Wi-Fi Technology Fundamentals

Module-5

Advanced Features and Standard Extensions

Session-5a

Advanced MAC Features, 802.11h/k/v/r

Part1: WiFi Technology Fundamentals – Basics

Module1: Introduction and History of Wi-Fi	
Tue – 26th Sept 2023	Session1a: Evolution of WiFi WiFi Generations, Residential/Enterprise WiFi Applications, Business Evolution
Thu – 28th Sept 2023	Session1b: WiFi Network Topologies Infrastructure/Mesh/Bridge/Adhoc Modes, Backhaul Mechanisms, Deployment Use cases
Tue – 3rd Oct 2023	Session1c: WLAN Standards and Amendments Alphabet Soup IEEE Standards Bodies, WiFi Alliance, Standards and their extensions
Thu – 5th Oct 2023	Session1d: Basic Functional building blocks of a WiFi AP/Router PHY, Baseband, Lower MAC, Upper MAC, various Interfaces, key functional blocks

Module2: WLAN PHY Layer	
Tue – 10th Oct 2023	Session2a: Frequency Allocation ISM and UNII Bands, unlicensed spectrum allocation, channels, Channel BW
Thu – 12th Oct 2023	Session2b: Modulation/Coding, MIMO Basics Basics of Digital Modulation and Coding, Multipath, MIMO, OFDMA, Spectral Efficiency
Tue – 17th Oct 2023	Session2c: MCS Table, PHY Data Rates PHY Data rates, MCS Table, Theoretical Throughput
Thu – 19th Oct 2023	Session2d: PHY Headers and key functions PHY Headers, PCLP and PMD Sub Layers, Key PHY layer functions

Module3: WLAN MAC Layer	
Tue- 24th Oct 2023	Session3a: Basic AP Management and Control Functions Beaconing, BSSID, Scanning, Basic Service Set and its Capabilities
Thu – 26th Oct 2023	Session3b: MAC Framing, Headers and Key Functions MAC headers and key functions, Management/Control/Data Frames
Tue – 31st Oct 2023	Session3c: Carrier Sense and Medium Access Physical/Virtual Carrier Sensing, DCF, Random Backoff, Interframe Spacing, EDCA Parameters
Tue- 7th Nov 2023	Session3d: Data Transfer and Aggregation Data Transfer, Medium Overhead, Aggregation, Admission Control

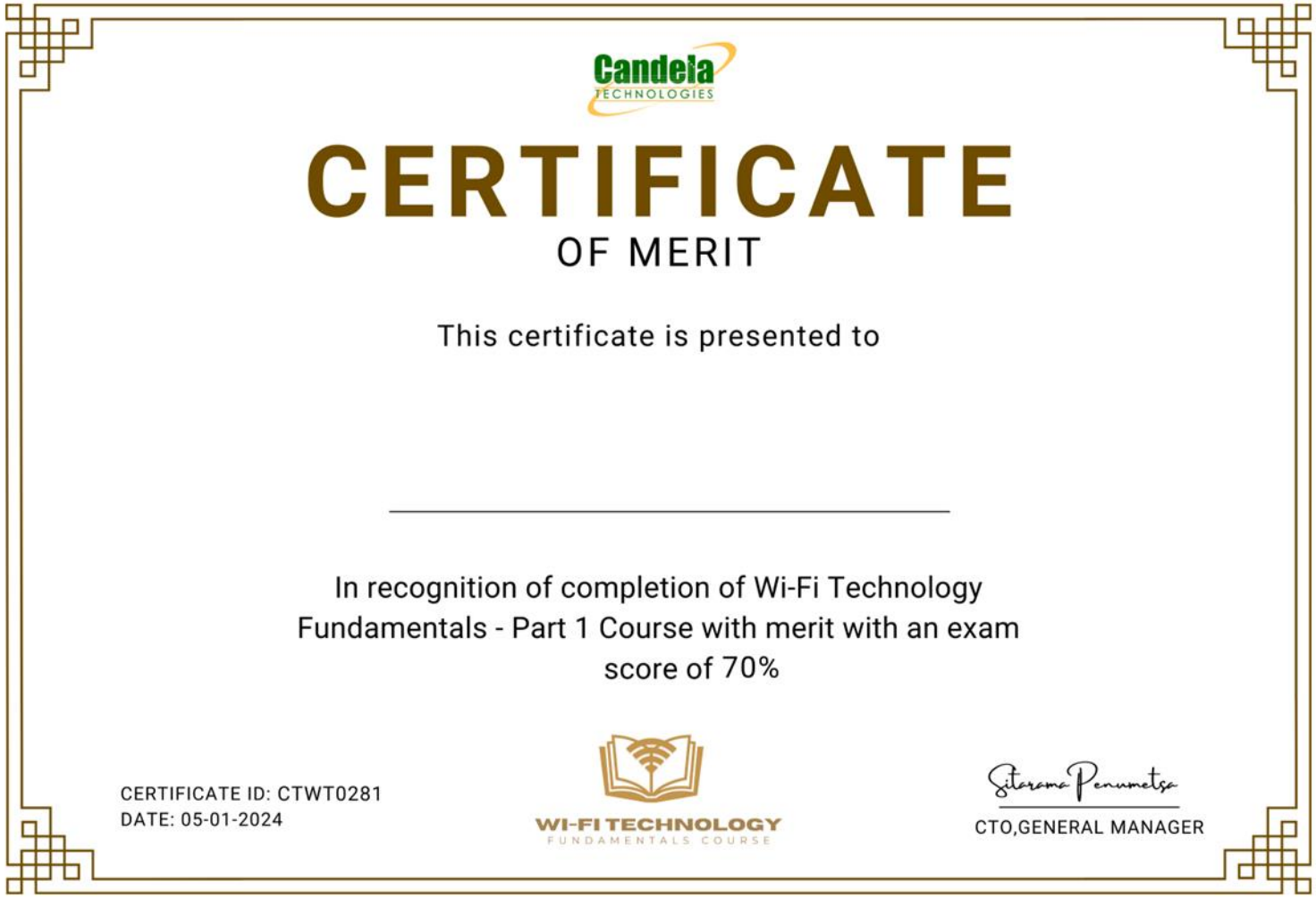
Module4: Security in Wi-Fi	
Tue- 14th Nov 2023	Session4a: Various WiFi Security Protocols Security basics, WEP, WPA/WPA2/WPA3, Enterprise/Personal, Captive Portal, WPS
Tue- 21st Nov 2023	Session4b: Basics of Authentication and Encryption EAP Methods, TKIP/CCMP, 802.1x connection, Key Generations, 4-way Handshake
Tue – 28th Nov 2023	Session4c: Attacks and Vulnerabilities DoS Attacks, Man in the Middle Attacks, Cracking Security Keys, PMF
Tue – 5th Dec 2023	Session4d: Seamless connectivity/Open Roaming Open Roaming Technology, WiFi to Cellular Handover, EAP-SIM/AKA

Part1 Exam Results and Certificates

Total Attended Exam: 160

Total Certificates Issued: 108

- Excellence (90% score or More) :1
- Merit (70%-90% Score) : 26
- Participation(50%-70% Score) : 81



Part2: WiFi Technology Fundamentals – Advanced

Module 5: Advanced Features and Standard Extensions		
Week 1	***Session5a: RRM, DFS, Power Save, Mobility*** *Load Balancing, Band Steering, ACS, DFS, TPC, Fast Roaming*	Slides | Video | Quiz | Q&A | Notes
Week 2	***Session5b: WiFi6 new features*** *ODFMA, Mu-MIMO, BSS Coloring, 1024 QAM, WPA3*	Slides | Video | Quiz | Q&A | Notes
Week 3	***Session5c: WiFi6E new features*** *6GHz spectrum allocation, 320Mhz channels, AFC*	Slides | Video | Quiz | Q&A | Notes
Week 4	***Session5d: WiFi7 new features*** *4K QAM, MLO, Preamble PuncturingC*	Slides | Video | Quiz | Q&A | Notes

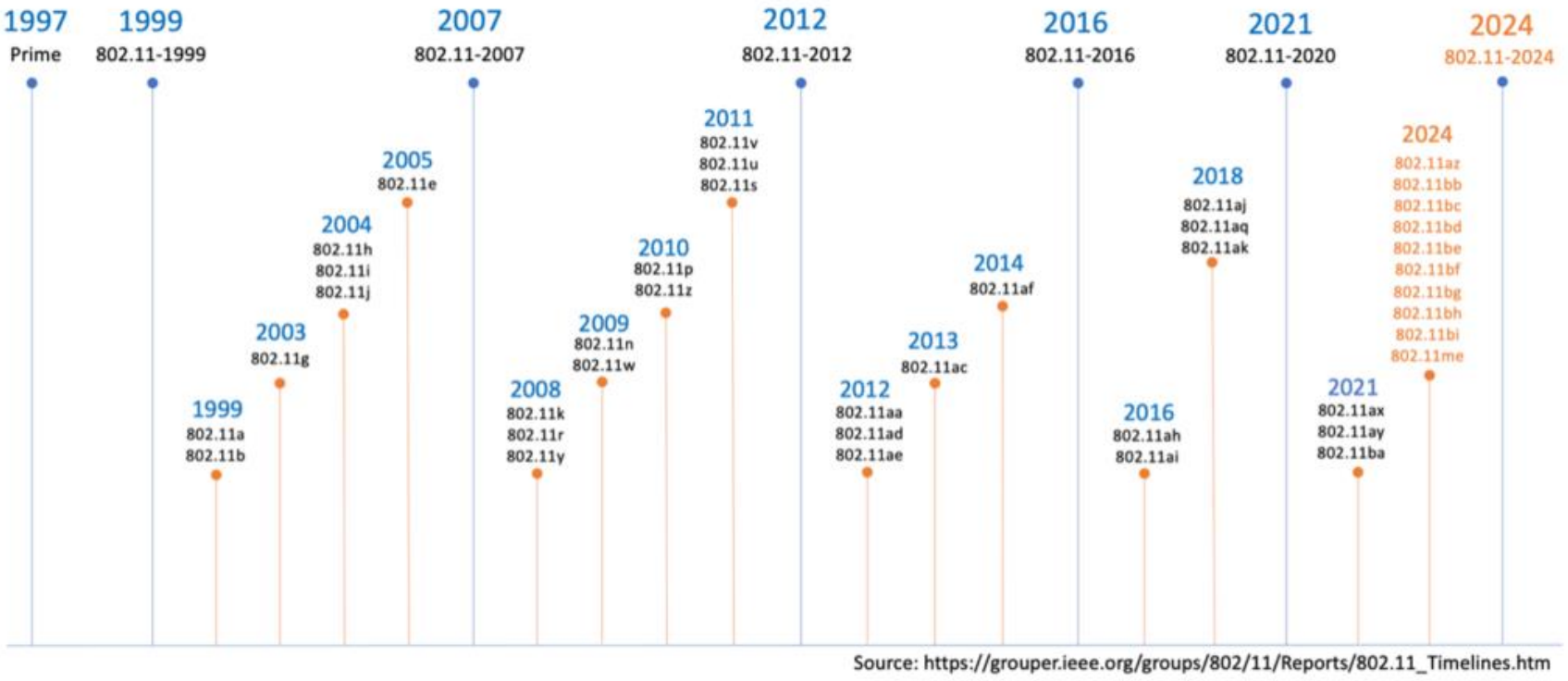
Module 6: Advanced WiFi Use Cases		
Week 5	***Session6a: WLAN AP/Controller Architectures*** *Thick AP, Thin AP models, Physical Controller, Cloud Controller*	Slides | Video | Quiz | Q&A | Notes
Week 6	***Session6b: Smart WiFi Features*** *Traffic Shaping/Policing, Parental Controls, Advanced Analytics, AI/ML*	Slides | Video | Quiz | Q&A | Notes
Week 7	***Session6c: WiFi Mesh Networks*** *Mesh Topologies, Various deployment models, Mesh Access/Backhaul/Roaming*	Slides | Video | Quiz | Q&A | Notes
Week 8	***Session6d: WiFi Monetization*** *Location Based Analytics, WiFi Sensing, Information Technology to Operational Technology*	Slides | Video | Quiz | Q&A | Notes

Module7: Basic Troubleshooting and Tools		
Week 9	***Session7a: Wireshark Capture Analysis*** *Wireshark WLAN filters, Radio tap headers, Information Element Analysis, I/O Charts*	Slides | Video | Quiz | Q&A | Notes
Week 10	***Session7b: Basic test/debug/spectrum analysis tools*** *iPerf, Ping, WiFi scanner tools, Kali Linux tools, Site Survey/Planning Tools, Heatmapping Tools*	Slides | Video | Quiz | Q&A | Notes
Week 11	***Session7c: Suppliant logs, AP logs, basic debug commands*** *APIs and Interfaces to AP config, Serial/Telnet/restAPIs, Supplicant and AP debug logs*	Slides | Video | Quiz | Q&A | Notes
Week 12	***Session7d: OpenWRT Basics*** *Basic overview and building blocks of OpenWRT project*	Slides | Video | Quiz | Q&A | Notes

Module8: WiFi Lab Testing		
Week 13	***Session8a: WiFi Testing Fundamentals*** *Basics of various approaches for WiFi testing, Lab/Field, Automation/Manual etc..*	Slides | Video | Quiz | Q&A | Notes
Week 14	***Session8b: Testing in the Lab*** *Benchmarking, Scale/Stress Testing, Repeatability/Automation*	Slides | Video | Quiz | Q&A | Notes
Week 15	***Session8c: Testing in Test Houses*** *Testing approach for testing in real houses/enterprise environments, testing challenges and solutions*	Slides | Video | Quiz | Q&A | Notes
Week 16	***Session8d: Testplan Development*** *Basics of how to develop testplans, execute them, use various engineering tools*	Slides | Video | Quiz | Q&A | Notes

IEEE 802.11 Standards

- **IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997**
- **IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)**
- **IEEE 802.11b: 5.5 Mbit/s and 11 Mbit/s, 2.4 GHz standard (1999)**
- **IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)**
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)
- **IEEE 802.11n: Higher Throughput WLAN at 2.4 and 5 GHz; 20 and 40 MHz channels; introduces MIMO to Wi-Fi (September 2009)**
- IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y, and z (March 2012)
- **IEEE 802.11ac: Very High Throughput WLAN at 5 GHz[e]; wider channels (80 and 160 MHz); Multi-user MIMO (down-link only)(Dec 2013)**
- IEEE 802.11-2016: A new release of the standard that includes amendments aa, ac, ad, ae, and af (December 2016)
- IEEE 802.11-2020: A new release of the standard that includes amendments ah, ai, aj, ak, and aq (December 2020)
- **IEEE 802.11ax: High Efficiency WLAN at 2.4, 5 and 6 GHz; introduces OFDMA to Wi-Fi (February 2021)**
- **IEEE 802.11be: Extr**

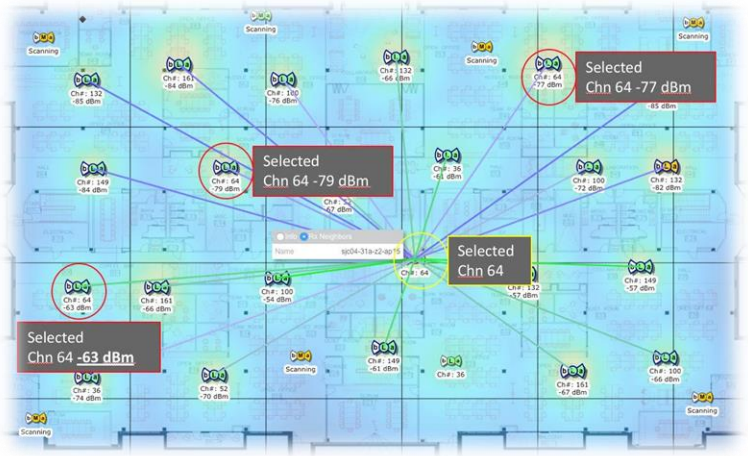


802.11 Standard Extensions

- IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997
- IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b: 5.5 Mbit/s and 11 Mbit/s, 2.4 GHz standard (1999)
- IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d: International (country-to-country) roaming extensions (2001)
- **IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)**
- IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- **IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)**
- **IEEE 802.11i: Enhanced security (2004)**
- IEEE 802.11j: Extensions for Japan (4.9-5.0 GHz) (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)
- **IEEE 802.11k: Radio resource measurement enhancements (2008)**
- IEEE 802.11n: Higher Throughput WLAN at 2.4 and 5 GHz; 20 and 40 MHz channels; introduces MIMO to Wi-Fi (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- **IEEE 802.11r: Fast BSS transition (FT) (2008)**
- **IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)**
- IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled
- **IEEE 802.11u: Improvements related to HotSpots and 3rd-party authorization of clients, e.g., cellular network offload (February 2011)**
- **IEEE 802.11v: Wireless network management (February 2011)**
- **IEEE 802.11w: Protected Management Frames (September 2009)**
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)

Source : Wikipedia

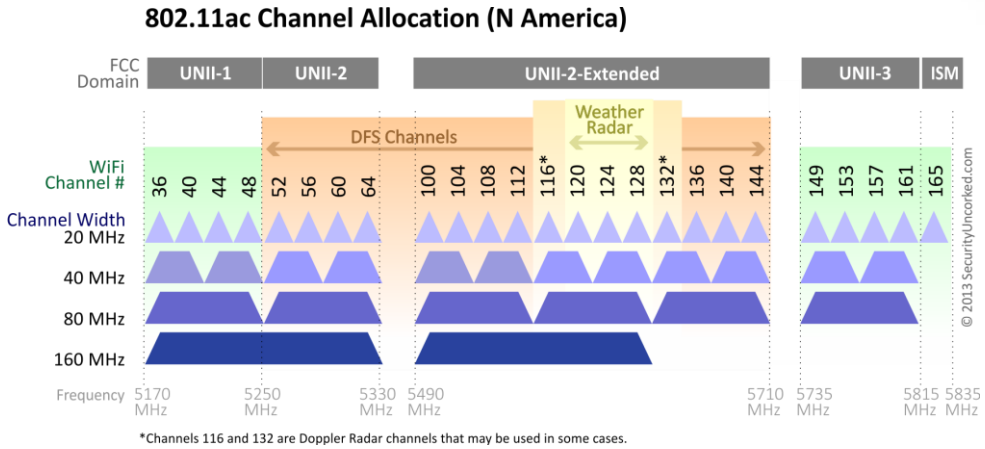
Challenges from Large Scale Wi-Fi Adoption in the Enterprise



High Density Deployments

The Frequency Reuse problem

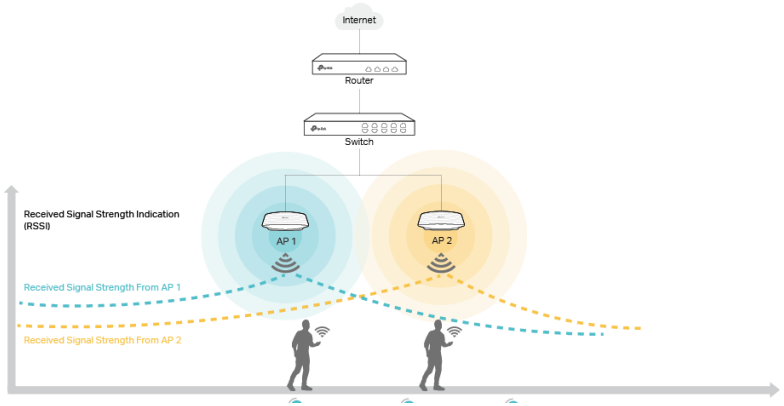
802.11k – Radios Resource Management



Need for more channels in 5GHz

The DFS problem

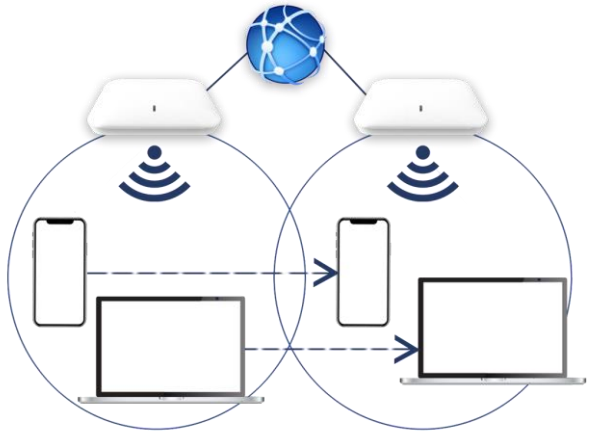
802.11h – DFS and TPC



Mobility when using delay sensitive applications on secure networks

The fast and secure roaming problem

802.11r – Fast Roaming



Lack of Proper network management from STAs

The need for network assisted handoff

802.11v – Wireless network management

Dynamic Frequency Selection (DFS)

- DFS is a channel allocation scheme that dynamically selects and/or changes the operating frequency to avoid interfering with other systems.
- Unlicensed wireless networking systems (e.g. 802.11a/n) using the 5250-5350 MHz and/or 5470-5725 MHz bands cannot interfere with radar systems.
- A system implementing DFS needs to be capable of avoiding interfering with radar systems by
  - Verifying a channel is free of radar before using it .
  - Monitoring for radar once a channel is in use and vacating the channel if radar is detected.
  - Remaining off of a “radar” channel once radar has been detected .

- **Channel Availability Check Time**: The time a system shall monitor a channel for presence of radar prior to initiating a communications link on that channel.
- **Interference Detection Threshold**: The minimum signal level, assuming a 0dBi antenna, that can be detected by the system to trigger the move to another channel.
- **Channel Move Time**: The time for the system to clear the channel and measured from the end of the radar burst to the end of the final transmission on the channel.
- **Channel Closing Transmission Time**: The total, or aggregate, transmission time from the system during the channel move time.
- **Non-Occupancy Time**: A period of time after radar is detected on a channel that the channel may not be used.

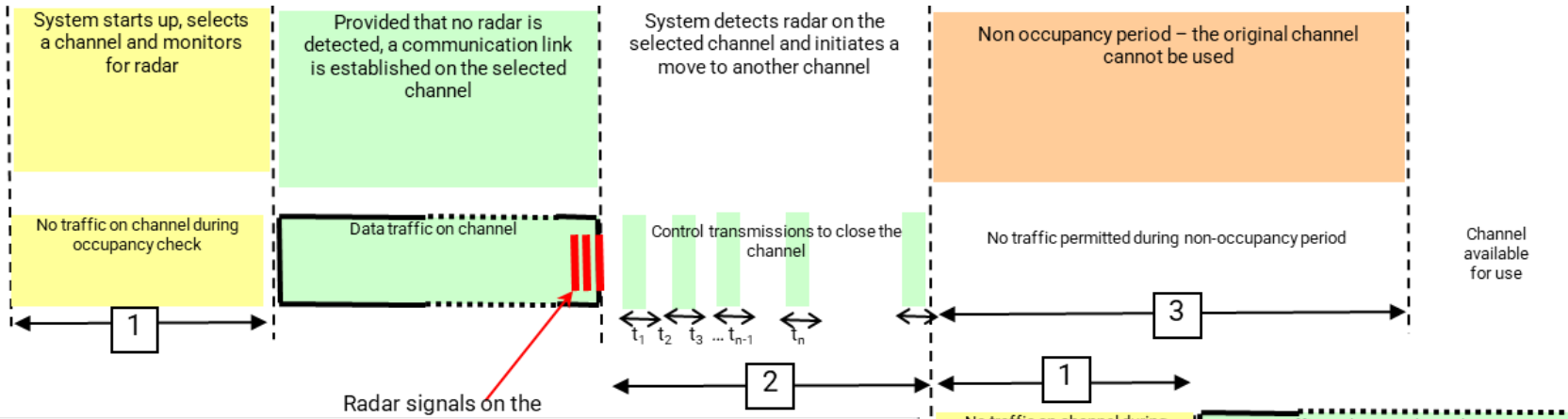
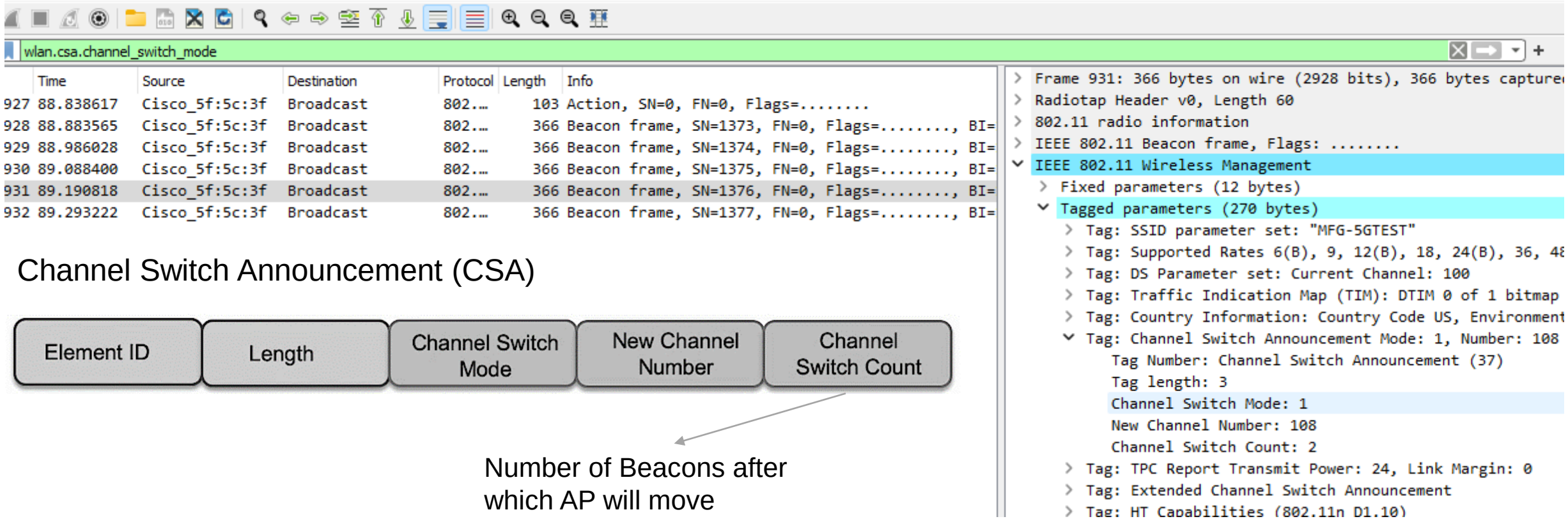


Table 2 EN 301 893 DFS Requirements

Parameter	Requirement
Minimum channel availability check time (CAC time)	60s outside 5600-5650 MHz 10 minutes for 5600-5650MHz sub-band
Off-channel channel availability check time	Up to 4 hours outside 5600-5650 MHz Up to 24 hours for 5600-5650MHz sub-band
Channel Move time	10s (maximum)
Channel Closing Time	1s (maximum)
Interference Detection Threshold	DFS Detection Threshold (dBm) = -62 + 10 - EIRP Spectral Density (dBm/MHz) + G (dBi) Shall not be lower than -64 dBm assuming a 0 dBi receive antenna gain.
Non-occupancy period	30 minutes (minimum)
Note – Client devices do not need radar detection capabilities unless they have an output power (eirp) that exceeds 200mW. All devices need to demonstrate compliance with the channel move and channel closing times.	

DFS Implementation

- **AP Behavior**
  - APs should be able to detect the different types of Radar pulses and send a Channel Switch Announcement (CSA) before moving to a new channel.
  - The CSA is usually sent in the Beacon frames and special CSA Action frames and it contains information about the new channel to which the AP is going to move to, so that the clients can follow the AP to the new channel.
- **Client Behavior**
  - Active scanning isn't allowed on DFS channels unless client hears AP beaconing
  - Client may choose to stay connected with the AP upon receiving CSA or choose to move to a new BSS



Channel Switch Announcement (CSA)

Number of Beacons after which AP will move

DFS Certification

TÜVRheinland®
Precisely Right.

Dynamic Frequency Selection Test Report

EUT Name: eero 6 and eero 6 Extender

Model No.: N010001 and Q010001

CFR 47 Part 15.407(h) 2020, RSS-247 (6.3) 2017 and KDB 905462 D02 UNII DFS Compliance Procedures New Rules v02

Prepared for:

eero LLC
660 3rd Street
San Francisco, CA 94107 U.S.A.

Prepared by:

TUV Rheinland of North America, Inc.
1279 Quarry Lane, Ste. A
Pleasanton, CA 94566
Tel: (925) 249-9123
Fax: (925) 249-9124
http://www.tuv.com/

Report/Issue Date: October 26, 2020
Report Number: 32063254.001
Job # 0234155861

1.3 Summary of Test Results

Table 1: Summary of Test Results for Master Device Mode

Requirements	Test Method KDB 905462	Description	Test Parameters	Measured Value	Result
20 MHz Bandwidth					
Detection Threshold	Sect. 7.8.1	EUT Min. Detection Level	-64 dBm ≥ 200 mW -62 dBm <200 mW	-62.95 dBm	Complied
Detection Bandwidth	Sect. 7.8.1	U-NII Detection Bandwidth	Min 100% of 99% BW.	20 MHz (detected bandwidth)	Complied
Performance Requirements Check	Sect. 7.8.2.1	Initial Channel Check	CAC ≥ 60s	See 80 MHz BW test result	Complied
	Sect. 7.8.2.2	Burst Radar at the beginning	150s (2.5min)	See 80 MHz BW test result	Complied
	Sect. 7.8.2.3	Burst Radar at the End	150s (2.5min)	See 80 MHz BW test result	Complied
In-Service Monitoring	Sect. 7.8.3	Channel Moving Time	CMT ≤ 10s	See 80 MHz BW test result	Complied
		Channel Closing Time Transmission	200 ms + an agg. Of 60 ms over remaining 10s.	See 80 MHz BW test result	Complied
		Non-Occupancy Period	≥ 30 min.	See 80 MHz BW test result	Complied
Radar Statistic Performance Check	Sect. 7.8.4	Waveform 1 - 4 Detections	60% in 30 trials 80% of Aggregate	Type 1A – 100% Type 1B – 100% Type 2 – 80.0% Type 3 – 83.3% Type 4 – 93.3% Aggre.1- 4 – 89.2%	Complied
		Waveform 5 Detections	80% in 30 trials	Type 5 – 96.7%	
		Waveform 6 Detections	70% in 30 trials	Type 6 – 100%	
Transmit Power Control	CFR47 15.407 (h)(1)		6 dB below 30 dBm EIRP or less than 500 mW.	Manufacturer's Statement	Complied
Uniform Spreading	CFR47 15.407 (h)(2)		Manufacturer's Statement		Complied

The detection probability Test aims to check if an AP can detect the RADAR pulses which are generated on the active channel of the AP. RADAR pulses will be generated based on different parameters like pulse width, number of pulses and Pulse Repeating Interval. For a given test case, certain number of trials must be conducted to see if AP detects RADAR. The parameters of pulses might vary for every trial based on the type of RADAR pulse being tested. The detection percentage of RADAR must be greater than or equal to the specified value by the respective governing bodies.

The detection bandwidth test will measure the range of frequencies in which the device can detect radar signals. Radar signals are injected in 1 step increments of 1 MHz in both the directions starting from the Centre frequency, this process is done until the DUT fails to detect the signal. The Total range in between the upper frequency limit and lower frequency limit is called as the detection bandwidth.

Timing Tests

- Channel Availability Check Time.
- Interference Detection Threshold
- Channel Move Time
- Channel Closing Transmission Time
- Non-Occupancy Time

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

IEEE 802.11ac VHT80 + VHT80

Table 1: Short Pulse Radar Test Waveforms.

Radar Type	Pulse Width (μsec)	PRI (μsec)	Number of Pulses	Number of Trials(Times)	Percentage of Successful Detection (%)
1	1	Test A: 15 unique PRI values randomly selected from the list of 23 PRI values in Table 5a	Roundup $\left\{\left(\frac{1}{360}\right)\cdot\left(\frac{19\cdot 10^6}{PRI_{\mu sec}}\right)\right\}$	30	93.3%
		Test B: 15 unique PRI values randomly selected within the range of 518-3066 μ sec, with a minimum increment of 1 μ sec, excluding PRI values selected in Test A			
2	1-5	150-230	23-29	30	90%
3	6-10	200-500	16-18	30	93.3%
4	11-20	200-500	12-16	30	90%
Aggregate (Radar Types 1-4)				120	91.65%

Table 2: Long Pulse Radar Test Waveform

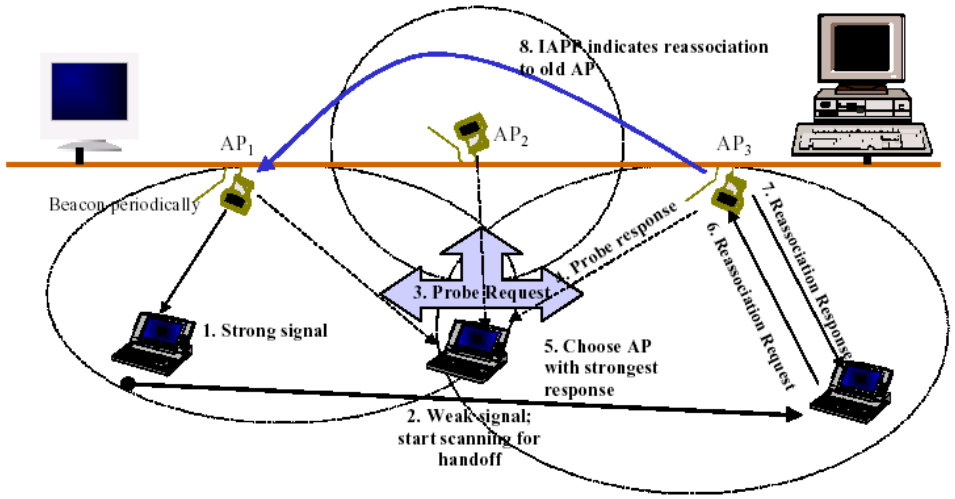
Radar Type	Pulse Width (μsec)	Chirp Width (MHz)	PRI (μsec)	Number of Pulses per Burst	Number of Bursts	Number of Trials(Times)	Percentage of Successful Detection (%)
5	50-100	5-20	1000-2000	1-3	8-20	30	90%

Table 3: Frequency Hopping Radar Test Waveform

Radar Type	Pulse Width (μsec)	PRI (μsec)	Pulses per Hop	Hopping Rate (kHz)	Hopping Sequence Length (msec)	Number of Trials(Times)	Percentage of Successful Detection (%)
6	1	333	9	0.333	300	30	100%

Traditional WLAN Roaming

- Roaming can be defined as the client moving between APs advertising the same or similar wireless network
- Since the WLAN clients are mobile and coverage range of a single AP is limited, roaming happens whenever the client passes the boundaries of a WLAN cell
- The roaming protocol should be implemented effectively in order to cause very minimal delays during the handoff
- The clients usually make the roaming decisions by scanning the various available wireless networks at all times and trying to connect to the best available network
- Decision to roam can be made on various factors such as RSSI, number of missed beacons, SNR, frame errors, etc.
- When a decision is made to roam the client can authenticate and associate with the new AP and continue its data communication through the new AP
- Roaming when security is enabled would involve setting up a new security session with the new AP



Last Data packet on AP1 14.09 secs

Perform 802.11 connection with AP2 starting at 14.22 secs

Start Data Transfer on AP2 at 14.24 seconds. Roaming delay is approximately 13 msecs

No	Time	Delta Time	PHY Rate	Source	Destination	Protocol	Info
14.094649	14.090.007465	1.0		Cisco_fa:ab:e1	Broadcast	IEEE 802	Beacon f
14.097093	14.090.002444	54.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.097173	14.090.000080	24.0			Cisco_fa:ab:e2	IEEE 802	Acknowle
14.107089	14.100.009916	54.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.107795	14.100.000706	54.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.108509	14.100.000714	48.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.109407	14.100.000898	36.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.110114	14.110.000707	24.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.110637	14.110.000523	18.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.111314	14.110.000677	12.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.112028	14.110.000714	11.0		172.16.86.171	172.16.138.65	TFTP	Unknown
14.113262	14.110.001234	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.114175	14.110.000913	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.114989	14.110.000814	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.115500	14.110.000511	54.0		Intel_d4:b3:b1	Cisco_fa:ab:e2	IEEE 802	Null fur
14.115542	14.110.000042	24.0			Intel_d4:b3:b1	IEEE 802	Acknowle
14.116216	14.110.000674	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.117309	14.110.001093	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.118276	14.110.000967	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.119226	14.110.000950	1.0		Cisco_fa:ab:e2	Broadcast	IEEE 802	Beacon f
14.121213	14.120.001987	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.121937	14.120.000724	1.0		Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.122378	14.120.000441	54.0		Intel_d4:b3:b1	Cisco_fa:ab:e2	IEEE 802	Null fur
14.122420	14.120.000042	24.0			Intel_d4:b3:b1	IEEE 802	Acknowle
14.131519	14.130.009099	1.0		Cisco_fa:ab:e4	Broadcast	IEEE 802	Beacon f
14.143806	14.140.012287	1.0		Cisco_fa:ab:e0	Broadcast	IEEE 802	Beacon f
14.197055	14.190.053249	1.0		Cisco_fa:ab:e1	Broadcast	IEEE 802	Beacon f
14.217181	14.210.020126	54.0		98:d1:50:27:a8	Cisco_fa:ab:e2	IEEE 802	Null fur
14.217225	14.210.000044	24.0			Intel_d4:b3:b1	IEEE 802	Acknowle
14.217805	14.210.000580	54.0		172.16.50.245	172.16.63.215	ICMP	Echo (p
14.217860	14.210.000055	24.0			Cisco_fa:ab:e2	IEEE 802	Acknowle
14.218919	14.210.001059	54.0		154.16.63.215	172.16.50.245	IP	Fragment
14.218970	14.210.000051	24.0			Intel_d4:b3:b1	IEEE 802	Acknowle
14.221631	14.220.002661	1.0		Cisco_fa:ab:e2	Broadcast	IEEE 802	Beacon f
14.233916	14.230.012285	1.0		Cisco_fa:ab:e4	Broadcast	IEEE 802	Beacon f
14.246204	14.240.012288	1.0		Cisco_fa:ab:e0	Broadcast	IEEE 802	Beacon f
14.299454	14.290.053250	1.0		Cisco_fa:ab:e1	Broadcast	IEEE 802	Beacon f
14.324030	14.320.024576	1.0		Cisco_fa:ab:e2	Broadcast	IEEE 802	Beacon f

AP1 Capture

Time	Delta Time	PHY Rate	Source	Destination	Protocol	Info
14.22486	0.015482	24.0	AbbottDi_0	Cisco_fb:27:12	IEEE 802	Probe Request, SN=0,
14.22491	0.000055	24.0		AbbottDi_01:00	IEEE 802	Acknowledgement, Flag
14.22499	0.000081	1.0	Cisco_fb:2	AbbottDi_01:00	IEEE 802	Probe Response, SN=37
14.22666	0.001666	1.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.22775	0.001091	24.0	AbbottDi_0	Cisco_fb:27:12	IEEE 802	Authentication, SN=1,
14.22780	0.000051	24.0		AbbottDi_01:00	IEEE 802	Acknowledgement, Flag
14.22818	0.000373	11.0	Cisco_fb:2	AbbottDi_01:00	IEEE 802	Authentication, SN=37
14.22840	0.000227	11.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.22976	0.001353	24.0	AbbottDi_0	Cisco_fb:27:12	IEEE 802	Association Request,
14.22981	0.000059	24.0		AbbottDi_01:00	IEEE 802	Acknowledgement, Flag
14.23119	0.001371	11.0	Cisco_fb:2	AbbottDi_01:00	IEEE 802	Association Response,
14.23142	0.000239	11.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.23396	0.002532	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=3703
14.24016	0.006200	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.24024	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.24625	0.006009	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=3705
14.25012	0.003875	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.25020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.25853	0.008333	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=3707
14.26054	0.002008	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.26062	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.27014	0.009516	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.27022	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.28012	0.009905	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.28020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.29211	0.011906	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.29219	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.30012	0.007936	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.30020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.31012	0.009917	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.31020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.31178	0.001581	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=3714
14.32012	0.008335	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.32020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.33012	0.009922	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)
14.33020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.33636	0.006156	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=3717
14.34012	0.003767	54.0	172.16.86.1	172.16.138.65	TFTP	Unknown (0xdd01)

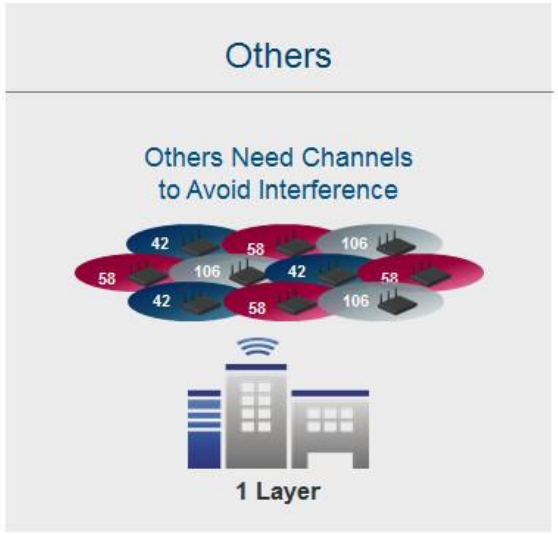
AP2 Capture

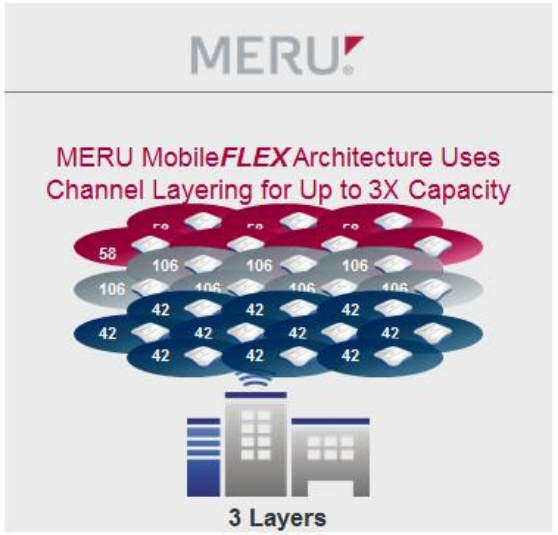
Evolution of Roaming Enhancements

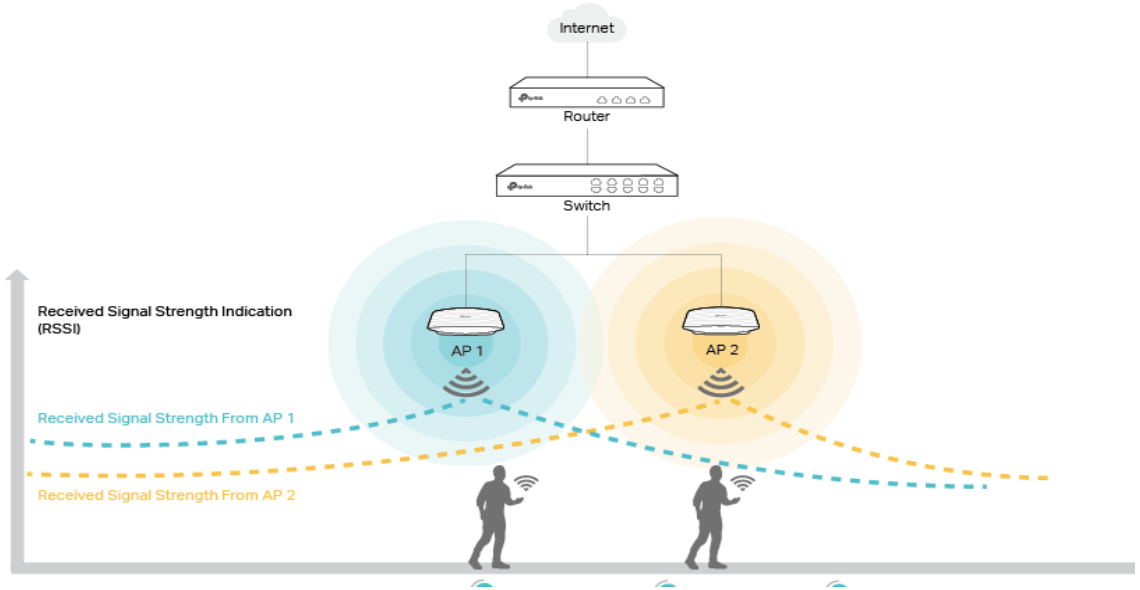
- Initial Solutions from Industry
  - Cisco CCX
  - Opportunistic Key Caching, Cisco CCKM
  - Meru Single Channel Implementations

- 802.11 Standard Extensions
  - 802.11e – QBSS Load Element
  - 802.11f – IAPP (Deprecated)
  - 802.11i - Security Enhancements
  - 802.11u - Internetworking with external networks
  - 802.11k – Radio Resource Management
  - 802.11v – Network Management
  - 802.11r – Fast Roaming

- Enhancement Goals
  - Support delay sensitive/real time applications
  - Avoid session disconnections
  - Reduce packet loss/Latency







802.11k – The basic concept

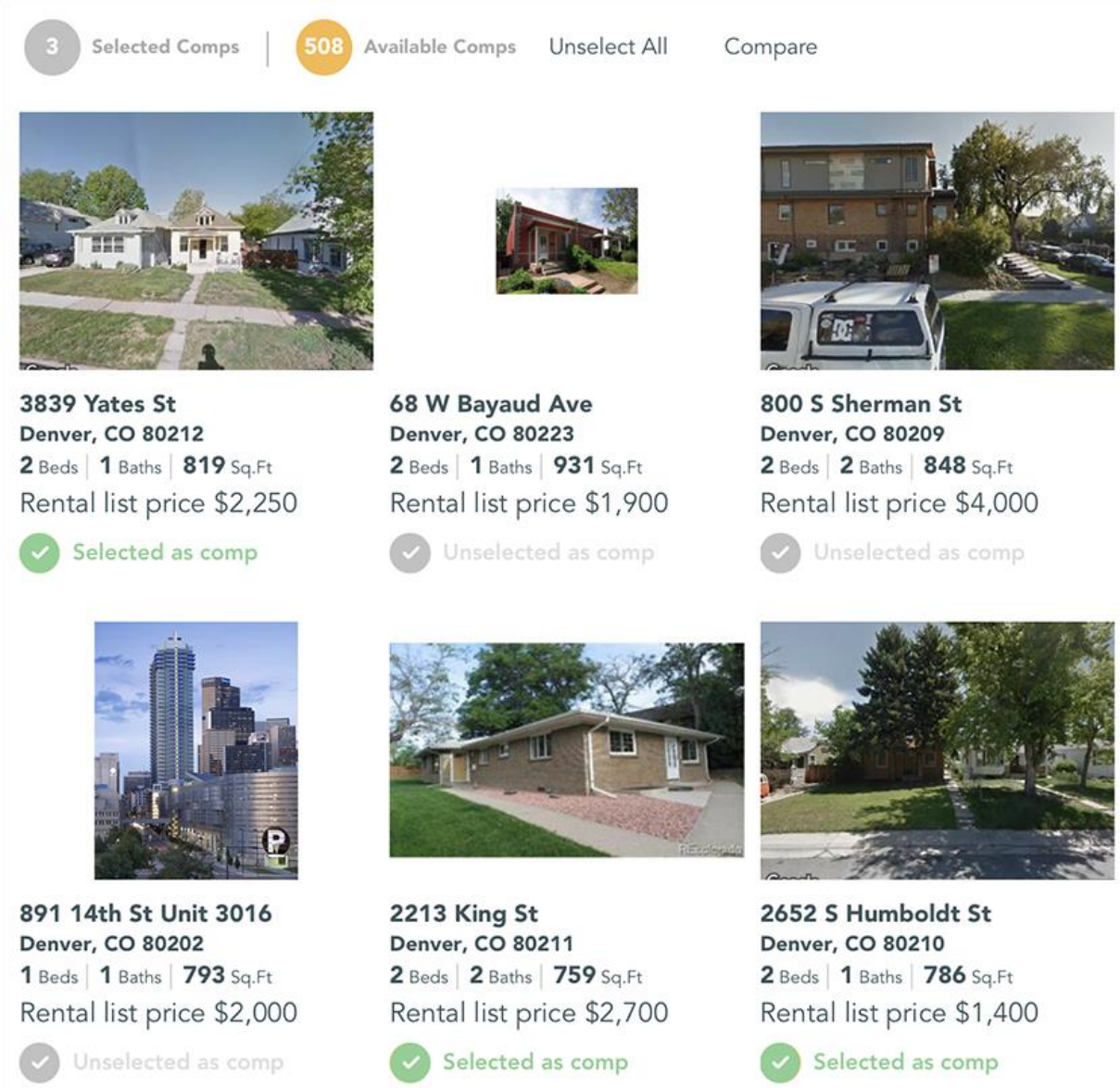
- Need to move to a new rental home?
- Want to check out for better rental options?

The not so efficient method:

- Go on the road and check every home in the neighborhood to see if its available for rent.
- Talk to all open house owners and make a list of potential rentals.
- Then shortlist and select.

The better method:

- Go to a rental agency website from the convenience of your home and ask for a list of all the homes available for rent.
- Check the list along with the details of each home and from that shortlist the home you want and then approach the owner and rent it.

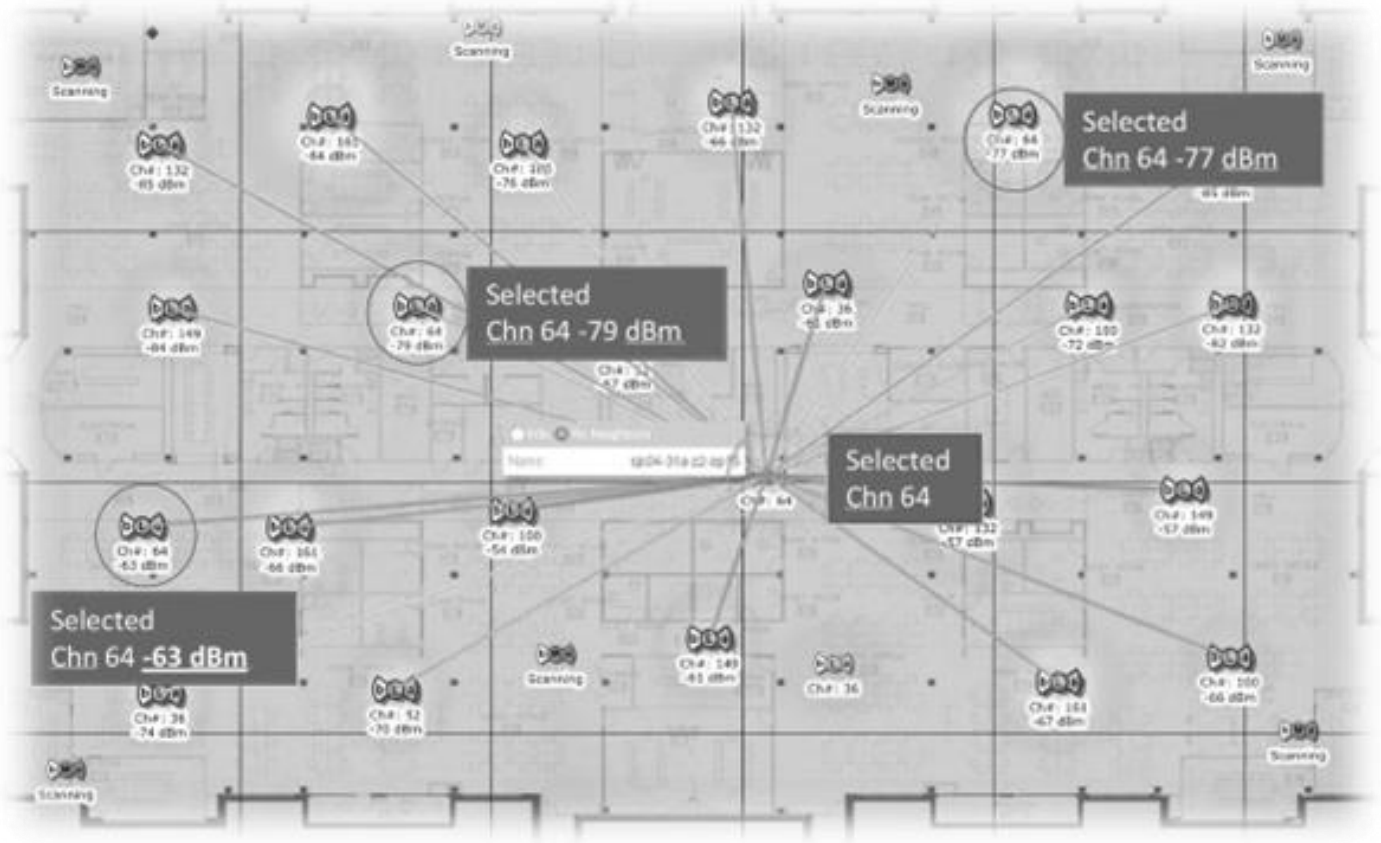


802.11k – The full RRM scope

- Simplify and/or automate WLAN radio configuration
- Achieve better performance in dense BSS deployments
- Better utilize radio resources across client stations
- Alert WLAN administrator to problems
- Notify client station users of current radio status
- Vendors use measurements to add value

The request/response measurements are:

- Beacon
- Frame
- Channel Load
- Noise Histogram
- STA Statistics
- Location Configuration Information
- **Neighbor Report**
- Link Measurement

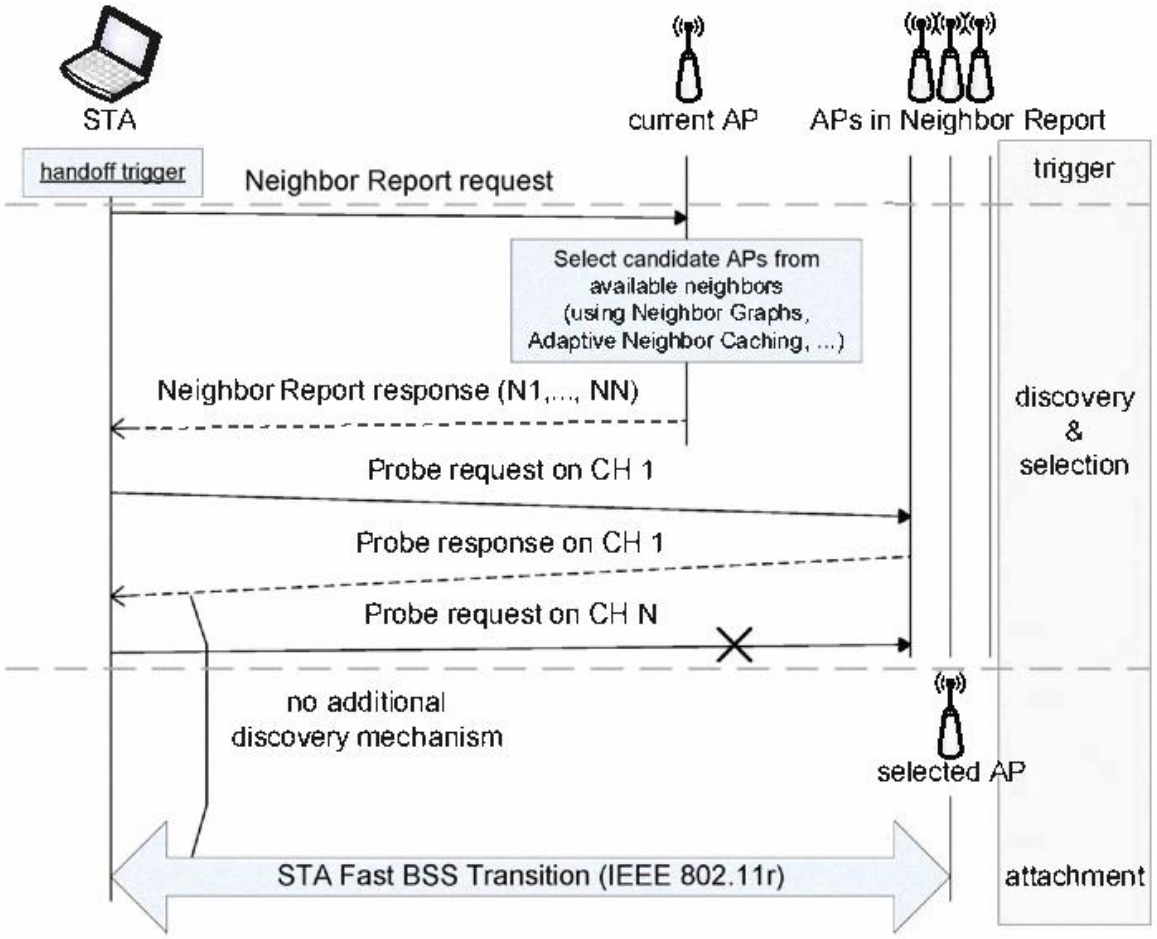


802.11k – Neighbor Report Request/Response

- When the client wants to find a better network to connect to, it sends its current AP a Neighbor report request frame.
- The current AP then sends a neighbor report response that will contain a list of all the candidate neighboring APs along with their capabilities.
- The client can then select from the list the AP it wants to connect to and then send go through the connection process with the new AP.

How it helps:

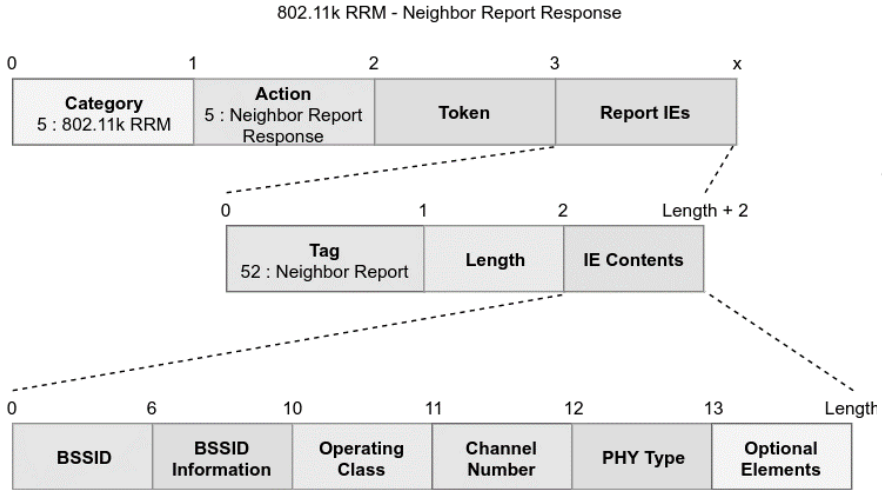
- Always finding the best network available to connect
- Making the search for a new AP much easier when its time to roam.
- Removes the need for moving off the current channel to find other networks.
- Much more efficient usage of the medium by reducing the amount of on air frames.



Neighbor Request/Response Frames

Neighbor Report Response Information Elements

- **BSSID**: MAC address of the target AP
- **BSSID Info**: Capabilities of the target AP
- **Operating Class**: Channel Set of the AP based on operating country
- **Channel Number**: Channel of target AP.
- **PHY Type**: PHY details of the target AP.
- **Sub elements**: Other vendor specific elements



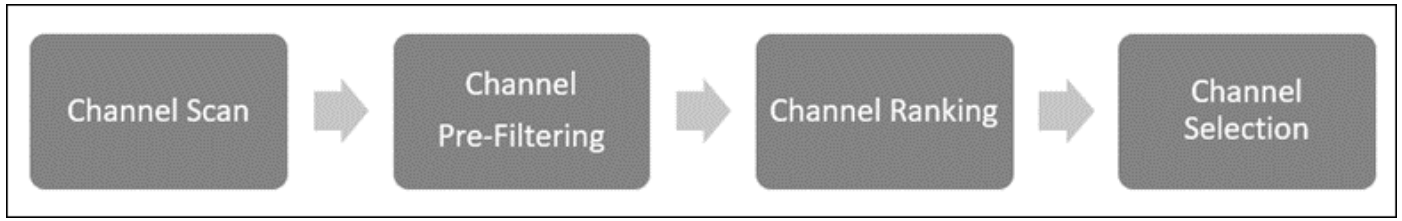

```
Frame 23968: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)
802.11 radio information
IEEE 802.11 Action, Flags: ........C
  Type/Subtype: Action (0x000d)
  Frame Control Field: 0xd000
  .000 0000 0010 1100 = Duration: 44 microseconds
  Receiver address: Cisco_6e:b7:ab
  Destination address: Cisco_6e:b7:ab
  Transmitter address: Aruba_35:90:56
  Source address: Aruba_35:90:56
  BSS Id: Cisco_6e:b7:ab
  .... .... .... 0000 = Fragment number: 0
  0000 0101 0000 .... = Sequence number: 80
  Frame check sequence: 0xdfad5504 [correct]
  [FCS Status: Good]
IEEE 802.11 wireless LAN
  Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Request (4)
    Dialog token: 0
  Tagged parameters (7 bytes)
    Tag: SSID parameter set: Ruckus
      Tag Number: SSID parameter set (0)
      Tag length: 5
      SSID: Ruckus
```

```
Frame 23970: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
802.11 radio information
IEEE 802.11 Action, Flags: ........C
  Type/Subtype: Action (0x000d)
  Frame Control Field: 0xd000
  .000 0000 0010 1100 = Duration: 44 microseconds
  Receiver address: Aruba_35:90:56
  Destination address: Aruba_35:90:56
  Transmitter address: Cisco_6e:b7:ab
  Source address: Cisco_6e:b7:ab
  BSS Id: Cisco_6e:b7:ab
  .... .... .... 0000 = Fragment number: 0
  1100 1011 0100 .... = Sequence number: 3252
  Frame check sequence: 0x1388d80c [correct]
  [FCS Status: Good]
IEEE 802.11 wireless LAN
  Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Response (5)
    Dialog token: 0
  agged parameters (91 bytes)
    Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_aa:81:ab
      BSSID Information: 0x000002f7
      Operating Class: 0
      Channel Number: 48 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_a7:07:0b
      BSSID Information: 0x000002f7
      Operating Class: 0
      Channel Number: 36 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_0c:b9:bb
      BSSID Information: 0x000002f7
      Operating Class: 0
      Channel Number: 40 (iterative measurements on that Channel Number)
      PHY Type: 0x07
```

Auto Channel Selection for RRM (Proprietary Implementations)

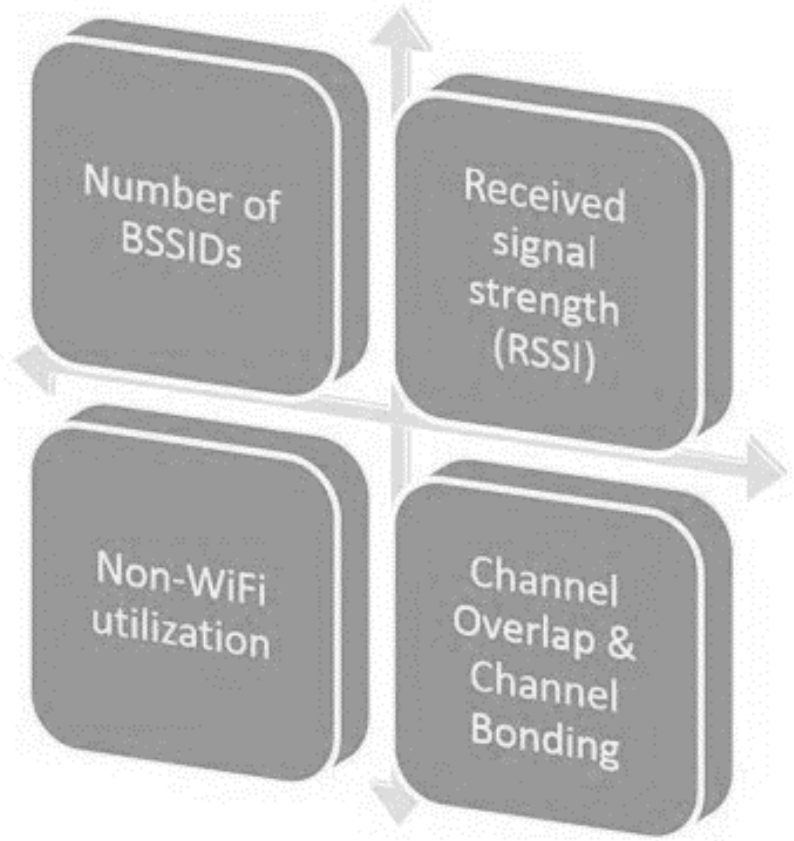
The objective of Auto Channel Selection (ACS) is to select, for each AP, an operating channel that minimizes interference from other APs and from non-Wi-Fi sources. Ways in which ACS is done:

•**Boot Time ACS** – Randomized boot interval to minimize the chance of neighbor APs selecting the same channel; and longer, more thorough channel scans to find the best channel
•**Periodic ACS** – The AP surveys its radio environment to find the best channel to change to and, if necessary, to select a new channel. The periodicity of ACS is configurable, the default being 12 hours.



Channel Scoring

- Each AP uses the Channel Scoring algorithm to rank all the channels scanned, and uses this ranking in its new channel selection.
- Each channel score depends on:
  - Number of BSSIDs already on that channel
  - The RSSI seen from all the networks on that channel
  - Non- WiFi medium utilization
  - If the channel is currently primary of secondary channel for other APs.



802.11v – Wireless Network Management

802.11v is an amendment standard for wireless network management, which defines numerous enhancements, such as power saving, load balancing, and BSS transition management (BTM). It allows clients to exchange network information and always associate with the optimal AP, which prolongs clients' battery life and improves user experience.

BSS max idle period management	An AP can report the amount of time that it does not disassociate stations due to absence of frames received.	Power saving and AP resource management
BSS transition management	An AP indicates a set of preferred APs to a station for a transition or request it to reassociate with a given AP.	Load balance and handover enhancement
Channel usage	The AP recommends channels to a station for non-infrastructure networks.	Interference avoidance
Collocated interference reporting	A station can get information about interference level at another station, so its own transmissions minimize the effect of interference from other radios at the measuring station.	Interference avoidance
Diagnostic report	A station can question other stations on hardware, configuration, and capabilities to diagnose and solve problems in the network.	Resource management and troubleshooting
Directed multicast service (DMS)	A station can ask the AP to send group addressed frames addressed to it as unicast frames.	Multicast transmission
Event reporting	A station can request other stations to send a message upon certain events (e.g., transitions, security, log reports or link status).	Handover, troubleshooting, resource management
Flexible multicast service (FMS)	A station can request to receive group addressed frames at a different interval. Its implementation is optional.	Multicast transmission, power management
Location services	Location information can be requested by the stations (radio resource measurements) or provided by the AP.	Resource management
Multicast diagnostic reporting	A station can provide statistics of the multicast traffic received successfully.	Multicast transmission, resource management
Multiple BSSID capability	Several BSSIDs can use a single beacon or probe response frame to announce its capabilities. Its implementation is optional.	Resource management
Proxy ARP	An AP can indicate that a station will not receive ARP frames.	Power saving
QoS traffic capability	A station can announce its own ability to support QoS traffic of a given priority.	Resource management
SSID list	A station can request information from a list of SSIDs instead of sending several separate probe request frames.	Resource management
Triggered STA statistics	According to a predefined threshold, stations can generate a statistics report.	Resource management
TIM broadcast	A station can reduce the time that it is awake by receiving an indication of buffered traffic independent of the beacon frame. Its implementation is optional.	Power saving
Timing measurement	This service allows a station to have an accurate estimate of its own offset with respect to another station's clock.	Synchronization
Traffic filtering service	An AP, upon request by a station, can filter the traffic it sends to the station, discarding the traffic that does not match the imposed criteria.	Power saving, resource management
U-APSD coexistence	APs and stations can agree on the most likely interval to transmit data avoiding interference.	Interference avoidance, resource management, power saving
WNM-notification	Stations can notify to each other of a management event. The only event defined is firmware update notification.	Resource management
WNM-sleep mode	A station can notify the AP of the amount of time that it will be in sleep mode. Its implementation is optional.	Power saving, resource management

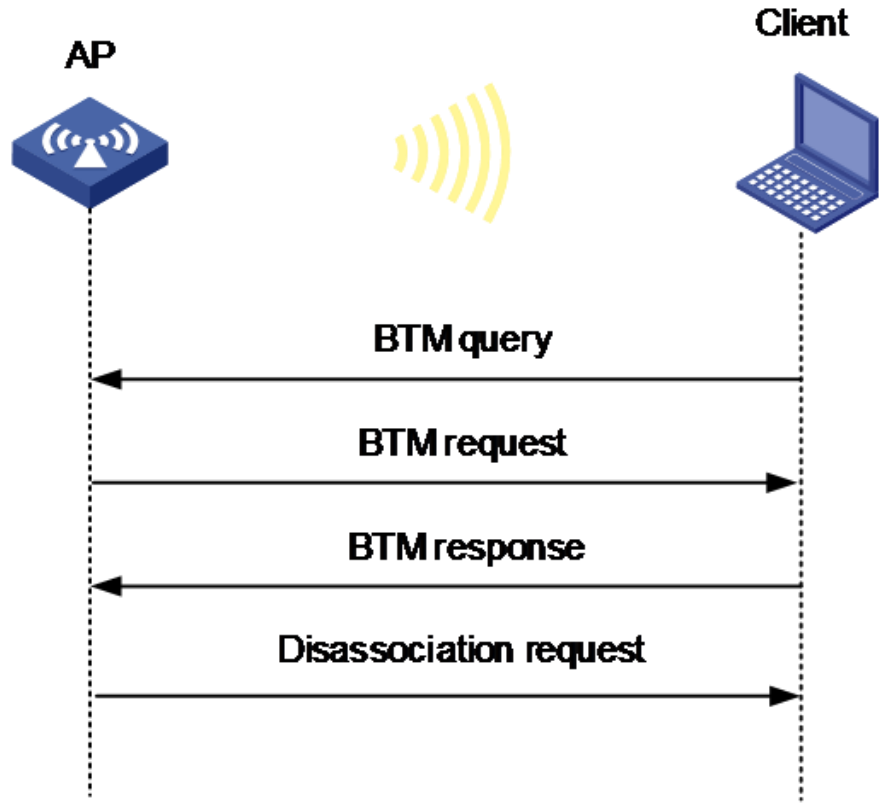
Only BSS transition management feature is used.

802.11v – BSS Transition Management

BSS transition management (BTM) enables clients to roam to the optimal AP if the signal strength of the current AP is low or if a better AP is discovered.

BTM operates as follows:

- The AP or the 802.11v client triggers a BSS transition:
  - **Unsolicited request**—If the AP detects that the RSSI of the client is lower than the RSSI threshold, it sends a BTM request to the client.
  - **Solicited request**—If the RSSI of the currently associated AP is too low or the client discovered a better AP, the client sends a BTM query to the associated AP. Upon receiving the query, the AP responds with a BTM request.
- A BTM request contains information about recommended BSSs.
- Upon receiving the BTM request, the client determines whether to disconnect from the current AP and roam to a recommended AP.
- If the client determines to perform a roaming, it sends a BTM response to the AP. If the client fails to leave the current BSS before the disassociation timer expires, the AP sends a disassociation request to the client and logs off the client.



BTM Request/Response

```
Tagged parameters (181 bytes)
  Tag: SSID parameter set: Test
  Tag: Supported Rates 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  Tag: Power Capability Min: 0, Max :11
  Tag: Supported Channels
  Tag: HT Capabilities (802.11n D1.10)
  Tag: RSN Information
  Tag: Mobility Domain
  Tag: RM Enabled Capabilities (5 octets)
  Tag: Extended Capabilities (8 octets)
    Tag Number: Extended Capabilities (127)
    Tag length: 8
    Extended Capabilities: 0x06 (octet 1)
      .... ...0 = 20/40 BSS Coexistence Management Support: Not supported
      .... ..1. = On-demand beacon: Supported
      .... .1.. = Extended Channel Switching: Supported
      .... 0... = WAVE indication: Not supported
      ...0 .... = PSMP Capability: Not supported
      ..0. .... = Reserved: 0x0
      .0.. .... = S-PSMP Support: Not supported
      0... .... = Event: Not supported
    Extended Capabilities: 0x00 (octet 2)
      .... ...0 = Diagnostics: Not supported
      .... ..0. = Multicast Diagnostics: Not supported
      .... .0.. = Location Tracking: Not supported
      .... 0... = FMS: Not supported
      ...0 .... = Proxy ARP Service: Not supported
      ..0. .... = Collocated Interference Reporting: Not supported
      .0.. .... = Civic Location: Not supported
      0... .... = Geospatial Location: Not supported
    Extended Capabilities: 0x88 (octet 3)
      .... ...0 = TFS: Not supported
      .... ..0. = WNM-Sleep Mode: Not supported
      .... .0.. = TIM Broadcast: Not supported
      .... 1... = BSS Transition: Supported
      ...0 .... = QoS Traffic Capability: Not supported
      ..0. .... = AC Station Count: Not supported
      .0.. .... = Multiple BSSID: Not supported
      1... .... = Timing Measurement: Supported
    Extended Capabilities: 0x80 (octet 4)
```

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Request (7)
    Dialog token: 0x07
    .... ...1 = Preferred Candidate List Included: 1
    .... ..0. = Abridged: 0
    .... .1.. = Disassociation Imminent: 1
    .... 0... = BSS Termination Included: 0
    ...0 .... = ESS Disassociation Imminent: 0
    Disassociation Timer: 1953
    Validity Interval: 200
    BSS Transition Candidate List Entries: 341074a02fb81e7df702000000240700000034108
```

```
0030  00 00 00 00 00 01 2e 33  96 20 18 40 2b 00 d0 00   .......3 . .@+...
0040  30 00 e4 b3 18 67 54 d0  88 1d fc 87 b8 bd 88 1d   0....gT. ........
0050  fc 87 b8 bd c0 9f 0a 07  07 05 a1 07 c8 34 10 74   ........ .....4.t
0060  a0 2f b8 1e 7d f7 02 00  00 00 24 07 00 00 00 34   ./..}... ..$....4
0070  10 88 1d fc 6a ba 0d f7  02 00 00 00 30 07 00 00   ....j... ....0...
0080  00 34 10 f0 7f 06 4d c6  7d f7 02 00 00 00 95 07   .4....M. }.......
0090  00 00 00 5b 8b 00 d2                               ...[...
```

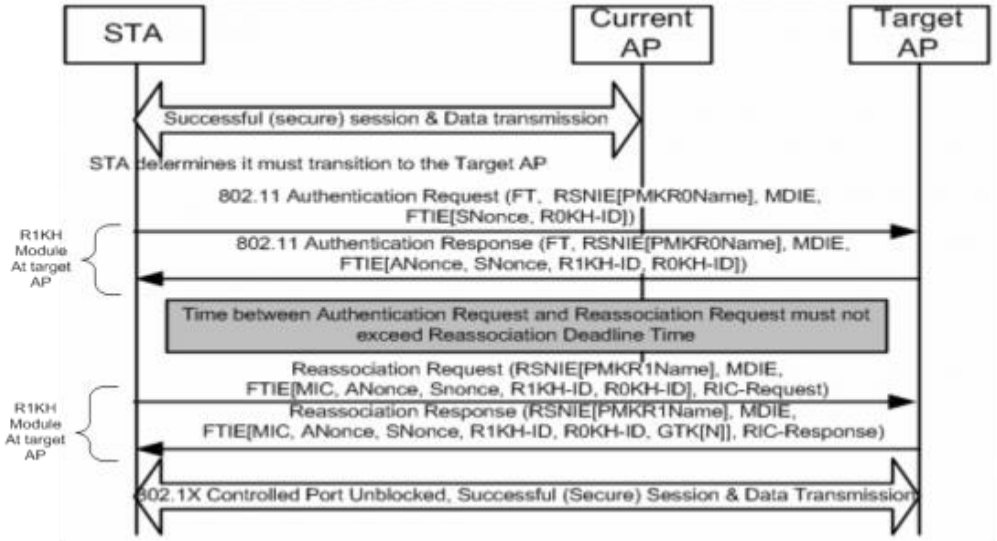
```
IEEE 802.11 wireless LAN management frame
  Fixed parameters
    Category code: WNM (10)
    Action code: BSS Transition Management Response (8)
    Dialog token: 0x07
    BSS Transition Status Code: 0
    BSS Termination Delay: 0
    BSS Transition Target BSS: CiscoInc_b8:1e:7d (74:a0:2f:b8:1e:7d)
```

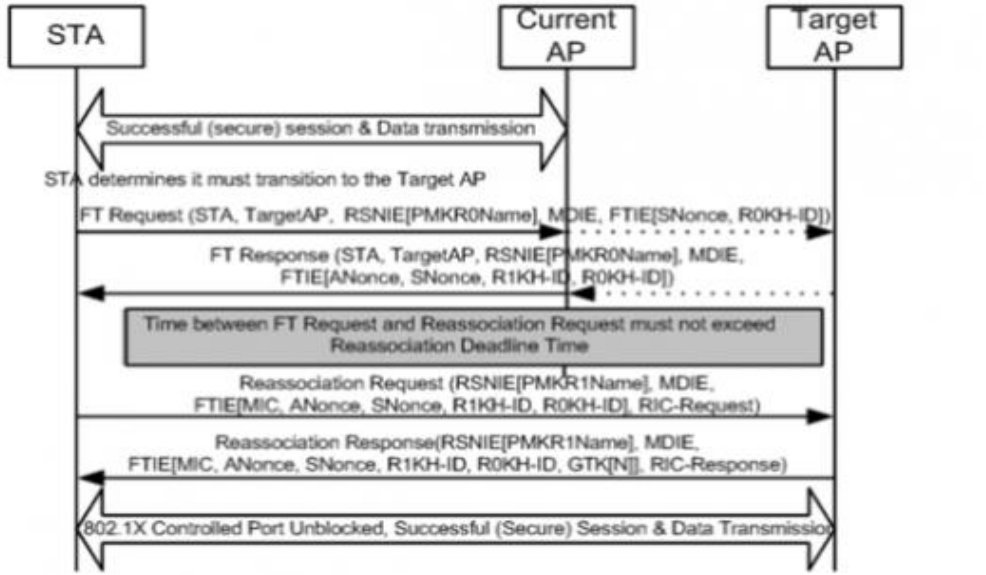
802.11r – Fast BSS Transition

IEEE 802.11r introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- **Over-the-Air**—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- **Over-the-DS**—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.





References

Dynamic Frequency Selection in Unlicensed Bands
https://nts.com/content/uploads/2017/12/6_Dynamic-Frequency-Selection-and-the-5GHz-Unlicensed-Band.pdf

Automatic and Dynamic Channel Selection
https://wifihelp.arista.com/post/automatic-and-dynamic-channel-selection

802.11k/v/r
https://www.youtube.com/watch?v=p_K9xHxFM8Y

Automatic and Dynamic Channel Selection
https://wifihelp.arista.com/post/automatic-and-dynamic-channel-selection


Q&A


?
QUIZ!
TIME