Basic Packet Filtering

By Laura Chappell, Protocol Analysis Institute, LLC <www.packet-level.com>

Note: This is Part One of a two-part article focusing on protocol analysis filtering for network troubleshooting, optimization and security.

Filtering reduces the amount of packets that are *placed in* the trace buffer or are *displayed from* the trace buffer. The following list gives some examples of the types of filters that you may want to apply on your network:

> All TCP/IP traffic: You aren't interested in any other traffic because you're working on some IP routing issues.
>
> All ICMP traffic: You want to know what types of error messages and possible hack probes are happening on your network.
>
> All traffic to/from your server: You are interested in identifying who communicates most often with your server.
>
> All packets that contain the value NLST at packet offset 36: You want to know who is listing files using the FTP list files (NLST) command regardless of the port number the FTP process is using.

These filters fit into three basic categories:

- Address filters
- Protocol filters
- Data set filters

Address Filters

> Address filters are used to specify the desired traffic based on the source or destination MAC (data link) address, IP address, or IPX address.
>
> It seems pretty obvious which address type you would filter on, however I have seen people select the wrong filter type at times. For example, which filter would used to capture all traffic to and from a DHCP boot up device?
>
> If you selected IP, you would've made in logical selection, but you would have missed the initial boot up traffic. The DHCP client will initially communicate using source IP address 0.0.0.0 -- thereby causing your filter to miss the traffic. Because of this, if we are ever capturing traffic that involves the DHCP boot up process, we must define a filter base of the MAC address of the device.

Note: For more information on DHCP functionality, refer to the NetWare Connections BrainShare Daily article on DHCP <http://www.nwconnection.com/brainshare/showdaily/thu_feature1.html>. There are also numerous DHCP trace files online at www.packet-level.com.

In Figure 1, we have set up in address filter to capture all traffic to and from the device using IP address 10.2.0.2. We have selected "IP" as the address type, and we have entered the address number in the table under the heading “Station 1”. Note that the arrow between the two machines (under the DIR heading) is pointing both ways. This indicates that we are interested in bidirectional traffic--traffic to and from device 10.2.0.2. Under the title “Station 2” we have entered the word "any". This indicates that any destination address would be acceptable to our filter.

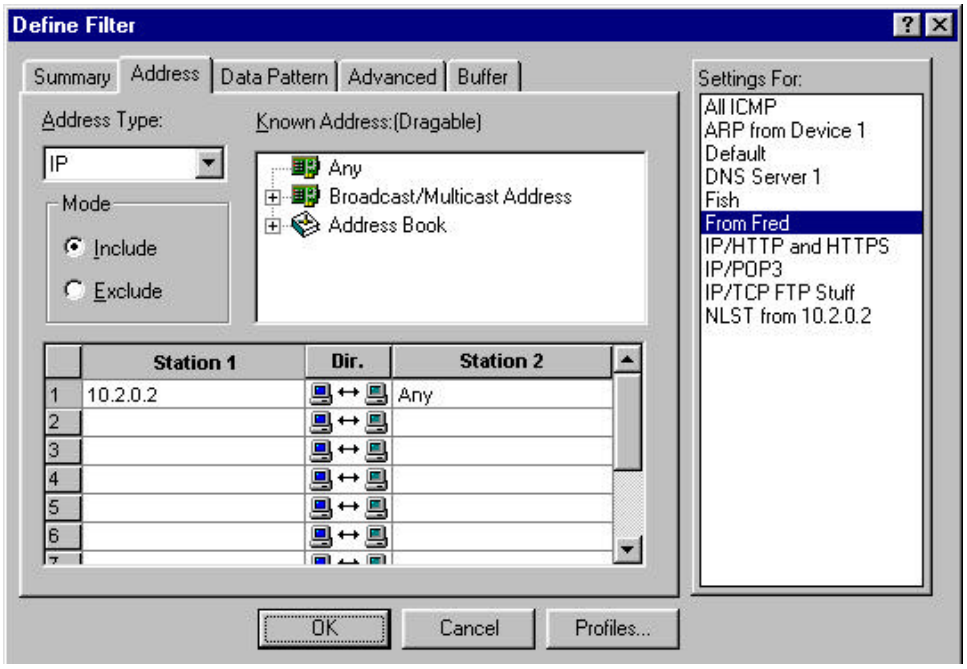

Figure 1: Looking for all traffic to and from 10.2.0.2.

Protocol Filters

Protocol filters help reduce the traffic based on functionality, or protocol. For example you may want to capture all ICMP traffic, DNS traffic, OSPF traffic, and so on. There are numerous protocols that are of interest on networks today. For example if I were to come to your network can take a look at your traffic, I would then begin applying filters looking for specific traffic such as all ICMP traffic. By analyzing this traffic, I'd get an idea of the various errors and misconfigurations that may exist on your network. Then, I may apply an OSPF filter to gather information about your network routing.

By viewing traffic based on protocol in used, we can break down a network by the applications that are running across the wire. This is how we get a real view how the network is truly being used.

In Figure 2, we are examining my ICMP filter that I have built for my analyzer. In this case, I am using Sniffer Pro 3.5. By simply clicking on to checkbox in front of ICMP, I have built a filter that will capture or display only ICMP traffic.

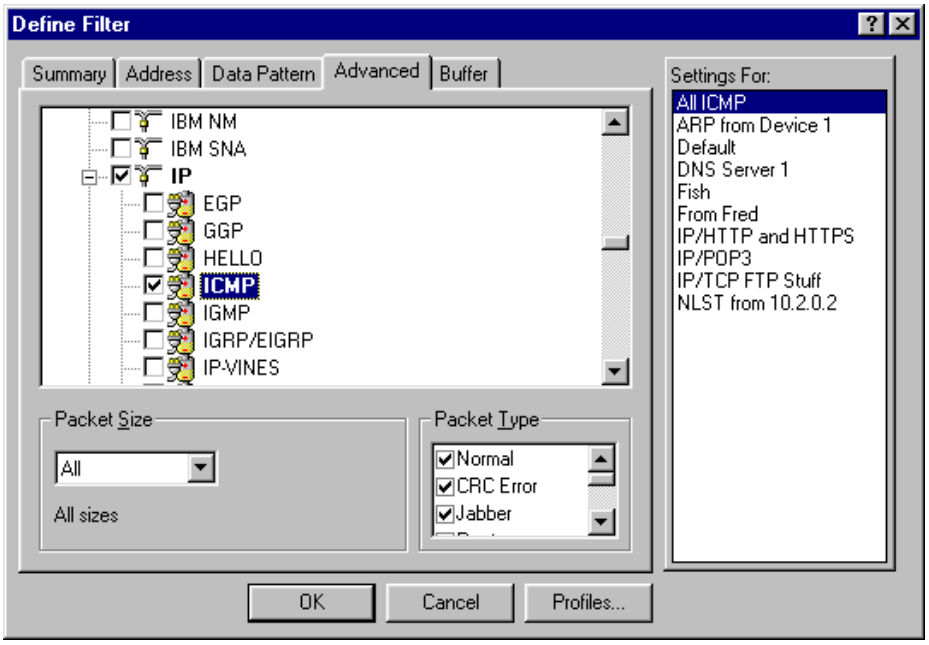

Figure 2: Simply clicking on the ICMP checkbox creates a filter for the number "01" in the IP header's Protocol field.

Warning: Be careful of trusting these "pre-defined protocol filters". These filters are based on the premise that all traffic uses standards-defined operation characteristics. For example, if we were to build an FTP filter by simply clicking the FTP checkbox, we would automatically capture all traffic to and from port number 21 (the number assigned to FTP control operations). We would, however, miss all of the other FTP traffic that uses other port numbers. Refer back to the NetWare Connections article entitled, "Analyzing FTP Communications" <September 2000, www.nwconnection.com> that addresses the various ports numbers that FTP can use to transfer information.

Data Set Filters

I consider data set filters to be advanced filters. Too often overlooked, these filters enable you to define interesting traffic based on a specific value at a specific offset within a packet.

For example, in Figure 3, we have set up a data filter that will look all packets that contain the value NLST at a specific offset. These packets are seen when an FTP client executes a command to view the directory contents.

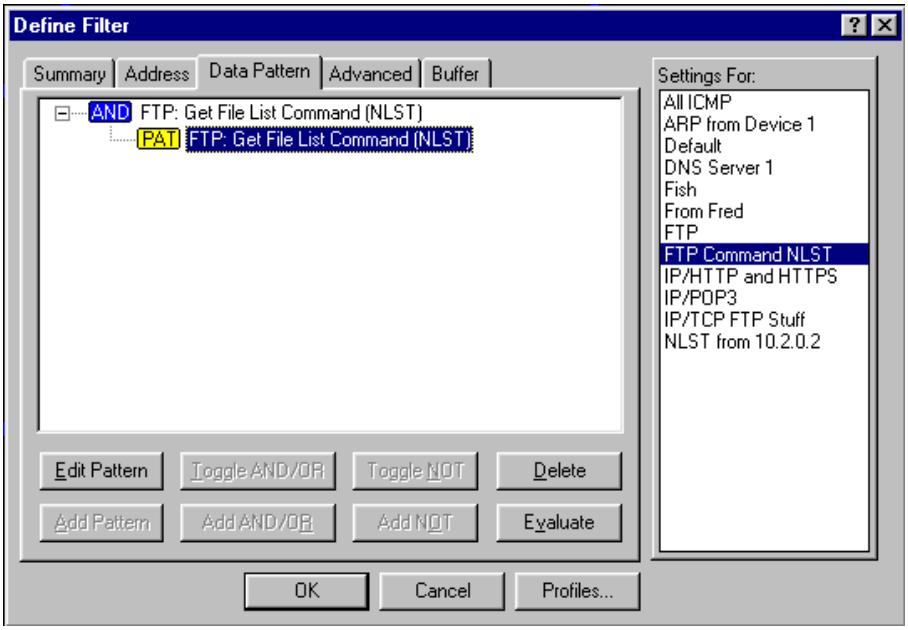

Figure 3: You can build filters on specific values located at specific offsets.

The following list is an example of some of the filters that you could build:

To and from your key servers	IP/UDP SNMP (Trap + Get)
To and from your firewall	IP/UDP DHCP + BOOTP
To and from your routers	IP/TCP All
To and from your computer	IP/TCP FTP
ICMP/All	IP/TCP FTP Commands
ICMP/Destination Unreachable	IP/TCP DNS (TCP and UDP)
ICMP/Echo	IP/TCP Telnet
ICMP/Redirect	IP/TCP Rlogin
ARP	IP/TCP/SMTP
IP/UDP All	IP/TCP POP
IP/UDP NetBIOS	IP/TCP HTTP + HTTPS
	And so on…

Note: For more information on data set filtering, refer to the article entitled "Advanced Data Filtering" available online at www.packet-level.com.

True, analyzers have different capabilities in the area of filtering. Make a point of checking out your analyzer's ability to filter traffic.

Archived Laura Chappell articles (www.packet-level.com/archives.htm):

- Looking at the Sniffer Dashboard
- Sniffer: Using the Capture Panel
- TrenchTime: Ports to Watch
- Did Your Know: Wireless Networks are Not Immune to Sniffing?
- The 10 Truths of Network Troubleshooting
- Carnivore?