

Packet Filtering and Decoding ICMP

www.thesolutionfirm.com

Packet Filtering and Decoding ICMP's Using Your Network Analyzer

Michael Gregg

Overview

This article examines several types of Internet Control Message Protocol (ICMP) and their meanings. It also outlines the steps required for setup and capture of ICMP traffic. The packet analysis displayed in this article was captured with Sniffer Basic, a protocol analyzer available from Network Associates, Inc.

Network analyzers are powerful tools that allow you to decode packet level communication on your company's network. Once you master the art of packet decoding you will become better equipped to troubleshoot networking problems, optimize your network, and protect against cyber attack.

Even though ICMP is carried inside Internet Protocol (IP) datagrams, this protocol is considered to be a parallel protocol running side-by-side with IP at the network layer. ICMP is documented and defined in RFC-792. All ICMP messages follow the same basic format as listed below in **Table 1**. The first byte of an ICMP indicates the type of ICMP message. There are eight (8) basic types. The following byte contains the code for its respective type of ICMP function.

(Byte 1) TYPE	(Byte 2) CODE	FUNCTION
0/8	0	Echo Response/Request (Ping)
3	0-15	Destination Unreachable
4	0	Source Quench
5	0-3	Redirect
11	0-1	Time Exceeded
12	0	Parameter Fault
13/14	0	Timestamp Request/Response
17/18	0	Subnet Mask Request/Response

Table 1

Ground Rules for ICMP

ICMP has basic limitations built into its specification to avoid the cure being worse than the disease.

1) Broadcast and multicast messages cannot create ICMP messages, and 2) ICMP error messages cannot create other ICMP messages. Both rules help avoid creating cascading errors that could flood the network with a broadcast storm.

Analyzer Setup

Almost all network analyzers have an ICMP filter. 1) Open your analyzer, 2) Select the capture filter setting from the tool bar as displayed in **Figure 1**,

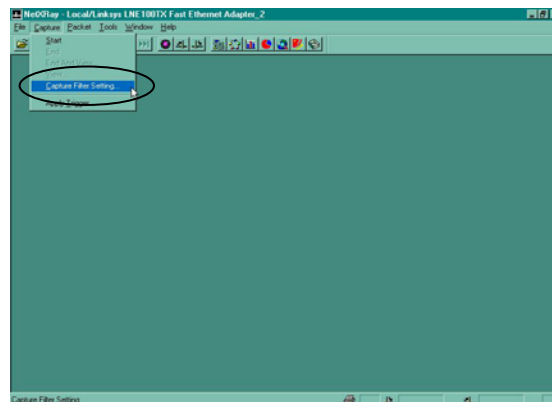


Figure 1

3) Capture Filter Setting Window will be displayed, and 4) Select the Advanced Filter Tab as shown in **Figure 3** and select ICMP. You are now ready to capture ICMP traffic.

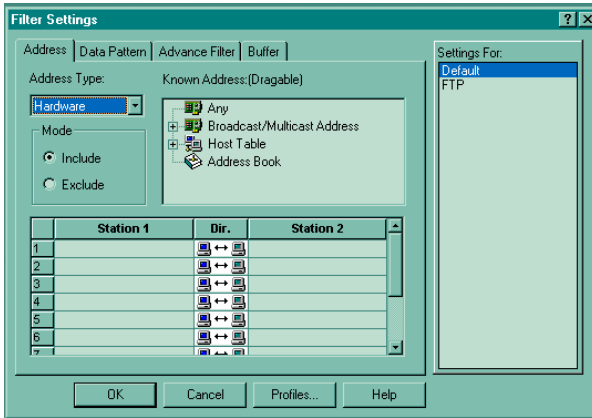


Figure 2

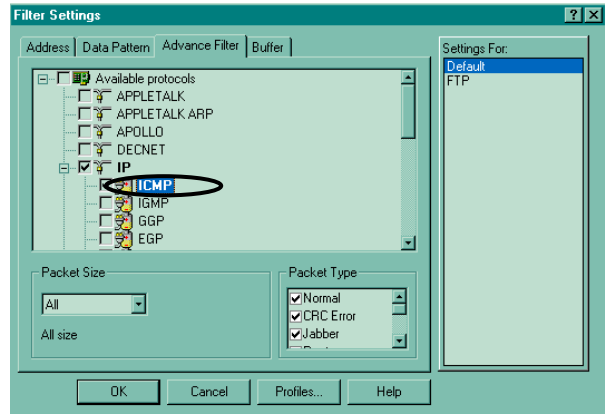


Figure 3

Destination Unreachable

Type 3, Code 3 are destination unreachable messages. This type of ICMP indicates there has been a failure somewhere in the process of addressing the datagram, which triggered the message. There are 16 codes that define the various reasons why an unreachable message was created. These code numbers are listed below in **Table 2**.

CODE	REASON	CODE	REASON
0	Network Unreachable	8	Source Host Unknown
1	Host Unreachable	9	Target Network Prohibited
2	Protocol Unreachable	10	Target Host Prohibited
3	Port Unreachable	11	Network TOS Problem
4	Fragmentation Needed	12	Host TOS Problem
5	Source Route Failed	13	Communication Prohibited
6	Target Network Unknown	14	Host Precedence Violation (RFC-1812)
7	Target Host Unknown	15	Precedence Cutoff in Effect (RFC-1812)

Table 2

The Internet Assigned Numbers Authority (IANA) is the governing board that controls the list of code numbers. To become a more skilled network professional, you should read the latest up-to-date information on the various protocols. Go to www.iana.org for current information.

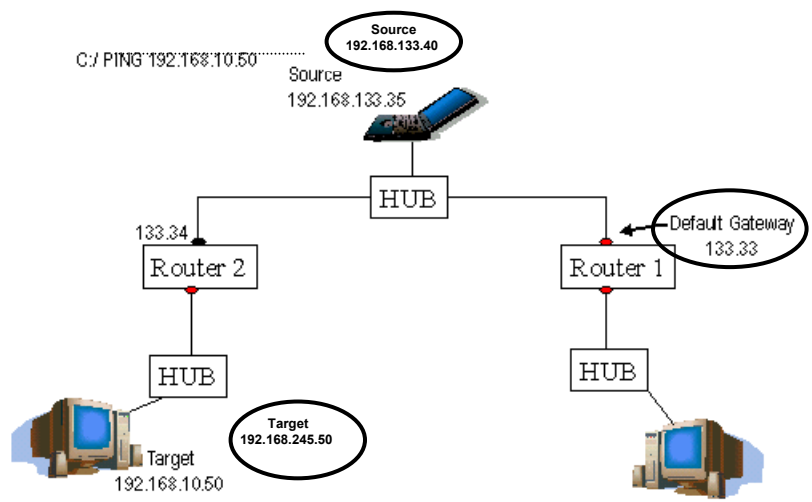
Hackers use ICMP's destination unreachable message (port unreachable) packets to determine which ports are listening on a target device. Once a hacker scans a target system's ports and waits for a response, inactive ports on the target device will return an ICMP unreachable message. This is how the status of various ports is determined. **Figure 4** shows the capture of an ICMP Type 3, Code 3.

No.	Sta.	Source Address	Dest Address	Layer	Summary
6	Ok	192.168.123.254	192.168.123.100	ICMP	Type=Echo Reply, ID=512, Seq No=20480
7	Ok	192.168.123.100	192.168.123.254	ICMP	Type=Echo Request, ID=512, Seq No=20736
8	Ok	192.168.123.254	192.168.123.100	ICMP	Type=Echo Reply, ID=512, Seq No=20736
9	Ok	192.168.123.100	192.168.123.254	ICMP	Type=Destination Unreachable, Code=Port Unreachable

Figure 4

Redirect

Another type of ICMP is the redirect. You do not want to allow redirects from outside your organization. Hackers can use this to exploit your network! Typically, this Type 5, Code 0 is generated when a host sends traffic to one router when another router is advertising a better route. This is a common occurrence on networks with more than one router. **Figure 5** below demonstrates this situation. Although 192.168.133.40 is attempting to ping 192.168.245.50, its default gateway, Router 1, is not the shortest path.



Although Router 1 forwards the ping message to its target, 192.168.245.50, it also generates an ICMP message that is sent back to the original source 192.168.133.40. This ICMP informs the source that there is a shorter path to use in subsequent communications. This ICMP redirect packet is illustrated below in Figure 6.

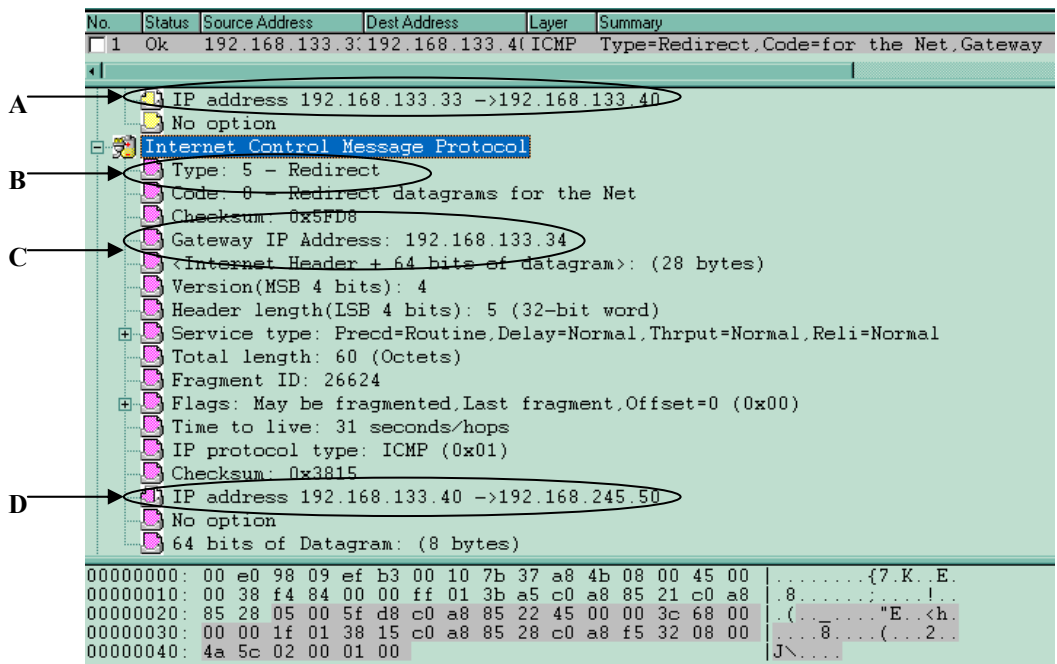


Figure 6

How much information is revealed in this single packet? **Figure 6-A** displays the router 192.168.133.33, which found the problem and the original source 192.168.133.40, which the router is sending the ICMP to. **Figure 6-B** displays the type of ICMP message, which is an ICMP redirect. **Figure 6-C** displays the new routing gateway 192.168.133.34, which is the location to route the next message for subsequent communication. **Figure 6-D** displays the original source and target address.

Conclusion

You should carefully analyze the type of traffic on your company's network. Start using your protocol analyzer and familiarize yourself with its various options and features. Download the latest revision of RFC-792 for your review. Finding ICMP packets and developing the skill to decode them will enable you to troubleshoot your network. Understanding the ICMP protocol will also help prevent your network from becoming an easy target for hackers.

About the Author

Michael C. Gregg is the COO of Superior Solutions, Inc., a security assessment and training firm. His current responsibilities include performing security assessments and evaluations for corporate and government entities. He has served as the developer of high-level security classes, study guides, has taught classes for many Fortune 500 companies and contributed to many books, including the Que publication, *CISA Exam Prep*.

