WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module 5: Advanced Features and Standard Extensions

Session 5a:

802.11 k/v/r, RRM, DFS, Fast Roaming

By

Rohini kaparapu

Nishtala kiranmai

Jami Harika

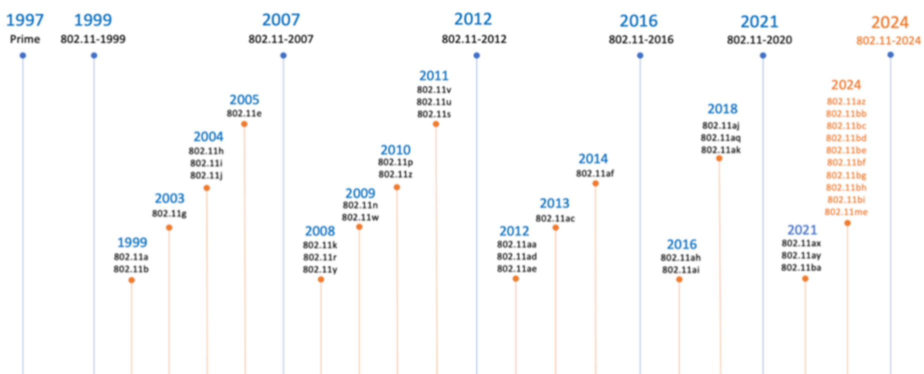
Shiny sayyad

Balla Deepika

Maddila Jaswanth

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: Extremely High Throughput (see also IEEE 802.11ax) (May 2024)**



Source: https://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

General Timeline:

- 1997: 802.11 (1/2 Mbps) - Basic standard for Wi-Fi.
- 1999: 802.11a (5 GHz) - Introduced higher frequency band for increased throughput.
- 2003: 802.11b/g (2.4 GHz) - Increased data rates and compatibility with earlier standards.
- 2009: 802.11n (MIMO) - Improved throughput and range with Multiple-Input Multiple-Output technology.
- 2013: 802.11ac (Wider channels) - Significantly increased speeds with wider channels and higher modulation schemes.
- 2016: 802.11ax (HE-Wi-Fi) - Improved efficiency and capacity for dense deployments.
- 2024: 802.11be (Extremely High Throughput) - Latest standard with further enhancements for speed and performance.

Key Milestones:

- QoS (802.11e): Prioritized traffic for real-time applications like voice and video calls.

- Security (802.11i): Enhanced security protocols like WPA and WPA2.
- Seamless Network Switching (802.11u): Improved roaming between access points for uninterrupted connectivity.
- DFS (Dynamic Frequency Selection): Utilizes radar-reserved channels while avoiding interference.

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

802.11e (QoS):

- Prioritizes traffic: Enables prioritization of different traffic types (voice, video, data) for smoother performance in real-time applications.
- Enhances user experience: Improves quality of service for delay-sensitive applications, especially in crowded networks.

802.11h (Spectrum and Transmit Power Management):

- Regulatory compliance: Ensures Wi-Fi devices adhere to European regulations for spectrum and power management.
- Reduces interference: Mitigates interference with other devices, such as radar systems and satellites.

802.11i (WPA/WPA2 Security):

- Stronger security: Addresses vulnerabilities in WEP encryption by introducing WPA and WPA2 for robust security in wireless networks.
- Essential for modern Wi-Fi: Widely adopted and considered a fundamental requirement for secure wireless communication.

802.11k (Radio Resource Management):

- Optimizes network performance: Facilitates efficient use of radio resources by providing information about network conditions and device capabilities.
- Improves roaming: Enhances handover between access points for seamless connectivity in large-scale deployments.

802.11r (Fast Roaming):

- Seamless transitions: Enables rapid and secure handoffs between access points, reducing delays and connection drops.
- Ideal for VoIP: Especially beneficial for voice over IP (VoIP) and other time-sensitive applications.

802.11s (Mesh Networking):

- Extended range: Expands Wi-Fi coverage by creating self-configuring, multi-hop wireless networks.
- Resilient connectivity: Provides alternative paths for data transmission, improving reliability in challenging environments.

802.11u (Interworking with External Networks):

- Seamless integration: Simplifies discovery and connection to external networks like cellular and public Wi-Fi hotspots.
- Enhanced user experience: Improves roaming and handover between different network types.

802.11v (Wireless Network Management):

- Efficient network administration: Enables remote configuration and management of devices for improved network efficiency and troubleshooting.
- Reduces maintenance costs: Streamlines network operations and reduces the need for manual interventions.

802.11w (Protected Management Frames):

- Enhanced security: Protects management frames from attacks, reducing vulnerabilities in network operations.
- Mitigates threats: Adds a layer of security to prevent unauthorized access and manipulation of network settings.

Challenges from Large-Scale Wi-Fi Adoption in the Enterprise:

1. High Density Deployments:

- Problem: Limited Spectrum and crowded Access Points (APs) lead to frequent channel reuse and interference.
- Impact: Reduced network performance, dropped connections, and sluggish user experience.
- Solution:
    - 802.11k Radio Resource Management (RRM): Optimizes channel selection and power control across APs for efficient resource utilization.
    - Careful Channel Planning: Strategies like dynamic frequency selection (DFS) and spatial reuse help minimize interference.

2. Need for more channels in 5GHz:

- Problem: Limited availability of channels in the popular 2.4 GHz band leads to congestion and performance issues.
- Impact: Similar to high density deployments, but potentially worse due to higher data rates in 5 GHz.
- Solution:
    - DFS (Dynamic Frequency Selection): Utilizes radar-reserved channels in 5 GHz while avoiding interference.
    - 802.11h DFS and Transmit Power Control (TPC): Ensures compliant operation with DFS regulations and optimizes power usage.

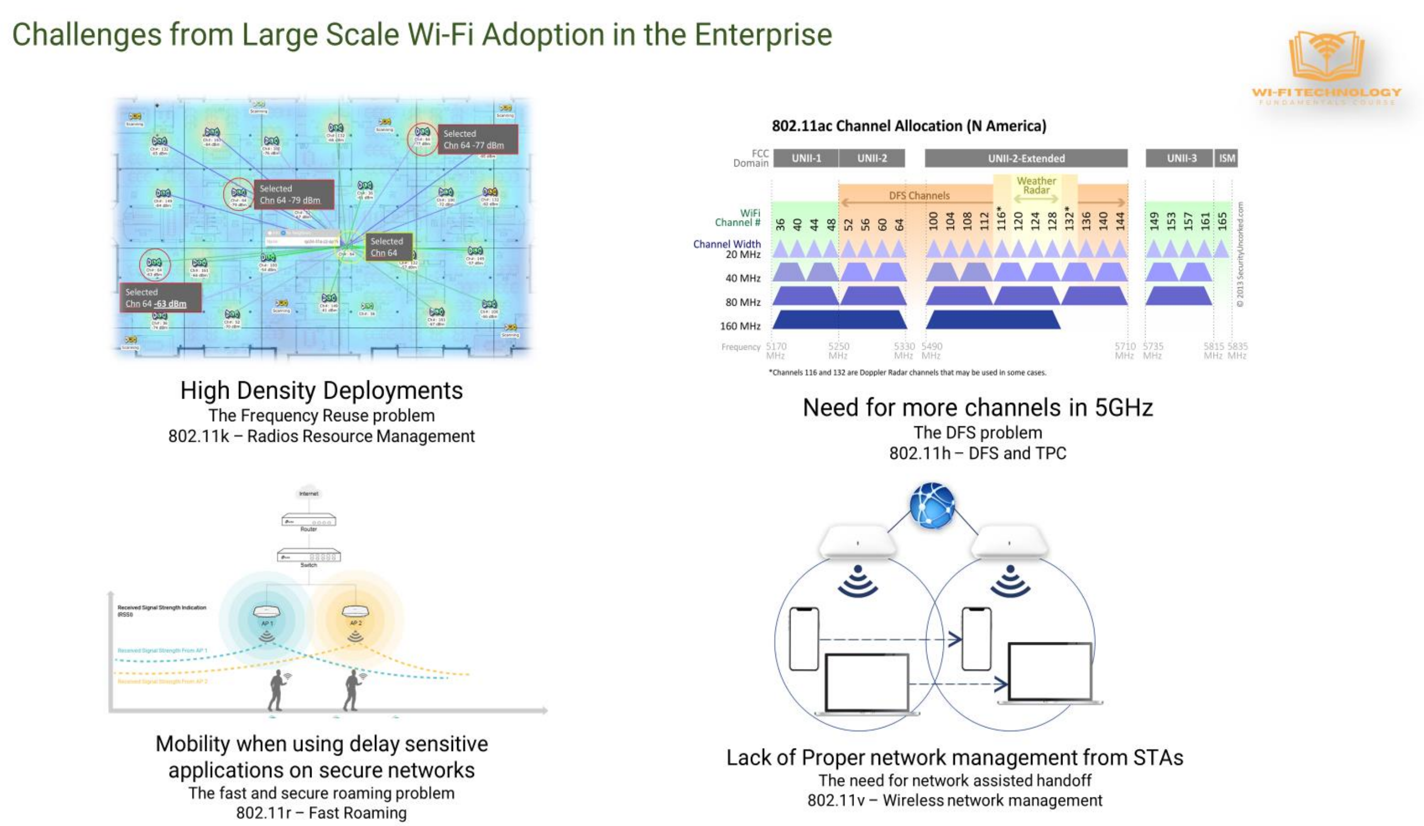
3. Mobility with Delay-Sensitive Applications:

- Problem: Seamless and secure handoff between APs is crucial for real-time applications like VoIP and video conferencing.
- Impact: Delays, audio/video drops, and disruptions in communication flow.
- Solution:

- 802.11r Fast Roaming: Enables rapid and secure handoff between APs, minimizing disruption for delay-sensitive applications.
- Optimized AP Placement and Configuration: Strategic positioning and channel configuration can facilitate smoother transitions.

4. Lack of Proper Network Management from STAs (Station Devices):

- Problem: "Sticky" clients resist roaming even with better signal strength, causing congestion and inefficient resource usage.
- Impact: Underutilization of APs, reduced overall network performance, and potential bandwidth bottlenecks.
- Solution:
  - 802.11v Wireless Network Management: Allows network control over client roaming behavior to encourage timely handoffs.
  - Client Software Updates: Updated drivers and firmware can improve roaming capabilities on the client side.



Dynamic Frequency Selection (DFS)

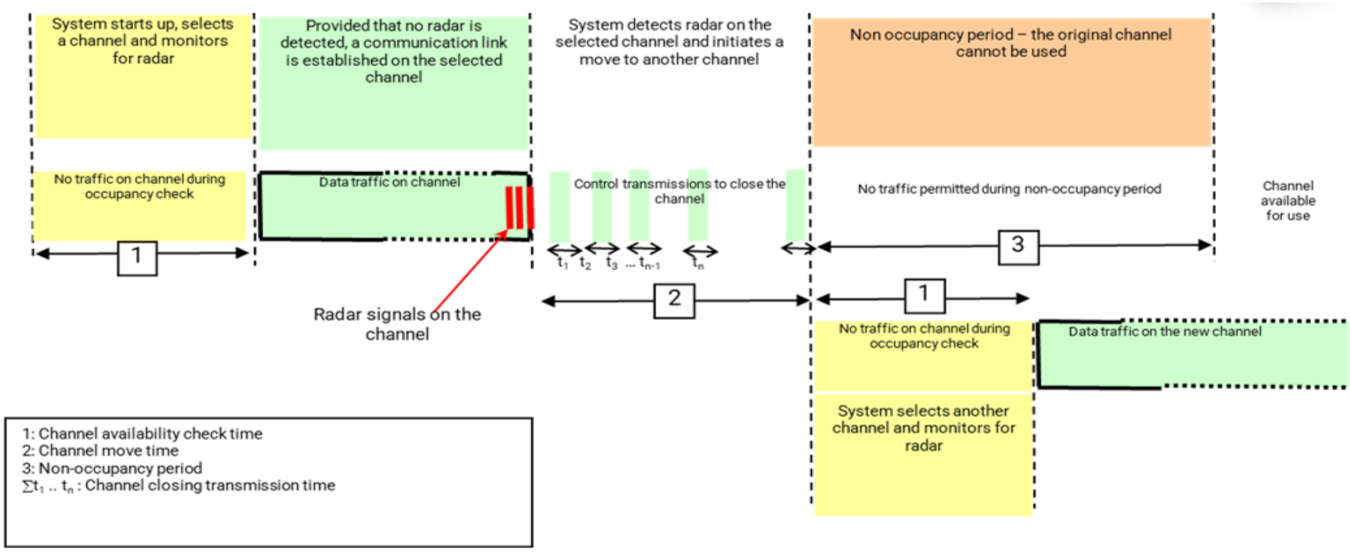
- DFS is a channel allocation scheme that dynamically selects and/or changes the operating frequency to avoid interfering with other systems.
- Unlicensed wireless networking systems (e.g. 802.11a/n) using the 5250-5350 MHz and/or 5470-5725 MHz bands cannot interfere with radar systems.
- A system implementing 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 .

In Dynamic Frequency Selection (DFS), the Access Point (AP) initiates a channel availability check to evaluate the suitability of the intended operating channel. This phase, known as "channel availability check time," involves comparing radar interference to an interference detection threshold. The AP responds differently based on the following scenarios:

- In the absence of a detected radar signal, the AP remains on the current channel.
- Upon detecting a radar signal, the AP opts to transition to an alternative channel. The time taken for this channel switch is termed "channel move time," during which there is a suspension of transmission referred to as "channel closing transmission time."

  Additionally, during the non-occupancy time, the AP refrains from monitoring the channel that detected the radar signal

.



- **Channel Availability Check Time [1]:** 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 [2]:** The time for the system to clear the channel and be 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 [3]:** A period of time after radar is detected on a channel that the channel may not be used.

DFS Implementation

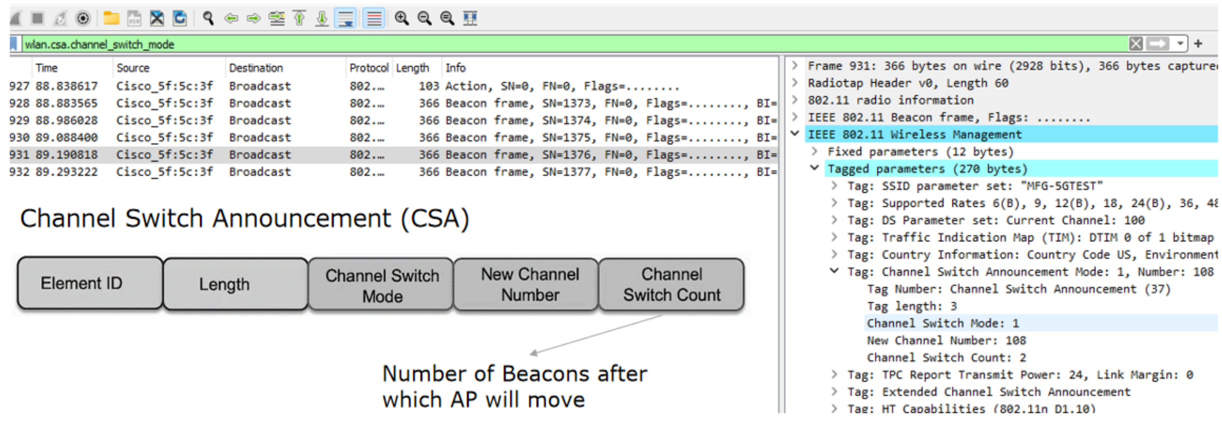
AP Behavior

- 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 the client hears AP beaconing.

- Client may choose to stay connected with the AP upon receiving CSA or choose to move to a new BSS



DFS certifications

Whenever a new model of AP is built or a new firmware is introduced in the market it has to go under different tests to ensure its proper functioning while operating on a DFS channel i.e, to ensure that the AP is following the rules . And to do so , every country has its own certification bodies or government regulatory bodies who plan certain test plans in order to certify the proper functionality of these APs . Since different types of radar pulses are utilized for various applications , our AP should be able to detect all these various radar pulses. For instance, some applications may require a short pulse radar , some may use a long pulse and so on. There are many DFS certification tests and out of those most important one's are the detection probability test and the detection bandwidth test .

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, a 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 the detection bandwidth.

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

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	$\text{Roundup}\left\{\left(\frac{1}{360}\right)\cdot\left(\frac{19\cdot 10^{6}}{PRI_{\mu sec}}\right)\right\}$	30	93.3%
		Test B: 15 unique PRI values randomly selected within the range of 518-3066 μsec, with a minimum increment of 1 μsec, 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%

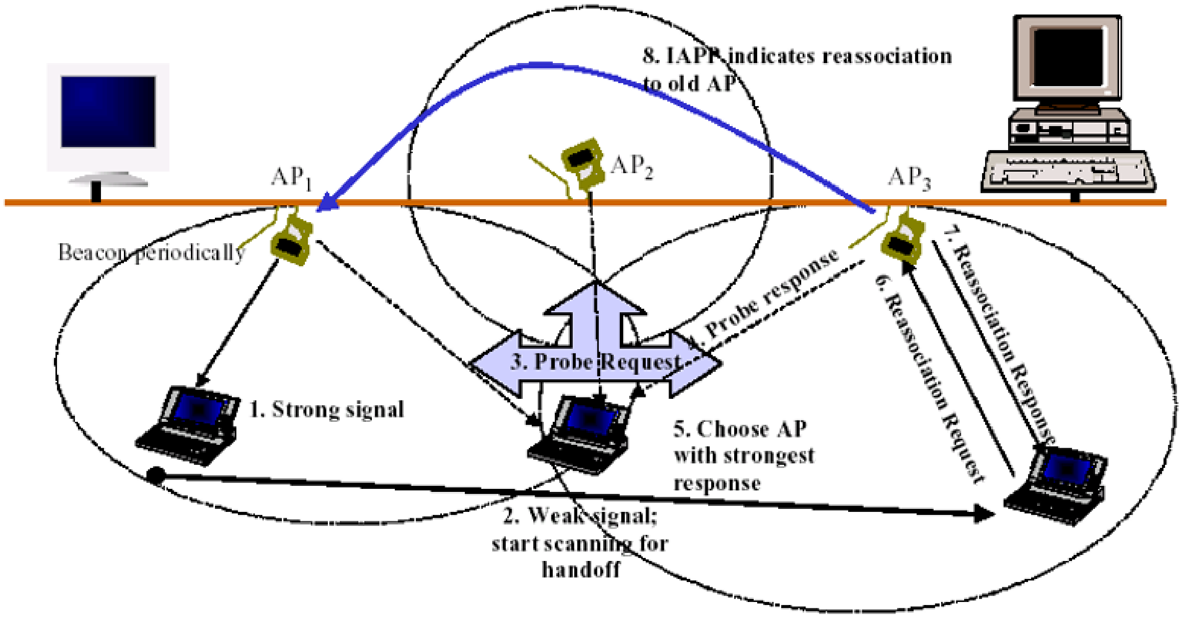
Table 2: Long Pulse Radar Test Waveform

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%

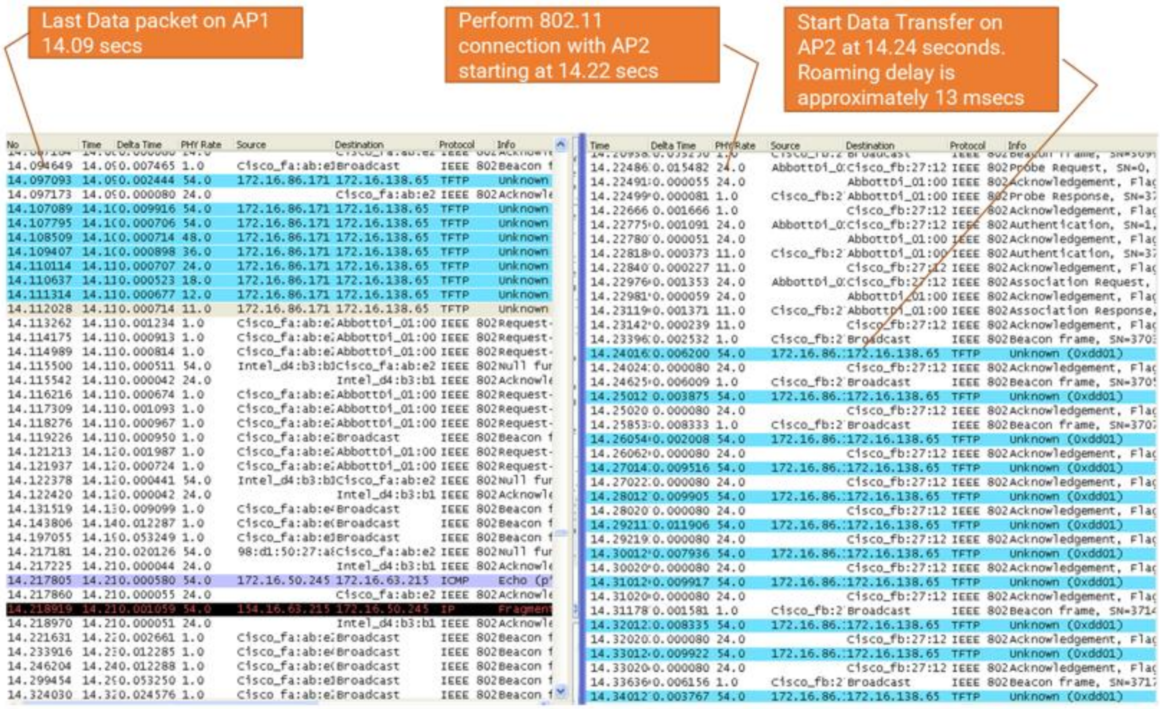
Table 3: Frequency Hopping Radar Test Waveform

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



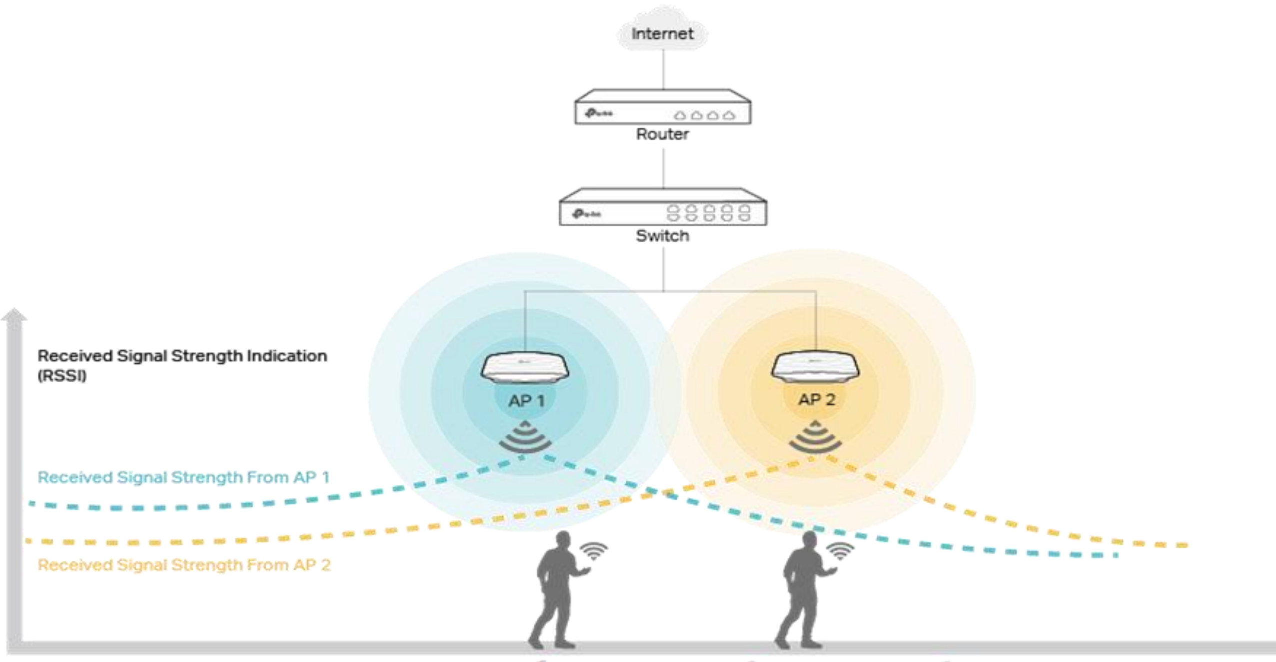
- Most standards attempt to address the issue of roaming.
- Roaming can be defined as the client moving between APs advertising the same or similar wireless network.
- In Wi-Fi, the conventional method of roaming involves a process called "break before you make." This means that you disconnect or dissociate from the current Access Point (AP), conduct a scan and move and then establish a connection with the new AP.
- The traditional roaming method may cause delays, especially with server-based security like .1X authentication, which involves certificate exchanges and generating a four-way handshake lasting hundreds of milliseconds.
- This delay is somewhat acceptable for tasks like email, but can be problematic while doing real-time voice or video communication.
- Improvements in roaming speed are being addressed by certain standard extensions.
- 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 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



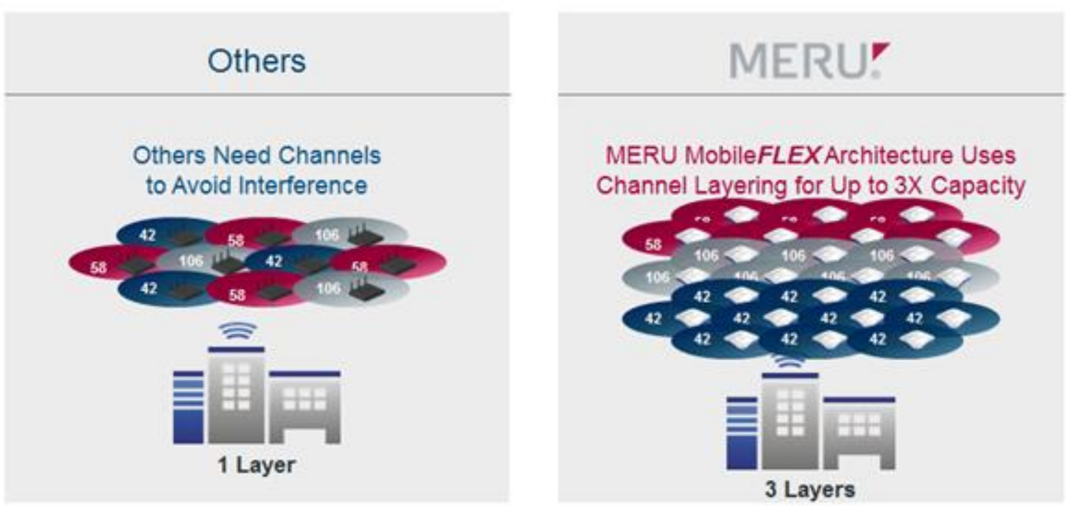
AP1 Capture

AP2 Capture

Evolution of Roaming Enhancements



- The evolution of roaming enhancements over the last 15 to 20 years was initially not based on standards because the standards bodies did not fully recognize the problem at the time.
- However, the initial companies deploying enterprise networks, such as Cisco, encountered this issue in the field.
- People attempting Voice over IP calls on enterprise networks were experiencing challenges with roaming.
- As a result, industries began developing proprietary solutions to address this real problem:
  - Cisco CCX
  - Opportunistic Key Caching, Cisco CCKM
  - Meru Single Channel Implementations



- **802.11 standard extensions:**
  - **802.11e:**
    - QBSS Load Element tells how much load that you have on the current AP.
  - **802.11f:**
    - IAPP (Deprecated)
  - **802.11i:**
    - Security Enhancements
  - **802.11u:**
    - Internetworking with external networks
    - Helped in seamless roaming between Wi-Fi and cellular networks and also between different Wi-Fi networks.
  - **802.11k:**
    - Helped in speeding up the roam decision process making it more efficient.
    - Radio Resource Management
  - **802.11v:**
    - Network Management
    - Help optimize the roam initiation process
  - **802.11r:**
    - Helped in speeding up the roam execution process.

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

802.11k - The Basic Concept

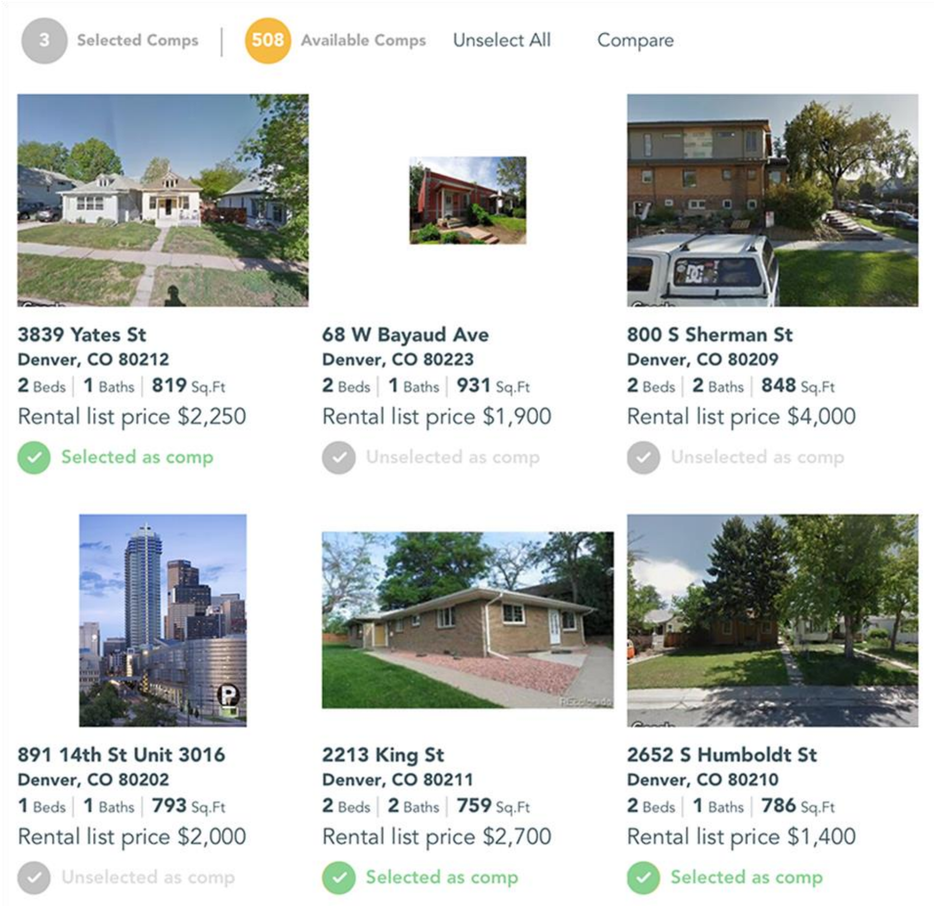
To comprehend 802.11k, let's consider the following analogy:

Imagine you currently reside in a rented home that doesn't provide a satisfactory experience, Whether due to high rent, limited space, or other reasons, you've decided to explore other housing options.

The not so efficient method:

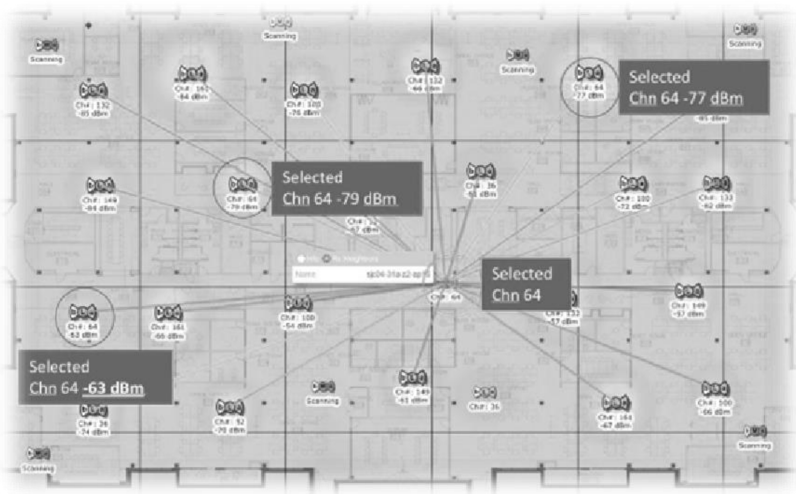
- Go on the road and check every home in the neighborhood to see if it is available for rent.
- Talk to all open house owners and make a list of potential rentals.
- Then shortlist and select.

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.
- Review the list along with the details of each home, shortlist the one you want, and then approach the owner to 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 Request/response measurements to add value

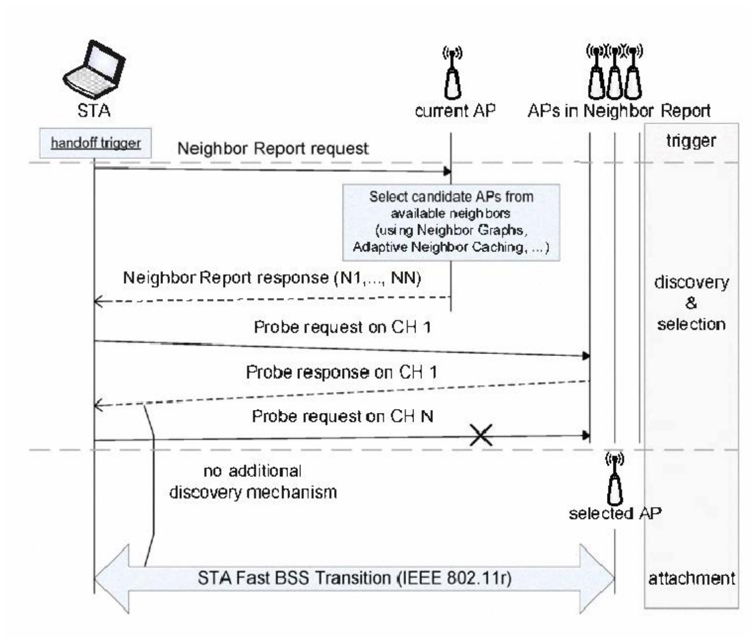
The request/response measurements include:

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

- Radio Resource Management (RRM): RRM is a set of techniques and algorithms used to manage the utilization of the radio frequency spectrum and other wireless resources in a network. This includes features like channel selection, transmit power control, and load balancing.
- Neighbor Reports: 802.11k introduces mechanisms for collecting and exchanging information about neighboring access points (APs). This information is crucial for making informed decisions regarding channel selection, handover, and other optimization tasks.
- Channel Selection: The standard provides a framework for improved channel selection algorithms. This helps in avoiding interference and congestion by dynamically choosing the optimal channel for communication based on the current network conditions.

- BSS Transition Management: 802.11k defines procedures for efficient and seamless client roaming between access points within the same Basic Service Set (BSS). This is particularly important for voice and real-time applications where uninterrupted connectivity is crucial.
- Load Balancing: The standard includes mechanisms for distributing clients across multiple APs to balance the load and avoid congestion on specific access points. This contributes to improved overall network performance.
- Radio Measurement: 802.11k allows for the collection of radio environment information. This information includes signal strength, noise level, and other metrics that aid in making informed decisions about optimizing the network.

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 it through the connection process with the new AP.

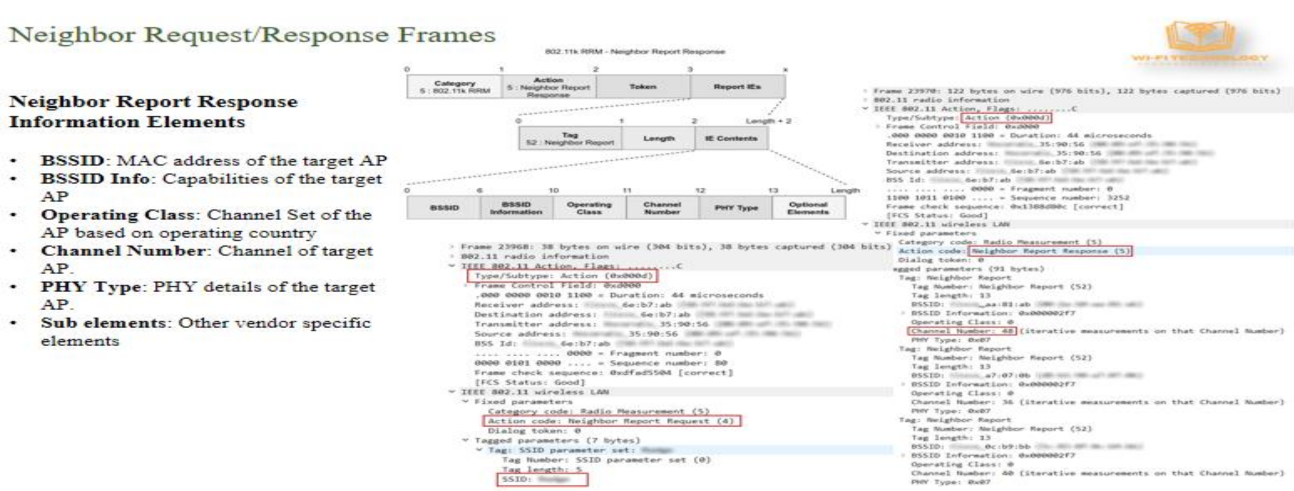
How it helps:

- To find the best network available to connect
- Making the search for a new AP much easier when it's 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 no of air frames.

Let's Consider an Example:

- Imagine you're using Wi-Fi on your phone, and you're connected to an access point (AP) on channel 36. Usually, when you want to roam or switch to a better AP, your phone would scan different channels (like channel 40, 44, 48, etc.) to find a suitable one.
- The problem is, this traditional scanning process takes time, and you might lose connection with your current AP, causing interruptions in your internet use.
- Now, with 802.11k, your phone can be smarter. Instead of blindly scanning all channels, it can directly ask its current AP, "Hey, can you tell me about all the nearby APs? I might want to switch."
- The current AP then does the work. It checks which APs are around, collects information about them (like signal strength, channel details, etc.), and sends all this info back to your phone in a neat report.
- Your phone gets this report and can now make an informed decision. It sees which nearby AP is the best option, based on factors like signal strength and performance. It then smoothly switches to the new AP without scanning all channels, reducing the risk of losing connection or interrupting your activities.
- 802.11k allows your device to ask its current Wi-Fi hot-spot about nearby options, get a handy list, and choose the best one for a seamless and efficient switch.

Neighbor Request/Response Frames

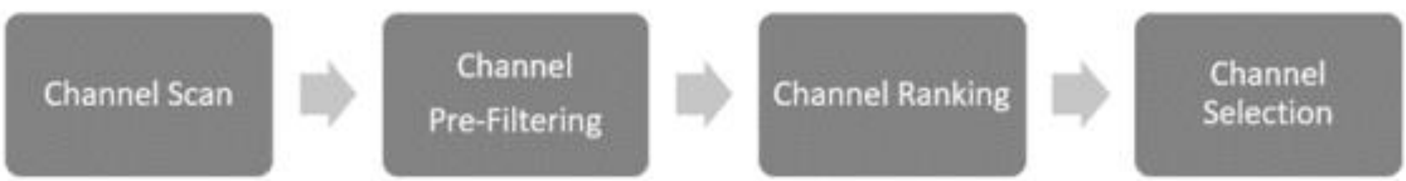


- Imagine your device (like a phone or laptop) wants to know about other Wi-Fi options nearby, like which Wi-Fi routers are available and how good they are. Your device sends a "neighbor report request" to the Wi-Fi router it's currently connected to.
- Now, the Wi-Fi router receives this request and does a bit of detective work. It looks around and makes a list of all the nearby Wi-Fi routers, noting things like which channel they're on, what type of Wi-Fi they use, and how strong their signals are. This list is called the "neighbor report."

- The Wi-Fi router then sends this neighbor report back to your device as a "neighbor report response." This response is like a detailed list that tells your device about all the Wi-Fi options it found.
- Now, with this information, your device can make a smart decision. It can see which nearby Wi-Fi router is the best choice based on factors like signal strength and other technical details. This helps your device decide if it's a good idea to switch to a different Wi-Fi router for a smoother and better connection.
- So, in a nutshell, the neighbor report request and response help your device gather information about nearby Wi-Fi options, making it easier to choose the best one for a solid and reliable connection.

Auto Channel Selection for RRM (Proprietary Implementations)

- The 802.11k is also about how to optimize the channel allocation.
- There are many proprietary mechanisms that are implemented, that are doing radio Resource Management, and is basically called the Auto channel selection.
- Basically APs can be intelligent about which channel to use and also figure out which channel to operate in.
- The goal of each AP is to operate on the least congested channel.
- The AP periodically scans and finds out the information about its neighboring APs and finds the information about the least busy channel.
- The AP ranks the channels based on the number of networks they are already on,channel bonding, channel overlap,signal strength and many other metrics.



- The AP can run an ACS (Auto Channel Selection) algorithm to do the scanning and change the channels.
- 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.

802.11v – Wireless Network Management

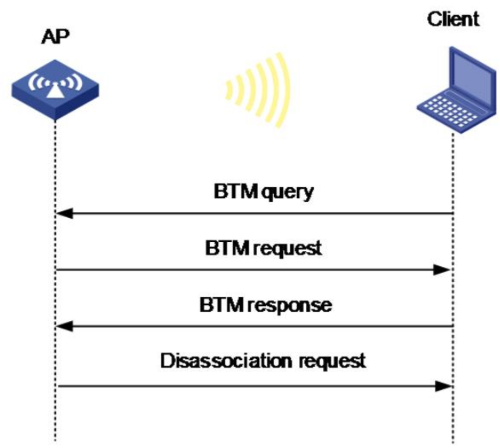
The 802.11v is a very big spec that covers so many different features, it is about 500-600 pages long.

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

802.11v - BSS Transition Management

- BSS transition management(BTM) is where the network can take control.
- BSS transition management 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.
- Let's say the client is at the edge of the AP's Cell, it normally has a very low signal which means that it will transmit at very low PHY data rates to maintain a good SNR.
- So the AP will detect the inefficient clients that are at the edge of the cell and be able to move the client to a more optimal AP.
- Either the client can send a BSS transition management query to transition from one AP to another AP.
- The AP can send a BSS transition management request, telling the client which AP to move.
- The client acknowledges the request and the AP will disassociate the client.
- The client will go and associate with the new AP, as the client already knows which AP to move.
- This is the network way of forcing the movement from one AP to the other AP.



BTM Request/Response

BSS Transition Management enables an AP to request a voice client to transition to a specific AP or suggest a set of preferred APs, contributing to network load balancing or BSS termination.
Facilitates voice clients in identifying the best AP to transition to during roaming, improving throughput, data rates, and QoS.
(ArubaOs supports BSS Transition Management features defined by the 802.11v standard.)

Frame Types:

1. Query Frame:
Sent by a voice client supporting BSS transition management.
Requests a BSS transition candidate list from its associated AP (if AP supports BSS transition capability).
2. Request Frame:
Sent by an AP supporting BSS Transition Management in response to a Query frame.
It sends unsolicited to a voice client supporting BSS Transition Management.
Contains a Disassociation flag, potentially leading to client disassociation if set, with a specified timeframe.
3. Response Frame
Sent by the voice client to the AP in response to a BSS Transition Management Request frame.Informs whether the client accepts or denies the transition.

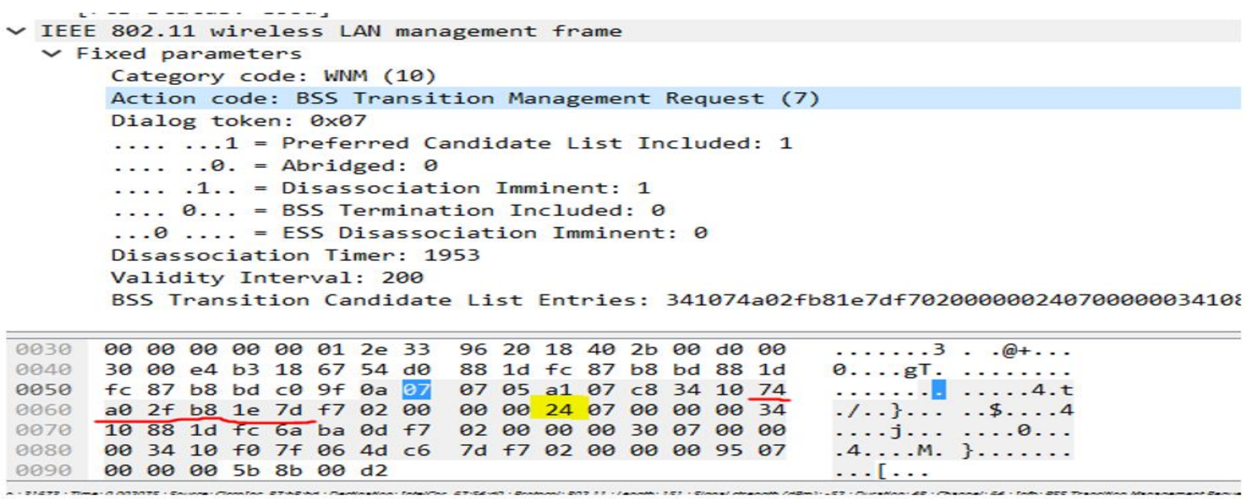
802.11k and 802.11v Clients:

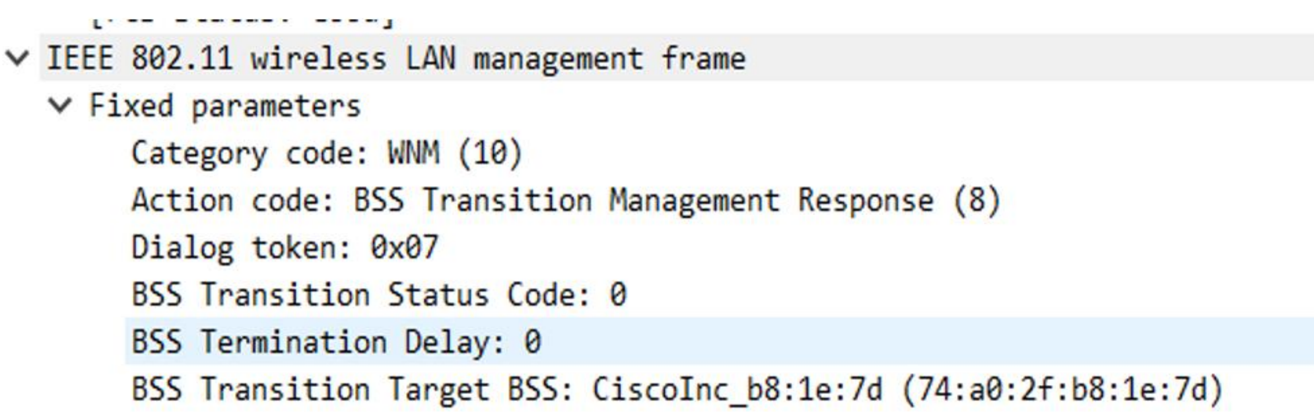
802.11k Clients:
Utilize the actual beacon report generated by the client in response to a beacon report request from the AP.
Replaces the virtual beacon report for that client.

802.11v Clients:
The controller uses the 802.11v BSS Transition message to steer clients to the desired AP upon receiving a client steer trigger from the AP.

In the BSS Transition Management process, the AP sends a BSS transition management request, providing a preferred candidate list to voice clients.
The AP informs the station about available options and enforces a forced relocation if necessary, indicating an imminent disassociation if the client doesn't comply within a set timeframe.

```
v 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)
  v Tag: Extended Capabilities (8 octets)
      Tag Number: Extended Capabilities (127)
      Tag length: 8
    v 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
    v 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
    v 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)
```





802.11r – Fast BSS Transition

IEEE 802.11r introduces the concept of Fast Transition (FT) Roaming.
FT allows the initial handshake with the new AP before the client roams, enabling Pairwise Transient Key (PTK) calculation in advance.

Fast Transition Protocols and Message Exchanges:

Over-the-Air Method:
The client communicates directly with the target AP using IEEE 802.11 authentication with the Fast Transition authentication algorithm.
The station connects to the current AP, and advertises 11r capabilities.

The security context is transferred during the authentication request, avoiding a full exchange.
Reassociation with the new AP establishes a secure connection without repeating the entire connection process.

Over-the-DS Method:

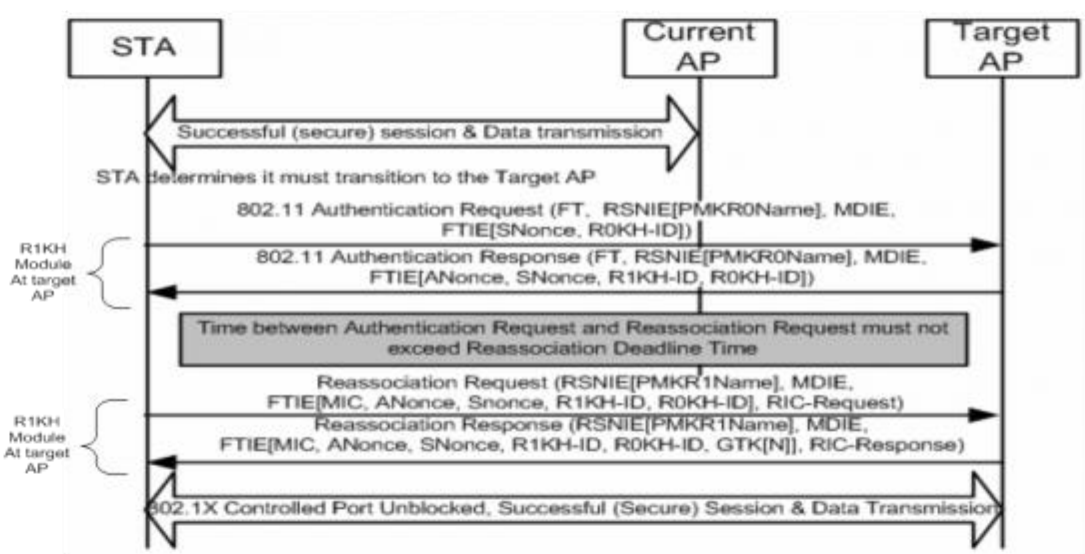
- The client communicates with the target AP through the current AP.
- Fast Transition action frames carry communication between the client and the current AP sent through the controller.
- The security context is transferred through a special action frame sent to the current AP.
- Information is relayed over the wired network to the new AP, followed by a reassociation process.

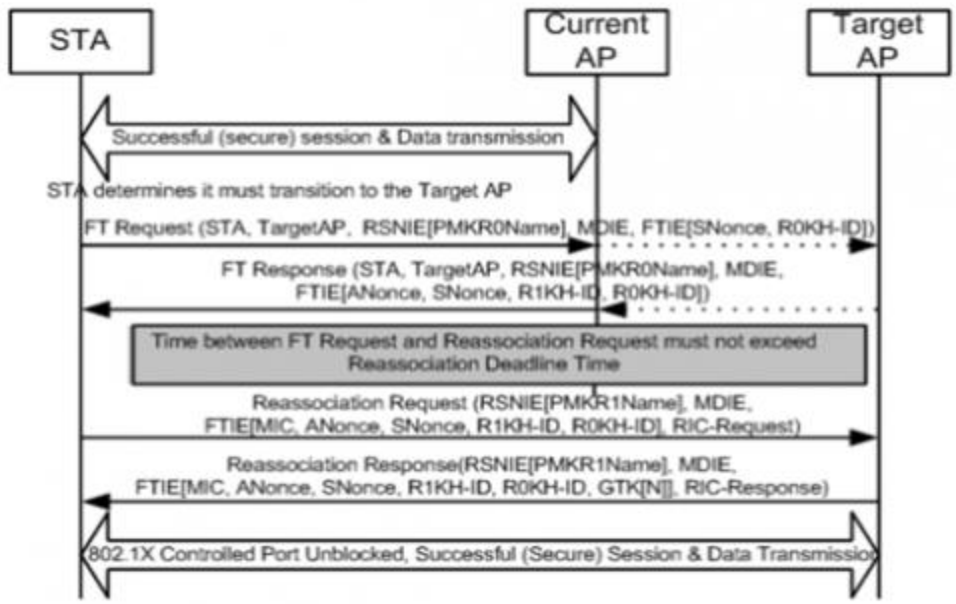
Benefits of Fast Transition:

- Improves roaming efficiency by conducting initial handshakes in advance.
- Allows PTK calculation beforehand, enhancing security during roaming.
- Reduces the time and steps involved in the connection process when moving to a new AP.

- 11r addresses the challenge of efficiently, securely, and quickly roaming between APs.
- Allows the transfer of security context from the current AP to the new AP, avoiding the need for the station to reestablish security context.

- 11k and 11v optimize the roaming initiation and decision process.
- 11r focuses on efficient and secure roaming by enabling the transfer of security context and avoiding initial handshakes.




STA
Current AP
Target AP
Successful (secure) session & Data transmission
STA determines it must transition to the Target AP
FT Request (STA, TargetAP, RSNIE[PMKR0Name], MDIE, FTIE[SNonce, R0KH-ID])
FT Response (STA, TargetAP, RSNIE[PMKR0Name], MDIE, FTIE[ANonce, SNonce, R1KH-ID, R0KH-ID])
Time between FT Request and Reassociation Request must not exceed Reassociation Deadline Time
Reassociation Request (RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID], RIC-Request)
Reassociation Response(RSNIE[PMKR1Name], MDIE, FTIE[MIC, ANonce, SNonce, R1KH-ID, R0KH-ID, GTK[N]], RIC-Response)
802.1X Controlled Port Unblocked, Successful (Secure) Session & Data Transmission