Answers for Session 5a - 802.11k/v/r, RRM, DFS, Fast Roaming

How does data traffic behave when a Channel Switch Announcement (CSA) is broadcasted from the Access Point (AP)?

When a CSA is broadcasted, connected clients are notified of an upcoming channel switch. Upon receiving the CSA, clients start preparing for the switch by scanning the new channel. The actual channel switch may cause a temporary disruption in data traffic as clients briefly disconnect from the current channel. After the channel switch is complete, data traffic resumes on the new channel. The time for clients to reconnect and resume normal data traffic depends on specific implementation and client device capabilities, ranging from seamless transitions to noticeable delays.

Does Automatic Channel Switching (ACS) operate solely on the Access Point (AP), or is it also implemented on client devices?

Automatic Channel Switching (ACS) primarily runs on the Access Point (AP) to determine and manage channel changes. Clients receive information about channel switches through mechanisms like Channel Switch Announcements (CSA) but typically do not perform ACS themselves.

What Wireshark filters should be employed to capture frames related to 802.11k, 802.11v, and 802.11r protocols?

Wireshark Display Filters related 802.11 k,v,r traffic:	**Filter corresponds to:**
wlan.fixed.action_code ==23	802.11v dms request
wlan.fixed.action_code ==24	802.11v dms respose
wlan.fixed.action_code == 4	802.11k neighbour request
wlan.fixed.action_code == 5	802.11k neighbour response
(wlan.fc.type_subtype==0)&&(wlan.rsn.akms.type==3)	802.11r auth request
(wlan.fc.type_subtype==1)&&(wlan.tag.number==55)	802.11r auth response
(wlan.fc.type_subtype==2)&&(wlan.tag.number==55)	802.11r re-association request
(wlan.fc.type_subtype==3)&&(wlan.tag.number==55)	802.11r re-association response
wlan.fixed.action_code==7	BSS Transition (Steering)
wlan.fixed.action_code==8	BSS Transition (Steering)

Display Filters related Weak signals:	
wlan_radio.signal_dbm < -67	weak signal filter
wlan.fc.type_subtype == 0x05 && wlan_radio.signal_dbm < -75	weak prob response
wlan.fc.type_subtype == 0x04 && wlan_radio.signal_dbm < -75	weak prob requests

In Auto RRM, which packets show automatic channel changes?

Generally when the AP switches the channel the AP informs the client that it is changing channel from the CSA frames either present in beacon frames/ action frames.
Listening to this the clients should be ready to switch the channel.

For Auto Radio Resource Management (Auto RRM), look for the following Wireshark display filters indicating automatic channel changes:

Beacon Frames with Channel Switch Announcement (CSA):
Display filter: wlan.fc.type_subtype == 0x08 && wlan.tag.number == 37
These filters capture management frames announcing automatic channel changes in a wireless network. Please adapt them based on your specific networking equipment and configurations.

What kind of authentication does 802.11r support?

802.11r supports Fast Basic Service Set (BSS) Transition (FT) authentication for seamless and fast roaming in wireless networks, particularly in the context of Wi-Fi.

I have many APs in my Lab, and I am planning to use only non-DFS channels. What is more efficient: (1) Auto mode or designing channels manually?

If you want to use only non-DFS (Dynamic Frequency Selection) channels in your lab, it may be more efficient to manually design the channel plan rather than relying on the auto mode. DFS channels are used in the 5 GHz frequency band and are subject to radar detection requirements, which can cause automatic channel changes.

When you set your access points (APs) to auto mode, they will typically select channels dynamically based on the environment and interference. This can lead to potential channel changes, especially if radar is detected on a DFS channel. If you want to avoid such automatic changes and ensure a stable channel plan, manually configuring non-DFS channels would be a more predictable approach.

By manually designing the channel plan, you have better control over interference management and can optimise the channel distribution to minimise co-channel

interference. This is particularly important in a lab environment where you have the flexibility to plan and optimise the wireless network settings.

How do beacon frames differ from data frames?

Feature	Beacon Frames	Data Frames
Function	Broadcasted by access points to announce network presence and provide essential information.	Used to carry actual payload data, such as user-generated traffic, between devices within the network.
Content	Contains information like SSID, supported data rates, and other network parameters.	Carries actual data along with control information such as source and destination addresses.
Timing	Transmitted periodically at regular intervals for network discovery and joining.	Sent as needed based on user activities and communication requirements.

Does 802.11u support only between Wi-Fi and cellular?

No, IEEE 802.11u is not limited to interactions between Wi-Fi and cellular networks. While one of the primary use cases for 802.11u is to enable seamless and secure transitions between Wi-Fi and cellular networks (specifically for offloading cellular traffic to Wi-Fi), the standard is designed to enhance overall network discovery and selection processes in Wi-Fi networks.

What is the difference between CSA and ECSA?

In addition to the regular Channel switch announcement Element parameters, the extended channel switch announcement element provides the operating class of the channel that the Access point is moving to.

Regular Channel Switch Announcement (CSA):
When a Wi-Fi AP decides to switch its operating channel, it sends a CSA frame to inform other devices in the network about the upcoming channel change. This frame typically contains the following parameters:

New Channel Number: Specifies the channel to which the AP is moving.
Countdown Timer: Indicates the time remaining before the channel switch occurs.
Channel Switch Announcement Mode: Specifies whether the channel switch is mandatory or optional.

Extended Channel Switch Announcement (ECSA):
In addition to the parameters mentioned above, ECSA includes an important enhancement – the "Operating Class" of the channel. The operating class provides information about the regulatory domain and the characteristics of the channel the AP is moving to.

Operating Class:
Definition: An operating class defines a set of regulatory requirements and characteristics associated with a group of channels within a specific frequency band.

Examples: In the context of Wi-Fi, different operating classes may define channels with varying channel widths, transmit power limits, and other parameters.

Significance of Including Operating Class in ECSA:
Regulatory Compliance: Including the operating class in ECSA ensures that neighbouring devices are informed not only about the new channel but also about the specific regulatory characteristics associated with that channel.

Improved Adaptation: Neighbouring devices can adjust their settings more accurately based on the operating class information, ensuring compliance with local regulations and optimising their own performance.