DATA COMMUNICATIONS MANAGEMENT

WORKING WITH TCP/IP UTILITIES

Gilbert Held

INSIDE
PING; Host_name or IP_Address; Federal Government Web Site; TRACEROUTE;
Command Format; FINGER; NSLOOKUP

OVERVIEW
There are four key TCP/IP utility application programs one can consider using to obtain information about networking devices, network usage, and the general state of a network. The utilities include PING, TRACEROUTE, FINGER, and NSLOOKUP. Of the four utility application programs, this article primarily focuses on the first three. The reason for this focus is that NSLOOKUP operates on the DNS database and the operation of the utility program requires a considerable amount of knowledge concerning the different types of records in the DNS database.

It is important to note that the ability to use one of the four previously mentioned utility programs depends on the manner by which a TCP/IP protocol stack developer includes or excludes certain utility programs. It is common that not all of the four previously mentioned programs are supported by a specific operating system. For example, while the programs PING and TRACEROUTE, implemented under the name TRACERT, are supported by Windows 95 and Windows 98, FINGER and NSLOOKUP are not. Although many UNIX operating systems support all four utility programs, certain flavors of that operating system lack support for one or more of the programs. Similarly, it is important to note that although

PAYOFF IDEA
The TCP/IP protocol suite includes a series of utility application programs that provides network users with the ability to test and troubleshoot a variety of potential network-related problems. In addition, the use of some utility programs can indicate that the network is not the cause of a reported problem, enabling users to turn their attention to an examination of workstation and server performance issues that may be the true culprit, causing what appears to be a network problem. Although TCP/IP utility application programs can provide a significant indication of the state of a network, their use can also result in potential security-related problems. Thus, it is important for network managers and LAN administrators to note how certain utility programs can be improperly used and actions they can take to minimize the impact of their improper utilization.
one or more of the TCP/IP utility programs covered in this article may be supported by several protocol stacks built into different operating systems, the manner in which they operate and the parameters they support can differ between protocol stacks. In fact, as noted later in this article, a popular implementation of the PING utility program includes an option that can be employed — either intentionally or nonintentionally — with the resulting effect equivalent to an unsophisticated denial of service attack. Now that there is an appreciation for the fact that the four key TCP/IP utility programs covered in this article may not be supported by all operating systems and if supported can be implemented with different options, attention can be turned to each utility program. In doing so, this article examines the basic use of each program and the basic parameters supported under one or more operating systems. When applicable, potential security hazards that can result from the improper use of the program and the manner by which network managers and LAN administrators can protect their networks from those hazards will be examined.

PING
PING is a TCP/IP utility application program that is included in every protocol stack with which this author has worked. Those protocol stacks include NetManage and FTP Software TCP/IP protocol stacks developed for use with Windows 3.1, several versions of UNIX, Windows 95, Windows 98, Windows NT, and the beta version of Windows 2000.

The name PING can be traced to two separate historical developments. First, according to some, the similarity in operation between PING and shipboard sonar determined the name. PING operates by generating an Internet Control Message Protocol (ICMP) echo message, which results in the destination address issuing an echo response message. Radar and shipboard sonar is similar in that the sonar unit generates a sonar signal and uses the ping response from the target to obtain a bearing and distance to the target. The distance is obtained by timing the delay between transmitting the signal and receiving its pinged reflection. That time represents the round-trip delay. Thus, dividing the time by two represents the time to the target. Because the velocity of propagation of a sonar wave is known, the time to the target, multiplied by the velocity of propagation, results in the distance to the target. Thus, according to legend, the echo response generated by an echo request was viewed similar to sonar pinging, resulting in the term PING being used for the TCP/IP application.

A second commonly told tale concerning the name of the PING application program reports that the name resulted as an acronym for Packet InterNetwork Groper. In this tale, the echo request message generated by the client is used to elicit or grope a response from the destination. Be-
cause the application was designed to cross network boundaries, it supported internetworking. Thus, the name PING was used as an acronym for Packet InterNetwork Groper.

Regardless of the actual manner by which the name PING evolved, this application utility program typically represents the first tool commonly used to test and troubleshoot network devices. For example, one can use PING to determine if a workstation, server, or another TCP/IP network device recently connected to a network is correctly cabled to the network and the protocol stack is operational and correctly configured. That is, after a device is connected to a network and its TCP/IP protocol stack is configured, one can test the cabling to the network and the operational state of the protocol stack by PINGing the device from another station on the network or located on a different network. If the PING elicits a response, the response informs one that the device is correctly cabled to the network and that the TCP/IP protocol stack is operational. Based on the fact that PING will also return the round-trip delay between source and destination, this application can also provide indirect information about network activity. That is, if round-trip delay time is relatively long in comparison to previously obtained round-trip delay times, the cause would normally be attributable to network congestion.

If one receives a timeout in response to issuing a PING that denotes the absence of an echo response message after a predefined period of time, one should not automatically assume the destination is not available or improperly cabled to a network. If the destination is on a different network, it is possible that one or more intermediary devices, such as a router or gateway, is not operational and the PING cannot reach its destination. As noted later in this article, if one obtains a timeout response to the use of PING when attempting to access an address on a different network, one should turn to the use of the TRACEROUTE utility program prior to concludes that the destination is not operational.

**Command Format**

Although most modern operating systems are based on the use of a graphic user interface (GUI), most implementations of the PING utility program require the use of a command line interface. One common command line interface is:

```
PING [-q] [-v] [-c count] [-s size] {Host_name|IP_Address}
```

Where the command line parameters are as follows:

- q implements the quiet mode, resulting only in the display of summary lines at startup and completion
- v implements verbose mode, resulting in the listing of ICMP packets received in addition to each echo response message
c specifies the number of echo requests (count) sent prior to conclud-
ing the test
s specifies the number of data bytes (size) transmitted with each echo
request message

Host_name or IP_Address Identifies the Target to be PINGed
To illustrate an example of the use of the PING utility, assume that a
computer with the IP address 198.78.46.8 has just been installed and the
host name is gil.feds.gov. To test the cabling of the computer to the net-
work and the operation of the protocol stack on the computer, one can
go to another station on the network and enter the following command:

PING-c 5 gil.feds.gov

This command line would result in the transmission of five echo re-
quest messages to the host address gil.feds.gov. Assume that the re-
sponse was five PING timeout messages, each indicating the lack of a
response from the destination host. Although one might assume that
there is a problem with the destination, it is important to note that rout-
ing is based on the use of IP addresses. Because TCP/IP-compliant de-
vices respond to IP addresses, it is quite possible that the host is up and
operational but, for some reason, an appropriate entry was not made into
the local DNS server to enable the host name to be resolved into an ap-
propriate IP address. Recognizing this potential problem, one would
then retry PING using the IP address of the destination as follows:

PING-c 5 198.78.46.8

The response to the PING would appear similar to the following:

72 bytes from 198.78.46.8 time = 12.2 ms
72 bytes from 198.78.46.8 time = 12.2 ms
72 bytes from 198.78.46.8 time = 12.2 ms
72 bytes from 198.78.46.8 time = 12.2 ms
72 bytes from 198.78.46.8 time = 12.2 ms

If one does not specify the number of data bytes to be used in each
echo request, a default size of 64 is used. Because the ICMP header adds
8 bytes to the data size, the result in the count of echo response packet
size being displayed is 72 bytes. Although the round-trip time for each
echo request to echo response message is shown as being the same at
12.2 ms, it is important to note that this is not always true. When one
uses a host address instead of an IP address, it is important to note that
most times the issuance of multiple echo requests will result in the first
round-trip delay having a longer time value than succeeding times. The reason is that the first PING is delayed by the address resolution process. During the address resolution process, the hostname is converted into an IP address to enable the echo request to be routed toward its destination. If one is using PING to obtain a precise round-trip delay time — such as to determine if a network structure can support voice over IP — it is important to recognize that the first round-trip delay time may significantly exceed succeeding delay times. Thus, it is a good and recommended procedure to issue at least two separate PING commands, permitting the first one to obtain the host IP address via the Address Resolution Protocol (ARP) and place that entry in the ARP table maintained by the PINGing device. Then, the second PING command to the same destination will reflect round-trip delay times that do not include the address resolution process.

In concluding this examination of the use of the PING application utility program, one can turn attention to the format of the program supported by Microsoft Corporation in Windows 95 and Windows 98. Exhibit 1 illustrates the command format for PING displayed in response to entering the command without any command line parameters.

In examining the command line entries supported by Microsoft's implementation of PING, note the -t option. The use of that option results in a continuous PINGing of the destination until the CTRL-BREAK key combination is pressed to interrupt the program.


Options:
-t ping the specified host until interrupted
-a resolve addresses to hostnames
-n count number of echo requests to send
-l size send buffer size
-f set Don't Fragment flag in packet
-i TTL Time To Live
-v TOS Type Of Service
-r count record route for count hops
-s count timestamp for count hops
-j host-list loose source route along host-list
-k host-list strict source route along host-list
-w timeout timeout in milliseconds to wait for each reply
Continuous PINGing requires a continuous response from the destination. Because the destination must suspend what it is doing to respond to the PING, its ability to perform its intended function, such as a Web server responding to HTTP queries, is degraded. In effect, continuous PINGing is often considered an unsophisticated hacker denial of service attack.

Another area of concern with respect to PING is that it can be used to discover network devices. That is, a sophisticated programmer can use PING within a shell program in an attempt to learn the addresses of network devices and then target those devices. To protect against the adverse effects of PING, some organizations use either a firewall or program a router’s access list to prevent PINGs from reaching their network. If a router’s access list is programmed, the denial of PINGs is usually expressed on a universal basis. Because a firewall has a more sophisticated filtering capability, many network managers and LAN administrators will configure the firewall to permit up to five PINGs per source IP address within a predefined period of time. This action permits a reasonable level of PINGing for a legitimate purpose to occur from users outside the organization’s network while precluding denial of service attacks based on the use of PINGs. An alternate option some network managers use is to program a firewall to allow employees behind the firewall to issue outbound PINGs but to bar inbound PINGs. The problem with this solution is the fact that, if every organization implemented it, nobody would be able to legitimately use PING. Having an appreciation for the operation and utilization of PING, one can now focus on the utility program that should be considered as a follow-on to its use — the TRACEROUTE program.

TRACEROUTE
The TRACEROUTE command invokes a program by that name, which provides information about the route packets take from source to destination. If one PINGs a device on a different network, the lack of a response via a timeout does not necessarily mean that the destination device is not operational. Instead, it is possible that one or more intermediate routers or gateways that provide a connection between networks are not operational. Thus, TRACEROUTE can be used to examine the route from source to destination to determine if a path to the destination is available. If a path is available but the destination cannot be reached, this would then indicate that there is a problem with the device previously PINGed.

Operation
TRACEROUTE operates by transmitting a series of User Datagram Protocol (UDP) datagrams to an invalid port address at the destination device.
First, the program transmits three datagrams in sequence, with each datagram having its time-to-live (TTL) field value set to unity. With this setting, each datagram will timeout as soon as it is processed by the first router in the path between the source and destination networks.

After the first router decrements the TTL field value by one and notes its value is zero, it generates an ICMP time exceeded message (TEM) response that indicates the datagram expired and sends it to the great bit bucket in the sky. The TEM response enables the device issuing the TRACEROUTE to compute the round-trip delay to the router for each of the three datagrams in the sequence. Next, the issuing device sets the TTL field value to 2 and transmits another sequence of three UDP datagrams. This sequence of three datagrams flows through the first router, which decrements their TTL field values to 1. However, the next router decrements their TTL field values to zero and returns TEM responses to each datagram, enabling the round-trip delay to the second router in the path to be determined.

This process continues until the datagrams either reach their destination or encounter a broken path. If the datagrams reach their destination, the use of an invalid port number in the UDP header results in the destination device generating an ICMP destination unreachable message in response to each of the three datagrams. This message tells the TRACEROUTE program that the destination was reached and it should terminate its operation. In the event an open path is encountered due to a router or gateway failure, TRACEROUTE terminates its operation when a timer expires. By noting that the last router that responded was not connected to the destination network, one can observe that a wide area network connection or router failure is the reason behind the inability to access a destination device.

Command Format
A commonly used TRACEROUTE command line format is shown below.

```
TRACEROUTE [-m ttl] [-q packets] {IP_Address| Host_name}
```

Where:
- `-m` represents the maximum allowable time-to-live (ttl) value, which is the number of hops allowed prior to the program terminating. The typical default ttl value used by most implementations of TRACEROUTE is 30.
- `-q` represents the number of UDP packets transmitted with each ttl setting. The common default value is 3.

Exhibit 2 illustrates the use of TRACERT from a Windows 95 client to determine the path to a device whose IP address is 205.131.176.15. It should be noted that the author used a commercial Internet service pro-
Exhibit 2 — Using Microsoft’s Windows 95 Version of TRACERT C:\WIND\DOWS>tracert 205.131.176.15

Tracing route to www5.opm.gov [205.131.176.15] over a maximum of 30 hops:

1  446 ms  410 ms  542 ms  hil-c45-068-eth00.as.wcom.net [209.154.36.97]
2  411 ms  407 ms  407 ms  hil-ppp1-fas1-1-0.wan.wcom.net [209.154.36.65]
3  405 ms  400 ms  403 ms  hil-core1-fas4-0-0.wan.wcom.net [205.156.214.145]
4  436 ms  421 ms  444 ms  hyt-core1-atm1-0-3.wan.wcom.net [205.156.223.134]
5  466 ms  451 ms  414 ms  hyt-peer1-fdd4-0.wan.wcom.net [205.156.223.68]
6  481 ms  440 ms  462 ms  hyt-mae-east-pos3-0-0.wan.wcom.net [205.156.223.98]
7  453 ms  445 ms  445 ms  maeeast2.bbnplanet.net [198.32.186.2]
8  453 ms  431 ms  538 ms  p2-2.vienna1 nbr2.bbnplanet.net [4.0.1.93]
9  456 ms  455 ms  559 ms  p1-0.vienna1 nbr3.bbnplanet.net [4.0.5.46]
10 480 ms  473 ms  460 ms  p1-2.atlanta1 nbr1.bbnplanet.net [4.0.5.142]
11 442 ms  465 ms  480 ms  p2-0-0.atlanta1 cr3.bbnplanet.net [4.0.5.113]
12 449 ms  459 ms  500 ms  s0-1-3.usopm.bbnplanet.net [4.0.156.110]
13 473 ms  573 ms  610 ms  www5.opm.gov [205.131.176.15]

Trace complete.
round-trip delay times per hop, it does not average those times. Other implementations of TRACEROUTE provide a statistical summary of round-trip response time. Similarly, other implementations may have one or more optional parameters that allow for control of timeout delays. However, because all versions of TRACEROUTE work in a similar manner, it is important to note that regardless of implementation, its use provides the ability to determine if a path is available to the destination.

**FINGER**
The FINGER utility program provides the ability to determine who is logged onto another computer and information about one or more users. The most common format of FINGER is as follows:

```
FINGER [username]@[host_name | IP_address]
```

If one enters a username, the remote system will, if configured to respond to FINGER, return the username, the user's real name, his process identifier, application being accessed, and terminal port number. If one enters the command without username, some destinations will provide the previously mentioned information for all users on the system.

In an era of privacy issues, many colleges and universities where FINGER was previously enabled have turned it off. In addition, its use enables a hacker to attempt to gain a person's password by noting persons on a system and calling them. Pretending to be the administrator, a common ploy is to tell them that their use of a specific application noted from FINGER caused a lockup and they need the user's password to unlock a process. More often than not, a hacker was able to use FINGER as a starting point for gaining illegal access to different computers. Although Windows NT supports FINGER, neither Windows 95 nor Windows 98 supports it.

**NSLOOKUP**
The last TCP/IP utility program discussed in this article is NSLOOKUP. Here, NS stands for the term “name server” and NSLOOKUP provides the ability to look up information from an organization's DNS server.

NSLOOKUP operates in two modes: interactive and noninteractive. If the program is entered without parameters, the user is placed in its interactive mode of operation. One would then enter the IP address of a DNS server, which would be used for querying DNS records concerning a target destination. Through the use of a range of DNS record types, one can obtain information about individual stations on a network, an organization's mail exchangers, and the set-up of a distant DNS. While the actual query types one is able to use can vary considerably between different implementations of the NSLOOKUP program, a few points concerning its
use can illustrate how it can indicate the reason for certain problems. Assume that the use of a host name always results in the inability to reach a network device, yet one can ping it using its IP address. Through the use of NSLOOKUP, one can determine if an appropriate A record is in the DNS server. If not, this action informs one that a call to the administrator of the DNS is in order.

SUMMARY
TCP/IP utility programs can provide a significant insight to potential and actual network problems. By understanding how the programs operate and using them at appropriate times, one can isolate network problems and initiate action to correct noted problems. Although the use of TCP/IP utility programs will not allow one to note software problems that only a protocol analyzer can denote, their use represents the first line of investigation readers should consider when operations do not appear to be correct.

Gilbert Held is an internationally recognized author and lecturer. Mr. Held is the author of over 40 technical books and 300 articles covering the field of data communications, and can be reached via e-mail at 235-8068@mcimail.com.