Detecting Rogue Host through Router Settings

Hello everyone, in todays topic we are going to discuss different settings that you can apply to detect rogue host from interfering with your networking infrastructure. Networking infrastructure is how you have your router set up within your home and safety measures that are installed to protect your system. This can be applied through different routers, modems, and switches. It just depends on how you have it implemented into your home through the use of the different equipment.

First, I would like to remind you that I currently am inventing a patent that is in the works currently to live stream criminals, hackers, and stalkers. I need your support from the community as I have supported you. Right now, we only have 4,500 dollars to go till the patent is created and be able to help you capture their communications. You will be able to find locations, departments, names, and hear when they are attacking you with the weapon systems. You can gather equipment, unions, agent numbers, screen names, capture the V2k, RNM, and AI system they are using against you. I am installing other software applications as well as a signal detection that will pinpoint where the signal is coming from and from whom. Bug detectors, and spectrum analyzers will be added as well. I have other software that I can add I am currently going through lists and seeing which ones will help the community most. I need your support in order to release this to you, I make sure to send all receipts of payment to you so you have proof and can claim on your taxes. Currently all my income is going to this project, and I need your help I can help you properly. After that I will be able to release all my step processes for the current detection method using Forensic detection so you can start analyzing yourself. I am able to pick up hackers, stalkers, computer programmers, geo experts, audio experts, laser experts, radars, sonars, drones, child/sex trafficking rings, and so much more. Here is a link if you are interested in supporting this cause and you can share within the community and your friends. https://www.gofundme.com/f/patent-live-stream-criminals-hackers-stalkers.

Back to detection: A rogue host or "Access Point" (AP) is a "wireless access point installed on a secure network without the knowledge of the system administrator."(Glover, G., 2020). This can be accessed by even attaching a cellular device by inserting a USB connection onto your computer or laptop. Making sure you have all the proper security measures in place will help you protect hackers, or unwanted guests, into your current system. (Glover, G., 2020).

Here is some **different software that you can install** to create a safer environment:

Encryptions, Key locks, Firewalls, VPN, Malwarebytes, and Two-way authentication processes.

Firewalls are a great deterrent for any hacker to be denied access. I will be working on a list of good free software for everyone to implement in a later segment. Although paid for software is the best route you can go, not everyone has the means to purchase the software.

For now, I want to make sure that you are properly securing your router to start the detection process so you can block the signals that are being attached.

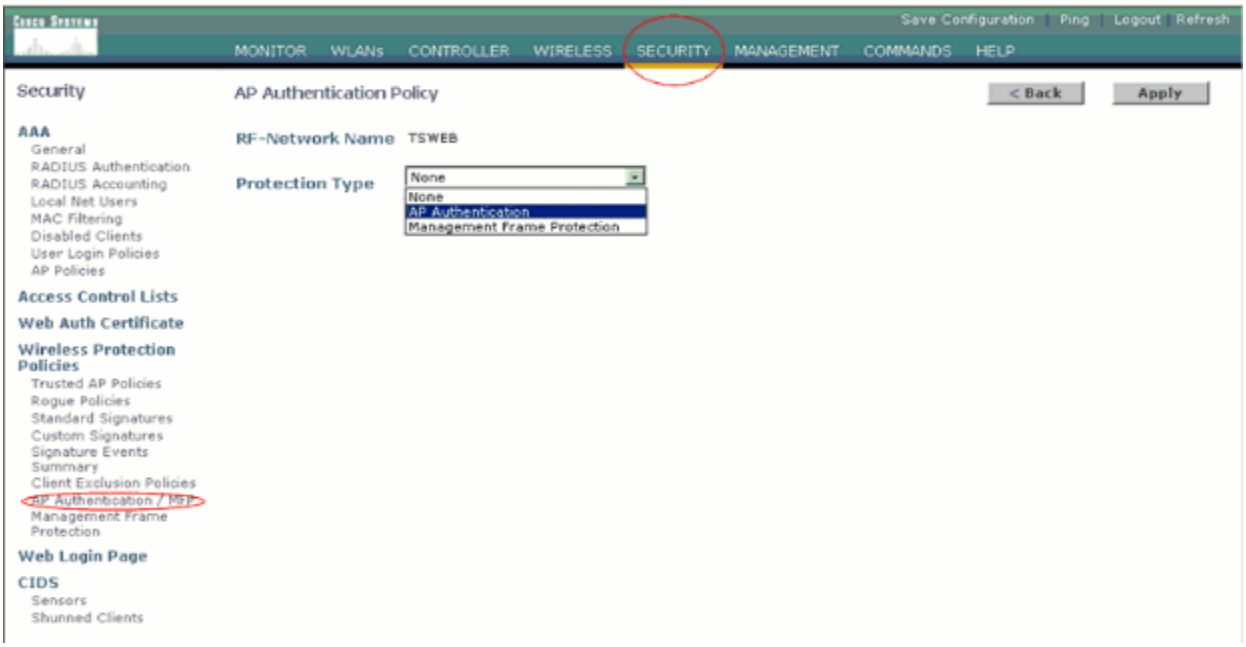
Configuration steps:

1) **First step is to gain access to your router configuration.** If you do not know how to gain access to your router there are a couple of ways to help you gain that access.
   A) Plug in your ethernet cable directly into the device.
   B) You can type in your IP address into a web browser and your router will pop up.
   C) If you go into your command bar and type in the search filed Command Prompt click on it and your command prompt screen will show up. Type in: **ipconfig** and this will give you're your systems IP address, and default gateway. You can write it down and type it into the web browser and gain access into your router control board.

2) **Second step is signing in**. you already have a username and password that you have to enter to gain access. If you do not know your username and password, chances are that is still in the default mood and you need to change that information right away once you gain access. Here is a website link that will give you all the default user names and passwords for which ever system you have. https://www.softwaretestinghelp.com/default-router-username-and-password-list/.

3) Go to: **Security>Rogue Policies** and click **Enabled** on the **Rogue Location Discovery Protocol**

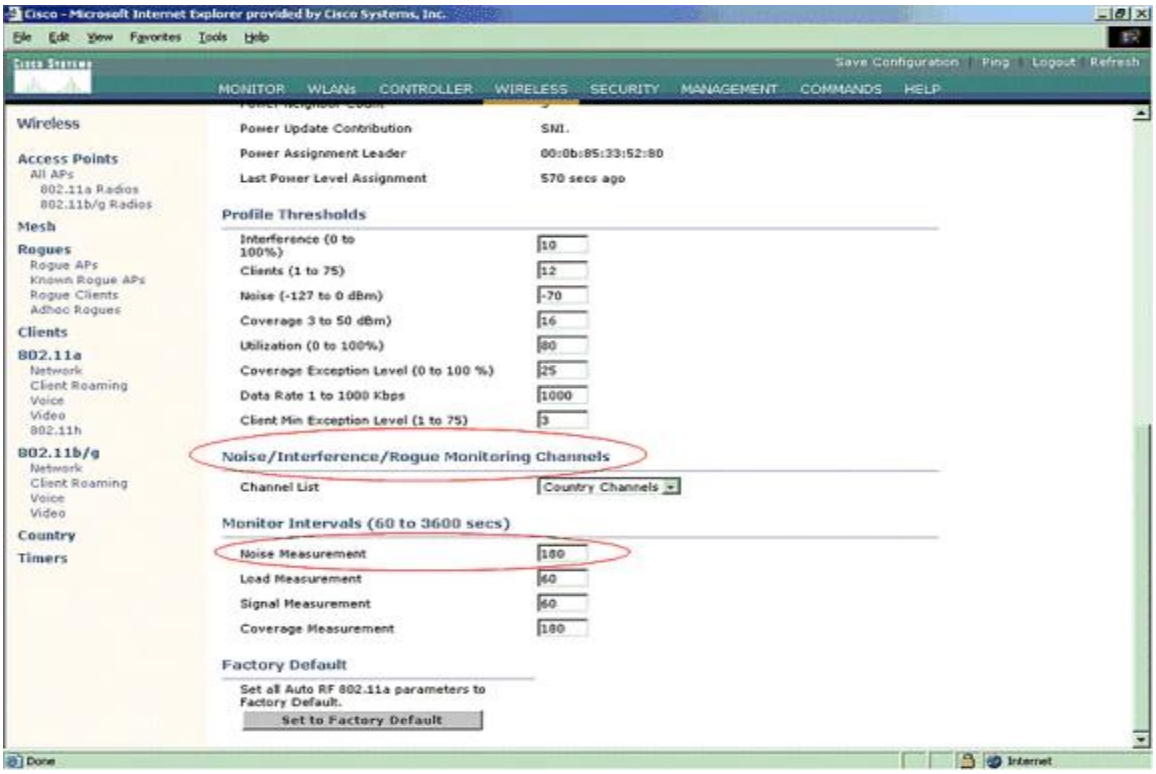
4) This is an optional step. When this feature is enabled, the APs sending RRM neighbor packets with different **RF Group** names are reported as rogues. This will be helpful in studying your RF environment. In order to enable it, choose **Security-> AP Authentication**. Then, choose **AP Authentication** as the Protection Type as shown in the figure.



Verify the channels to be scanned in these steps:

5) Select **Wireless > 802.11a Network**, then **Auto RF** in the right-hand side as shown in the figure.

6) On the **Auto RF** page, scroll down and choose **Noise/Interference/Rogue Monitoring Channels**.



1.

a. The Channel List details the channels to be scanned for rogue monitoring, in addition to other controller and AP functions. Refer to Lightweight Access Point FAQ for more information on Lightweight APs, and Wireless LAN Controller (WLC) Troubleshoot FAQ for more information on wireless controllers.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

2. Set the Time Period for scanning selected channels:

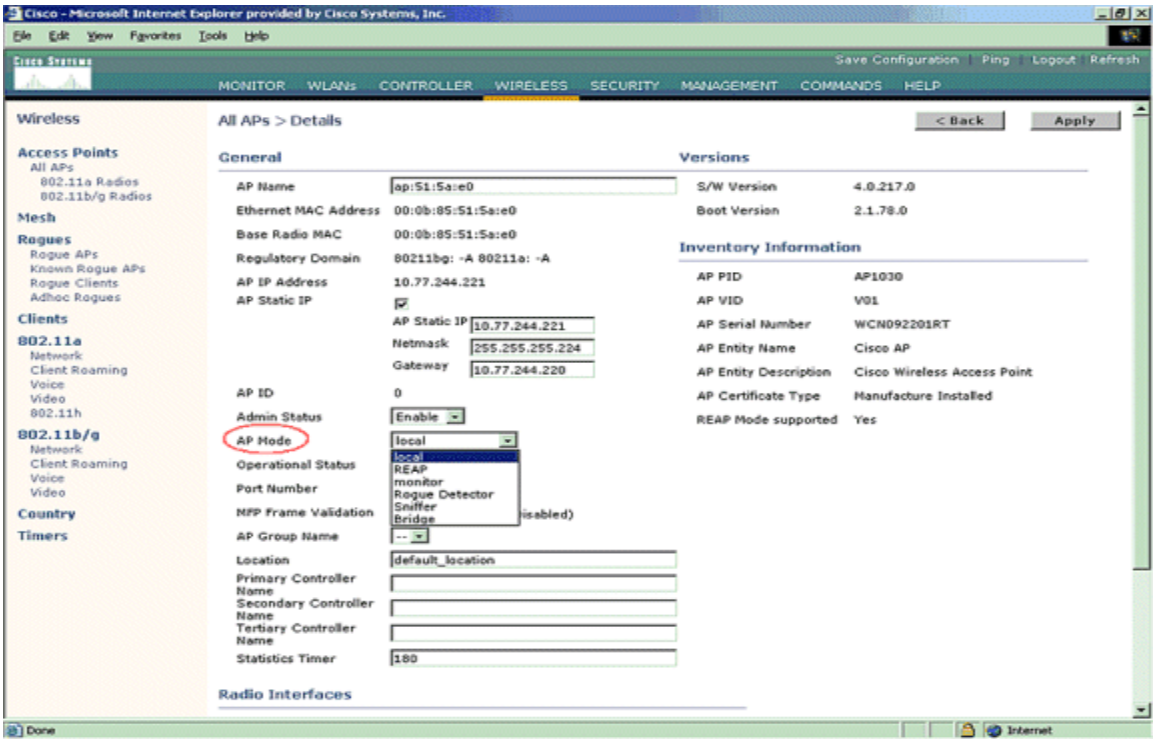
The scanning duration of the defined group of channels is configured under **Monitor Intervals > Noise Measurement**, and the allowable range is from 60 to 3600 seconds. If left at the default of 180 seconds, the APs scan each channel in the channel group once, for 50 ms, every 180 seconds. During this period, the AP radio changes from its service channel to the specified channel, listens and records values for a period of 50 ms, and then returns to the original channel. The hop time plus the dwell time of 50 ms takes the AP off-channel for approximately 60 ms each time. This means that each AP spends approximately 840 ms out of the total 180 seconds listening for rogues.
The "listen" or "dwell" time cannot be modified and is not changed with an adjustment of the Noise Measurement value. If the Noise Measurement timer is lowered, the rogue discovery process is likely to find more rogues and to find them more quickly. However, this improvement comes at the expense of data integrity and client service. A higher value, on the other hand, allows for better data integrity but lowers the ability to find rogues quickly.

3. Configure the AP mode of operation:

   A Lightweight AP mode of operation defines the role of the AP. The modes related to the information presented in this document are:

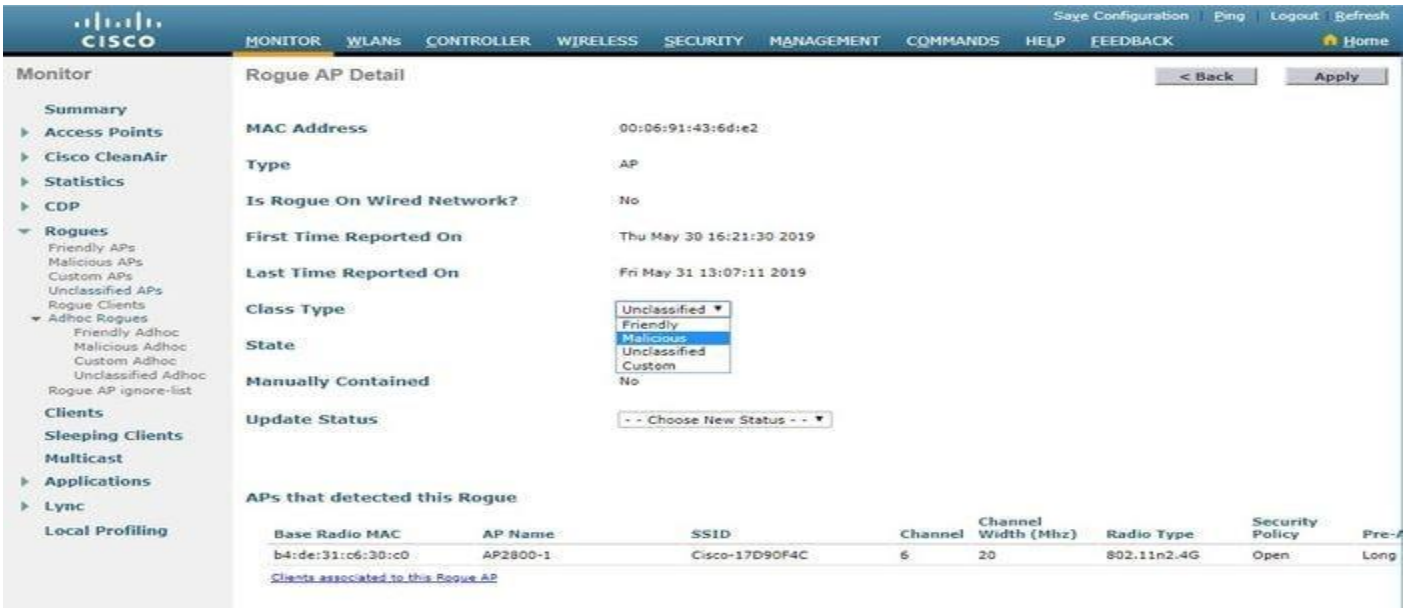
- **Local**—This is the normal operation of an AP. This mode allows data clients to be serviced while configured channels are scanned for noise and rogues. In this mode of operation, the AP goes off-channel for 50 ms and listens for rogues. It cycles through each channel, one at a time, for the period specified under the Auto RF configuration.
- **Monitor**—This is radio receive only mode, and allows the AP to scan all configured channels every 12 seconds. Only de-authentication packets are sent in the air with an AP configured this way. A monitor mode AP can detect rogues, but it cannot connect to a suspicious rogue as a client in order to send the RLDP packets.
  Note: DCA refers to non-overlapping channels that are configurable with the default modes.
- **Rogue Detector**—In this mode, the AP radio is turned off, and the AP listens to wired traffic only. The controller passes the APs configured as rogue detectors as well as lists of suspected rogue clients and AP MAC addresses. The rogue detector listens for ARP packets only, and can be connected to all broadcast domains through a trunk link if desired.

You can configure an individual AP mode simply, once the Lightweight AP is connected to the controller. In order to change the AP mode, connect to the controller web-interface and navigate to **Wireless**. Click on **Details** next to the desired AP to in order to display a screen similar to this one:

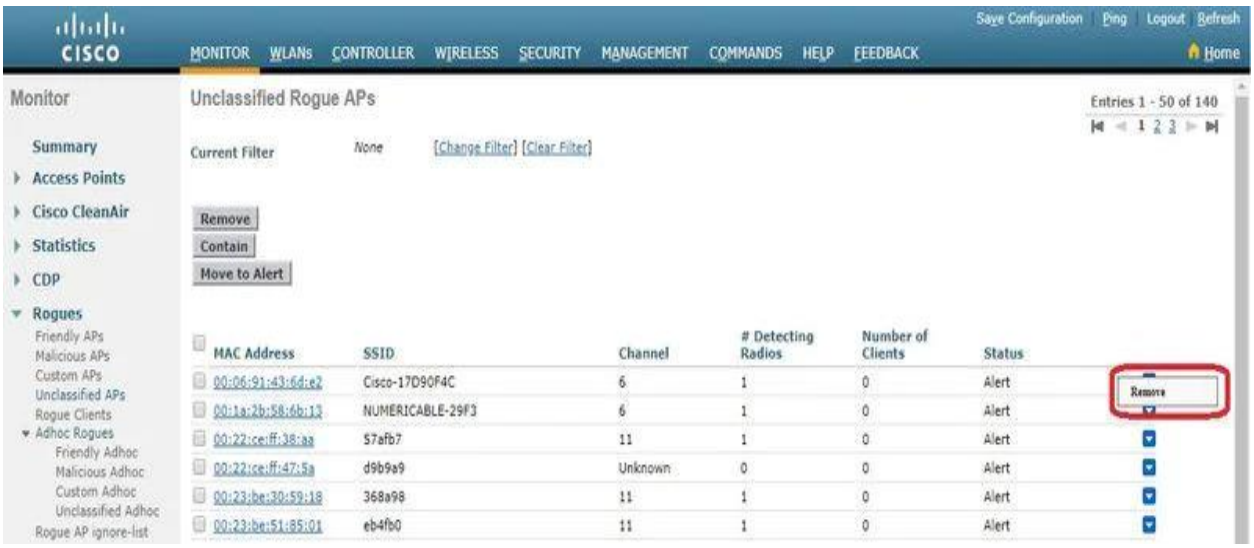


Depending on the type of harassment, torture that you are experiencing you can change the settings to your needs. Some of the settings can be set in a decibel level. From the audio analysis portion I can say they range from a -60 to a -200 DB level.

7) **Manually Classify a Rogue Access point.** In order to classify a rogue AP as friendly, malicious, or unclassified, navigate to **Monitor > Rogue > Unclassified APs**, and click the particular rogue AP name. Choose the option from the drop-down list, as shown in the image.

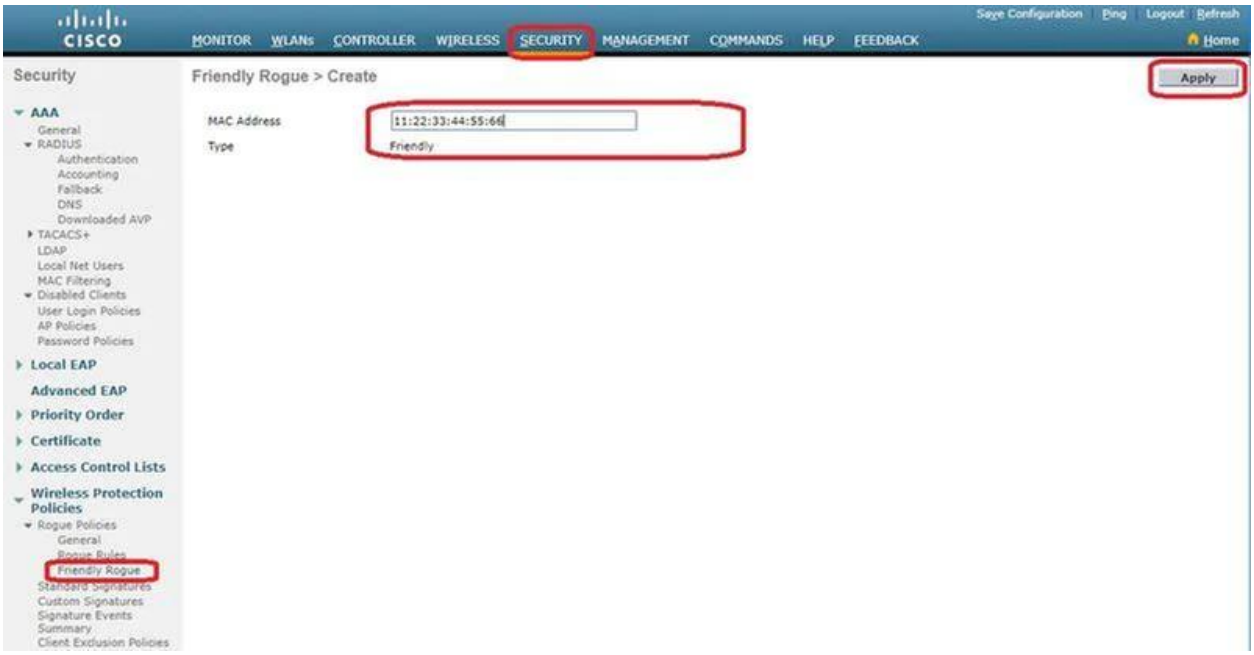


8) In order to remove a rogue entry manually from the rogue list, navigate to **Monitor > Rogue > Unclassified APs**, and click**Remove**, as shown in the image.



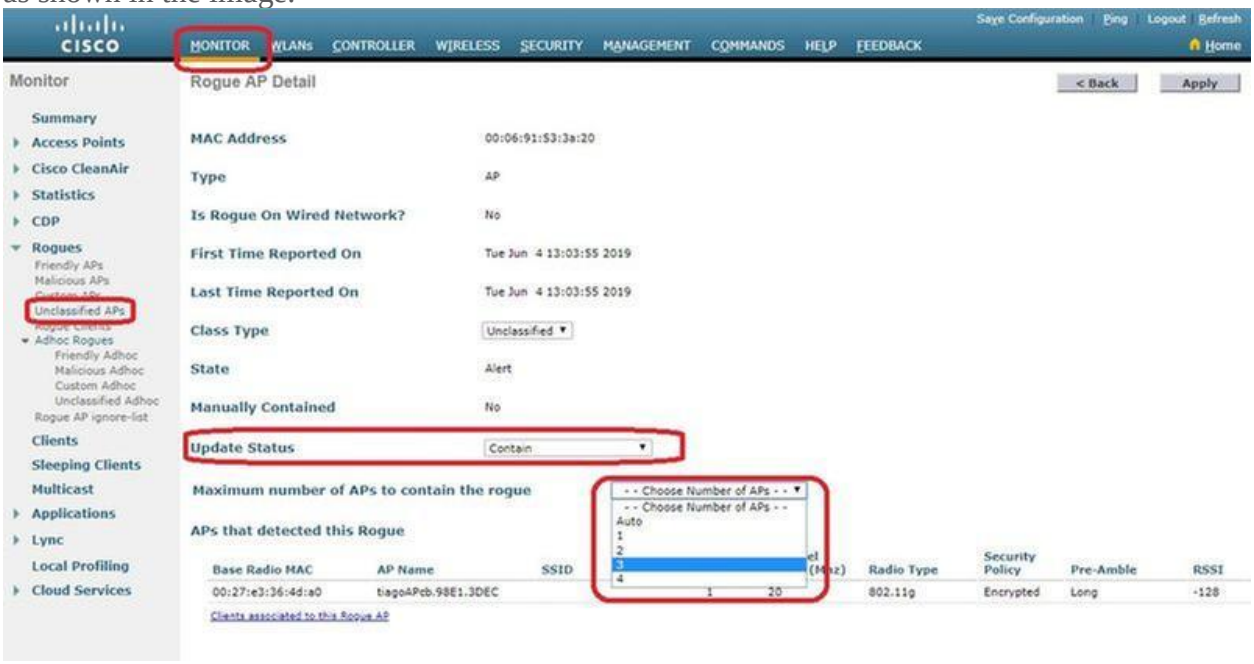
9) In order to configure a Rogue AP as a friendly AP, navigate to **Security > Wireless Protection Policies > Rogue Policies > Friendly Rogues** and add the rogue MAC address.

The added friendly rogue entries can be verified from **Monitor > Rogues > Friendly Rogue** page, as shown in the image.

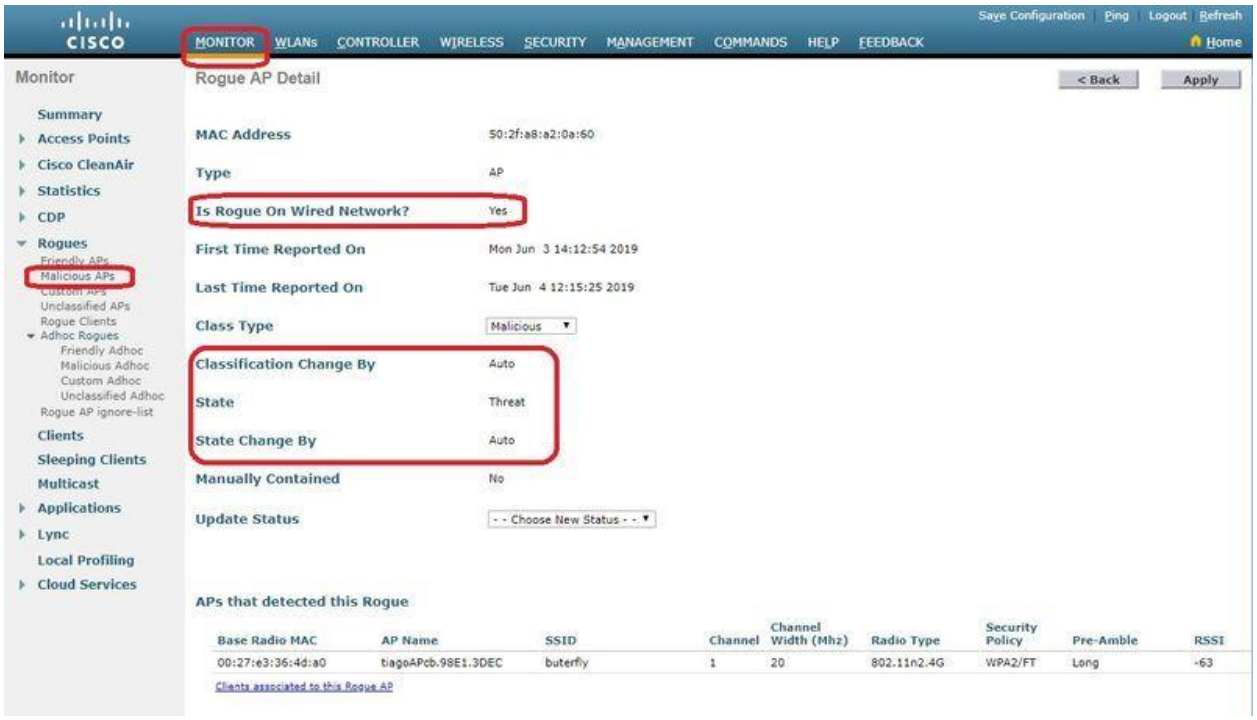


Configure Manual Containment

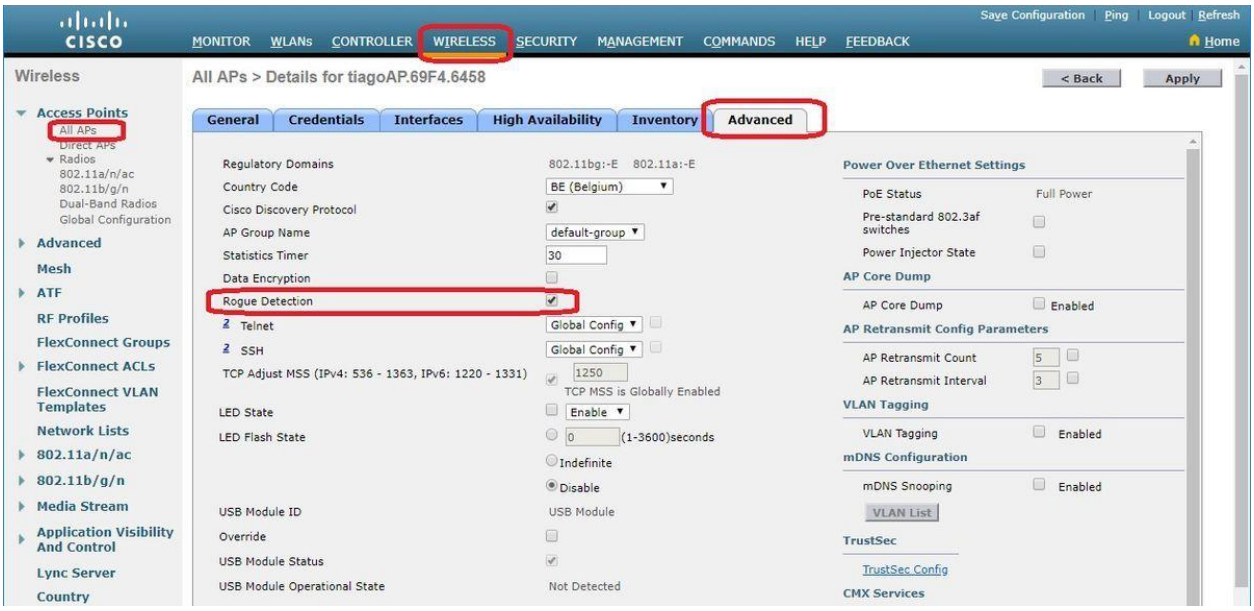
10) In order to contain a rogue AP manually, navigate to **Monitor** > **Rogues** > **Unclassified**, as shown in the image.



11) Click a particular rogue entry in order to get the details of that rogue. Here is an example of a Rogue detected on wired network:

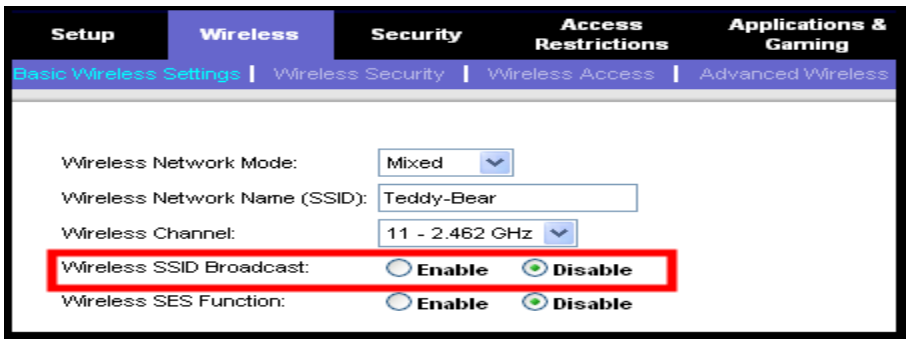


12) If The Rogue Is Not Detected **Verify that rogue detection is enabled on the AP. On the GUI:**



Once you remove your rogue hosts and you detected and blocked them with the proper settings you will need to take extra security measures to gain your security on your system.

13) **Change the SSID.** Although there are mixed feelings about this type of change it can help hide your system from the outside world. Although hackers can still gain access using a NetSpot or other software mapping applications, it can hide you from plain sight. It will not deter the hackers but that is why you applied a firewall right. Wi-Fi network names, or service set identifiers (SSIDs), can range from the mundane ("Café Hotspot") to the intimidating ("FBI Surveillance Van"). Whatever the inspiration behind your SSID is, it serves a more important role than just personalization. With that being said, just because you see ("FBI surveillance van") on your network does not mean it is the FBI. Any one person can write in the SSID as they want to scare people. But by Law any law enforcement agencies have to announce themselves other wise it is considered entrapment. **Wireless>Basic Wireless Settings**

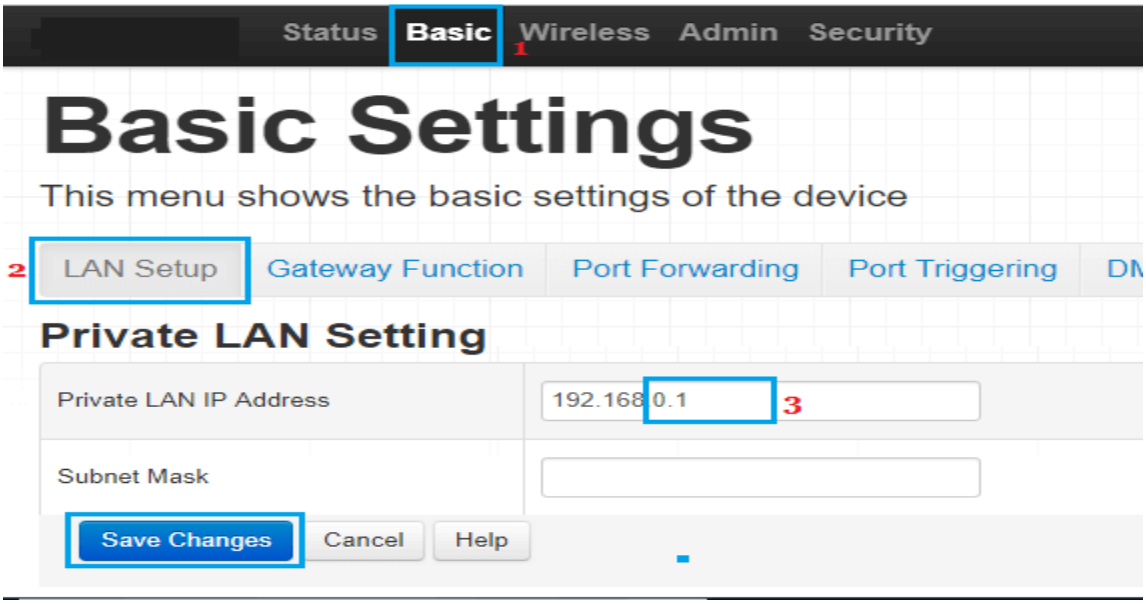


14) **Select Wi-Fi encryption.** Go to **Wireless>Wireless** Security you want to change your Encryption to a **WPA2 PSK (AES) or WPA3** if allowed. These are the most secure settings that you can choose and is standard today.

15) **Choose a new password and username.** This is under your security settings. Make sure to write your password down unless you memorized it. If you are having V2k, RNM, AI, problems, I suggest you get a friend or someone you trust to create a password for you. You want to throw away the password once you reset your internet, TV mobile devices, tablets, and so forth.

16) Change IP address. The last suggestion that I have for you is to change your IP address. This will kick you out and allow for a set up of all your information. This should be done last it will also reset your router and kick all the rogue hosts out of your system.

Go to **LAN Setup> Private LAN Setting.** Type in your new IP address and Subnet Mask.



Note: In these last two fields, you can use any number between 1 and 254.

Caution: Restrict IP Address change only to the third and fourth fields (ex: 192.168.11.xxx). Making changes to first and second fields can lead to network conflicts while connecting with your main network.

Click on Save Changes and note down your New Router IP Address. Or use **ipconfig** in your command prompt.

Now you can enter and reconfigure all your devices to gain access. You also can keep going into your router configurations and monitor your network for rogue hosts and block them when necessary.

I know this is a lot of information to take in and I will take you a step at a time. There are other configurations that a person needs to know to secure your router. I will eventually come out with a full video tutorial to show the whole configuration process. At least for now you can start monitoring your network securely. I would like to thank you for your time and enjoy helping you all in the future.

References

CISCO. (2007, September 24). In *Rogue Detection under Unified Wireless Networks*. Retrieved from https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html.

CISCO. (2019, August 21). In *Rogue Management in an Unified Wireless Network*. Retrieved from https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#anc23.

Glover, G. (n.d.). Steps To Find Rogue Wi-Fi Networks And Comply With PCI DSS Requirement 11.1. In *Security Metrics*. Retrieved from https://www.securitymetrics.com/blog/wireless-access-point-protection-finding-rogue-wi-fi-networks.

NJCCIC. (2018, April 5). In *Configuring & Securing a Home Wi-Fi Router*. Retrieved from https://www.cyber.nj.gov/instructional-guides/how-to-configure-and-secure-a-home-wi-fi-router.

Patwegar, W. (n.d.). How to Change Router IP Address. In *Techbout*. Retrieved from https://www.techbout.com/change-router-ip-address-45926/#:~:text=Follow%20the%20steps%20below%20to%20change%20Router%20IP,and%20Password%20to%20log%20into%20Router%20Settings.%204.

Software Testing Help. (2020, August 2). How To Find Default Router Username And Password?. In *Default Router Login Password For Top Router Models (2020 List)*. Retrieved from https://www.softwaretestinghelp.com/default-router-username-and-password-list/.