Wireshark 802.11 Display Filter Field Reference

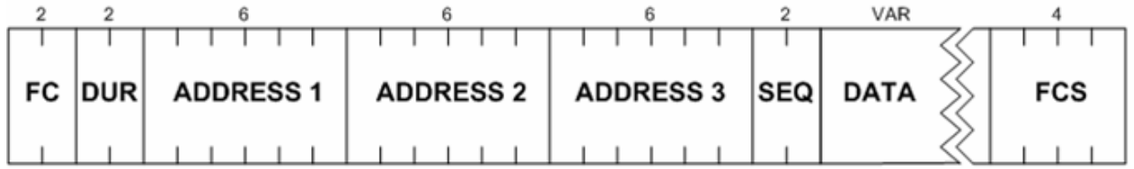
Frame Type/Subtype	Filter
Management frames	wlan.fc.type eq 0
Control frames	wlan.fc.type eq 1
Data frames	wlan.fc.type eq 2
Association request	wlan.fc.type_subtype eq 0
Association response	wlan.fc.type_subtype eq 1
Reassociation request	wlan.fc.type_subtype eq 2
Reassociation response	wlan.fc.type_subtype eq 3
Probe request	wlan.fc.type_subtype eq 4
Probe response	wlan.fc.type_subtype eq 5
Beacon	wlan.fc.type_subtype eq 8
Announcement traffic indication map (ATIM)	wlan.fc.type_subtype eq 9
Disassociate	wlan.fc.type_subtype eq 10
Authentication	wlan.fc.type_subtype eq 11
Deauthentication	wlan.fc.type_subtype eq 12
Action frames	wlan.fc.type_subtype eq 13
Block ACK Request	wlan.fc.type_subtype eq 24
Block ACK	wlan.fc.type_subtype eq 25
Power-Save Poll	wlan.fc.type_subtype eq 26
Request to Send	wlan.fc.type_subtype eq 27
Clear to Send	wlan.fc.type_subtype eq 28
ACK	wlan.fc.type_subtype eq 29
Contention Free Period End	wlan.fc.type_subtype eq 30
Contention Free Period End ACK	wlan.fc.type_subtype eq 31
Data + Contention Free ACK	wlan.fc.type_subtype eq 33
Data + Contention Free Poll	wlan.fc.type_subtype eq 34
Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 35
NULL Data	wlan.fc.type_subtype eq 36
NULL Data + Contention Free ACK	wlan.fc.type_subtype eq 37
NULL Data + Contention Free Poll	wlan.fc.type_subtype eq 38
NULL Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 39
QoS Data	wlan.fc.type_subtype eq 40
QoS Data + Contention Free ACK	wlan.fc.type_subtype eq 41
QoS Data + Contention Free Poll	wlan.fc.type_subtype eq 42
QoS Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 43
NULL QoS Data	wlan.fc.type_subtype eq 44
NULL QoS Data + Contention Free Poll	wlan.fc.type_subtype eq 46
NULL QoS Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 47

IEEE 802.11
Pocket Reference Guide
SANS Institute
www.sans.org

Acronyms

AES	Advanced Encryption Standard	PEAP	Protected EAP
AID	Association Identifier	PMK	Pairwise Master Key
AP	Access Point	PRGA	Pseudo-Random Generation Algorithm
BS	Base Station	PSK	Pre-Shared Key
BSS	Basic Service Set	PSPF	Publicly Switched Packet Forwarding
BSSID	Basic Service Set Identifier	PTK	Pairwise Temporal Key
CCA	Clear Channel Assessment	RF	Radio Frequency
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol	RFMON	Radio Frequency Monitoring
		RSSI	Received Signal Strength Indicator
		RTS	Request to Send
CTS	Clear to Send	SNR	Signal to Noise Ratio
DS	Distribution System	SS	Subscriber Station
EAP	Extensible Authentication Protocol	SSID	Service Set Identifier
FAST	Flexible Authentication via Secure Tunneling	STA	Station
		TIM	Traffic Indication Map
ESS	Extended Service Set	TKIP	Temporal Key Integrity Protocol
FMS	Fluhrer, Mantin, Shamir	TLS	Transport Layer Security
ICV	Integrity Check Value	TTLS	Tunneled TLS
ISM	Industrial, Scientific, Medical	WDS	Wireless Distribution System
IV	Initialization Vector	WEP	Wired Equivalence Privacy
LEAP	Lightweight EAP	WIDS	Wireless Intrusion Detection System
MAC	Message Authenticity Check	WPA	WiFi Protected Access
MAC	Media Access Control	WZC	Wireless Zero Config
MIC	Message Integrity Check		
NAV	Network Allocation Vector		
OUI	Organizationally Unique Identifier		

IEEE 802.11 Header Reference



Address Order

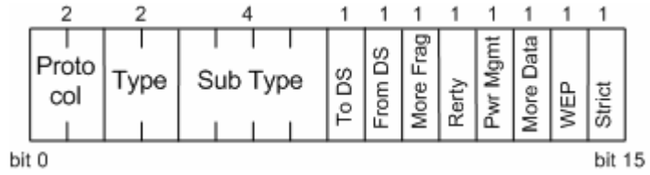
From DS Set, To DS Clear:
- Address 1: Destination
- Address 2: BSSID
- Address 3: Source

From DS Clear, To DS Set:
- Address 1: BSSID
- Address 2: Source
- Address 3: Destination

From DS Clear, To DS Clear:
- Address 1: Destination
- Address 2: Source
- Address 3: BSSID

From DS Set, To DS Set:
- Address 1: Receiver
- Address 2: Transmitter
- Address 3: Destination
- Address 4: Source

Frame Control Sub-Fields

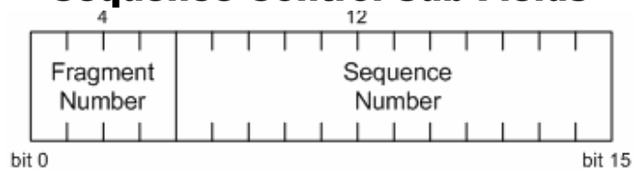


Frame Control Sub-Field Data

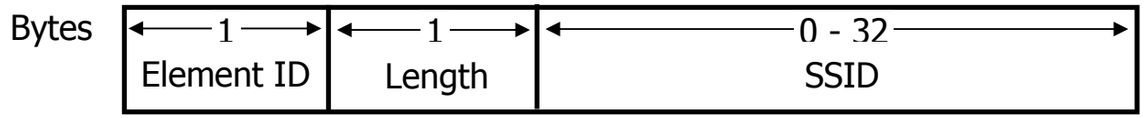
Protocol: 0, only supported protocol identifier
Type:
- 0 Management Frame
- 1 Control Frame
- 2 Data Frame

Subtype: Function of the frame based on frame type
From DS set, To DS Clear: From Wired to Wireless
From DS clear, To DS Set: From Wireless to Wired
From DS clear, To DS Clear: Ad-hoc is type is data
From DS Set, To DS Set: WDS network
More Frag: Set, more fragments remaining
Retry: Set, packet is being retransmitted
Power Management: Set, STA is entering power conservation state
More Data: Set, AP has more buffered frames for STA
WEP/Privacy Bit: Set, data frame is encrypted using WEP, TKIP or CCMP
Strict: Set, station requires frames to be delivered in order

Sequence Control Sub-Fields



Management Frame Information Element Format



Common Management Tag Values

0	SSID	1	Supported data rates
2	Frequency Hopping Channel Set	3	Direct Sequence Channel Set
4	Contention Free period	5	Traffic Indication Map
6	IBSS (Ad-hoc) parameter set	7	Country Information
0x30	RSN Information Element	0x85	Cisco CCX Extensions 1
0x88	Cisco CCX Extensions 2	0x95	Cisco CCX Extensions 3
0x2D	High Throughput (.11n) capability	0x34	AP Neighbor Report
0x3d	High Throughput (.11n) information	0x2E	QoS Capability
0x22	Transmit Power Control Request	0x23	Transmit Power Control Response
0x24	Supported Channels	0x32	Extended supported data rates

Kismet Quick Reference

Panels Reference		Popup Windows	
e	List Kismet servers	h	Help
z	Toggle full-screen view	n	Name current network
m	Toggle muting of sound	i	View detailed information for network
t	Tag or untag selected network	s	Sort network list
g	Group tagged networks	l	Show wireless card power levels
u	Ungroup current group	d	Dump printable strings
c	Show clients in current network	r	Packet rate graph
L	Lock channel hopping to selected channel	a	View network statistics
H	Return to normal channel hopping	p	Dump packet type
+/-	Expand/collapse groups	f	Follow network center
CTRL+L	Re-draw the screen	w	Track alerts
Q	Quit Kismet	x	Close popup window

Network Type Flags

P	Probe Request	A	Access Point
H	Ad-Hoc Network	T	Turbocell
G	Group	D	Data only network

Status Flags

F	Vulnerable factor configuration	T#	TCP traffic # frames identified
U#	UDP traffic # frames identified	A#	ARP traffic # frames identified
D	Address identified through DHCP	W	WEP network decrypted