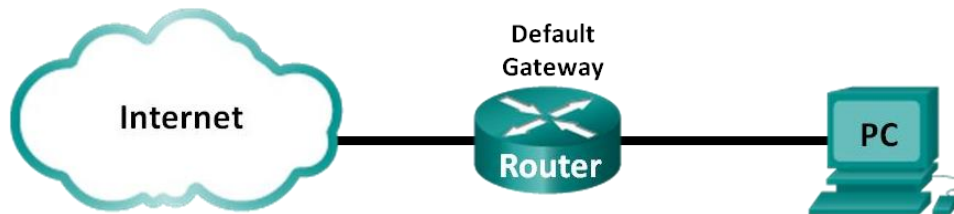




Lab - Testing Network Latency with Ping and Traceroute

Topology



Objectives

Part 1: Use Ping to Document Network Latency

Part 2: Use Traceroute to Document Network Latency

Background / Scenario

To obtain realistic network latency statistics, this activity must be performed on a live network. Be sure to check with your instructor for any local security restrictions against using the **ping** command on the network.

Instructor Note: Some institutions disable ICMP echo replies throughout the network. Before students begin this activity, make sure there are no local restrictions related to ICMP datagrams. This activity assumes that ICMP datagrams are not restricted by any local security policy.

The purpose of this lab is to measure and evaluate network latency over time, and during different periods of the day to capture a representative sample of typical network activity. This will be accomplished by analyzing the return delay from a distant computer with the **ping** command. Return delay times, measured in milliseconds, will be summarized by computing the average latency (mean) and the range (maximum and minimum) of the delay times.

Required Resources

- 1 PC (Windows 10,8,7, or Vista with Internet access)

Part 1: Use Ping to Document Network Latency

In Part 1, you will examine network latency to several websites in different parts of the globe. This process can be used in an enterprise production network to create a performance baseline.

Introduction:

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. It's usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

For example, you might find that there are no responses when pinging a network printer, only to find out that the printer is offline and its cable needs replaced. Or maybe you need to ping a router to verify that your computer can connect to it, to eliminate it as a possible cause for a networking issue.



Ping Command Availability

```
Command Prompt

C:\Users\student5>ping /?

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] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] 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 (IPv4-only).
  -i TTL       Time To Live.
  -v TOS       Type Of Service (IPv4-only. This setting has been deprecated
               and has no effect on the type of service field in the IP
               Header).
  -r count     Record route for count hops (IPv4-only).
  -s count     Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout   Timeout in milliseconds to wait for each reply.
  -R           Use routing header to test reverse route also (IPv6-only).
               Per RFC 5095 the use of this routing header has been
               deprecated. Some systems may drop echo requests if
               this header is used.
  -S srcaddr   Source address to use.
  -c compartment Routing compartment identifier.
  -p           Ping a Hyper-V Network Virtualization provider address.
  -4           Force using IPv4.
  -6           Force using IPv6.
```

The ping command is available from within the Command Prompt in Windows 10, Windows 8, Windows 7, Windows Vista, and Windows XP operating systems. It's also available in older versions of Windows like Windows 98 and 95. This command can also be found in Command Prompt in the Advanced Startup Options and System Recovery Options repair/recovery menus.

Ping Command Syntax

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [-w timeout] [-R] [-S srcaddr] [-p] [-4] [-6] target [/?]

Ping Command Options	
Item	Explanation
-t	Using this option will ping the <i>target</i> until you force it to stop by using Ctrl+C .
-a	This ping command option will resolve, if possible, the hostname of an IP address <i>target</i> .
-n count	This option sets the number of ICMP Echo Requests to send, from 1 to 4294967295. The ping command will send 4 by default if -n isn't used.
-l size	Use this option to set the size, in bytes , of the echo request packet from 32 to 65,527. The ping command will send a 32-byte echo request if you don't use the -l option.
-f	Use this ping command option to prevent ICMP Echo Requests from being fragmented by routers between you and the <i>target</i> . The -f option is most often used to troubleshoot Path Maximum Transmission Unit (PMTU) issues.
-i TTL	This option sets the Time to Live (TTL) value, the maximum of which is 255.
-v TOS	This option allows you to set a Type of Service (TOS) value. Beginning in Windows 7, this option no longer functions but still exists for compatibility reasons.

Ping Command Options

-r count	Use this ping command option to specify the number of <u>hops</u> between your computer and the <i>target</i> computer or device that you'd like to be recorded and displayed. The maximum value for <i>count</i> is 9, so use the <u>tracert command</u> instead if you're interested in viewing all the hops between two devices.
-s count	Use this option to report the time, in Internet Timestamp format, that each echo request is received and echo reply is sent. The maximum value for <i>count</i> is 4, meaning that only the first four hops can be time stamped.
-w timeout	Specifying a <i>timeout</i> value when executing the ping command adjusts the amount of time, in milliseconds, that ping waits for each reply. If you don't use the -w option, the default timeout value of 4000 is used, which is 4 seconds.
-R	This option tells the ping command to trace the round trip path.
-S srcaddr	Use this option to specify the source address.
-p	Use this switch to ping a <i>Hyper-V Network Virtualization</i> provider address.
-4	This forces the ping command to use IPv4 only but is only necessary if <i>target</i> is a hostname and not an IP address.
-6	This forces the ping command to use IPv6 only but as with the -4 option, is only necessary when pinging a hostname.
<i>target</i>	This is the destination you wish to ping, either an IP address or a hostname.
/?	Use the <u>help switch</u> with the ping command to show detailed help about the command's several options.

Ping Command Examples

Below are several examples of commands that use ping.

PING GOOGLE.COM

```
ping -n 5 -l 1500 www.google.com
```

In this example, the ping command is used to ping the hostname *www.google.com*. The **-n** option tells the ping command to send 5 ICMP Echo Requests instead of the default of 4, and the **-l** option sets the packet size for each request to 1500 bytes instead of the default of 32 bytes.

The result displayed in the Command Prompt window will look something like this:

```
Reply from 172.217.1.142: bytes=1500 time=30ms TTL=54
Reply from 172.217.1.142: bytes=1500 time=30ms TTL=54
Reply from 172.217.1.142: bytes=1500 time=29ms TTL=54
Reply from 172.217.1.142: bytes=1500 time=30ms TTL=54
Reply from 172.217.1.142: bytes=1500 time=31ms TTL=54
Ping statistics for 172.217.1.142:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 31ms, Average = 30ms
```

The *0% loss* reported under *Ping statistics for 172.217.1.142* explains that each ICMP Echo Request message sent to *www.google.com* was returned. This means that, as far as this network connection goes, it can communicate with Google's website just fine.

PING LOCALHOST

```
ping 127.0.0.1
```

In the above example, we're pinging *127.0.0.1*, also called the IPv4 localhost IP address or IPv4 loopback IP address, without options. Using the ping command with this address is an excellent way to test that Windows' network features are working properly but it says nothing about your own network hardware or your connection to any other computer or device. The IPv6 version of this test would be **ping ::1**.



FIND HOSTNAME WITH PING

```
ping -a 192.168.1.22
```

In this example, we're asking the ping command to find the hostname assigned to the `192.168.1.22` IP address, but to otherwise ping it as normal. The command might resolve the IP address, `192.168.1.22`, as the hostname `J3RTY22`, for example, and then execute the remainder of the ping with default settings.

Step 1: Verify connectivity.

Ping the following Regional Internet Registry (RIR) websites to verify connectivity:

```
C:\Users\User1> ping www.arin.net
```

```
C:\Users\User1> ping www.lacnic.net
```

```
C:\Users\User1> ping www.afrinic.net
```

```
C:\Users\User1> ping www.apnic.net
```

Note: Because `www.ripe.net` does not reply to ICMP requests, it cannot be used for this lab.



Step 2: Collect network data.

You will collect a sufficient amount of data to compute statistics on the **ping** output by sending out 25 echo requests to each address listed in Step 1. Record the results for each website to text files.

- a. At the command prompt, type **ping** to list the available options.

```
C:\Users\User1> ping
```

```
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] [-R] [-S srcaddr] [-4] [-6] 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 (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated

<output omitted>

- b. Using the **ping** command with the count option, you can send 25 echo requests to the destination as illustrated below. Furthermore, it will create a text file with filename of **arin.txt** in the current directory. This text file will contain the results of the echo requests.

```
C:\Users\User1> ping -n 25 www.arin.net > arin.txt
```

Note: The terminal remains blank until the command has finished, because the output has been redirected to a text file, **arin.txt**, in this example. The **>** symbol is used to redirect the screen output to the file and overwrite the file if it already exists. If appending more results to the file is desired, replace **>** with **>>** in the command.

- c. Repeat the **ping** command for the other websites.

```
C:\Users\User1> ping -n 25 www.afrinic.net > afrinic.txt
```

```
C:\Users\User1> ping -n 25 www.apnic.net > apnic.txt
```

```
C:\Users\User1> ping -n 25 www.lacnic.net > lacnic.txt
```

Step 3: Verify data collection.

To see the results in the file created, use the **more** command at the command prompt.

```
C:\Users\User1> more arin.txt

Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
<output omitted>
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45

Ping statistics for 192.149.252.75:
    Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 107ms, Maximum = 121ms, Average = 111ms
```

Note: Press the Spacebar to display the rest of the file or press **q** to exit.

To verify that the files have been created, use the **dir** command to list the files in the directory. Also the wildcard ***** can be used to filter only the text files.

```
C:\Users\User1> dir *.txt

Volume in drive C is OS
Volume Serial Number is 0A97-D265

Directory of C:\Users\User1

02/07/2013  12:59 PM                1,642 afrinic.txt
02/07/2013  01:00 PM                1,615 apnic.txt
02/07/2013  12:40 PM                1,641 arin.txt
02/07/2013  12:58 PM                1,589 lacnic.txt
               4 File(s)              6,487 bytes
               0 Dir(s)  34,391,453,696 bytes free
```

Record your results in the following table.

	Minimum	Maximum	Average
www.afrinic.net	359 ms	389 ms	369 ms
www.apnic.net	201	210	204
www.arin.net	107	121	112
www.lacnic.net	216	226	218

Compare the delay results. How is delay affected by geographical location?

In most instances, the response time is longer when compared to the physical distance to the destination.

Part 2: Use Traceroute to Document Network Latency

The routes traced may go through many hops and a number of different ISPs depending on the size of the ISPs and the location of the source and destination hosts. The **traceroute** commands can also be used to observe network latency. In Part 2, the **tracert** command is used to trace the path to the same destinations in Part 1.

The **tracert** command uses ICMP TTL Exceed packets and ICMP echo replies to trace the path.

Step 1: Use the tracert command and record the output to text files.

Copy the following commands to create the traceroute files:

```
C:\Users\User1> tracert www.arin.net > traceroute_arin.txt
C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt
C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt
C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt
```

Step 2: Use the more command to examine the traced path.

- a. Use the **more** command to access the content of these files:

```
C:\Users\User1> more traceroute_arin.txt
```

```
Tracing route to www.arin.net [192.149.252.75]
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	11 ms	12 ms	11 ms	10.39.0.1
3	10 ms	15 ms	11 ms	172.21.0.116
4	19 ms	10 ms	11 ms	70.169.73.90
5	13 ms	10 ms	11 ms	chnddsrj01-ae2.0.rd.ph.cox.net [70.169.76.229]
6	72 ms	71 ms	70 ms	mrfddsrj02-ae0.0.rd.dc.cox.net [68.1.1.7]
7	72 ms	71 ms	72 ms	68.100.0.146
8	74 ms	83 ms	73 ms	172.22.66.29
9	75 ms	71 ms	73 ms	172.22.66.29
10	74 ms	75 ms	73 ms	wsip-98-172-152-14.dc.dc.cox.net [98.172.152.14]
11	71 ms	71 ms	71 ms	host-252-131.arin.net [192.149.252.131]
12	73 ms	71 ms	71 ms	www.arin.net [192.149.252.75]

```
Trace complete.
```

In this example, it took less than 1 ms to receive a reply from the default gateway (192.168.1.1). In hop count 6, the round trip to 68.1.1.7 took an average of 71 ms. For the round trip to the final destination at www.arin.net took an average of 72 ms.

Between lines 5 and 6, there is more network delay as indicated by the round trip time increase from an average of 11 ms to 71 ms

- b. Perform the same analysis with the rest of the tracert results.

What can you conclude regarding the relationship between the roundtrip time and geographical location?

In most instances, the response time is longer when compared to the physical distance to the destination.

Reflection

1. The **tracert** and **ping** results can provide important network latency information. What do you need to do if you want an accurate baseline picture regarding network latency for your network?

Answers will vary. You will need to perform careful delay analysis over successive days and during different periods of the day.

2. How can you use the baseline information?

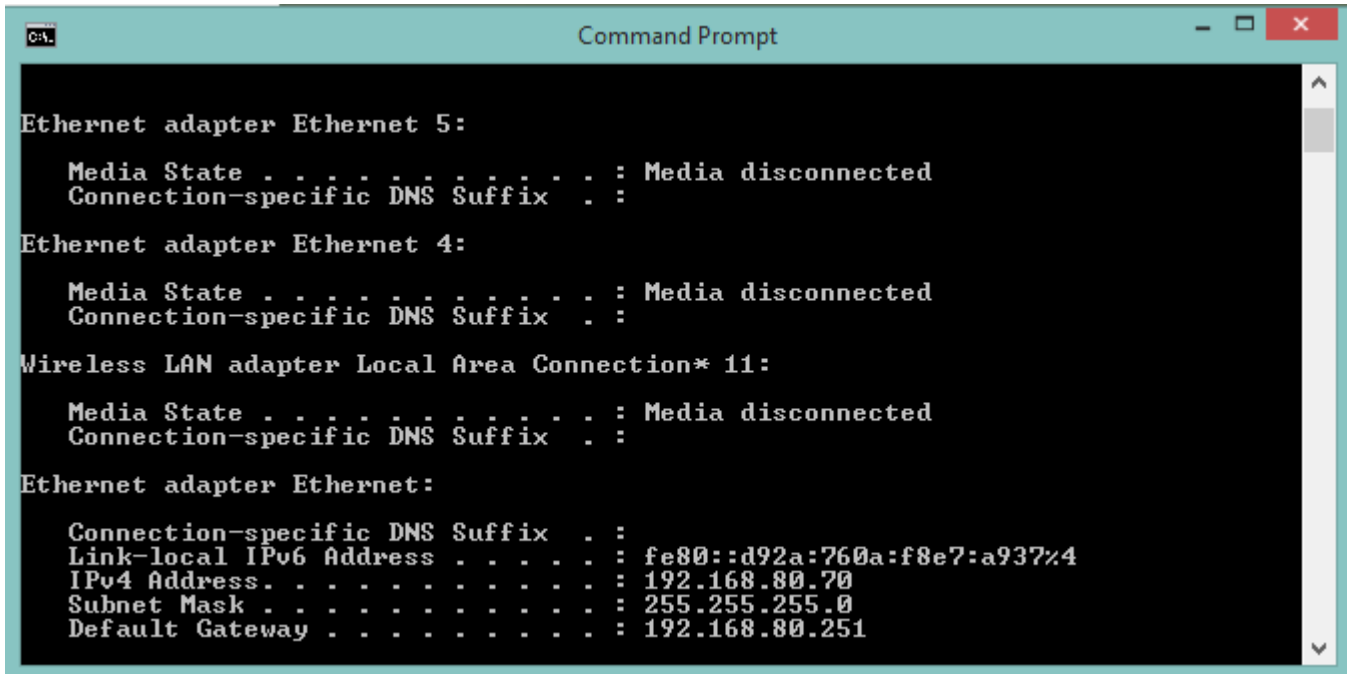
You can compare baseline data against current data to determine if there has been a change in network response times. This analysis may assist with troubleshooting network issues and scheduling of routine data transfer during off-peak hours.

Part 3: ipconfig - Windows Command Line Utility

In Windows, ipconfig is a console application designed to run from the Windows command prompt. This utility allows you to get the IP address information of a Windows computer. It also allows some control over your network adapters, IP addresses (DHCP-assigned specifically), even your DNS cache. Ipconfig replaced the older winipcfg utility.

Using ipconfig

From the command prompt, type ipconfig to run the utility with default options. The output of the default command contains the IP address, network mask, and gateway for all physical and virtual network adapters.



```
Command Prompt

Ethernet adapter Ethernet 5:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Ethernet adapter Ethernet 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d92a:760a:f8e7:a937%4
    IPv4 Address. . . . . : 192.168.80.70
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.80.251
```

The **ipconfig** command supports several command line options. The command

```
ipconfig/?
```

displays the set of available options.

Ipconfig /all

This option displays the same IP addressing information for each adapter as the default option. Additionally, it displays DNS and WINS settings for each adapter as well as a whole host of additional information.

Ipconfig /release

This option terminates any active TCP/IP connections on all network adapters and releases those IP addresses for use by other applications. **Ipconfig/release** can be used with specific Windows connection names. In this case, the command affects only the specified connections, not all connections. The command accepts either full connection names or wildcard names. Examples:

```
ipconfig /release "Local Area Connection 1"
ipconfig /release *Local*
```

Ipconfig /renew

This option re-establishes TCP/IP connections on all network adapters. As with the release option, **ipconfig /renew** takes an optional connection name specifier. Both /renew and /release options only work on clients configured for dynamic (DHCP) addressing.

Part 4: How to Use the Netstat Command

The netstat command, meaning network statistics, is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices.

Specifically, the netstat command can show details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.

Netstat Command Availability

The netstat command is available from within the Command Prompt in most versions of Windows including Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server operating systems, and some older versions of Windows, too.

Netstat is a cross-platform command, which means it's also available in other operating systems like macOS and Linux.

Netstat Command Syntax

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p protocol] [-r] [-s] [-t] [-x] [-y] [time_interval] [/?]

```
Media State . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\student5>netstat

Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:5939          Student:49185           ESTABLISHED
TCP   127.0.0.1:49185        Student:5939            ESTABLISHED
TCP   127.0.0.1:56754        Student:56755           ESTABLISHED
TCP   127.0.0.1:56755        Student:56754           ESTABLISHED
TCP   127.0.0.1:61862        Student:61863           ESTABLISHED
TCP   127.0.0.1:61863        Student:61862           ESTABLISHED
TCP   192.168.80.70:49156    Acc-PC:51001            TIME_WAIT
TCP   192.168.80.70:49156    Acc-PC:51002            TIME_WAIT
```

Netstat Command List

Option	Explanation
netstat	Execute the netstat command alone to show a relatively simple list of all active TCP connections which, for each one, will show the local IP address (your computer), the foreign IP address (the other computer or network device), along with their respective port numbers, as well as the TCP state.
-a	This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.
-b	This netstat switch is very similar to the -o switch listed below, but instead of displaying the PID, will display the process's actual file name. Using -b over -o might seem like it's saving you a step or two but using it can sometimes greatly extend the time it takes netstat to fully execute.
-e	Use this switch with the netstat command to show statistics about your network connection. This data includes bytes, unicast packets, non-unicast packets, discards, errors, and unknown protocols received and sent since the connection was established.
-f	The -f switch will force the netstat command to display the Fully Qualified Domain Name (FQDN) for each foreign IP addresses when possible.
-n	Use the -n switch to prevent netstat from attempting to determine host names for foreign IP addresses. Depending on your current network connections, using this switch could considerably reduce the time it takes for netstat to fully execute.
-o	A handy option for many troubleshooting tasks, the -o switch displays the process identifier (PID) associated with each displayed connection. See the example below for more about using netstat -o.
-p	Use the -p switch to show connections or statistics only for a particular protocol. You can not define more than one protocol at once, nor can you execute netstat with -p without defining a protocol.
protocol	When specifying a protocol with the -p option, you can use tcp, udp, tcpv6, or udpv6. If you use -s with -p to view statistics by protocol, you can use icmp, ip, icmpv6, or ipv6 in addition to the first four I mentioned.
-r	Execute netstat with -r to show the IP routing table. This is the same as using the route command to execute route print.
-s	The -s option can be used with the netstat command to show detailed statistics by protocol. You can limit the statistics shown to a particular protocol by using the -soption and specifying that protocol, but be sure to use -s before -p protocol when using the switches together.
-t	Use the -t switch to show the current TCP chimney offload state in place of the typically displayed TCP state.
-x	Use the -x option to show all NetworkDirect listeners, connections, and shared endpoints.
-y	The -y switch can be used to show the TCP connection template for all connection. You cannot use -y with any other netstat option.
time_interval	This is the time, in seconds, that you'd like the netstat command to re-execute automatically, stopping only when you use Ctrl-C to end the loop.
/?	Use the help switch to show details about the netstat command's several options.