Display Filters

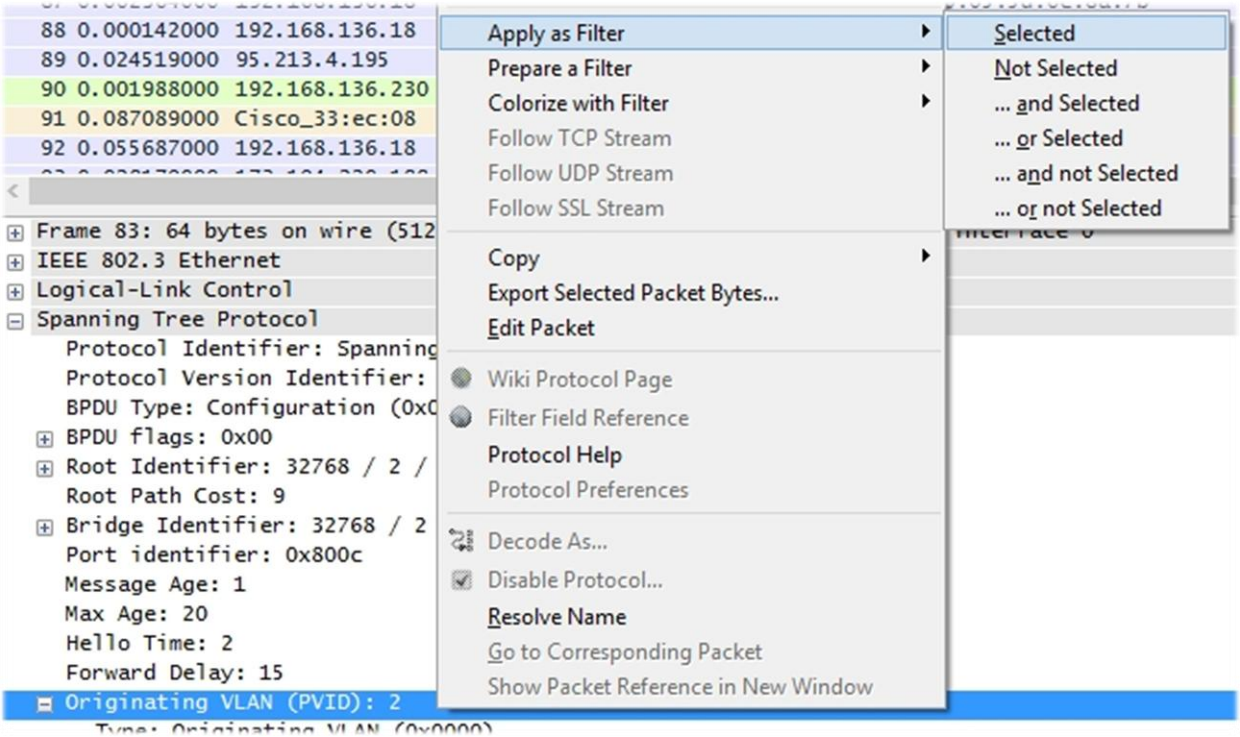
Wireshark Display Filters allow to control the traffic that is displayed in Wireshark. It is not necessary to restart the capture after the filter change when using Display Filters.
The syntax of the Display Filter looks like this:

Expression 1					Logical Operations	Expression 2 etc.	
Protocol	**option1**	**option2**	**Relation**	**Value**		**Protocol**	**option1**
ip.	***tos.***	***precedence***	***==***	***7***	***and***	***tcp.***	***ack***

- **Protocol**: *arp, ip, icmp, udp, tcp, telnet, ssl etc.*
- **Option**: various protocol fields
- **Relation**: Comparison**:** *eq(==), ne(!=), gt(>), lt(<), ge(>=), le(<=),*

  Search and match**:** *(is present), contains(to search a simple string), matches* (is used with Regular Expressions)
- **Value types**: unsigned integer (8/16/24/32/64 bit), signed integer (8/16/24/32/64 bit), boolean, string(text) etc.
- **Logical Operations**: *and(&&), or(||), not(!)*
- The complex logical constructions may be put in brackets **()**. Other symbols like square brackets **[]** etc. are often used with Regular Expressions to search the complex text strings inside of the frames.

There are a lot of options to construct a display filter. One of the easiest methods is to use the packet details pane. Every field in the packet details pane may be used as a filter string.



From the course *"Wireshark: The Art of Sniffing"*