Wireshark Most Common 802.11 Filters v1.1

Filter Addresses

Addresses used for 802.11 communications

Up to 4 different MAC addresses can be used in an IEEE 802.11 frame:
- The transmitter MAC address or TA
- The receiver MAC address or RA
- The source MAC address or SA
- The destination MAC address or DA

Filters

Filter for a specific client by MAC address: **wlan.addr ==** *MAC_address*
Ex: wlan.addr == 00:11:22:33:44:55

Filter by the transmitter address (TA): **wlan.ta ==** *MAC_address*
Ex: wlan.ta == 00:11:22:33:44:55

Filter by the receiver address (RA): **wlan.ra ==** *MAC_address*
Ex: wlan.ra == 00:11:22:33:44:55

Filter by the source address (SA): **wlan.sa ==** *MAC_address*
Ex: wlan.sa == 00:11:22:33:44:55

Filter by the destination address (DA): **wlan.da ==** *MAC_address*
Ex: wlan.da == 00:11:22:33:44:55

Filter Wi-Fi Networks

BSSID vs SSID

BSSID is the MAC address of the radio transmitting in the AP
The BSSID is specific to 1 AP

SSID is the name of the global Wi-Fi network
The SSID can be used by multiple APs in a WLAN infrastructure

Filters

Filter by BSSID (by AP): **wlan.bssid ==** *AP_radio_MAC_address*
Ex: wlan.bssid == 00:11:22:33:44:55

Filter by SSID: **wlan_mgt.ssid ==** *"your_SSID"*
Ex: wlan_mgt.ssid == "SemFio"

Filter 802.11 Management Frames

Description

802.11 Management Frames are used by stations to join and leave a BSS
There is a total of 12 802.11 Management Frames:

- Association request (subtype 0x0)
- Association response (subtype 0x1)
- Reassociation request (subtype 0x2)
- Reassociation response (subtype 0x3)
- Probe request (subtype 0x4)
- Probe response (subtype 0x5)
- Beacon (subtype 0x8)
- ATIM (subtype 0x9)
- Disassociation (subtype 0xa)
- Authentication (subtype 0xb)
- Deauthentication (subtype 0xc)
- Action (subtype 0xd)

Filters

Filter for all management frames:	**wlan.fc.type == 0**
Filter for Association Requests:	**wlan.fc.type_subtype == 0**
Filter for Association Responses:	**wlan.fc.type_subtype == 1**
Filter for Reassociation Requests:	**wlan.fc.type_subtype == 2**
Filter for Resssociation Responses:	**wlan.fc.type_subtype == 3**
Filter for Probe Requests:	**wlan.fc.type_subtype == 4**
Filter for Probe Responses:	**wlan.fc.type_subtype == 5**
Filter for Beacons:	**wlan.fc.type_subtype == 8**
Filter for ATIMs:	**wlan.fc.type_subtype == 9**
Filter for Disassociations:	**wlan.fc.type_subtype == 10**
Filter for Authentications:	**wlan.fc.type_subtype == 11**
Filter for Deauthentications:	**wlan.fc.type_subtype == 12**
Filter for Actions:	**wlan.fc.type_subtype == 13**

Filter 802.11 Control Frames

Description

802.11 Control Frames assist with the delivery of data frames (type = 1)
There is a total of 8 802.11 Control Frames:

- Block ACK request (subtype 0x8)
- Block ACK (subtype 0x9)
- PS-Poll (subtype 0xa)
- Ready To Send (subtype 0xb)
- Clear To Send (subtype 0xc)
- ACK (subtype 0xd)
- CF-End (subtype 0xe)
- CF-End/CF-Ack (subtype 0xf)

Filters

Filter for all control frames:	**wlan.fc.type == 1**
Filter for Block ACK Requests:	**wlan.fc.type_subtype == 24**
Filter for Block ACKs:	**wlan.fc.type_subtype == 25**
Filter for PS-Polls:	**wlan.fc.type_subtype == 26**
Filter for Ready To Sends:	**wlan.fc.type_subtype == 27**
Filter for Clear To Sends:	**wlan.fc.type_subtype == 28**
Filter for ACKs:	**wlan.fc.type_subtype == 29**
Filter for CF-Ends:	**wlan.fc.type_subtype == 30**
Filter for CF-Ends/CF-Acks:	**wlan.fc.type_subtype == 31**

Filter 802.11 Data Frames

Description

802.11 Data Frames are mainly used to carry data (tupe = 2)
There is a total of 15 802.11 Data Frames:

- Data (subtype 0x0)
- Data+CF-Ack (subtype 0x1)
- Data+CF-Poll (subtype 0x2)
- Data+CF-Ack+CF-Poll (subtype 0x3)
- Null (subtype 0x4)
- CF-Ack (subtype 0x5)
- CF-Poll (subtype 0x6)
- CF-Ack+CF-Poll (subtype 0x7)
- QoS Data (subtype 0x8)
- QoS Data+CF-Ack (subtype 0x9)
- QoS Data+CF-Poll (subtype 0xa)
- QoS Data+CF-Ack+CF-Poll (0xb)
- QoS Null (subtype 0xc)
- QoS CF-Poll (subtype 0xe)
- QoS CF-Ack+CF-Poll (subt. 0xf)

Filters

Filter for all data frames:	**wlan.fc.type == 2**
Filter for Data:	**wlan.fc.type_subtype == 32**
Filter for Data+CF-Ack:	**wlan.fc.type_subtype == 33**
Filter for Data+CF-Poll:	**wlan.fc.type_subtype == 34**
Filter for Data+CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 35**
Filter for Null:	**wlan.fc.type_subtype == 36**
Filter for CF-Ack:	**wlan.fc.type_subtype == 37**
Filter for CF-Poll:	**wlan.fc.type_subtype == 38**
Filter for CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 39**
Filter for QoS Data:	**wlan.fc.type_subtype == 40**
Filter for QoS Data+CF-Ack:	**wlan.fc.type_subtype == 41**
Filter for QoS Data+CF-Poll:	**wlan.fc.type_subtype == 42**
Filter for QoS Data+CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 43**
Filter for QoS Null:	**wlan.fc.type_subtype == 44**
Filter for QoS CF-Poll:	**wlan.fc.type_subtype == 46**
Filter for QoS CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 47**

RadioTap Header Information

Description

RadioTap Headers provide additional information (channel frequency, data rate, signal strength...) to any 802.11 frame when capturing frames.

Filters

Filter a specific channel: **radiotap.channel.freq ==** *frequency*
Ex: radiotap.channel.freq == 5240

Filter a specific data rate: **radiotap.datarate ==** *rate_in_Mbps*
Ex: radiotap.datarate <= 6

Filter by signal strength (RSSI): **radiotap.dbm_antsignal ==** *rate_in_dBm*
Ex: radiotap.dbm_antsignal >= -60

Sources: https://www.wireshark.org/docs/dfref/w/wlan.html (11/25/15), https://www.wireshark.org/docs/dfref/r/radiotap.html (11/25/15), CWAP Official Study Guide (2011)