Looking for Trouble: ICMP and IP Statistics to Watch

Laura Chappell, Senior Protocol Analyst
Protocol Analysis Institute [lchappell@packet-level.com]
HTCIA Member, IEEE Associate

During the US/Canada road show this past two years, I’ve had the opportunity to share many of my favorite tools, tricks and techniques for network troubleshooting and cybercrime detection and testing.

One area that I spend a bit of time on is the Summary Statistics window provided by EtherPeek – it’s hot! Using the information provided in the summary statistics window, I can identify a network that is experiencing the following traffic behavior:

- ARP scans are looking for active systems on a subnet
- Ping scans are looking for active systems on the entire network
- Port scans are looking for active services over TCP or UDP
- Routing configurations are causing packet redirection or advertising new default gateway settings
- OS fingerprinting is attempting to identify operating system types and versions
- Services are not configured properly or services are not functioning properly
- Traceroute is attempting to discover network paths

In this article, I’ll walk you through two categories that I focus on most often during onsite analysis visits:

ICMP Analysis
IP Analysis

To open the Summary Statistics window in EtherPeek, click on the Summary Statistics icon on the main toolbar.

**ICMP Analysis Summary Information**

This is one of my first stops during the ‘laying on of hands’ (my process for baselining network performance and identifying the ‘personality’ of the network).

ICMP is one of the most informative protocols available in the TCP/IP protocol suite. This protocol is used for good… and bad. On one hand, some ICMP packets help us isolate network configuration and performance problems. On the other hand, ICMP is the protocol of choice for folks who perform reconnaissance...
on your network, your operating systems and your network services for the eventual purpose of hacking in.

Figure 1 shows the ICMP Analysis details within EtherPeek’s Summary Statistics window.

Figure 1: The ICMP Analysis section can help identify configuration problems as well as OS fingerprinting and UDP-based port scans.
Ping Packet Statistics (ICMP Echo Packets)

There are three items in the Summary Statistics window that deal with ping operations:

- Pings Unanswered
- Ping Requests
- Ping Responses

The “pings unanswered” value is equal to the ping requests minus the ping responses.

If I see a high number of ping requests (and even a counter that increments as I watch) and a low number of pings unanswered, I know that one device is pinging another device successfully. A high number of pings is not normal on a network – typically ping is used for a short-term connectivity test. A high number of pings may indicate a user is playing with ping command. The next step in this case may be to identify the devices who are sending continuous pings and get them to CLAM UP!

If I see a high number of ping requests and a high number of pings unanswered, however, I will look for someone performing a ping scan on the network. A ping scan is used to identify all the active systems on a network. Is there any reason a system should perform such an operation? Watch out for your network management tools – they may use a ping scan to build one of those lovely network maps. Whatever the reason, you need to check out who is ping scanning and why. We certainly don’t want ping scans coming in from the Internet – consider blocking all inbound ICMP Echo requests to thwart these probes.

OS Fingerprinting Packets

OS Fingerprinting is a technology used to identify the operating system and version running on a computer. There are several tools that are used for OS fingerprinting: Xprobe (http://www.sys-security.com/html/projects/X.html), nmap (http://www.insecure.org/nmap/nmap-fingerprinting-article.html), and LANguard Network Scanner (www.gfi.com).

In the early days of OS fingerprinting, tools used TCP connections and banner pages to determine what OS was running on a system. Banners are initial connection details that are displayed when you reach an open service such as FTP or telnet. Many times, the operating system identifies itself when the initial connection is established.
In recent years, however, many FTP servers do not disclose their operating system by default anymore. This makes OS fingerprinting with TCP difficult or impossible – this is where ICMP comes into play.

ICMP-based OS fingerprinting uses a technique documented by Ofir Arkin in “ICMP Usage in Scanning” (http://www.sys-security.com/html/projects/icmp.html). ICMP-based OS fingerprinting tools send an assortment of ICMP packets that are well-formed or malformed and watch the replies. Operating systems respond in a variety of ways – enabling the attacker to classify those operating systems and decide the next step based on operating system vulnerabilities.

The following ICMP packets are commonly used during OS fingerprinting:

- Echo requests (ICMP Type 8) and replies (ICMP Type 0)
- Host Parameter Problem (ICMP Type 12)
- Time stamp requests (ICMP Type 13) and replies (ICMP Type 14)
- Information request (ICMP Type 15) and replies (ICMP Type 16)
- Address mask request (ICMP Type 17) and replies (ICMP Type 18)
- Router Solicitation (ICMP Type 10) and replies (ICMP Type 9)

OS fingerprinting tools may not use all these packet types, but they do typically use several of them during their fingerprinting operation. In reviewing the EtherPeek Summary Statistics window shown in Figure 1, we can see ICMP Router Solicitations, Timestamp Requests/Responses and Address Mask Requests/Replies have been seen. Since these types of ICMP messages are rarely used for legitimate purposes, we must look closely to see if someone is running OS fingerprinting on the network. Perhaps we would place a protocol analyzer on the network and define special filters simply looking for these suspect packet types.

Network/Host Redirection

When a host sends a packet to a router that knows it is not the best router to get to the destination, that receiving router sends an ICMP Redirect for Network/Host packet back to the source. This redirection packet contains the IP address of the preferred router that the host should use.

When a host receives an ICMP network/host redirection message, it will update its routing tables with a dynamic entry for the destination network/host. By typing ‘route print’ in the command box, you can see the new entry.

If a network shows a high number of these redirection packets, either the default gateway setting is not appropriate for the network hosts or someone may be trying to redirect packets for a malicious purpose.
To know which case is true, we’d need to capture the traffic for a while and watch the redirections packets. By examining who is sending the redirection packets and the preferred router information within the packets, we can tell if the redirection is because the router did not offer the best path or the redirection pointed to a system that should not be offering routes. In the latter case, we may have a hacker in our midst. By redirecting the packets through his/her system, the hacker can read the traffic to identify user names, passwords, unencrypted data, etc.

Destination Unreachables and UDP Port Scans

The EtherPeek Summary Statistics window contains a list of ICMP Destination Unreachable packet types:

- Network unreachable
- Host unreachable
- Protocol unreachable
- Port unreachable

I pay particular attention to the port unreachable statistics. If there are a high number of port unreachable packets, either we have a host misconfiguration or a UDP port scan may be underway.

In the case of a misconfigured host, the device sends a message to a desired destination (such as a DNS server). If the destination doesn’t support the services, it responds with an ICMP Destination Unreachable message – specifically a ‘port unreachable’ message. The ICMP communication needs to be examined to watch the systems sending the ICMP port unreachable messages. Since these are basically service refusals, we need to their cause and the solution to eradicate these messages from the network.

During a UDP port scan, a hacker sends a series of UDP packets to a range of ports (most often paying attention to the ports that offer vulnerable or interesting services over UDP, such as DHCP, DNS and SNMP). If the service is not available on a target, the target sends back an ICMP port unreachable message. When a network has a rapidly increasing number of ICMP port unreachable messages, it’s important to look at the traffic to determine if a system is sending a series of packets to a range of destination port numbers. Such behavior is not normal or acceptable on the network.
**IP Analysis Summary Information**

Another section that I look at is the IP Analysis section. In this area, EtherPeek lists out the number of ARP requests, ARP responses, TCP SYNs (synchronize sequence number requests), FINs (notifications that a task is completed) RST (resetting or refusing a connection), and RARP (Reverse ARP) operations. (See Figure 2.)

These statistics also can indicate if a network configuration problem exists or if someone is scanning your network.

![Figure 2: The IP Analysis section can be used to identify misconfigurations, ARP scans and TCP scans.](image)

**Excessive Unanswered ARPs**

A high number of unanswered ARPs indicates that a system is looking up the hardware address of a local device that is not responding. This lack of response may be due to a network mask misconfiguration (the sending host thinks the target is on the same network when it is not) or a target system that is not functioning (hence the lack of response).

A high number of unanswered ARPs may also indicate that an ARP scan is underway. ARP scanning is used to find out all the hardware addresses of the systems running on the local network. Although some management systems may use this technique to build those beautiful maps, we need to capture the traffic to determine if that is actually case.
TCP-based Port Scanning

Earlier we discussed UDP-based port scanning – the process that looks for systems supporting UDP-based services such as DNS, DHCP, and SNMP. TCP-based scanning looks for services running over TCP. Since most of the really interesting services run over TCP (such as FTP, telnet, HTTP, etc.), we need to watch out for these TCP scans on the network.

TCP scans generate an unusually high number of Reset (RST) packets. During a TCP scan, a host sends a series of packets to the desired port (such as the FTP port 21) on a target system. If the system does support the service, it sends a TCP SYN ACK (synchronize with acknowledgment) response. If that system does not support the service, it sends a TCP Reset in response.

Although many people believe resets are sent at the end of every TCP communication to close the connection, in actuality, Finish (FIN) packets are typically used. For example, when you close a web browser, Finish packets are sent between the web client and the web server to indicate that the client is done with the tasks it was performing.

When you see a high number of RSTs (greater than 30% of the number of SYN packets), check out the traffic to see if you have a TCP port scan underway on your network.

WildPackets did a great job of putting together key information in one location. When you launch EtherPeek, immediately open the Summary Statistics window and check the ICMP Analysis and IP Analysis sections regularly to look for any unusual traffic patterns. From client misconfigurations to hackers performing reconnaissance on your network, you can identify possible problems without even capturing a single packet!

Notes:
Download the ICMP protocol poster from the Library Section at Protocol Analysis Institute - www.packet-level.com.

Laura Chappell is the Senior Protocol Analyst for the Protocol Analysis Institute. She is the author of numerous books and self-paced courseware available online at www.packet-level.com and www.podbooks.com. Laura also lectures on analysis, optimization and cybercrime. Her course schedule is online at www.packet-level.com.