

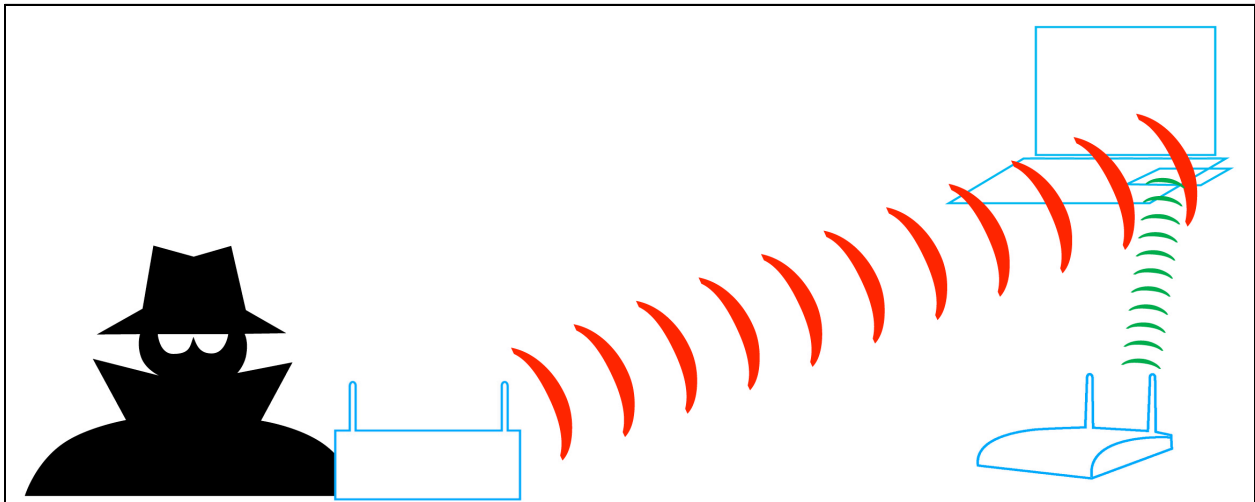
## Section 6

### Wireless Denial of Service Attacks

RF is vulnerable!

You are now going to prove that statement. We'll be using devices and software from your student kit to jam both narrowband and broadband RF signals to disrupt 802.11 traffic.

We'll also use the 802.11 protocol itself - against itself - to cause Denial of Service against your Wireless LAN.



## Lab 6.1 Narrowband RF Jamming

The purpose of this lab is to show the damaging effects of a DoS attack on a wireless network. A wireless DoS attacks can occur at Layer 1 or Layer 2.

A layer 1 RF jamming attack is perpetrated by a high power RF signal over powering a wireless access point's signal. The high RF noise signature essentially blocks out the signal from the AP and consequently the stations are unable to connect or pass traffic.

A layer 2 DoS attack can be just as damaging as a Layer 1 RF Jamming attack and is usually comes in the form of a Deauth attack. The Linux script can be used to deauth a single client or all the clients on a network. The Prism test utility creates an attack know as the Queensland attack which exploits the CSMA/CA access mechanism on 802.11 wireless networks and continuously transmits on the wireless channel.

### Product Information

#### Source

YDI Power Signal Generator (PSG)  
Commercial

#### Where, When, Why

Most wireless DoS attacks are just a nuisance and do not result in any confidential information being revealed to a hacker. The real problem is that a wireless DoS attack usually precedes another attack such as client hijacking or an Evil Twin attack. To test if clients or access point are susceptible to these types of attacks a wireless security tester might use a narrowband RF jammer, wideband RF jammer, or the Queensland attack (layer 2 DoS attack).

A wireless security auditor might employ these DoS tools to demonstrate that a wireless LAN should not be used for mission critical apps. Or as a way of knocking wireless clients off the network to hijack them and in preparation for another attack.

#### Usage and Features

- Take down the wireless network and cause service disruption
- Disconnect wireless users from the network in preparation for another attacks

#### Requirements / Dependencies

1. Wireless AP
2. Wireless client with connectivity to the AP

**What you will do in this lab:**

- Narrowband RF Jamming DoS attack
- 3. Wideband RF Jamming DoS attack
- 4. Queensland DoS attack
- 5. Deauth Attacks

---

**Lab Part 1 - Connect a wireless client to the internet and jam the signal**

- Step 1. Connect the Nokia N800 to the classroom AP - SSID HOTlabs.
- Step 2. Open Hitcast on the Nokia N800 and start it playing some music.
- Step 3. You should hear the music playing, if not try turning up the volume with the top buttons.
- Step 4. Connect your WLSAT laptop to the classroom AP - SSID HOTlabs
- Step 5. Open a command prompt and type ping www.yahoo.com -t.
- Step 6. Leave the constant ping running and plug in the Wispy spectrum analyzer and open the chanalyzer program.
- Step 7. Turn on the wireless video camera on channel 6 - see the documentation to change the 'dip switch' settings. On these video cameras there are only four channel settings - here is a list of what frequency they use:

CH 1: 2.434 GHz, CH 2: 2.453 GHz, CH 3: 2.473 GHz and  
CH 4: 2.411 GHz.



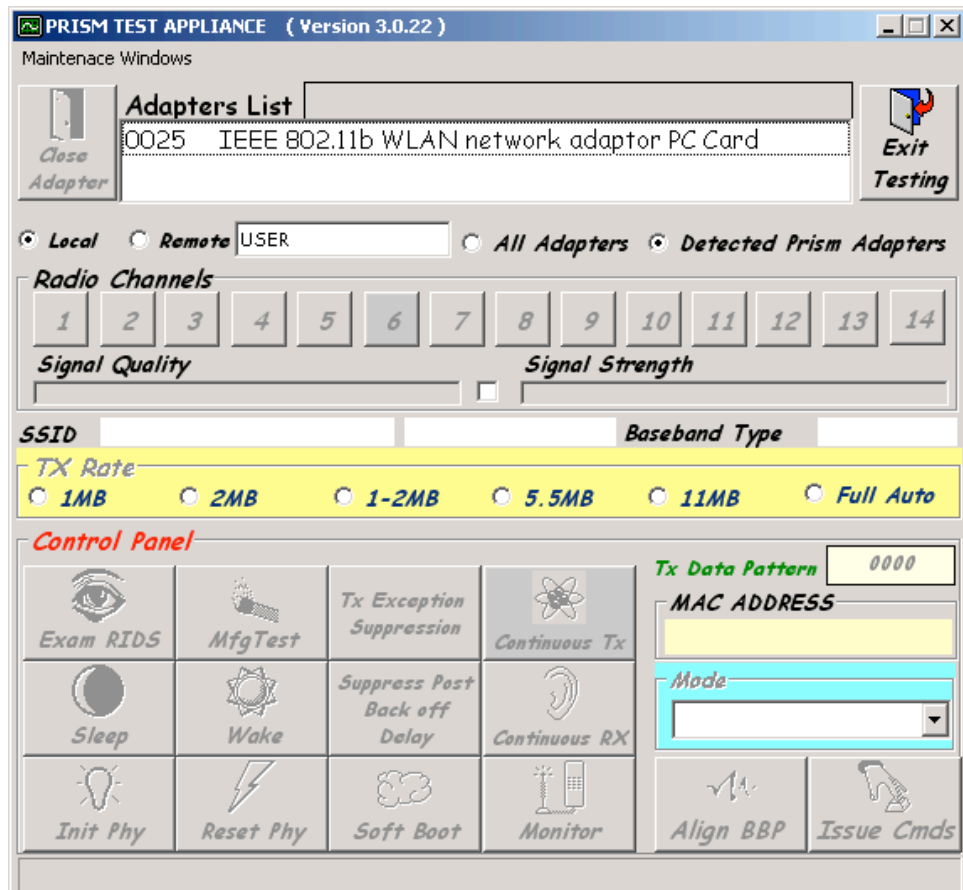
- Step 8. The music should stop playing on the Nokia N800 because the channel has been jammed by the wireless video camera.
- Step 9. Turn off the camera and the music should start again.
- Step 10. View the WLSAT laptop constant ping. It should stop when you turn on the RF jammer video camera.
- Step 11. The instructor will demonstrate wideband RF Jamming with a RF signal generator across the entire 2.4 Ghz band.
- Step 12. Watch this with your copy of WiSpy running so you can see the effect of the jammer on the RF in the room.
- Step 13. What happens? Why?

## Lab 6.3: Queensland DoS

- Step 1. Put the Prism card (Senao) in the WLSAT Laptop.



- Step 2. Open the Prism test Utility - **Start à Wireless Tools à Prism Test Utility**.

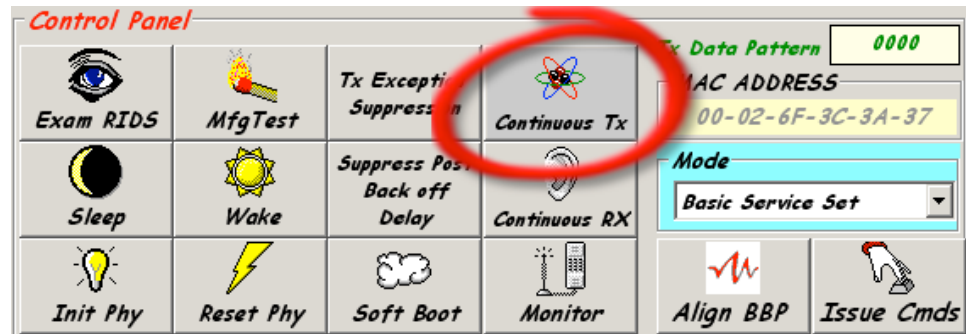


- Step 3. Click on the **IEEE 802.11b WLAN network adaptor PC Card** (the name of our Senao card) on the top of the screen.

- Step 4. Click the **Channel 6** button.



- Step 5. Click the **Continuous Tx** button.



Step 6. The music from the Nokia N800 should stop playing.

**NOTE:** The Prism Test Utility is an unsupported, non commercially available software and therefore there is no support for the software. It is supposed to be used as a diagnostic tool and sometimes locks up the application or system. You may have to pull the card in order to stop the card from transmitting and DoS.

Step 7. Stop the Prism test utility by clicking the Continuous Tx button a second time, and the music should start again.



Step 8. What happens to the constant ping when the Prism card is continuously transmitting? \_\_\_\_\_

Step 9. How does the Queensland attack appear in Chanalyzer using the Wispy USB?  
\_\_\_\_\_

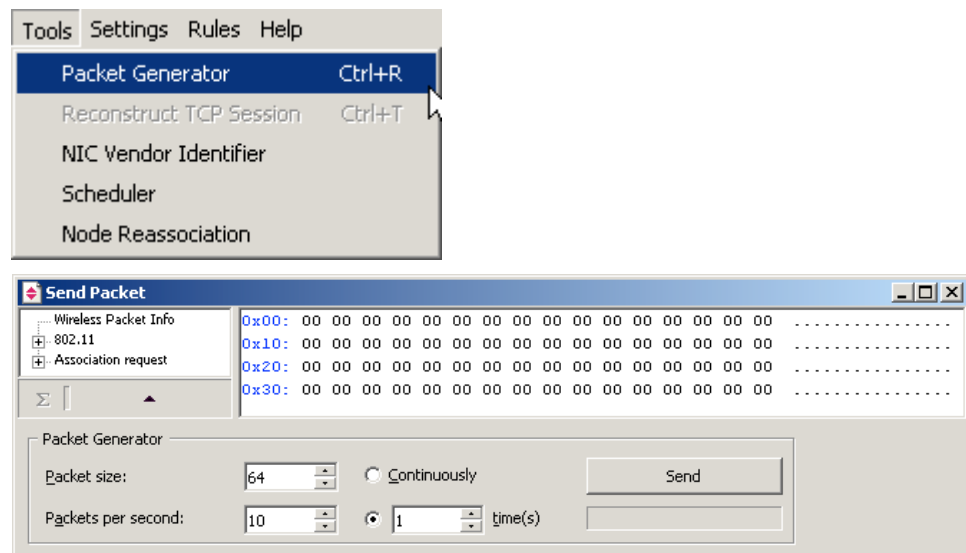
## Lab 6.3: Windows Deauth Attacks

### What you will do in this lab:

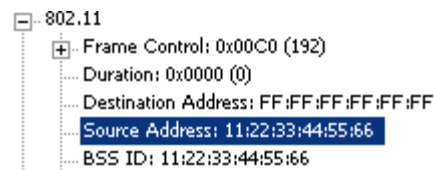
- Use Tamosoft Commview to generate Deauth Frames
- Use AirDefense AirTerminate to Deauth a client

### Lab Part 1 - Use CommView to generate deauth frames

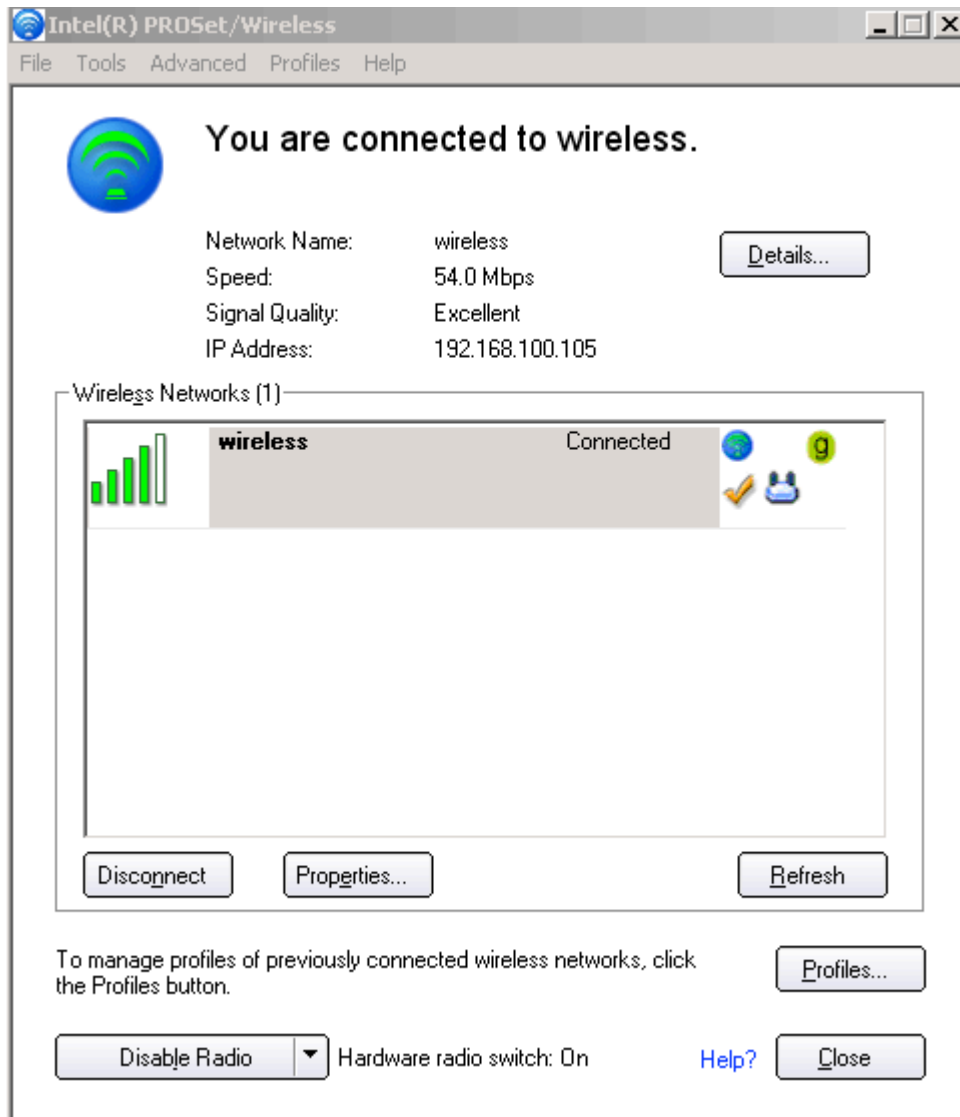
- Step 1. Set your driver for the Ubiquiti card to Commview for WiFi.
- Step 2. Open Commview - Start à Wireless Tools à Commview for Wifi.
- Step 3. Click the Tools à Packet Generator from the menu.





- Step 4. Drag the *CommViewDeauth file* from the student folder onto the **packet** generator tool.



- Step 5. Connect your WLSAT laptop to the classroom AP - SSID **Hotlabs**
- Step 6. *Identify the MAC address of the AP by clicking the properties button in the Intel Pro Set utility and looking for the BSSID of the WLAN.*



Access Points in this Network (1):

	Channel	BSSID
 	11	00:12:17:CF:77:2E

- Step 7. Write down the MAC address of the AP. \_\_\_\_\_ We will be spoofing this address in Commview.

Deauthentication  
Reason: 0x0002 (2) - Previous authentication no longer valid

- Step 8. In CommView change the Source and BSSID address of the frame to be the MAC address of the AP.

802.11  
+ Frame Control: 0x00C0 (192)  
Duration: 0x0000 (0)  
Destination Address: FF:FF:FF:FF:FF:FF  
Source Address: 11:22:33:44:55:66  
BSS ID: 11:22:33:44:55:66

- Step 9. Click start to generate a continuous death from the AP to all clients.

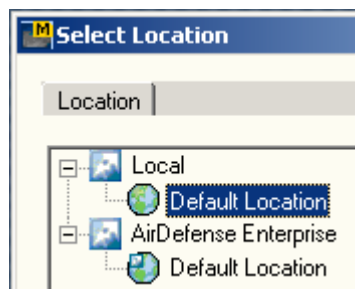


- Step 10. Stop the death by **closing** the **send packet window**. The music should start again on the Nokia N800.

**NOTE:** An individual station may be deauthed by configuring the destination address in the frame.

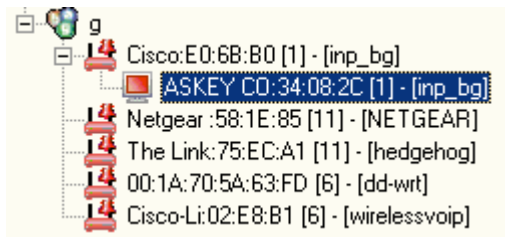
## Lab Part 2 - Use AirDefense active terminate to disconnect clients

- Step 1. Verify the Hitcast Internet Radio application is playing on the Nokia N800 and the music is playing.
- Step 2. Reset the Ubiquiti Driver to AirDefense.
- Step 3. Open AirDefense - Start à Wireless Tools à AirDefense Mobile.
- Step 4. Select the Default Location then click OK.

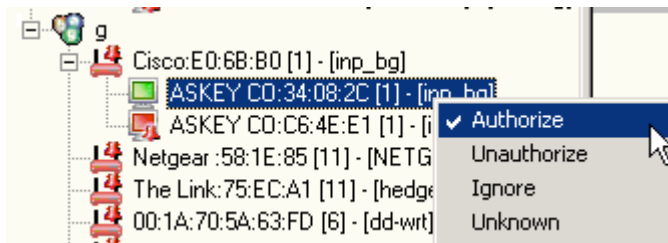


- Step 5. Click **Yes** to start scanning the 802.11 network.

- Step 6. Let your system run for a couple of minutes. It will take a while for the software to get enough packets while scanning all the channels to find all the Access Points and Clients in the area.

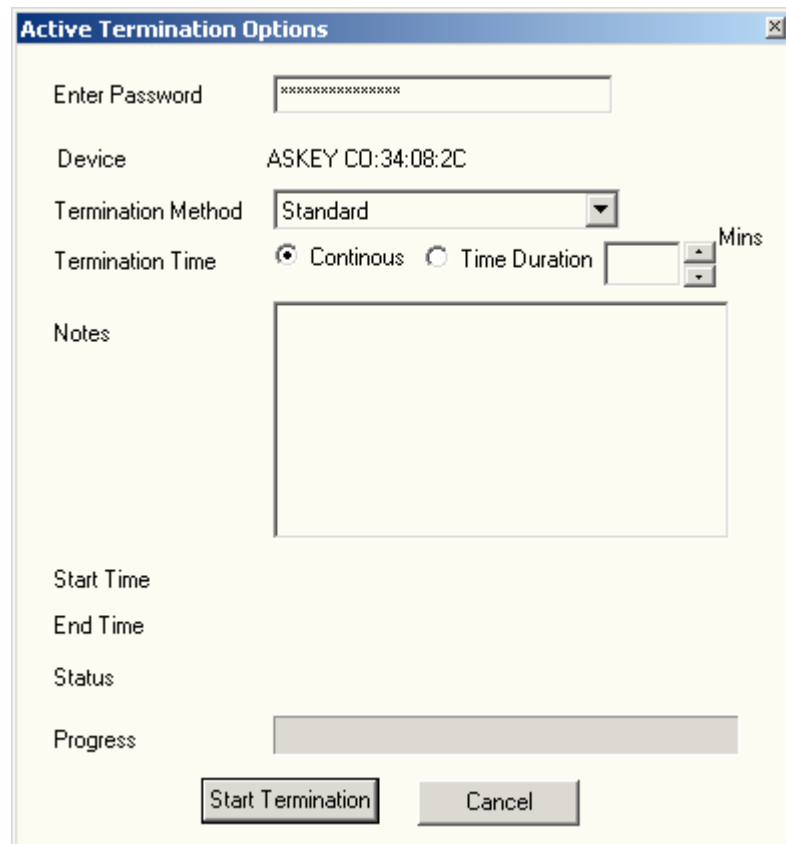


- Step 7. Select your *Nokia client MAC address* in the left hand pane. **Right click** on the MAC address and choose **Authorize**.



- Step 8. Now that your device is authorized we can again right click, but this time choose **Active Terminate**.

- Step 9. Type in the *password given from your Instructor*.



- Step 10. Set the **Time Duration** for **1** minute.

Step 11. Click **Start Termination**.

The music should stop playing on the Nokia N800.

Step 12. Click **Cancel** in the Active Termination window to stop the termination.

Note: You can always 'watch' this process by running a 'sniffer' or packet analyzer while this Deauth attack is taking place.

---

### What you learned in this Lab:

In this Lab you learned to use:

- a narrowband RF Jammer to jam a single channel
- a wideband jammer to jam the all the 802.11b/g channels
- Use Queensland attack to exploit the CSMA/CA mechanism
- Use CommView to generate custom crafted frames including Deauth
- Use AirDefense Mobile to active terminate wireless clients

## Lab 6.4: Linux Deauth Attacks

In this lab we will use Linux tools and scripts to issue denial of services against access points and stations.

### Product Information

#### Where, When, Why

Hackers use Denial of Service attacks to actually disrupt services or to aid them in an attack. Besides disruption, a denial of service attack can be used to: downgrade encryption, get clients to connect to a rouge network under the hackers control, cause a device to 'fail-open', and force clients to reconnect so that the attacker can view the authentication for an offline attack.

#### Usage and Features


- Cause all clients associated with an access point to disconnect
- Cause a target client to disconnect from an access point

#### Requirements / Dependencies

- Software and hardware capable to sniff wireless connections
- Wireless drivers capable of packet injection

#### What you will do in this lab:

- Find a wireless client that is attached to a wireless network and cause them to disconnect

Step 1. To open a command prompt click on the **terminal icon** in the lower left-hand corner. 

Step 2. At the command prompt type 8oh2 to open our custom script.

Step 3. Select option 'D' to deauth one station. Airodump-ng will appear so that you can find the MAC address of your target.

```
::::: DENIAL OF SERVICE (DoS) ::::::  
D - Deauthenticate a station
```

BSSID	STATION	PWR	Lost	Packets	Probes
00:0F:66:85:F5:32	00:18:DE:AB:D6:FB	71	0	667	
00:0F:66:85:F5:32	00:18:DE:2D:94:76	46	0	6	yourap
00:16:B6:25:15:5C	00:13:CE:13:F1:ED	27	0	7	livingroom1
(not associated)	00:90:4B:C0:42:58	5	0	1	
(not associated)	00:14:A5:5E:87:82	5	0	8	Apt 305 Secure
(not associated)	00:13:02:CD:C7:AF	1	0	1	andrew

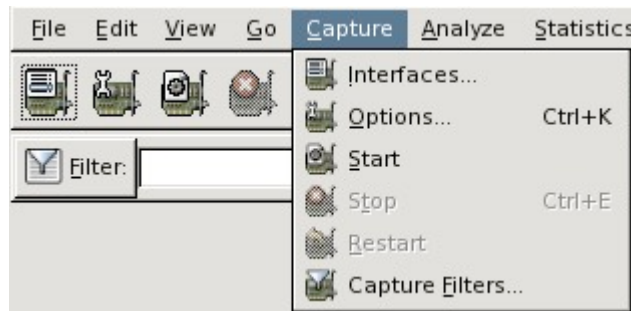
We can see down at the bottom of Airodump-ng's output that we are in range of 6 wireless clients but only 3 of them are actually talking on a network; two of which belong to the 'yourap' network with BSSID 00:0F:66:85:F5:32.

- Step 4. **Connect to your access point using your N800 as a client.** Watch the client appear on the airodump-ng screen as a station. That is your victim. Having picked a victim, we are ready to forge our packets to send to the N800. For this tutorial I will pick the client at Station MAC 00:18:DE:2D:94:76.

**NOTE:** For demonstration purposes it is a good idea to start hitcast on your N800's so that you can audibly hear a disruption in services. Keep in mind that some buffering does occur with hitcast so it wont be immediate.

- Step 5. Now we want to open up wireshark in order to view the whole process. From the command line type **wireshark**.

Once wireshark is opened you will need to configure it before you use it. Select **Capture > Interfaces**



Then you will want to select the interface that we will use to view traffic of our target network. In our case it's the **eth1** interface

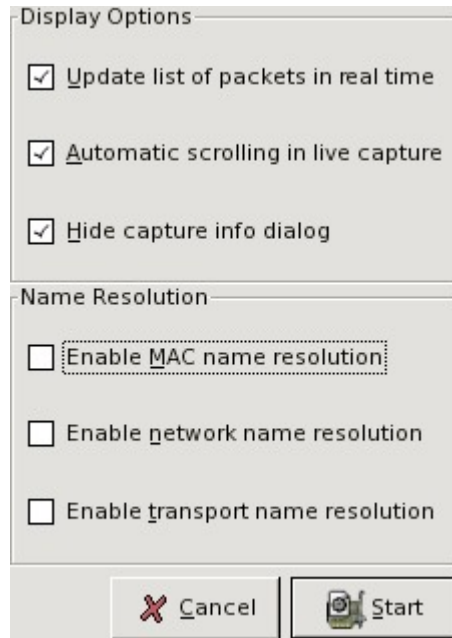
Note: if you don't see interface eth1 in the list go back out to your command prompt and type **ifconfig eth1 up**

It is evident that we have traffic on this network as our packets are increasing. Select **Options** to configure the interface



The changes we will make will allow us to see the traffic in real-time so that we can view the deauth packet being sent. **Simply put the check mark in all the boxes under display options and remove all the checks from the Name Resolution section and hit Start.**

**NOTE:** For demonstration purposes it is a good idea to start hitcast on your N800's so that you can audibly hear a disruption in services. Keep in mind that some buffering does occur with hitcast so it wont be immediate.



- Step 6. The custom script is waiting for you to input your targets BSSID (the access points MAC) and the victim station MAC. Enter them in and click enter to see the attack take place both from the debugging output of the script as well wireshark that we just opened up.

The N800's music stream should cease after a few seconds and wireshark should show you the deauthenticate frames that were sent.

The image shows a Wireshark packet capture window. The filter bar at the top contains the filter: wlan.fc.type==0 and wlan.fc.subtype==12. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, and Info. The packets listed are IEEE 802.11 Deauthentication frames with various SN and FN values.

No.	Time	Source	Destination	Protocol	Info
4123	187.759172	00:18:de:2d:94:76	00:1a:70:5a:63:fd	IEEE 802.11	Deauthentication, SN=507, FN=0
4125	187.762514	00:1a:70:5a:63:fd	00:18:de:2d:94:76	IEEE 802.11	Deauthentication, SN=508, FN=0
4126	187.766525	00:18:de:2d:94:76	00:1a:70:5a:63:fd	IEEE 802.11	Deauthentication, SN=509, FN=0
4129	187.770489	00:1a:70:5a:63:fd	00:18:de:2d:94:76	IEEE 802.11	Deauthentication, SN=510, FN=0
4130	187.774615	00:18:de:2d:94:76	00:1a:70:5a:63:fd	IEEE 802.11	Deauthentication, SN=511, FN=0
4160	188.078654	00:1a:70:5a:63:fd	00:18:de:2d:94:76	IEEE 802.11	Deauthentication, SN=540, FN=0

By following the scripts direction you just kicked your N800 offline.

## Lab Part 2 - Use custom script to death all clients

To open a command prompt click on the **terminal icon** in the lower left-hand corner.

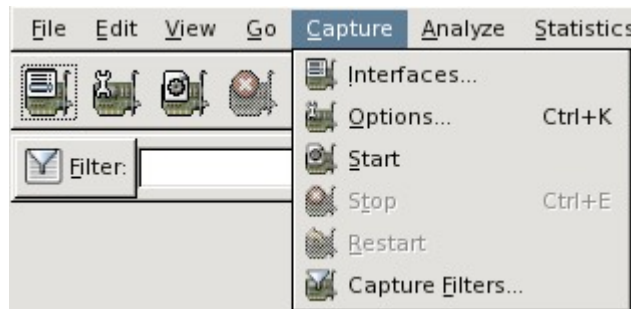


- Step 1. At the command prompt type **8oh2** to open our custom script.
- Step 2. Select **option 'De'** to death all stations. **Airodump-ng** will appear so that you can find the MAC of your target access point.

BSSID	STATION	PWR	Lost	Packets	Probes
00:0F:66:85:F5:32	00:18:DE:AB:D6:FB	71	0	667	
00:0F:66:85:F5:32	00:18:DE:2D:94:76	46	0	6	yourap
00:16:B6:25:15:5C	00:13:CE:13:F1:ED	27	0	7	livingroom1
(not associated)	00:90:4B:C0:42:58	5	0	1	
(not associated)	00:14:A5:5E:87:82	5	0	8	Apt 305 Secure
(not associated)	00:13:02:CD:C7:AF	1	0	1	andrew

We can see down at the bottom of Airodump-ng's output that we are in range of 6 wireless clients but only 3 of them are actually talking on a network; two of which belong to the 'yourap' network with BSSID 00:0F:66:85:F5:32.

- Step 3. **Connect to your access point using your N800 as a client.** Watch the client appear on the airodump-ng screen as a station. We are ready to forge our packets to send to the broadcast address of the network.
- Step 4. Start Hitcast on your N800's.
- Step 5. Now we want to open up Wireshark in order to view the whole process. From the command line type **wireshark**.
- Step 6. Once Wireshark is opened you will need to configure it before you use it. Select **Capture > Interfaces**.



- Step 7. Then you will want to select the interface that we will use to view traffic of our target network. In our case it's the **eth1** interface

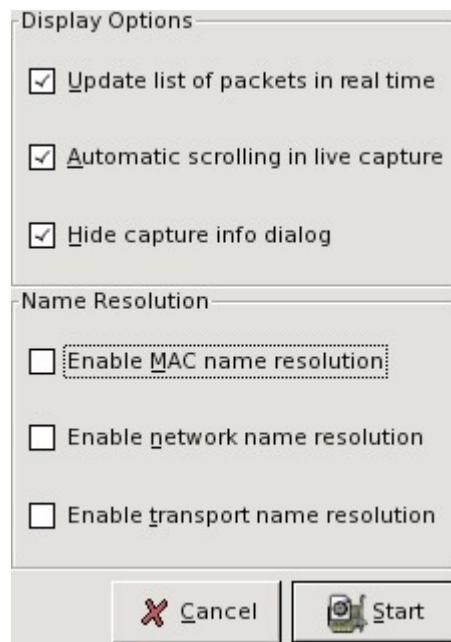
**NOTE:** if you don't see interface eth1 in the list go back out to your command prompt and type **ifconfig eth1 up**

It is evident that we have traffic on this network as our packets are increasing. Select **Options** to configure the interface



The changes we will make will allow us to see the traffic in real-time so that we can view the death frame being sent. **Simply put the check mark in all the boxes under display options and remove all the checks from the Name Resolution section and hit Start.**

**NOTE:** For demonstration purposes it is a good idea to start hitcast on your N800's so that you can audibly hear a disruption in services. Keep in mind that some buffering does occur with hitcast so it wont be immediate.



- Step 8. The custom script is waiting for you to input your target BSSID (the access points MAC). **Enter them in** and click **enter** to see the attack take place both from the debugging output of the script as well wireshark that we just opened up.

The N800's music stream should cease after a few seconds and wireshark should show you the deauthenticate frames that were sent.

No.	Time	Source	Destination	Protocol	Info
915	37.058492	00:1a:70:5a:63:fd	ff:ff:ff:ff:ff:ff	IEEE 802.11	Deauthentication, SN=1804, FN=0
916	37.062436	00:1a:70:5a:63:fd	ff:ff:ff:ff:ff:ff	IEEE 802.11	Deauthentication, SN=1805, FN=0
917	37.066436	00:1a:70:5a:63:fd	ff:ff:ff:ff:ff:ff	IEEE 802.11	Deauthentication, SN=1806, FN=0


By following the scripts direction you just kicked your N800 offline.

The only difference between this attack and the previous single death attack is that it sends to the broadcast address instead of the MAC of a single client.

## Lab Part 3 - Use custom script to deny all users access with a Clear-To-Send frame

Connect to your access point with your N800 AND your eth1 interface before you continue with this lab.

```
iwconfig eth1 essid "<your ap SSID>"
ifconfig eth1 up
dhcpcd eth1
ping www.google.com
```

Step 1. To open a command prompt click on the **black terminal window icon** in the lower left-hand corner. 

Step 2. Type 8oh2 to launch our custom script.

Step 3. Type 'Dx' to select the mass DoS attack.

```
::::: DENIAL OF SERVICE (DoS) ::::::
D - Deauthenticate a station
Dx - Disrupt service to all stations associated with a particular access point
```

Step 4. The next step is to find a MAC address of *any* client on the network you want to severely disrupt service to.

BSSID	STATION	PWR	Lost	Packets	Probes
00:0F:66:85:F5:32	00:18:DE:AB:D6:FB	53	735	491	
00:0F:66:85:F5:32	00:18:DE:2D:94:76	38	101	55	
(not associated)	00:14:A5:5E:87:82	19	0	8	Apt 305 Secure
(not associated)	00:0E:9B:53:B0:CA	19	0	2	west
(not associated)	00:13:CE:F6:45:ED	8	0	7	Bob's wireless
(not associated)	00:16:B6:A1:49:E5	5	135	6	Booyaw208

We see two Stations that are connected to BSSID 00:0F:66:85:F5:32 so we can pick either one of those; for this attack it doesn't matter which you choose. For this demonstration we will use 00:18:DE:AB:D6:FB.

Step 5. Now we need to enter the **MAC address and channel** for our target. Again, this is any MAC of any client that is authenticated with the access point.

```
What is the MAC address of -any- station on that network? 00:18:DE:AB:D6:FB
What channel is the victim network on? 6

Press Ctrl + C when you want to stop the attack.
Press any key to continue
```

Step 6. The next messages lets you know that the attack will continue until you break it with **ctrl + C** to stop it. Once you click **enter** then you will send forged CTS out to every client on that network.

**NOTE:** The nature of this type of attack is an interesting one. Under normal circumstances a client can send out a Request-To-Send (RTS) to the access point if they have something large to transfer. If the access point agrees then a Clear-To-Send (CTS) will be sent out and everyone has to stop transmitting in order for that large transmission to arrive uninterrupted and more efficiently. It's an issue because **802.11** is designed to play well with others. We exploit that and forge CTS. You can really see the effects of this attack if you have a victim client constantly ping something else. You will first see the milliseconds significantly increase and then, depending on conditions, the communication will cease all together.

You can send a constant ping with the following commands:

```
ping www.google.com -t ← for Windows clients
```

```
ping www.google.com ← for Linux clients
```

---

## What you learned in this Lab:

In this Lab you learned to:

- Use the custom script to forge CTS's to send to all hosts on the wireless network