Laura Chappell

Basic Packet Filtering

Using Your Network Analyzer

When you are using a network analyzer to capture traffic on your company's network, filtering reduces the number of packets that are placed in the trace buffer or are displayed by the trace buffer. The following list provides some examples of the types of filters that you may want to apply on your network:

- **All TCP/IP Traffic.** You may use this filter if you are only interested in reviewing TCP/IP traffic. For example, you may be trying to resolve IP routing issues.
- **All ICMP Traffic.** You may use this filter if you want to know what types of error messages and possible hack probes are occurring on your company's network.
- **All Traffic to/from a Server.** You may use this filter if you are interested in identifying which devices communicate most often with a server.
- **All Packets That Contain the Value NLST at Packet Offset 36.** You may use this filter is 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 the following three 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 Media Access Control (MAC) address (data link), IP address, or IPX address. Selecting to filter by address type seems fairly straightforward; however, I have seen people select the wrong filter type. For example, which filter would you choose to capture all traffic to and from a Dynamic Host Configuration Protocol (DHCP) bootup device?

If you selected the IP address filter, you would make a logical selection, but you would miss the initial bootup traffic. Because the DHCP client initially communicates using source IP address 0.0.0.0, the IP address filter on your network analyzer would miss this traffic. Consequently, if you capture traffic that involves the DHCP bootup process, you must define a filter based on the MAC address of the device.

Note. For more information about DHCP functionality, refer to the *Novell Connection* BrainShare Daily article, "Inside DHCP," at www.ncmag.com/brainshare/showdaily/thu_feature1.html. You can also view numerous DHCP trace files online at www.packetlevel.com.

Illustration: Norman Felchle

In Figure 1, I have set up an address filter to capture all traffic to and from the device using IP address 10.2.0.2. I have selected IP as the address type, and I have entered the address number in the table. Notice that the arrow between the two computers (under the Dir. heading) is pointing both ways. This arrow indicates that I am interested in bidirectional traffic—traffic to and from device 10.2.0.2. Under the title "Station 2," I have entered the word *any* to indicate that any destination or source address should be added to the filter.

PROTOCOL FILTERS

Protocol filters help reduce the traffic based on functionality or protocol. For example, you may want to capture all Internet Control Message Protocol (ICMP) traffic, Domain Naming System (DNS) traffic, or Open Shortest Path First (OSPF) traffic. For example, if I were to look at the traffic on your company's network, I would begin applying filters to look for specific traffic, such as all ICMP traffic. By analyzing this traffic, I would get an idea of the various errors and misconfigurations that may exist on that network. Then, I may apply an OSPF filter to gather information about your network routing.

By viewing traffic based on protocols, you can break down a network by the applications that are running across the wire. In this way, you can begin to understand how the network is truly being used. Figure 2 shows the ICMP filter on Network Associates' Sniffer Pro 3.5. By simply clicking the checkbox in front of ICMP, I have created a filter that will capture or display only ICMP traffic.

Warning. You need to be careful of trusting these predefined protocol filters on network analyzers. These filters are based on

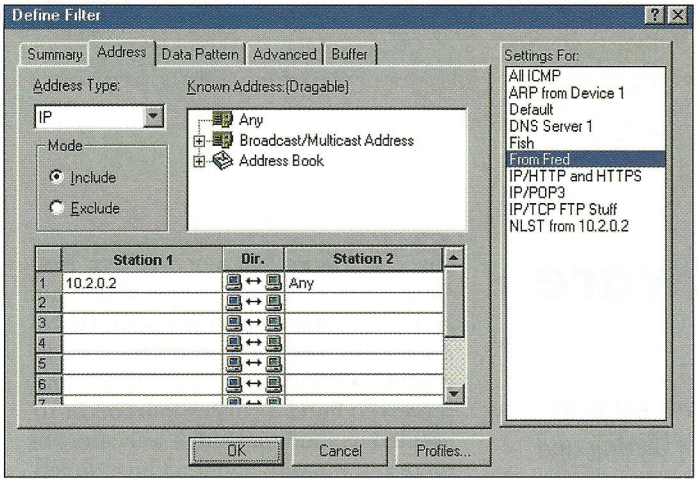

Figure 1. *You can set up an address filter to capture all traffic to and from a specific device. In this case, the device's IP address is* 10.2.0.2.

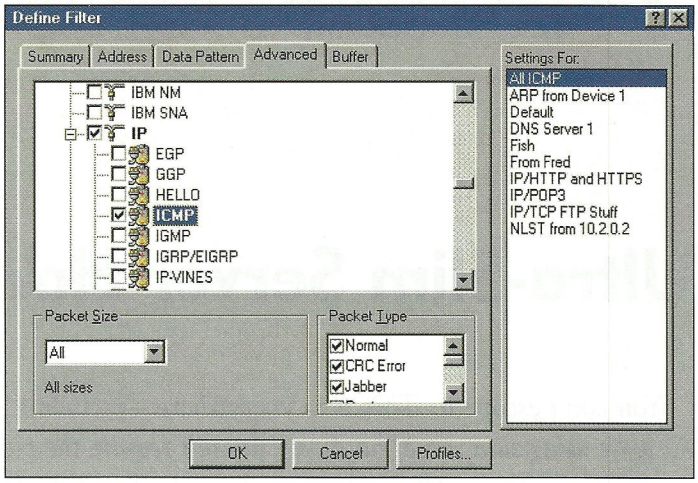

Figure 2. *Simply clicking on the ICMP checkbox creates a filter for the number "01" in the IP header's protocol field.*

the premise that all traffic uses standards-defined operation characteristics. For example, if you were to select an FTP filter by simply clicking the FTP checkbox, you would automatically capture all traffic to and from port number 21 (the number assigned to FTP control operations). However, you would miss the FTP traffic that uses other port numbers. (For more information about the port numbers that FTP can use to transfer information, see "Analyzing FTP Communications," *Novell Connection*, Sept. 2000, pp. 22–34. You can download this article from www.ncmag.com/past.)

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, I have set up a data filter that will look at all packets that contain the value NLST at a specific offset. These packets are used when an FTP client executes a command to view the directory contents. The following list is an example of some of the filters that you could build:

- To and from your company's key servers
- To and from your company's firewall
- To and from your company's routers
- To and from your PC
- ICMP/All
- ICMP/Destination Unreachable
- ICMP/Echo
- ICMP/Redirect
- ARP
- IP/UDP All
- IP/UDP NetBIOS
- IP/UDP SNMP (Trap + Get)
- IP/UDP DHCP + BOOTP
- IP/TCP All
- IP/TCP FTP
- IP/TCP FTP Commands
- IP/TCP DNS (TCP and UDP)
- IP/TCP Telnet
- IP/TCP Rlogin
- IP/TCP/SMTP
- IP/TCP POP
- IP/TCP HTTP + HTTPS

Note. For more information about data set filtering, read "Advanced Packet Filtering," at www.packet-level.com.

CONCLUSION

Choosing the right filter when analyzing network communications can mean the difference between success and failure in troubleshooting problems. This critical first step in analyzing communications can help you accurately pinpoint problems or leave you floundering, looking for answers.

Before you choose a filter, check out your network analyzer's ability to filter traffic. Not surprisingly, network analyzers have different capabilities in the area of filtering.

You should also carefully review your company's network and analyze the kind of traffic being sent across the wire. This careful evaluation will help you find the answers you're looking for. In addition, simply practicing filtering on different types of traffic will help you understand how each filter works.

Laura Chappell has just released "Advanced Network Analysis Techniques," available online at www.podbooks.com.

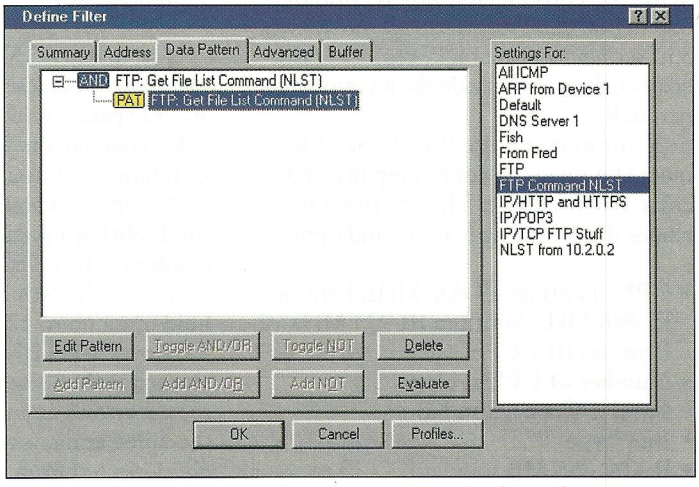

Figure 3. *You can build a filter on a specific value located at a specific offset within a packet.*