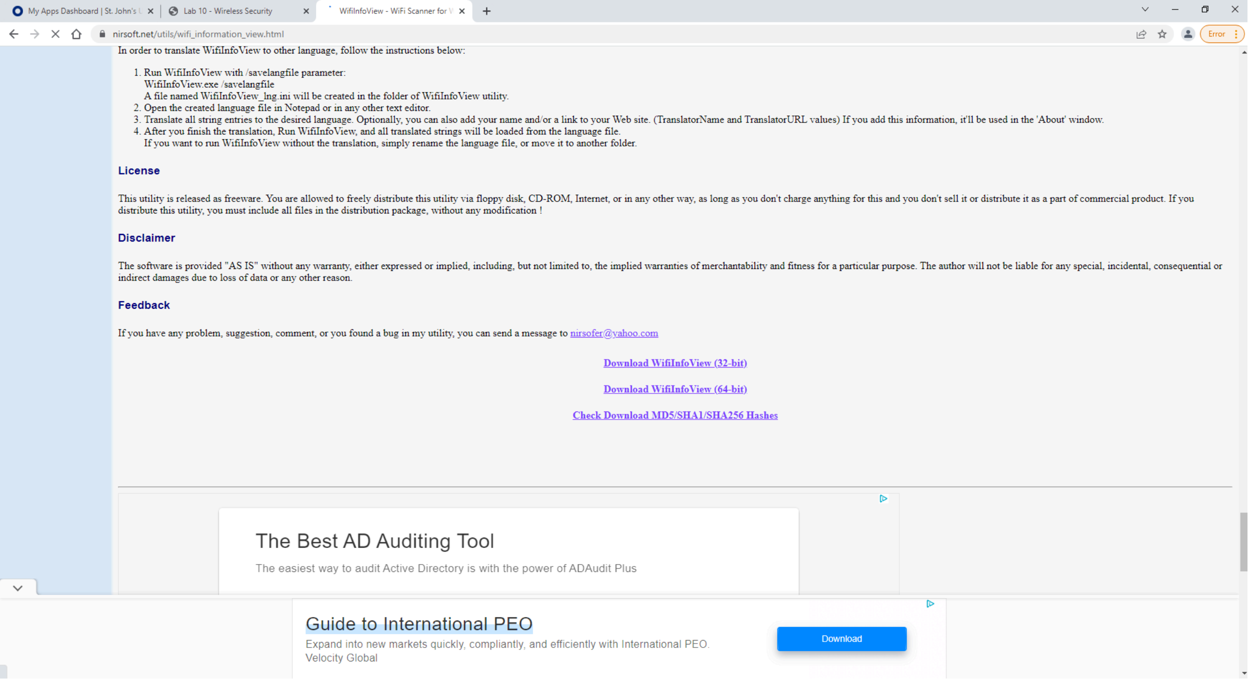
Lab 10

Project 11-1

1. Step one is to go to this URL (www.nirsoft.net/utils/wifi_information_view.html) and scroll down and download “WifiInfoView”


My Apps Dashboard | St. John's U
Lab 10 - Wireless Security
WifiInfoView - WiFi Scanner for W
nirsoft.net/utils/wifi_information_view.html
Error

In order to translate WifiInfoView to other language, follow the instructions below:

1. Run WifiInfoView with /savelangfile parameter:
   WifiInfoView.exe /savelangfile
   A file named WifiInfoView_lng.ini will be created in the folder of WifiInfoView utility.
2. Open the created language file in Notepad or in any other text editor.
3. Translate all string entries to the desired language. Optionally, you can also add your name and/or a link to your Web site. (TranslatorName and TranslatorURL values) If you add this information, it'll be used in the 'About' window.
4. After you finish the translation, Run WifiInfoView, and all translated strings will be loaded from the language file.
   If you want to run WifiInfoView without the translation, simply rename the language file, or move it to another folder.

License

This utility is released as freeware. You are allowed to freely distribute this utility via floppy disk, CD-ROM, Internet, or in any other way, as long as you don't charge anything for this and you don't sell it or distribute it as a part of commercial product. If you distribute this utility, you must include all files in the distribution package, without any modification !

Disclaimer

The software is provided "AS IS" without any warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The author will not be liable for any special, incidental, consequential or indirect damages due to loss of data or any other reason.

Feedback

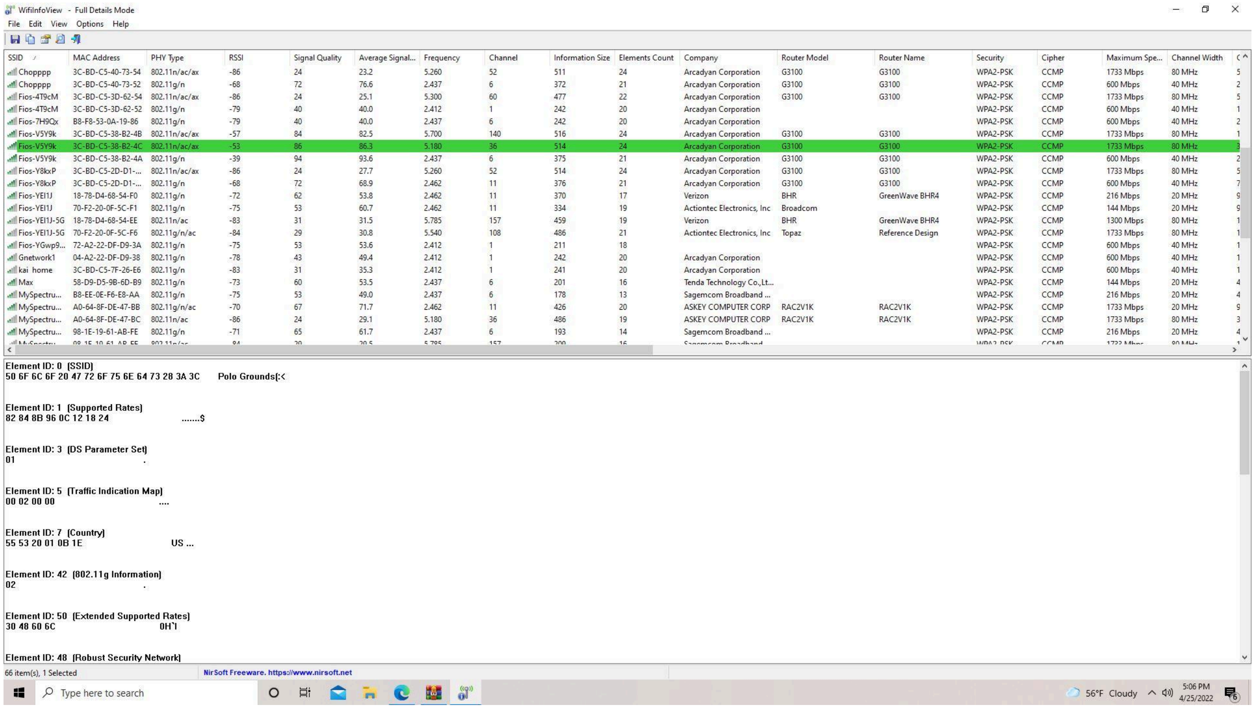
If you have any problem, suggestion, comment, or you found a bug in my utility, you can send a message to nirsofer@yahoo.com

Download WifiInfoView (32-bit)

Download WifiInfoView (64-bit)

Check Download MD5/SHA1/SHA256 Hashes

2. Once we download WifiInfoView, we need to launch the program and all the wifi networks pop up. I was surprised by how many popped up, I thought it was gonna be maybe 30 networks but it looks like there are a lot more than that.

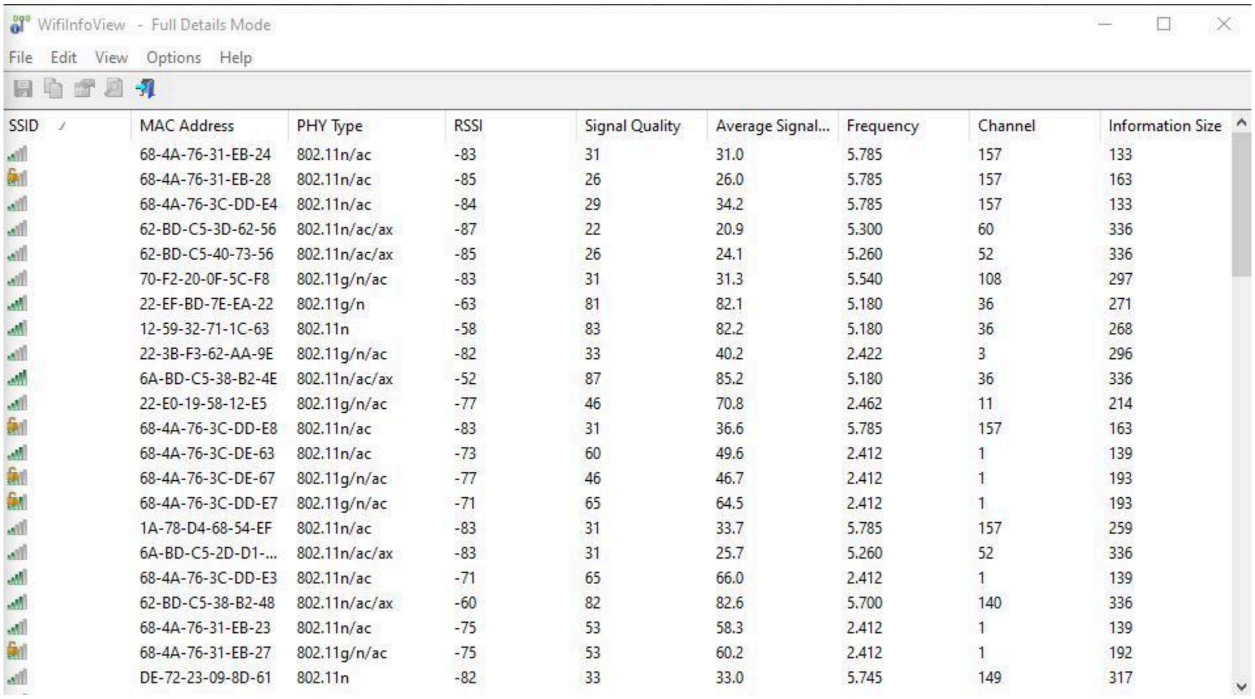


SSID	MAC Address	PHY Type	RSSI	Signal Quality	Average Signal...	Frequency	Channel	Information Size	Elements Count	Company	Router Model	Router Name	Security	Cipher	Maximum Spe...	Channel Width	C
Chopppp	3C-BD-C5-40-73-54	802.11n/ac/ax	-86	24	23.2	5.260	52	511	24	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	5
Chopppp	3C-BD-C5-40-73-52	802.11g/n	-68	72	76.6	2.437	6	372	21	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	600 Mbps	40 MHz	2
Fios-4T9cM	3C-BD-C5-3D-62-54	802.11n/ac/ax	-86	24	25.1	5.300	60	477	22	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	5
Fios-4T9cM	3C-BD-C5-3D-62-52	802.11g/n	-79	40	40.0	2.412	1	242	20	Arcadyan Corporation			WPA2-PSK	CCMP	600 Mbps	40 MHz	1
Fios-7H9Qx	B8-F8-53-0A-19-86	802.11g/n	-79	40	40.0	2.437	6	242	20	Arcadyan Corporation			WPA2-PSK	CCMP	600 Mbps	40 MHz	2
Fios-V5Y9k	3C-BD-C5-38-B2-4B	802.11n/ac/ax	-57	84	82.5	5.700	140	516	24	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	1
Fios-V5Y9k	3C-BD-C5-38-B2-4C	802.11n/ac/ax	-53	86	86.3	5.180	36	514	24	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	3
Fios-V5Y9k	3C-BD-C5-38-B2-4A	802.11g/n	-39	94	93.6	2.437	6	375	21	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	600 Mbps	40 MHz	2
Fios-Y8kxP	3C-BD-C5-2D-D1-...	802.11n/ac/ax	-86	24	27.7	5.260	52	514	24	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	5
Fios-Y8kxP	3C-BD-C5-2D-D1-...	802.11g/n	-68	72	68.9	2.462	11	376	21	Arcadyan Corporation	G3100	G3100	WPA2-PSK	CCMP	600 Mbps	40 MHz	7
Fios-YEI1J	18-78-D4-68-54-F0	802.11g/n	-72	62	53.8	2.462	11	370	17	Verizon	BHR	GreenWave BHR4	WPA2-PSK	CCMP	216 Mbps	20 MHz	9
Fios-YEI1J	70-F2-20-0F-5C-F1	802.11g/n	-75	53	60.7	2.462	11	334	19	Actiontec Electronics, Inc	Broadcom		WPA2-PSK	CCMP	144 Mbps	20 MHz	9
Fios-YEI1J-5G	18-78-D4-68-54-EE	802.11n/ac	-83	31	31.5	5.785	157	459	19	Verizon	BHR	GreenWave BHR4	WPA2-PSK	CCMP	1300 Mbps	80 MHz	1
Fios-YEI1J-5G	70-F2-20-0F-5C-F6	802.11g/n/ac	-84	29	30.8	5.540	108	486	21	Actiontec Electronics, Inc	Topaz	Reference Design	WPA2-PSK	CCMP	1733 Mbps	80 MHz	1
Fios-YGwp9...	72-A2-22-DF-D9-3A	802.11g/n	-75	53	53.6	2.412	1	211	18				WPA2-PSK	CCMP	600 Mbps	40 MHz	1
Gnetwork1	04-A2-22-DF-D9-38	802.11g/n	-78	43	49.4	2.412	1	242	20	Arcadyan Corporation			WPA2-PSK	CCMP	600 Mbps	40 MHz	1
kai home	3C-BD-C5-7F-26-E6	802.11g/n	-83	31	35.3	2.412	1	241	20	Arcadyan Corporation			WPA2-PSK	CCMP	600 Mbps	40 MHz	1
Max	58-D9-D5-9B-6D-B9	802.11g/n	-73	60	53.5	2.437	6	201	16	Tenda Technology Co.,Lt...			WPA2-PSK	CCMP	144 Mbps	20 MHz	4
MySpectru...	B8-EE-0E-F6-E8-AA	802.11g/n	-75	53	49.0	2.437	6	178	13	Sagemcom Broadband ...			WPA2-PSK	CCMP	216 Mbps	20 MHz	4
MySpectru...	A0-64-8F-DE-47-BB	802.11g/n/ac	-70	67	71.7	2.462	11	426	20	ASKEY COMPUTER CORP	RAC2V1K	RAC2V1K	WPA2-PSK	CCMP	1733 Mbps	20 MHz	9
MySpectru...	A0-64-8F-DE-47-BC	802.11n/ac	-86	24	29.1	5.180	36	486	19	ASKEY COMPUTER CORP	RAC2V1K	RAC2V1K	WPA2-PSK	CCMP	1733 Mbps	80 MHz	3
MySpectru...	98-1E-19-61-AB-FE	802.11g/n	-71	65	61.7	2.437	6	193	14	Sagemcom Broadband ...			WPA2-PSK	CCMP	216 Mbps	20 MHz	4

```
Element ID: 0  (SSID)
50 6F 6C 6F 20 47 72 6F 75 6E 64 73 28 3A 3C      Polo Grounds(:<


Element ID: 1  (Supported Rates)
82 84 8B 96 0C 12 18 24                          .......$


Element ID: 3  (DS Parameter Set)
01                                               .


Element ID: 5  (Traffic Indication Map)
00 02 00 00                                      ....


Element ID: 7  (Country)
55 53 20 01 0B 1E                                US ...


Element ID: 42  (802.11g Information)
02                                               .


Element ID: 50  (Extended Supported Rates)
30 48 60 6C                                      0H`l


Element ID: 48  (Robust Security Network)
```

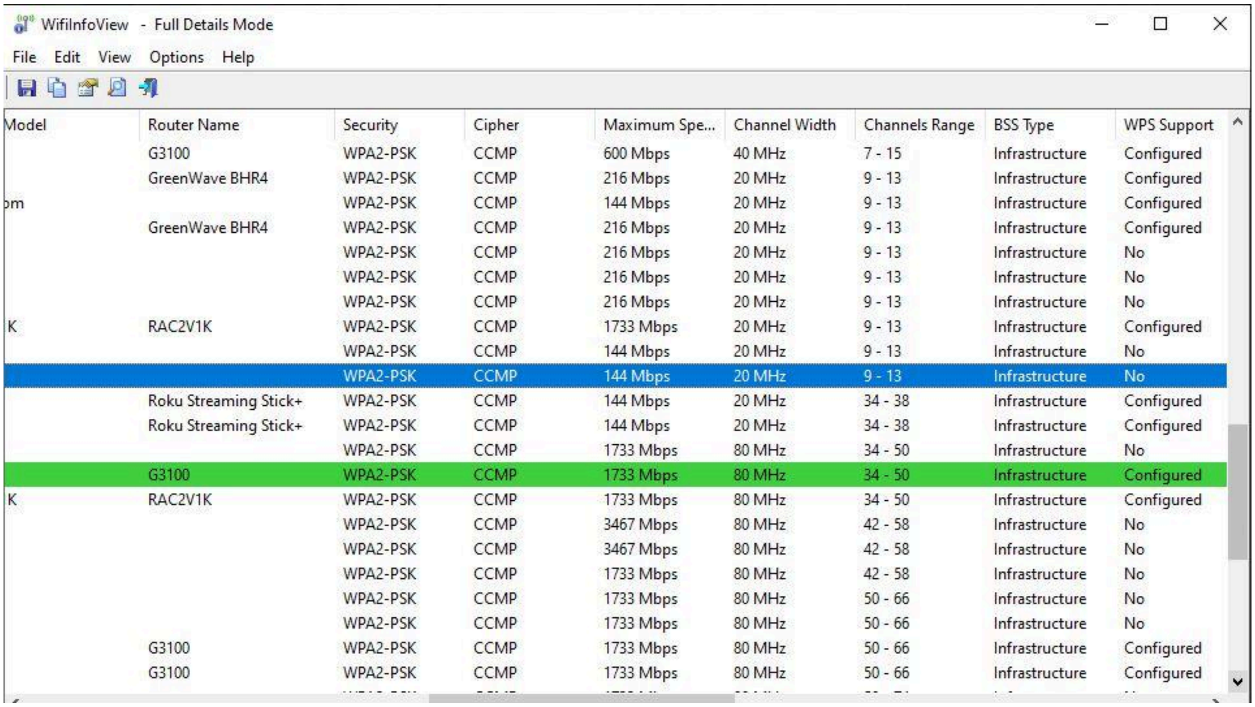
66 item(s), 1 Selected | NirSoft Freeware. https://www.nirsoft.net

3. The next step is to look at the SSID of each network around me. There is a service set identifier on most of them, but not all of them, the SSID also shows how strong the wifi signal is and if it is locked or not. I think the reason why an ssid might not show up is because some of these networks have been hidden on purpose. This gives an added level of security because you cannot directly see the name of the network that is showing up.



SSID	MAC Address	PHY Type	RSSI	Signal Quality	Average Signal...	Frequency	Channel	Information Size
	68-4A-76-31-EB-24	802.11n/ac	-83	31	31.0	5.785	157	133
	68-4A-76-31-EB-28	802.11n/ac	-85	26	26.0	5.785	157	163
	68-4A-76-3C-DD-E4	802.11n/ac	-84	29	34.2	5.785	157	133
	62-BD-C5-3D-62-56	802.11n/ac/ax	-87	22	20.9	5.300	60	336
	62-BD-C5-40-73-56	802.11n/ac/ax	-85	26	24.1	5.260	52	336
	70-F2-20-0F-5C-F8	802.11g/n/ac	-83	31	31.3	5.540	108	297
	22-EF-BD-7E-EA-22	802.11g/n	-63	81	82.1	5.180	36	271
	12-59-32-71-1C-63	802.11n	-58	83	82.2	5.180	36	268
	22-3B-F3-62-AA-9E	802.11g/n/ac	-82	33	40.2	2.422	3	296
	6A-BD-C5-38-B2-4E	802.11n/ac/ax	-52	87	85.2	5.180	36	336
	22-E0-19-58-12-E5	802.11g/n/ac	-77	46	70.8	2.462	11	214
	68-4A-76-3C-DD-E8	802.11n/ac	-83	31	36.6	5.785	157	163
	68-4A-76-3C-DE-63	802.11n/ac	-73	60	49.6	2.412	1	139
	68-4A-76-3C-DE-67	802.11g/n/ac	-77	46	46.7	2.412	1	193
	68-4A-76-3C-DD-E7	802.11g/n/ac	-71	65	64.5	2.412	1	193
	1A-78-D4-68-54-EF	802.11n/ac	-83	31	33.7	5.785	157	259
	6A-BD-C5-2D-D1-...	802.11n/ac/ax	-83	31	25.7	5.260	52	336
	68-4A-76-3C-DD-E3	802.11n/ac	-71	65	66.0	2.412	1	139
	62-BD-C5-38-B2-48	802.11n/ac/ax	-60	82	82.6	5.700	140	336
	68-4A-76-31-EB-23	802.11n/ac	-75	53	58.3	2.412	1	139
	68-4A-76-31-EB-27	802.11g/n/ac	-75	53	60.2	2.412	1	192
	DE-72-23-09-8D-61	802.11n	-82	33	33.0	5.745	149	317

4. A threat actor can use the value under the MAC address column because a threat actor can use your MAC address to act like they are from your network to spoof into other networks.
5. The next step is to click on channels and sort the channels out. There are multiple networks using the same channel, this can be a problem because it can cause network traffic and can cause your internet speed to become slower.
6. The security that my network is using is WPA2-PSK, the security that the other network that I chose is also using WPA2-PSK.

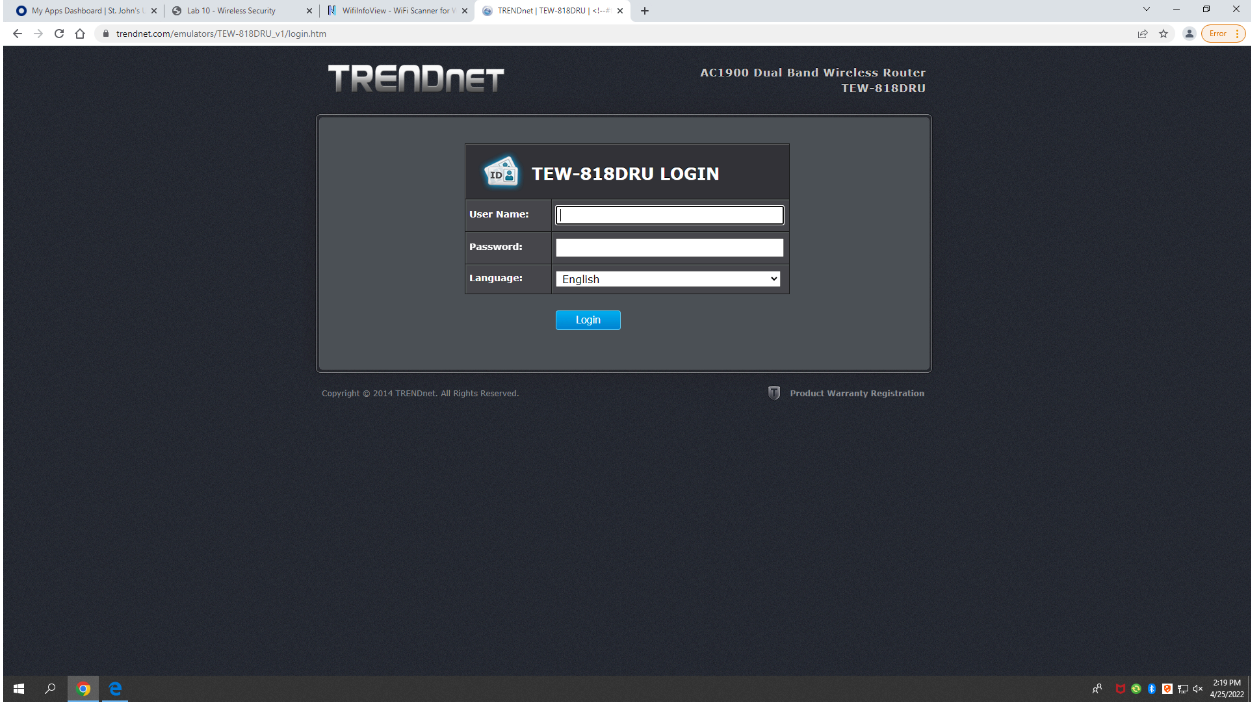


Model	Router Name	Security	Cipher	Maximum Spe...	Channel Width	Channels Range	BSS Type	WPS Support
	G3100	WPA2-PSK	CCMP	600 Mbps	40 MHz	7 - 15	Infrastructure	Configured
	GreenWave BHR4	WPA2-PSK	CCMP	216 Mbps	20 MHz	9 - 13	Infrastructure	Configured
om		WPA2-PSK	CCMP	144 Mbps	20 MHz	9 - 13	Infrastructure	Configured
	GreenWave BHR4	WPA2-PSK	CCMP	216 Mbps	20 MHz	9 - 13	Infrastructure	Configured
		WPA2-PSK	CCMP	216 Mbps	20 MHz	9 - 13	Infrastructure	No
		WPA2-PSK	CCMP	216 Mbps	20 MHz	9 - 13	Infrastructure	No
		WPA2-PSK	CCMP	216 Mbps	20 MHz	9 - 13	Infrastructure	No
K	RAC2V1K	WPA2-PSK	CCMP	1733 Mbps	20 MHz	9 - 13	Infrastructure	Configured
		WPA2-PSK	CCMP	144 Mbps	20 MHz	9 - 13	Infrastructure	No
		WPA2-PSK	CCMP	144 Mbps	20 MHz	9 - 13	Infrastructure	No
	Roku Streaming Stick+	WPA2-PSK	CCMP	144 Mbps	20 MHz	34 - 38	Infrastructure	Configured
	Roku Streaming Stick+	WPA2-PSK	CCMP	144 Mbps	20 MHz	34 - 38	Infrastructure	Configured
		WPA2-PSK	CCMP	1733 Mbps	80 MHz	34 - 50	Infrastructure	No
	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	34 - 50	Infrastructure	Configured
K	RAC2V1K	WPA2-PSK	CCMP	1733 Mbps	80 MHz	34 - 50	Infrastructure	Configured
		WPA2-PSK	CCMP	3467 Mbps	80 MHz	42 - 58	Infrastructure	No
		WPA2-PSK	CCMP	3467 Mbps	80 MHz	42 - 58	Infrastructure	No
		WPA2-PSK	CCMP	1733 Mbps	80 MHz	42 - 58	Infrastructure	No
		WPA2-PSK	CCMP	1733 Mbps	80 MHz	50 - 66	Infrastructure	No
		WPA2-PSK	CCMP	1733 Mbps	80 MHz	50 - 66	Infrastructure	No
	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	50 - 66	Infrastructure	Configured
	G3100	WPA2-PSK	CCMP	1733 Mbps	80 MHz	50 - 66	Infrastructure	Configured

7. After checking the encryption protocol used, we now need to scroll to “WPS Support”. About ⅓ of the networks that are shown use WPS Support. WPS is easy and convenient to use, but it does have some security flaws within it.
8. Additional information that I find useful will be the channel width, that is when data can travel faster through a network. Another thing I find useful is the channel ranges, because you can tell where the network would reside, and if it's not on one channel, you know the range that the network can be sitting on.

Project 11-3

1. The first step is to go to this URL (www.trendnet.com/emulators/TEW-818DRU_v1/login.htm) and continue by logging in without a username and password by clicking the “Login” button.


My Apps Dashboard | St. John's
Lab 10 - Wireless Security
WifiInfoView - WiFi Scanner for
TRENDnet | TEW-818DRU |
Error
2:19 PM
4/25/2022

trendnet.com/emulators/TEW-818DRU_v1/login.htm

AC1900 Dual Band Wireless Router
TEW-818DRU

TEW-818DRU LOGIN

User Name:

Password:

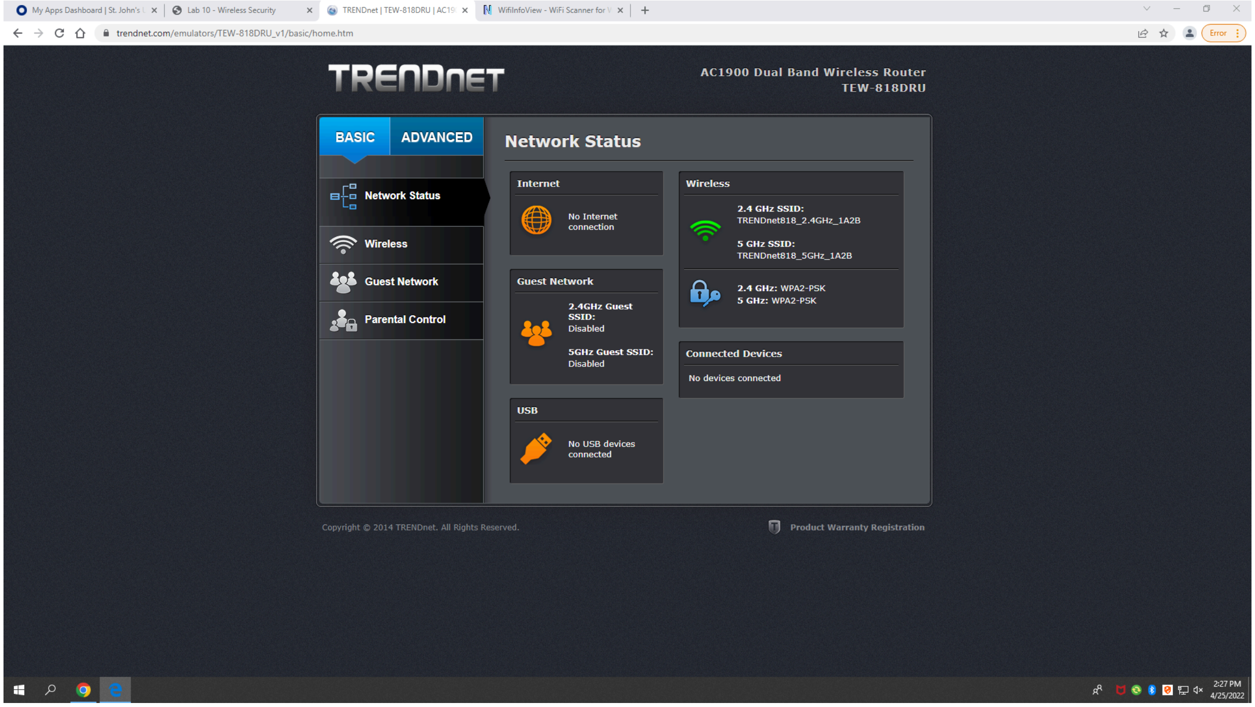
Language: English

Login

Copyright © 2014 TRENDnet. All Rights Reserved.

Product Warranty Registration

2. Once logged in, we have to make sure that we are under the basic tab, not the advanced tab. The network status says No internet connection, the guest network has both the 2.4 and 5 ghz SSID's disabled, there are no usb devices connected, the wireless connection has both the 2.4 and the 5 ghz under "TRENDnet818_2.4GHz_1A2B.


My Apps Dashboard | St. John's
Lab 10 - Wireless Security
TRENDnet | TEW-818DRU | AC19
WifiInfoView - WiFi Scanner for
Error
BASIC
ADVANCED
Network Status
Wireless
Guest Network
Parental Control
2:27 PM
4/25/2022

trendnet.com/emulators/TEW-818DRU_v1/basic/home.htm

AC1900 Dual Band Wireless Router
TEW-818DRU

Network Status

Internet
No Internet connection

Wireless
2.4 GHz SSID: TRENDnet818_2.4GHz_1A2B
5 GHz SSID: TRENDnet818_5GHz_1A2B
2.4 GHz: WPA2-PSK
5 GHz: WPA2-PSK

Guest Network
2.4GHz Guest SSID: Disabled
5GHz Guest SSID: Disabled

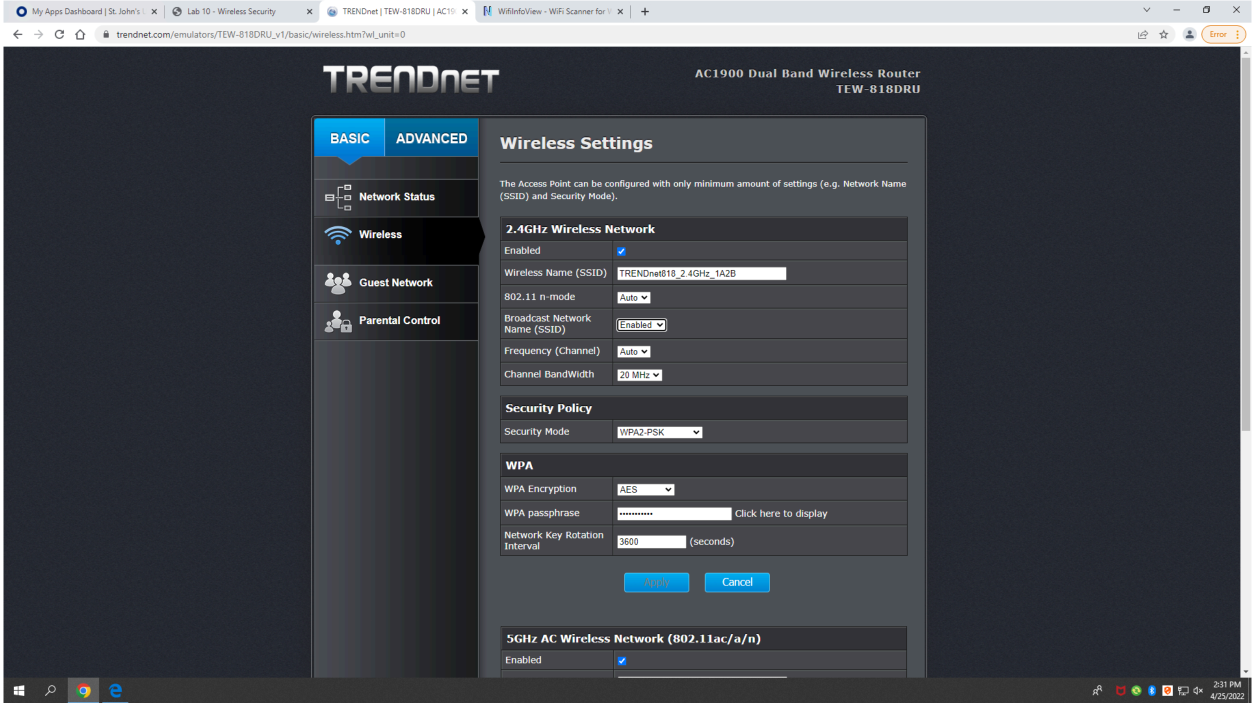
Connected Devices
No devices connected

USB
No USB devices connected

Copyright © 2014 TRENDnet. All Rights Reserved.

Product Warranty Registration

3. The next step is to go to the wireless tab and read the information displayed. Focusing on the option called “Broadcast Network Name (SSID)” clicking on the arrow next to it gives me two options, enabled and disabled. By default it is enabled. The benefit of disabling this option is that it created a more secure wireless network by preventing others from detecting our SSID.


My Apps Dashboard | St. John's
Lab 10 - Wireless Security
TRENDnet | TEW-818DRU | AC19
WifiInfoView - WiFi Scanner for
trendnet.com/emulators/TEW-818DRU_v1/basic/wireless.htm?wl_unit=0
Error
TRENDnet
AC1900 Dual Band Wireless Router
TEW-818DRU
BASIC
ADVANCED
Network Status
Wireless
Guest Network
Parental Control
Apply
Cancel
2:31 PM
4/25/2022

Wireless Settings

The Access Point can be configured with only minimum amount of settings (e.g. Network Name (SSID) and Security Mode).

2.4GHz Wireless Network	
Enabled	☑
Wireless Name (SSID)	TRENDnet818_2.4GHz_1A2B
802.11 n-mode	Auto
Broadcast Network Name (SSID)	Enabled
Frequency (Channel)	Auto
Channel BandWidth	20 MHz

Security Policy	
Security Mode	WPA2-PSK

WPA	
WPA Encryption	AES
WPA passphrase	••••••••••• Click here to display
Network Key Rotation Interval	3600 (seconds)

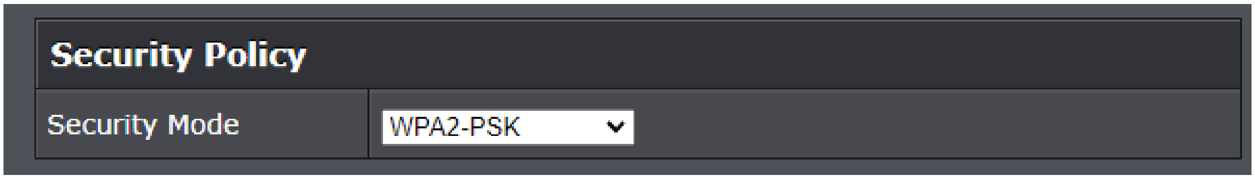
5GHz AC Wireless Network (802.11ac/a/n)	
Enabled	☑

4. The next step asks us to focus on “Frequency (Channel)” and see that the default for this option is auto. This means that the channel selection will set the access points to the best frequency channel. Now lets click the down arrow, it gives us options from 1 all the way to 11, you would want to change the channel when your internet access is slow, by changing the channel, your router will communicate on a different frequency, avoiding the interference that may be making your internet speed slow.

5. The next step asks us to focus on “Channel BandWidth”, more specifically to click the down arrow on 20 MHz. The other option is 40 MHz. You would usually want to choose a higher MHz when you need greater speed and faster transfer rates between channels.

6. The next step is to look at “Security Policy” and under it look at “Security Mode.” The default option for the security mode is WPA2-PSK. This is the usual default option for routers to support AES. WPA2-PSK is Wifi Protected Access 2. This holds a Wi-Fi encryption standard and an AES encryption protocol within it. Now

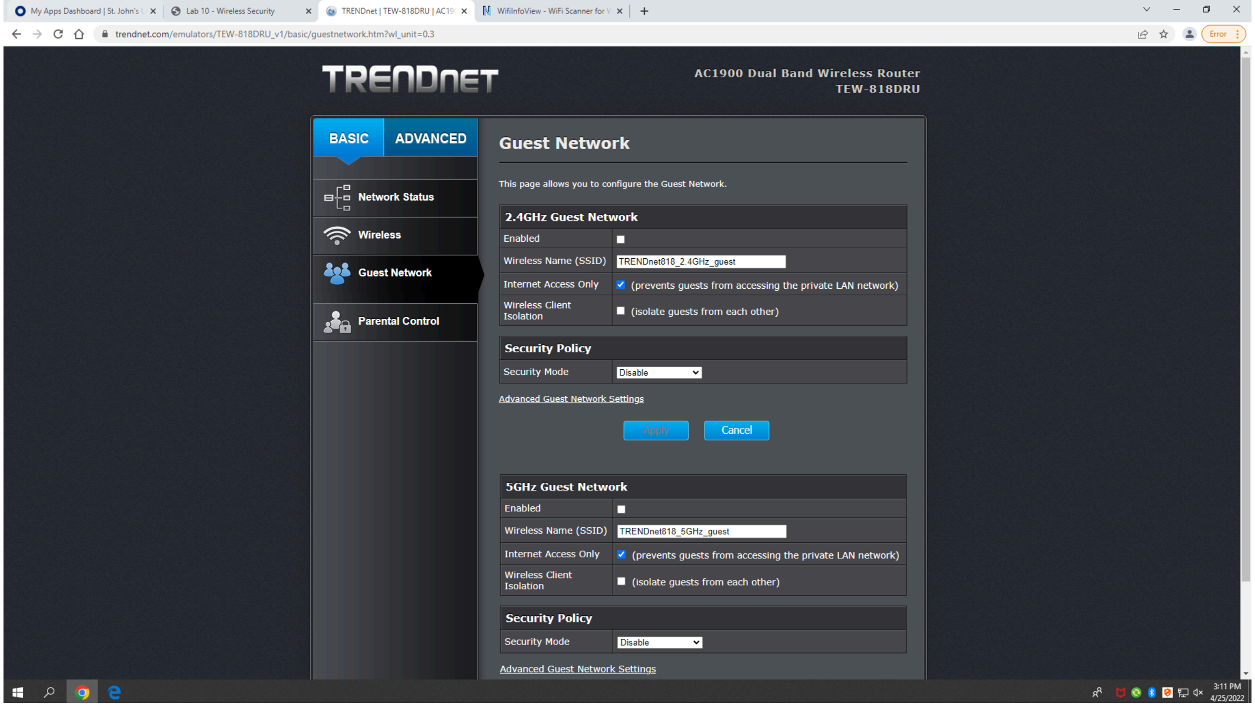
lets click the down arrow and see the different options. The other options are WPA, WPA-PSK, WPA2-PSK Mixed, WPA2, WPA2 Mixed. These other options are just other security programs for routers. Some are older than others, such as WPA being older than WPA2.



Security Policy

Security Mode	WPA2-PSK

7. The next step is to look at the "WPA" tab, more specifically "WPA Encryption." After clicking the down arrow, the two options are AES and TKIP+AES. AES was the default option. TKIP+AES is the combination of both the TKIP encryption protocol and the AES encryption protocol. Next we need to look at the "WPA Passphrase" and see how long the passphrase is. The passphrase is 11 characters. It would be sufficient if the passphrase included uppercase, lowercase, and special characters as well, but if it was just 11 lowercase letters then I don't think that 11 characters would be sufficient enough.
8. Next we need to click on "Guest Network" on the left side. This can be an advantage because people can log on to your network and there is no way for them to be able to harm the network by, for example, using a malware infected device on your network.



My Apps Dashboard | St. John's
Lab 10 - Wireless Security
TRENDnet | TEW-818DRU | AC19
WifiInfoView - WiFi Scanner for
Error
TRENDnet
BASIC
ADVANCED
Network Status
Wireless
Guest Network
Parental Control
3:11 PM
4/25/2022

trendnet.com/emulators/TEW-818DRU_v1/basic/guestnetwork.htm?wl_unit=0.3

AC1900 Dual Band Wireless Router
TEW-818DRU

Guest Network

This page allows you to configure the Guest Network.

2.4GHz Guest Network

Enabled	□
Wireless Name (SSID)	TRENDnet818_2.4GHz_guest
Internet Access Only	☑ (prevents guests from accessing the private LAN network)
Wireless Client Isolation	□ (isolate guests from each other)

Security Policy

Security Mode	Disable

Advanced Guest Network Settings

Apply Cancel

5GHz Guest Network

Enabled	□
Wireless Name (SSID)	TRENDnet818_5GHz_guest
Internet Access Only	☑ (prevents guests from accessing the private LAN network)
Wireless Client Isolation	□ (isolate guests from each other)

Security Policy

Security Mode	Disable

Advanced Guest Network Settings

9. Noting the option "Internet Access Only" this would be selected if you only want to give the guest basic internet access and nothing else, so they can browse the web

and do everything else you can do with the internet, but nothing else that a regular network would provide for you.

10. Noting another option called “Wireless Client Isolation” this is not enabled by default because depending on how many people you have connecting to your guest network, it's more convenient to have it off by default, and if you do have a network where there are tons of people connecting per day, then you probably should enable wireless client isolation.
11. Under security policy for the guest network, the security mode for it is set to default. This is because if there was to be an encryption protocol for the guest network, they would need some sort of access to our actual network, which is not what you want when running a guest network, you want your private network to be separate from a guest network in the case of any network attacks.
12. The next step is to go to the “Advanced” panel and click security. Under access control, the LAN Client Filter Function is a filter used to restrict access to internet services from certain clients. This does not provide the strongest security if it was enabled and people can still spoof addresses to bypass the filter.
13. This interface was very easy to understand and navigate. It provides a ton of information on the network and everything is right there waiting for you to read it.