

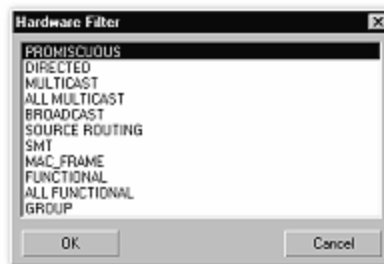
Sniff'em 1.01 Whitepaper

Filter facility

Hardware Filter

Sniff'em™ is able to make use of several advanced Hardware filter modes, these modes include:

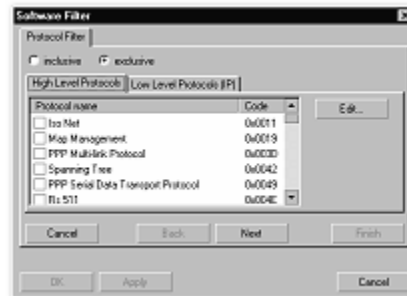
1. **Promiscuous** : captures all Packets.
All Functional: All functional address packets, not just the ones in the current functional address.
2. **All Multicast** :
All multicast address packets, not just the ones enumerated in the multicast address list.
3. **Broadcast** : Broadcast packets
4. **Directed** : Directed packets.
Directed packets contain a destination address equal to the station address of the NIC.
5. **Functional** : Functional address packets sent to addresses included in the current functional address.
6. **Group** : Packets sent to the current group address.
7. **Mac Frame** : NIC driver frames that a Token Ring NIC receives.
8. **Multicast** : Multicast address packets sent to addresses in the multicast address list. A protocol driver can receive Ethernet (802.3) multicast packets or Token Ring (802.5) functional address packets by specifying the multicast or functional address packet type. Setting the multicast address list or functional address determines which multicast address groups the NIC driver enables.
9. **SMT** : SMT packets that an FDDI NIC receives.
10. **Source Routing** : All source routing packets.
If the protocol driver sets this bit, the NDIS library attempts to act as a source routing bridge.



Software Filter

Additionally to the Hardware filters Sniff'em™ offers very flexible and advanced Software Filters, these sometimes complex filters can be integrated with ease using the foolproof Graphical User interface. Software filters are able to Filter based on:

1. High-Level protocol (IP, X75, X25..)
2. Low-Level protocol (ICMP, IGMP, TCP..)
3. IP Source (Wildcards supported)
4. IP Destination (Wildcards supported)
5. Source Port (Port ranges supported)
6. Destination Port (Port ranges supported)
7. MAC Destination
8. MAC Source
8. ASCII Packet data
9. TCP State (SYN, ACK, RST) and Size



Exclusive Filters

Available for all filters, these settings will capture and display packets that are NOT selected. It will exclude the selected Protocol, Port, Mac address, etc.

Inclusive Filters

Available for all filters, this settings will only capture and display protocols, which are selected and ignore the others.

Practical uses for Filter

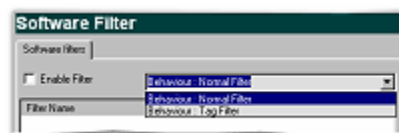
1. Filter out the Packet valuable for Network analysis. (Broadcast, ICMP error)
2. Monitor internet usage (Filter HTTP traffic for words like "Porn", "sex", etc)
3. Special Events (Trigger Mode) Capture traffic immediately AFTER a special predefined event occurred (ftp login, smtp message)

Filter Modes (introduced in version 1.1)

Tagging Filter

Using this Filter mode Sniff'em™ will capture and display all the Traffic and takes in consideration the Filters that were set. The difference here is that if given Tag filter is hit by an Network packet;

Sniff'em™ will tag it by assigning a special value to the Tag index, this features allows users to immediately see the packets they wanted to get hold of while still capturing the whole data traffic crossing the network.



Normal Filter

Only Packets that are specified in the Filter settings (In case of the

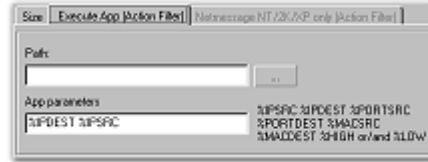
inclusive filter set) will be captured others will be "dropped". (Vice versa for the Exclusive filter)

Action Filter (introduced in version 1.1)

Execute (Shell)

Action filter allow special action to be done when a predefined filter is hit, as example if a predefined packet hits the network Sniff'em is able to spawn "trace.exe %ip.source >> %

ip.source.txt". Note that the executable that is spawned supports dynamic parameters and that MS-DOS batch files may be called too and as such you are able to shell an unlimited number of Applications with dynamic parameters.



Net Message

The Net message will send a Net message to a machine over a network once the Filter was hit, this is ideal for Intrusion Detection as well as special events, break-ins, policy infringement (Games, Surfing etc)
