Laura Chappell

Routing Sequences for ICMP

Editor's Note: This article supplements Laura Chappell's session TUT232, "Troubleshooting with ICMP," at Novell BrainShare 2001 in Salt Lake City. (For more information about Novell BrainShare 2001, visit www.novellbrainshare.com.)

Illustration: Norman Felchle

Although routing protocols such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) provide route information to routers on a network, Internet Control Messaging Protocol (ICMP) can provide some routing information to hosts. For example, routers can use ICMP to provide a default gateway setting to a host. Routers can also send ICMP messages to redirect a host to another router that is believed to have an optimal route. (For more information about how IP routers should handle ICMP error messages and query messages, see Section 4.3 of Request For Comments [RFC] 1812, "Requirements for IP Version 4 Routers" at www.rfc-editor.org/go.html.)

ROUTER DISCOVERY

IP hosts typically learn about routes through manual configuration of the default gateway parameter and redirection messages. If a host boots up without a default gateway setting, that host may issue an ICMP Router Solicitation packet to locate a local router. For example, Windows 2000 and 98 hosts automatically send ICMP Router Solicitation packets when they boot up without a default gateway setting.

This process is referred to as ICMP Router Solicitation and ICMP Router Discovery. IP hosts send ICMP Router Solicitations, and routers reply with ICMP Router Advertisements.

By default, the ICMP Router Solicitation packet is sent to the all-routers IP multicast address 224.0.0.2. Although RFC 1812 dictates that IP routers "must support the router part of the ICMP Router Discovery Protocol on all connected networks on which the router supports either IP multicast or IP broadcast addressing," many IP routers do not. If an IP router does not support the router portion of ICMP Router Discovery, the host's Router Solicitation Requests will not be answered.

If an IP host resides on a network that supports multiple IP routers, the IP host may receive multiple replies—one reply from each of the locally connected IP routers. Typically, the hosts accept and use the first reply received as the default gateway.

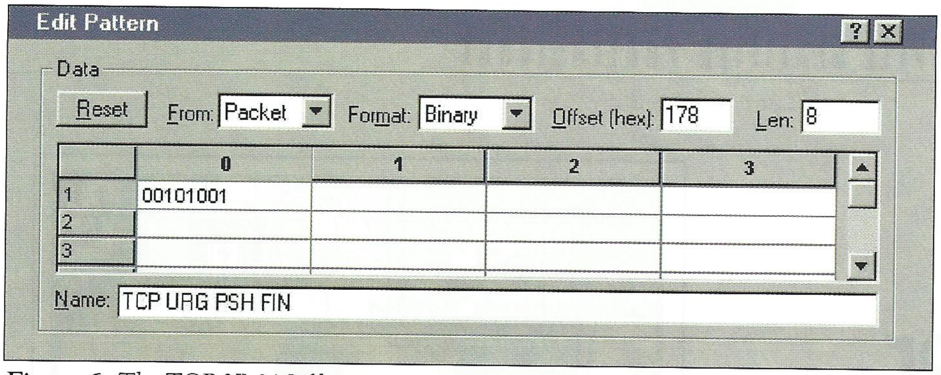
Figure 1 on page 34 shows a internetwork that includes multiple routers and a host that does not have a default gateway setting. In this example, Host A, 10.2.10.2, sends an IP multicast to locate a local router to use as a default gateway. Since Router 1 supports the router portion of ICMP Router Discovery, Router 1 replies with its own IP address. Host A adds Router 1's IP address to its routing tables.

In Figure 1, only one router—the local router (Router 1)—replies to the ICMP Router Solicitation Request generated by Host A. Router 2 is not on the same network segment as Host A, and Router 1 does not forward the IP multicast. Because Host B is already configured with a default gateway, Host B does not need to send an ICMP Router Solicitation Request packet.

You can reconfigure Windows 2000 hosts so that they will not use ICMP Router Solicitation. (You may want to reconfigure Windows 2000 to not use ICMP Router Solicitation if you have manually configured a default gateway.) You simply edit the PerformRouterDiscovery Registry setting as shown in the list below:

REGISTRY INFORMATION	**DETAILS**
Location	HKEY_LOCAL_ MACHINE\SYSTEM\ CurrentControlSet\Services\Tcpip\Parameters \Interfaces\<*interface*>
Data Type	REG_DWORD
Valid Range	0-1
Default Value	1
Present by Default	Yes

Changing the PerformRouterDiscovery value to 0 disables the ICMP Router Discovery process.



Edit Pattern

Data

Reset   From: Packet   Format: Binary   Offset (hex): 178   Len: 8

	0	1	2	3
1	00101001			
2				
3				

Name: TCP URG PSH FIN

Figure 6. *The TCP XMAS filter*

shows the flag setting used in TCP ACK scan packets.)

The purpose of the TCP ACK packet is to simply determine if the host is active. Also, hackers do not then need to use the ping packet.

If the target device is available and the HTTP port is open, the target device sends a TCP RST packet in reply.

TCP SYN/FIN With Fragments Scan

Hackers often use the TCP SYN/FIN With Fragments scan to bypass a filtering device. To perform this scan, hackers fragment a packet inside the TCP header. Unless the filtering device reassembles the packet, this device will not know that the incoming packet is a TCP SYN/FIN packet.

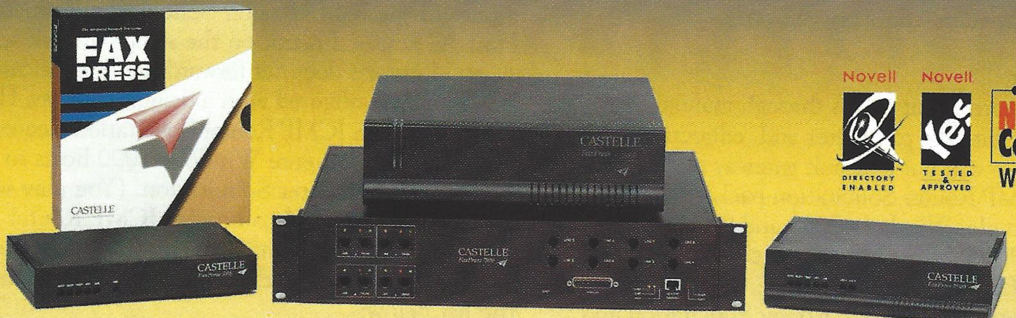
CATCHING SCANS WITH A PROTOCOL ANALYZER

Using a protocol analyzer, you can easily set up a series of filters that can identify the flag patterns used in scan packets. For example, in Figure 6, I created a filter to catch all TCP XMAS scan packets. These packets contain the value 0x29 at the flags' offset in the TCP header.

"Creating Filters to Detect Cyber Attacks" on page 24 will help you identify the most common types of scans and the filters you can use to detect these attacks. In some cases, a single packet signals a problem on the network. In other cases, a low threshold should trigger an alarm.

Since performing a scan is the first step to launching a cyber attack, detecting scans as quickly as possible is important. For more information about building advanced filters for your protocol analyzer, see the "Advanced Packet Filtering" article, which is posted online at www.packet-level.com. You can also attend the "Advanced Network Analysis" session TUT231 at BrainShare 2001 in Salt Lake City.

Laura Chappell has just released Advanced Network Analysis Techniques, *which is available online at www.podbooks.com.* ●



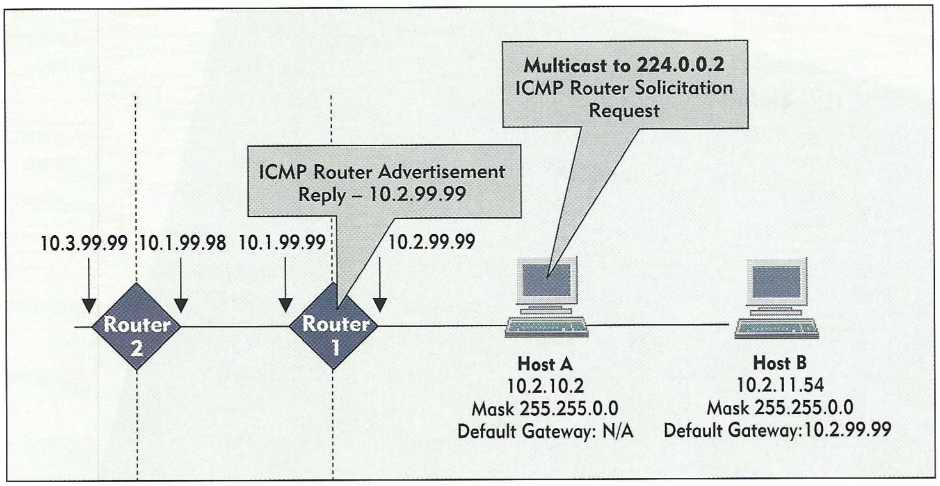


Figure 1. *The route discovery process on a network that includes more than one router*

On Windows 2000 hosts, you can configure the SolicitationAddressBCast Registry setting to use a subnet broadcast (such as 10.2.255.255 in the network shown in Figure 1) during the router discovery process instead of the all-routers multicast address. The SolicitationAddressBCast Registry settings are explained in the following list:

REGISTRY INFORMATION	DETAILS
Location	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<*interface*>
Data Type	REG_DWORD
Valid Range	0-1
Default Value	0
Present by Default	No

Changing SolicitationAddressBCast value to 1 enables the Windows 2000 host to use the IP subnet broadcast to perform ICMP Router Solicitation.

ROUTER ADVERTISEMENT

IP hosts typically learn about routes through the manually configured default gateway setting and the process of redirection. Alternately, some routers can be configured to send periodic ICMP Router Advertisement packets. These periodic ICMP Router Advertisements do not mean that ICMP is a routing protocol. The ICMP Router Advertisements simply allow hosts to passively learn about available routes.

Routers can send these advertisements periodically and in response to ICMP Router Solicitation packets. If configured to do so, routers periodically send unsolicited ICMP Router Advertisements to the all-hosts multicast address 224.0.0.1.

These advertisements usually include the IP address of the router that sent the ICMP Router Advertisement packet. The router also includes a Lifetime value to indicate how long the receiving host should keep the route entry. The default Lifetime value for route entries is 30 minutes.

After 30 minutes has passed, the expired route entry is removed from the route tables. The host may then send a new ICMP Router Solicitation packet or wait and passively listen for a ICMP Router Advertisement packet. The default advertising rate is between seven to ten minutes. (For more information about ICMP Router Advertisements, see RFC 1256, "ICMP Router Discovery Messages" at www.rfc-editor.org/go.html.)

Router Advertisement and Router Solicitation Packets

As mentioned earlier, hosts send Router Solicitation packets, and routers respond with Router Advertisement packets. ICMP Router Solicitation packets use the simple structure shown in Figure 2.

The ICMP Router Solicitation packet does not need to contain any information other than the ICMP Type and Code number. As mentioned earlier in this article, these packets are addressed to the all-router multicast address 224.0.0.2 by default. In some cases, hosts may be configured to send these packets to the broadcast address (in case the local routers do not process multicast packets).

ICMP Router Advertisement packets use the structure shown in Figure 3. These packets include the following fields after the ICMP Checksum field:

- **# of Addresses.** This field specifies the number of router addresses advertised in this packet.
- **Address Size.** This field specifies the number of 4-byte increments used to define each router address advertised. Because this example includes a 4-byte precedence field and a 4-byte IP address field, the Address Size value is 2 (2 x 4 bytes).
- **Lifetime.** This field indicates the maximum number of seconds that this router information may be considered valid.
- **Router Address 1.** This field contains the sending router's IP address.
- **Precedence 1.** This field indicates the Preference value of each router address advertised. Higher values indicate greater preferences. You may configure a higher precedence level at a router (if the router supports the option) to ensure that one router is more likely to become the default gateway for local hosts.

CONCLUSION

ICMP is associated with testing (ping and traceroute), but it actually offers much more information. The ICMP Router Solicitation and Advertisement process is just one example of what ICMP can do. (For more information about ICMP functionality, see the ICMP trace files online at www.packet-level.com/traces.htm and attend the TUT232 session, "Troubleshooting with ICMP," at Novell BrainShare 2001.)

Note. If you want more information about managing your company's TCP/IP network, you can attend Laura Chappell's full-day lecture on "TCP/IP Analysis and Troubleshooting." She will be visiting the following areas: Atlanta on April 19, Dallas on April 28th, and Orange County on May 5. Laura Chappell joins Gary Porter and Joe Doupnik on this three-city lecture tour. For more information about the tour, visit www.conference-bookings.com.

Laura Chappell, a popular writer and lecturer, has just released Advanced Network Analysis Techniques, *which is available online at www.podbooks.com.*

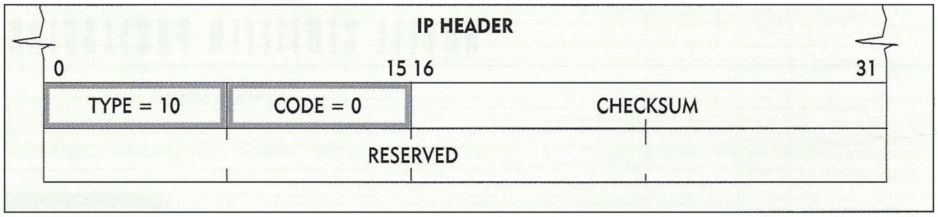


Figure 2. ICMP Router Solicitation packets have a simple structure.

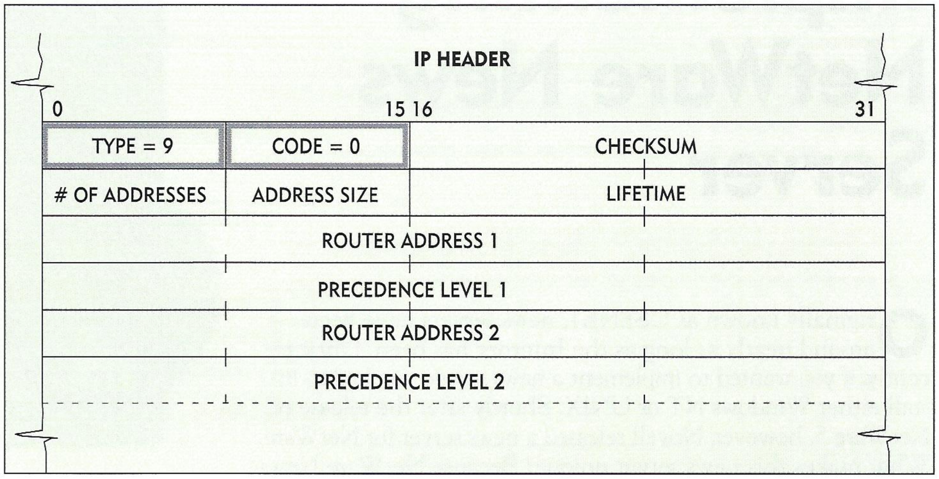


Figure 3. ICMP Router Advertisement packets use a more complex structure than ICMP Router Solicitation packets use.