Filters Manual

PUBLISHED BY

CACE Technologies, Inc.

1949 5th Street, Suite 103

Davis, CA 95616

CACE Pilot Filters Manual

Document Revision: 1.8

Document Date: May 2010

http://www.cacetech.com

Contents

Introduction

Pilot supports filters of different kinds expanding views capabilities and Wireshark communication tools. The filters supported are:

- Wireshark capture
- Wireshark display
- Time
- Pilot

Wireshark Filters

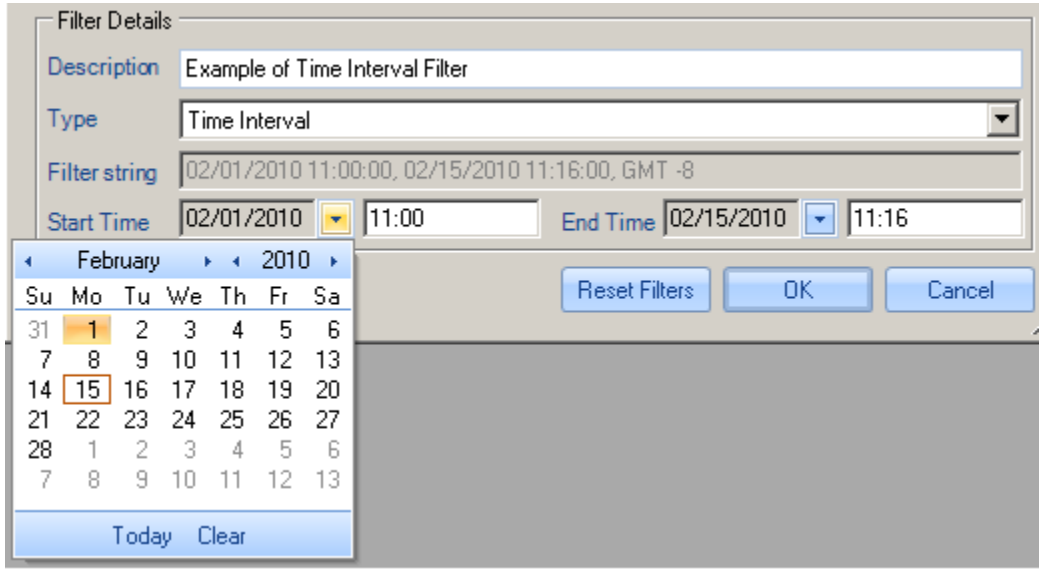
Wireshark capture filters: these filters are low level, highly efficient filters which can be applied when capturing packets. More accurate information about syntax and language is presented on the Wireshark web site http://wiki.wireshark.org/CaptureFilters

Wireshark display filters: these filters work with packets already imported and shown on the Wireshark interface. They are more flexible than the capture filters but maybe slower when used to analyze large trace files. More information is available at http://wiki.wireshark.org/DisplayFilters

Both of these filter languages are large topics and outside the scope of this document. Refer to the appropriate sources for a better understanding of their use.

Pilot Time Filters

Time filtering allows the selection of a time interval inside a trace file or live source. These filters are especially useful for selecting time intervals within massive amounts of network traffic are analyzed. The following interface is used to modify start and end time:



Pilot Filters

Filters are used by Pilot engine to filter out specific data from a trace file or live source before data are sent to a file, to Wireshark or calculated and displayed in a view. A view can be applied with an existing or a new filter created by the user. Pilot comes with a useful library of commonly used filters (capture and display filters for Wireshark and pilot filters), but users are allowed to create new filters with all these filter languages. Further, Pilot selections in a chart (bar, pie,...) correspond to filters. It is possible to view and save these "selection" filters using the chart's context menu. This is a good way to generate examples of pilot filters. In this section we are going to show how to apply, modify and create a filter in Pilot.

Apply a Filter

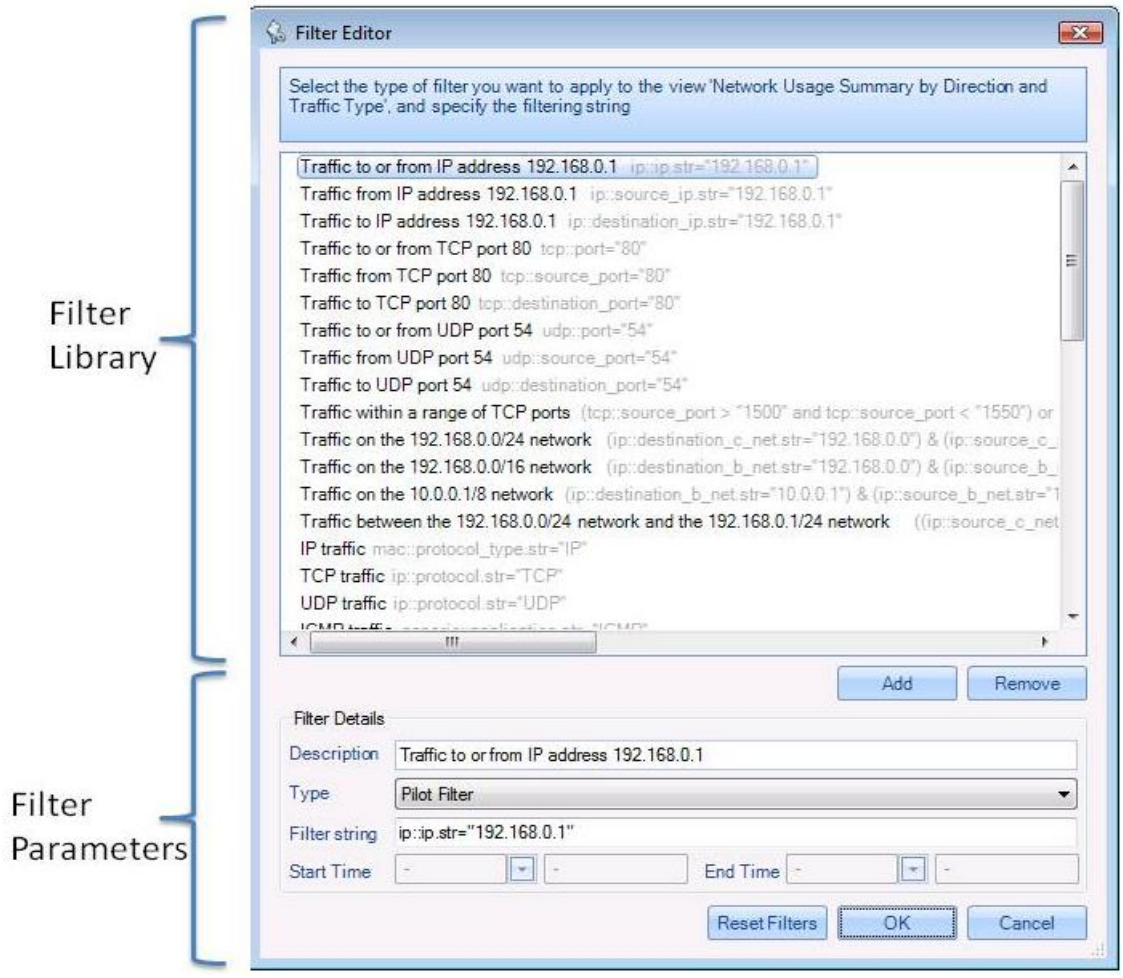
There are different ways to apply a view with a filter:

- ctrl+drag and drop of a view on a source (in source panel)
- right click on a view in the view panel-> apply with filter

In the same way it is possible to 'Send To' file or Wireshark applying a filter before data are sent out.

- right click on a source/file -> send to file/Wireshark with filter
- home ribbon button -> send to file/Wireshark with filter

The Filter Editor dialog appears after selecting any option listed above.



In order to apply filters simply select one from Filter Library and click on the OK button. The Filter Library contains a list of pre-packaged filters useful for the most common operations. The action selected (Send To or View) will be completed after data have been filtered. Please note that an incorrectly written filter may discard all incoming traffic.

Customize a Filter

Using the Filter Editor dialog is also possible to add/remove/modify existing filters. Filters can be added and removed with the Add and Remove buttons respectively or modified by simply typing in new lines. The Filter Details section allows selecting the type of filter and syntax to be used in the filter string. Pilot filer syntax is described below with helpful examples and comparisons to Wireshark filter syntax.

> Note : a modified filter is saved automatically whether OK or CANCEL is pressed.

> Note: the reset filter button removes all the custom saved filters.

Create a Filter

As described above, a new filter can be created by filling in the Filter Details and clicking the Add button. Further, Pilot offers the option of saving a filter from a selection within a chart. The saved filter can be modified in the Filter Editor as described above.

Pilot Filters Syntax

Pilot uses its own language for filters. The syntax is explained in this section and comparison with other Wireshark filters is carried out.

```
extractor::field OPERATOR "value"
```

ex: ip::ip.str != "192.168.77.2"

No space between extractor and field is allowed. The value must always be between " ". Further, no space between the " and the value is allowed. Note that Pilot filters are case sensitive.

Extractors

An extractor corresponds to a class of data elements available within a network packet. Each extractor makes a specific set of fields available for filter comparisons. Extractors available for Pilot filters include the following:

Extractor	Description
dns	Type of DNS packets, Transaction ID, Response Time etc...
generic	Repository of fields to count bytes, packets, packets length, absolute packet number or to identify IP protocol, TCP port or UDP port converted into a traffic type string (e.g. 'Email' or 'Web')
http	Type of web traffic (http, https...), HTTP request type (GET, POST, etc.), number of HTTP requests etc...
ieee80211	Fields to work with ieee802.11 wireless packets such as channels, type of encryption used, etc...
ipres	For resolution of internet domain and country of the domain
mac	Source and destination MAC address, vendor prefix, etc...
pseudo	PPI 802.11 Common / Radiotap - Channel Frequency, Channel Numbers, Types...
voip	VoIP traffic, callers and telephone numbers
tcp	Selection of TCP ports, TCP byte count, TCP packet count etc...
tcp_state	TCP round trip time, number of requests to the server, TCP error type, etc...
udp	Selection of IP source and destination, UDP packet/byte/bit count, etc

Fields

Examples of filter use are shown later.

Relational and Boolean operators

Operator Name	Symbol
OP_EQ	=
OP_LT	<
OP_GT	>

OP_IN	contains
OP_NE	!=
OP_LE	<=
OP_GE	>=

ex: ip::source_ip.str="192.168.77.250"

Operator Name	Symbol
OP_OR	|
OP_AND	&
OP_NOT	!

Ex: (ip::source_ip.str= "192.168.246.128") & (ip::destination_ip.str= "192.168.246.2")

Value format

Values used for comparison must be of a specific format, and inside the " " to avoid errors while the filter is applied.

Filter examples

Here we present a short catalog of the most useful filters.

Generic

generic::application.str

This expression depends on a set of customizable parameters better described in a section called proto-groups. The idea is to associate a list of port/protocols to a common name as 'Web' or 'Email' for frequently used filters. Thus, the language becomes more flexible and expression becomes more compact.

Ex: (generic::application.str="Email")

802.11

pseudo::80211_common.channel.str

This expression allows you to filter on packets using 802.11 channel representation strings such as BG 001, BG 002 ...

Allowed values: <BG | A | N | Nhigh | NLow> space <3 digits channel number>

Ex: (pseudo::80211_common.channel.str="BG 002")

pseudo::80211_common.channel.freq

This expression allows you to filter on packets using 802.11 channel frequency in MHz (2412,2417, ...)

Ex: (pseudo::80211_common.channel.freq="2447")

ieee80211::bssid.essid.str

This expression allows you to filter on packets using the Extended Service Set IDentifier (ESSID) string.

Ex: (ieee80211::bssid.essid.str="CACE_WIFI")

ieee80211::frame_control.source_type.str (::frame_control.destination_type.str)

This expression allows you to filter on source (destination) wireless nodes according to their function as access points (AP) or stations (STA).

Allowed values: (AP, STA)

Ex: (ieee80211::frame_control.source_type.str="AP")

pseudo::80211_common.channel.type.designator_per_station.str

This expression allows you to filter on the string of the channel type designator.

Allowed values: For PPI valid values are (A, B, G, N), for Radiotap valid values are (A, B, G)

Ex: (pseudo::80211_common.channel.type.designator_per_station.str="B")

ieee80211::frame_control.protection_type_simple.str

This filter allows to select the type of encryption used based on the AP to which the client is associated.

Allowed value: (Unknown, WEP, WPA [TKIP], WPA2 [CCMP], None)

Ex: (ieee80211::frame_control.protection_type_simple.str="WPA [TKIP]")

ieee80211::frame_control.type.str

This expression allows you to filter on the string of the frame type.

Allowed values: (Management, Control, Data, Reserved)

Ex: (ieee80211::frame_control.type.str="Data")

ieee80211::frame_control.type_subtype.str

This expression allows you to filter on the string of the frame type/subtype.

Allowed values: (Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, ATIM, Disassociation, Authentication, Deauthentication, Action, Action No Ack, Control Wrapper, Block Ack Request (BlockAckReq), Block Ack (BlockAck), PS-Poll, RTS, CTS, ACK, CF-End, CF-End + CF-Ack, Data, Data + CF-Ack, Data + CF-Poll, Data + CF-Ack + CF-Poll, Null (no data), CF-Ack (no data), CF-Poll (no data), CF-Ack + CF-Poll (no data), QoS Data, QoS Data + CF-Ack, QoS Data + CF-Poll, QoS Data + CF-Ack + CF-Poll, QoS Null (no data), QoS CF-Poll (no data), QoS CF-Ack + CF-Poll (no data))

Ex: (ieee80211::frame_control.type_subtype.str="ACK")

mac::mac.str (::source_mac.str, ::destination_mac.str)

This expression allows you to filter on Ethernet host addresses. ::mac.str selects the packets if either the source or the destination matches the value. Replace the field ::mac.str with the expressions in parenthesis if you are interested only in packets coming from a specific source or going to a specific destination address.

EX: (mac::source_mac.str="00:1d:6a:b8:a6:3f")

mac::mac.vendor.str (::source_mac.vendor.str, ::destination_mac.vendor.str)

This expression allows you to filter on vendor name. ::mac.vendor.str selects the packets if eiher the source or the destination matches the value. Replace the field ::mac.str with the expressions in parenthesis if you are interested only in packets coming from a specific source or going to a specific destination vendor.

Allowed values: values are stored in a file called manuf in the directory \server\configuration of Pilot installation.

Ex: (mac::source_mac.vendor.str="Cisco-Link")

mac::mac.vendor_with_mac.str

(::source_mac.vendor_with_mac.str, ::destination_mac.vendor_with_mac.str)

This expression allows you to filter on a string defined as destination vendor name with last 3 bytes of the MAC address. ::mac.vendor_with_mac.str selects the packets if either the source or the destination matches the value. Replace the field ::mac.str with the expressions in parenthesis if you are interested only in packets coming from a specific source or going to a specific destination address.

Ex: (mac::source_mac.vendor_with_mac.str="Cisco-Link_0c:08:78")

mac::local.str="Local" (::mac::local.str="Non Local")

The expression Local is based on the setting of subnet mask and works only for the local traffic (it does not work for probes). If the traffic is "Local" (i.e. both the source and the destination are inside the subnet) the packets are considered, otherwise the packets are discharged. Using the expression "Non Local" a packet is selected if either the source or the destination is inside the subnet.

EX: (mac::local.str="Local"))

mac::protocol_type.str

This expression allows you to filter on the specified protocol at the network layer.

Allowed values: (Unknown, IP, IPv6, ARP, RARP, XEROX, DLOG, X.75, NBS, ECMA, Chaosnet, X.25, AARP, EAPS, IPX, SNMP, MPCP, PPP, GSMP, MPLS, MPLS, PPPoE, EAPOL, AoE, LWAPP, LLDP, WSMP)

EX: (mac::protocol_type.str="IP")

mac::destination_mac.delivery_type.str (::source_mac.delivery_type.str)

This filter selects the type of delivery used for the MAC layer transmission. Destination or source can be specified.

Allowed values: (Broadcast, Multicast, Unicast)

Ex: (mac::destination_mac.delivery_type.str="Multicast")

mac::vlan.id

This expression allows you to filter on the VLAN Identifier.

Ex: (mac::vlan.id="1")

IP

ip::ip.str (::source_ip.str, ::destination_ip.str)

This expression allows you to filter on a host IP address or name. Replace the field ::ip.str with the expressions in parenthesis if you are interested only in IP source or destination address or name.

Ex: (ip::source_ip.str="74.125.155.103")

ip::destination_ip.delivery_type.str

This expression allows you to filter on IP 'Unicast', 'Broadcast', 'Multicast', 'Source-Specific Multicast' and 'GLOP'.

Allowed values: (Broadcast, Multicast, Unicast)

Ex: (ip::destination_ip.delivery_type.str="Unicast")

ip::protocol.str

This expression allows you to filter on the specified protocol at the transport layer contained in the IP protocol.

Allowed values: (TCP, UDP, ICMP, HOPOPT, IGMP, GGP, IP, ST, CBT, EGP, IGP, BBN-RCC-MON, NVP-II, PUP, ARGUS, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, RDP, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, DCCP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6 SDRP, IPv6-Route, IPv6-Frag, IDRP, RSVP, GRE, DSR, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-ICMP, IPv6-NoNxt, IPv6-Opts, CFTP, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, SAT-MON, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MON, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VMTP, VINES, TTP, NSFNET-IGP, DGP, TCF, EIGRP, OSPFIGP, Sprite-RPC, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, ENCAP, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Peer, IPX-in-IP, VRRP, PGM, L2TP, DDX, IATP, STP, SRP, UTI, SMP,SM, PTP, ISIS, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility Header, UDPLite, MPLS-in-IP)

Ex: (ip::protocol.str="TCP") or (ip::protocol.str="UDP")

ip::c_net.str (source_c_net.str, destination_c_net.str)

This filter allows you to filter on traffic coming or going to a IP Class C source or destination subnet.

Ex: (ip::c_net.str="192.168.77.0")

ipres::domain.str (::source_domain.str, ::destination_domain.str)

This filter allows you to filter on traffic coming from or going to a selected Internet Domain. It is possible to specify only source or destination with using the expressions in parenthesis.

Ex: (ipres::domain.str="1e100.net")

ip::ip.country.geoip (::source_ip.country.geoip, ::destination_ip.country.geoip)

This filter selects the Source and Destination Country Based on a GeoIP lookup. Use the expression in parenthesis to select only source or destination.

Ex: (ip::destination_ip.country.geoip="Russian Federation")

ip::source_ip.internal.str (::destination_ip.internal.str)

This filter allows specifying the IP address of the source (destination) interface if the host is in the internal net. To get all the traffic coming from (or going to) an external host use the expression "Remote".

Ex: (ip::source_ip.internal.str="Remote")

ip::fragmented_traffic

This expression allows selecting between "Fragmented" and "Not Fragmented" traffic.

Ex: (ip::fragmented_traffic="Fragmented")

ip::time_to_live

This filters specifies the maximum time (in seconds) that a datagram is allowed to survive

Ex: (ip::time_to_live="53")

TCP / UDP

tcp::ports (::source_port,::destination_port)

This expression allows you to filter on TCP port numbers. Replace the field ::ports with the expressions in parenthesis if you are interested only in TCP source or destination ports and packets respectively.

Ex: (tcp::destination_port="80")

tcp::identification_port.str

This expression allows you to use strings such as "pop3s" instead of port numbers to filter on TCP ports.

Allowed values are contained in the port-numbers file. For more information see port-numbers section.

Ex: (tcp::identification_port.str="pop3s")

tcp::flags.str

This filter allows filtering packets according to TCP flags.

Allowed values: (SYN, FIN, RST, PSH, ACK, URG, No Flags or any combination, e.g. SYN-ACK, PSH-ACK)

Ex: (tcp::flags.str="PSH-ACK")

tcp_state::error.type.str

This filter allows selecting packets according to TCP errors.

Allowed values: (Retransmissions, Timeouts, Out of Order, Lost Segments, Duplicate Acks, Zero Windows, Resets)

Ex: (tcp:: error.type.str="Reset")

tcp_state::server.address

This filter allows selecting packets specifying IP address of the hosts that receive TCP connections.

Ex: (tcp_state::server.address="87.255.33.136")

tcp_state::client.address

This filter allows selecting packets IP address of the hosts that start TCP connections.

Ex (tcp_state::client.address="192.168.77.115")

udp::ports(::source_port,::destination_port)

This expression allows you to filter on UDP port numbers. Replace the field ::ports with the expressions in parenthesis if you are interested only in UDP source or destination ports and packets respectively.

Ex: (udp::source_port="19543")

udp::identification_port.str

This expression allows you to use strings such as "DNS" instead of port numbers to filter on UDP ports.

Ex: (udp::identification_port.str="DNS")

HTTP

http::uri

This expression allows you to filter on all or part of the URI.

Ex: (http::uri contains "1A8928AF6E4E4255BBECE04056B00DA038/TC2.pdb")

http::host

This expression allows you to filter on the Host name in the http header.

Ex: (http::host contains "youtube")

http::resource

This expression allows you to filter on the HTTP resource path and name

Ex: (http::resource contains "/books?id=Vi05")

http::method

This expression allows you to filter on the HTTP request type

Allowed values: (GET, POST, HEAD, PUT, DELETE, TRACE, OPTIONS, CONNECT)

Ex: (http::method="GET")

http::content.type

This expression allows you to filter on the HTTP content type

Allowed values: any of the http mime types, see http://www.iana.org/assignments/media-types

Ex: (http::content.type contain "image")

http::status.code

This expression allows you to filter on the status code, as listed in http://en.wikipedia.org/wiki/List_of_HTTP_status_codes

Ex: (http::status.code="200")

VoIP

voip::call.user.number.str (:call.caller.number.str, ::call.receiver.number.str)

This expression allows filtering on the phone number of the caller or the receiver of the VoIP call. ::call.user.number.str is used to filter if either the caller OR the receiver matches the specified phone number. Use the expression in parenthesis to select the caller and the receiver separately.

Ex: (voip::call.user.number.str="15023591801")

voip::call.user.ip.str (::call.caller.ip.str, ::call.receiver.ip.str)

This expression allows selecting caller or receiver IP address. Use the expression in parenthesis to select caller and receiver separately.

Ex: (voip:: call.caller.ip.str ="192.168.77.27")

voip::call.call_id

This expression can be used to filter the Call-ID of a call.

Ex: (voip::call.call_id="7603a6824759d0f8366970ae6ba3c4c9@192.168.77.27")

voip::call.end.status.str

This expression can be used to filter on the state of a terminated call.

Allowed values: (Canceled, Rejected, Completed, TimeOut)

Ex: (voip::call.end.status.str="Completed")

voip::call.voip.protocol

This expression can be used to filter on the protocol used during the call (SIP or H.323).

Allowed values: (SIP, H.323)

Ex: (voip::call.voip.protocol ="SIP")

Filter comparison

Here follows a quick comparison of the most common filters in the two filter's syntaxes.

PURPOSE	WIRESHARAK CAPTURE	PILOT
Capture only traffic to or from IP address 172.18.5.4:	host 172.18.5.4	ip::ip.str="172.18.5.4"
A capture filter for telnet that captures traffic to and from a particular host	host 10.0.0.5 and tcp port 23	ip::ip.str="10.0.0.5" & generic::application.str="SHH/ Telnet" (*1)
Capturing all telnet traffic not from 10.0.0.5	tcp port 23 and not src host 10.0.0.5	generic::application.str="SHH/ Telnet" (*1) & ip::source_ip.str != "10.0.0.5"
Capture only DNS (port 53) traffic:	port 53	generic::application.str != "DSN" (*1)
Capture non-HTTP and non-SMTP traffic on your server (both are equivalent):	host www.example.com and not (port 80 or port 25) or host www.example.com and not port 80 and not port 25	http::host="www.example.com" & (tcp::port="80" | tcp::port="25")
Capture except all ARP and DNS traffic:	port not 53 and not arp	generic::application.str != "DSN" & generic::application.str != "ARP" (*1)
Capture only IP traffic - the shortest filter, but sometimes very useful to get rid of lower layer protocols like ARP and STP:	ip	mac::protocol_type.str="IP"
Capture only unicast traffic - useful to get rid of noise on the network if	not broadcast and not multicast	ip::destination_ip.delivery_type. str="Unicast"

you only want to see traffic to and from your machine, not, for example, broadcast and multicast announcements:		
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 [http://seclists.org/tcpdump/2004/q4/95|tcpdump-workers mailing list].	port 80 and tcp[((tcp[12:1] & 0xf0) >> 2):4]=0x47455420	http::method="GET"
Select of all the URLs that contains a certain word like "google"		http::uri contains "google"

Special values: In contrast to Wireshark filters, Pilot filters use customizable constants as comparison values. These values like “Local” or “Web” are defined in files editable by users.

Port-numbers file

‘port-numbers’ file associates TCP/UDP ports with well-known protocol names, that can be used to create more meaningful expression in Pilot filters:

Example:

ftp-data 20/tcp File Transfer [Default Data]

ftp-data 20/udp File Transfer [Default Data]

Pilot Filter: (tcp::identification_port.str="ftp-data")

In case of a standalone system, the file can be found in the server\configuration folder contained in pilot installation folder. For a Win Xp system generally: C:\Program Files\CACE Technologies\Pilot Console v2.2\server\configuration\port-numbers.

Proto-groups

'proto-groups' group together different port/protocols and associate them with a single value (such as Email) to filter with a simple expression more than one item at the same time.

Ex:

Email

Email	25/tcp	SMTP
Email	465/tcp	Secure SMTP
Email	587/tcp	SMTP
Email	110/tcp	POP3
Email	995/tcp	POP3 over SSL

Email	143/tcp	IMAP
Email	585/tcp	Secure IMAP
Email	993/tcp	IMAP over SSL
Email	119/tcp	NNTP

Pilot Filter: (generic::application.str="Email")

This list is accessible and customizable by the user. In case of a standalone system, the file can be found in the server\configuration folder contained in pilot installation folder. For a Win Xp system generally: C:\Program Files\CACE Technologies\Pilot Console v2.2\server\configuration\proto-groups. A copy of the file is added in the Appendix.

Sub-net mask

Refer to Pilot Manual for more information on the subnet mask. Values in the subnet mask influence what is considered "Local" in filters like: **mac::local.str="Local"**. In case of Shark Distributed Monitoring System, the subnet mask is defined only for the local system.

Appendix: proto-groups

```
# Web
Web                             80/tcp              HTTP
Web                             8080/tcp            HTTP
Web                             443/tcp                   HTTPS
#Web                            3128/tcp            SQUID
# Email
Email                   25/tcp      SMTP
Email                   465/tcp           Secure SMTP
Email                   587/tcp           SMTP
Email                   110/tcp           POP3
Email                   995/tcp           POP3 over SSL
Email                   143/tcp           IMAP
Email                   585/tcp           Secure IMAP
Email                   993/tcp           IMAP over SSL
Email                   119/tcp           NNTP
# Data-Transfer
Data-Transfer           20/tcp  File Transfer [Default Data]
Data-Transfer           20/udp  File Transfer [Default Data]
Data-Transfer           21/tcp  File Transfer [Control]
Data-Transfer           21/udp  File Transfer [Control]
Data-Transfer           115/tcp      Simple File Transfer Protocol
Data-Transfer           115/udp      Simple File Transfer Protocol
Data-Transfer           69/tcp  Trivial File Transfer
Data-Transfer           69/udp  Trivial File Transfer
Data-Transfer           989/tcp      ftp protocol, data, over TLS/SSL
Data-Transfer           989/udp      ftp protocol, data, over TLS/SSL
Data-Transfer           990/tcp      ftp protocol, control, over TLS/SSL
Data-Transfer           990/udp      ftp protocol, control, over TLS/SSL
Data-Transfer           873/tcp  rsync
# SSH/Telnet
SSH/Telnet              22/tcp      SSH
SSH/Telnet              23/tcp      Telnet
SSH/Telnet              514/tcp           RSH
# SMB
MS-Networking                       137/tcp           SBM
MS-Networking                       137/udp           SBM
MS-Networking                       138/tcp           SBM
MS-Networking                       138/udp           SBM
MS-Networking                       139/tcp           SBM
MS-Networking                       139/udp           SBM
MS-Networking                       445/tcp           SBM
MS-Networking                       445/udp           SBM
MS-Networking                       135/tcp           DCE endpoint mapper
MS-Networking                       135/udp           DCE endpoint mapper
MS-Networking                       389/tcp           LDAP
MS-Networking                       389/udp           LDAP
MS-Networking                       636/tcp           LDAP over TLS/SSL
MS-Networking                       636/udp           LDAP over TLS/SSL
MS-Networking                       631/tcp           IPP
MS-Networking                       631/udp           IPP
MS-Networking                       2701/tcp    SMS Remote Control (control)
```

```
MS-Networking                          2701/udp     SMS Remote Control (control)
MS-Networking                          2702/tcp     SMS Remote Control (data)
MS-Networking                          2702/udp     SMS Remote Control (data)
MS-Networking                          2703/tcp     SMS Remote Chat
MS-Networking                          2703/udp     SMS Remote Chat
MS-Networking                          2704/tcp     SMS Remote File Transfer
MS-Networking                          2704/udp     SMS Remote File Transfer
# SNMP
SNMP                        161/tcp            SNMP
SNMP                        161/udp            SNMP
SNMP                        162/tcp            SNMP
SNMP                        162/udp            SNMP
# VPN/Tunnel
VPN/Tunnel                        1723/tcp     PPTP
VPN/Tunnel                        1723/udp     PPTP
VPN/Tunnel                        1701/tcp     l2f/l2tp
VPN/Tunnel                        1701/udp     l2f/l2tp
VPN/Tunnel                        1194/tcp     OpenVPN
VPN/Tunnel                        1194/udp     OpenVPN
VPN/Tunnel                        47/ip        GRE
VPN/Tunnel                        137/ip       MPLS-in-IP
VPN/Tunnel                        4/ip         IP-in-IP
VPN/Tunnel                        41/ip        Tunnel Broker
VPN/Tunnel                        50/ip        IPsec ESP
VPN/Tunnel                        51/ip        IPsec AH
VPN/Tunnel                        55/ip        Minimal Encapsulation Protocol
# Remote-Desktop
Remote-Desktop              3389/tcp           MS RDP
Remote-Desktop              3389/udp           MS RDP
Remote-Desktop              5800/tcp           VNC-Web
Remote-Desktop              5801/tcp           VNC-Web
Remote-Desktop              5900-5905/tcp      VNC
Remote-Desktop              5631/tcp    pcANYWHEREdata
Remote-Desktop              5631/udp    pcANYWHEREdata
Remote-Desktop              5632/tcp    pcANYWHEREstat
Remote-Desktop              5632/udp    pcANYWHEREstat
Remote-Desktop              6000-6063/tcp      X Window System
Remote-Desktop              6000-6063/udp      X Window System
Remote-Desktop              1494/tcp     citrix-ica
Remote-Desktop              1494/udp     citrix-ica
Remote-Desktop              1604/tcp     citrix-icabrowser
Remote-Desktop              1604/udp     citrix-icabrowser
# Voice/Video - Videoconference
Voice/Video                 1270/tcp     WebEx
Voice/Video                 1503/tcp     This port is registered to Databeam and is used
for T.120 file sharing
Voice/Video                 1503/udp     This port is registered to Databeam and is used
for T.120 file sharing
# Voice/Video - VoIP
Voice/Video                 5060/tcp     SIP
Voice/Video                 5060/udp     SIP
Voice/Video                 5061/tcp     SIP-TLS
Voice/Video                 5061/udp     SIP-TLS
Voice/Video                 1718/tcp     h323gatedisc
Voice/Video                 1718/udp     h323gatedisc
Voice/Video                 1719/tcp     h323gatestat
```

```
Voice/Video              1719/udp    h323gatestat
Voice/Video              1720/tcp    h323hostcall
Voice/Video              1720/udp    h323hostcall
Voice/Video              1731/tcp    msiccp Audio Call Control
Voice/Video              1731/udp    msiccp Audio Call Control
Voice/Video              1300/tcp    This port is registered to Intel and is used to
secure a H.323 host call – h 323hostcsllsc (must be bi-directional)
Voice/Video              1300/udp    This port is registered to Intel and is used to
secure a H.323 host call – h 323hostcsllsc (must be bi-directional)
Voice/Video              2000/tcp    SCCP/Skinny
Voice/Video              2000/udp    SCCP/Skinny
Voice/Video              2001/tcp    Analogue Skinny Gateway
Voice/Video              2001/udp    Analogue Skinny Gateway
Voice/Video              2002/tcp    Digital Skinny Gateway
Voice/Video              2002/udp    Digital Skinny Gateway
Voice/Video              2427/udp    Cisco MGCP
Voice/Video              6901/tcp    MSN Messenger (Voice)
Voice/Video              6901/udp    MSN Messenger (Voice)
# Authentication
Authentication           1645/tcp    RADIUS Authentication
Authentication           1645/udp    RADIUS Authentication
Authentication           1646/tcp    RADIUS Accounting
Authentication           1646/udp    RADIUS Accounting
Authentication           49/tcp      Login Host Protocol (TACACS)
Authentication           49/udp      Login Host Protocol (TACACS)
Authentication           65/tcp      TACACS-Database Service
Authentication           65/udp      TACACS-Database Service
# DHCP
DHCP             67/tcp    Bootstrap Protocol Server
DHCP             67/udp    Bootstrap Protocol Server
DHCP             68/tcp    Bootstrap Protocol Client
DHCP             68/udp    Bootstrap Protocol Client
#DNS
DNS              53/tcp    Domain Name Server
DNS              53/udp    Domain Name Server
DNS              5353/udp  Multicast DNS
# Database
Database           3306/tcp   MySQL
Database           3306/udp   MySQL
Database           1433/tcp   Microsoft-SQL-Server
Database           1433/udp   Microsoft-SQL-Server
Database           1434/tcp   Microsoft-SQL-Monitor
Database           1434/udp   Microsoft-SQL-Monitor
Database           66/tcp    Oracle SQL*NET
Database           66/udp    Oracle SQL*NET
Database           66/tcp    Oracle SQL*NET
Database           66/udp    Oracle SQL*NET
Database           1521/tcp    Oracle SQL*NET
Database           1521/udp    Oracle SQL*NET
Database           1526/tcp    Oracle SQL*NET
Database           1526/udp    Oracle SQL*NET
Database           523/tcp    IBM-DB2
Database           523/udp    IBM-DB2
Database           5432/tcp     Postgre SQL
#Database
Pilot              61898/tcp  Pilot Probe default control port
```

```
Pilot             61899/tcp  Pilot Probe default data port
# ICMP
ICMP              1/ip         ICMP
ICMP              58/ip        ICMPv6
# Routing
Routing                  9/ip       IGRP
Routing                  99/ip      EIGRP
Routing                  89/ip      OSPF
Routing                  179/tcp    Border Gateway Protocol
Routing                  179/udp    Border Gateway Protocol
Routing                  520/udp    RIP
Routing                  521/tcp    ripng
Routing                  521/udp    ripng
#instant messaging
IM                       194/tcp            Internet Relay Chat Protocol
IM                       194/udp            Internet Relay Chat Protocol
IM                       1863/tcp    MSN messenger
IM                       5190/tcp    America-Online
IM                       5190/udp    America-Online
IM                       5191/tcp    AmericaOnline1
IM                       5191/udp    AmericaOnline1
IM                       5192/tcp    AmericaOnline2
IM                       5192/udp    AmericaOnline2
IM                       5193/tcp    AmericaOnline3
IM                       5193/udp    AmericaOnline3
IM                       5222/tcp    XMPP/Jabber - client connection
IM                       5223/tcp    XMPP/Jabber - default port for SSL Client
Connection
IM                       5269/tcp    XMPP/Jabber - server connection
IM                       6891-6900/tcp      MSN Messenger (File Transfer)
IM                       8010/tcp    XMPP/Jabber file transfers
IM                       4000/udp    ICQ
IM                       5010/tcp    Yahoo Messenger
IM                       5010/udp    Yahoo Messenger
#IGMP
IGMP              2/ip         IGMP
```