

FIT9137 Applied Session

Week-7

Topics

- Local Area Networks (LAN) and Wireless LAN (WLAN)

Covered Learning Outcomes:

- Analyze and formulate the functions and architectures of (wireless) local area networks, wide area networks and the Internet.

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (peers) to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the “Teaching Team and Unit Resources” tile in the FIT9137 Moodle site.

ACTIVITY: Detection of Wireless Networks

This activity can only be performed on your laptop equipped with a wireless network interface card (WNIC).

Activity 1.1: War-Driving and War-Walking

Wireless LANs are often not secure. It is simple to bring your laptop computer into a public area and listen for wireless networks. This is called War-Driving (if you are in a car) or War-Walking (if you're walking). As long as you do not attempt to use any networks without authorization, War-Driving and War-Walking are quite legal. There are many good software tools available for War-Driving.

- NetSpot for Windows or Mac OS: <http://www.netspotapp.com>
- Acrylic Wifi for Windows: <https://www.acrylicwifi.com/en/>
- inSSIDer-2 for Windows: <https://inssider.informer.com/2.0/>
- Net Stumbler for Windows: <http://www.netstumbler.com/downloads/>

The first step is to download and install a WLAN sniffing tool on a laptop computer that has wireless capability. Once you have installed the software, simply walk or drive to a public area and start it up. For each network, note the MAC address of the access point (or physical address if you prefer to use that term). Note the SSID, the channel number the AP is configured to use, the speed of the network, the access point vendor, and the type of encryption in use (if any). Also note the signal strength both by color coding the network (green is good) and by showing the signal-to-noise ratio (SNR) and the strength of the signal and the noise.

You will see a mix of WLANs. The channels we usually use for 802.11b and 802.11g are channels 1, 6, and 11. Notice a mix of channels 1 and 6, plus one channel 8 WLAN. 802.11b and 802.11g can be configured to use four channels (1, 4, 8, and 11), although the channels overlap to some extent. So, if you run an AP on channel 1 and another on channel 4, there will be some interference between the two APs. The best practice recommendation that most companies follow is to use a three-channel configuration.












































SSID	BSSID	Alias	Channel	Band	Security	Vendor	Mode	Level (SNR)	Signal	Signal %	Avg	Max	Min	Noise	Noise %	Last seen
  eduroam	00:14:1B:B5:70:22		1	2.4GHz	WPA/WPA2 E...	CISCO	g	<div><div></div></div> -71	29%	-71	-71	-71	-71	-92	8%	6s ago
  Linc	18:1E:78:A7:7B:E8		1	2.4GHz	WPA/WPA2 Pe...	SAGEMCOM	n	<div><div></div></div> -85	15%	-85	-85	-85	-85	-92	8%	6s ago
  guest-wir...	00:23:33:C2:3E:B1		1	2.4GHz	Open	CISCO	g	<div><div></div></div> -77	23%	-77	-77	-77	-77	-92	8%	6s ago
  guest-wir...	00:15:2C:49:64:FE		153	5GHz	Open	CISCO	a	<div><div></div></div> -71	29%	-74	-70	-78	-92	8%	6s ago	
  guest-wir...	00:14:1B:B5:70:2E		149	5GHz	Open	CISCO	a	<div><div></div></div> -83	17%	-84	-83	-85	-92	8%	6s ago	
  eduroam	00:15:2C:4B:84:02		6	2.4GHz	WPA/WPA2 E...	CISCO	g	<div><div></div></div> -42	58%	-42	-41	-43	-92	8%	6s ago	
  eduroam	00:23:33:C2:3E:BD		149	5GHz	WPA/WPA2 E...	CISCO	a	<div><div></div></div> -84	16%	-81	-80	-84	-92	8%	6s ago	
  eduroam	00:23:33:C2:3E:B2		1	2.4GHz	WPA/WPA2 E...	CISCO	g	<div><div></div></div> -75	25%	-75	-74	-76	-92	8%	6s ago	
  guest-wir...	00:15:2C:4B:B4:01		6	2.4GHz	Open	CISCO	g	<div><div></div></div> -41	59%	-42	-41	-42	-92	8%	6s ago	
  eduroam	0C:D9:96:82:EB:D2		11	2.4GHz	WPA/WPA2 En...	CISCO	g/n	<div><div></div></div> -	0%	-80	-80	-80	-	0%	16s ago	
  eduroam	00:15:2C:4B:B4:0D		48	5GHz	WPA/WPA2 E...	CISCO	a	<div><div></div></div> -52	48%	-53	-52	-54	-91	9%	6s ago	
  guest-wir...	00:14:1B:B5:70:21		1	2.4GHz	Open	CISCO	g	<div><div></div></div> -73	27%	-73	-73	-73	-92	8%	6s ago	
  eduroam	00:15:2C:49:64:FD		153	5GHz	WPA/WPA2 E...	CISCO	a	<div><div></div></div> -71	29%	-74	-70	-78	-92	8%	6s ago	
  eduroam	00:14:1B:B5:43:42		11	2.4GHz	WPA/WPA2 E...	CISCO	g	<div><div></div></div> -87	13%	-87	-87	-87	-92	8%	6s ago	
  guest-wir...	00:15:2C:4B:B4:0E		48	5GHz	Open	CISCO	a	<div><div></div></div> -52	48%	-53	-52	-54	-92	8%	6s ago	
  guest-wir...	0C:D9:96:82:EB:D1		11	2.4GHz	Open	CISCO	g/n	<div><div></div></div> -	0%	-81	-81	-81	-	0%	26s ago	
  TPG-4XFG	E8:08:8B:12:9D:C8		2	2.4GHz	WPA/WPA2 Pe...	Huawei	b/g/n	<div><div></div></div> -89	11%	-89	-89	-89	-92	8%	6s ago	
  eduroam	00:15:2C:49:64:F2		1	2.4GHz	WPA/WPA2 E...	CISCO	g	<div><div></div></div> -55	45%	-56	-55	-57	-92	8%	6s ago	
  Charn Cit...	AC:F1:DF:DF:07:7C		1	2.4GHz	WPA2 Personal	D-Link	b/g	<div><div></div></div> -	0%	-85	-85	-85	-	0%	16s ago	
  eduroam	00:14:1B:B5:70:2D		149	5GHz	WPA/WPA2 E...	CISCO	a	<div><div></div></div> -82	18%	-83	-82	-83	-92	8%	6s ago	
  guest-wir...	00:23:33:C2:3E:BE		149	5GHz	Open	CISCO	a	<div><div></div></div> -84	16%	-82	-80	-84	-92	8%	6s ago	
  guest-wir...	00:15:2C:49:64:F1		1	2.4GHz	Open	CISCO	g	<div><div></div></div> -55	45%	-55	-54	-57	-92	8%	6s ago	
  guest-wir...	00:14:1B:B5:43:41		11	2.4GHz	Open	CISCO	g	<div><div></div></div> -87	13%	-87	-87	-87	-92	8%	6s ago	

Figure 1: Netspot showing details of detected wireless networks

If you click on an access point in the left panel, the tool shows you a real time graph of the signal and noise for that network. You will see how the signal strength changed for one of the networks as you walked through the building. The left edge of the graph shows that the network started with a good signal (the green or light-colored area at the top of the bars) was much higher than the noise (the red or dark colored area at the bottom of the bars). As you walked around, the signal became weaker; the signal was barely higher than the noise. As you walked more, the signal dropped so that it was too weak for me to detect it from the noise.

Note: If you're interested to learn about why signal values can be negative, you can refer to the following link:

<https://www.quora.com/What-is-the-reason-for-using-negative-dBm-values-for-WiFi-signal-strength>

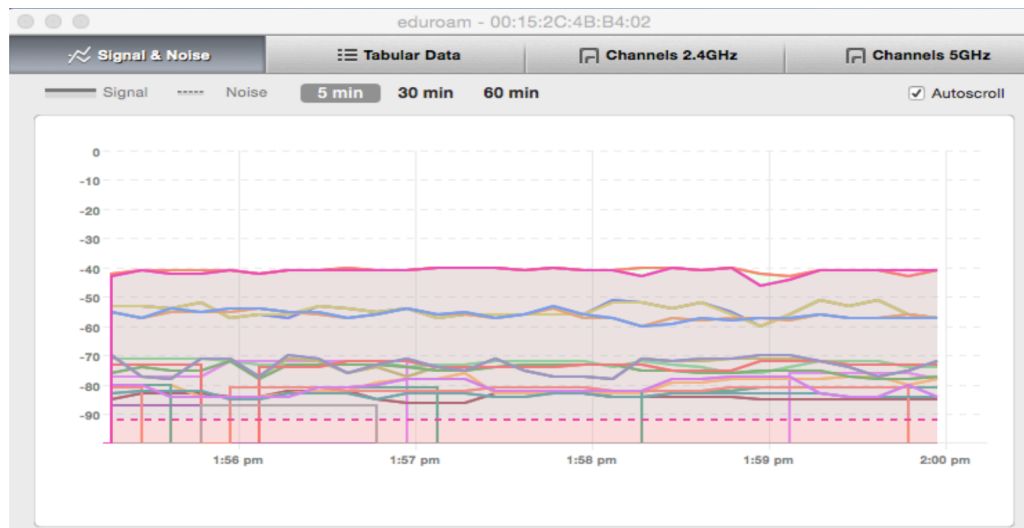


Figure 2: Netspot showing a real time graph of the signal and noise for eduroam

Activity 1.2: Survey Detectable Wireless Networks at Home/workplace

Install one of the aforementioned pieces of software and survey your residence for available networks.

1. Create a list of available wireless access points and observe the characteristics such as *SSID*, *MAC Address*, *Signal Strength*, *Signal to Noise Ratio (SNR)*, *Frequency Band*, *Mode*, *Security*, etc.
2. Investigate the Channel Occupancy.
 - a) Are different access points competing on the same channels?
 - b) Are they configured to use overlapping channels?
 - c) Could the configuration be improved?

Note: Since you may lose your Wi-Fi signal try the following tests before or after the Applied session.

3. Investigate the attenuation from the walls, doors, and other obstacles. Select your access point from the list to see the graph. Stand as close as possible to the AP for the first measurement. Then measure the signal strength at various points in order to answer the following questions:
 - a) How do different materials affect signal strength and/or noise?
4. Inspect the coverage of your WiFi router. Measure the signal strength at various points in your home and answer the following questions:
 - a) Does your access point sufficiently cover the desired area?
 - b) Could the placement or configuration be improved?
 - c) How does distance affect the signal strength?