University of Dhaka

Department of Computer Science and Engineering

CSE-3111 : Computer Networking Lab

Lab Report 1 : Lab exercises on LAN configuration and troubleshooting tools

Submitted By:

Name : Tanzeem Maliat

Roll No : 51

Submitted On :

January 19, 2023

Submitted To :

Dr. Md. Abdur Razzaque

Md Mahmudur Rahman

Md. Ashraful Islam

Md. Fahim Arefin

1 Introduction

The preliminary objective of this lab is to get accustomed to LAN configuration troubleshooting tools.We executed fundamental networking commands such as ping, traceroute, ipconfig, nslookup, netstat, arp, rarp in order to monitor network connections.

1.1 Objectives

- Learnt how to use fundamental networking commands
- Monitored network connections
- Inspected the network enviroment

2 Using the 'PING' command

We used the ping command to identify if a particular host is reachable or not.

2.1 Output for 'ping google.com'

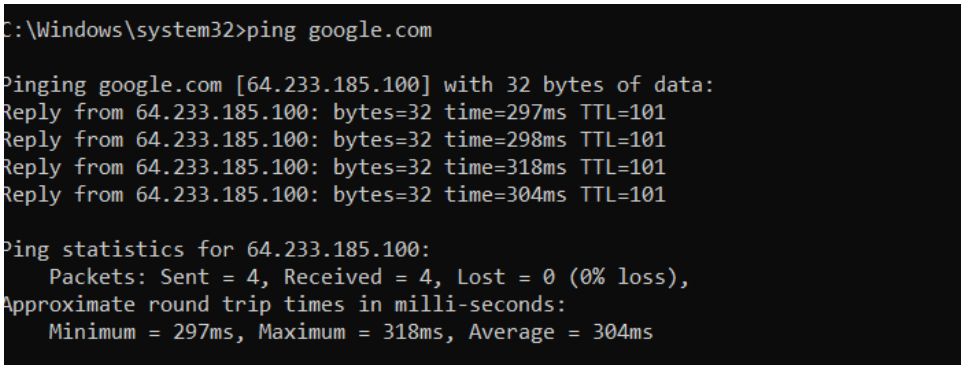

Figure 1: Output for 'ping google.com'

2.2 Output for 'ping -n 2 google.com'

```
C:\Windows\system32>ping -n 2 google.com

Pinging google.com [64.233.185.100] with 32 bytes of data:
Reply from 64.233.185.100: bytes=32 time=297ms TTL=101
Reply from 64.233.185.100: bytes=32 time=300ms TTL=101

Ping statistics for 64.233.185.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 297ms, Maximum = 300ms, Average = 298ms
```

Figure 2: Output for 'ping -n 2 google.com'

2.3 Output for 'ping 10.0.0.24'

```
C:\Windows\system32>ping 10.0.0.24

Pinging 10.0.0.24 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3: Output for 'ping 10.0.0.24'

3 Using the 'TRACERT' command

We used the traceroute command to track the path that a packet takes to reach a specific host.

3.1 Output for 'tracert 8.8.8.8'

```
C:\Windows\system32>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     2 ms     7 ms     5 ms  XiaoQiang [192.168.31.1]
  2     9 ms     8 ms     8 ms  172.16.128.1
  3     8 ms     7 ms     8 ms  114.130.132.62
  4     4 ms     4 ms     6 ms  180.211.200.129
  5     6 ms     5 ms     6 ms  123.49.8.61
  6    14 ms    13 ms    14 ms  123.49.8.146
  7    35 ms    44 ms    41 ms  142.250.160.186
  8   100 ms    40 ms    37 ms  142.251.77.23
  9    46 ms    37 ms    36 ms  142.251.52.207
 10    37 ms    37 ms    37 ms  dns.google [8.8.8.8]

Trace complete.
```

Figure 4: Output for 'tracert 8.8.8.8'

3.2 Output for 'tracert -h 5 8.8.8.8'

```
C:\Windows\system32>tracert -h 5 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 5 hops:

  1    11 ms     2 ms     3 ms  XiaoQiang [192.168.31.1]
  2    10 ms     8 ms     9 ms  172.16.128.1
  3     5 ms     8 ms     8 ms  114.130.132.62
  4    11 ms     5 ms     4 ms  180.211.200.129
  5     7 ms     5 ms     5 ms  123.49.8.61

Trace complete.
```

Figure 5: Output for 'tracert -h 5 8.8.8.8'

3.3 Output for 'tracert -w 5 8.8.8.8'

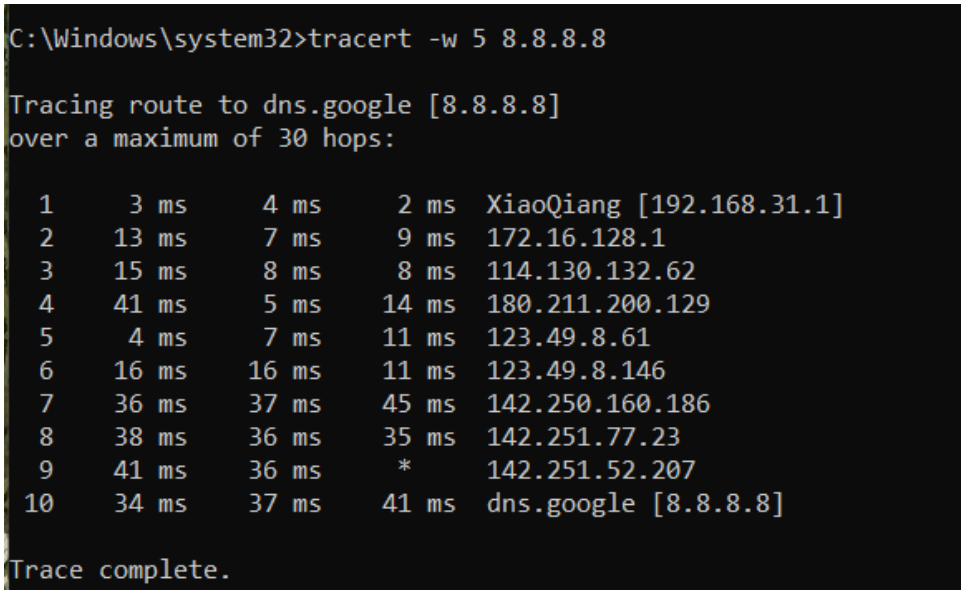

Figure 6: Output for 'tracert -w 5 8.8.8.8'

4 Using the 'IPCONFIG' command

We used the ipconfig command to display information about network interfaces configure them. With ipconfig, we can configure the IP addresses, netmask other settings for a network interface. The command is also used to check the status of the network interfaces

4.1 Output for 'ipconfig'

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Local Area Connection* 11:

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

Wireless LAN adapter Local Area Connection* 12:

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

Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b91a:c974:1fa8:124e%11
   IPv4 Address. . . . . . . . . . . : 192.168.31.56
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.31.1

Ethernet adapter Bluetooth Network Connection 2:

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

Figure 7: Output for 'ipconfig'

4.2 Output for 'ipconfig /all'

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-V49RBC1
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 30-D0-42-13-A4-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 1A-47-3D-45-2A-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : 2A-47-3D-45-2A-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter #2
   Physical Address. . . . . . . . . : 18-47-3D-45-2A-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Figure 8: Output for 'ipconfig /all'

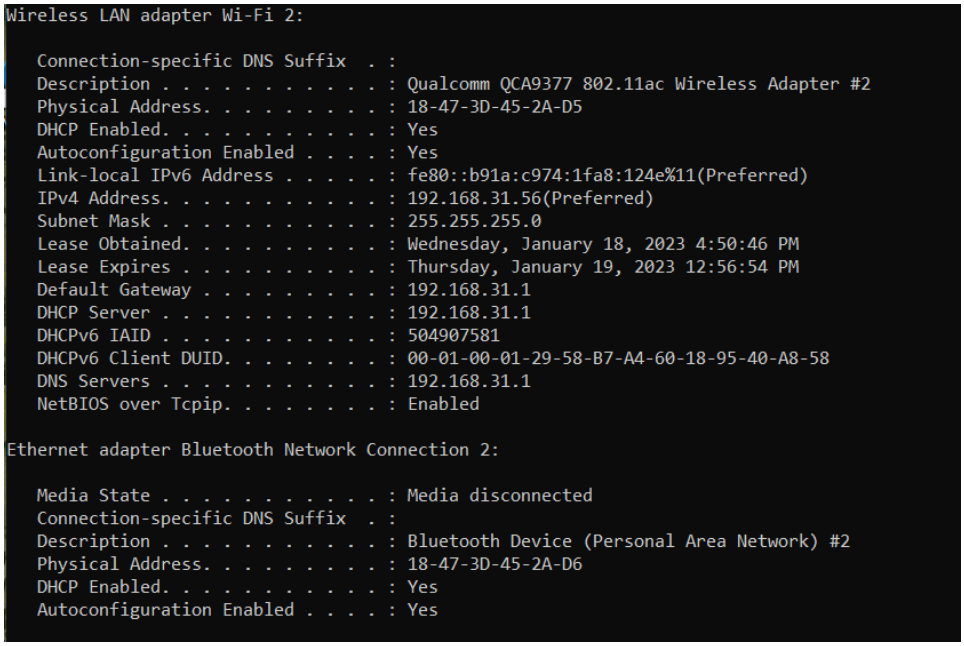

Figure 9: Output for 'ipconfig /all'

5 Using the 'NETSTAT' command

Netstat command is used for displaying various network related information for example network connections, routing tables, interface statics, masquerade connections etc.

5.1 Output for 'netstat'

```
C:\Windows\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.31.56:51528    47:https               ESTABLISHED
  TCP    192.168.31.56:51553    64:https               ESTABLISHED
  TCP    192.168.31.56:61593    47:https               ESTABLISHED
  TCP    192.168.31.56:61594    218:4070               ESTABLISHED
  TCP    192.168.31.56:61595    20.198.119.143:https   ESTABLISHED
  TCP    192.168.31.56:61596    sl-in-f188:5228        ESTABLISHED
  TCP    192.168.31.56:61665    server-13-33-30-231:https  ESTABLISHED
  TCP    192.168.31.56:62104    172.67.70.134:https    ESTABLISHED
  TCP    192.168.31.56:62359    1:https                ESTABLISHED
  TCP    192.168.31.56:62563    194:https              ESTABLISHED
  TCP    192.168.31.56:63027    25:https               ESTABLISHED
  TCP    192.168.31.56:63054    152.199.43.62:https    CLOSE_WAIT
  TCP    192.168.31.56:63977    131:https              ESTABLISHED
  TCP    192.168.31.56:64042    131:https              ESTABLISHED
  TCP    192.168.31.56:64325    ec2-13-250-173-68:https  ESTABLISHED
  TCP    192.168.31.56:64423    13.107.5.88:https      ESTABLISHED
  TCP    192.168.31.56:64443    40.79.141.152:https    ESTABLISHED
  TCP    192.168.31.56:64444    40.99.31.146:https     ESTABLISHED
  TCP    192.168.31.56:64445    40.99.31.146:https     ESTABLISHED
  TCP    192.168.31.56:64446    20.44.220.42:https     ESTABLISHED
  TCP    192.168.31.56:64447    40.79.141.152:https    ESTABLISHED
  TCP    192.168.31.56:64448    40.119.240.74:https    ESTABLISHED
  TCP    192.168.31.56:64455    151.101.66.137:https   ESTABLISHED
  TCP    192.168.31.56:64456    104.18.36.94:https     ESTABLISHED
  TCP    192.168.31.56:64457    server-52-85-126-91:https  ESTABLISHED
^C
```

Figure 10: Output for 'netstat'

6 Using the 'ARP' command

arp command manipulates the system's ARP cache. It also allows a complete dump of the arp cache. ARP stands fro Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its MAC address.

6.1 Output for 'arp /a'

```
C:\Windows\system32>arp /a

Interface: 192.168.31.56 --- 0xb
  Internet Address      Physical Address      Type
  192.168.31.1          28-d1-27-1a-5f-5c     dynamic
  192.168.31.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 11: Output for 'arp /a'

7 Using the 'NSLOOKUP' command

Nslookup stands for Name Server Lookup. This command is a useful command for getting infromation from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

7.1 Output for 'nslookup www.google.com'

```
C:\Windows\system32>nslookup
Default Server:  XiaoQiang
Address:  192.168.31.1

> www.google.com
Server:  XiaoQiang
Address:  192.168.31.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:4002:c09::93
          2607:f8b0:4002:c09::67
          2607:f8b0:4002:c09::63
          2607:f8b0:4002:c09::68
          64.233.185.103
          64.233.185.104
          64.233.185.99
          64.233.185.147
          64.233.185.105
          64.233.185.106
```

Figure 12: Output for 'nslookup www.google.com'

7.2 Output for 'nslookup -type=ns google.com'

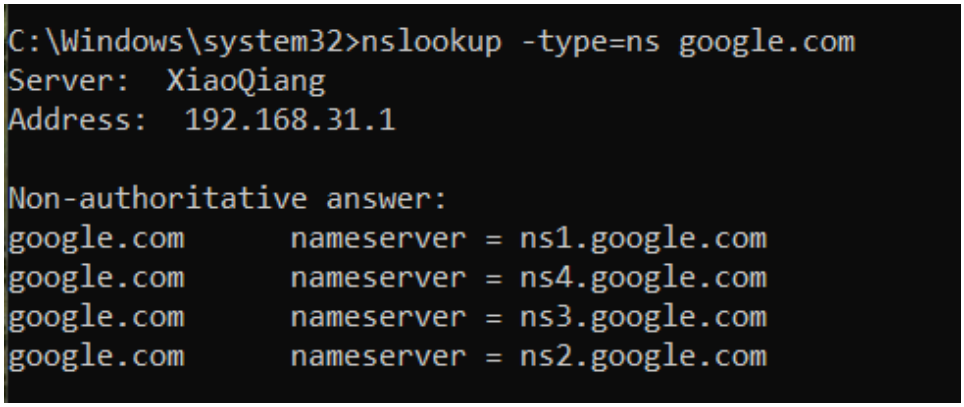

Figure 13: Output for 'nslookup -type=ns google.com'

8 Experience

In the Lab 1, we learned how to use fundamental networking commands on Windows Command Prompt to troubleshoot configure network connections interface.

References

[1] Computer networking : a top-down approach 6th ed.

[2] LifeWire : `https://www.lifewire.com/netstat-command-2618098`

[3] Steve's Internet Guide : `http://www.steves-internet-guide.com/using-nslookup/`