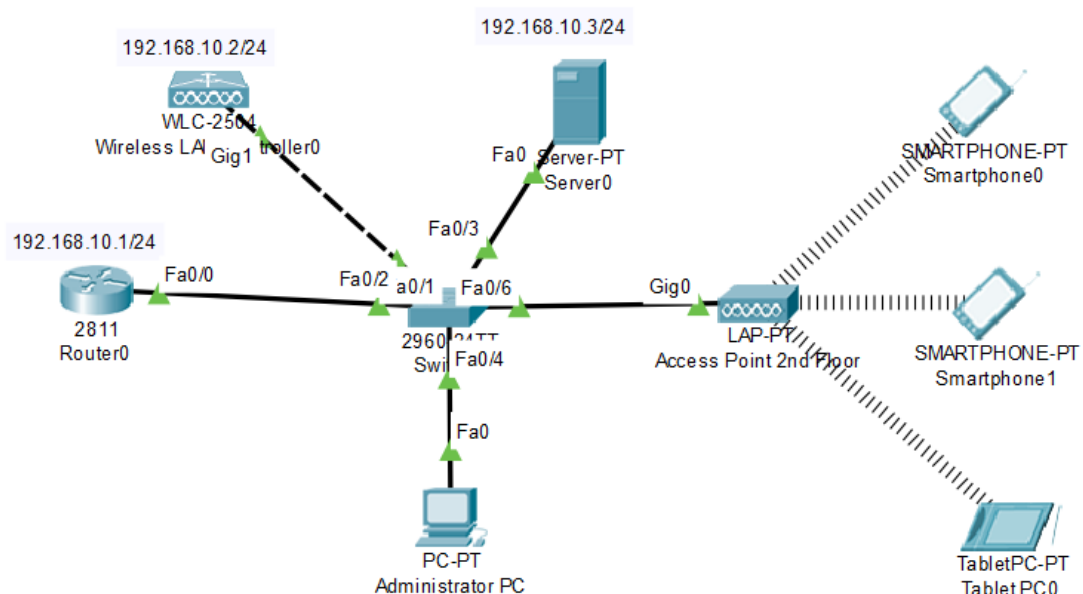


## WLAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. This gives users the ability to move around within the area and remain connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.



Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.

## Architecture

### Stations:

All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or non-portable devices such as desktop computers, printers, and workstations that are equipped with a wireless network interface.

**Basic service set:**

The basic service set (BSS) is a set of all stations that can communicate with each other at PHY layer. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

**Independent basic service set:**

An IBSS is a set of STAs configured in ad hoc (peer-to-peer) mode.

**Extended service set:**

An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

**Distribution system:**

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use.

## Types of wireless LANs

The IEEE 802.11 has two basic modes of operation: infrastructure and ad hoc mode. In ad hoc mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through a wireless access point (WAP) that serves as a bridge to other networks (such as the Internet or a local area network).

Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms: Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2, WPA3), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network.

Short for Wi-Fi Protected Access 2 - Pre-Shared Key, and also called WPA or WPA2 Personal, it is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server.

## WPA2-PSK

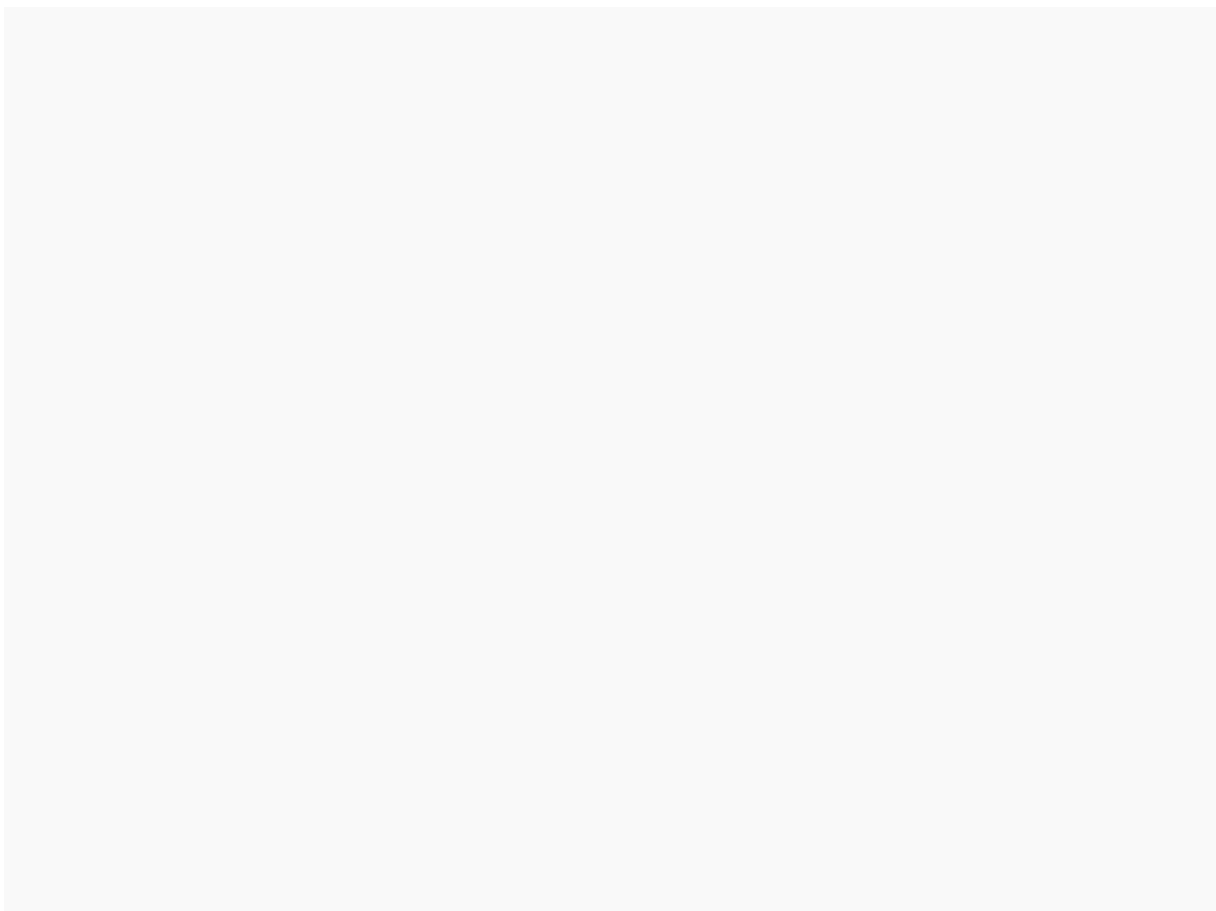
To encrypt a network with WPA2-PSK you provide your router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called TKIP (for Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. Although WEP also supports passphrases, it does so only as a way to more easily create static keys, which are usually comprised of the hex characters 0-9 and A-F.

## AAA in networking

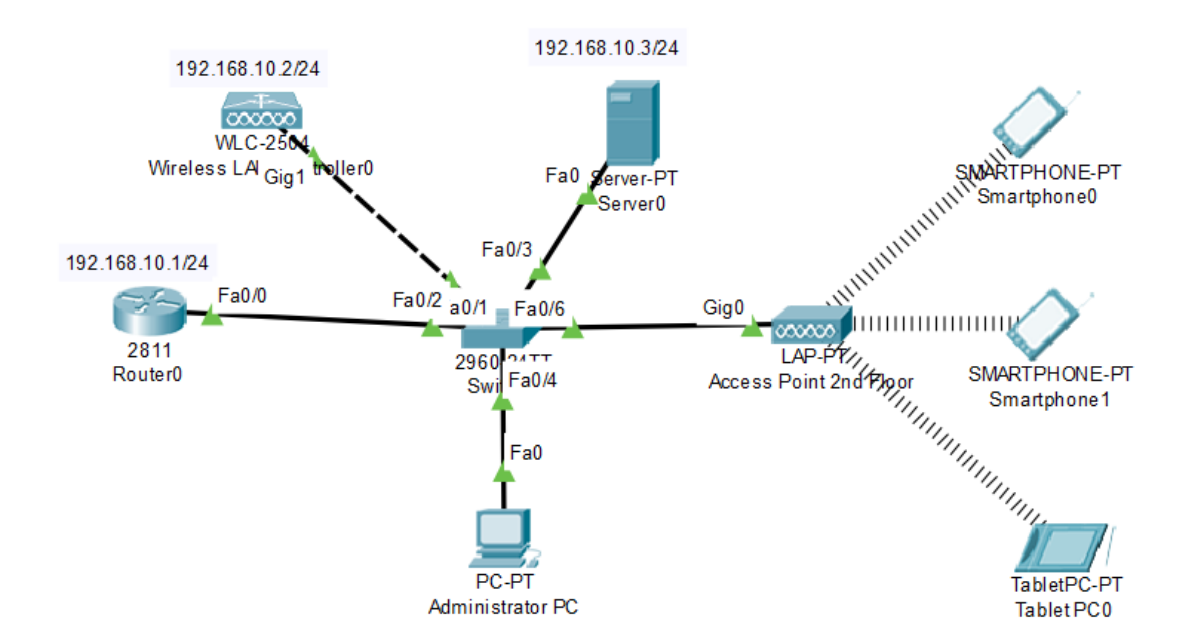
AAA stands for authentication, authorization, and accounting. AAA is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

Usually, **authorization** occurs within the context of **authentication**. Once you have **authenticated** a user, they may be authorized for different types of access or activity. The final plank in the AAA framework is **accounting**, which measures the resources a user consumes during access.

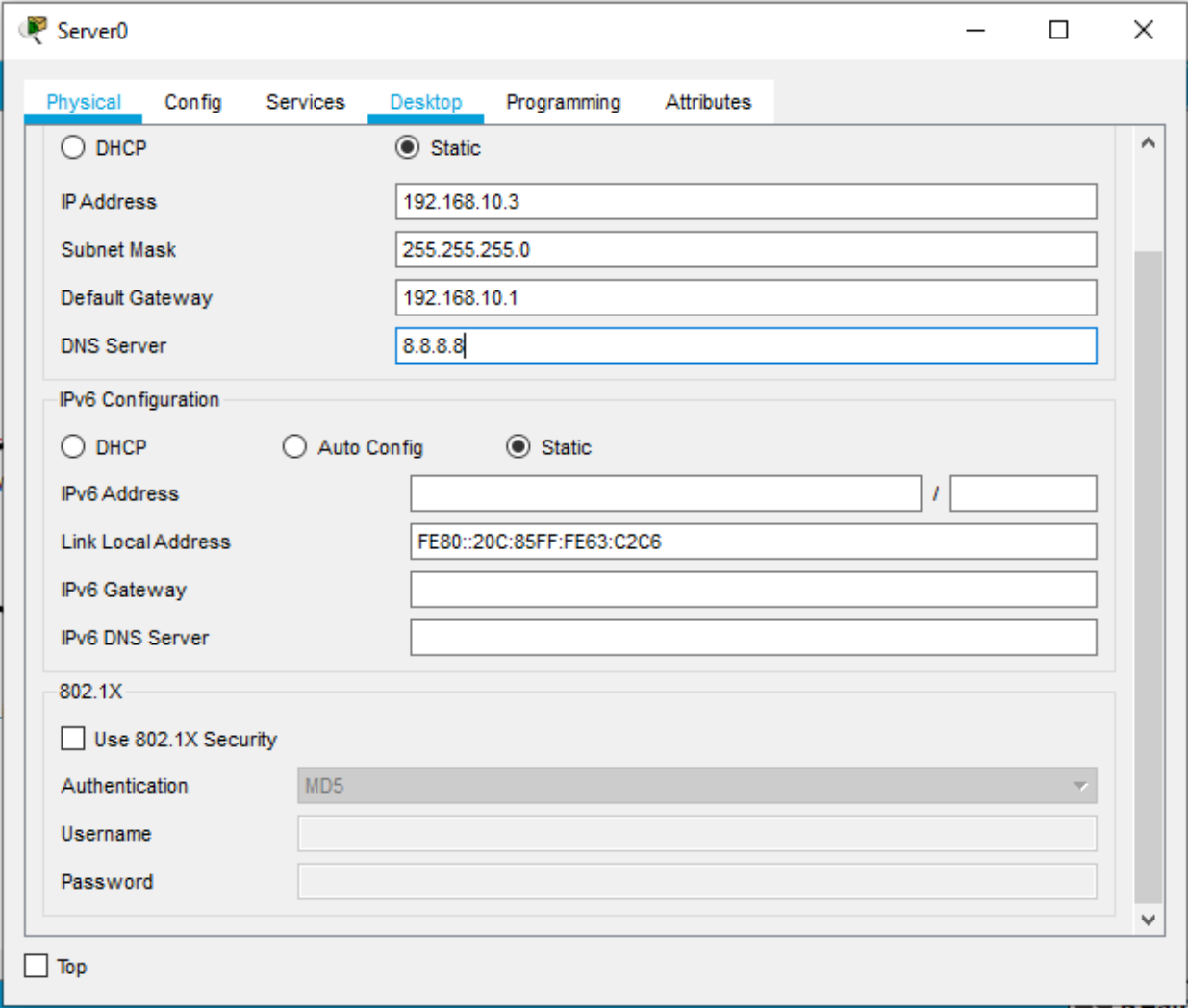
The AAA profile configures the authentication for a WLAN. The AAA profile defines the type of authentication (802.1X in this example), the authentication Device group, and the default user role for authenticated users.



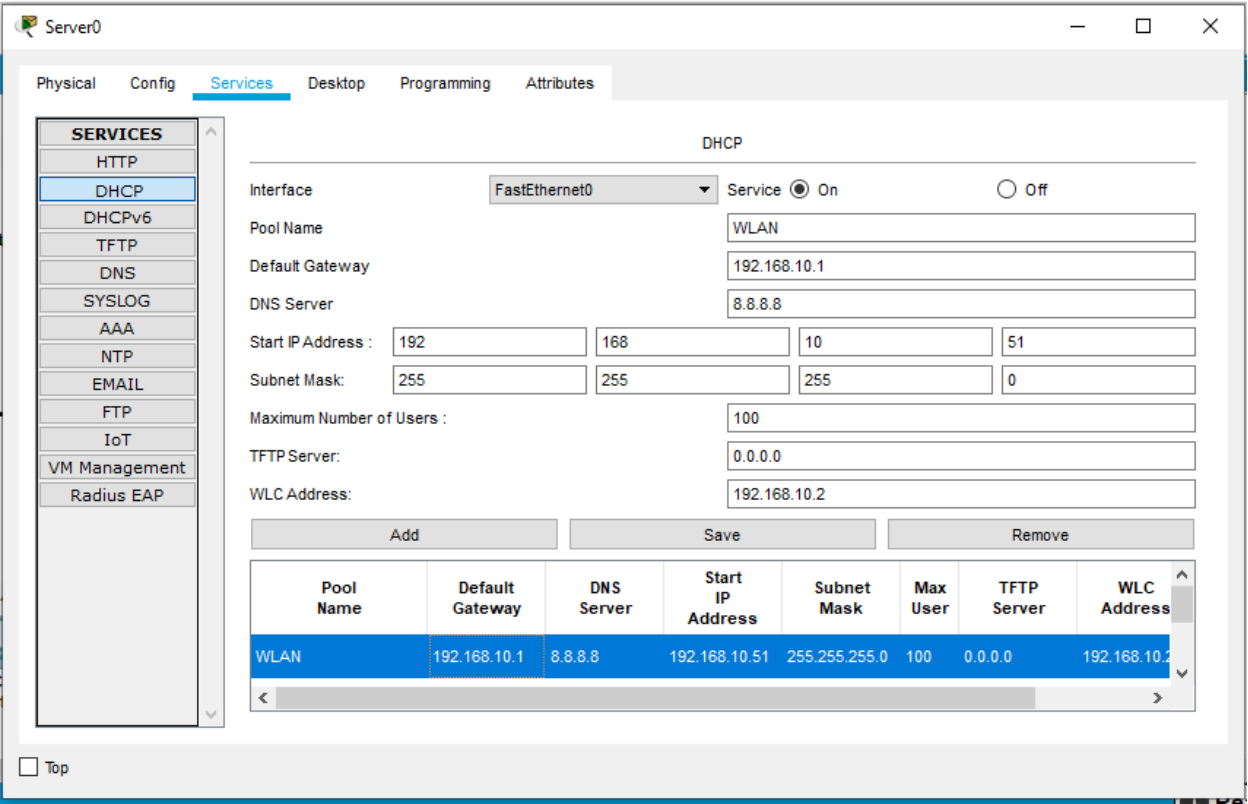
# Configure WLAN using WPA2 PSK and AAA using the GUI



First of we will configure Basic Configuration and DHCP in Server



Static IP Configuration in Server 0



DHCP Configuration in Server 0

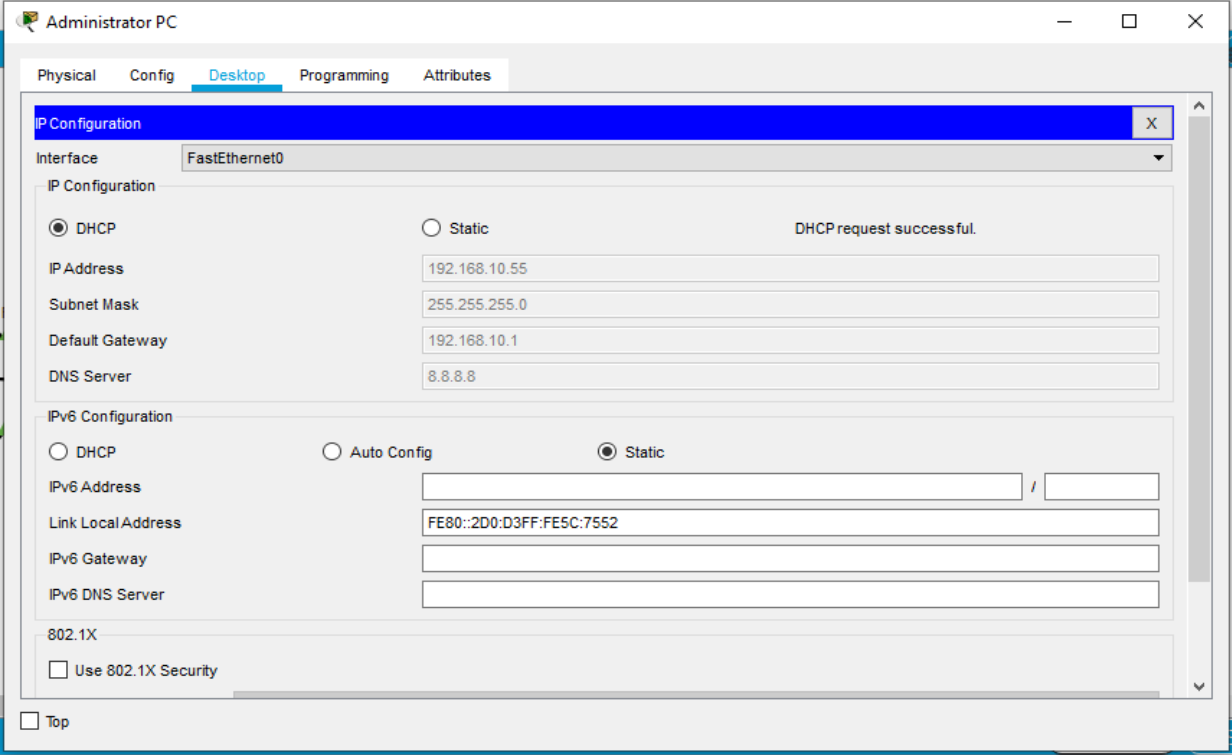
Now we will configure IP Address in Router Interface:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown

Router#show ip interface brief
```

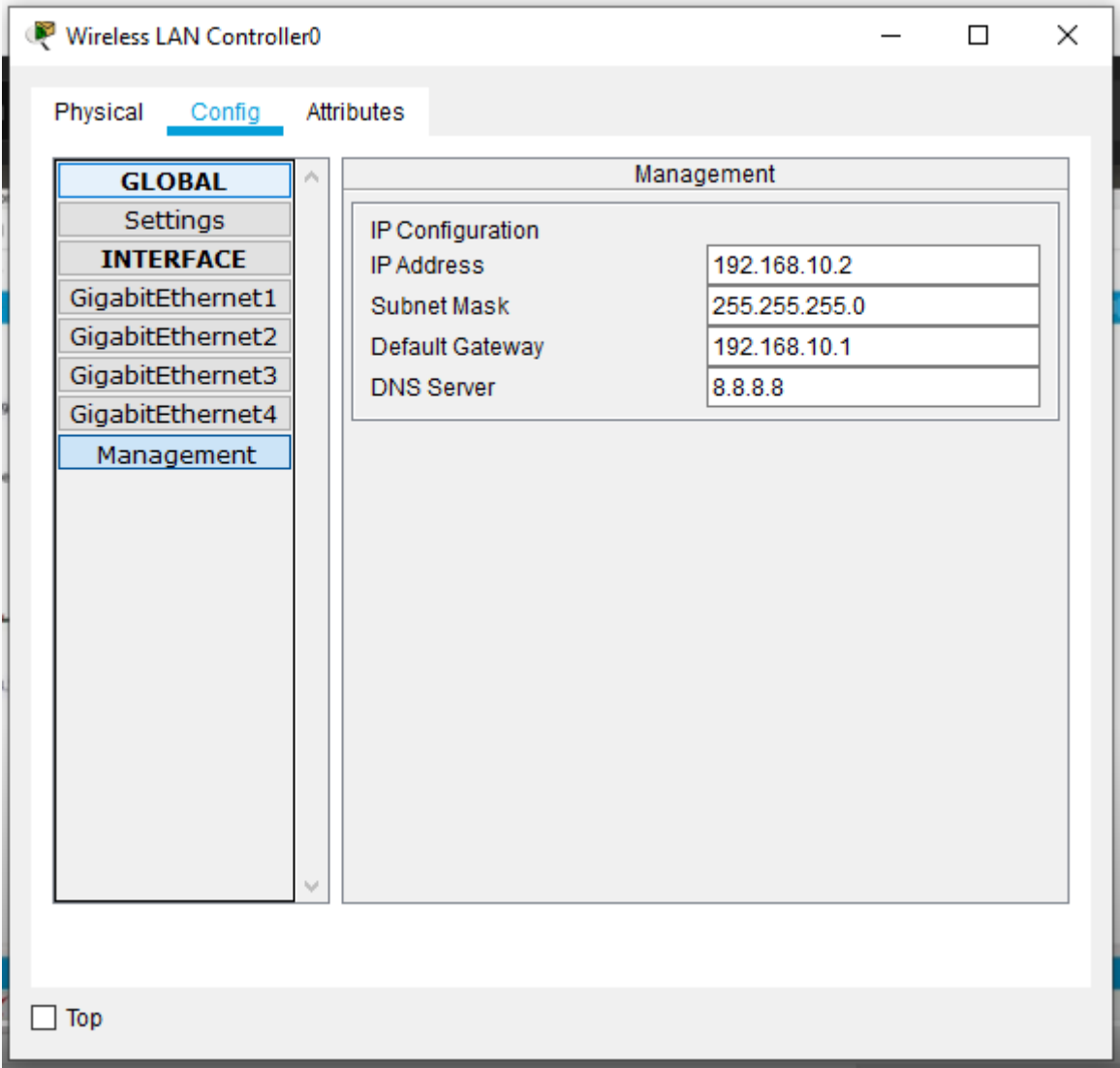
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.10.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

Configure DHCP IP Address in Administrator PC:



DHCP IP Address in Administrator PC

Now Static IP configuration in Management interface of WLC Device:



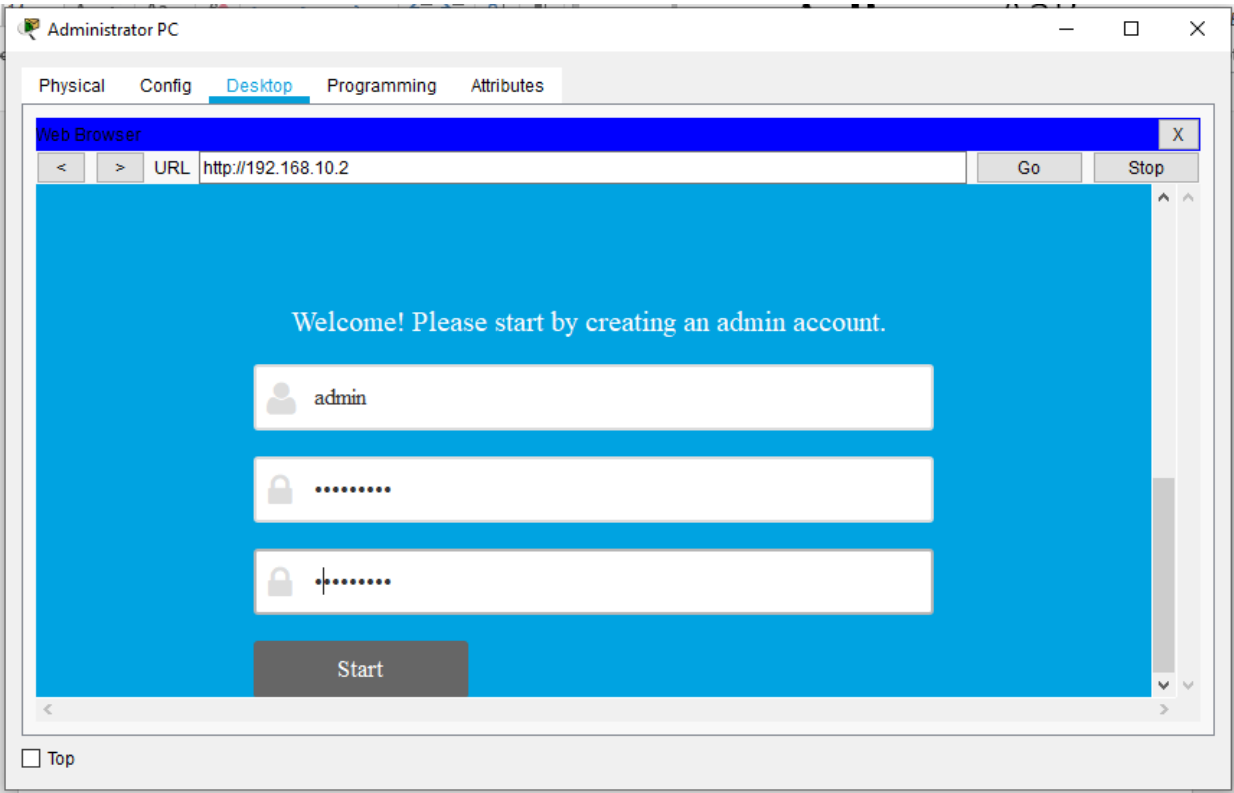
Static IP Address in WLC

Basic Configuration for this LAB has been finished. Now we will go for Configuring WLAN using WPA2 PSK and AAA using the GUI.

Go to Web Browser of Administrator PC and type WLC IP Address (192.168.10.2) then hit enter.



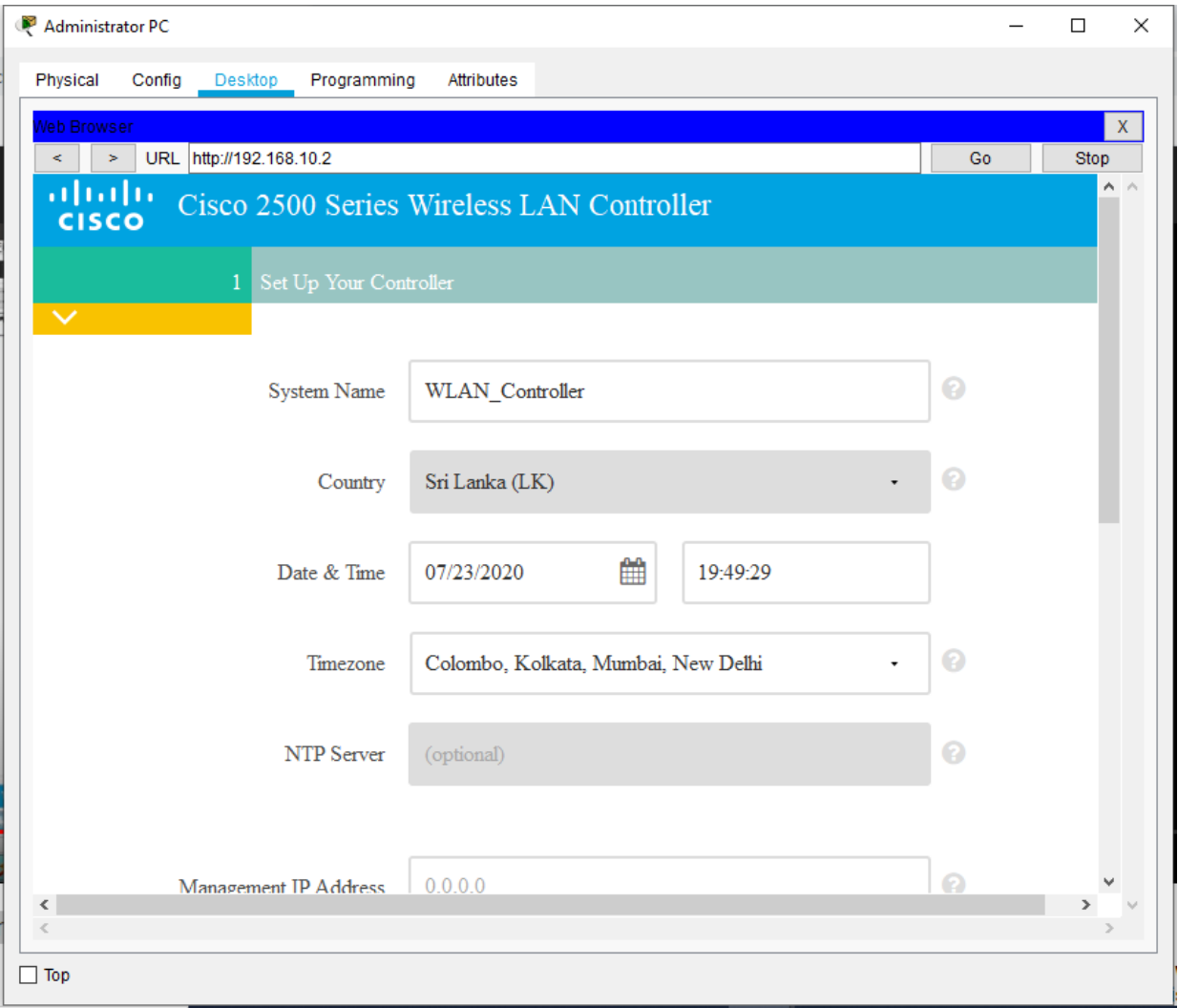
Scroll down and Create Administrator Account and Password:

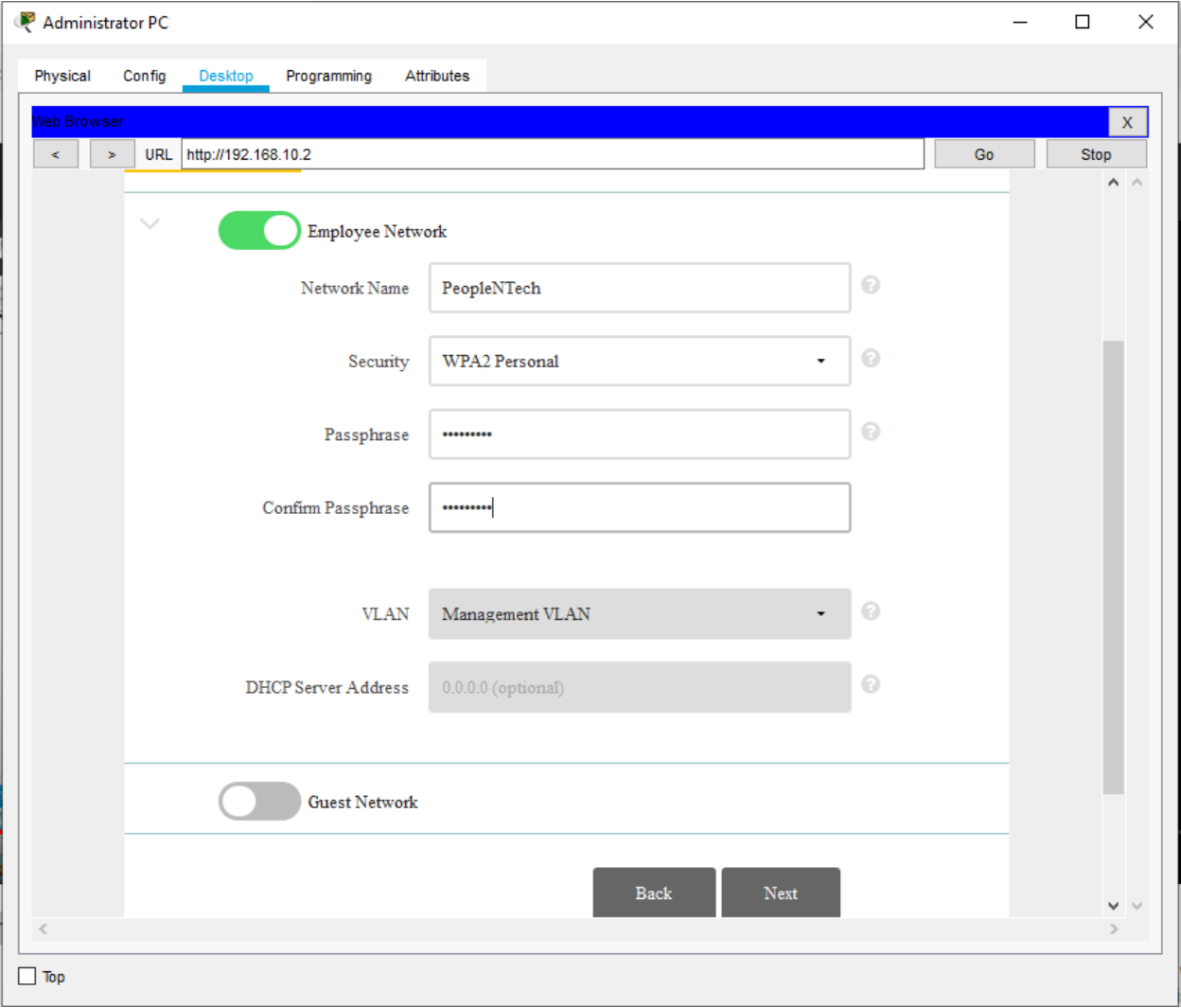
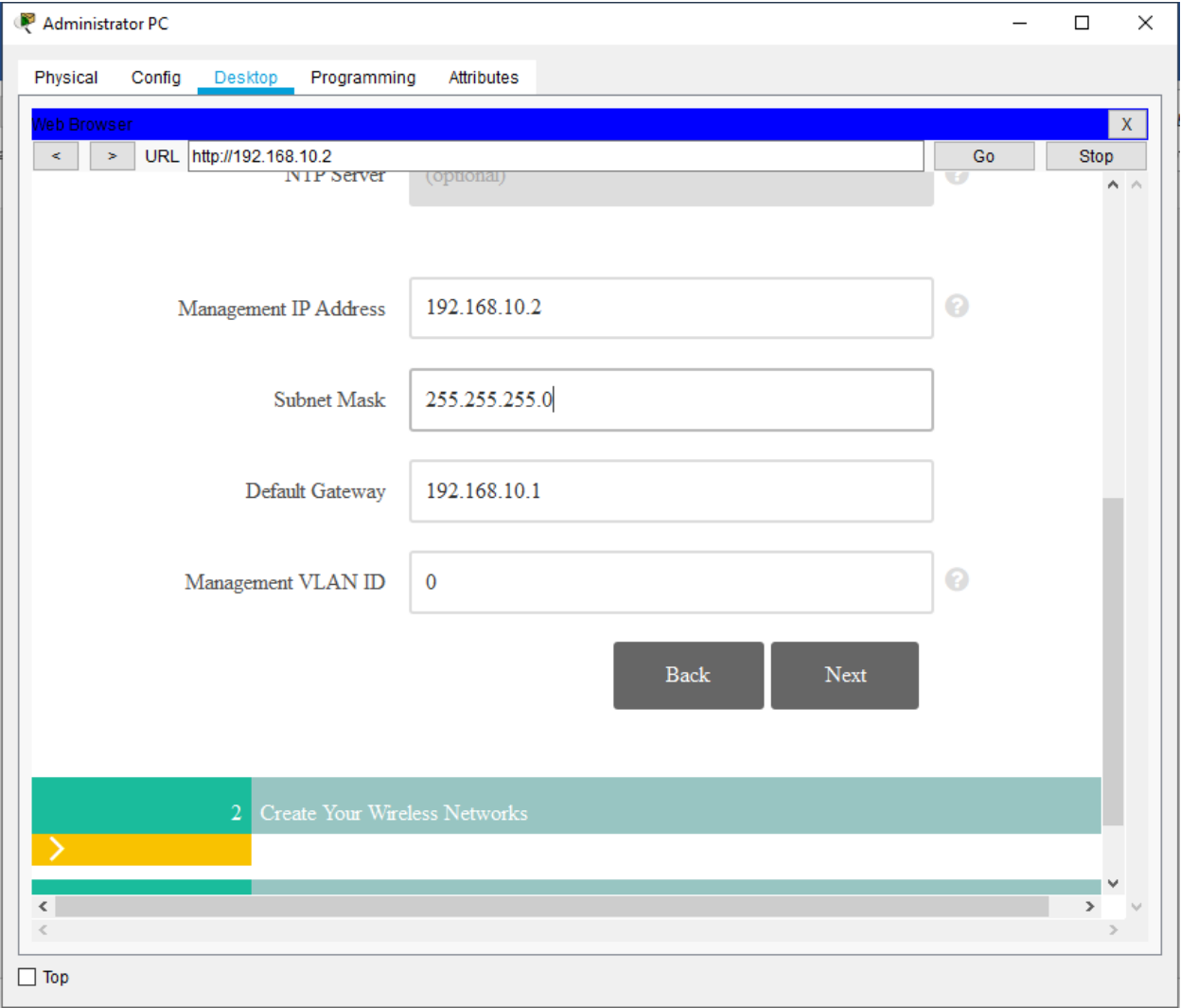


My user is admin and password is Cisco1234

Now Click on Start.

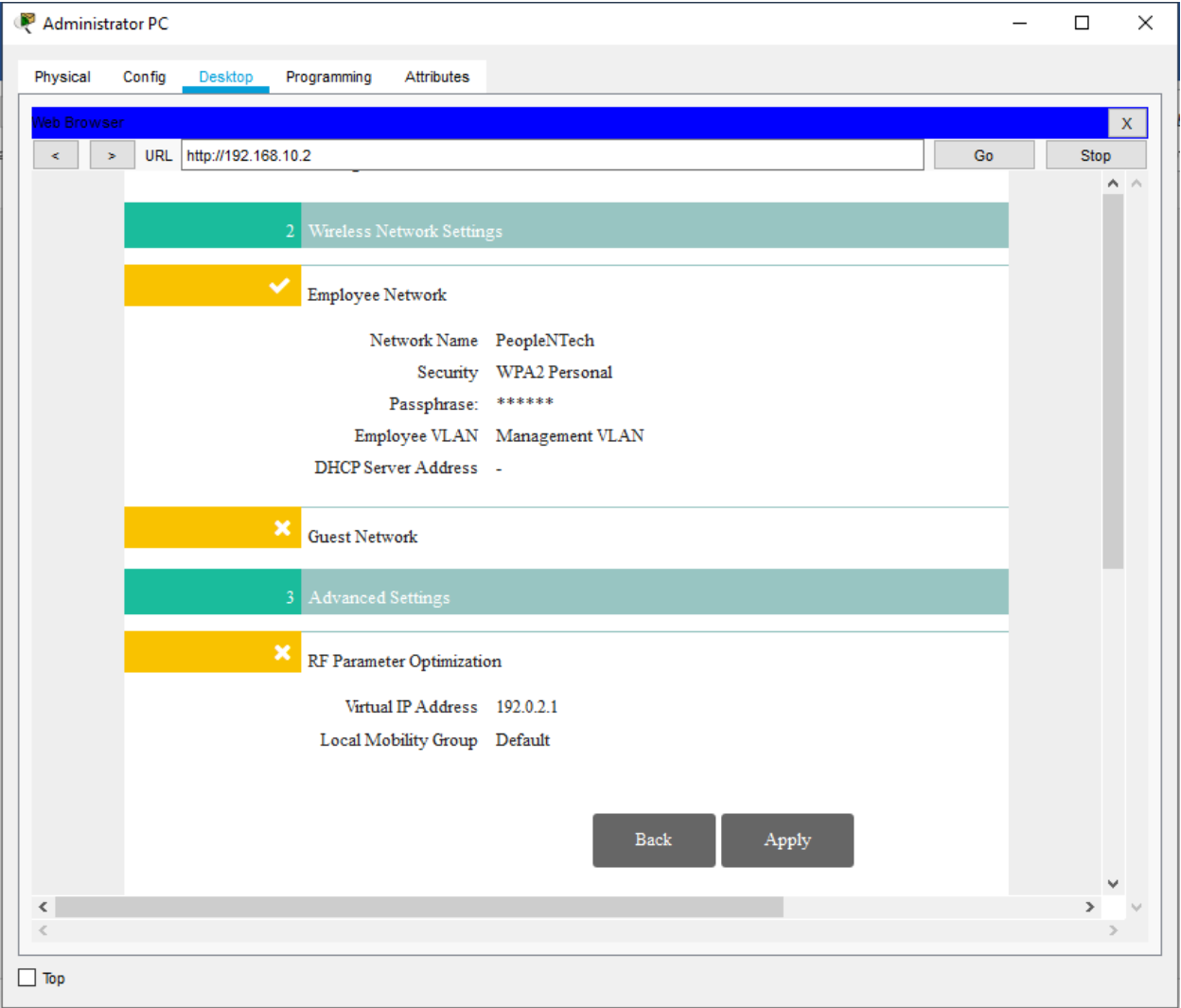
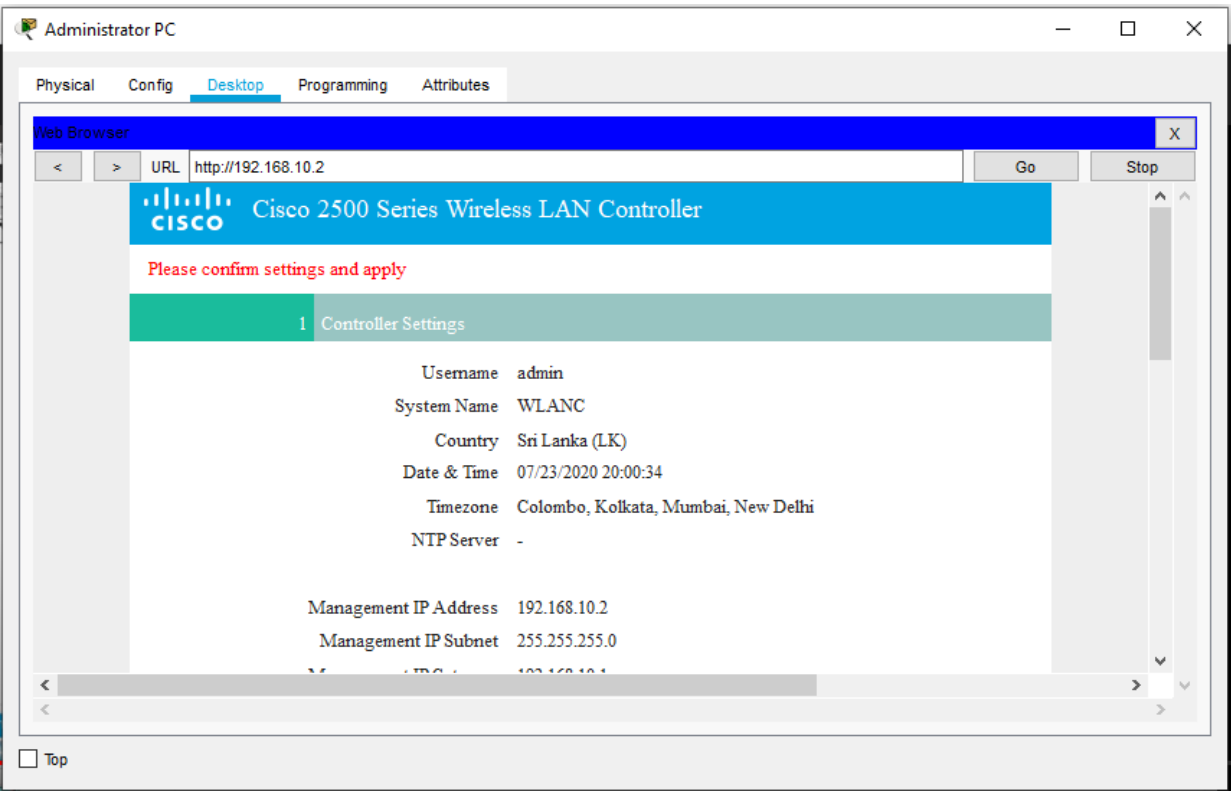
Configure WLC:





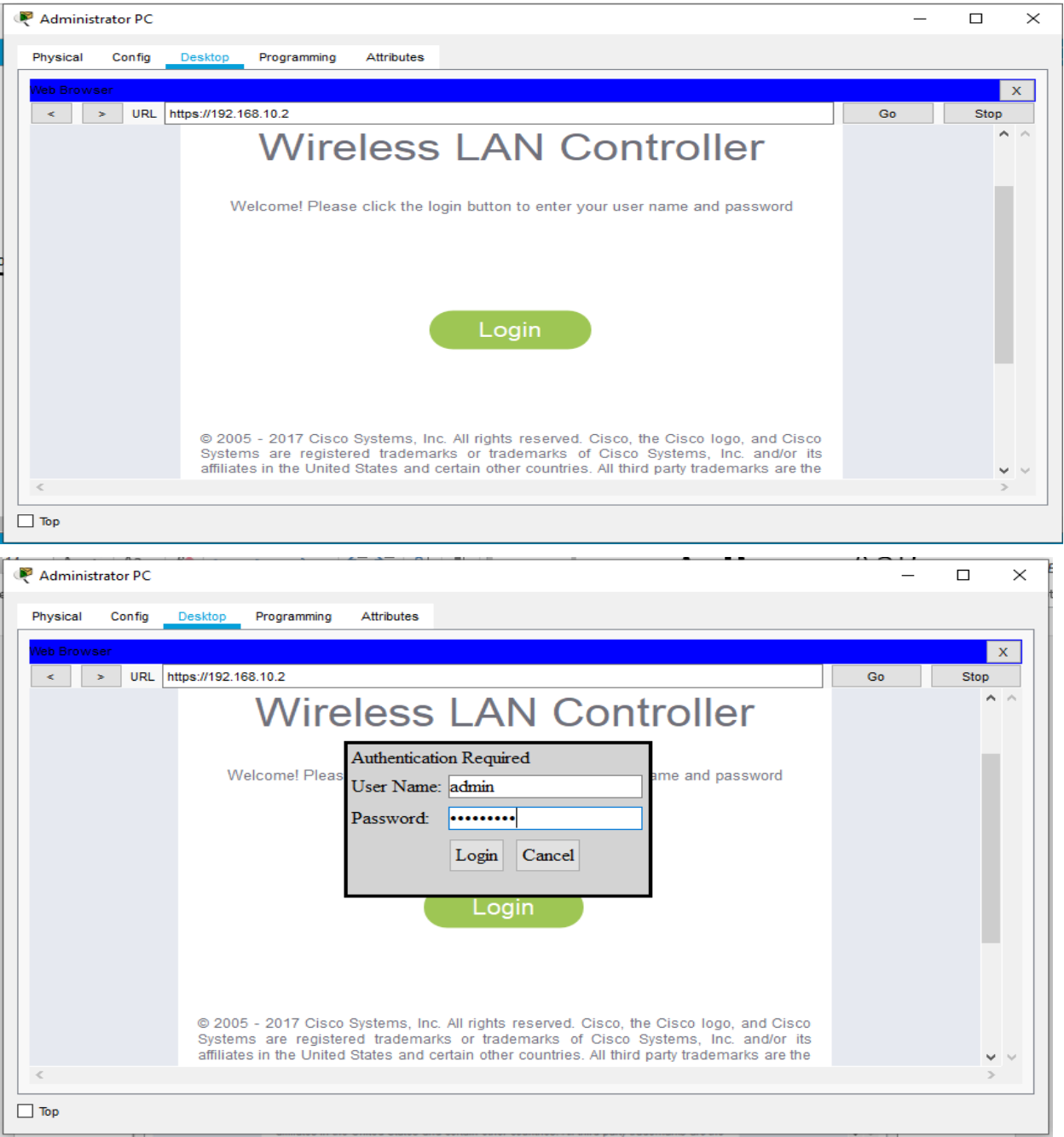
Here Network Name is your SSID



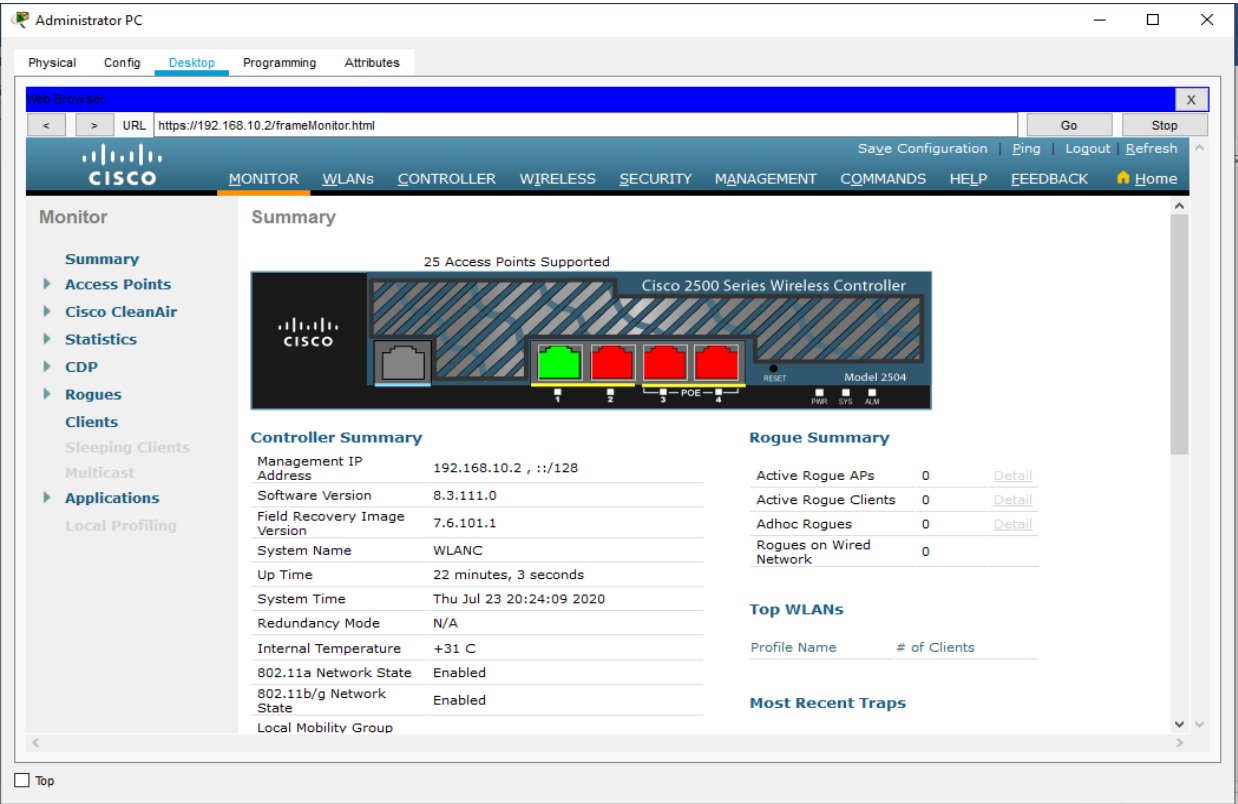


After Press Apply, The system will reboot

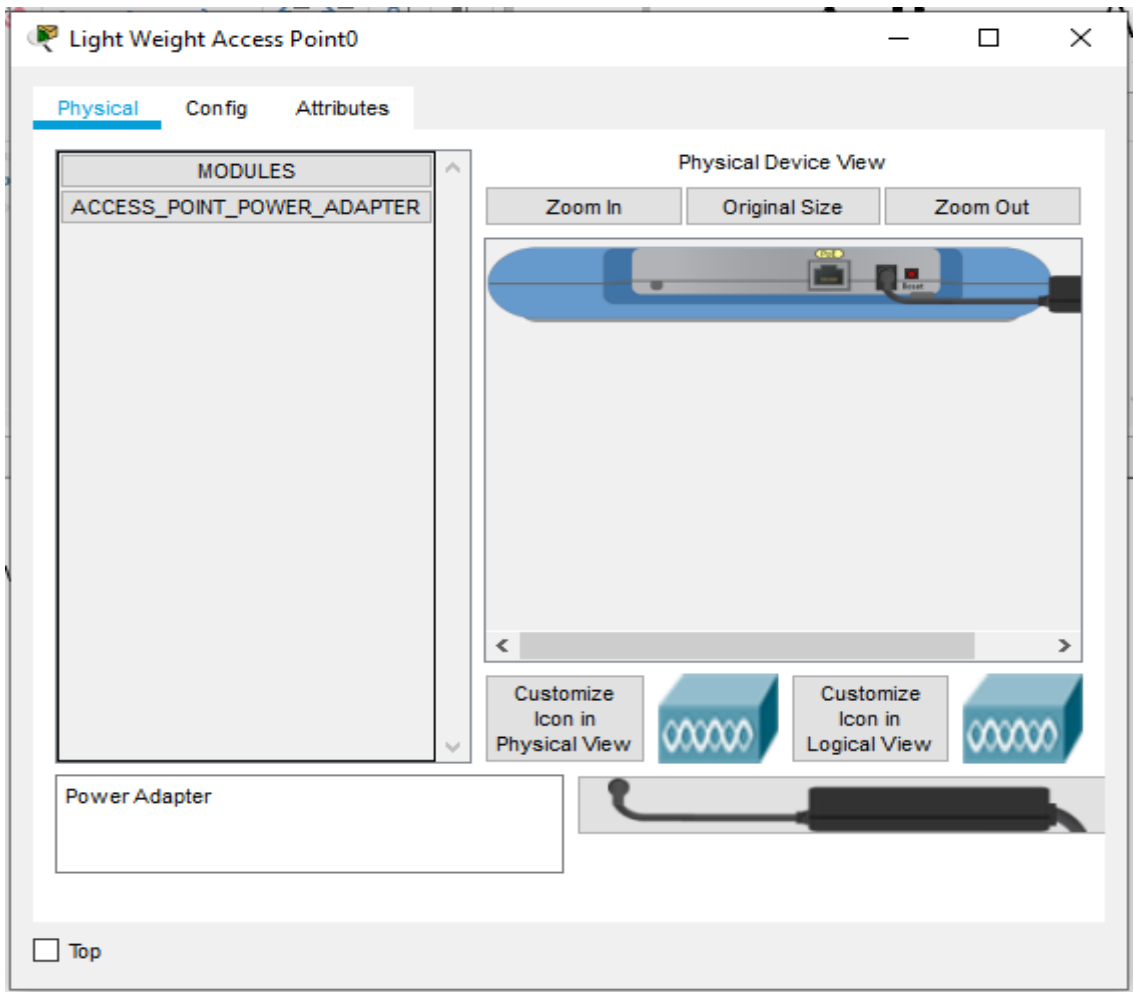
Now close the browser and open again. Now you have to browse WLC Device using https.



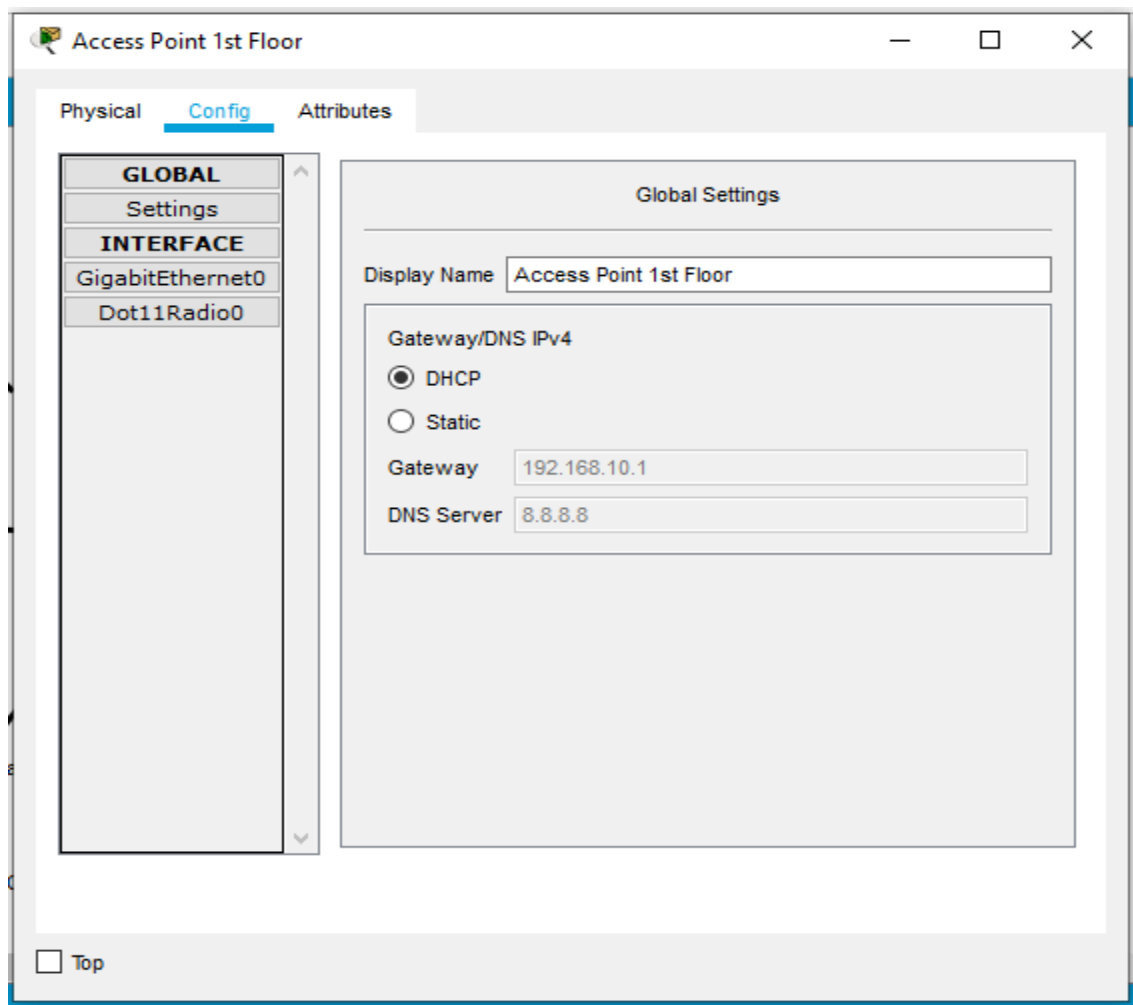
Interface will look like as follow:



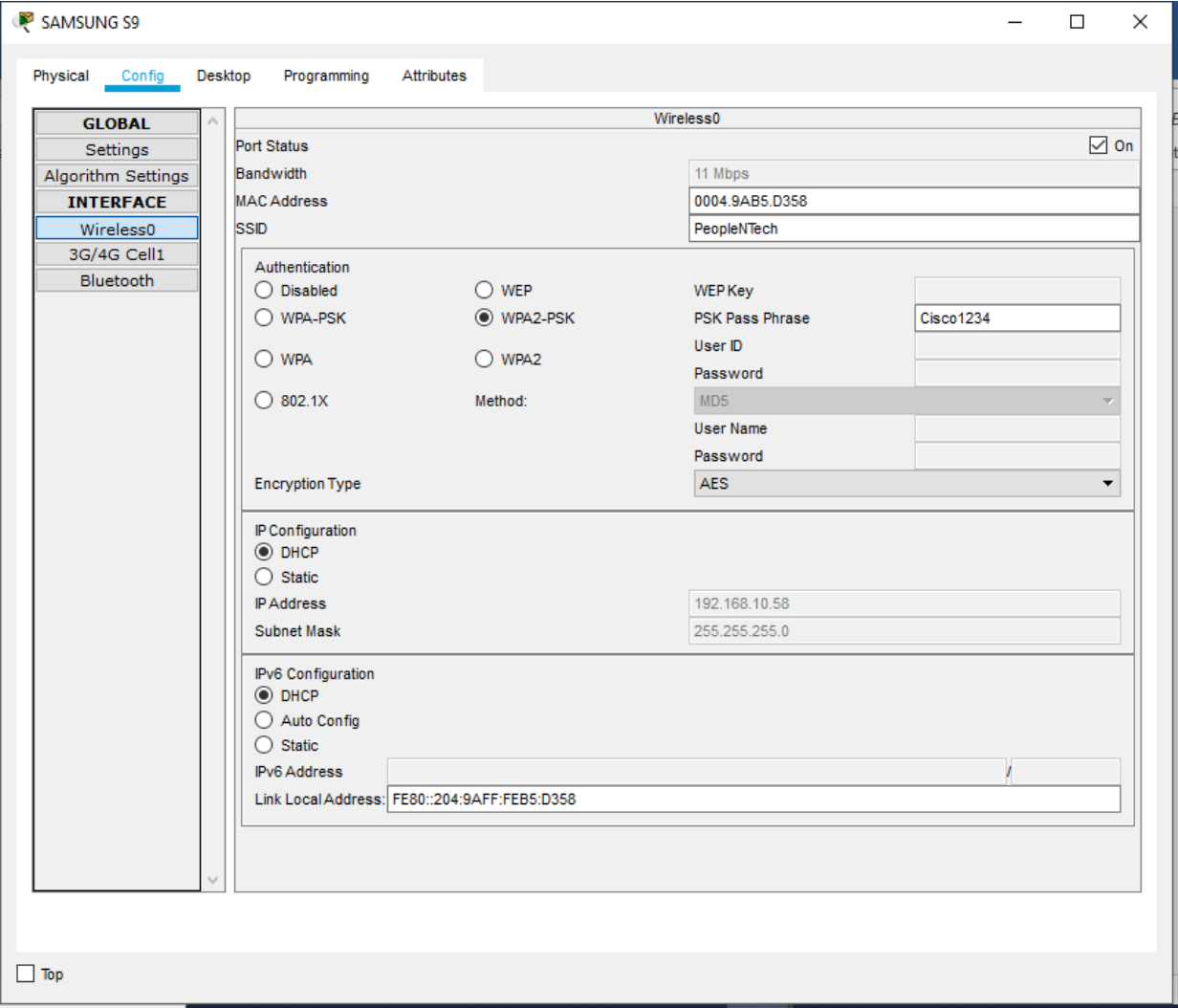
Now we will configure Access Point. Open Access Point and add a wireless LAN Card.



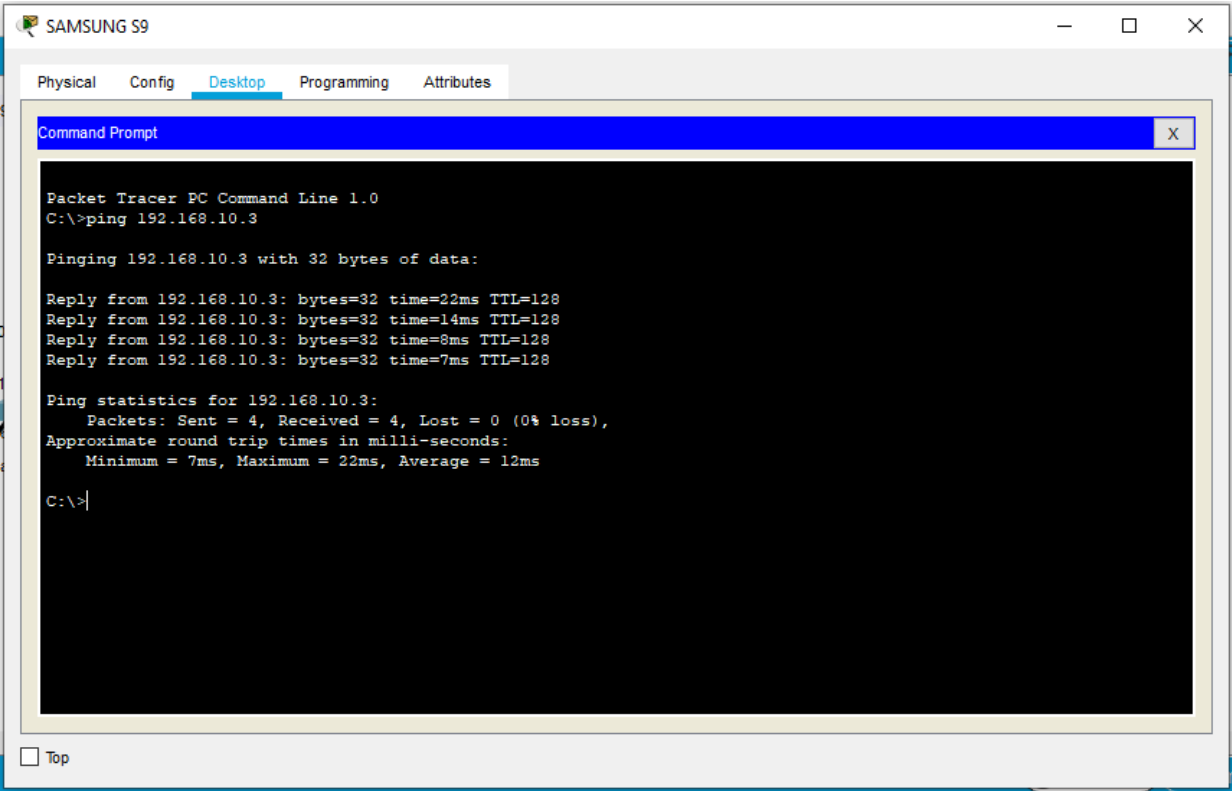
Click on config Tab and click on DHCP then see the Default Gateway and DNS already configured.



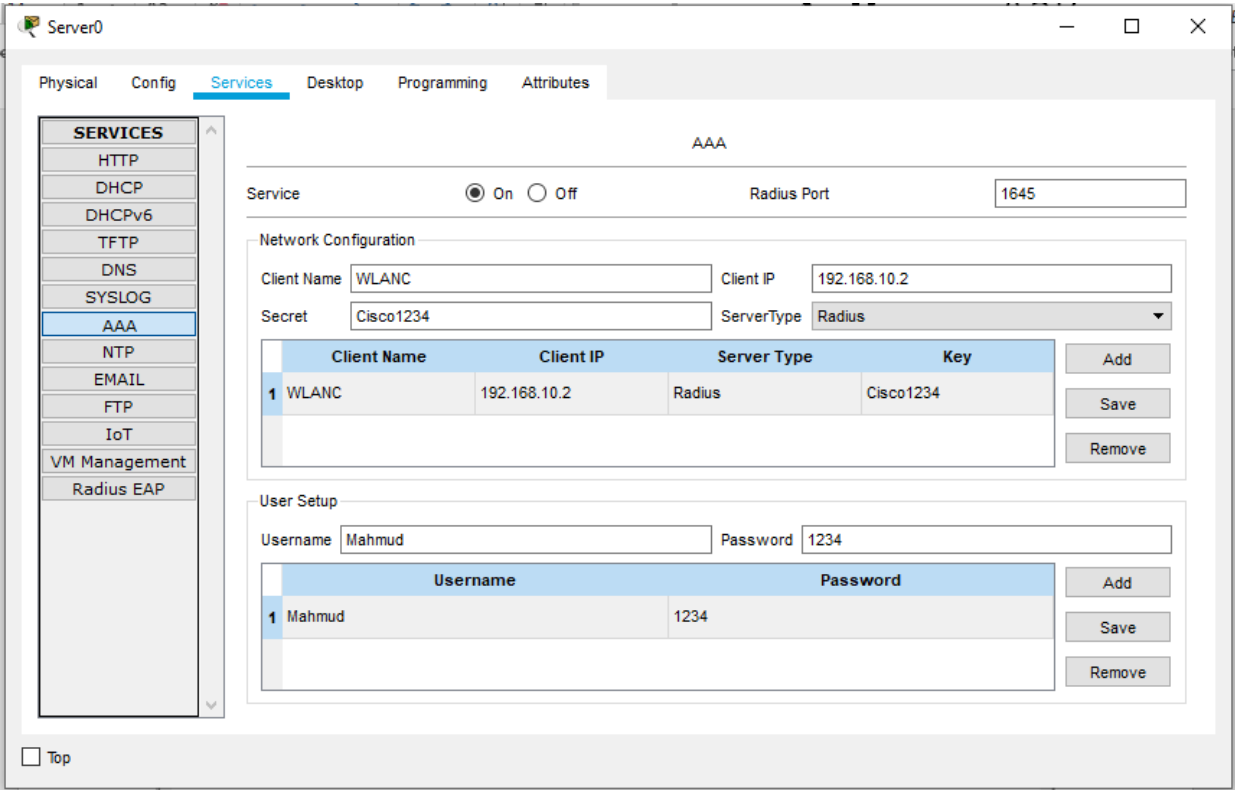
Now Open a Moblie Phone and Configure SSID and WAP2-PSK Pass Phrase and see the IP address already configured from DHCP Server.



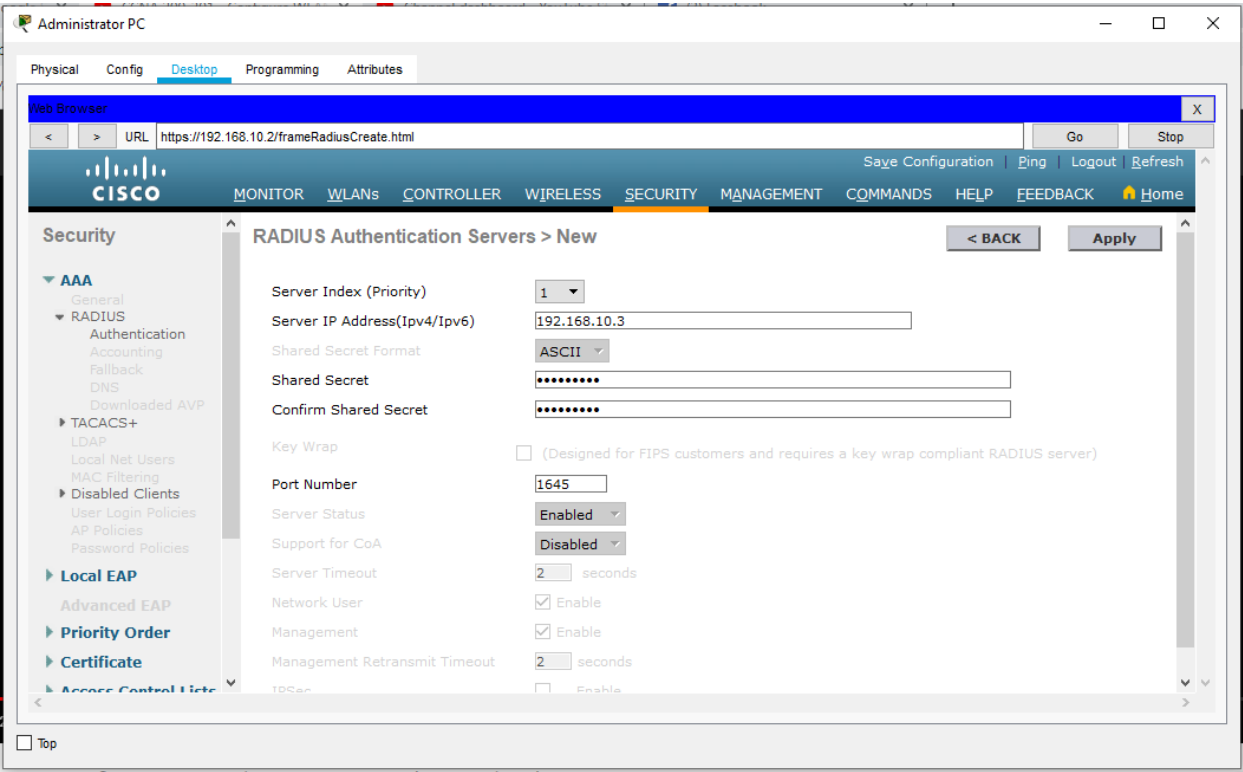
Now Ping From Mobile to Server:



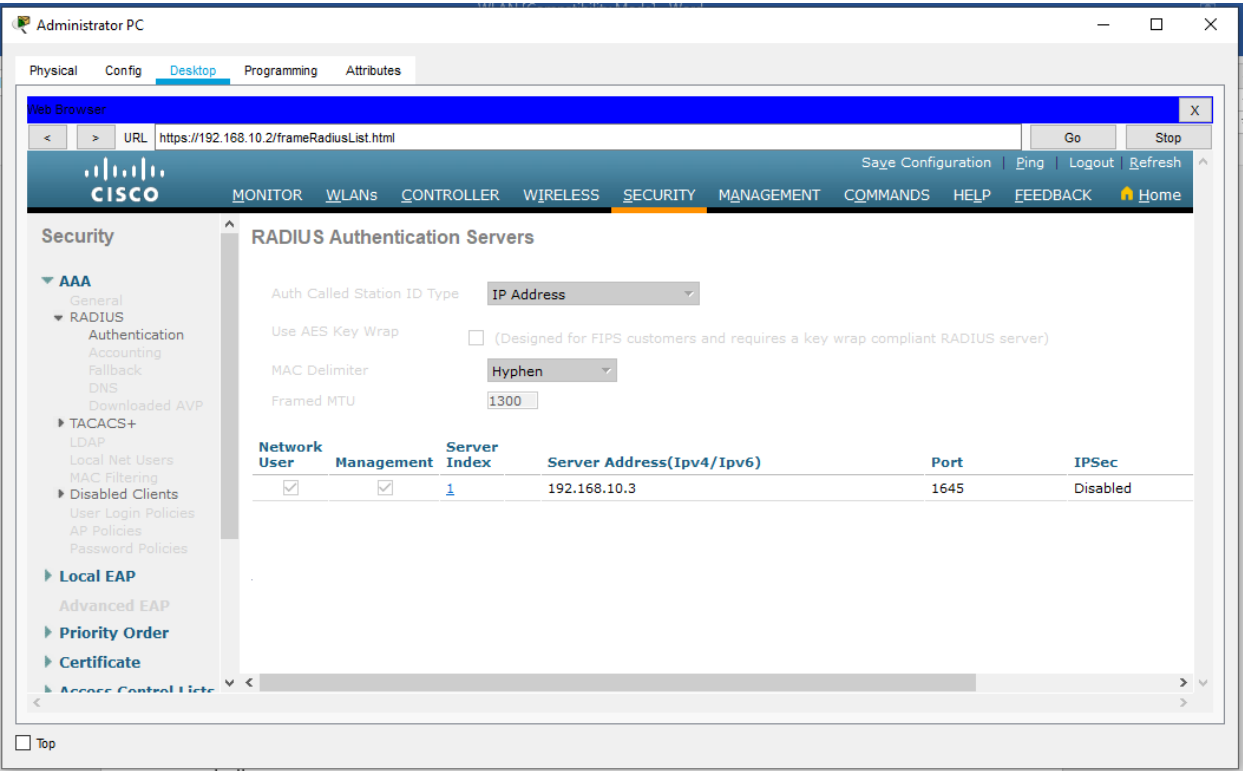
Now we will Apply AAA Authentication. Go to Server, Click on Services and Click on AAA:



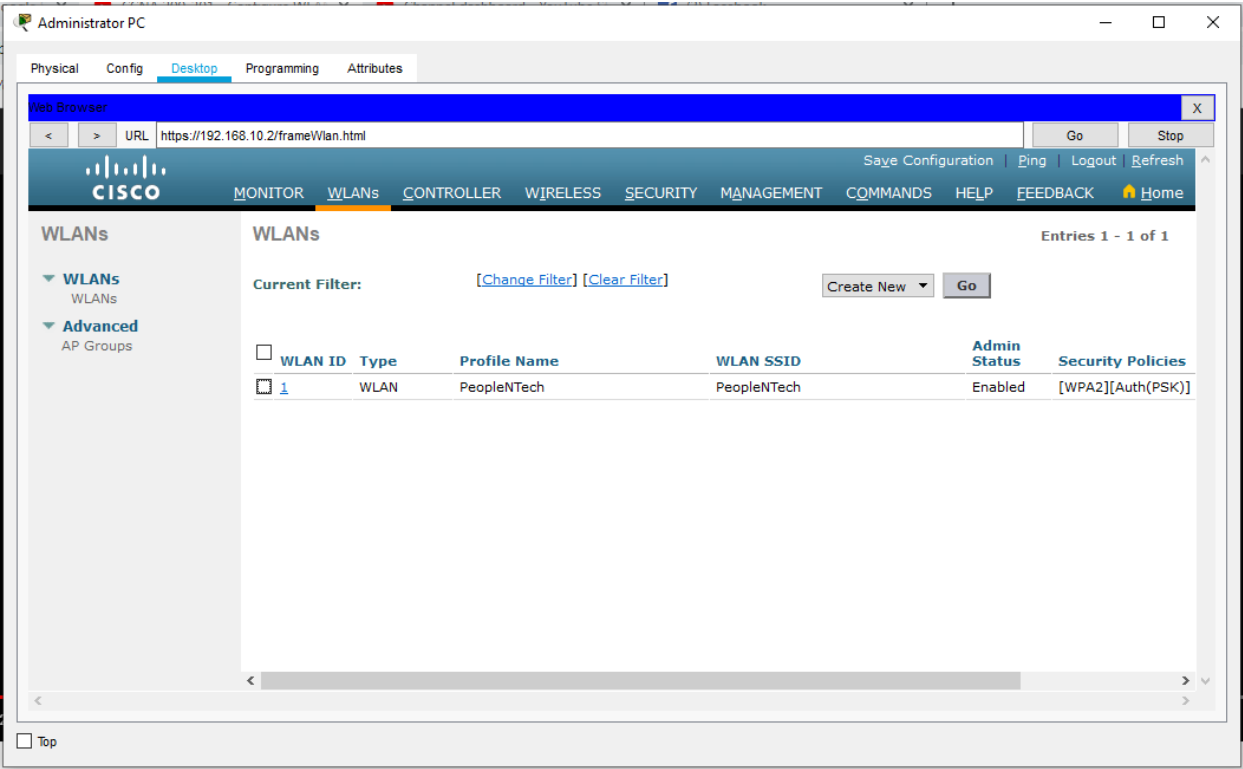
Now go to WLC Device using PC Browser. Click Security Tab, Click New and configure as follows:



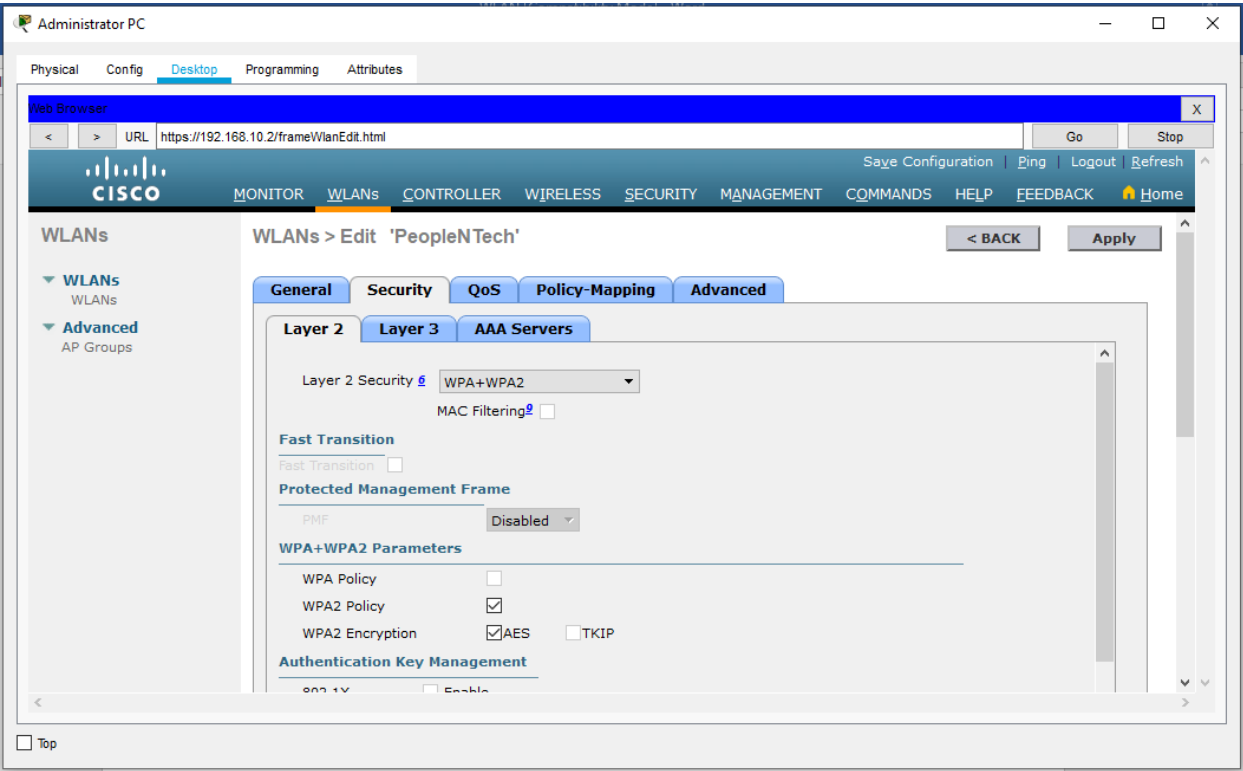
You will get Port Number in RADIS Server. Now click on apply. And Index will see as bellow:



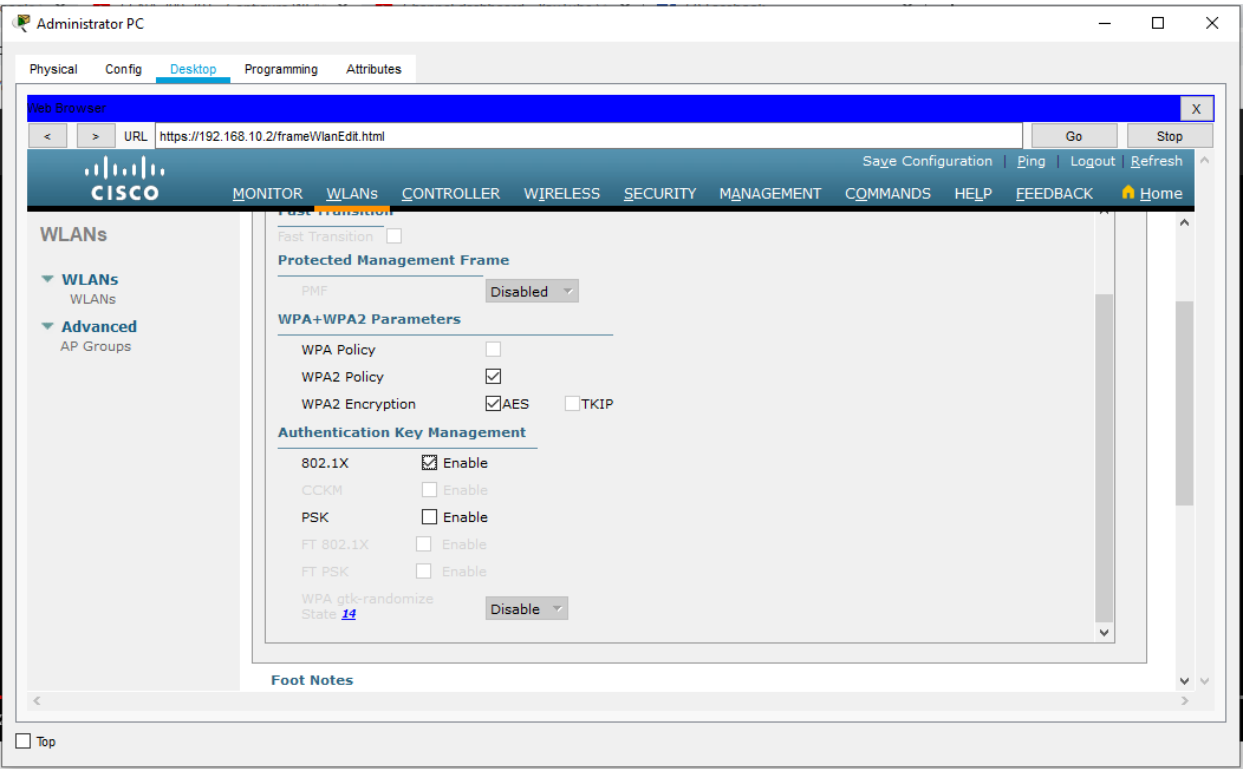
Click on WLANs and on 1 in the table:



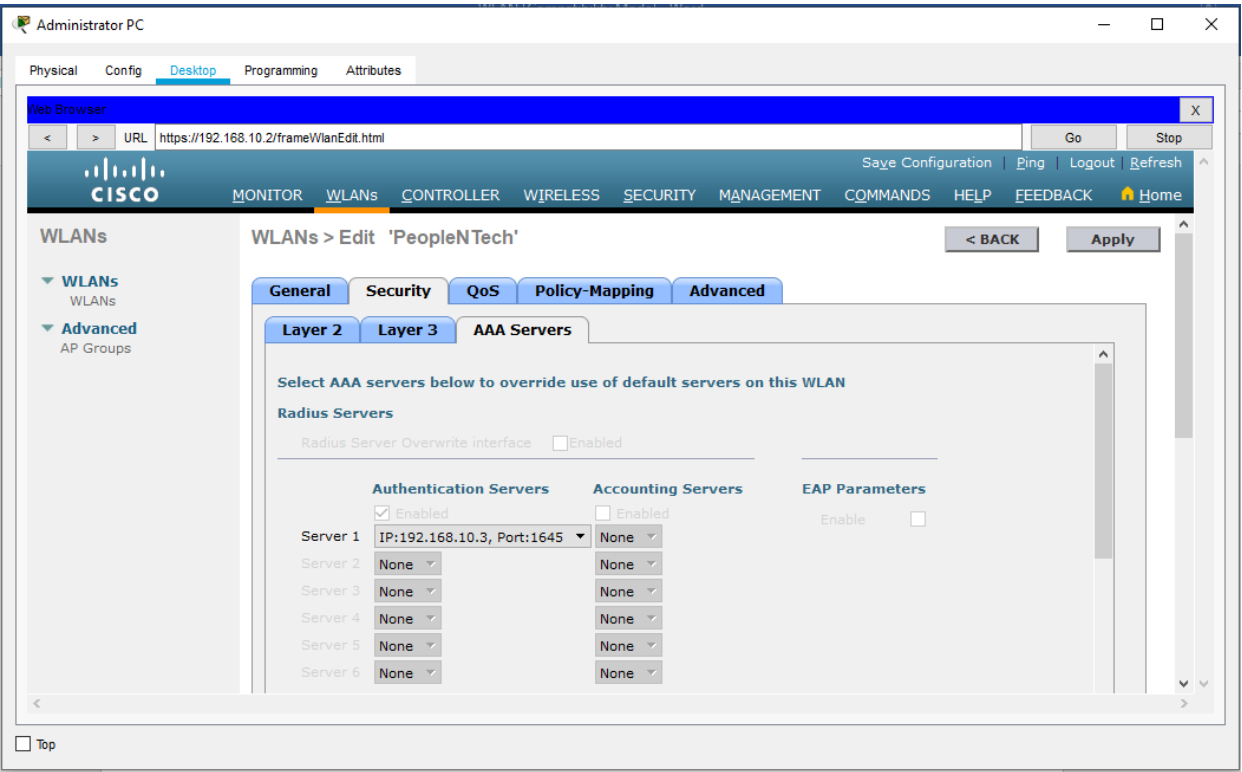
Click on Security Tab and Click on Layer 2 Tab:



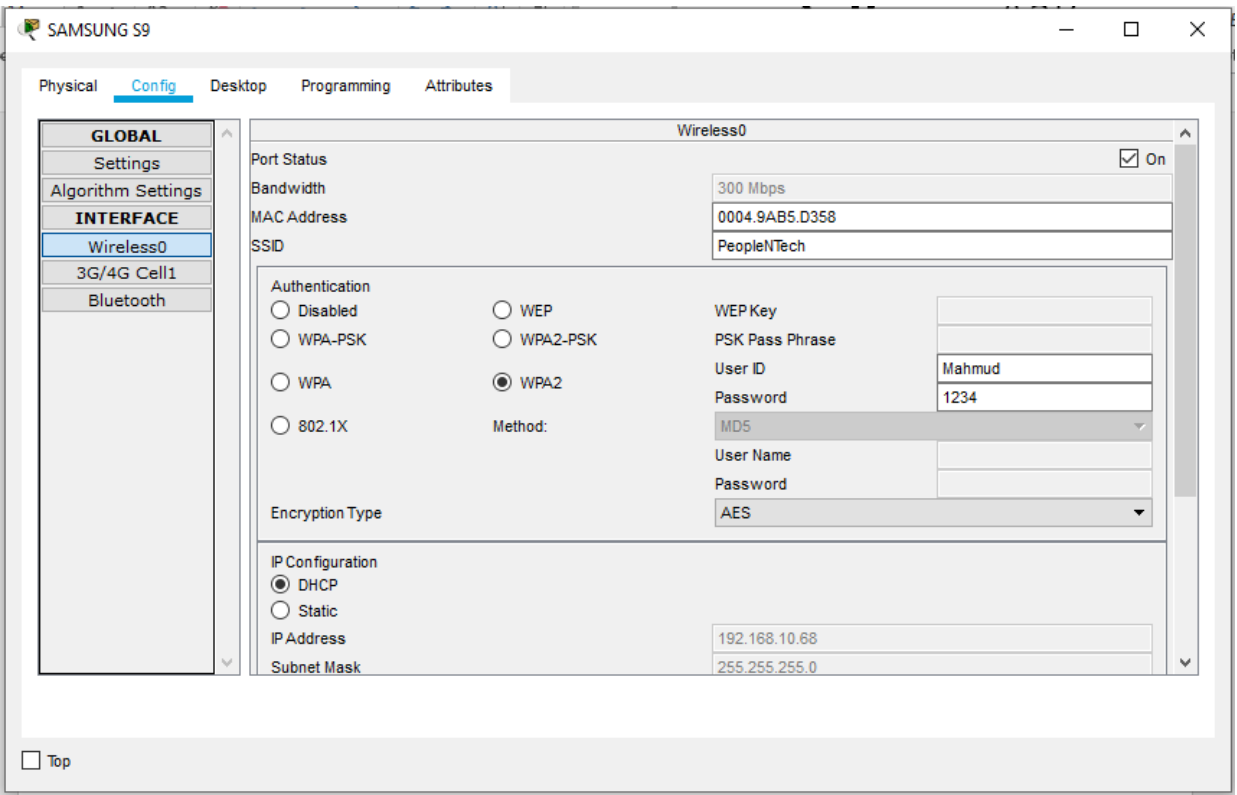
Now uncheck PSK and Check on 802.1X:



Now Click on AAA Server Tab. Select your Server IP and Port Number then Apply:

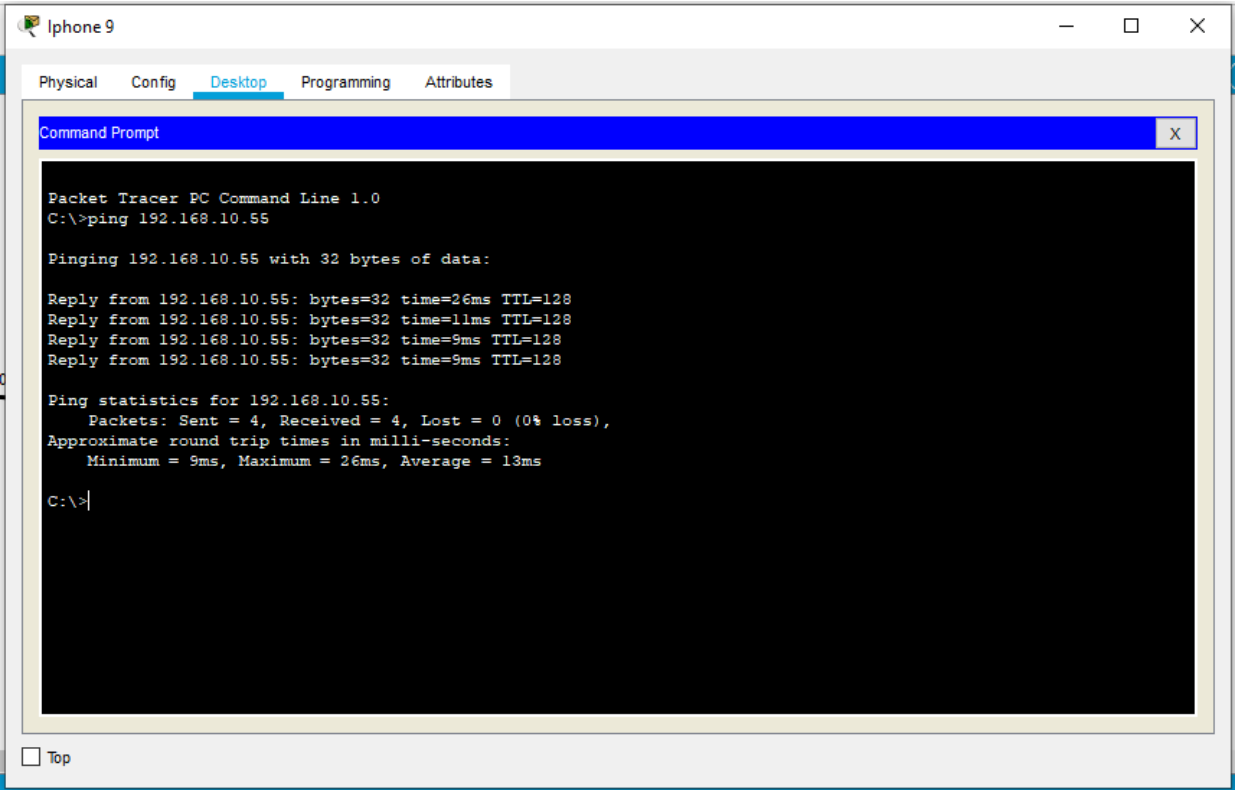


Now Go to Smart Phone, select on Wireless Interface and Click on WPA2 and set username and password:





Now you can ping from Mobile to Administrator PC:



This is all. Thank you very much.