

Using administrative tools and utilities to capture network routes to intranet and internet

(netstats, ipconfig, NSlookup, Ping, Pathping, PingTester basic and pro, Traceroute and Visualroute)

OBJECTIVES

Using various DOS-based and WINDOWS-based administrative tools and utilities to capture network, server, routers, switches, and firewall information and understand how these utilities utilize ICMP protocol for their functionality.

PROCEDURE

Find Response Time, Time to live and Target IP Addresses, when typing in a website.

Using **DOS prompt**, Type the following:

1. ping 127.0.0.1 : What does this verify ?
2. *First practice using the two following pinging exercises, PING “Three” additional academia sites around the world (of your choice) and capture information. Now change packet size to 32, 64, and 256 bytes and # of times to 10 and capture all the information.*

Practice with:

- ping www.SFU.ca. use sfu or bcit or ubc.
- ping -l 64 -n 10 www.stanford.edu “to see the results with packets 64 bytes long.

Parameter/ Academia									
	32	64	256	32	64	256	32	64	256
IP Address									
Time To Live(TTL)									
Return Transit Time (RTT)									
Default #of time systems sends a message									

- a. Plot an X-Y graph to display the relationship (if any) between the distance and RTT. Is there any relationship between distance and TTL? Please comment.

- b. Is there a relationship between byte size and TTL and RTT.
 - c. What is your expectation if you decided to ping these sites at different times of the day?
 - d. What can you identify from RTT? Hint: Assume velocity of propagation in Ethernet cable is $0.71C$. C being speed of light in free space.
- 3. Try pathping command and capture additional information about the same sites. What additional information do you capture as compared to “ping”?
 - 4. Try tracert for above sites and capture all information.

5. Type “ipconfig/All” at DOS prompt and explain information displayed on screen.
6. Type “netstat” at DOS prompt and explain information displayed on screen.
7. Use netstat with various options. What different parameters can you capture?
8. Use nslookup and capture all information.

Windows Utilities:

9. Download free version of Visual-route Lite from internet and install. Try BCIT, UBC and SFU websites and capture all information displayed. Briefly explain parameters you discover.

Additional Questions:

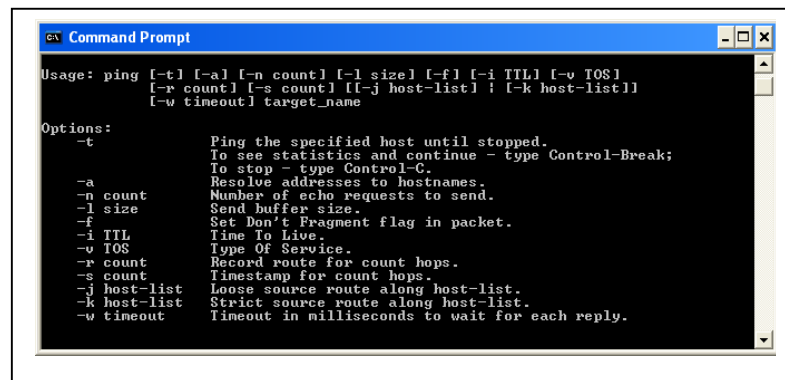
- What does ping stand for?
- Draw the packet diagram (not frame format) used by *ping*, *pathping* and *tracert* utilities. Hint: Check web for help.
- Can ping, pathping and tracert “function” without using the ICMP protocol? Your answer should contain a summary of ICMP protocol operation.
- What information do you capture from Visualroute? Find if any sites have parallel servers, firewalls or any distinct information.

Appendix:

THE PING PROCESS

1. The source host generates an [ICMP](#) protocol data unit.
2. The [ICMP](#) PDU is encapsulated in an [IP datagram](#), with the *source* and *destination* [IP addresses](#) in the [IP header](#). At this point the datagram is most properly referred to as an [ICMP ECHO datagram](#), but we will call it an [IP datagram](#) from here on since that's what it looks like to the networks it is sent over.
3. The source host notes the local time on it's clock as it transmits the [IP datagram](#) towards the destination. Each host that receives the [IP datagram](#) checks the destination address to see if it matches their own [address](#) or is the *all hosts address* (all 1's in the host field of the [IP address](#)).
4. If the destination [IP address](#) in the [IP datagram](#) does not match the local host's address, the [IP datagram](#) is forwarded to the [network](#) where the [IP address](#) resides.
5. The destination host receives the [IP datagram](#), finds a match between itself and the destination address in the [IP datagram](#).
6. The destination host notes the [ICMP ECHO](#) information in the [IP datagram](#), performs any necessary work then destroys the original [IP/ICMP ECHO datagram](#).
7. The destination host creates an [ICMP ECHO REPLY](#), encapsulates it in an [IP datagram](#) placing it's own [IP address](#) in the source [IP address](#) field, and the original sender's [IP address](#) in the destination field of the [IP datagram](#).
8. The new [IP datagram](#) is routed back to the originator of the PING. The host receives it, notes the time on the clock and finally prints PING output information, including the elapsed time.

The process above is repeated until all requested [ICMP ECHO](#) packets have been sent and their responses have been received or the default 2-second timeout expired. The default 2-second timeout is local to the host initiating the PING and is NOT the Time-To-Live value in the datagram.



```
Command Prompt

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] target_name

Options:
  -t             Ping the specified host until stopped.
                 To see statistics and continue - type Control-Break;
                 To stop - type Control-C.
  -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.
```

Using the pathping command

The **pathping** command is a route tracing tool that combines features of the **ping** and **tracert** commands with additional information that neither of those tools provides. The **pathping** command sends packets to each router on the way to a final destination over a period of time, and then computes results based on the packets returned from each hop. Since the command shows the degree of packet loss at any given router or link, it is easy to determine which routers or links might be causing network problems. A number of switches are available, as shown in the following table.

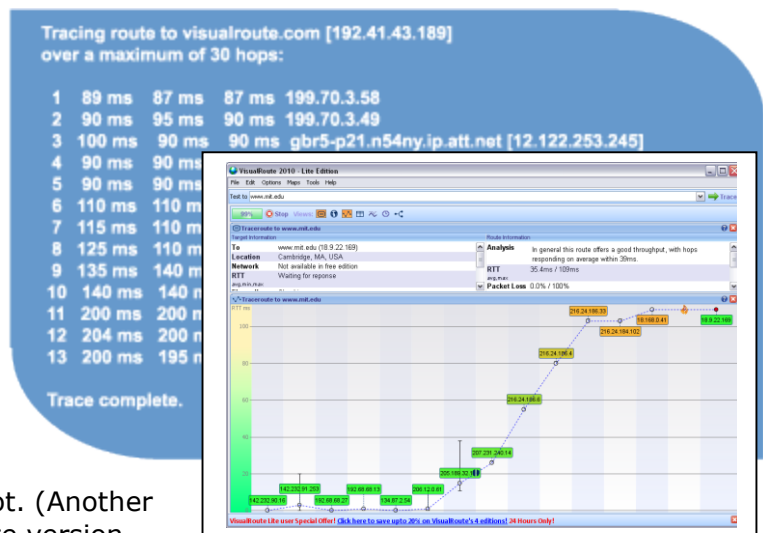
Switch	Name	Function
-n	Hostnames	Does not resolve addresses to host names.
-h	Maximum hops	Maximum number of hops to search for target.
-g	Host-list	Loose source route along host list.
-p	Period	Number of milliseconds to wait between pings.
-q	Num_queries	Number of queries per hop.
-w	Timeout	Waits this many milliseconds for each reply.
-T	Layer Two tag	Attaches a Layer Two priority tag (for example, for IEEE 802.1p) to the packets and sends it to each of the network devices in the path. This helps in identifying the network devices that do not have Layer Two priority configured properly. The -T switch is used to test for Quality of Service (QoS) connectivity.
-R	RSVP test	Checks to determine whether each router in the path supports the Resource Reservation Protocol (RSVP), which allows the host computer to reserve a certain amount of bandwidth for a data stream.

The default number of hops is 30, and the default wait time before a time-out is 3 seconds. The default period is 250 milliseconds, and the default number of queries to each router along the path is 100.

The following is a typical **pathping** report. The compiled statistics that follow the hop list indicate packet loss at each individual router.

Tracert (and ping) are both command line utilities that are built into Windows and most other computer systems. The basic tracert command syntax is "tracert hostname".

For example, "tracert www.apple.com" and the output might look like:



Here is a similar trace route as it would appear in a [VisualRoute](#) snapshot. (Another Utility on the web) – Obtain the free lite version from Shareout in 4550 folder, install it and take snapshots and include in the report.

Discover the path: Tracert sends an ICMP echo packet, but it takes advantage of the fact that most Internet routers will send back an ICMP 'TTL expired in transit' message if the TTL field is ever decremented to zero by a router. Using this knowledge, we can discover the path taken by IP Packets.

How tracert works: Tracert sends out an ICMP echo packet to the named host, but with a TTL of 1; then with a TTL of 2; then with a TTL of 3 and so on. Tracert will then get 'TTL expired in transit' message back from routers until the destination host computer finally is reached and it responds with the standard ICMP 'echo reply' packet.

Try it yourself: To see this in action yourself, just use the '-i' option of ping, which allows you to set the TTL value of outgoing ping packets. For example, "ping -i 1 visualroute.com" and you will see "Reply from 199.70.3.58: TTL expired in transit" (where the router IP Address returned, 199.70.3.58, is specific to your Internet connection). Then again with "ping -i 2 visualroute.com", and get back "Reply from 199.70.3.49: TTL expired in transit", and so on. Finally at "ping -i 13 visualroute.com" you get "Reply from 192.41.43.189: bytes=32 time=198ms TTL=245", which is the destination host responding.

Round Trip Times: Each millisecond (ms) time in the table is the round-trip time that it took (to send the ICMP packet and to get the ICMP reply packet). The faster (smaller) the times the better. A *ms* times of 0 mean that the reply was faster than the computers timer of 10 milliseconds, so the time is actually somewhere between 0 and 10 milliseconds.

Packet Loss: Packet loss kills throughput. So, having no packet loss is critical to having a connection to the Internet that responds well. A slower connection with zero packet loss can easily outperform a faster connection with some packet loss. Also, packet loss on the last hop, the destination, is what is most important. Sometimes routers in-between will not send ICMP "TTL expired in transit" messages, causing what looks to be high packet loss at a particular hop, but all it means is that the particular router is not responding to ICMP echo.

Ping

The basic ping command syntax is "ping *hostname*". For example, "ping visualroute.com" and the output might look like:

Pinging visualroute.com [192.41.43.189] with 32 bytes of data:

```
Reply from 192.41.43.189: bytes=32 time=218ms TTL=245
Reply from 192.41.43.189: bytes=32 time=210ms TTL=245
Reply from 192.41.43.189: bytes=32 time=205ms TTL=245
Reply from 192.41.43.189: bytes=32 time=204ms TTL=245
```

```
Ping statistics for 192.41.43.189:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 204ms, Maximum = 218ms, Average = 209ms
```

TTL reply: Ping sends an ICMP echo packet (with the TTL value set to the host default) to the host listed on the ping command line. Ping expects back an ICMP 'echo reply' packet. The millisecond time displayed is the round trip time. The "TTL=245" above says that the incoming ICMP echo reply packet has its TTL field set to 245. Because this value was decremented by one at each hop on the way back, this tells us that visualroute.com is probably setting the initial TTL value to 255.

TTL Expired in Transit: Most computers today initialize the TTL value of outgoing IP Packets 128 or higher. If you ever see a reply above with a "TTL=5" (or some other low TTL number) this tells you that the computer being pinged should most likely have its default TTL value increased. Otherwise, anyone trying to communicate with the computer that is at a hop count higher than the TTL will not be able to communicate with the computer. For example, if you are 40 hops away from www.xyz.com, and www.xyz.com sets TTL fields in IP packets that it sends out to 32, the IP Packets will not reach you. They will 'expire in transit' before they reach you.

Discover your TTL: To discover the default TTL value of your computer, 'ping localhost' and examine the TTL reply value. For older Windows machines this value is 32. For newer Windows machines, this value is 128.

Pathping

Pathping is a TCP/IP based utility that provides useful information about network latency and network loss at intermediate hops between a source address and a destination address.

It is a Windows based command-line tool is similar to the **tracert** tool in a sense that it traces the path that an Internet Protocol (IP) packet takes from a source to its destination.

Pathping will determine the path taken to the destination the same way like tracert, but provides more information.

Where is PATHPING used?

The pathping command is used to visually see a network packet being sent and received. It also shows the amount of network hops required for that packet to get to its destination.

Pathping provides additional information such as **network latency** and **network loss** which makes it a good tool for researching network issues.

Pathping syntax

Windows XP Syntax

pathping [-g host-list] [-h maximum hops] [-i address] [-n]
[-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]
[-4] [-6] target name

-g host-list

Loose source route along host-list.

-h maximum hops

Maximum number of hops to search for target.

-n

Prevents pathping from attempting to resolve the IP addresses of intermediate routers to their names. This is good to consider if the problem is with name resolution, or if DNS for example is not configured on the. The time spent trying to contact a name server can be avoided using this switch.

-h

Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-i address

Use the specified source address.

-P

Specifies the number of milliseconds to wait between consecutive pings. The default is 250 milliseconds (1/4 second).

-q

Specifies the number of Echo Request messages sent to each router in the path. The default is 100 queries.

-w

Specifies the number of milliseconds to wait for each reply. The default is 3000 milliseconds (3 seconds).

/?

Displays help at the command prompt

How is Pathping used?

In Windows 2000 or XP, go to Start -> Run, and type cmd and press the ENTER.

To run the pathping type pathping [hostname] where the [hostname] is the name of the server that you are connection testing.

This test will take a while. It will generate a list of the connection along the way and some information about the speed of the steps too.

Useful tip

If you have difficulty copying the pathping information from the command prompt screen, you can send the pathping output to a text file. In that case, type:

pathping [hostname] > C:\pathping_output.txt

What is Time-to-Live?

Time to Live or TTL is a term related to networking concepts.

ICMP Protocol Overview

Internet Control Message Protocol (ICMP), documented in [RFC 792](#), is a required protocol tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation. Of course, since ICMP uses IP, ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problem. Some of ICMP's functions are to:

- **Announce network errors**, such as a host or entire portion of the network being unreachable, due to some type of failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.
- **Announce network congestion**. When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP *Source Quench* messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed. Of course, generating too many Source Quench messages would cause even more network congestion, so they are used sparingly.
- **Assist Troubleshooting**. ICMP supports an *Echo* function, which just sends a packet on a round-trip between two hosts. [Ping](#), a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round-trip times and computing loss percentages.
- **Announce Timeouts**. If an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact. [TraceRoute](#) is a tool which maps network routes by sending packets with small TTL values and watching the ICMP timeout announcements.

ping

See the [help pages](#) for ping and tracert.

When you invoke ping, the default value is to send 32 bytes of data.

How many bits is 32 bytes of data?

Ping is an acronym for **p**acket **i**nternet **g**roper, a utility that sends a short request to a remote computer and elicits a response from that computer.

[Ping, Tracert and PathPing](#)

[Ping and Tracert](#)

If you are unable to contact to a remote server, there are two common tools that you can use. Use the ping command to verify that a host computer can connect to the TCP/IP network and network resources. Use the tracert command to examine the route taken to a destination.

[Using ping](#)

When troubleshooting, you can use ping to verify IP-level connectivity. You should perform the following steps when using ping:

1. Ping the loopback address to verify that TCP/IP is configured correctly on the local computer - ping 127.0.0.1
2. Ping the IP address of the local computer to verify that it was added to the network correctly - ping *IP_address_of_local_host*
3. Ping the IP address of the default gateway to verify that the default gateway is functioning and that you can communicate with a local host on the local network - ping *IP_address_of_default_gateway*
4. Ping the IP address of a remote host to verify that you can communicate through a router - ping *IP_address_of_remote_host*

If you can ping a remote computer's IP but not the ComputerName (Time out), this is likely caused by a name resolution failure, rather than network connectivity. You need to check the network settings such as DHCP, DNS, WINS and NetBIOS over TCP/IP.

If you cannot ping both IP and ComputerName, 1) Ping the loopback address (by using the ping 127.0.0.1 command) to verify that TCP/IP is installed and working correctly on the local computer. 2) Ping the IP address of the local computer to verify that it was added to the network correctly. 3) Ping the IP address of the default gateway to verify that the gateway is functional and it is possible to connect to a local host on the local network. You can obtain the IP address of the local default gateway by using the *ipconfig /renew* command. 4) Ping the IP address of another remote host to verify that you can communicate through a router.

To Test Connections by Using Tracert.exe

Tracert.exe is a route-tracing utility that you can use to determine the network path to a destination. To determine the path that a packet takes on the network and where that path may be ending.

For example, your LAN works fine but no one can access the Internet. You may want to use tracert to determine the network path to a Internet destination like yahoo.com before you call your ISP. You

can use `tracert` to examine the results to determine the length of time that the packet took to reach each network segment and the point at which the connection may stop working.

PathPing display all routers along the way

Using PathPing can displays information for the destination computer and all routers along the way. For example, to display the information of all router paths to `yahoo.com`, use command *`pathping yahoo.com`*.

