802.11 Wireshark Filters

wirelessLAN PROFESSIONALS

Management Frames	`wlan.fc.type == 0`
Association Request	`wlan.fc.type_subtype == 0`
Association Response	`wlan.fc.type_subtype == 1`
Reassociation Request	`wlan.fc.type_subtype == 2`
Reassociation Response	`wlan.fc.type_subtype == 3`
Probe Request	`wlan.fc.type_subtype == 4`
Probe Response	`wlan.fc.type_subtype == 5`
Beacon	`wlan.fc.type_subtype == 8`
Disassociation	`wlan.fc.type_subtype == 10`
Authentication	`wlan.fc.type_subtype == 11`
Deauthentication	`wlan.fc.type_subtype == 12`
Action	`wlan.fc.type_subtype == 13`

Control Frames	`wlan.fc.type == 1`
Block ACK Request	`wlan.fc.type_subtype == 24`
Block ACK	`wlan.fc.type_subtype == 25`
PS-Poll	`wlan.fc.type_subtype == 26`
Ready To Send (RTS)	`wlan.fc.type_subtype == 27`
Clear to Send (CTS)	`wlan.fc.type_subtype == 28`
ACK	`wlan.fc.type_subtype == 29`

Data Frames	`wlan.fc.type == 2`
Data	`wlan.fc.type_subtype == 32`
Null	`wlan.fc.type_subtype == 36`
QoS Data	`wlan.fc.type_subtype == 40`
QoS Null	`wlan.fc.type_subtype == 44`

Display Filter Operators		
Equal	`==`	`eq`
Not Equal	`!=`	`ne`
And	`&&`	`and`
Or	`||`	`or`
Xor	`^^`	`xor`
Not	`!`	`not`
Contains	`wlan.xxx contains "xx:xx"`	

Addresses	
MAC address	`wlan.addr == MAC_address`
Transmitter Address (TA)	`wlan.ta == MAC_address`
Receiver Address (RA)	`wlan.ra == MAC_address`
Source Address (SA)	`wlan.sa == MAC_address`
Destination Address (DA)	`wlan.da == MAC_address`

Access Points and SSIDs	
BSSID	`wlan.bssid == AP_radio_MAC_address`
SSID	`wlan_mgt.ssid == SSID`

Radio Tap Header	
Specific Channel	`radiotap.channel.freq == frequency`
Specific Data Rate	`radiotap.datarate == rate_in_Mbps`
RSSI	`radiotap.dbm_antsignal == rate_in_dBm`

802.11k,v,r	
802.11v DMS request	`wlan.fixed.action_code == 23`
802.11v DMS response	`wlan.fixed.action_code == 24`
802.11k Neighbor request	`wlan.rm.action_code == 4`
802.11k Neighbor response	`wlan.rm.action_code == 5`
802.11r FT auth req	`(wlan.fc.type_subtype==0) && (wlan.rsn.akms.type == 3)`
802.11r FT auth res	`(wlan.fc.type_subtype==1) && (wlan.tag.number == 55)`
802.11r FT reassoc req	`(wlan.fc.type_subtype==2) && (wlan.tag.number == 55)`
802.11r FT reassoc res	`(wlan.fc.type_subtype==3) && (wlan.tag.number == 55)`

Retries	
Retry	`wlan.fc.retry==1`

Weak Signal and Probes	
Weak Signal	`wlan_radio.signal_dbm < -dB`
Weak Probe responses	`wlan.fc.type_subtype == 5 && wlan_radio.signal_dbm < -dB`
Weak Probe requests	`wlan.fc.type_subtype == 4 && wlan_radio.signal_dbm < -dB`

4-Way Handshake Filter	`wlan.addr == MAC && eapol`