Department of
Computer Science and Engineering

Title: Basic Ping and Traceroute commands

Computer Networking Lab
CSE 312

Green University of Bangladesh

1 Objective(s)

- To use the ipconfig command to test and visualize different network adapters.
- To use the ping command to verify simple TCP/IP network connectivity.
- To use the tracert/trace route command to verify TCP/IP connectivity.

2 Problem analysis

Two tools that are indispensable when testing TCP/IP network connectivity are ping and tracert. The **ping** utility is available on Windows, Linux, and Cisco IOS, and tests network connectivity. The **tracert** utility is available on Windows, and a similar utility, traceroute, is available on Linux and Cisco IOS. In addition to testing for connectivity, **tracert** can be used to check for network latency. For example, when a web browser fails to connect to a web server, the problem can be anywhere between client and the server. A network engineer may use the ping command to test for local network connectivity or connections where there are few devices. In a complex network, the **tracert** command would be used. Where to begin connectivity tests has been the subject of much debate; it usually depends on the experience of the network engineer and familiarity with the network.The Internet Control Message Protocol (ICMP) is used by both **ping** and **tracert** to send messages between devices. ICMP is a TCP/IP Network layer protocol, first defined in RFC 792, September, 1981. ICMP message types were later expanded in RFC 1700.

Before ping or tracert commands, using the command **ipconfig** an administrator can verify the network connectivity inside a host machine. With the help of this command, a user can get an idea about all the network-related adaptors that host machine is connected to or has an ability to get connected in the future.

3 Algorithm

3.1 ipconfig command

The **ipconfig** is one of the most simple command in the networking connectivity checking related to any host or server. It gives a list of all the available network adapters of the host on which the command is run on. Generally, the adapters which are disconnected do not print out any more information. In contrast, the adapters connected to the internet provide a lot more information about the host and its default connection using the adapter. A network adapter is a piece of hardware that acts as the interface for a computer to a network. This way, computers/hosts can communicate across a network.
Task: Verify the network connectivity on the local host computer and visualize the available network adapters.

1. Open a Windows terminal and type **ipconfig** and press enter.
2. Observe the given list of network adapters and record necessary information.

The output gives a list of available network adapters connected with the host computer. It will be visible that some adapters are having a *Media State: Media disconnected.* This implies that those network adapters are currently unavailable in getting a connection with the internet.
Other adapters are successful in creating the network connection. In these adapters, several information is seen to be listed.

- DNS Suffix: This provides the DNS resolved hostname of the immediate router/switch this host machine is connected
- IPv6 Address: This provides the IP version 6 address of the host machine.
- IPv4 Address: The IP address of the host as in version 4.
- Subnet Mask: The subnet masking this host is following to get connected to the internet. If this host machine is a client device at the very network edge, then usually it will be 255.255.255.0
- Default Gateway: This gives the IP address of the router/switch that takes this host to get connected with the network.

An example output of an example host machine can be found in Figure 1a.

3.2 ping command

The **ping** command is used to verify TCP/IP Network layer connectivity on the local host computer or another device in the network. The command can be used with a destination IP address or qualified name, such as eagle-server.example.com, to test domain name services (DNS) functionality. For this lab, both IP addresses and hostnames will be used. The ping operation is straightforward. The source host computer sends an ICMP echo request to the destination. The destination responds with an echo reply. If there is a break between the source and destination, a router may respond with an ICMP message that the host is unknown or the destination network is unknown. Otherwise, if a clear connection is found, 4 replies are generated from the destination and sent back to the source host machine.
Task: Use the ping command to verify simple TCP/IP network connectivity with a certain given destination.

1. Open a Windows terminal and type **ping** followed by either an IP address of a destination or an entire hostname of the destination and press enter.

2. Observe the output of all the operations and record and understand.

The source machine sends 4 request ICMP messages to the destination IP address. If the hostname of the destination is entered after the **ping** command, the hostname is first DNS resolved through the host machine, After that the ping command commences to that destination IP. If direct destination IP is provided by host, nothing to do.
Once 4 ICMP requests get forwarded, if network connectivity is there, 4 replies generate from destination towards source. At each reply message are listed the memory space of the message thoruhg the network, the entire round trip time for that request to reach the destination adn come back to the host machine, and a TTL value. TTL value denotes a time-to-live value pre-decided by the destination server to be locally cached for DNS resolution.
At the end of the 4 reply messages is seen a summary of the 4 messages after eaching back to the source host. If all 4 is received, then host gets a 0% loss. In addition, summary regarding round trip times are also seen. If any of the four replies faces problems, then the message *Request Timed Out* is put on that row of the message.Thus with the help of this command, one can verify the entire availability of the host machine with a particular given destination server.
An example output for an example destination server can be found in Figure 1b.

3.3 tracert command

The **tracert** command is useful for learning about network latency and path information. Instead of using the **ping** command to test connectivity of each device to the destination, one by one, the **tracert** command can be used. On Linux and Cisco IOS devices, the equivalent command is **traceroute**. If a user wants to test and visulaize each and every node starting from this host source towards a destination, then **tracert** command can be used.
Task: Use the tracert command to verify simple TCP/IP network connectivity with a certain given destination along with visualizing each node in the entire path.

1. Open a Windows terminal and type **tracert** followed by either an IP address of a destination or an entire hostname of the destination and press enter.

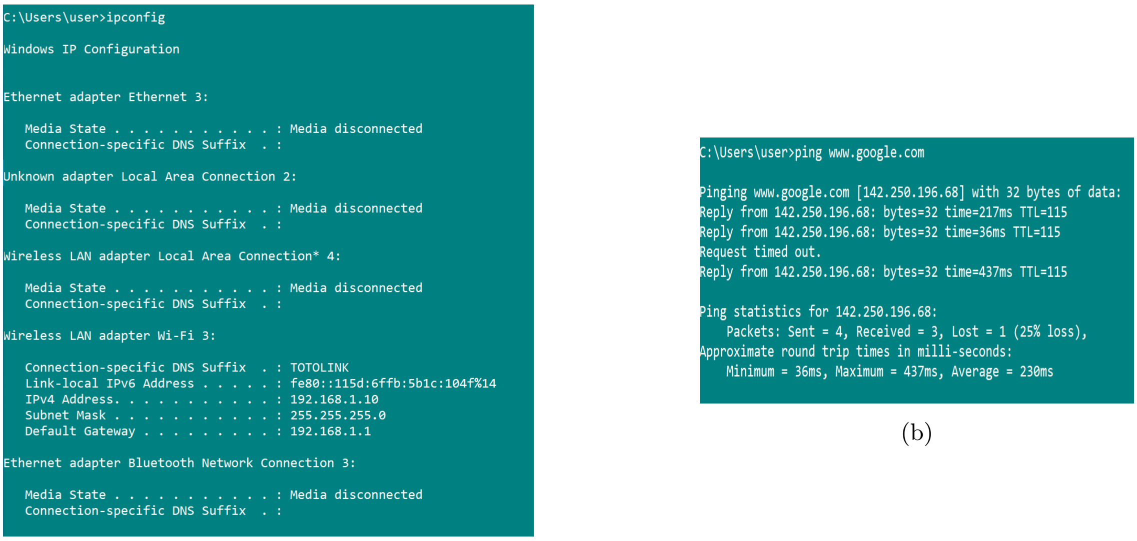
2. Observe the output of all the operations and record and understand each row of the entire output.

This command can be done with help of both IP address or only hostname of the destination server, just similar to the **ping** command before. The command sends out ICMP echo request towards the destination.
The output of the command is a very detailed information about each node along the entire path to the destination. Output is in the form of a table. In the table, each row denotes a **hop**. A hop occurs when a packet is passed from one network segment to the next. in other words, a hop is simply a network node with simple network connectivity. Each row shows the sending of ICMP requests to that serial hop from the source. For example, in the first row hop is 1. This means ICMP request reaches only the first hop from the source. The following three columns denote the round trip times for three such ICMP requests to the same hop. The last column denotes the IP address of that hop. If there exists a canonical DNS resovled name, this is also printed out by the command for that particular hop.
If some round trip time of some hop is shown as an *asterisk* * mark, it means the ICMP request and response faced problem in the connectivity at that very moment and ICMP could not travelled back to the source. In that case, the hop fails for that particular ICMP request only, but no other ICMP.

The command works in hop-by-hop basis. This means, at every hop the command tests whether that hop is the destination IP supplied at the beginning of the tracing. So, after some hops, when the destination is finally reached out, the tracing completes. The **tracert** command can trace like this upto 30 hops at maximum. If any destination is further from 30 hops from this source host, the command fails. Thus with the help of **tracert** command, a user can test the entire path and all the network nodes in the path from source host to destination host/server.
An example output for an example destination server can be found in Figure 2.

4 Input/Output

In this section, a sample input/output for the three commands are given for further understanding.



```
C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

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

Unknown adapter Local Area Connection 2:

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

Wireless LAN adapter Local Area Connection* 4:

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

Wireless LAN adapter Wi-Fi 3:

   Connection-specific DNS Suffix  . : TOTOLINK
   Link-local IPv6 Address . . . . . : fe80::115d:6ffb:5b1c:104f%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection 3:

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

(a)

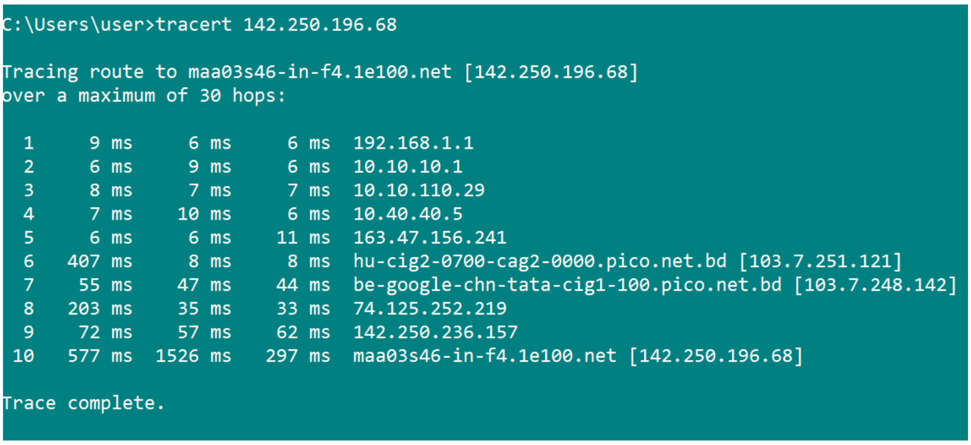
```
C:\Users\user>ping www.google.com

Pinging www.google.com [142.250.196.68] with 32 bytes of data:
Reply from 142.250.196.68: bytes=32 time=217ms TTL=115
Reply from 142.250.196.68: bytes=32 time=36ms TTL=115
Request timed out.
Reply from 142.250.196.68: bytes=32 time=437ms TTL=115

Ping statistics for 142.250.196.68:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 437ms, Average = 230ms
```

(b)

Figure 1: Inputs and outputs of **ipconfig** and **ping** commands. The **ping** command is done on a certain web server's hostname.



```
C:\Users\user>tracert 142.250.196.68

Tracing route to maa03s46-in-f4.1e100.net [142.250.196.68]
over a maximum of 30 hops:

  1     9 ms     6 ms     6 ms  192.168.1.1
  2     6 ms     9 ms     6 ms  10.10.10.1
  3     8 ms     7 ms     7 ms  10.10.110.29
  4     7 ms    10 ms     6 ms  10.40.40.5
  5     6 ms     6 ms    11 ms  163.47.156.241
  6   407 ms     8 ms     8 ms  hu-cig2-0700-cag2-0000.pico.net.bd [103.7.251.121]
  7    55 ms    47 ms    44 ms  be-google-chn-tata-cig1-100.pico.net.bd [103.7.248.142]
  8   203 ms    35 ms    33 ms  74.125.252.219
  9    72 ms    57 ms    62 ms  142.250.236.157
 10   577 ms  1526 ms   297 ms  maa03s46-in-f4.1e100.net [142.250.196.68]

Trace complete.
```

Figure 2: Input and output of **tracert** command on a destination IP address

5 Discussion & Conclusion

The **ipconfig** command helps user to know abou the host machines network adapters. The **ping** command helps to verify the entire end-to-end connectivity with a host source machine with a destination server. The **tracert** command also aids in verifying this connectivity with a destination, but also includes all and detailed information of all the hops along the way towards the destination hop/server/host. This is the primary difference between the **ping** and **tracert** commands.

Based on the focused objective(s) to understand about three important commands, the additional lab tasks and thinking exercises will made the student more confident towards the fulfilment of the objectives(s).

6 Lab Task (Please implement/think yourself and show the output to the instructor)

1. Why are there numbers at the end of the names of each network adapter after getting output using **inconfig**?

2. Why is there any need of sending 4 ICMP requests messages while verifying connectivity using **ping** command, instead of just a single ICMP requerst and response?

3. In case of **tracert** command, is an entire row for any particular hop has three of its values as *asterisk* *, then what does it mean? Does it mean that the hop is completely failed so that the entire path is damaged and disconnected for forever? If so, then even after that, how can the **tracert** command completes the tracing and reaching the destination?

4. Practice by giving an IP destination address using the **ping** command.

5. Practice by providing a destination server;s hostname using the **tracert** command and observe the output.

7 Policy

Copying from internet, classmate, seniors, or from any other source is strongly prohibited. 100% marks will be *deducted* if any such copying is detected.