Wireshark Capture Filters

Examples

Capture only traffic to or from IP address 172.18.5.4:

- host 172.18.5.4

Capture traffic to or from a range of IP addresses:

- net 192.168.0.0/24

or

- net 192.168.0.0 mask 255.255.255.0

Capture traffic from a range of IP addresses:

- src net 192.168.0.0/24

or

- src net 192.168.0.0 mask 255.255.255.0

Capture traffic to a range of IP addresses:

- dst net 192.168.0.0/24

or

- dst net 192.168.0.0 mask 255.255.255.0

Capture only DNS (port 53) traffic:

- port 53

Capture non-HTTP and non-SMTP traffic on your server (both are equivalent):

- host www.example.com and not (port 80 or port 25)

  host www.example.com and not port 80 and not port 25

Capture except all ARP and DNS traffic:

- port not 53 and not arp

Capture traffic within a range of ports

- (tcp[0:2] > 1500 and tcp[0:2] < 1550) or (tcp[2:2] > 1500 and tcp[2:2] < 1550)

or, with newer versions of libpcap (0.9.1 and later):

- tcp portrange 1501-1549

Capture only Ethernet type EAPOL:

- ether proto 0x888e

Reject ethernet frames towards the Link Layer Discovery Protocol Multicast group:

- not ether dst 01:80:c2:00:00:0e

Capture only IP traffic - the shortest filter, but sometimes very useful to get rid of lower layer protocols like ARP and STP:

- ip

Capture only unicast traffic - useful to get rid of noise on the network if you only want to see traffic to and from your machine, not, for example, broadcast and multicast announcements:

- not broadcast and not multicast

Capture IPv6 "all nodes" (router and neighbor advertisement) traffic. Can be used to find rogue RAs:

- dst host ff02::1

Capture HTTP GET requests. This looks for the bytes 'G', 'E', 'T', and ' ' (hex values 47, 45, 54, and 20) just after the TCP header. "tcp[12:1] & 0xf0) >> 2" figures out the TCP header length. From Jefferson Ogata via the tcpdump-workers mailing list.

- port 80 and tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420

Wireshark Display Filters · Part 1

packetlife.net

Ethernet

eth.addr	eth.len	eth.src
eth.dst	eth.lg	eth.trailer
eth.ig	eth.multicast	eth.type

IEEE 802.1Q

vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer

IPv4

ip.addr	ip.fragment.overlap.conflict
ip.checksum	ip.fragment.toolongfragment
ip.checksum_bad	ip.fragments
ip.checksum_good	ip.hdr_len
ip.dsfield	ip.host
ip.dsfield.ce	ip.id
ip.dsfield.dscp	ip.len
ip.dsfield.ect	ip.proto
ip.dst	ip.reassembled_in
ip.dst_host	ip.src
ip.flags	ip.src_host
ip.flags.df	ip.tos
ip.flags.mf	ip.tos.cost
ip.flags.rb	ip.tos.delay
ip.frag_offset	ip.tos.precedence
ip.fragment	ip.tos.reliability
ip.fragment.error	ip.tos.throughput
ip.fragment.multipletails	ip.ttl
ip.fragment.overlap	ip.version

IPv6

ipv6.addr	ipv6.hop_opt
ipv6.class	ipv6.host
ipv6.dst	ipv6.mipv6_home_address
ipv6.dst_host	ipv6.mipv6_length
ipv6.dst_opt	ipv6.mipv6_type
ipv6.flow	ipv6.nxt
ipv6.fragment	ipv6.opt.pad1
ipv6.fragment.error	ipv6.opt.padn
ipv6.fragment.more	ipv6.plen
ipv6.fragment.multipletails	ipv6.reassembled_in
ipv6.fragment.offset	ipv6.routing_hdr
ipv6.fragment.overlap	ipv6.routing_hdr.addr
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type
ipv6.fragments	ipv6.src
ipv6.fragment.id	ipv6.src_host
ipv6.hlim	ipv6.version

ARP

arp.dst.hw_mac	arp.proto.size
arp.dst.proto_ipv4	arp.proto.type
arp.hw.size	arp.src.hw_mac
arp.hw.type	arp.src.proto_ipv4
arp.opcode	

TCP

tcp.ack	tcp.options.qs
tcp.checksum	tcp.options.sack
tcp.checksum_bad	tcp.options.sack_le
tcp.checksum_good	tcp.options.sack_perm
tcp.continuation_to	tcp.options.sack_re
tcp.dstport	tcp.options.time_stamp
tcp.flags	tcp.options.wscale
tcp.flags.ack	tcp.options.wscale_val
tcp.flags.cwr	tcp.pdu.last_frame
tcp.flags.ecn	tcp.pdu.size
tcp.flags.fin	tcp.pdu.time
tcp.flags.push	tcp.port
tcp.flags.reset	tcp.reassembled_in
tcp.flags.syn	tcp.segment
tcp.flags.urg	tcp.segment.error
tcp.hdr_len	tcp.segment.multipletails
tcp.len	tcp.segment.overlap
tcp.nxtseq	tcp.segment.overlap.conflict
tcp.options	tcp.segment.toolongfragment
tcp.options.cc	tcp.segments
tcp.options.ccecho	tcp.seq
tcp.options.ccnew	tcp.srcport
tcp.options.echo	tcp.time_delta
tcp.options.echo_reply	tcp.time_relative
tcp.options.md5	tcp.urgent_pointer
tcp.options.mss	tcp.window_size
tcp.options.mss_val	

UDP

udp.checksum	udp.dstport	udp.srcport
udp.checksum_bad	udp.length	
udp.checksum_good	udp.port	

Operators

eq or **==**
ne or **!=**
gt or **>**
lt or **<**
ge or **>=**
le or **<=**

Logic

and or **&&**	Logical AND
or or **||**	Logical OR
xor or **^^**	Logical XOR
not or **!**	Logical NOT
[n] […]	Substring operator

Wireshark Display Filters · Part 2

packetlife.net

Frame Relay

- fr.becn
- fr.chdlctype
- fr.control
- fr.control.f
- fr.control.ftype
- fr.control.n_r
- fr.control.n_s
- fr.control.p
- fr.control.s_ftype
- fr.control.u_modifier_cmd
- fr.control.u_modifier_resp
- fr.cr
- fr.dc
- fr.de
- fr.dlci
- fr.dlcore_control
- fr.ea
- fr.fecn
- fr.lower_dlci
- fr.nlpid
- fr.second_dlci
- fr.snap.oui
- fr.snap.pid
- fr.snaptype
- fr.third_dlci
- fr.upper_dlci

PPP

- ppp.address
- ppp.control
- ppp.direction
- ppp.protocol

MPLS

- mpls.bottom
- mpls.cw.control
- mpls.cw.res
- mpls.exp
- mpls.label
- mpls.oam.bip16
- mpls.oam.defect_location
- mpls.oam.defect_type
- mpls.oam.frequency
- mpls.oam.function_type
- mpls.oam.ttsi
- mpls.ttl

ICMP

- icmp.checksum
- icmp.checksum_bad
- icmp.code
- icmp.ident
- icmp.mtu
- icmp.redir_gw
- icmp.seq
- icmp.type

DTP

- dtp.neighbor
- dtp.tlv_len
- dtp.tlv_type
- dtp.version
- vtp.neighbor

VTP

- vtp.code
- vtp.conf_rev_num
- vtp.followers
- vtp.md
- vtp.md5_digest
- vtp.md_len
- vtp.seq_num
- vtp.start_value
- vtp.upd_id
- vtp.upd_ts
- vtp.version
- vtp.vlan_info.802_10_index
- vtp.vlan_info.isl_vlan_id
- vtp.vlan_info.len
- vtp.vlan_info.mtu_size
- vtp.vlan_info.status.vlan_susp
- vtp.vlan_info.tlv_len
- vtp.vlan_info.tlv_type
- vtp.vlan_info.vlan_name
- vtp.vlan_info.vlan_name_len
- vtp.vlan_info.vlan_type

ICMPv6

- icmpv6.all_comp
- icmpv6.checksum
- icmpv6.checksum_bad
- icmpv6.code
- icmpv6.comp
- icmpv6.haad.ha_addrs
- icmpv6.identifier
- icmpv6.option
- icmpv6.option.cga
- icmpv6.option.length
- icmpv6.option.name_type
- icmpv6.option.name_type.fqdn
- icmpv6.option.name_x501
- icmpv6.option.rsa.key_hash
- icmpv6.option.type
- icmpv6.ra.cur_hop_limit
- icmpv6.ra.reachable_time
- icmpv6.ra.retrans_timer
- icmpv6.ra.router_lifetime
- icmpv6.recursive_dns_serv
- icmpv6.type

RIP

- rip.auth.passwd
- rip.auth.type
- rip.command
- rip.family
- rip.ip
- rip.metric
- rip.netmask
- rip.next_hop
- rip.route_tag
- rip.routing_domain
- rip.version

BGP

- bgp.aggregator_as
- bgp.aggregator_origin
- bgp.as_path
- bgp.cluster_identifier
- bgp.cluster_list
- bgp.community_as
- bgp.community_value
- bgp.local_pref
- bgp.mp_nlri_tnl_id
- bgp.mp_reach_nlri_ipv4_prefix
- bgp.mp_unreach_nlri_ipv4_prefix
- bgp.multi_exit_disc
- bgp.next_hop
- bgp.nlri_prefix
- bgp.origin
- bgp.originator_id
- bgp.type
- bgp.withdrawn_prefix

HTTP

- http.accept
- http.accept_encoding
- http.accept_language
- http.authbasic
- http.authorization
- http.cache_control
- http.connection
- http.content_encoding
- http.content_length
- http.content_type
- http.cookie
- http.date
- http.host
- http.last_modified
- http.location
- http.notification
- http.proxy_authenticate
- http.proxy_authorization
- http.proxy_connect_host
- http.proxy_connect_port
- http.referer
- http.request
- http.request.method
- http.request.uri
- http.request.version
- http.response
- http.response.code
- http.server
- http.set_cookie
- http.transfer_encoding
- http.user_agent
- http.www_authenticate
- http.x_forwarded_for