

Lab 2: Important Network Commands for Testing and Troubleshooting

Introduction

Network troubleshooting is an essential skill for any network administrator or IT professional. Network commands help identify, diagnose, and resolve network connectivity issues, check system configurations, and ensure that devices communicate correctly. In this lab, we explore important network commands and their practical usage for testing and troubleshooting network problems.

Objectives

- Learn essential network commands used for testing and troubleshooting.
- Understand how to check network connectivity, IP configuration, and network routes.
- Identify and diagnose common network issues using command-line tools.

Materials Required

- Computer with Windows/Linux/Mac OS
- Active network connection (LAN or Wi-Fi)
- Command Prompt (Windows) / Terminal (Linux, Mac)

Network Commands and Usage

1. ping

- Purpose: Test connectivity to another host on the network.
- Syntax: `ping <IP address or hostname>`
- Use: Shows if the target is reachable and the time it takes for packets to travel.
- Example:

```
C:\Users\mrsar>ping google.com

Pinging google.com [2404:6800:4002:805::200e] with 32 bytes of data:
Reply from 2404:6800:4002:805::200e: time=26ms
Reply from 2404:6800:4002:805::200e: time=18ms
Reply from 2404:6800:4002:805::200e: time=19ms
Reply from 2404:6800:4002:805::200e: time=66ms

Ping statistics for 2404:6800:4002:805::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 66ms, Average = 32ms
```

2. ipconfig

- Purpose: Display your computer's IP address, subnet mask, and gateway.
- Syntax: ipconfig (windows) / ifconfig(Linux)
- Use: Helps identify which router or hop is slowing down or dropping packets.
- Example:

```
Command Prompt

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

Wireless LAN adapter Local Area Connection* 3:

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

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::3acd:c2e6:66df:36f4%24
IPv4 Address. . . . . : 192.168.20.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::58ac:420b:6d25:236e%13
IPv4 Address. . . . . : 192.168.132.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter WiFi:

Connection-specific DNS Suffix  . :
IPv6 Address. . . . . : 2400:1a00:3b2d:8c67:ba2:b704:9574:2510
Temporary IPv6 Address. . . . . : 2400:1a00:3b2d:8c67:c400:22f5:dacd:8637
Link-local IPv6 Address . . . . . : fe80::7882:f224:dd18:60bd%26
IPv4 Address. . . . . : 192.168.1.83
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%26
                             192.168.1.254

C:\Users\mrsar>
```

3. tracert

- Purpose: Find the path that data takes to reach a destination.
- Syntax: tracert <hostname or IP>
- Use: Helps identify which router or hop is slowing down or dropping packets.
- Example:

```
C:\Users\mrsar>tracert google.com

Tracing route to google.com [2404:6800:4002:824::200e]
over a maximum of 30 hops:

  1     2 ms     6 ms     2 ms  2400:1a00:3b2d:8c67::1
  2    12 ms    12 ms    13 ms  2400:1a00:3b02::1
  3     *        *        *    Request timed out.
  4    10 ms    10 ms    21 ms  2400:1a00:0:41::170
  5     6 ms     8 ms     8 ms  2400:1a00:0:41::128
  6    12 ms    25 ms    16 ms  2400:1a00:dccc:1:72:9:128:67
  7     *        *        *    Request timed out.
  8    30 ms    19 ms    22 ms  2001:4860:1:1::126a
  9    27 ms   128 ms    24 ms  2001:4860:0:1::78ab
 10    31 ms    28 ms    27 ms  2001:4860:0:1::50b
 11    26 ms    26 ms    27 ms  del12s07-in-x0e.1e100.net [2404:6800:4002:824::200e]

Trace complete.
```

4. nslookup

- Purpose: Check if a domain name correctly resolves to an IP address.
- Syntax: nslookup <domain>
- Use: Useful to troubleshoot DNS issues.
- Example:

```
C:\Users\mrsar>nslookup www.microsoft.com
Server:    UnKnown
Address:   fe80::1

Non-authoritative answer:
Name:      e13678.dscb.akamaiedge.net
Addresses: 2600:140f:2e00:784::356e
           2600:140f:2e00:78b::356e
           124.41.246.67
Aliases:   www.microsoft.com
           www.microsoft.com-c-3.edgekey.net
           www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
```

5. netstat

- Purpose: See all active network connections and open ports on your computer.
- Syntax: netstat -a
- Use: Monitor which applications are using network connections.
- Example:

```
C:\Users\mrsar>netstat -a

Active Connections

   Proto Local Address           Foreign Address         State
   TCP    0.0.0.0:135              Sarozz:0                LISTENING
   TCP    0.0.0.0:445              Sarozz:0                LISTENING
   TCP    0.0.0.0:902              Sarozz:0                LISTENING
   TCP    0.0.0.0:912              Sarozz:0                LISTENING
   TCP    0.0.0.0:1031             Sarozz:0                LISTENING
   TCP    0.0.0.0:1036             Sarozz:0                LISTENING
   TCP    0.0.0.0:5040             Sarozz:0                LISTENING
   TCP    0.0.0.0:7680             Sarozz:0                LISTENING
   TCP    0.0.0.0:8733             Sarozz:0                LISTENING
   TCP    0.0.0.0:9007             Sarozz:0                LISTENING
   TCP    0.0.0.0:49664            Sarozz:0                LISTENING
   TCP    0.0.0.0:49665            Sarozz:0                LISTENING
   TCP    0.0.0.0:49666            Sarozz:0                LISTENING
   TCP    0.0.0.0:49667            Sarozz:0                LISTENING
   TCP    0.0.0.0:49668            Sarozz:0                LISTENING
```

6. arp

- Purpose: Display or modify the ARP cache (which maps IPs to MAC addresses).
- Syntax: arp -a
- Use: Find MAC addresses of devices on the local network or detect IP conflicts.
- Example:

```
C:\Users\mrsar>arp -a

Interface: 192.168.132.1 --- 0xd
Internet Address      Physical Address      Type
192.168.132.254       00-50-56-eb-c5-35     dynamic
192.168.132.255       ff-ff-ff-ff-ff-ff     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
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.20.1 --- 0x18
Internet Address      Physical Address      Type
192.168.20.254        00-50-56-ed-a8-2f     dynamic
192.168.20.255        ff-ff-ff-ff-ff-ff     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

Interface: 192.168.1.83 --- 0x1a
Internet Address      Physical Address      Type
192.168.1.254         c8-9c-bb-75-22-60     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     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
```

7. route

- Purpose: View your computer's IP routing table and diagnose routing paths.
- Syntax: route print
- Use: Check network routes and identify potential routing problems.
- Example:

```
C:\Users\mrsar>route print
=====
Interface List
 4...08 8f c3 27 33 0f .....Killer E2600 Gigabit Ethernet Controller
10...00 ff 48 1a ce 31 .....TAP-Windows Adapter V9
 8...00 ff 2f 0a 66 6c .....TAP-Windows Adapter V9 #2
 5...00 ff 27 16 a2 05 .....TAP-Windows Adapter V9 #3
21...00 ff bb 56 c2 27 .....TAP-Windows Adapter V9 #4
12...f6 7b 09 74 d6 be .....Microsoft Wi-Fi Direct Virtual Adapter
19...f4 7b 09 74 d6 bf .....Microsoft Wi-Fi Direct Virtual Adapter #3
24...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
13...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
26...f4 7b 09 74 d6 be .....Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface           Metric
0.0.0.0                    0.0.0.0          192.168.1.254       192.168.1.83         45
127.0.0.0                  255.0.0.0         On-link             127.0.0.1            331
127.0.0.1                  255.255.255.255   On-link             127.0.0.1            331
127.255.255.255            255.255.255.255   On-link             127.0.0.1            331
192.168.1.0                255.255.255.0     On-link             192.168.1.83         301
192.168.1.83               255.255.255.255   On-link             192.168.1.83         301
192.168.1.255              255.255.255.255   On-link             192.168.1.83         301
192.168.20.0               255.255.255.0     On-link             192.168.20.1         291
192.168.20.1               255.255.255.255   On-link             192.168.20.1         291
192.168.20.255             255.255.255.255   On-link             192.168.20.1         291
192.168.132.0              255.255.255.0     On-link             192.168.132.1        291
192.168.132.1              255.255.255.255   On-link             192.168.132.1        291
192.168.132.255            255.255.255.255   On-link             192.168.132.1        291
224.0.0.0                  240.0.0.0         On-link             127.0.0.1            331
224.0.0.0                  240.0.0.0         On-link             192.168.20.1         291
```

8. telnet

- Purpose: Test connectivity to a specific TCP port on a remote host.
- Syntax: telnet <hostname_or_IP> <port>
- Use: Verify if services like web servers, mail servers, or SSH are reachable.
- Example:

```
C:\Users\mrsar>telnet 192.168.1.1 80
Connecting To 192.168.1.1...|
```

10. netsh

- Purpose: Configure, reset, or troubleshoot network interfaces and Windows Firewall.
- Syntax: netsh interface show interface
- Use: View interface status, reset TCP/IP stack, or troubleshoot network configuration issues.
- Example:

```
C:\Users\mrsar>netsh interface show interface
```

| Admin State | State | Type | Interface Name |
|-------------|--------------|-----------|-------------------------------|
| Enabled | Disconnected | Dedicated | Local Area Connection |
| Enabled | Disconnected | Dedicated | Local Area Connection 3 |
| Enabled | Disconnected | Dedicated | Local Area Connection 2 |
| Enabled | Disconnected | Dedicated | WhitehatVPN |
| Enabled | Connected | Dedicated | VMware Network Adapter VMnet1 |
| Enabled | Connected | Dedicated | VMware Network Adapter VMnet8 |
| Enabled | Disconnected | Dedicated | Ethernet |
| Enabled | Connected | Dedicated | WiFi |
| Enabled | Disconnected | Dedicated | Local Area Connection* 1 |

11. getmac

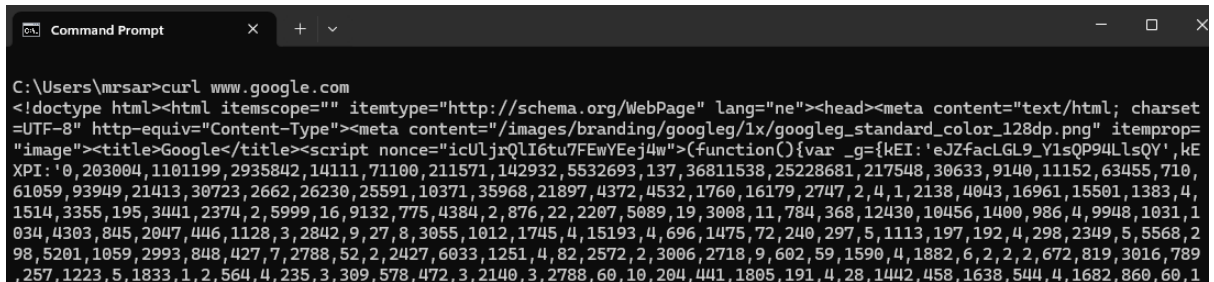
- Purpose: Display MAC addresses of all network adapters on your computer.
- Syntax: getmac
- Use: Identify network interface MAC addresses for troubleshooting or inventory.
- Example:

```
C:\Users\mrsar>getmac
```

| Physical Address | Transport Name |
|-------------------|--|
| 08-8F-C3-27-33-0F | Media disconnected |
| 00-FF-48-1A-CE-31 | Media disconnected |
| 00-50-56-C0-00-01 | \Device\Tcpip_{CD83D087-CD34-445C-8CF5-4693320FFB41} |
| 00-50-56-C0-00-08 | \Device\Tcpip_{5B0B94F3-01AC-4F24-BDC9-E951E8C226E9} |
| 00-FF-2F-0A-66-6C | Media disconnected |
| 00-FF-27-16-A2-05 | Media disconnected |
| F4-7B-09-74-D6-BE | \Device\Tcpip_{E9207A49-FEF1-4A52-B795-3771E0EB92BB} |
| F6-7B-09-74-D6-BE | Media disconnected |
| 00-FF-BB-56-C2-27 | Media disconnected |

12. curl

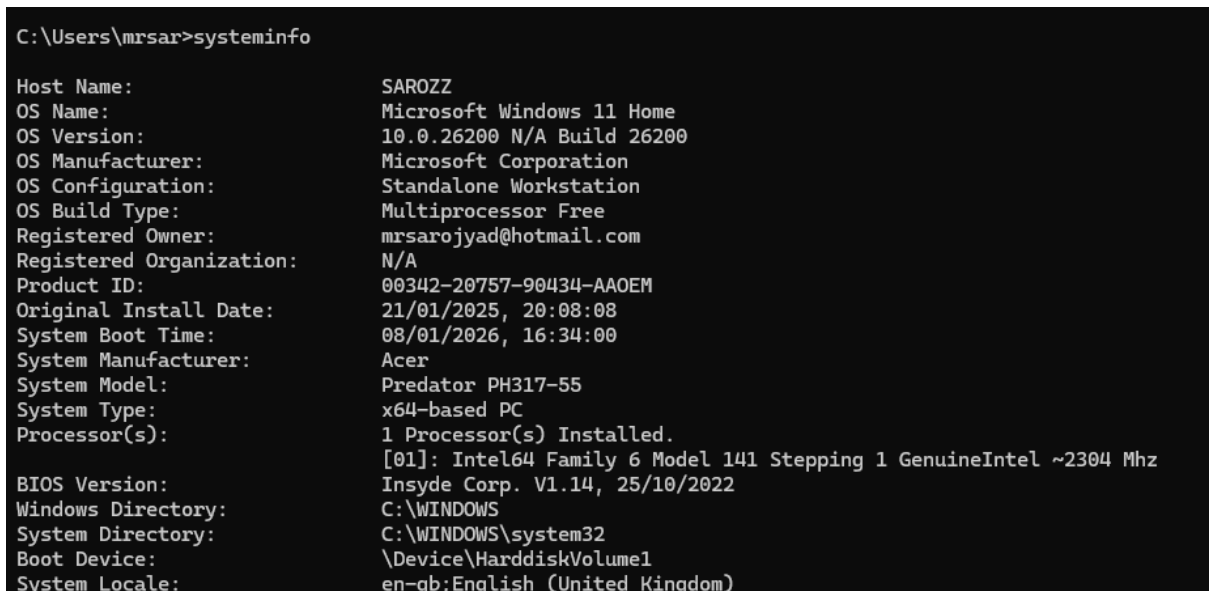
- Purpose: Test connectivity and HTTP requests to a URL or API.
- Syntax: curl <URL>
- Use: Verify website accessibility, response codes, or download content for testing.
- Example:



```
C:\Users\mrsar>curl www.google.com
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="ne"><head><meta content="text/html; charset
=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop=
"image"><title>Google</title><script nonce="icUljrQLI6tu7FEwYEEj4w">(function(){var _g={kEI:'eJZfacLGL9_Y1sQP94LLsQY',kE
XPI:'0,203004,1101199,2935842,14111,71100,211571,142932,5532693,137,36811538,25228681,217548,30633,9140,11152,63455,710,
61059,93949,21413,30723,2662,26230,25591,10371,35968,21897,4372,4532,1760,16179,2747,2,4,1,2138,4043,16961,15501,1383,4,
1514,3355,195,3441,2374,2,5999,16,9132,775,4384,2,876,22,2207,5089,19,3008,11,784,368,12430,10456,1400,986,4,9948,1031,1
034,4303,845,2047,446,1128,3,2842,9,27,8,3055,1012,1745,4,15193,4,696,1475,72,240,297,5,1113,197,192,4,298,2349,5,5568,2
98,5201,1059,2993,848,427,7,2788,52,2,2427,6033,1251,4,82,2572,2,3006,2718,9,602,59,1590,4,1882,6,2,2,2,672,819,3016,789
,257,1223,5,1833,1,2,564,4,235,3,309,578,472,3,2140,3,2788,60,10,204,441,1805,191,4,28,1442,458,1638,544,4,1682,860,60,1
```

13. systeminfo

- Purpose: View detailed system information including network adapters and host info.
- Syntax: systeminfo
- Use: Check OS, network adapters, and hardware info that might affect connectivity.
- Example:



```
C:\Users\mrsar>systeminfo

Host Name: SAROZZ
OS Name: Microsoft Windows 11 Home
OS Version: 10.0.26200 N/A Build 26200
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: mrsarojyad@hotmail.com
Registered Organization: N/A
Product ID: 00342-20757-90434-AAOEM
Original Install Date: 21/01/2025, 20:08:08
System Boot Time: 08/01/2026, 16:34:00
System Manufacturer: Acer
System Model: Predator PH317-55
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
               [01]: Intel64 Family 6 Model 141 Stepping 1 GenuineIntel ~2304 Mhz
BIOS Version: Insyde Corp. V1.14, 25/10/2022
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-gb;English (United Kingdom)
```

Procedure:

1. Open CMD (Windows) or Terminal (Linux/Mac).
2. Execute each command using a target IP or domain.
3. Observe and record the output.
4. Take screenshots after running each command.
5. Analyse the results to understand connectivity, routing, or DNS issues.

Results:

- All commands executed successfully.
- ping confirmed connectivity, ipconfig showed IP settings, tracert traced network paths.
- nslookup verified DNS resolution, netstat monitored active connections.

Conclusion:

These network commands allow us to efficiently identify and resolve connectivity and configuration issues. Tools such as ping, tracert, nslookup, and netstat provide valuable insights into network performance, routing paths, and service availability. Mastery of these commands is essential for effective network troubleshooting and maintaining reliable network operations.