# COMP 311 Computer Networks

## Lab 02 – Basic Network Utilities

## Learning Objectives:

Students are expected to learn the basic network utilities and tools and can use them to troubleshoot the networks.

## Evaluation:

Students should be able to demonstrate the basic network utilities and tools and could be asked questions for their basic understanding.

## Basic Network Utilities:

## IPCONFIG

*ipconfig* is used to view the Network Interface Information configuration.

***Objective:*** In this computer lab, your computer connects to the LAN via one of its Network Interface Cards (NIC). Operating systems allow the user to view information about the current NIC connection. In this task you will be able to see the NIC information.

## Tasks:

1. Type ***ipconfig*** at the command prompt and press enter:

Record the following information for your computer and then compare the information of your computer with any other neighboring computer.

|  |  |  |
| --- | --- | --- |
|  | **Your Computer** | **Your Neighboring Computer** |
| **IP Address** | 172.20.10.11 | 172.20.10.5 |
| **Subnet mask** | 255.255.255.240 | 255.255.240 |
| **Default gateway** | 172.20.10.1 | 172.20.10.1 |

1. What is similar about the IP Address?

172.20.10. this part of the id address is same. Indicating its part of the same network

1. Any other Similarities:

Subnet mask and Default gateway are both same

1. Type ***­***  at the command prompt and press enter:

Add the screen shot of your out below here. Observe the information shown here and try to understand this information.



Highlight or write down the following information.

1. What is the MAC address of your computer?

Physical Address: A0-29-42-65-F5-0F

1. What is your DNS address?

DNS Servers: 172.20.10.1

1. What is your DHCP server address?

DHCP Server : 172.20.10.1

1. Type ***ipconfig /?***  at the command prompt and press enter:

Observe the options available for ***ipconfig***.

 shahb on Hafsah at 󰋜 ~ ipconfig /?  
  
USAGE:  
 ipconfig [/allcompartments] [/? | /all |  
 /renew [adapter] | /release [adapte  
r] |  
 /renew6 [adapter] | /release6 [adap  
ter] |  
 /flushdns | /displaydns | /register  
dns |  
 /showclassid adapter |  
 /setclassid adapter [classid] |  
 /showclassid6 adapter |  
 /setclassid6 adapter [classid] ]  
  
where  
 adapter Connection name  
 (wildcard characters \* and ? allowed, see exa  
mples)  
  
 Options:  
 /? Display this help message  
 /all Display full configuration information.  
 /release Release the IPv4 address for the specified a  
dapter.  
 /release6 Release the IPv6 address for the specified a  
dapter.  
 /renew Renew the IPv4 address for the specified ada  
pter.  
 /renew6 Renew the IPv6 address for the specified ada  
pter.  
 /flushdns Purges the DNS Resolver cache.  
 /registerdns Refreshes all DHCP leases and re-registers D  
NS names  
 /displaydns Display the contents of the DNS Resolver Cac  
he.  
 /showclassid Displays all the dhcp class IDs allowed for   
adapter.  
 /setclassid Modifies the dhcp class id.  
 /showclassid6 Displays all the IPv6 DHCP class IDs allowed  
 for adapter.  
 /setclassid6 Modifies the IPv6 DHCP class id.  
  
  
The default is to display only the IP address, subnet mask and  
default gateway for each adapter bound to TCP/IP.  
  
For Release and Renew, if no adapter name is specified, then the IP   
address  
leases for all adapters bound to TCP/IP will be released or renewed.  
  
  
For Setclassid and Setclassid6, if no ClassId is specified, then the  
 ClassId is removed.  
  
Examples:  
 > ipconfig ... Show information  
 > ipconfig /all ... Show detailed information  
 > ipconfig /renew ... renew all adapters  
 > ipconfig /renew EL\* ... renew any connection that h  
as its  
 name starting with EL  
 > ipconfig /release \*Con\* ... release all matching connec  
tions,  
 eg. "Wired Ethernet Connect  
ion 1" or  
 "Wired Ethernet Connect  
ion 2"  
 > ipconfig /allcompartments ... Show information about all  
 compartments  
 > ipconfig /allcompartments /all ... Show detailed information a  
bout all  
 compartments

## PING

The **ping** command is used to test the ability of the source computer to reach a specified destination computer.

***Objective:*** The main objective of ***PING*** is to diagnose the connectivity of a network i.e. whether one computer can communicate with another computer on the network or not. This is normally performed using the Internet Control Message Protocol (ICMP).

## Tasks:

1. Type ***ping <Your neighboring computer’s IP>*** at the command prompt and press enter. Observe the displayed information and fill in the following table.
2.  shahb on Hafsah at 󰋜 ~ ping -l 64 172.20.10.5  
     
   Pinging 172.20.10.5 with 64 bytes of data:  
   Request timed out.  
   Request timed out.  
   Request timed out.  
     
   Ping statistics for 172.20.10.5:  
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

|  |  |
| --- | --- |
| **Field** | **Value** |
| Size of packet | 32 |
| Number of packets sent | 4 |
| Number of replies | 0 |
| Number of lost packets | 4 |
| Minimum delay | No replies |
| Maximum delay | No replies |
| Average delay | No replies |

1. Type ping ***<any URL>*** at the command prompt and press enter. Observe the displayed information and fill in the following table.
2.  shahb on Hafsah at 󰋜 ~ ping www.google.com  
     
   Pinging www.google.com [192.178.24.196] with 32 bytes of data:  
   Reply from 192.178.24.196: bytes=32 time=132ms TTL=49  
   Reply from 192.178.24.196: bytes=32 time=342ms TTL=49  
   Reply from 192.178.24.196: bytes=32 time=106ms TTL=49  
   Reply from 192.178.24.196: bytes=32 time=163ms TTL=49  
     
   Ping statistics for 192.178.24.196:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
   Approximate round trip times in milli-seconds:  
    Minimum = 106ms, Maximum = 342ms, Average = 185ms

|  |  |
| --- | --- |
| **Field** | **Value** |
| Size of packet | 32 |
| Number of packets sent | 4 |
| Number of replies | 4 |
| Number of lost packets | 0 |
| Minimum delay | 106ms |
| Maximum delay | 342ms |
| Average delay | 185ms |

1. Open command prompt and repeat the step (ii) with modified command. You need to type ***ping –l 64 <destination IP>*** and click enter. Observer and try to understand what has changed. Write in 1-2 lines.

The difference is in the packet size sent: the first command uses the default size of 32 bytes, while the second command sets it to 64 bytes explicitly.

 shahb on Hafsah at 󰋜 ~ ping -l 64 www.google.com  
  
Pinging www.google.com [192.178.24.196] with 64 bytes of data:  
Reply from 192.178.24.196: bytes=64 time=147ms TTL=49  
Reply from 192.178.24.196: bytes=64 time=451ms TTL=49  
Reply from 192.178.24.196: bytes=64 time=181ms TTL=49  
Reply from 192.178.24.196: bytes=64 time=259ms TTL=49  
  
Ping statistics for 192.178.24.196:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
 Minimum = 147ms, Maximum = 451ms, Average = 259ms

1. Open command prompt and type ***ping /?*** and click enter. Observer and try to understand what information is displayed to you.
2.  shahb on Hafsah at 󰋜 ~ 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-Bre  
   ak;  
    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 (IP  
   v6-only).  
    Per RFC 5095 the use of this routing header has b  
   een  
    deprecated. Some systems may drop echo requests i  
   f  
    this header is used.  
    -S srcaddr Source address to use.  
    -c compartment Routing compartment identifier.  
    -p Ping a Hyper-V Network Virtualization provider ad  
   dress.  
    -4 Force using IPv4.  
    -6 Force using IPv6.
3. Try other options of your choice. Which option you have tried? Write in 1-2 lines.

-t Ping the specified host until stopped.

To see statistics and continue - type Control-Break

 shahb on Hafsah at 󰋜 ~ ping -t 172.20.10.11  
  
Pinging 172.20.10.11 with 32 bytes of data:  
Reply from 172.20.10.11: bytes=32 time<1ms TTL=128  
Reply from 172.20.10.11: bytes=32 time<1ms TTL=128  
Reply from 172.20.10.11: bytes=32 time<1ms TTL=128  
Reply from 172.20.10.11: bytes=32 time<1ms TTL=128  
Reply from 172.20.10.11: bytes=32 time<1ms TTL=128  
  
Ping statistics for 172.20.10.11:  
 Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

1. Ping the IP address of default gateway. Was the ping successful?

Yes

 shahb on Hafsah at 󰋜 ~ ping 172.20.10.1  
  
Pinging 172.20.10.1 with 32 bytes of data:  
Reply from 172.20.10.1: bytes=32 time=77ms TTL=64  
Reply from 172.20.10.1: bytes=32 time=77ms TTL=64  
Reply from 172.20.10.1: bytes=32 time=5ms TTL=64  
Reply from 172.20.10.1: bytes=32 time=4ms TTL=64  
  
Ping statistics for 172.20.10.1:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
 Minimum = 4ms, Maximum = 77ms, Average = 40ms

1. Ping the IP address of DHCP Server. Was the ping successful? Yes
2.  shahb on Hafsah at 󰋜 ~ ping 172.20.10.1  
     
   Pinging 172.20.10.1 with 32 bytes of data:  
   Reply from 172.20.10.1: bytes=32 time=21ms TTL=64  
   Reply from 172.20.10.1: bytes=32 time=3ms TTL=64  
   Reply from 172.20.10.1: bytes=32 time=13ms TTL=64  
   Reply from 172.20.10.1: bytes=32 time=20ms TTL=64  
     
   Ping statistics for 172.20.10.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
   Approximate round trip times in milli-seconds:  
    Minimum = 3ms, Maximum = 21ms, Average = 14ms
3. Ping the IP address of DNS Server. Was the ping successful?

A screenshot of a computer program

Description automatically generated

1. Try the following commands and observe the purpose
   1. Try C:\ping -n 10 [www.google.com](http://www.google.com) > test.txt
   2. Try C:\ more test.txt
   3. Try C:\ dir \*.txt

A screenshot of a computer screen

Description automatically generated

## TRACERT

The **tracert** command can be used to trace the route from your PC to another

host on the Internet.

***Objective:*** To evaluate a useful network connectivity test is to determine the path (or route) that a packet takes.

## Tasks:

1. Type ***tracert <any URL>*** at the command prompt and press enter. Observe the displayed information and write down your observation in 2-3 lines.

The traceroute shows the connection passing through local and private network routers before reaching a public IP address, potentially belonging to an ISP. However, there's a discrepancy in the displayed destination IP address for www.google.com.

A screen shot of a computer

Description automatically generated

1. Open command prompt and type ***tracert /?*** and click enter. Observer and try to understand by trying other options.

A screenshot of a computer program

Description automatically generated

1. Try **pathping** <***any URL***>. What is purpose of pathping? Write in 1-2 lines.

Pathping combines the features of traceroute and ping to provide a comprehensive analysis of network latency and packet loss along the route to a destination, helping diagnose network issues more effectively.

A screenshot of a computer

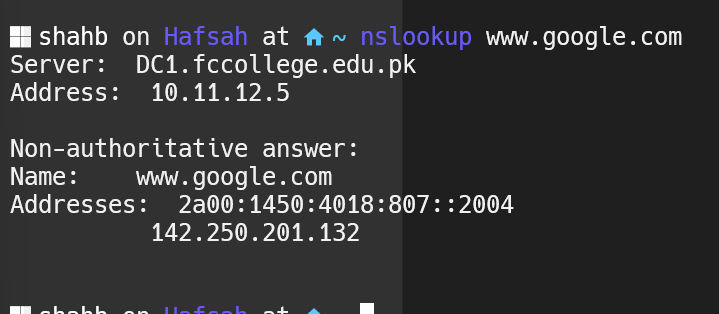
Description automatically generated

## NSLOOKUP

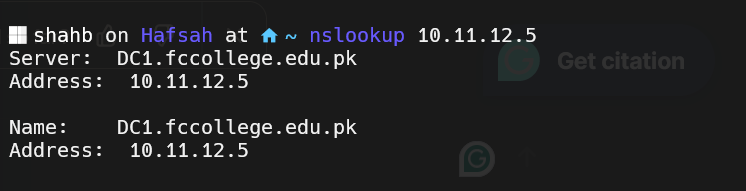
***Objective:*** The **nslookup** is a network administration command-line tool available in many computer operating systems for querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records..

1. Type ***nslookup*** [***www.google.com***](http://www.google.com)at the command prompt and press enter. Observe the displayed information and write down your observation in 2-3 lines.

These are non-authoritative answers, meaning they were obtained from a DNS server other than the authoritative DNS server for the domain.



1. Type ***nslookup*** with other URLs and IP addresses.



A screen shot of a computer

Description automatically generated

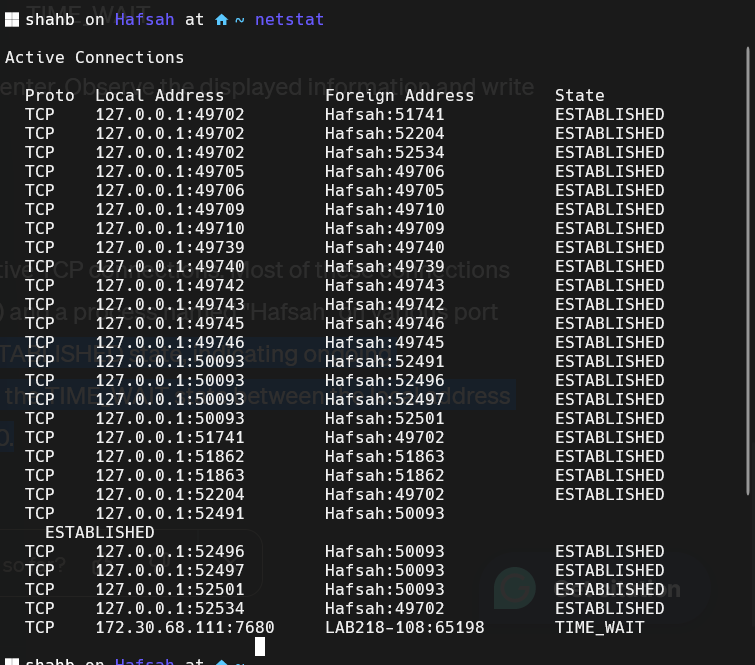
## NETSTAT

The **netstat** command generates displays that show network status and protocol.

***Objective:*** To display the status of TCP and UDP endpoints in table format, routing table information, and interface information. netstat displays various types of network data depending on the command line option selected.

## Tasks:

1. Type ***netstat*** at the command prompt and press enter. Observe the displayed information and write down your observation in 2-3 lines.



The connections are mainly in the ESTABLISHED state, indicating ongoing communication. There's also one connection in the TIME\_WAIT state between the local address 172.30.68.111 and a remote address on port 7680.

1. Type ***netstat -n*** at the command prompt and press enter. Observe the displayed information and write down your observation in 2-3 lines.

The "netstat -n" command displays active TCP connections with numerical addresses and port numbers, without hostname resolution. It's useful for troubleshooting network problems or getting a clearer view of network activity.

A screenshot of a computer screen

Description automatically generated

## Geographical location of any IP Address

Write how you can get geographical location of any IP address.

with APIs, such as MaxMind GeoIP2, IP2Location, or IPinfo. provide accurate location data based on the IP address queried, including country, city, latitude, and longitude coordinates.

