



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 (PING, Traceroute, ARP, netstat, ifconfig, nslookup,etc.)

Submitted By:

Name: Md Shamsur Rahman Sami

Roll No : 57

Name: Md Rakib Hossain

Roll No : 55

Submitted On :

January 26, 2024

Submitted To :

Dr. Md. Abdur Razzaque

1 Introduction

In this comprehensive laboratory exercise focused on Local Area Network (LAN) configuration and troubleshooting tools. The lab delved into fundamental aspects of LAN setup, including ARP (Address Resolution Protocol), static routing, and configuration of network interfaces using tools such as Ifconfig. Troubleshooting skills were honed through the use of diagnostic utilities like PING and Traceroute, which enabled participants to identify and address connectivity issues. Additionally, participants gained insights into monitoring network activity with NETSTAT and resolving domain-related queries with NSLOOK. The lab fostered a practical understanding of essential networking tools, empowering participants with the knowledge and skills necessary for effective LAN configuration and troubleshooting.

2 Theory

In the realm of computer networking, Local Area Networks (LANs) play a pivotal role in connecting devices within a confined geographical area. The theory underlying LAN configuration revolves around the essential tasks of assigning IP addresses, configuring subnet masks, and establishing gateway addresses to facilitate seamless communication among networked devices. Address Resolution Protocol (ARP) becomes a critical component in this context, serving to map IP addresses to physical MAC addresses within the local network. Additionally, the concept of static routing involves the manual configuration of routing tables, offering a straightforward method for specifying network paths in environments where routing changes infrequently. The indispensable network utilities, PING and Traceroute, contribute to network troubleshooting and diagnostics by testing reachability and identifying the path to a destination, enhancing the overall understanding and management of LAN environments.

3 Methodology

- First open the cmd terminal in the windows system
- Run the following command in the terminal and get the output result and take the screenshot of the output.
 - **IP Configuration:** ipconfig
 - **PING:** ping [IP address or hostname]

- Traceroute (Tracert in Windows): `tracert [IP address or hostname]`
- ARP (Address Resolution Protocol): `arp -a`
- Netstat (Network Statistics): `netstat -a`
- Nslookup (DNS Queries): `nslookup [hostname or IP address]`

4 Command Output

Some Snapshots of the command output can be seen in the following figures:

4.1

```

Microsoft Windows [Version 10.0.19042.590]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SWE>ping google.com

Pinging google.com [142.250.193.174] with 32 bytes of data:
Reply from 142.250.193.174: bytes=32 time=4ms TTL=56
Reply from 142.250.193.174: bytes=32 time=4ms TTL=56
Reply from 142.250.193.174: bytes=32 time=4ms TTL=56
Reply from 142.250.193.174: bytes=32 time=4ms TTL=56

Ping statistics for 142.250.193.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\SWE>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time=0ms TTL=128
Reply from 192.168.0.11: bytes=32 time=0ms TTL=128
Reply from 192.168.0.11: bytes=32 time=0ms TTL=128
Reply from 192.168.0.11: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\SWE>ping -c 5 192.168.0.11
Access denied. Option -c requires administrative privileges.

C:\Users\SWE>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\SWE>ping 192.168.0.12

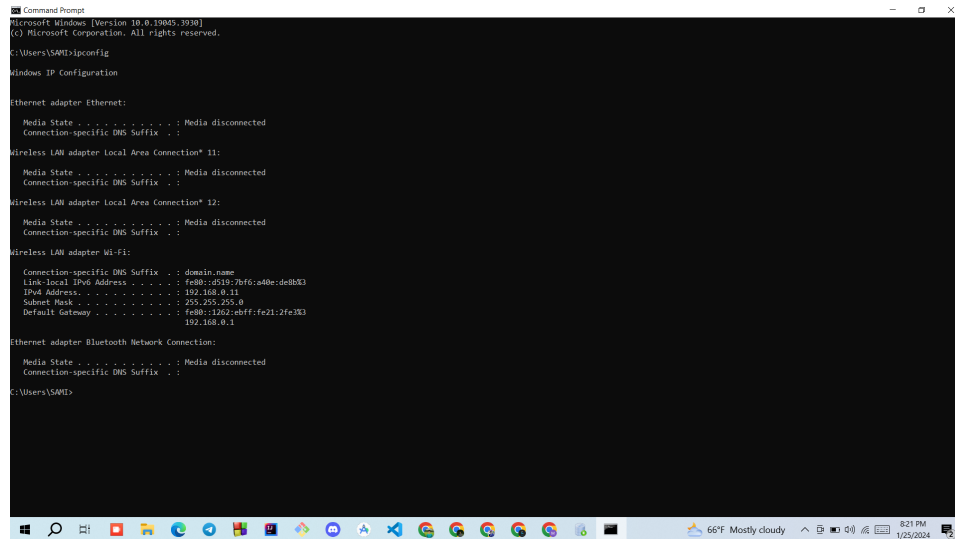
Pinging 192.168.0.12 with 32 bytes of data:
Reply from 192.168.0.11: Destination host unreachable.
Reply from 192.168.0.11: Destination host unreachable.

```

Figure 1: PING Command

- The ‘ping’ command is a network utility used to check the availability and responsiveness of a host on an IP network.
- It sends ICMP Echo Request messages to the target, waits for Echo Replies, and displays round-trip time statistics.
- This tool is crucial for troubleshooting network connectivity and measuring latency.

4.2



```
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\SAMI>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    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:

    Connection-specific DNS Suffix . : domain.name
    Link-local IPv6 Address . . . . . : fe80::d83-70fd:a0e:de803
    IPv4 Address. . . . . : 192.168.0.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1202:abff:fe21:2fa3e3
                                   192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\SAMI>
```

Figure 2: Ifconfig Command

- The ‘ipconfig’ command in Windows provides essential information about a computer’s network configuration.
- This includes its IP address, subnet mask, default gateway, and DNS servers.
- It is a valuable tool for diagnosing and troubleshooting network issues.

4.3

- The ‘tracert’ command is a network utility used to trace the route that packets take to reach a destination.
- It shows the IP addresses of each hop along the way and the time it takes for packets to travel from the source to each intermediate destination.
- This tool is helpful for identifying network bottlenecks, locating connectivity issues, and understanding the path data takes through the network.

```
Command Prompt
C:\Users\SAMI>tracert google.com

Tracing route to google.com [142.250.196.78]
over a maximum of 30 hops:
  0  3 ms  2 ms  2 ms 192.168.0.1
  1 13 ms  5 ms  67 ms 172.19.164.1
  2 12 ms  4 ms  5 ms 103.159.19.81
  3 13 ms  6 ms  69 ms 10.159.19.97
  4  5 ms  6 ms  4 ms *
C:\Users\SAMI>tracert 192.168.0.1

Tracing route to 192.168.0.1 over a maximum of 30 hops:
  0 11 ms  4 ms  3 ms 192.168.0.1
Trace complete.
```

Figure 3: Traceroute Command

4.4

```
Command Prompt
C:\Users\SAMI>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-v] [if_addr]

-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed. If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
            entries and entries on the loop-back interface will be shown.
if_addr     Specifies an Internet address.
-if_addr    Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr. The Physical address is
            given as 6 hexadecimal bytes separated by hyphens. The entry
            is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-80 .... Adds a static entry.
> arp -a          .... Displays the arp table.

C:\Users\SAMI>arp -a

Interface: 192.168.0.1 --- 0x0
Internet Address      Physical Address      Type
192.168.0.1           30-62-e0-21-2f-e3    dynamic
192.168.0.255         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-00-00-1b    static
224.0.0.252           01-00-5e-00-00-1c    static
230.235.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Figure 4: ARP Command

- The ‘arp’ command is a network utility used to display and manage

the Address Resolution Protocol (ARP) cache on a system.

- It shows the mapping between IP addresses and corresponding physical MAC addresses.
- This tool is essential for troubleshooting network connectivity issues, as it helps in identifying the devices present on the local network and their associated MAC addresses.

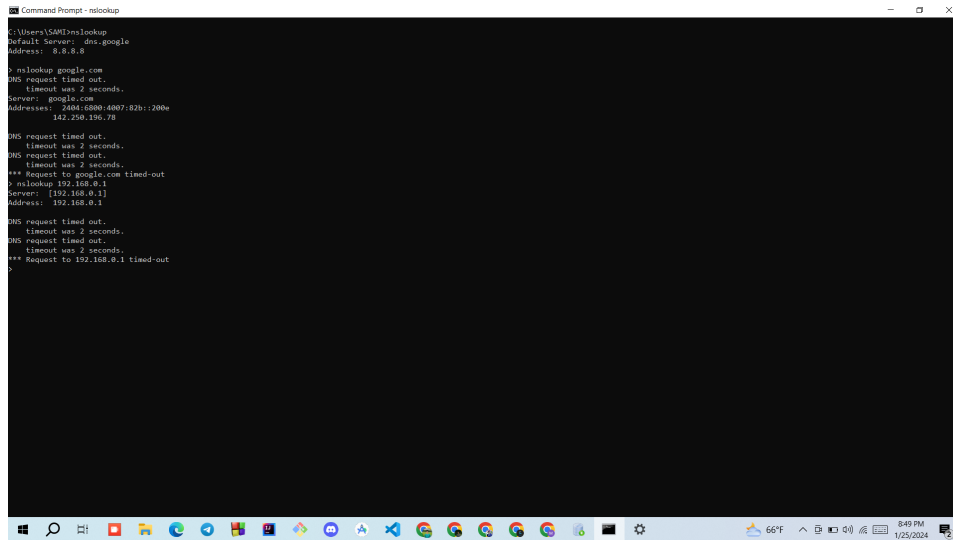
4.5

```
Command Prompt
C:\Users\SAMI>netstat -a

Active Connections
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135               Sami:0                  LISTENING
TCP    0.0.0.0:445               Sami:0                  LISTENING
TCP    0.0.0.0:1025              Sami:0                  LISTENING
TCP    0.0.0.0:2869              Sami:0                  LISTENING
TCP    0.0.0.0:3806              Sami:0                  LISTENING
TCP    0.0.0.0:5840              Sami:0                  LISTENING
TCP    0.0.0.0:5857              Sami:0                  LISTENING
TCP    0.0.0.0:8733              Sami:0                  LISTENING
TCP    0.0.0.0:9087              Sami:0                  LISTENING
TCP    0.0.0.0:49664             Sami:0                  LISTENING
TCP    0.0.0.0:49665             Sami:0                  LISTENING
TCP    0.0.0.0:49666             Sami:0                  LISTENING
TCP    0.0.0.0:49667             Sami:0                  LISTENING
TCP    0.0.0.0:49668             Sami:0                  LISTENING
TCP    127.0.0.1:6463            Sami:0                  LISTENING
TCP    192.168.0.11:139          Sami:0                  LISTENING
TCP    192.168.0.11:1926         20.180.118.190:https    ESTABLISHED
TCP    192.168.0.11:5945         162.159.135.234:https    ESTABLISHED
TCP    192.168.0.11:6324         sa-lan-f188:528         ESTABLISHED
TCP    192.168.0.11:6333         66:https                ESTABLISHED
TCP    192.168.0.11:6391         150:https                ESTABLISHED
TCP    192.168.0.11:6400         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6409         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6412         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6413         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6414         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6415         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6416         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6417         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6418         a184-26-54-161:https    CLOSE_WAIT
TCP    192.168.0.11:6419         a184-26-54-178:https    CLOSE_WAIT
TCP    192.168.0.11:6420         204.79.197.222:https     CLOSE_WAIT
TCP    192.168.0.11:6421         52.98.123.194:https     CLOSE_WAIT
TCP    192.168.0.11:6424         13.107.0.254:https       CLOSE_WAIT
TCP    192.168.0.11:6425         172.202.64.254:https     CLOSE_WAIT
TCP    192.168.0.11:6439         1:https                  ESTABLISHED
TCP    192.168.0.11:6448         64:https                  ESTABLISHED
TCP    192.168.0.11:6459         20.44.229.132:https      ESTABLISHED
TCP    192.168.0.11:6461         62.2.3.89:72-25:https    CLOSE_WAIT
TCP    [::]:135                  Sami:0                  LISTENING
TCP    [::]:445                  Sami:0                  LISTENING
TCP    [::]:1025                 Sami:0                  LISTENING
TCP    [::]:2869                 Sami:0                  LISTENING
TCP    [::]:3806                 Sami:0                  LISTENING
```

Figure 5: Netstat Command

- The ‘netstat’ command is a network utility used to display active network connections, listening ports, and related information on a system.
- It provides details about established connections, listening ports, routing tables, and network interface statistics.
- This tool is valuable for diagnosing network issues, identifying open ports, and monitoring network activity on a computer.



```
Command Prompt - nslookup
C:\Users\SAM\cmd\nslookup
Default Server: dns.google
Address: 8.8.8.8

> nslookup google.com
DNS request timed out.
  timeout was 2 seconds.
Server: google.com
Address: 2404:6800:4007:82b::200e

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
*** Request to google.com timed-out
> nslookup 192.168.0.1
Server: [192.168.0.1]
Address: 192.168.0.1

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
*** Request to 192.168.0.1 timed-out
>
```

Figure 6: Nslookup Command

4.6

- The ‘nslookup’ command is a network utility used for querying Domain Name System (DNS) servers to obtain information about domain names and IP addresses.
- It allows users to perform DNS lookups, find the IP address of a domain, and retrieve information about the DNS records associated with a specific hostname.
- This tool is useful for troubleshooting DNS-related issues, verifying DNS records, and obtaining information about domain name resolution.

5 Experience

- Explored practical examples to showcase the command's functionality.
- Tested the command on Linux, highlighting its usage and nuances.
- Recognized variations in command syntax when transitioning to the Windows environment.
- Emphasized the need for adaptability across different operating systems.

References

- [1] Windows IP Commands: <https://www.networkstraining.com/windows-ip-commands/>