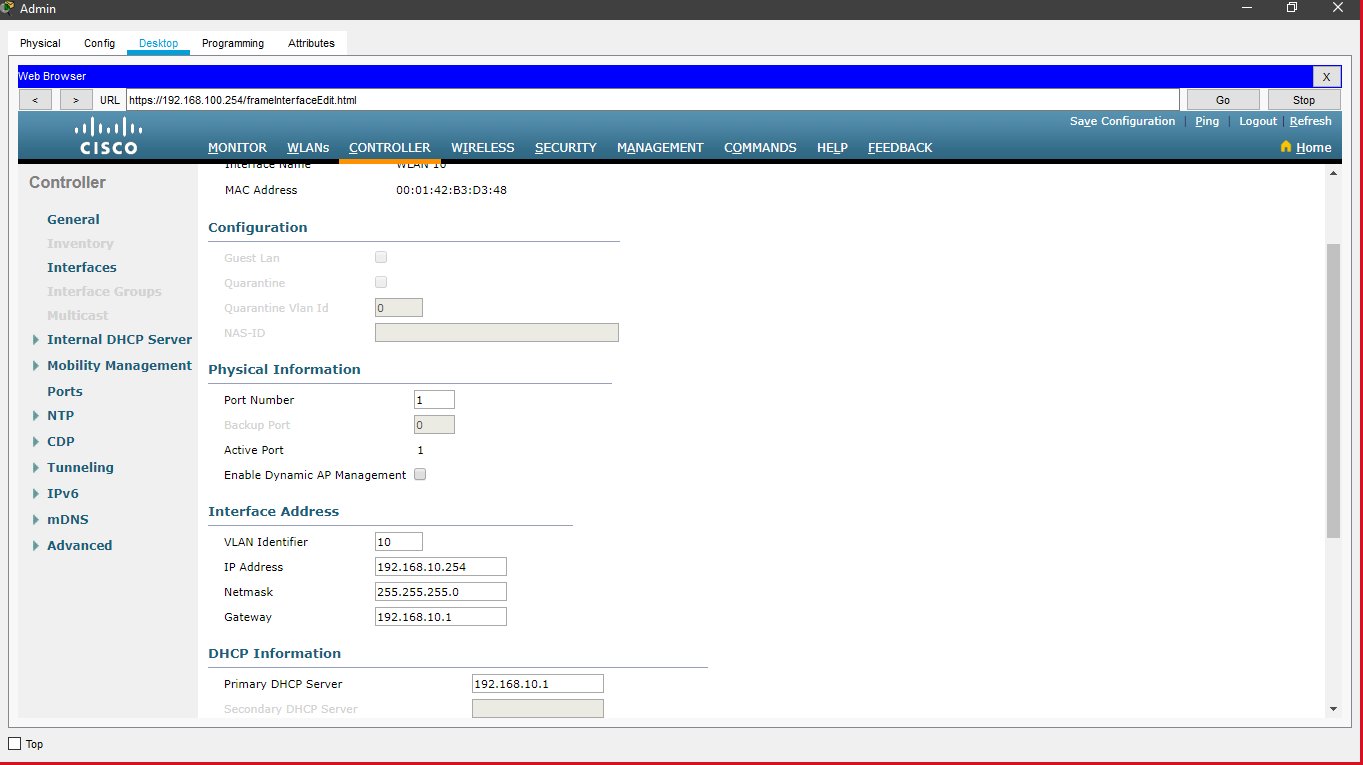
In this part, we configured the wireless LAN controller to provide access wireless access to the network. Username and password are the default admin/admin.

1. **Configure a VLAN interface**

* A new interface, WLAN 10, was created. This interface uses VLAN 10.
* Information in the addressing table was used to configure the addressing settings for the interface. The interface uses a DHCP pool that assigns addresses on the network configured on the sub-interface assigned to VLAN 10 on router Branch 101.

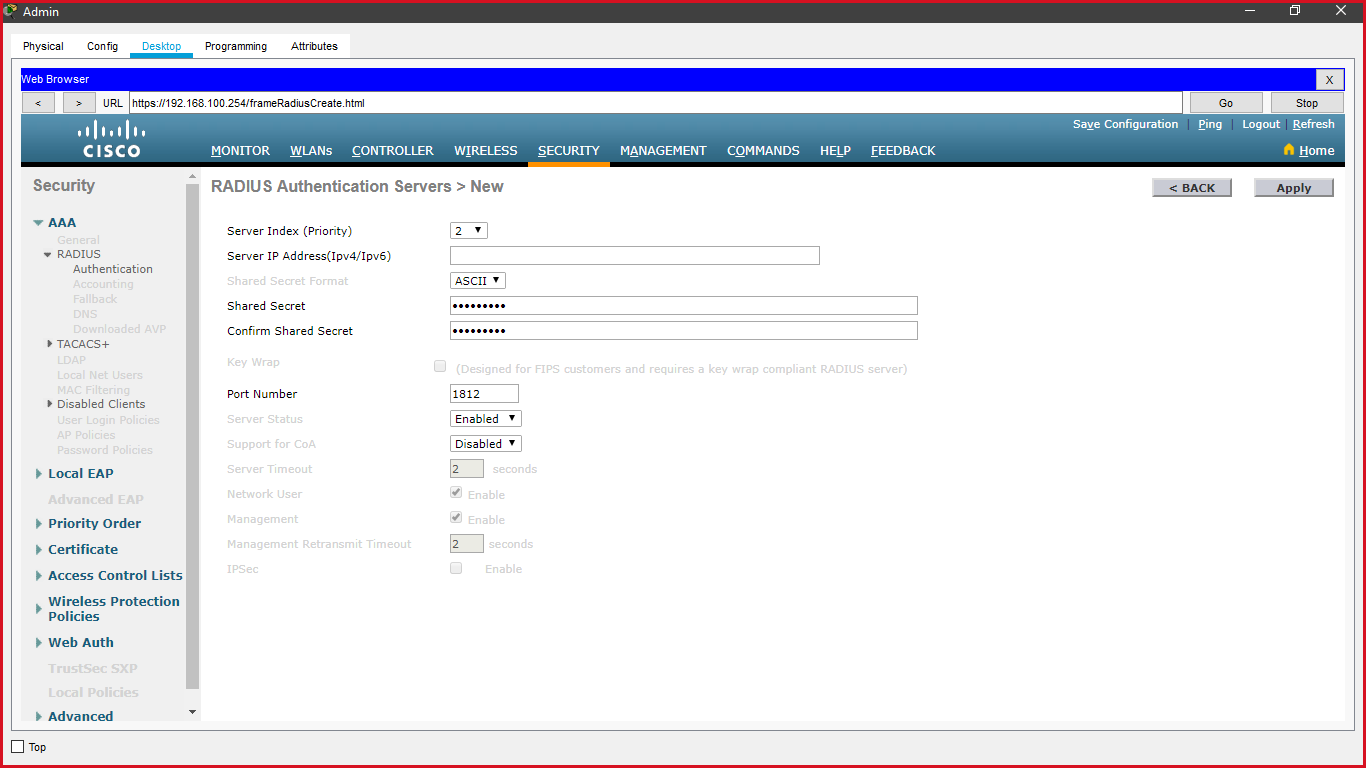






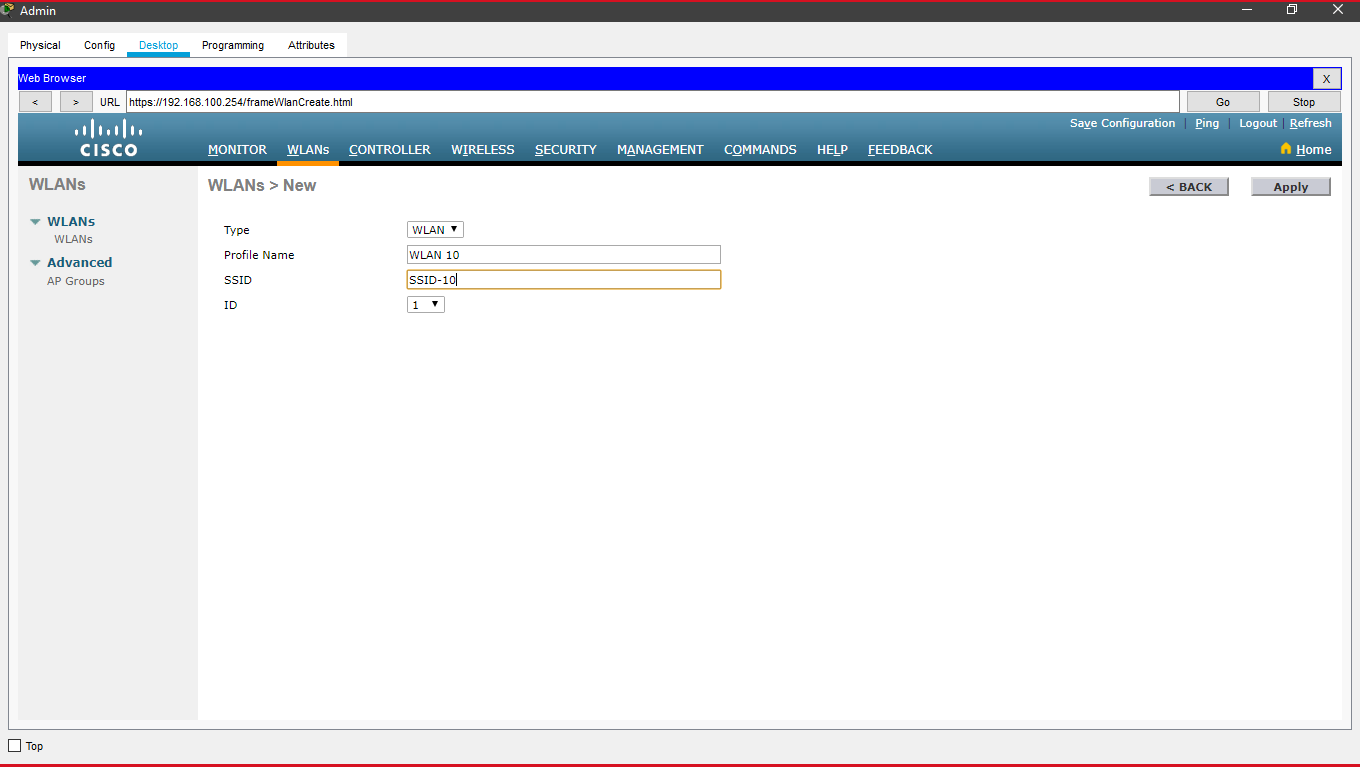
1. **Configure a Radius Server**

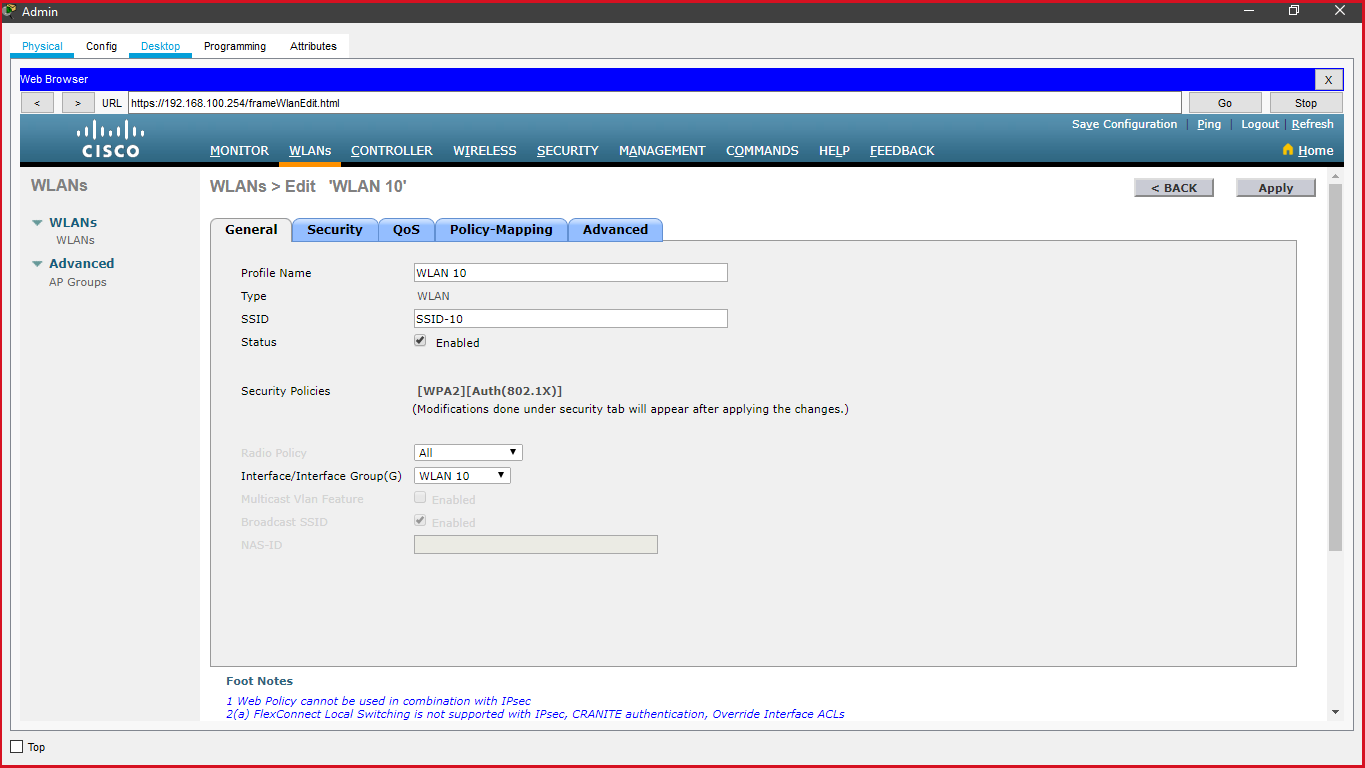
* Configure the WLC with the RADIUS server IPv4 address
* Use a shared secret of RAD secret

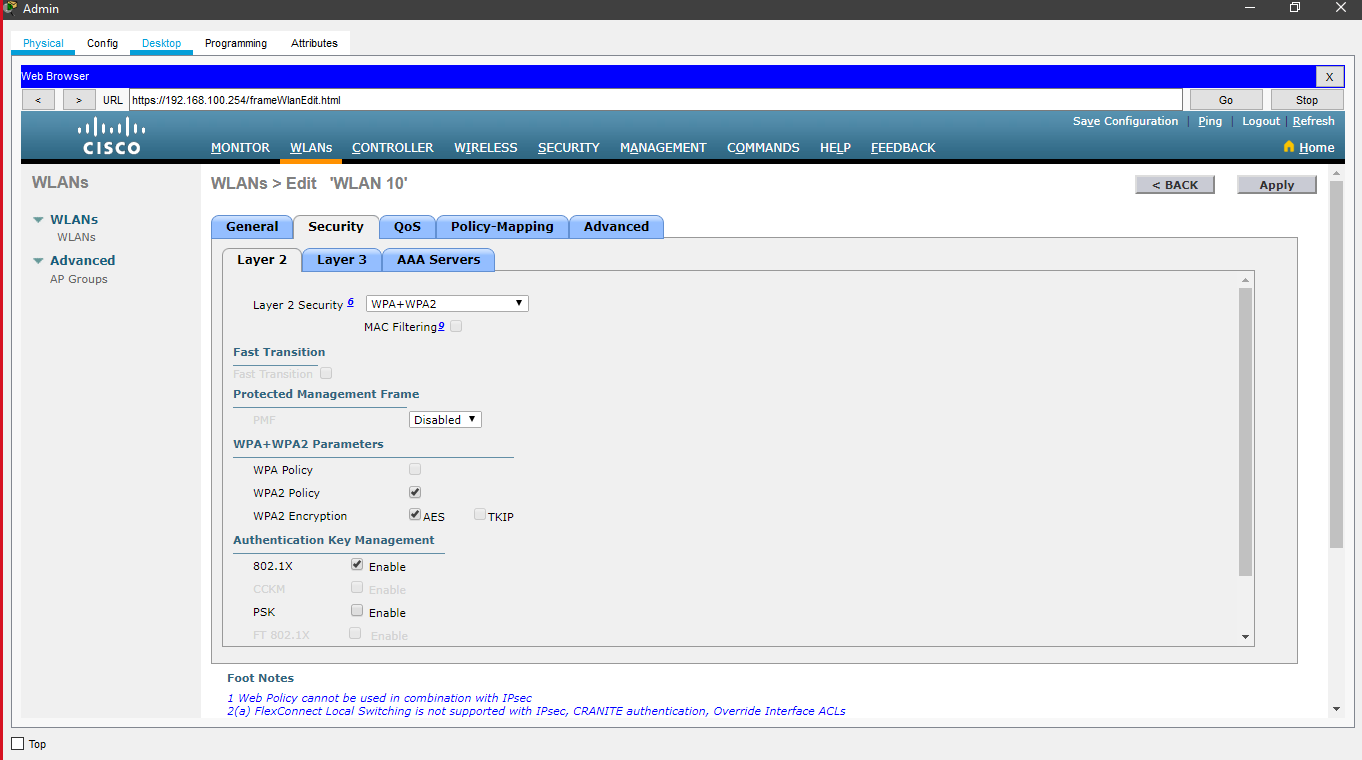


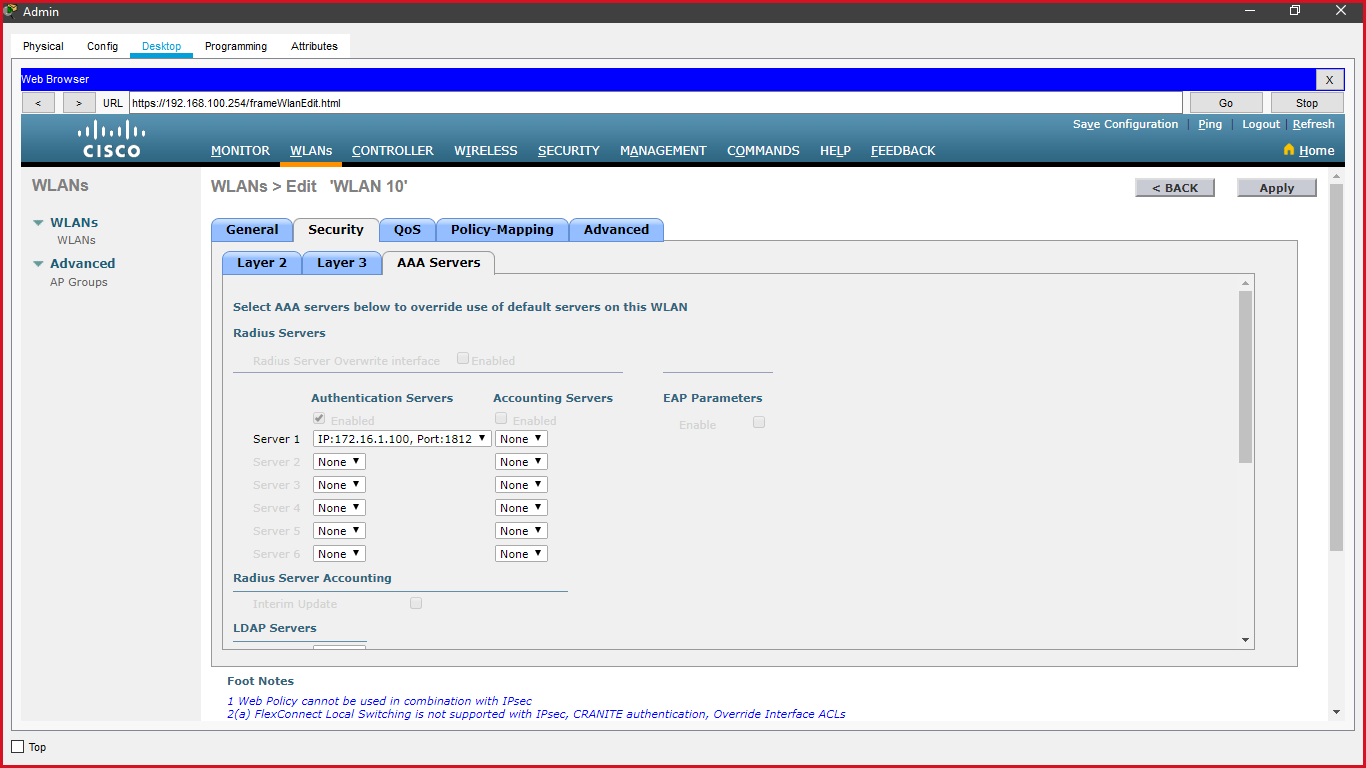
1. **Configure a wireless LAN**

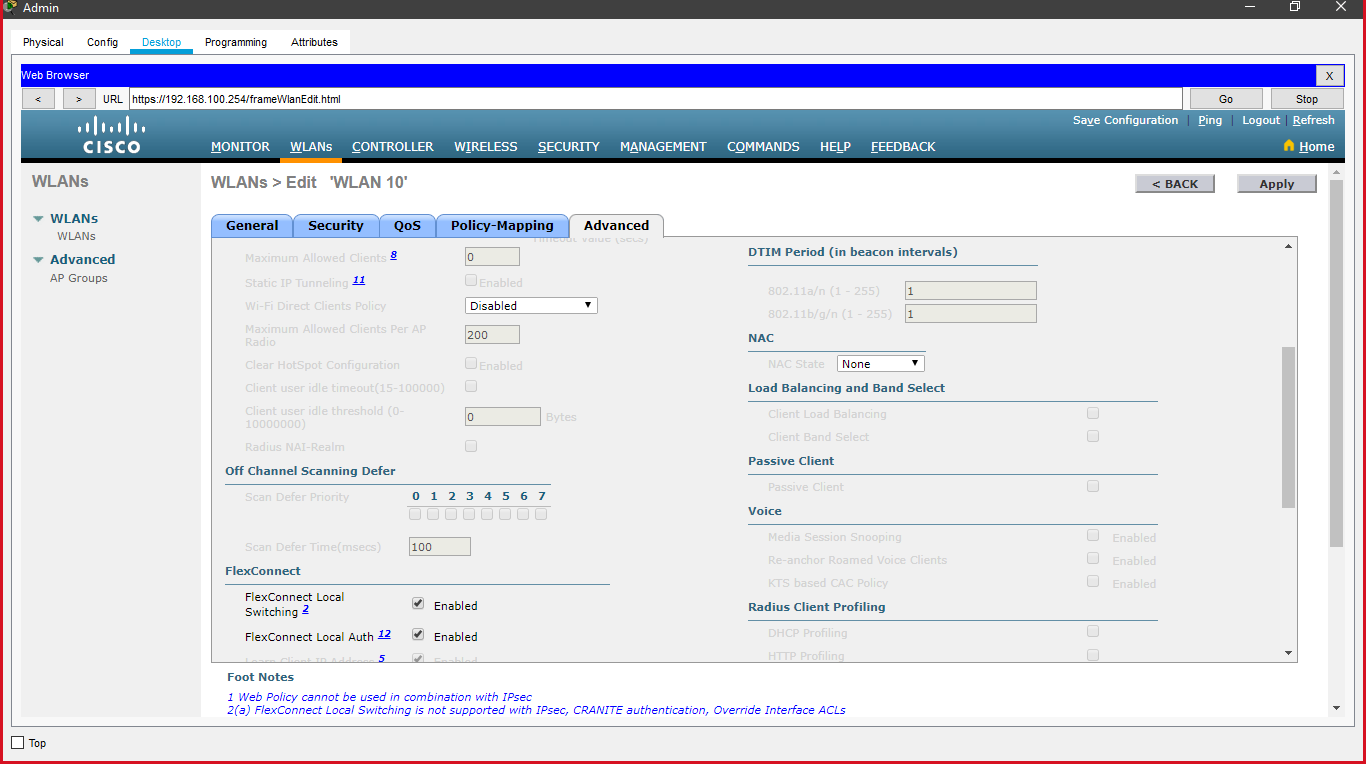
* Created a new WLAN named WLAN 10 and configured the SSID as SSID-10.
* Configured the WLAN to use the WPA2 security policy and dot1x Authentication Key Management.
* Configured the WLAN to use the RADIUS server that was previously configured to authenticate wireless users.
* Open the Advanced tab and scroll down to the Flex-connect sections. Activate Flex-Connect Local Switching and Flex-Connect Local Auth.
* We verify that the WLAN is configured and operational.

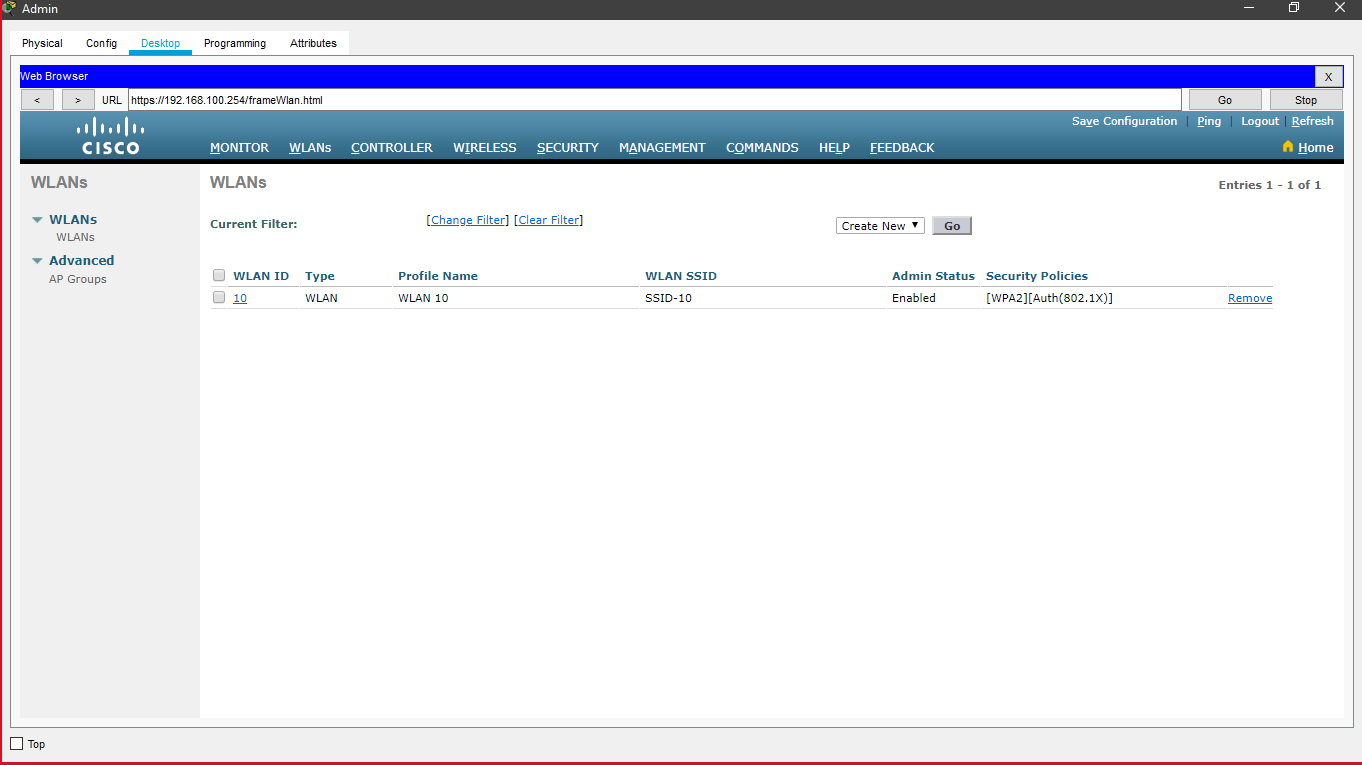






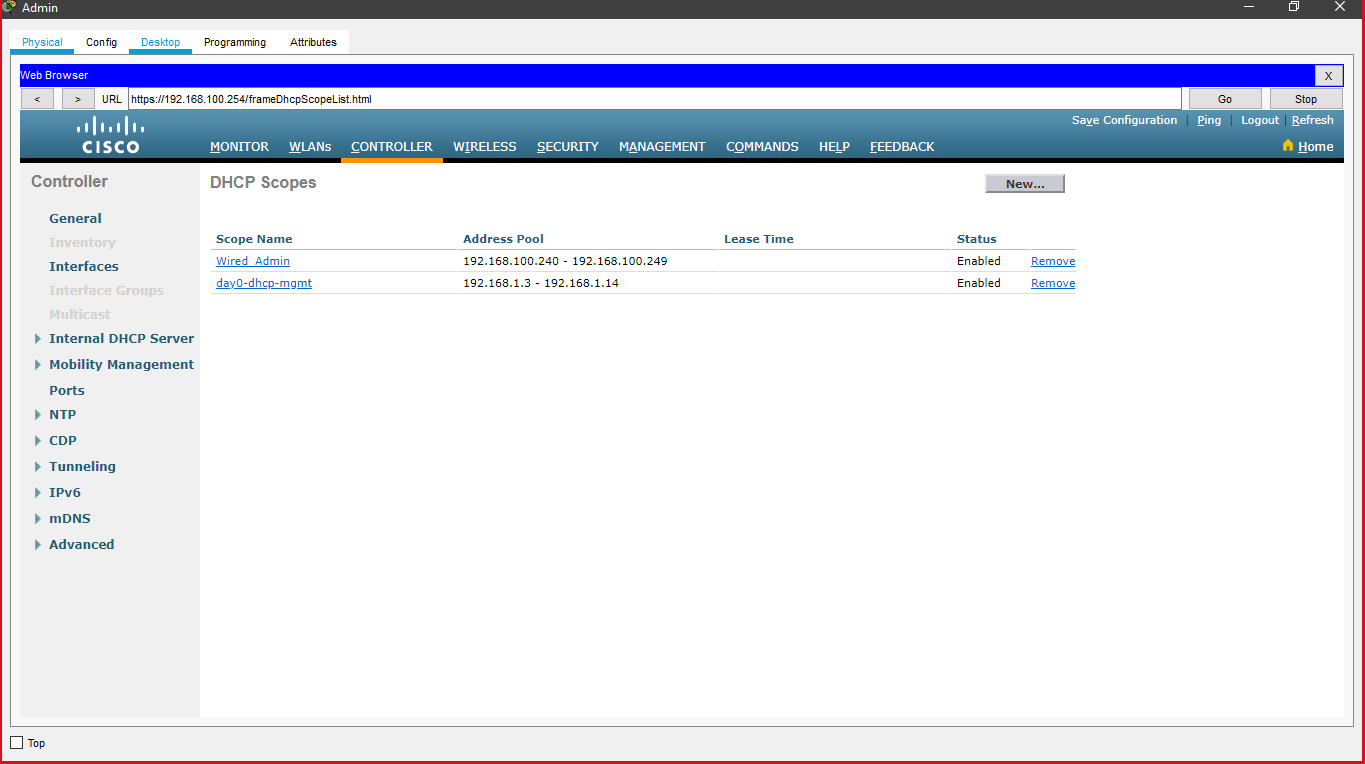


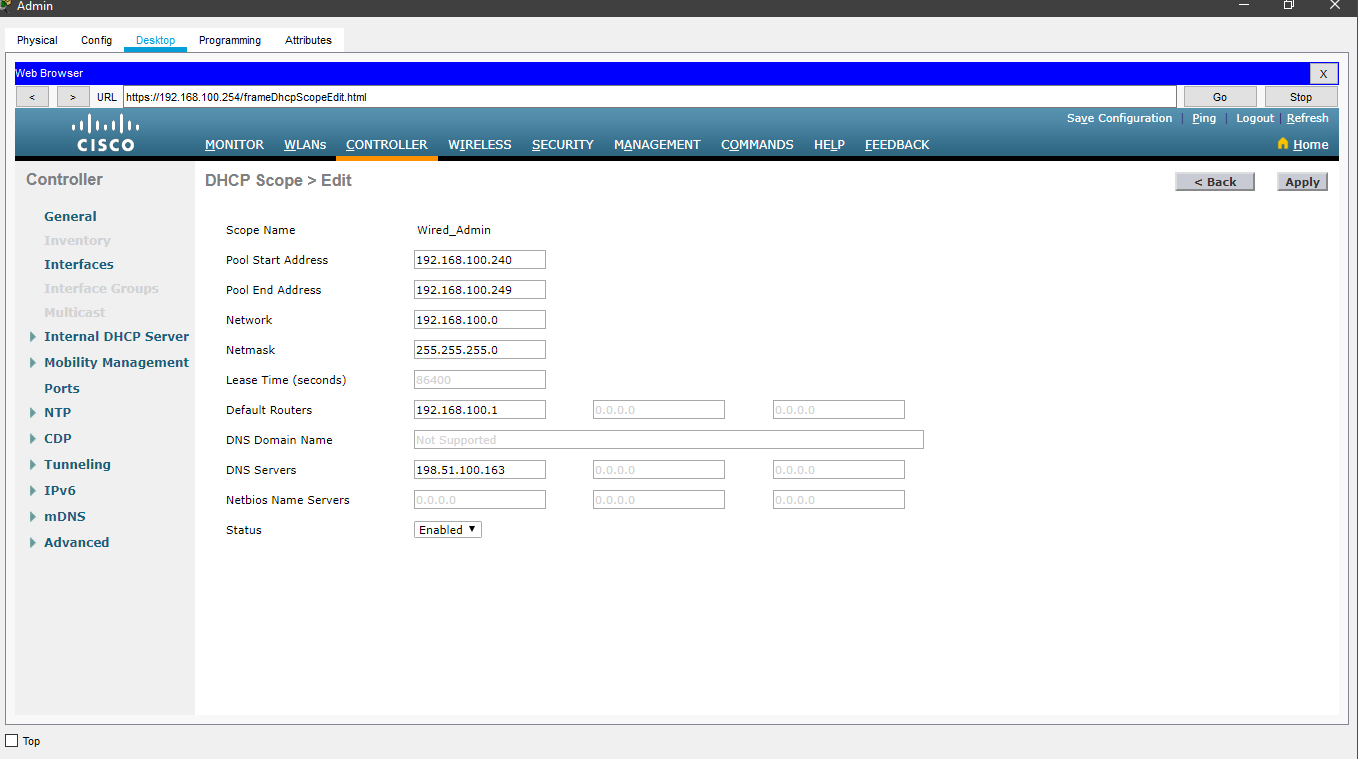




1. **Configured a DHCP scope for the management network**

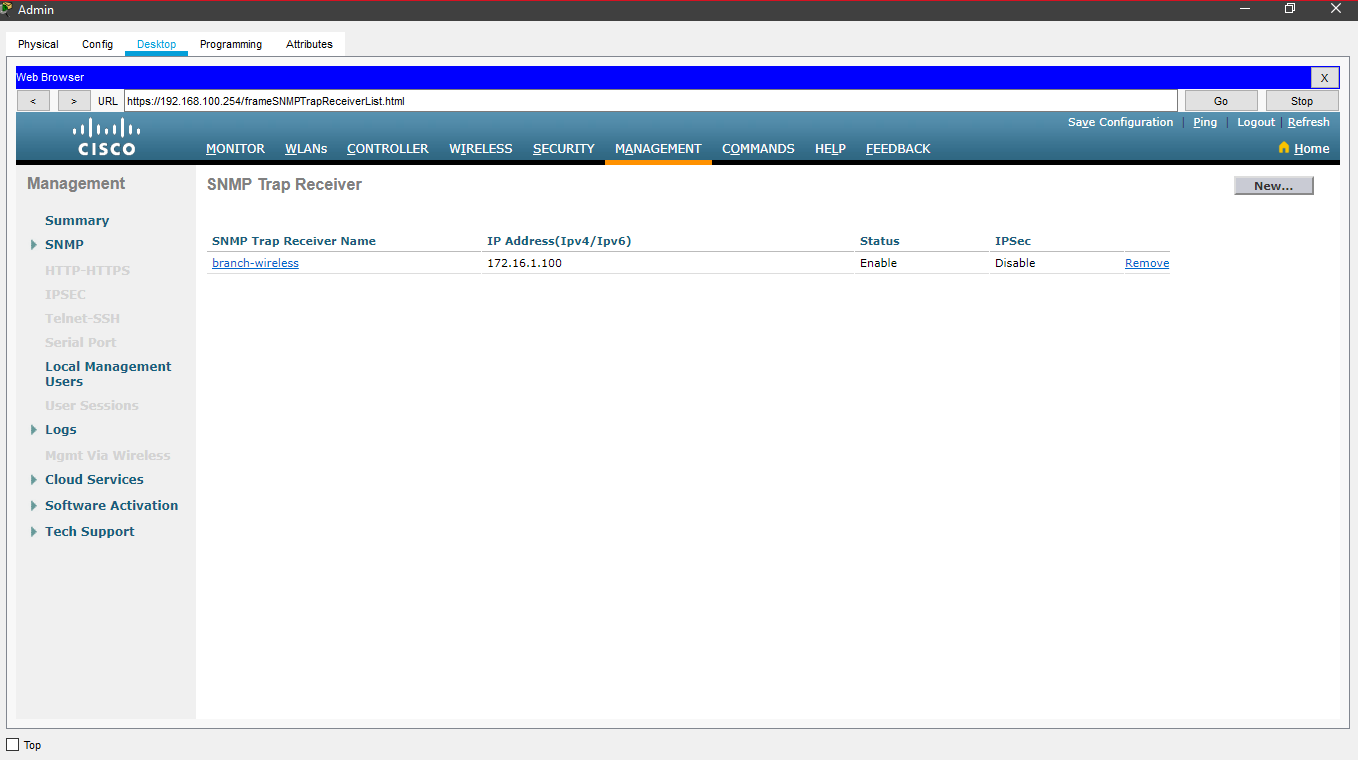
* Name the DHCP scope Wired\_Admin.
* Start the scope at address 192.168.100.240. End the scope at address 192.168.100.249.
* Other information that is required can be found in the Addressing Table.





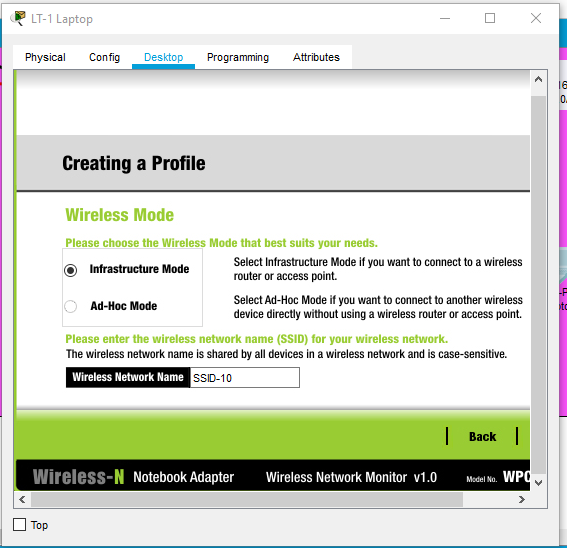
1. **Configure an SNMP server to receive traps from the WLC.**

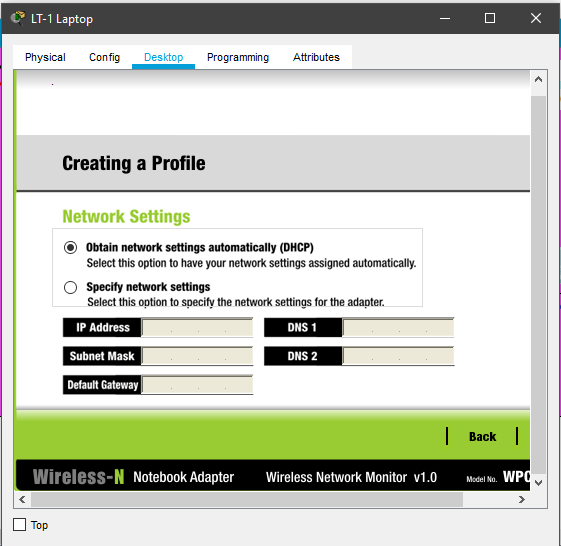
* We use the community name branch-wireless
* Use 172.16.1.100 as the server address

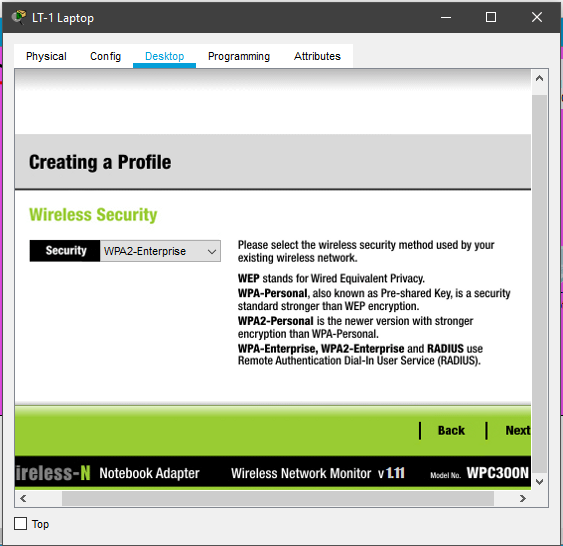


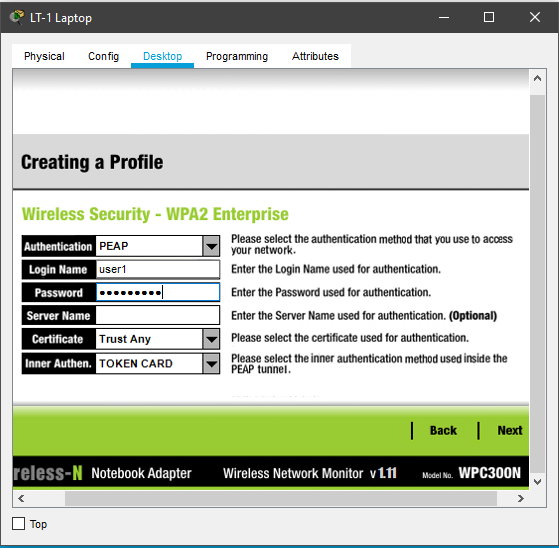
1. **Configure the wireless host (connecting laptop to the WLAN)**

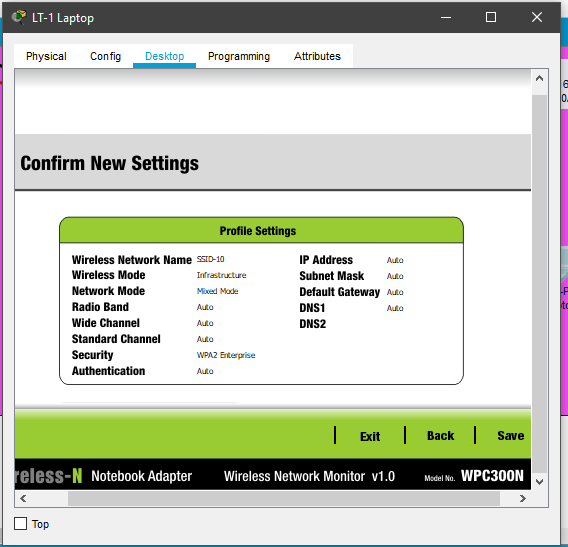
* Create a new wireless profile on the host and use the name work net for the profile.
* Configure the profile for the SSID of the WLAN
* We use enterprise authentication with a username of user1 and password of user1Pass and connect to network.

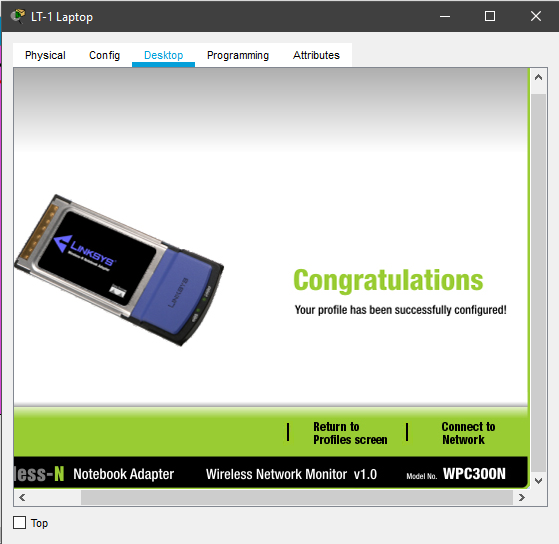






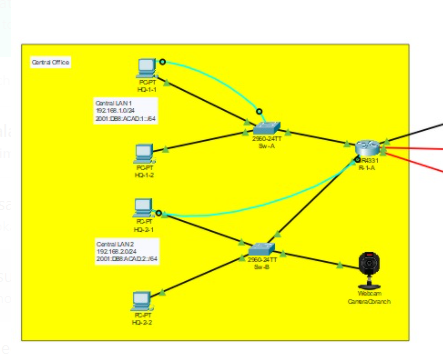








**Additional IoT Component:**



In our network, we added a camera for the surveillance purposes. The camera was placed in the central office and it was configured in a way that the authorize personal can access the device from anywhere in the network.