Introduction to Wireless

Campus Network Design & Operations Workshop

UNIVERSITY OF OREGON

Last updated 29th May 2018

NSRC
Network Startup Resource Center

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

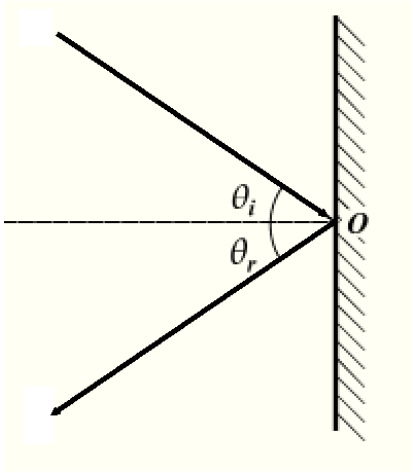
Radio Waves: Absorption

- 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

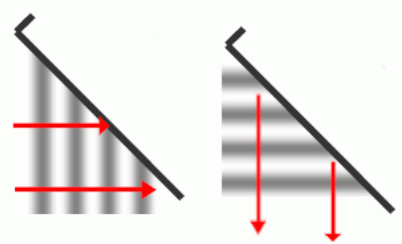
Radio Waves: Reflection

e.g. on Metal

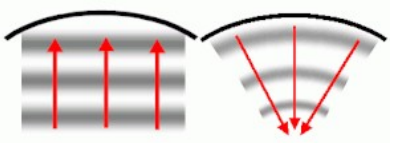
angle in = angle out



plane

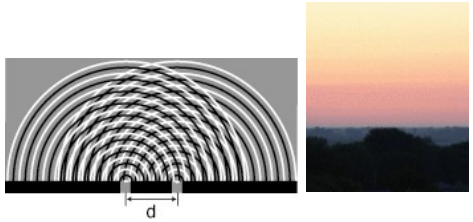


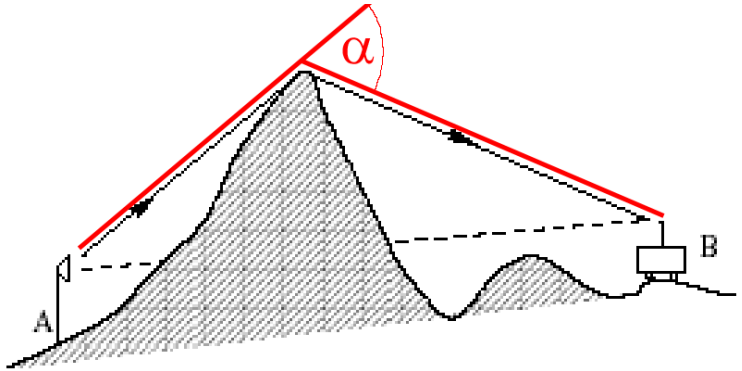
parabola



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

Capacity →

5GHz:	Wi-Fi
2.4GHz:	Wi-Fi
2.1GHz:	3G & LTE
1.8GHz:	2G & LTE
900MHz:	3G
700MHz:	LTE
500-700MHz:	UHF Television
100MHz:	Radio

Antenna Size ↓

Better Propagation →

The decibel (dB)

- Definition: $10 * \text{Log}_{10} (P_1 / P_0)$
- 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 mW = 0 dBm
  - 100 mW = 20 dBm
  - 1 W = 30 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 ½ Wi-Fi data rate

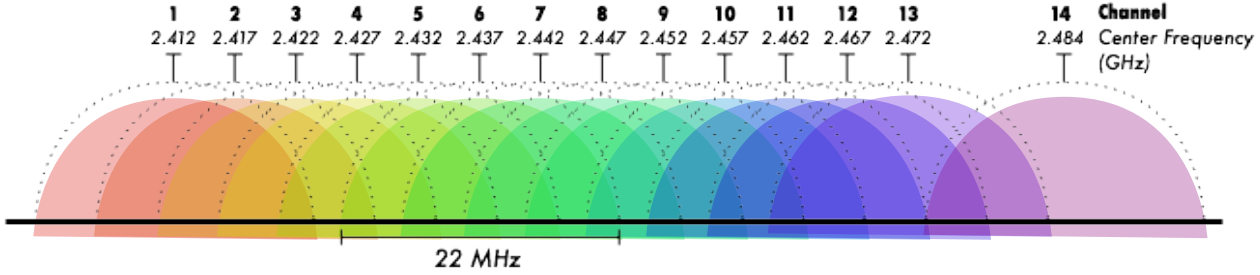
Compatibility of Standards

Access Point

Client

	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

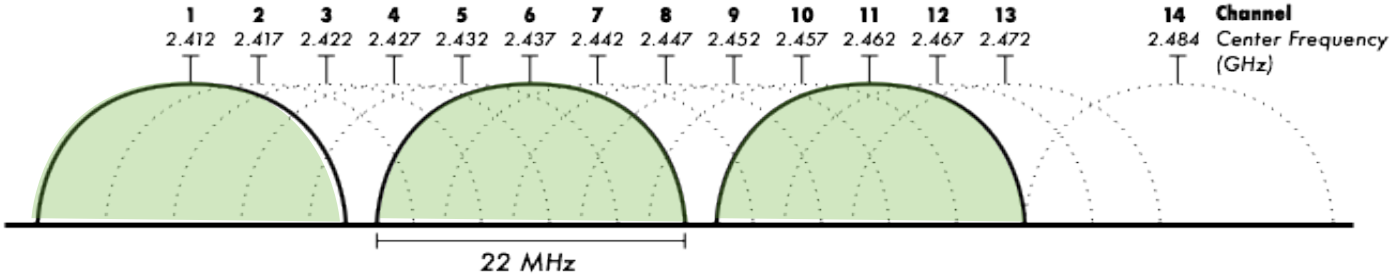


- Frequency bands are divided into channels
- 2.4 GHz has 14 overlapping channels of 22 MHz each
- 5 GHz has 25 non-overlapping channels of 20 MHz each
  - Country dependent
  - https://en.wikipedia.org/wiki/List_of_WLAN_channels
- Wi-Fi devices must use the same channel
- Wi-Fi devices send and receive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

802.11 5GHz Channels

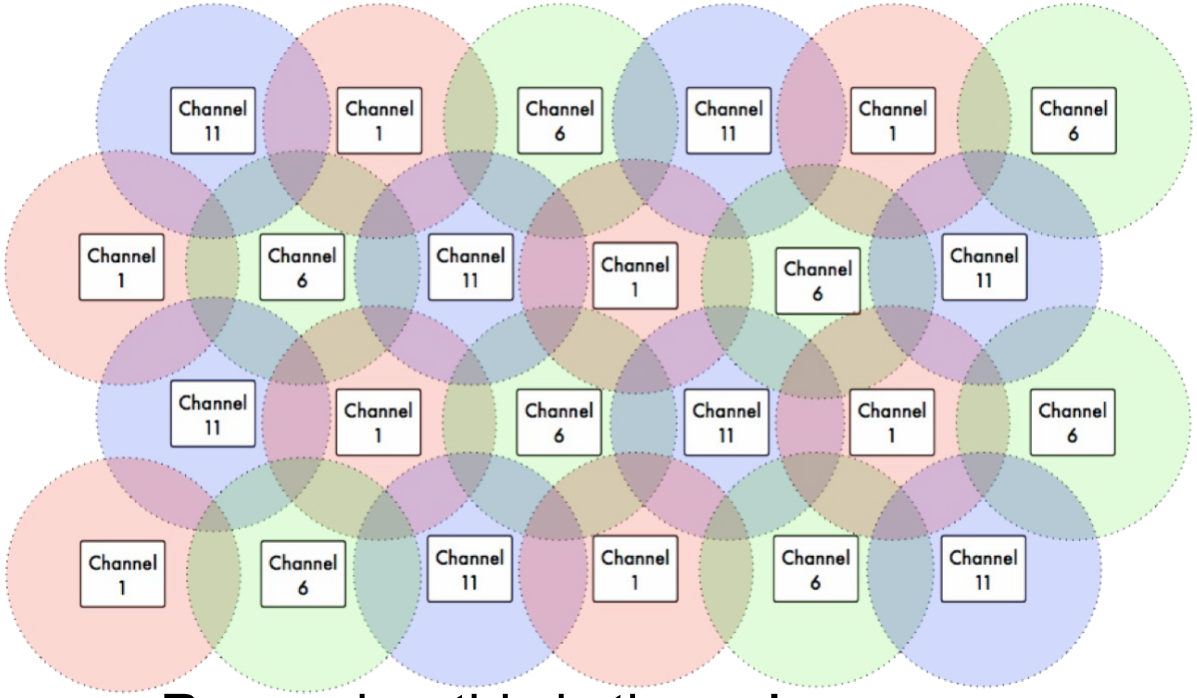
- 5 GHz has 25 non-overlapping channels:
  - U-NII-1: 5170-5250 has 4 of 20 MHz each
    - 36 ,40, 44, 48
  - U-NII-2A: 5250-5330 has 4 of 20 MHz each
    - 52, 56, 60, 64
  - U-NII-2C: 5490-5730 has 12 of 20 MHz each
    - 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144
  - U-NII-3: 5735-5835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

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

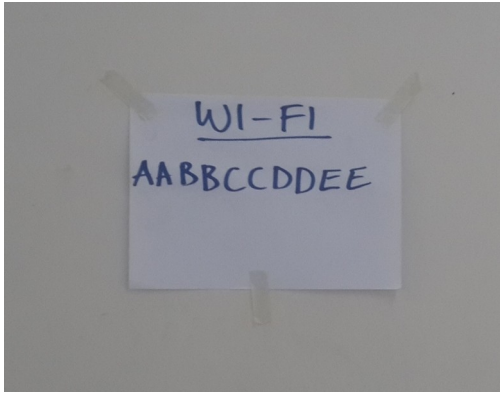
- Authentication can happen in many ways:
  - MAC Address Restrictions
  - Pre-Shared Key based Authentication
    - WPA-PSK – insecure, not scalable
  - Captive Portal Authentication
    - Better than a pre-shared key, but not the ideal
  - 802.1x based Authentication = Ideal!
    - Performed on centralized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

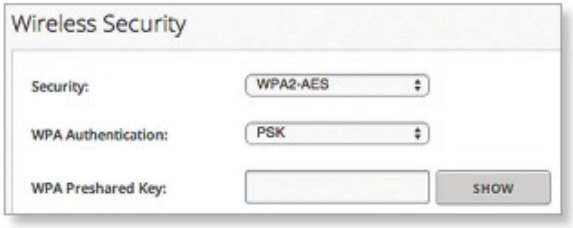
- Useful for some tasks
  - Non-critical Sensor devices with no Internet Access
  - Temporary Workshops
- Not recommended for General Use
  - Unless coupled with Portal-based authentication
- Keys will be shared!



802.1x/WPA2 Enterprise Authentication

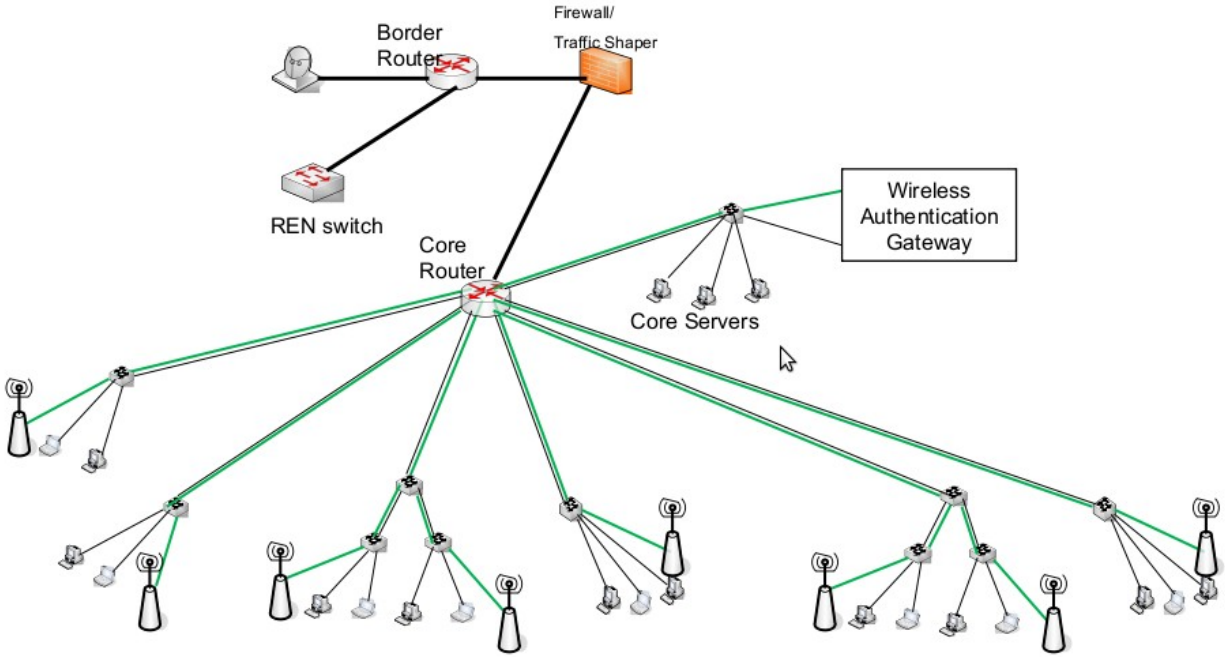
WPA2-AES

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.



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

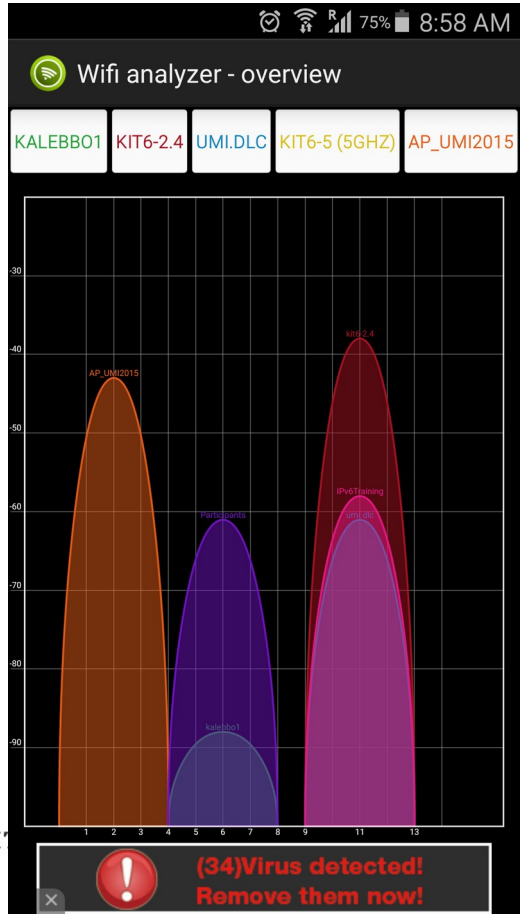
Authentication on wireless networks

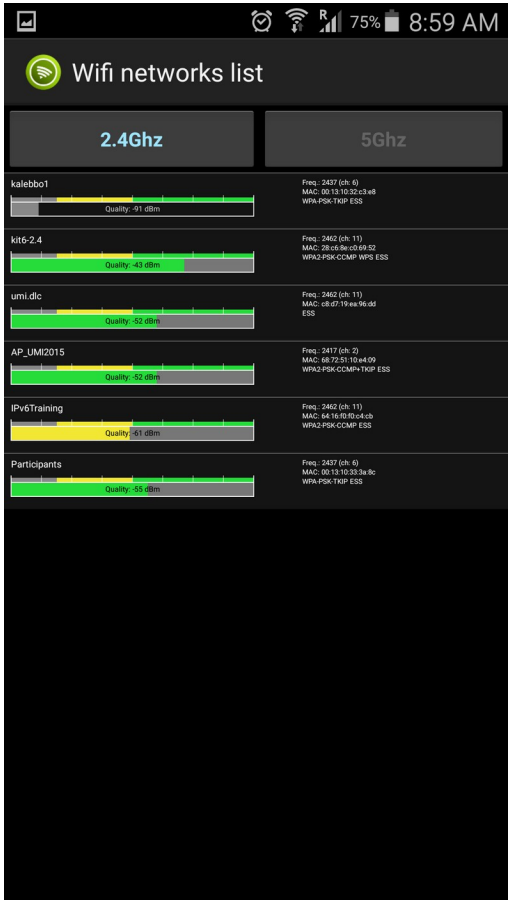


Spectrum Analysers

- 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

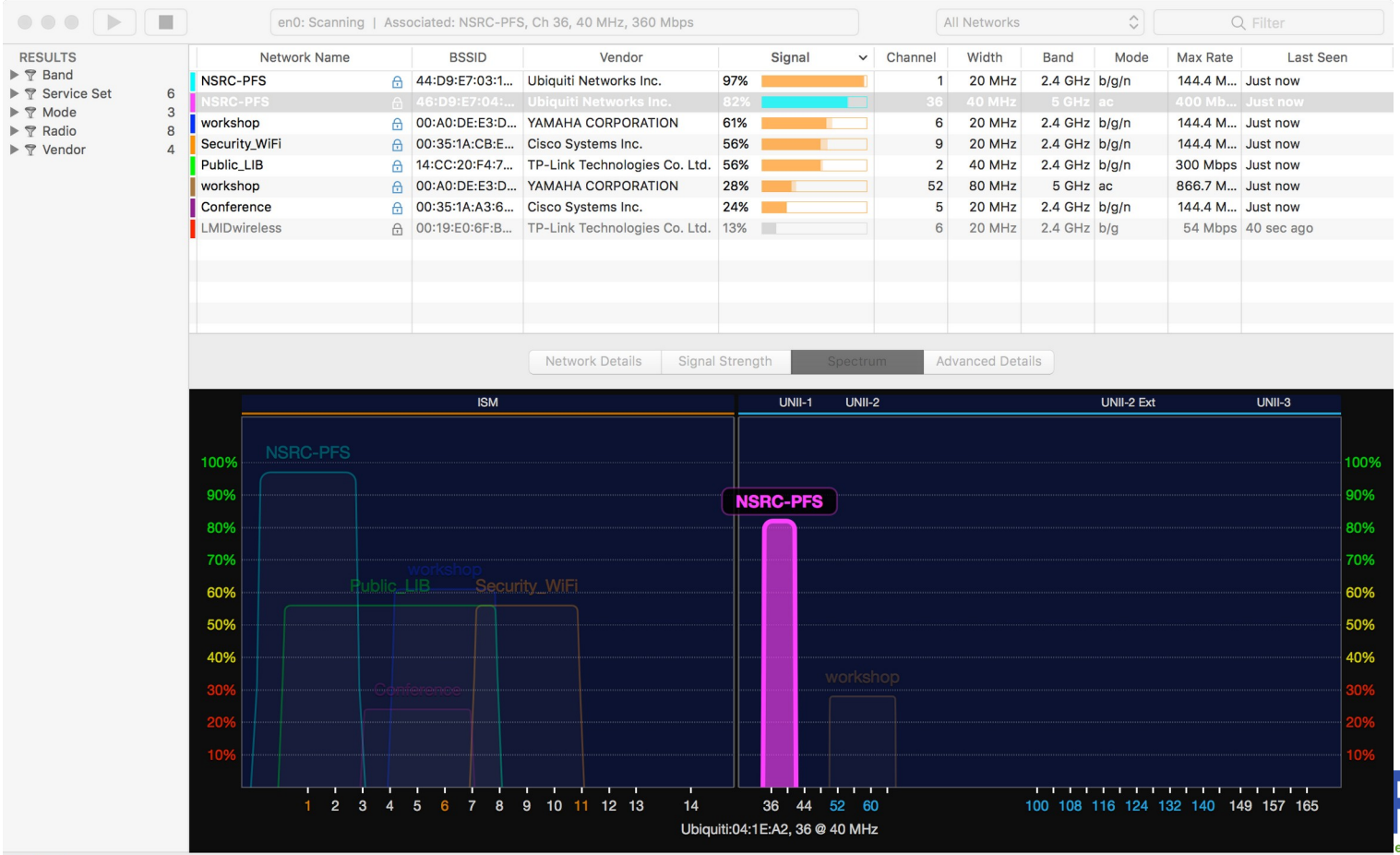




UNIVERSI

NSRC
Network Startup Resource Center

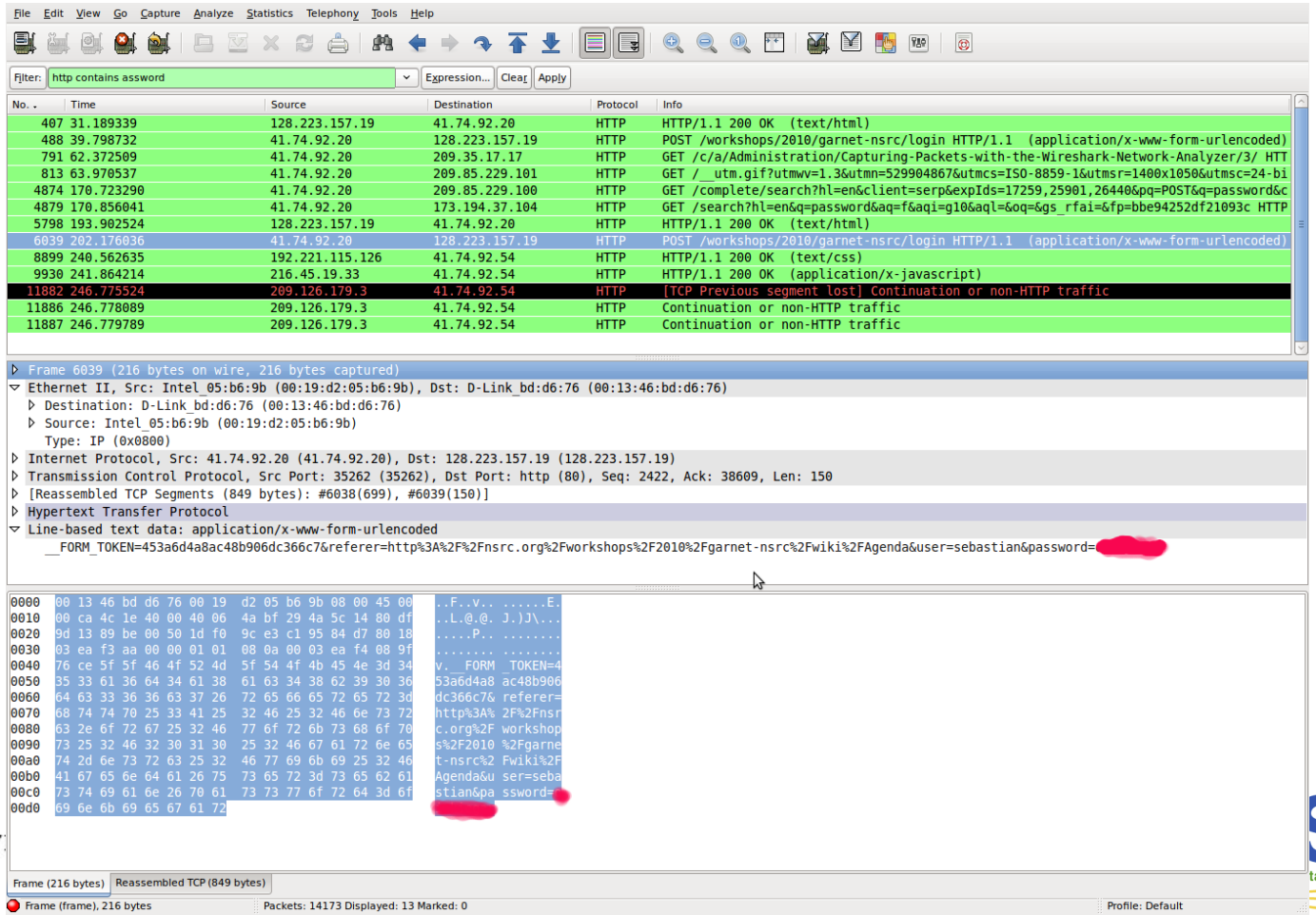
WiFi Explorer



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



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?