

BPF Reference Guide

SYNTAX

[Protocol] [Direction] [Type] {ip/subnet/port/portrange}

PROTOCOL		DIRECTION		TYPE	
<i>Limit the match to a specific protocol. If no protocol is supplied, all protocols consistent with the type are assumed.</i>		<i>Transfer direction to and/or from the type. If no direction is supplied, 'src or dst' is assumed.</i>		<i>Type of entity, port, or range of ports. If no type is supplied, host is assumed.</i>	
ether	<i>ethernet</i>	src or dst (default)	<i>source or destination</i>	host (default)	<i>ip address</i>
fddi	<i>alias for ether</i>	src and dst	<i>source and destination</i>	net	<i>ip address or subnet</i>
icmp	<i>internet control message protocol</i>	src	<i>source only</i>	port	<i>tcp/udp port number</i>
wlan	<i>wireless lan; alias for ether</i>	dst	<i>destination only</i>	portrange	<i>range of tcp/udp ports (xxxx-xxxx)</i>
ip	<i>ipv4</i>	[proto] broadcast	proto must be ip or ether		
ip6	<i>ipv6</i>	OPERATORS			
arp	<i>address resolution protocol</i>	'='	<i>equal to</i>	' ' 'or'	<i>logical or</i>
tcp	<i>transmission control protocol</i>	'!' or 'not'	<i>not equal to</i>	'<' 'less'	<i>less than</i>
udp	<i>user datagram protocol</i>	'&&' 'and'	<i>logical and</i>	'>' 'greater'	<i>greater than</i>

COMMON EXPRESSIONS

host xxx.xxx.xxx.xxx	<i>all packets to/from a host</i>
src host xxx.xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx	<i>all packets from a source host to a destination host</i>
dst port 23	<i>all packets to port 23 (telnet)</i>
udp src net xxx.xxx.xxx && dst host xxx.xxx.xxx.xxx	<i>only udp packets from a dotted pair subnet to destination host</i>
ip6 && not net xxx.xxx.xxx	<i>only IPv6 packets outside of a dotted triple subnet</i>
src host xxx.xxx.xxx.xxx && (dst portrange xxxx-xxxx && dst net xxx.xxx.xxx)	<i>all packets from a source host to a destination port range in a dotted triple subnet</i>
dst portrange 49152-65535 && gateway xxx.xxx.xxx.xxx	<i>all packets to non-standard ports on a gateway</i>
host xxx.xxx.xxx.xxx host xxx.xxx.xxx.xxx	<i>all packets to/from host A or host B</i>

BYTE LEVEL FILTERING

ip[9]!=47	<i>all packets where IP protocol field is GRE (tunnel)</i>
ip[8]<64	<i>all packets where IP time-to-live (TTL) is less than 64</i>
icmp[0]=3	<i>all packets with ICMP message type 3 (destination unreachable)</i>
tcp[13]=32 tcp[13]=8	<i>all packets with TCP flags set to PSH or URG</i>

HOW TO READ PACKET HEADERS

Word 0																															
Byte Offset 0								Byte Offset 1								Byte Offset 2								Byte Offset 3							
Nibble 0				Nibble 1				Nibble 2				Nibble 3				Nibble 4				Nibble 5				Nibble 6				Nibble 7			
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

TCP HEADER - RFC 793																																	
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31																																	
Offset 0								Offset 1								Offset 2								Offset 3									
Source Port Number																Destination Port Number																	
Offset 4								Offset 5								Offset 6								Offset 7									
Sequence Number																																	
Offset 8								Offset 9								Offset 10								Offset 11									
Acknowledgement Number																																	
Offset 12								Offset 13								Offset 14								Offset 15									
Hacker Length				Reserved				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size																	
Offset 16								Offset 17								Offset 18								Offset 19									
Checksum																Urgent Pointer																	
Offset 20								Offset 21								Offset 22								Offset 23									
TCP Options																																	
Data																																	

UDP HEADER - RFC 768																															
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31																															
Offset 0								Offset 1								Offset 2								Offset 3							
Source Port Number																Destination Port Number															
Offset 4								Offset 5								Offset 6								Offset 7							
Length																Checksum															
Offset 8								Offset 9								Offset 10								Offset 11							
Data																															

ICMP HEADER - RFC 792																															
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31																															
Offset 0								Offset 1								Offset 2								Offset 3							
Message Type								Message Code								Checksum															
Offset 4								Offset 5								Offset 6								Offset 7							
(Variable Contents Depending on Type and Code)																															

IPv4 HEADER – RFC 791																																			
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
Offset 0				Offset 1								Offset 2								Offset 3															
Version		IP Header Length		Type of Service								Total Length (in Offsets)																							
Offset 4				Offset 5								Offset 6								Offset 7															
IP Identification Number																x	D	M	Fragment Offset																
Offset 8				Offset 9								Offset 10								Offset 11															
Time to Live (TTL)				Protocol								Header Checksum																							
Offset 12				Offset 13								Offset 14								Offset 15															
Source IP Address																																			
Offset 16				Offset 17								Offset 18								Offset 19															
Destination IP Address																																			
Offset 20				Offset 21								Offset 22								Offset 23															
IP Options																																			
Data																																			

FLAGS
 x = Reserved D = Do Not Fragment M = More Fragments Follow

IPv6 HEADER – RFC 2460																															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Offset 0				Offset 1								Offset 2								Offset 3											
Version		Traffic Class								Flow Label																					
Offset 4				Offset 5								Offset 6								Offset 7											
Payload Length																Next Header								Hop Limit							
Offset 8				Offset 9								Offset 10								Offset 11											
Source IP Address																															
Offset 12				Offset 13								Offset 14								Offset 15											
Source IP Address (continued)																															
Offset 16				Offset 17								Offset 18								Offset 19											
Source IP Address (continued)																															
Offset 20				Offset 21								Offset 22								Offset 23											
Source IP Address (continued)																															
Offset 24				Offset 25								Offset 26								Offset 27											
Destination IP Address																															
Offset 28				Offset 29								Offset 30								Offset 31											
Destination IP Address (continued)																															
Offset 32				Offset 33								Offset 34								Offset 35											
Destination IP Address (continued)																															
Offset 36				Offset 37								Offset 38								Offset 39											
Destination IP Address (continued)																															
Offset 40				Offset 41								Offset 42								Offset 43											
Net Header				Extension Header Information																											
Extension Header																															
Data																															