Wireshark Filters – Part 1

ARP

- arp.dst.hw
- arp.dst.hw_mac
- arp.dst.pln
- arp.dst.proto
- arp.dst.proto_ipv4
- arp.duplicate-address-detected
- arp.duplicate-address-frame
- arp.hw.size
- arp.hw.type
- arp.isgratuitous
- arp.opcode
- arp.packet-storm-detected
- arp.proto.size
- arp.proto.type
- arp.seconds-since-duplicate-address-frame
- arp.src.hw
- arp.src.hw_mac
- arp.src.pln
- arp.src.proto
- arp.src.proto_ipv4

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.ssa_l2tpv3_cookie
- bgp.ssa_l2tpv3_cookie_len
- bgp.ssa_l2tpv3_pref
- bgp.ssa_l2tpv3_s
- bgp.ssa_l2tpv3_session_id
- bgp.ssa_l2tpv3_Unused
- bgp.ssa_len
- bgp.ssa_t
- bgp.ssa_type
- bgp.ssa_value
- bgp.type
- bgp.withdrawn_prefix

CHAP

- chap.code
- chap.identifier
- chap.length
- chap.message
- chap.name
- chap.value
- chap.value_size

CPHA

- cpha.cluster_number
- cpha.dst_id
- cpha.ethernet_addr
- cpha.filler
- cpha.ha_mode
- cpha.ha_time_unit
- cpha.hash_len
- cpha.id_num
- cpha.if_trusted
- cpha.ifn
- cpha.in_assume_up
- cpha.in_up
- cpha.ip
- cpha.machine_num
- cpha.magic_number
- cpha.opcode
- cpha.out_assume_up
- cpha.out_up
- cpha.policy_id
- cpha.random_id
- cpha.reported_ifs
- cpha.seed
- cpha.slot_num
- cpha.src_id
- cpha.src_if
- cpha.status
- cpha.version

HSRP

- hsrp.adv.activegrp
- hsrp.adv.passivegrp
- hsrp.adv.reserved1
- hsrp.adv.reserved2
- hsrp.adv.state
- hsrp.adv.tlvlength
- hsrp.adv.tlvtype
- hsrp.auth_data
- hsrp.group
- hsrp.hellotime
- hsrp.holdtime
- hsrp.md5_ip_address
- hsrp.opcode
- hsrp.priority
- hsrp.reserved
- hsrp.state
- hsrp.version
- hsrp.virt_ip
- hsrp2._md5_algorithm
- hsrp2._md5_flags
- hsrp2.active_groups
- hsrp2.auth_data
- hsrp2.group
- hsrp2.group_state_tlv
- hsrp2.hellotime
- hsrp2.holdtime
- hsrp2.identifier
- hsrp2.interface_state_tlv
- hsrp2.ipversion
- hsrp2.md5_auth_data
- hsrp2.md5_auth_tlv
- hsrp2.md5_key_id
- hsrp2.opcode
- hsrp2.passive_groups
- hsrp2.priority
- hsrp2.state
- hsrp2.text_auth_tlv
- hsrp2.version
- hsrp2.virt_ip
- hsrp2.virt_ip_v6

EIGRP

- eigrp.ack
- eigrp.as
- eigrp.at_cbl.routerid
- eigrp.at_ext.as
- eigrp.at_ext.bandwidth
- eigrp.at_ext.delay
- eigrp.at_ext.flags
- eigrp.at_ext.flags.default
- eigrp.at_ext.flags.ext
- eigrp.at_ext.hopcount
- eigrp.at_ext.load
- eigrp.at_ext.metric
- eigrp.at_ext.mtu
- eigrp.at_ext.origrouter
- eigrp.at_ext.proto
- eigrp.at_ext.reliability
- eigrp.at_ext.reserved
- eigrp.at_ext.tag
- eigrp.at_int.bandwidth
- eigrp.at_int.delay
- eigrp.at_int.hopcount
- eigrp.at_int.load
- eigrp.at_int.mtu
- eigrp.at_int.reliability
- eigrp.at_int.reserved
- eigrp.auth.data
- eigrp.auth.keyid
- eigrp.auth.keysize
- eigrp.auth.nullapd
- eigrp.auth.type
- eigrp.checksum
- eigrp.flags
- eigrp.flags.condrecv
- eigrp.flags.init
- eigrp.ip_ext.as
- eigrp.ip_ext.bandwidth
- eigrp.ip_ext.delay
- eigrp.ip_ext.flags
- eigrp.ip_ext.flags.default
- eigrp.ip_ext.flags.ext
- eigrp.ip_ext.hopcount
- eigrp.ip_ext.load
- eigrp.ip_ext.metric
- eigrp.ip_ext.mtu
- eigrp.ip_ext.nexthop
- eigrp.ip_ext.origrouter
- eigrp.ip_ext.prefixlen
- eigrp.ip_ext.proto
- eigrp.ip_ext.reliability
- eigrp.ip_ext.reserved
- eigrp.ip_ext.reserved2
- eigrp.ip_ext.tag
- eigrp.ip_int.bandwidth
- eigrp.ip_int.delay
- eigrp.ip_int.dst
- eigrp.ip_int.hopcount
- eigrp.ip_int.load
- eigrp.ip_int.mtu
- eigrp.ip_int.nexthop
- eigrp.ip_int.prefixlen
- eigrp.ip_int.reliability
- eigrp.ip_int.reserved
- eigrp.nms
- eigrp.opcode
- eigrp.par.holdtime
- eigrp.par.k1
- eigrp.par.k2
- eigrp.par.k3
- eigrp.par.k4
- eigrp.par.k5
- eigrp.par.reserved
- eigrp.seq
- eigrp.seq.addrlen
- eigrp.seq.ip6addr
- eigrp.seq.ipaddr
- eigrp.stub_flags
- eigrp.stub_flags.connected
- eigrp.stub_flags.leakmap
- eigrp.stub_flags.recvonly
- eigrp.stub_flags.redist
- eigrp.stub_flags.static
- eigrp.stub_flags.summary
- eigrp.sv.eigrp
- eigrp.sv.ios
- eigrp.tlv
- eigrp.tlv.size
- eigrp.version

ESP

- esp.iv
- esp.pad_len
- esp.protocol
- esp.sequence
- esp.spi

Ethernet

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

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_length_header
- 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

Wireshark Filters – Part 2

GLBP

- glbp.auth.authlength
- glbp.auth.authtype
- glbp.auth.authunknown
- glbp.auth.md5chainhash
- glbp.auth.md5chainindex
- glbp.auth.md5hash
- glbp.auth.plainpass
- glbp.group
- glbp.hello.addrlen
- glbp.hello.addrtype
- glbp.hello.helloint
- glbp.hello.holdint
- glbp.hello.priority
- glbp.hello.redirect
- glbp.hello.timeout
- glbp.hello.unknown10
- glbp.hello.unknown11
- glbp.hello.unknown12
- glbp.hello.unknown13
- glbp.hello.vgstate
- glbp.hello.virtualipv4
- glbp.hello.virtualipv6
- glbp.hello.virtualunk
- glbp.length
- glbp.ownerid
- glbp.reqresp.forwarder
- glbp.reqresp.priority
- glbp.reqresp.unknown21
- glbp.reqresp.unknown22
- glbp.reqresp.vfstate
- glbp.reqresp.virtualmac
- glbp.reqresp.weight
- glbp.tlv
- glbp.type
- glbp.unknown.data
- glbp.unknown1
- glbp.unknown2
- glbp.version

ICAP

- icap.options
- icap.other
- icap.reqmod
- icap.respmod
- icap.response

ICMP

- icmp.checksum
- icmp.checksum_bad
- icmp.code
- icmp.ident
- icmp.mip.b
- icmp.mip.challenge
- icmp.mip.coa
- icmp.mip.f
- icmp.mip.flags
- icmp.mip.g
- icmp.mip.h
- icmp.mip.length
- icmp.mip.life
- icmp.mip.m
- icmp.mip.prefixlength
- icmp.mip.r
- icmp.mip.reserved
- icmp.mip.rt
- icmp.mip.seq
- icmp.mip.type
- icmp.mip.u
- icmp.mip.v
- icmp.mip.x
- icmp.mpls
- icmp.mpls.checksum
- icmp.mpls.checksum_bad
- icmp.mpls.class
- icmp.mpls.ctype
- icmp.mpls.exp
- icmp.mpls.label
- icmp.mpls.length
- icmp.mpls.res
- icmp.mpls.s
- icmp.mpls.ttl
- icmp.mpls.version
- icmp.mtu
- icmp.redir_gw
- icmp.seq
- icmp.seq_le
- icmp.type

PAGP

- pagp.flags
- pagp.flags.automode
- pagp.flags.slowhello
- pagp.flags.state
- pagp.flushlocaldevid
- pagp.flushpartnerdevid
- pagp.localdevid
- pagp.localearncap
- pagp.localgroupcap
- pagp.localgroupifindex
- pagp.localportpri
- pagp.localsentportifindex
- pagp.numtlvs
- pagp.partnercount
- pagp.partnerdevid
- pagp.partnergroupcap
- pagp.partnergroupifindex
- pagp.partnerlearncap
- pagp.partnerportpri
- pagp.partnersentportifindex
- pagp.tlv
- pagp.tlvagportmac
- pagp.tlvdevname
- pagp.tlvportname
- pagp.transid
- pagp.version

IPv4

- ip.addr
- ip.checksum
- ip.checksum_bad
- ip.checksum_good
- ip.dsfield
- ip.dsfield.ce
- ip.dsfield.dscp
- ip.dsfield.ect
- ip.dst
- ip.dst_host
- ip.flags
- ip.flags.df
- ip.flags.mf
- ip.flags.rb
- ip.flags.sf
- ip.frag_offset
- ip.fragment
- ip.fragment.error
- ip.fragment.multipletails
- ip.fragment.overlap
- ip.fragment.overlap.confli
- ip.fragment.toolongfragme
- ip.fragments
- ip.geoip.asnum
- ip.geoip.city
- ip.geoip.country
- ip.geoip.dst_asnum
- ip.geoip.dst_city
- ip.geoip.dst_country
- ip.geoip.dst_isp
- ip.geoip.dst_lat
- ip.geoip.dst_lon
- ip.geoip.dst_org
- ip.geoip.isp
- ip.geoip.lat
- ip.geoip.lon
- ip.geoip.org
- ip.geoip.src_asnum
- ip.geoip.src_city
- ip.geoip.src_country
- ip.geoip.src_isp
- ip.geoip.src_lat
- ip.geoip.src_lon
- ip.geoip.src_org
- ip.hdr_len
- ip.host
- ip.id
- ip.len
- ip.proto
- ip.reassembled.length
- ip.reassembled_in
- ip.src
- ip.src_host
- ip.tos
- ip.tos.cost
- ip.tos.delay
- ip.tos.precedence
- ip.tos.reliability
- ip.tos.throughput
- ip.ttl
- ip.version

ISIS

- isis.csnp.pdu_length
- isis.hello.circuit_type
- isis.hello.clv_ipv4_int_addr
- isis.hello.clv_ipv6_int_addr
- isis.hello.clv_mt
- isis.hello.clv_ptp_adj
- isis.hello.clv_restart.neighbor
- isis.hello.clv_restart.remain_time
- isis.hello.clv_restart_flags
- isis.hello.clv_restart_flags.ra
- isis.hello.clv_restart_flags.rr
- isis.hello.clv_restart_flags.sa
- isis.hello.holding_timer
- isis.hello.lan_id
- isis.hello.local_circuit_id
- isis.hello.pdu_length
- isis.hello.priority
- isis.hello.source_id
- isis.irpd
- isis.len
- isis.lsp.att
- isis.lsp.checksum
- isis.lsp.checksum_bad
- isis.lsp.checksum_good
- isis.lsp.clv_ipv4_int_addr
- isis.lsp.clv_ipv6_int_addr
- isis.lsp.clv_mt
- isis.lsp.clv_te_router_id
- isis.lsp.hostname
- isis.lsp.is_type
- isis.lsp.lsp_id
- isis.lsp.overload
- isis.lsp.partition_repair
- isis.lsp.pdu_length
- isis.lsp.remaining_life
- isis.lsp.sequence_number
- isis.max_area_adr
- isis.psnp.pdu_length
- isis.reserved
- isis.sysid_len
- isis.type
- isis.version
- isis.version2

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

Ethernet

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

Wireshark Filters – Part 3

OSPF

ospf.advrouter
ospf.dbd
ospf.dbd.i
ospf.dbd.m
ospf.dbd.ms
ospf.dbd.r
ospf.lls.ext.options
ospf.lls.ext.options.lr
ospf.lls.ext.options.rs
ospf.lsa
ospf.lsa.asbr
ospf.lsa.asext
ospf.lsa.attr
ospf.lsa.member
ospf.lsa.mpls
ospf.lsa.network
ospf.lsa.nssa
ospf.lsa.opaque
ospf.lsa.router
ospf.lsa.summary
ospf.lsid_opaque_type
ospf.lsid_te_lsa.instance
ospf.mpls.bc
ospf.mpls.linkcolor
ospf.mpls.linkid
ospf.mpls.linktype
ospf.mpls.local_addr
ospf.mpls.local_id
ospf.mpls.remote_addr
ospf.mpls.remote_id
ospf.mpls.routerid
ospf.msg
ospf.msg.dbdesc
ospf.msg.hello
ospf.msg.lsack
ospf.msg.lsreq
ospf.msg.lsupdate
ospf.oif.local_node_id
ospf.oif.remote_node_id
ospf.srcrouter
ospf.v2.grace
ospf.v2.grace.ip
ospf.v2.grace.period
ospf.v2.grace.reason
ospf.v2.options
ospf.v2.options.dc
ospf.v2.options.dn
ospf.v2.options.e
ospf.v2.options.l
ospf.v2.options.mc
ospf.v2.options.mt
ospf.v2.options.np
ospf.v2.options.o
ospf.v2.router.lsa.flags
ospf.v2.router.lsa.flags.b
ospf.v2.router.lsa.flags.e
ospf.v2.router.lsa.flags.n
ospf.v2.router.lsa.flags.v
ospf.v2.router.lsa.flags.w
ospf.v3.as.external.flags
ospf.v3.as.external.flags.e
ospf.v3.as.external.flags.f
ospf.v3.as.external.flags.t
ospf.v3.lls.drop.tlv
ospf.v3.lls.ext.options
ospf.v3.lls.ext.options.lr
ospf.v3.lls.ext.options.rs
ospf.v3.lls.ext.options.tlv
ospf.v3.lls.fsf.tlv
ospf.v3.lls.relay.added
ospf.v3.lls.relay.options
ospf.v3.lls.relay.options.a
ospf.v3.lls.relay.options.n
ospf.v3.lls.relay.tlv
ospf.v3.lls.rf.tlv
ospf.v3.lls.state.options
ospf.v3.lls.state.options.a
ospf.v3.lls.state.options.n
ospf.v3.lls.state.options.r
ospf.v3.lls.state.scs
ospf.v3.lls.state.tlv
ospf.v3.lls.willingness
ospf.v3.lls.willingness.tlv
ospf.v3.options
ospf.v3.options.af
ospf.v3.options.dc
ospf.v3.options.e
ospf.v3.options.f
ospf.v3.options.i
ospf.v3.options.l
ospf.v3.options.mc
ospf.v3.options.n
ospf.v3.options.r
ospf.v3.options.v6
ospf.v3.prefix.options
ospf.v3.prefix.options.la
ospf.v3.prefix.options.mc
ospf.v3.prefix.options.nu
ospf.v3.prefix.options.p
ospf.v3.router.lsa.flags
ospf.v3.router.lsa.flags.b
ospf.v3.router.lsa.flags.e
ospf.v3.router.lsa.flags.v
ospf.v3.router.lsa.flags.w

IPv4

ip.addr
ip.checksum
ip.checksum_bad
ip.checksum_good
ip.dsfield
ip.dsfield.ce
ip.dsfield.dscp
ip.dsfield.ect
ip.dst
ip.dst_host
ip.flags
ip.flags.df
ip.flags.mf
ip.flags.rb
ip.flags.sf
ip.frag_offset
ip.fragment
ip.fragment.error
ip.fragment.multipletails
ip.fragment.overlap
ip.fragment.overlap.confli
ip.fragment.toolongfragme
ip.fragments
ip.geoip.asnum
ip.geoip.city
ip.geoip.country
ip.geoip.dst_asnum
ip.geoip.dst_city
ip.geoip.dst_country
ip.geoip.dst_isp
ip.geoip.dst_lat
ip.geoip.dst_lon
ip.geoip.dst_org
ip.geoip.isp
ip.geoip.lat
ip.geoip.lon
ip.geoip.org
ip.geoip.src_asnum
ip.geoip.src_city
ip.geoip.src_country
ip.geoip.src_isp
ip.geoip.src_lat
ip.geoip.src_lon
ip.geoip.src_org
ip.hdr_len
ip.host
ip.id
ip.len
ip.proto
ip.reassembled.length
ip.reassembled_in
ip.src
ip.src_host
ip.tos
ip.tos.cost
ip.tos.delay
ip.tos.precedence
ip.tos.reliability
ip.tos.throughput
ip.ttl
ip.version

TCP

tcp.ack
tcp.analysis.ack_lost_segment
tcp.analysis.ack_rtt
tcp.analysis.acks_frame
tcp.analysis.bytes_in_flight
tcp.analysis.duplicate_ack
tcp.analysis.duplicate_ack_frame
tcp.analysis.duplicate_ack_num
tcp.analysis.fast_retransmission
tcp.analysis.flags
tcp.analysis.keep_alive
tcp.analysis.keep_alive_ack
tcp.analysis.lost_segment
tcp.analysis.out_of_order
tcp.analysis.retransmission
tcp.analysis.reused_ports
tcp.analysis.rto
tcp.analysis.rto_frame
tcp.analysis.window_full
tcp.analysis.window_update
tcp.analysis.zero_window
tcp.analysis.zero_window_probe
tcp.analysis.zero_window_probe_acl
tcp.checksum
tcp.checksum_bad
tcp.checksum_good
tcp.continuation_to
tcp.data
tcp.dstport
tcp.flags
tcp.flags.ack
tcp.flags.cwr
tcp.flags.ecn
tcp.flags.fin
tcp.flags.ns
tcp.flags.push
tcp.flags.res
tcp.flags.reset
tcp.flags.syn
tcp.flags.urg
tcp.hdr_len
tcp.len
tcp.nxtseq
tcp.options
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echo_reply
tcp.options.md5
tcp.options.mood
tcp.options.mood_val
tcp.options.mss
tcp.options.mss_val
tcp.options.qs
tcp.options.sack
tcp.options.sack_le
tcp.options.sack_perm
tcp.options.sack_re
tcp.options.scps
tcp.options.scps.binding
tcp.options.scps.vector
tcp.options.scpsflags.bets
tcp.options.scpsflags.compress
tcp.options.scpsflags.nlts
tcp.options.scpsflags.reserved1
tcp.options.scpsflags.reserved2
tcp.options.scpsflags.reserved3
tcp.options.scpsflags.snack1
tcp.options.scpsflags.snack2
tcp.options.snack
tcp.options.snack.le
tcp.options.snack.offset
tcp.options.snack.re
tcp.options.snack.size
tcp.options.time_stamp
tcp.options.wscale
tcp.options.wscale_val
tcp.pdu.last_frame
tcp.pdu.size
tcp.pdu.time
tcp.port
tcp.proc.dstcmd
tcp.proc.dstpid
tcp.proc.dstuid
tcp.proc.dstuname
tcp.proc.srccmd
tcp.proc.srcpid
tcp.proc.srcuid
tcp.proc.srcuname
tcp.reassembled.length
tcp.reassembled_in
tcp.segment
tcp.segment.error
tcp.segment.multipletails
tcp.segment.overlap
tcp.segment.overlap.conflict
tcp.segment.toolongfragment
tcp.segments
tcp.seq
tcp.srcport
tcp.stream
tcp.time_delta
tcp.time_relative
tcp.urgent_pointer
tcp.window_size

VLAN 802.1Q

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

Wireshark Filters – Part 4

UDP

- udp.checksum
- udp.checksum_bad
- udp.checksum_good
- udp.dstport
- udp.length
- udp.port
- udp.proc.dstcmd
- udp.proc.dstpid
- udp.proc.dstuid
- udp.proc.dstuname
- udp.proc.srccmd
- udp.proc.srcpid
- udp.proc.srcuid
- udp.proc.srcuname
- udp.srcport

VRRP

- vrrp.addr_count
- vrrp.adver_int
- vrrp.auth_type
- vrrp.count_ip_addrs
- vrrp.ip_addr
- vrrp.ipv6_addr
- vrrp.prio
- vrrp.reserved_mbz
- vrrp.short_adver_int
- vrrp.type
- vrrp.typever
- vrrp.version
- vrrp.virt_rtr_id

Operators

eq or **==**

ne or **!=**

gt or **>**

lt or **<**

ge or **>=**

le or **<=**

contains

is present

matches

Logic

and or **&&** Logical AND

or or **||** Logical OR

xor or **^^** Logical XOR

not or **!** Logical NOT

[n] […] Substring operator