



CAPTURE FILTERS

ARP

ARP arp

MAC FILTERS

Ether Host ether host 00:11:95:2f:cc:cc
 Mac Address ether host 00:11:95:2f:cc:cc
 Eth Source First 3 Bytes ether.src [6 :3] == 00:11:95
 LLDP (802.1AB) ether dst 01:80:c2:00:cc:0e
 MAC This PC ether host 00:16:35:ee:ee:eb
 MAC 2 ether host 00:16:35:ee:ee:eb

IP FILTERS

Dest Host dst host 10.10.1.1
 IP h
 IP#2 host 192.168.20.32
 Host host 10.10.1.1
 Host Name host www.gearbit.com
 Source Host srd host 10.10.1.1
 IP Addr & Port host 10.10.10.1 && port 80
 IP Addr & Not Port 80 host 192.168.1.100 && not port 80
 IP Add or IP Address host 192.168.1.100 or host 192.168.1.101

BROADCAST & MULTICAST FILTERS

IP Multicast ip multicast
 Ethernet Multicast ether multicast
 Broadcast ether broadcast
 Broadcast xxx.xxx.xxx.255 || xxx.xxx.xxx.0
 Broadcast (ip[19]=0xff) || (ip[19]=0x00)

DNS

DNS Zone Transfer tcp && dst port 53

ICMP

All ICMP Except Ping icmp && icmp[0] != 8 && icmp[0] != 0
 Fragment Needed But DF Flag Set
 (icmp[0] = 3) && (icmp[1] = 4)
 Fragmented ICMP icmp && (ip[6:1] & 0x20 != 0)
 In Out Going Smurf Attack icmp && (ip[19:1] = 255)
 In Out Going Frag Attack icmp && ip[6:2] & 16383 != 0
 Loki Filter ((icmp[0] = 0) || (icmp[0] = 8)) &&
 ((icmp[6:2]= 0xf001) || (icmp[6:2] =
 0x01f0))
 ICMP Addr Mask Requests icmp[0] = 17
 Frag required but DF set ((icmp[0] = 3) && (icmp[1] = 4))
 Source Route Failed (icmp[0] = 3) && (icmp[1] = 5)
 Source Quench icmp[0] = 4
 Redirect icmp[0] = 5
 Router Advertisement icmp[0] = 9
 Router Solicitation icmp[0] = 10
 Parameter Problem icmp[0] = 12
 Timestamp Request icmp[0] = 13
 Timestamp Reply icmp[0] = 14
 Information Request icmp[0] = 15
 Information reply icmp[0] = 16
 Address Mask Request icmp[0] = 17
 Address Mask Reply icmp[0] = 18
 ICMP ip proto \ icmp

SPECIFIC ETHER TYPE

Reverse ARP ip proto rarp
 DHCP & BOOTP udp port 67 or udp port 68
 CDP, VTP, other Cisco Ether dst 01:00:0c:cc:cc:cc
 RARP ether proto 8035
 Apple Talk atlak
 IP ether proto 0800
 IP Ver 6 ip6
 Dec Net dec-net



LAT ether proto 6004
 Netbeui netbeui

PROTOCOL & PORTS

ICMP proto \icmp
 IGMP and DVMRP proto 2
 IPX Ethernet_II ether proto 0x8137

HTTP

HTTP Port 80 port 80
 HTTP Source Port 80 src port 80
 HTTP Destination Port 80 dst port 80
 Incoming HTTP Requests (tcp[13:1]&18 = 2) && (port 80) && (ip dst 192.168.1.40)
 TCP ip proto tcp
 Port 80 tcp[0:2] = 80

FTP

FTP ftp
 FTP tcp[0:2] = 21 || tcp[2:2] == 21
 FTP tcp port 20 or tcp port 21
 LLDP (802.1AB) ether dst 01:80:c2:00:00:0e

UDP

UDP udp
 IP ether proto \ip

TFTP
 udp port 69

TELNET

TELNET tcp[2:2] = 23
 TELENT (tcp[(tcp[12]>>2):2] > 0xffff) &&
 (tcp[(tcp[12]>>2):2] < 0xffff)

TCP

TCP all tcp
 TCP Port port 80
 TCP Port port http
 Time To Live tcp=1 ip[8]
 SYN tcp[13] & 0x02=2
 Time To Live ip[8]

TCP Basic Filter tcp[13] = 2 /*
 TCP Source Port tcp[0:2]
 TCP Destination Port tcp[2:2]
 TCP FINAL tcp[13] & 0x01 = 0x01
 TCP SYN 1 tcp[13] & 0x02 = 0x02
 TCP SYN 2 tcp.flags.syn == 1
 TCP SYN 3 tcp.flags == 0x02
 TCP RST tcp[13] & 0x04 = 0x04
 TCP All Flags tcp[13] & 0x07 != 0
 TCP PUSH tcp-push
 TCP URGENT tcp-urg

TCP Zero Window Size WITHOUT a reset
 tcp.window_size==0 && !(tcp.flags==0x14) &&
 !(tcp.flags==0x04)tcp.window_size==0 && !(tcp.flags.reset == 1)

TCP All External to 192.168.1.0/24
 tcp and not (src net 192.168.1 && dst net 192.168.1)

ROUTING PROTOCOLS

OSPF ip proto 89
 PVST+ ether dst 01:00:0c:cc:cc:cd
 RIP udp port 520 and dst net 255.255.255.255
 RIPv2 udp port 520 and dst net 224.0.0.9

NETWORK & HOST TO HOST

Network Address net 192.168
 Source Network Address src net 192.168
 Dest Network Address dst net 192.168
 Host to Host host 10.10.10.1 and host 10.10.10.2

SMTP

SMTP All
 port 25 and (tcp[12] & 0xf0>0x50 or tcp[20:4] = 0x48454C4F or tcp[20:4] = 0x4D41494C or tcp[20:4] = 0x52435054 or tcp[20:4] = 0x44415441 or tcp[20:4] = 0x52534554 or tcp[20:4] = 0x53454E44 or tcp[20:4] = 0x534F4D4C or tcp[20:4] = 0x53414D4C or tcp[20:4] = 0x56524659 or tcp[20:4] = 0x4558504E or tcp[20:4] = 0x4E4F4F50 or tcp[20:4] = 0x51554954 or tcp [20:4] = 0x5455524E)

UDP HEADER

Source Port	Destination Port
Length	Checksum

UDP DETAIL

Common UDP Well-Known Server Ports

7 echo	138 netbios-dgm
19 chargen	161 snmp
37 time	162 snmp-trap
53 domain	500 isakmp
67 bootps (DHCP)	514 syslog
68 bootpc (DHCP)	520 rip
69 tftp	33434 traceroute
137 netbios-ns	

Length (Number of bytes in entire datagram including ; minimum value = 8)

Checksum (Covers pseudo- and entire UDP datagram)

ARP HEADER

Hardware Address Type		Protocol Address Type
H/w Addr Len	Prot. Addr Len	Operation
Source Hardware Address		
Source Hardware Addr (cont.)		Source Protocol Address
Source Protocol Addr (cont.)		Target Hardware Address
Target Hardware Address (cont.)		
Target Protocol Address		

ARP Parameters (for Ethernet and IPv4)

Hardware Address Type

- 1 Ethernet
- 6 IEEE 802 LAN

Protocol Address Type

2048 IPv4 (0x0800)

Hardware Address Length

6 for Ethernet/IEEE 802

Protocol Address Length

4 for IPv4

Operation

- 1 Request
- 2 Reply

DNS HEADER

LENGTH (TCP ONLY)							
ID.							
QR	Opcode	AA	TC	RD	RA	Z	RCODE
QDCOUNT							
ANCOUNT							
NSCOUNT							
ARCOUNT							
Question Section							
Answer Section							
Authority Section							
Additional Information Section							

Query/Response

- 0 Query
- 1 Response

Opcode

- 0 Standard query (QUERY)
- 1 Inverse query (IQUERY)
- 2 Server status request (STATUS)

AA (1 = Authoritative Answer)

TC (1 = TrunCation)

RD (1 = Recursion Desired)

RA (1 = Recursion Available)

Z (Reserved; set to 0)

Response code

- 0 No error
- 1 Format error
- 2 Server failure
- 3 Non-existent domain (NXDOMAIN)
- 4 Query type not implemented
- 5 Query refused

QDCOUNT (No. of entries in Question section)

ANCOUNT(No. of resource records in Answer section)

NSCOUNT(No. of name server resource records in Authority section)

ARCOUNT (No. of resource records in Additional Information section.)

TCP HEADER

Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Offset (Header Length)	Reserved	Flags	Window
Checksum		Urgent Pointer	
Options (optional)			

Common TCP Well-Known Server Ports

7	echo	110	pop3
19	chargen	111	sunrpc
20	ftp-data	119	nntp
21	ftp-control	139	netbios-ssn
22	ssh	143	imap
23	telnet	179	bgp
25	smtp	389	ldap
53	domain	443	https (ssl)
79	finger	445	microsoft-ds
80	http	1080	socks

Flags (CEUAPRSF)

ECN bits (used when ECN employed; else 00)

CWR (1 = sender has cut congestion window in half)

ECN-Echo (1 = receiver cuts congestion window in half)

U (1 = Urgent pointer valid)

A (1 = Acknowledgement field value valid)

P (1 = Push data)

R (1 = Reset connection)

S (1 = Synchronize sequence numbers)

F (1 = no more data; Finish connection)

Checksum-Covers pseudo and entire TCP segment

Urgent Pointer-Points to the seq number of the byte following urgent data.

Options

0 End of Options list 3 Window scale

1 No operation (pad) 4 Selective ACK ok

2 Maximum segment size 8 Timestamp



Products | Services | Training

PO Box 91059, Austin, TX 78709-1059

www.gearbit.com sales@gearbit.com

IP HEADER

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options (optional)				

IP DETAIL

Version IP version 4

Internet Length

Number of 32-bit words in IP ; minimum

value = 5 (20 bytes) & maximum value = 15 (60 bytes)

Type of Service (PreDTRCx) --> Differentiated Services

Precedence (000-111) 000

D (1 = minimize delay) 0

T (1 = max throughput) 0

R (1 = max reliability) 0

C (1 = minimize cost) 1 = ECN capable

x (reserved and set to 0) 1 = congestion experienced

Total Length Number of Bytes in Packet

Normal 1514 plus 4 CRC TOTAL 1518

JUMBO packet; maximum length = 65,535

Flags (xDM)

x (reserved and set to 0)

D (1 = Don't Fragment)

M (1 = More Fragments)

Fragment Offset

Position of this fragment in the original datagram,
in units of 8 bytes

Protocol

1 ICMP 17 UDP 57 SKIP

2 IGMP 47 GRE 88 EIGRP
6 TCP 50 ESP 89 OSPF
9 IGRP 51 AH 115 L2TP

Checksum

Covers IP only

Addressing

NET_ID RFC 1918 PRIVATE ADDRESSES

0-127 Class A 10.0.0.0-10.255.255.255

128-191 Class B 172.16.0.0-172.31.255.255

192-223 Class C 192.168.0.0-192.168.255.255

224-239 Class D (multicast)

240-255 Class E (experimental)

255 Broadcast

Options (0-40 bytes; padded to 4-byte boundary)

0 End of Options list 68 Timestamp

1 No operation (pad) 131 Loose source route

7 Record route 137 Strict source route

ICMP HEADER

Type	Code	Checksum
Other message-specific information...		

Type Name/Codes (Code=0 unless otherwise specified)

0 Echo Reply

3 Destination Unreachable

0 Net Unreachable

1 Host Unreachable

2 Protocol Unreachable

3 Port Unreachable

4 Fragmentation Needed & DF Set

5 Source Route Failed

6 Destination Network Unknown



Products | Services | Training

PO Box 91059, Austin, TX 78709-1059

www.gearbit.com sales@gearbit.com

- 7 Destination Host Unknown
- 8 Source Host Isolated
- 9 Network Administratively Prohibited
- 10 Host Administratively Prohibited
- 11 Network Unreachable for TOS
- 12 Host Unreachable for TOS
- 13 Communication Administratively Prohibited
- 4 Source Quench
- 5 Redirect
 - 0 Redirect Datagram for the Network
 - 1 Redirect Datagram for the Host
 - 2 Redirect Datagram for the TOS & Network
 - 3 Redirect Datagram for the TOS & Host
- 8 Echo
- 9 Router Advertisement
- 10 Router Selection
- 11 Time Exceeded
 - 0 Time to Live exceeded in Transit
 - 1 Fragment Reassembly Time Exceeded
- 12 Parameter Problem
 - 0 Pointer indicates the error
 - 1 Missing a Required Option
 - 2 Bad Length
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply
- 17 Address Mask Request
- 18 Address Mask Reply
- 30 Traceroute

