

**Implementation MAC FILTERING and Switch Port Access For SOHO**

**Created By : David Ardian Alim**

**Septian Nugroho**

**Class : 4NAP2**

**Faculty : Tri Agus Riyadi, S.Kom., MT**

**Semester : 4**

**Quarter : 1**

Continuing Education Program Center for Computing and Information Technology

Faculty of Engineering, University of Indonesia

2020

**PROJECT ON**

**Implementation MAC FILTERING and Switch Port Access For SOHO**

**Developed by**

**Name : David Ardian Alim**

**Reg. No :**

**Name : Septian Nugroho**

**Reg. No : 1801010266**

****

Batch Code : 4 NAP 2

Start Date : 03 April 2020

End Date : 20April 2020

Name of Coordinator : Tri Agus Riyadi, S.Kom., MT

Names of Developer : David Ardian Alim

Septian Nugroho

Date of Submission: 23 of April 2020

**MAC Address Filtering and Switchport for SOHO**

****

**CERTIFICATE**

This is to certify that this report titled ***“* *Implementation MAC FILTERING and Switch Port Access For SOHO”*** embodies the original work done by ***David Aardian Alim and Septian Nugroho*** in partial fulfillment of their course requirement at NIIT and CompTIA.

Coordinator:

Tri Agus Riyadi, S.Kom., MT

**ACKNOWLEDGEMENT**

Authors have benefited lot from the feedback and suggestions given to Author by Mr. Tri Agus Riyadi, S.Kom, MT and other faculty members. Therefore, authors feel very grateful that can be a part of this project.

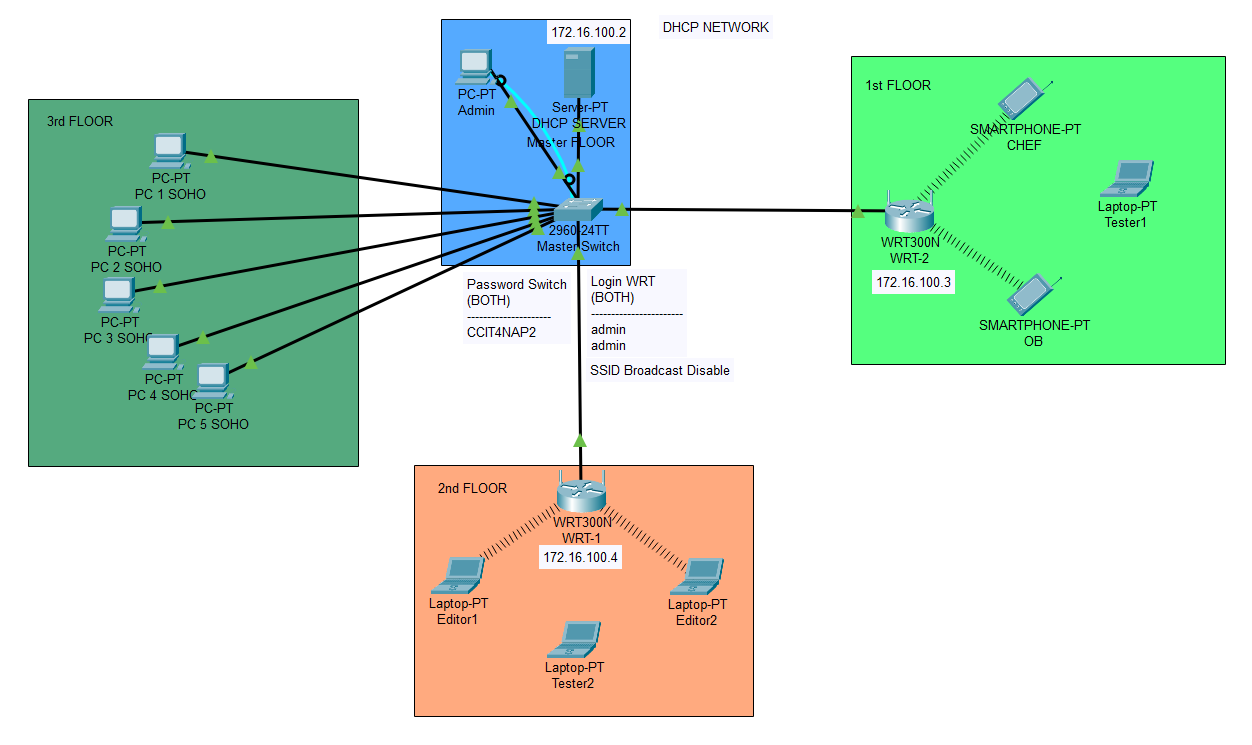
Author Project assignment can’t be good as it now without any help, feedback and suggestion that given to Author by Author friends within the campus. So, authors say thanks to all of them.

**SYSTEM ANALYSIS**

**System Summary :**

Implementation Mac Filtering and Switch Port Access For SOHO is a project to explain how to secure the network from phising and freeloaders.

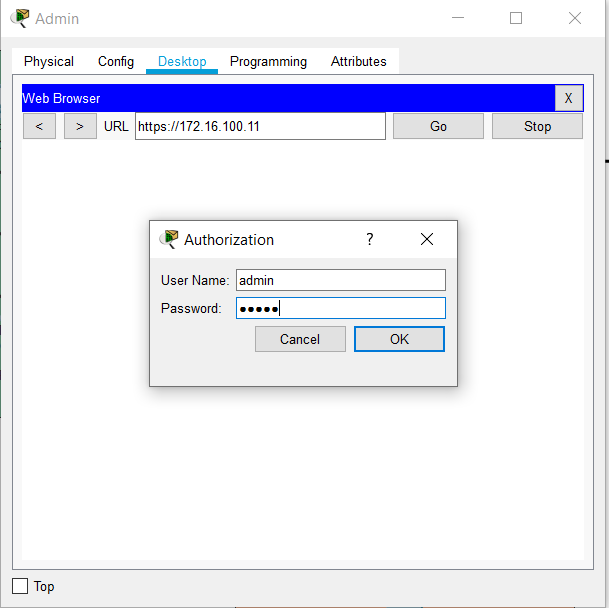
**NETWORK DIAGRAM**



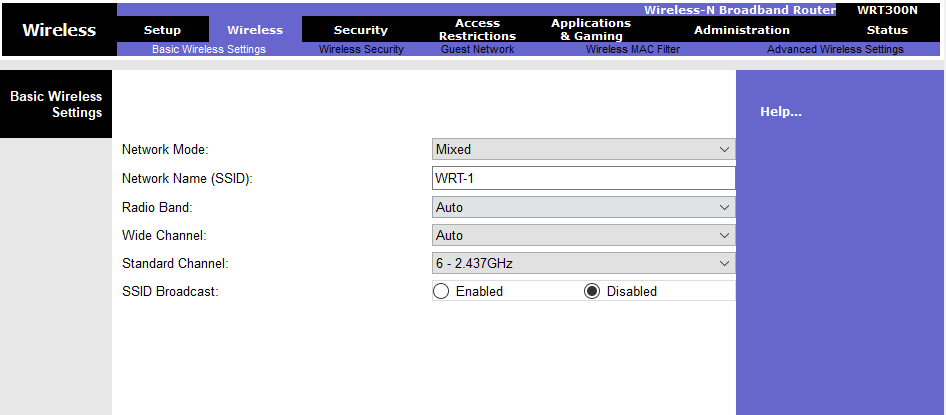
The picture above describes a network design that will help readers to visualize the network relations from each floor in the office. For all the wireless device in first and second floor are use Cisco-Linksys WRT300N with mac filtering and all the ssid broadcast are disable for a basic security. In the third floor we implement switchport security on Cisco catalyst 2960-24TT, so only the employees can use the Internet. If you are a new employee, you should ask permission to the network admin to register your mac address and using all the internet.

**MAC ADDRESS FILTERING**

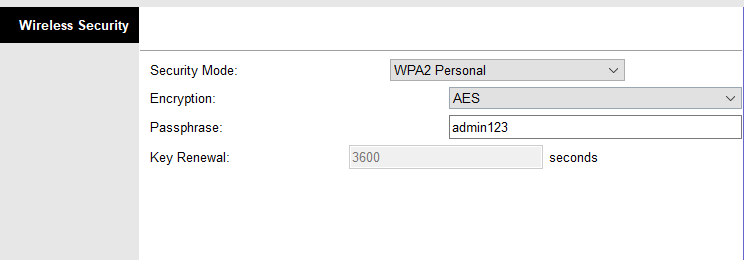
This MAC Address Filter feature works to help you prevent foreign (unwanted) users who intend to access your wireless router network. By implementing this feature, only wireless devices that have a registered MAC address (assigned) can gain access to the wireless router.



To configure the wireless, we can call wireless ip with https:176.16.100.10 and than login.

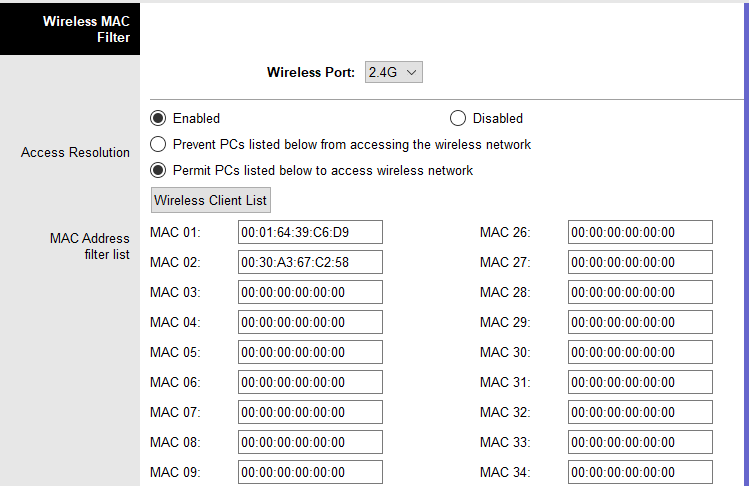


In basic wireless setting we disable the SSID to avoid phising.



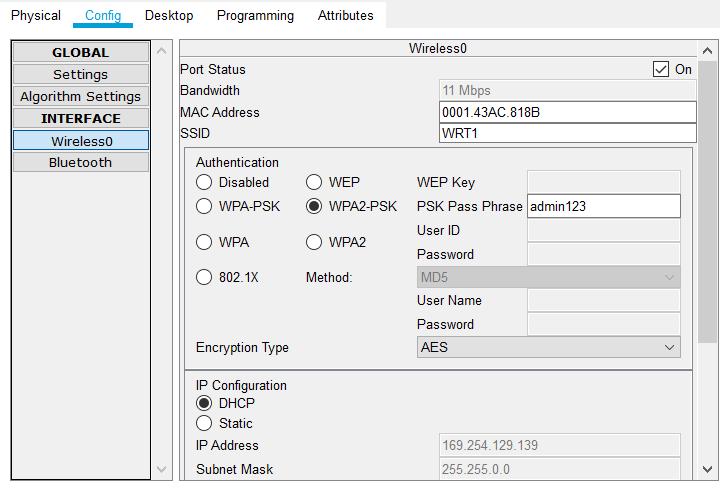
On basic wireless we use WPA2-Personal because we are just SOHO, with 11 employee 11 devices, WPA2-personal completely the best choices for small company.

**MAC ADDRESS FILTERING**



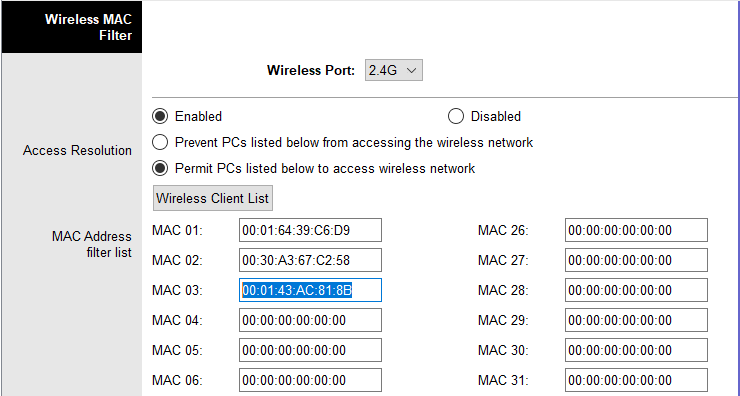
In Mac Filter we enabled “Permit PCs listed below to access wireless network”, so only the listed devices can access the wifi.

Here’s the step by step to connect using mac address:

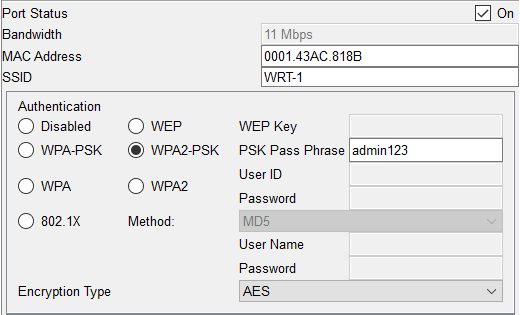


1. Go to your wireless setting and find the MAC Address from your device, and note it.

**MAC ADDRESS FILTERING**

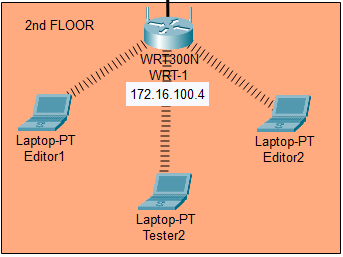


1. Ask permission to admin, admin will listed your mac address and give you the SSID and password



1. Input SSID and the password on your device

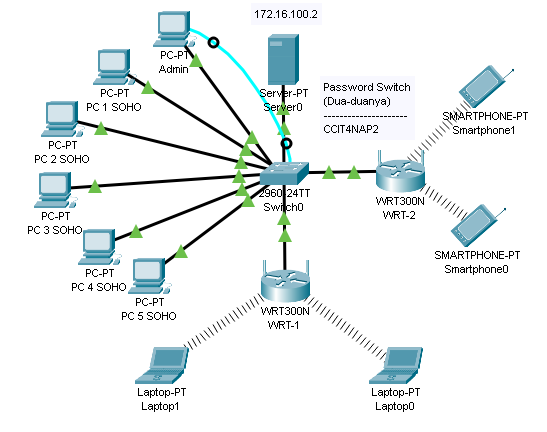
**MAC ADDRESS FILTERING**



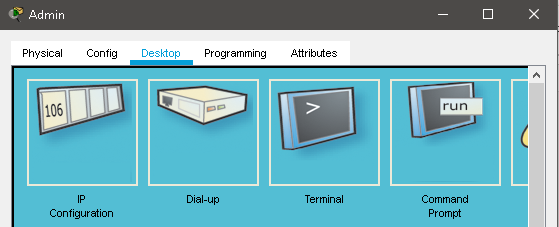
4. And your device is connected

**MAC ADDRESS FILTERING**

We already have known how to enable Mac Filtering in the wireless router device, now we will enable it in the switch. Most of us know it with switchport security. It is easy to enable and configure. First we need to go to the configuration command line in switch by using CLI tab or connect it via console and terminal.

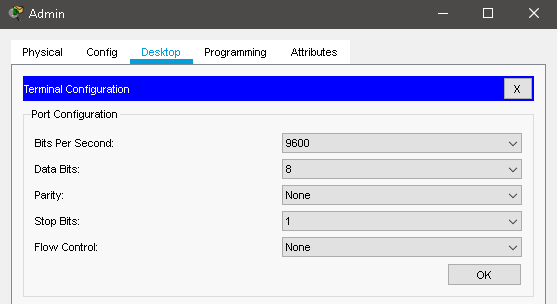


The blue cable is the console cable, connect it to PC to RS232 port and to console port in the switch. Then click on the PC and select Desktop tab, then click on terminal.

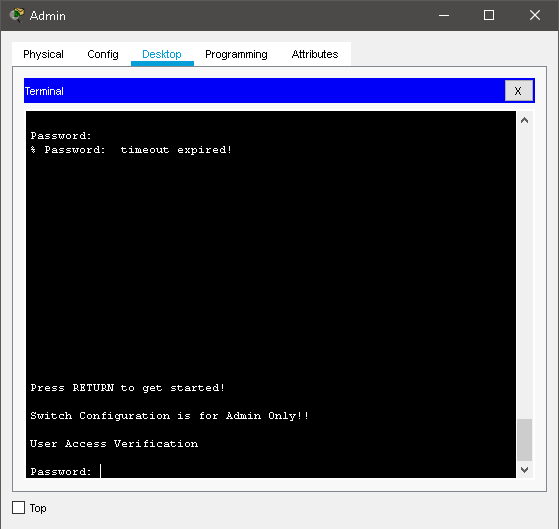


**MAC ADDRESS FILTERING**

Then you will be greeted by this screen



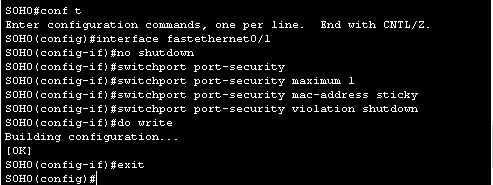
Just click on the OK button, and after that you will be transported to this screen



**MAC ADDRESS FILTERING**

After that you can configure your switch in your PC, you can apply username and password, apply banner and enable the switchport, but for the sake of this project, we will only include the steps on how to enable the switchport and do the mac address filtering so only the registered mac address can connect to the switch through the registered port.

Here’s Step by Step Configuration on How to Enable Switchport Security :

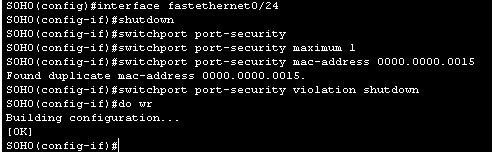


1. The first one is we need to get into the interface that we want to apply the configuration to, in this case we choose interface fastethernet0/1
2. We need to set the connection mode to access, so type in the command switchport mode access
3. Then we type no shutdown to make the interface active because you’re gonna use this interface to connect to the switch
4. Then we type switchport port-security to enable the configuration
5. After that we need to input the maximum number of how many devices that can register their mac address into this port, in this case, we input 1
6. If you don’t want to add the mac address manually, then you can use the mac-address sticky command to register the mac address automatically
7. You can use the manual input mac address to prevent the unwanted client to connect to the switch, later after this

**MAC ADDRESS FILTERING**

1. Then you can use the violation, we use the shutdown violation, so when the unwanted client connect and try to access the network via this port, it will automatically shutdown the port
2. That’s basically it, do it to the port that you’re gonna use in your network

We’ve already know how to set up the configuration of switchport port-security to permit the registered mac address to connect to the network, now because switch has so many ports, and we’re not gonna use all of those port unless you’re leading a big company, then there are some ports those are open for the attacker to use to connect to your network. Here’s the solution of that problem :



1. First we need to enter the interface that we want to use to prevent the unwanted client from connecting to the network, in this case we choose interface fastethernet0/24
2. Then we need to change the connection mode to access, so type in switchport mode access command
3. Then we need to shutdown it because we don’t need to use this port for normal connection

**MAC ADDRESS FILTERING**

1. After that, type in the switchport port-security command to enable the security
2. Then we need to set the maximum mac address that can be registered to this port, so we need to input 1
3. After you input the maximum number of mac address, then you can manual input the mac address to your liking, mine is 0000.0000.0015 so only that mac address that can connect to this port. It is preventing the other mac address to connect since the mac address is basically the factory number of the device with random words and numbers so it will prevent almost any device to be able to connect to this port if you input it with very little numbers and words
4. Then we also use violation to make the port still in the shutdown state
5. That’s basically it, and don’t forget to apply it in the unused ports

**CONFIGURATION**

**Hardware :** ASUS-PC

**Operating system :** Windows 10

**Software :** Cisco Packet Tracer 7.3.0