

Introduction to Wireless

Campus Network Design & Operations Workshop



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(<http://creativecommons.org/licenses/by-nc/4.0/>)



UNIVERSITY OF OREGON

Last updated 29th May 2018



Wireless Networking Frequencies

- Wi-Fi is typically used in:
 - 2.4 GHz – 802.11b/g/n
 - 5.x GHz – 802.11a/n/ac
- Other bands interesting to us
 - 415/433 MHz
 - 868 MHz
 - 915 MHz
 - 3.5 GHz
 - 24 GHz
 - 60-80 GHz

Radio Waves

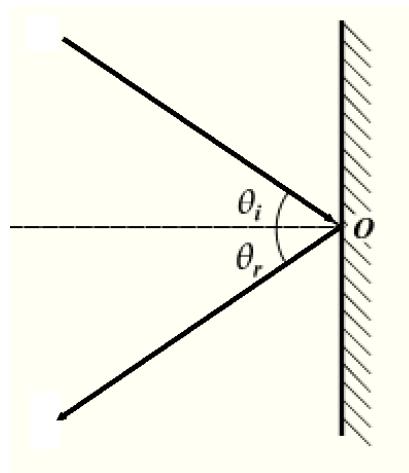
- Affected by:
 - Absorption
 - Reflection
 - Diffraction
 - Interference

Radio Waves: Absorption

- Absorption:
 - Converts energy into heat
 - Decreases power exponentially (linear decrease in dB)
 - Water, Metal, Oxygen
 - Stones, Bricks, Concrete
 - Wood, Trees
- Causes:
 - Plasterboard / Drywall Wall: 3-5dB
 - Metal Door: 6-10dB
 - Window: 3dB
 - Concrete Wall: 6-15dB
 - Block Wall: 4-6dB

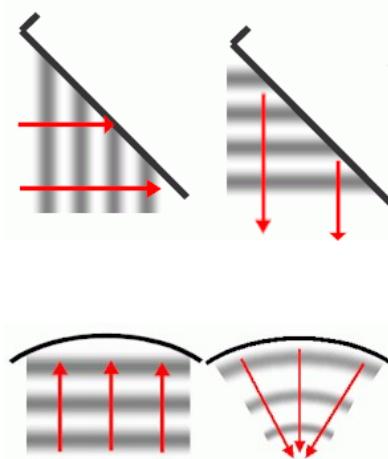
Radio Waves: Reflection

e.g. on Metal
angle in = angle out



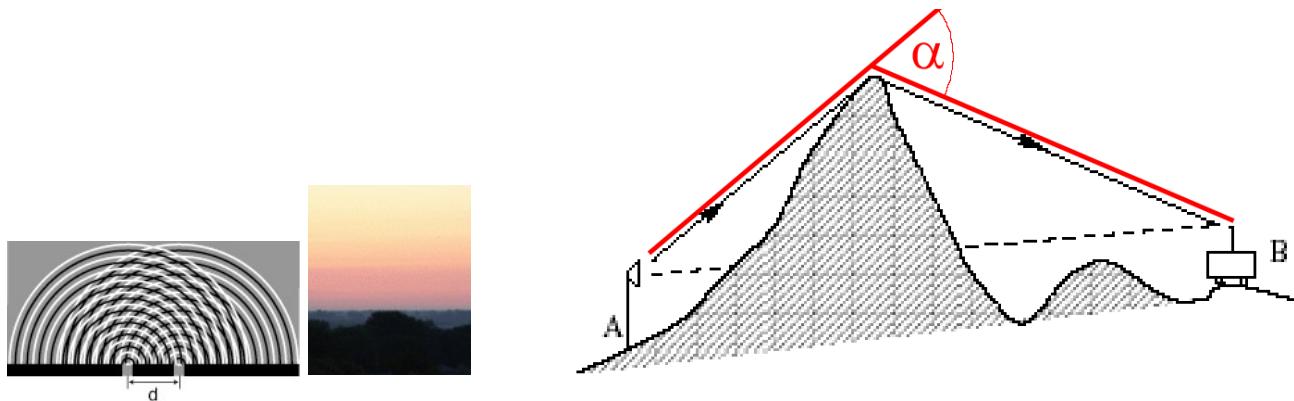
plane

parabola



Radio Waves: Diffraction

- Diffraction is the apparent bending and spreading of waves when they meet an obstruction. Scales roughly with wavelength.



Radio Waves: Interference

- Interference:
 - Interference is misunderstood
 - Is it really interference?
 - Or are we too lazy to find the real problem?
 - Maybe we don't care!
- Physicist's View:
 - The behaviour of waves
- Engineer's View:
 - Noise that causes problems
- Both are important for Wireless
 - In different ways!

Frequency Dependent Behaviour

- Lower Frequencies / Longer Wavelengths
 - Travel further
 - Travel through obstacles
 - Bend around obstacles
 - Need bigger antennas
- Higher Frequencies / Shorter Wavelengths
 - Can transport more data
 - Have higher re-usability
 - Need smaller antennas

Not All Spectrum is Created Equal

5GHz:	Wi-Fi	Better Propagation → ↓ Antenna Size →
2.4GHz:	Wi-Fi	
2.1GHz:	3G & LTE	
1.8GHz:	2G & LTE	
900MHz:	3G	
700MHz:	LTE	
500-700MHz:	UHF Television	
100MHz:	Radio	

The decibel (dB)

- Definition: $10 * \log_{10} (P_1 / P_0)$
- 3 dB = 2x power
- 6 dB = 4x power
- 10 dB = 10x power = order of magnitude
- Calculating in dBs
- Relative dBs
 - dBm = relative to 1 mW
 - dBi = relative to ideal isotropic antenna

The dB: Examples

- dBm is decibels relative to 1 milliwatt
 - Transmitters have power in dBm
 - Cables have loss in dBm
 - $1 \text{ mW} = 0 \text{ dBm}$
 - $100 \text{ mW} = 20 \text{ dBm}$
 - $1 \text{ W} = 30 \text{ dBm}$
- dBi is decibels relative to a perfect antenna
 - The “i” stands for isotropic
 - An omni antenna with 6 dBi gain
 - A parabolic dish with 29dBi gain

What is Wi-Fi?



- A Wi-Fi Alliance Trademark
 - Not strictly a technical term
- Wi-Fi is commonly used to refer to the 802.11 family of wireless standards
- Wi-Fi can run in ISM (Industrial, Scientific, Medical) bands
- Wi-Fi is designed for shared spectrum

Current 802.11 Standards

Standard	Data rate [Mbps]	Frequency [GHz]	Channel Access
802.11b	11	2.4	DSSS
802.11g	54	2.4	DSSS, OFDM
802.11a	54	5	OFDM
802.11n	150/300/600	2.4 / 5	DSSS, OFDM, MIMO
802.11ac	1300	5	OFDM, Mu-MIMO

Emerging 802.11 standards

Standard	Data rate [Mbps]	Frequency	Channel Access
802.11ad	>6000	60 GHz	Milimetre waves Very short range
802.11af	10-100	2.4	TV White Spaces Non Line of Sight

The Speed of Wi-Fi

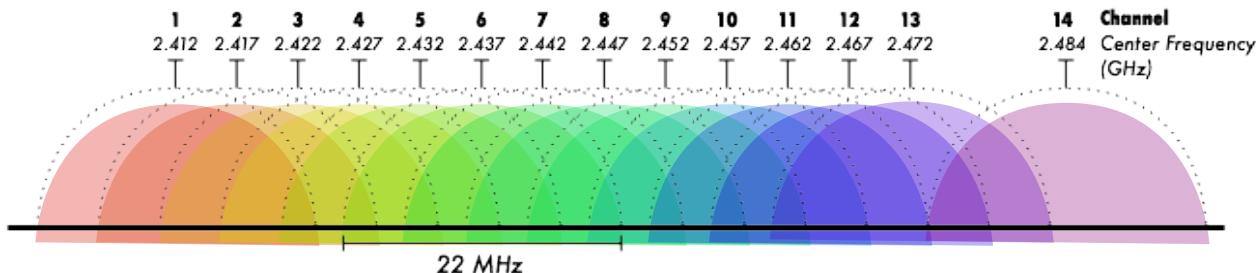
- Wi-Fi Data Rates – 11Mbps, 54Mbps, 1300Mbps
 - Peak raw radio symbol rates
 - Half-duplex, not full duplex!
 - Not actual TCP/IP throughput rates
 - Lower Speeds result due to:
 - Protocol overhead
 - Adaptive modulation
- Practical Wi-Fi advice, on a perfect link:
 - TCP/IP throughput is $\frac{1}{2}$ Wi-Fi data rate

Compatibility of Standards

Access Point

	802.11a	802.11b	802.11g	802.11n	802.11ac
802.11a	Yes			@5GHz	@5GHz
802.11b		Yes	(slower)	(slower)	
802.11g		(slower)	Yes	(slower)	
802.11n	@5GHz	@2.4GHz	@2.4GHz	Yes	(slower)
802.11ac	@5GHz			@5GHz	Yes

802.11 Wi-Fi Channels

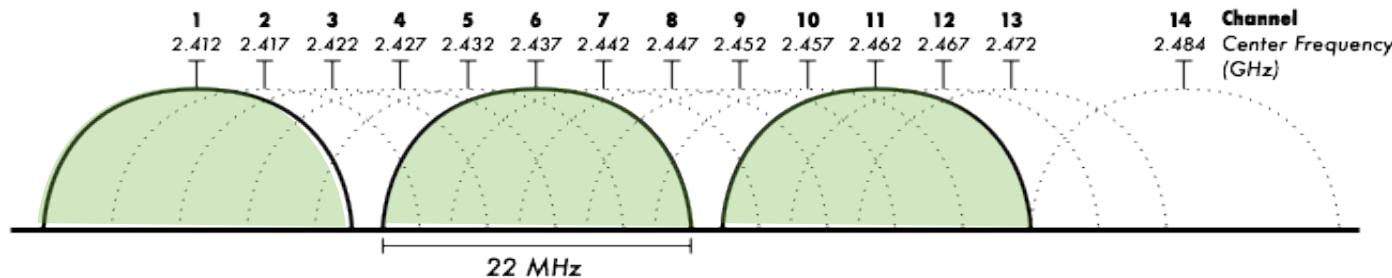


- Frequency bands are divided into channels
- 2.4 GHz has 14 overlapping channels of 22 MHz each
- 5 GHz has 25 non-overlapping channels of 20 MHz each
 - Country dependent
 - https://en.wikipedia.org/wiki/List_of_WLAN_channels
- Wi-Fi devices must use the same channel
- Wi-Fi devices send and receive on the same channel
 - This kind of connection is called half-duplex.

802.11 5GHz Channels

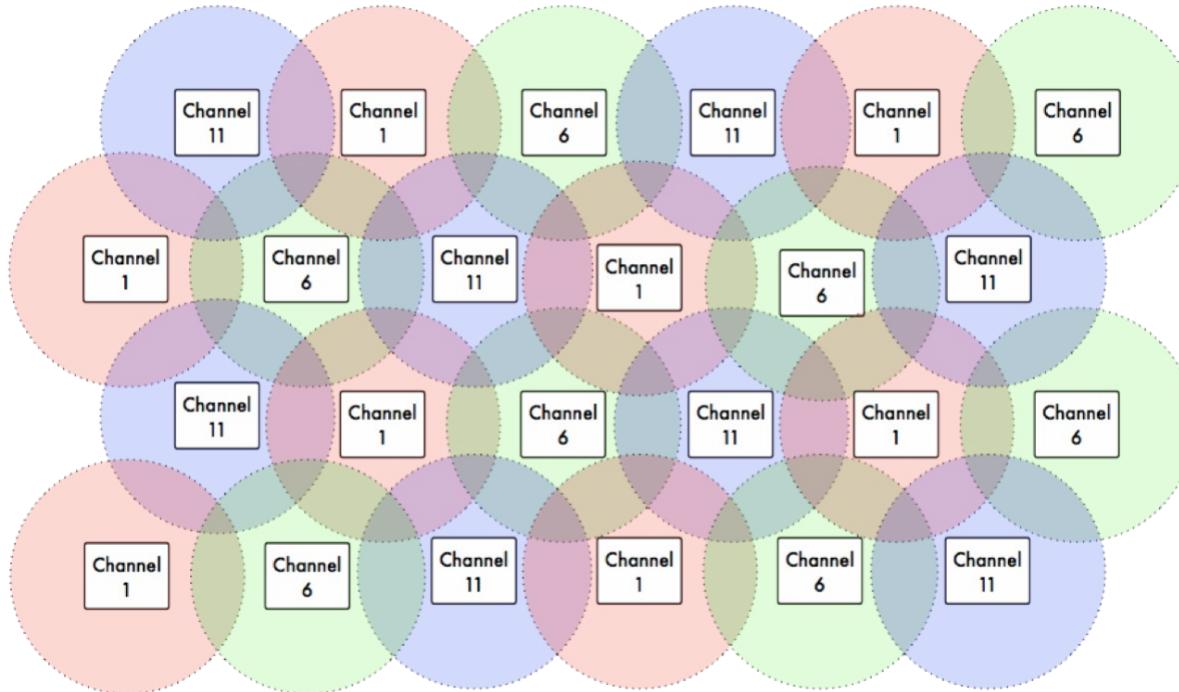
- 5 GHz has 25 non-overlapping channels:
 - U-NII-1: 5170-5250 has 4 of 20 MHz each
 - 36, 40, 44, 48
 - U-NII-2A: 5250-5330 has 4 of 20 MHz each
 - 52, 56, 60, 64
 - U-NII-2C: 5490-5730 has 12 of 20 MHz each
 - 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144
 - U-NII-3: 5735-5835 has 5 of 20 MHz each
 - 149, 153, 157, 161, 165
- Wider channels allow bigger bandwidths

Non-Overlapping Channels 1, 6, 11, 14



- Not All Countries Allow All Channels!
- Channel 14 is not allowed in the USA

Three Channel Coverage Design



Remember this is theory!
Reality does not look this nice.



UNIVERSITY OF OREGON



How Many Clients?

- How many end users on one AP?
 - 100 moderate users
 - 10-30 heavy users
- Limitations
 - Radio Spectrum
 - Slowest Clients
 - Backhaul & Core Network
 - Access Point CPU / Packets Per Second
 - Not all Access Points are created equal!

Problems for the Future

- Bring Your Own Device (BYOD) means 2-4 devices per person
- Power over Ethernet (PoE) at 100Mbps is no longer enough
- 1Gbps Ethernet is not enough for some 802.11ac access points
- Network security is difficult, and getting more difficult
- How will you manage your users?

Wireless Network Planning

- **Planning is required**; needed to solve new problems wireless brings
 - Frequency monitoring & management
 - Reach & Power planning: Link budgets, Antennas
 - SSID planning: Names matter!
 - Rogue activity monitoring and management
 - Plan Subnet Sizes
 - Tradeoff between roaming ease & network scalability

Essential Planning: Site Surveys

- No matter what network you are building
 - Core infrastructure or edge access
 - Indoor or outdoor
 - Small or big
- **A site survey is mandatory**
- Results of the site survey are the basis for your technology and process decisions

Wireless at Layer 3

- Wi-Fi Routers do many things
 - Routing, NAT, Firewall, DHCP
 - These are Layer 3 functions!
- Keep Layer 3 functions in the wired core
 - You cannot scale a network with Wi-Fi Routers
- An Access Point simply bridges networks
 - This is a layer 2 function: 802.3 <-> 802.11
 - **Scalable networks use Access Points, not Wi-Fi Routers**

Wireless at Layer 2

- Wireless Modes
 - Master – used for Access Points
 - Managed – for Stations (Clients)
 - Ad-hoc – for Nodes in a Mesh Network
- SSID (**Service Set Identifier**)
 - The “Network Name”
 - Often Human Readable

Wireless at Layer 2: SSIDs

- SSIDs can provide user information:
 - MyUniv-Library
 - MyUniv-Dorm 1
 - MyUniv-AdminWing
- Tempting SSIDs are a bad idea
 - Campus-Security
 - Finance-Department
- SSID choice has impact on:
 - Roaming
 - Network design

Roaming Considerations

- What happens when wireless clients move:
 - From one AP to another, in the same building?
 - From one building to another?
 - To a different part of campus, or a remote campus?
- Is it important to stay on the network, without interruption (for example, to have a Voice over IP chat or video chat)?
- Is it acceptable to log on again, when entering a new network zone?

Wireless Roaming

- Ability to move around and stay on the network
- Two kinds of roaming:
 - Nomadic: interrupted, yet able to pick up again
 - Seamless: uninterrupted, always on
- Users prefer Seamless Roaming:
 - Avoids interruption
 - Avoids re-authentication
 - Keeps state and session

Wireless Network Authentication

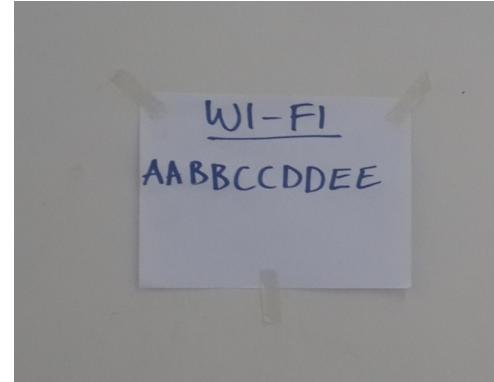
- Authentication can happen in many ways:
 - MAC Address Restrictions
 - Pre-Shared Key based Authentication
 - WPA-PSK – insecure, not scalable
 - Captive Portal Authentication
 - Better than a pre-shared key, but not the ideal
 - 802.1x based Authentication = Ideal!
 - Performed on centralized servers in the core

MAC Address Restriction

- MAC addresses identify machines, not people
- MAC addresses are easily spoofed
- Adds a lot of work for the helpdesk
 - Move/add/change for end user devices
- MAC restriction ok for infrastructure links & IoT
- Not suitable for user access control

Pre-Shared Keys

- Useful for some tasks
 - Non-critical Sensor devices with no Internet Access
 - Temporary Workshops
- Not recommended for General Use
 - Unless coupled with Portal-based authentication
- Keys will be shared!



802.1x/WPA2 Enterprise Authentication

WPA2-AES

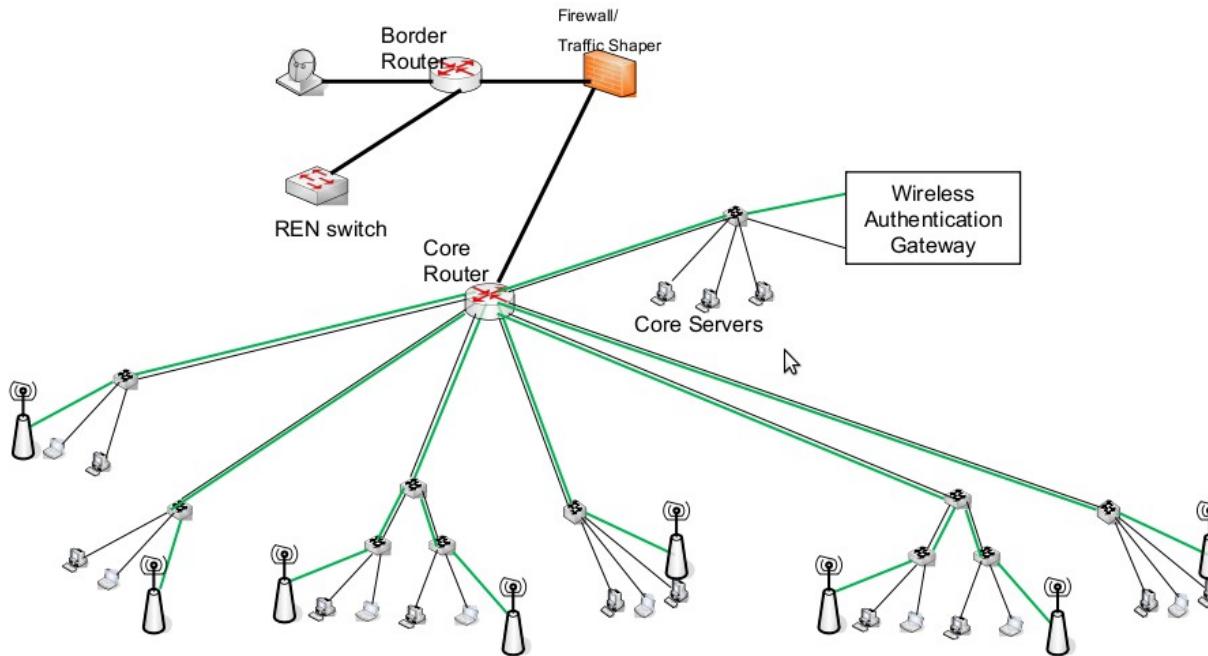
To secure your wireless network, select **WPA2-AES**, which is WPA2 (Wi-Fi Protected Access 2) security mode with AES (Advanced Encryption Standard) support only. AES is also known as CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which uses the AES algorithm.



The image shows a 'Wireless Security' configuration dialog box. It has three main settings: 'Security' set to 'WPA2-AES', 'WPA Authentication' set to 'PSK', and a 'WPA Preshared Key' field with a 'SHOW' button to its right.

- WPA2-AES is the only recommended security mode.
- WPA1 and WEP are no longer secure.

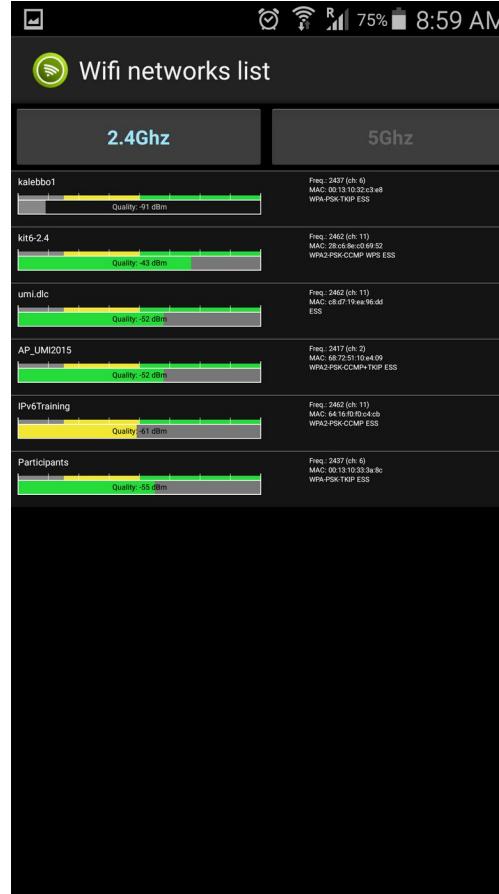
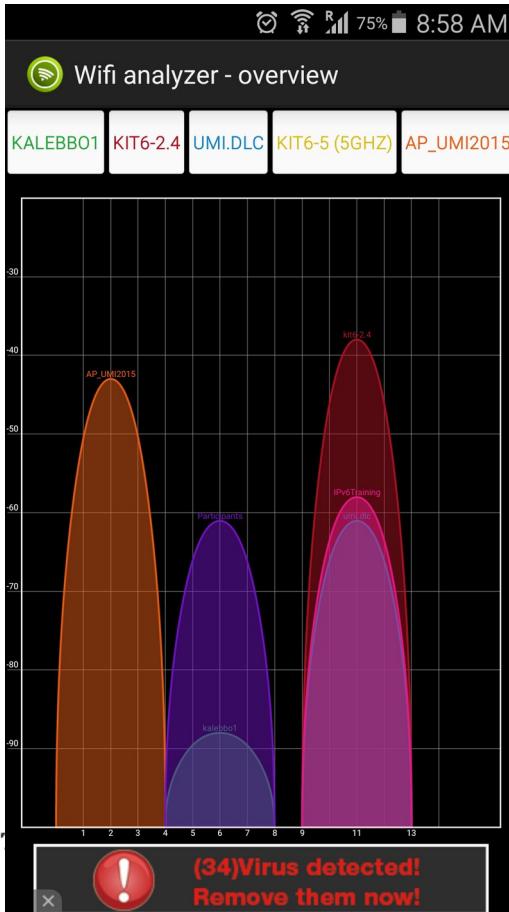
Authentication on wireless networks



Spectrum Analysers

- Spectrum Analysers are Layer 1
 - They can represent the physical layer!
 - Can show non-Wi-Fi signals, for example:
 - Microwave ovens, Bluetooth devices, jamming
- Real spectrum analysers are very expensive
- Some equipment includes spectrum analysis
 - For example, Ubiquiti outdoor radios
- USB analysers or RF Explorer can work well
 - e.g. AirView (2.4 GHz), WiSpy (2.4 – 5.8 GHz)

Android WiFi analyzers



WiFi Explorer

en0: Scanning | Associated: NSRC-PFS, Ch 36, 40 MHz, 360 Mbps

All Networks

Filter

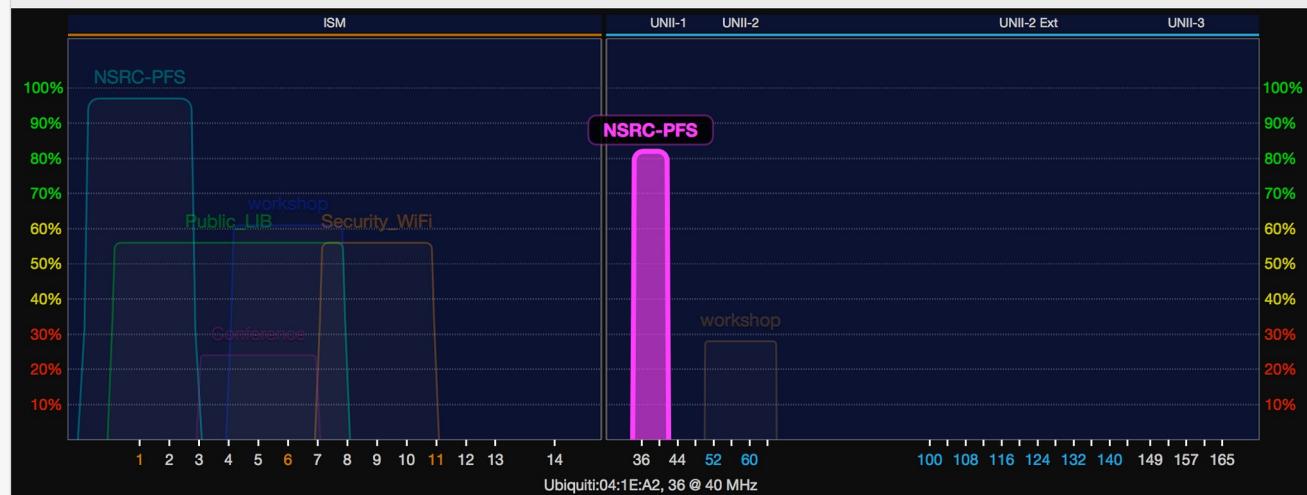
RESULTS	Network Name	BSSID	Vendor	Signal	Channel	Width	Band	Mode	Max Rate	Last Seen
6	NSRC-PFS	44:D9:E7:03:1...	Ubiquiti Networks Inc.	97%	1	20 MHz	2.4 GHz	b/g/n	144.4 M...	Just now
3	NSRC-PFS	46:D9:E7:04:...	Ubiquiti Networks Inc.	82%	36	40 MHz	5 GHz	ac	400 Mb...	Just now
8	workshop	00:A0:DE:E3:D...	YAMAHA CORPORATION	61%	6	20 MHz	2.4 GHz	b/g/n	144.4 M...	Just now
4	Security_WiFi	00:35:1A:CB:E...	Cisco Systems Inc.	56%	9	20 MHz	2.4 GHz	b/g/n	144.4 M...	Just now
	Public_LIB	14:CC:20:F4:7...	TP-Link Technologies Co. Ltd.	56%	2	40 MHz	2.4 GHz	b/g/n	300 Mbps	Just now
	workshop	00:A0:DE:E3:D...	YAMAHA CORPORATION	28%	52	80 MHz	5 GHz	ac	866.7 M...	Just now
	Conference	00:35:1A:A3:6...	Cisco Systems Inc.	24%	5	20 MHz	2.4 GHz	b/g/n	144.4 M...	Just now
	LMDwireless	00:19:E0:6F:B...	TP-Link Technologies Co. Ltd.	13%	6	20 MHz	2.4 GHz	b/g	54 Mbps	40 sec ago

Network Details

Signal Strength

Spectrum

Advanced Details



Wireshark

- A free and open-source packet analyzer.
- Used for network troubleshooting, analysis, software and communications protocol development, and education.
- Filter for fast identification of protocols, IP numbers, or keywords

Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: http contains password Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
407	31.189339	128.223.157.19	41.74.92.20	HTTP	HTTP/1.1 200 OK (text/html)
488	39.798732	41.74.92.20	128.223.157.19	HTTP	POST /workshops/2010/garnet-nsrc/login HTTP/1.1 (application/x-www-form-urlencoded)
791	62.372509	41.74.92.20	209.35.17.17	HTTP	GET /c/a/Administration/Capturing-Packets-with-the-Wireshark-Network-Analyzer/3. HTT
813	63.970537	41.74.92.20	209.85.229.101	HTTP	GET /_utm.gif?utmwv=1.3&utmn=529904867&utmcs=ISO-8859-1&utmrs=1400x1050&utmfc=24-bi
4874	170.723290	41.74.92.20	209.85.229.100	HTTP	GET /complete/search?hl=en&client=serp&expIds=17259,25901,26440&pq=POST&q=password&c
4879	170.9056041	41.74.92.20	173.194.37.104	HTTP	GET /search?hl=en&client=serp&expIds=17259,25901,26440&pq=POST&q=password&c
5798	193.902524	128.223.157.19	41.74.92.20	HTTP	HTTP/1.1 200 OK (text/html)
6039	202.176036	41.74.92.20	128.223.157.19	HTTP	POST /workshops/2010/garnet-nsrc/login HTTP/1.1 (application/x-www-form-urlencoded)
8899	240.562635	192.221.115.126	41.74.92.54	HTTP	HTTP/1.1 200 OK (text/css)
9930	241.864214	216.45.19.33	41.74.92.54	HTTP	HTTP/1.1 200 OK (application/x-javascript)
11882	246.775524	209.126.179.3	41.74.92.54	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
11886	246.778089	209.126.179.3	41.74.92.54	HTTP	Continuation or non-HTTP traffic
11887	246.779789	209.126.179.3	41.74.92.54	HTTP	Continuation or non-HTTP traffic

Frame 6039 (216 bytes on wire, 216 bytes captured)
Ethernet II, Src: Intel_05:b6:9b (00:19:d2:05:b6:9b), Dst: D-Link_bd:d6:76 (00:13:46:bd:d6:76)
Destination: D-Link_bd:d6:76 (00:13:46:bd:d6:76)
Source: Intel_05:b6:9b (00:19:d2:05:b6:9b)
Type: IP (0x0800)
Internet Protocol, Src: 41.74.92.20 (41.74.92.20), Dst: 128.223.157.19 (128.223.157.19)
Transmission Control Protocol, Src Port: 35262 (35262), Dst Port: http (80), Seq: 2422, Ack: 38609, Len: 150
[Reassembled TCP Segments (849 bytes): #6038(699), #6039(150)]
[HyperText Transfer Protocol
Line-based text data: application/x-www-form-urlencoded
_FORM_TOKEN=453a6d4a8ac48b906dc366c7&referter=http%3A%2F%2Fnsrsrc.org%2Fworkshops%2F2010%2Fgarnet-nsrc%2Fwiki%2Fagenda&user=sebastian&password=

0000 00 13 46 bd d6 76 00 19 d2 05 b6 9b 08 00 45 00 .F...v.....E.
0010 00 ca 4c le 40 00 40 06 4a bf 29 4a 5c 14 80 df ..L@. @. J.)J...
0020 9d 13 89 be 00 50 1d f0 9c e3 c1 95 84 d7 80 18P.....
0030 03 ea f3 aa 00 00 01 01 08 0a 00 03 ea f4 08 9f
0040 76 ce 5f 5f 46 4f 52 4d 5f 54 4f 4b 45 4e 3d 34 v_ FORM _TOKEN=4
0050 35 33 61 36 64 34 61 38 61 63 34 38 62 39 30 36 53a6d4a8 ac48b966
0060 64 63 33 36 63 37 26 72 65 66 65 72 65 72 3d dc366c7& referter=
0070 68 74 70 25 33 41 25 32 46 25 32 46 67 61 72 6e 65 http%3A%2F%2Fnsr
0080 63 2e 6f 72 67 25 32 46 77 6f 72 6b 73 68 6f 70 c.org%2F workshop
0090 73 25 32 46 32 30 31 30 25 32 46 67 61 72 6e 65 s%2F2010 %2Fgarne
00a0 74 2d 6e 73 62 25 32 46 77 69 6b 69 25 32 46 t-nsr%2F wiki%2F
00b0 41 67 65 66 64 61 26 75 73 65 72 3d 73 65 62 61 Agenda&u ser=seba
00c0 73 74 69 61 6e 26 70 61 73 73 77 6f 72 64 3d 6f stian&pa ssword=

Frame (216 bytes) Reassembled TCP (849 bytes)

Frame (frame), 216 bytes Packets: 14173 Displayed: 13 Marked: 0

Profile: Default

O UNIV SRC startup Resource Center

Summary

- Site-survey
 - AP placement is critically important
- Be aware of overlapping channels
 - Overlap = interference
- Use 5GHz as much as you can
 - 2.4GHz has only 4 non-overlapping channels
 - Implement band-steering if APs/Controller supports it
- SSIDs matter
 - Same SSID allows roaming
 - Different SSID means reauthenticating to change APs
- 802.1x/WPA2 authentication
 - Pre-shared key only useful for temporary set ups

Questions?

This document is a result of work by the Network Startup Resource Center (NSRC at <http://www.nsrc.org>). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.