

|       |                   |
|-------|-------------------|
| Name  | Aarush Maheshwari |
| UID   | 2023200076        |
| Batch | A4                |

## Experiment: FCAPS Network Management (Windows & Ubuntu)

### Aim

To study and implement the FCAPS (Fault, Configuration, Accounting, Performance, and Security) network management model using Windows and Ubuntu operating systems.

### Objectives

- To understand the FCAPS network management model
- To identify and analyze network faults
- To perform configuration management on networked systems
- To monitor accounting and performance parameters
- To apply basic security management techniques

### Tools / Software Required

- Windows 10/11 OS
- Ubuntu Linux OS
- Command Prompt / PowerShell
- Nmap
- Wireshark
- SNMP utilities
- iPerf
- Windows Defender Firewall / UFW

### 1. Fault Management

Objective: To detect unreachable or faulty devices in the network.

#### Windows Steps

1. Open Command Prompt.
2. Execute: ping <IP\_address>

```

C:\Users\Admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=116
Reply from 8.8.8.8: bytes=32 time=1ms TTL=116
Reply from 8.8.8.8: bytes=32 time=1ms TTL=116
Reply from 8.8.8.8: bytes=32 time=1ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Admin>

```

Observation: The ping 8.8.8.8 command is used to test network connectivity to a remote host. The output shows all packets were successfully received with 0% packet loss and an average response time of 1 ms, indicating a stable and fast network connection.

3. Observe packet loss or timeout messages.

4. Execute: tracert <IP\_address>

```

C:\Users\CCN>tracert 8.8.8.8

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

  1  <1 ms  <1 ms  <1 ms  10.10.53.1
  2  <1 ms  <1 ms  <1 ms  194.0.0.1
  3  11 ms   3 ms    1 ms   static-5.21.248.49-tataidc.co.in [49.
248.21.5]
  4  *        *        *        Request timed out.
  5  2 ms     *        *        10.129.21.54
  6  2 ms     2 ms    2 ms    72.14.210.20
  7  27 ms    22 ms   20 ms   216.239.57.17
  8  2 ms     2 ms    2 ms    142.251.69.105
  9  *        2 ms    2 ms    dns.google [8.8.8.8]

Trace complete.

C:\Users\CCN>show startup-config
'show' is not recognized as an internal or external command,
operable program or batch file.

```

Observation: The `tracert 8.8.8.8` command displays the path taken by packets from the local system to the destination host. The output shows multiple intermediate routers with their response times, and a few timed-out hops, indicating normal routing behavior before successfully reaching the destination.

5. Identify where the connection fails.

Connection fails at hop 4 where the request has been timed out.

### Ubuntu Steps

1. Open Terminal.
2. Execute: `ping <IP_address>`
3. Stop ping using `Ctrl+C`.

```
dell@dell-OptiPlex-Tower-7020:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=1.94 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=2.30 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=2.18 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=1.99 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=2.21 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=1.89 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=117 time=2.27 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=117 time=1.85 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=117 time=2.00 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=117 time=2.07 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=117 time=2.38 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=117 time=1.83 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=117 time=1.97 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=117 time=2.18 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=117 time=1.96 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=117 time=2.16 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=117 time=1.90 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=117 time=2.13 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=117 time=1.92 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=117 time=1.93 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=117 time=2.14 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=117 time=39.8 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=117 time=2.46 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=117 time=2.63 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=117 time=2.38 ms
^C
--- 8.8.8.8 ping statistics ---
25 packets transmitted, 25 received, 0% packet loss, time 24034ms
rtt min/avg/max/mdev = 1.834/3.620/39.849/7.397 ms
dell@dell-OptiPlex-Tower-7020:~$
```

Observation: The ping 8.8.8.8 command checks reachability of the destination host from the system. The output shows 25 packets transmitted and received with 0% packet loss and low average delay, indicating a stable and reliable network connection.

4. Execute: traceroute <IP\_address>

```
dell@dell-OptiPlex-Tower-7020:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.10.50.1)  0.552 ms  0.509 ms  0.493 ms
 2  194.0.0.1 (194.0.0.1)  0.264 ms  0.250 ms  0.234 ms
 3  static-5.21.248.49-tataidc.co.in (49.248.21.5)  2.123 ms  1.907 ms  2.094 ms
 4  43.252.192.229 (43.252.192.229)  1.227 ms  1.213 ms  1.196 ms
 5  103.205.124.81 (103.205.124.81)  1.303 ms  10.129.21.54 (10.129.21.54)  2.39 ms
 6  27.109.1.149 (27.109.1.149)  1.138 ms  72.14.210.20 (72.14.210.20)  1.789 ms
 7  72.14.204.217 (72.14.204.217)  1.521 ms  *  1.652 ms
 8  * * *
 9  dns.google (8.8.8.8)  1.777 ms  2.671 ms  2.644 ms
dell@dell-OptiPlex-Tower-7020:~$
```

Observation: The traceroute 8.8.8.8 command displays the sequence of network hops between the source and destination. The output lists intermediate gateways with their response times and successfully reaches the destination, showing normal packet routing across the network.

5. Identify unreachable hops.

Hop 8 is unreachable

## 2. Configuration Management

Objective: To view and manage network configuration details.

### Windows Steps

1. Open Command Prompt.
2. Execute: ipconfig /all

```

C:\Users\Admin>ipconfig /all

Windows IP Configuration

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

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Ethernet Connection (17) I219-LM
Physical Address. . . . . : E8-CF-83-38-45-50
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::57a4:d56b:7035:b6c3%5(Preferred)
IPv4 Address. . . . . : 10.10.50.209(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : 03 February 2026 09:38:25
Lease Expires . . . . . : 03 February 2026 10:08:25
Default Gateway . . . . . : 10.10.50.1
DHCP Server . . . . . : 10.10.50.1
DHCPv6 IAID . . . . . : 115920771
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-AE-FF-D9-E8-CF-83-38-45-50
DNS Servers . . . . . : 172.16.10.4
                        172.16.10.5
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Admin>

```

Observation: The ipconfig /all command displays detailed network configuration of the system. The output shows IP address, subnet mask, default gateway, DNS servers, and DHCP status, confirming correct network interface configuration.

3. Note IP address, gateway, and DNS details.

IP address : 10.10.50.209

Gateway : 10.10.50.1

DNS servers: 172.16.10.4 and 172.16.10.5

4. (Optional) Use SNMP tools to fetch system info.

### Ubuntu Steps

1. Open Terminal.
2. Execute: ifconfig OR ip a




```
dell@dell-OptiPlex-Tower-7020:~$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.50.209 netmask 255.255.254.0 broadcast 10.10.51.255
    inet6 fe80::567:c182:206c:7e72 prefixlen 64 scopeid 0x20<link>
    ether e8:cf:83:38:45:50 txqueuelen 1000 (Ethernet)
    RX packets 149536 bytes 135605544 (135.6 MB)
    RX errors 0 dropped 1861 overruns 0 frame 0
    TX packets 45838 bytes 22173329 (22.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 memory 0x70500000-70520000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2524 bytes 265075 (265.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2524 bytes 265075 (265.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

dell@dell-OptiPlex-Tower-7020:~$
```

Observation: The ifconfig command provides information about network interfaces and their status. The output indicates the assigned IP address, MAC address, packet statistics, and confirms that the interface is active and running.

3. Execute: hostnamectl

```
dell@dell-OptiPlex-Tower-7020:~$ hostnamectl
Static hostname: dell-OptiPlex-Tower-7020
    Icon name: computer-desktop
    Chassis: desktop 
    Machine ID: 2a59fb1414ad424d92ee1fe56fafb474
    Boot ID: 48cb61b73c3043eba46b23f04b83d133
Operating System: Ubuntu 24.04.2 LTS
    Kernel: Linux 6.14.0-34-generic
    Architecture: x86-64
Hardware Vendor: Dell Inc.
    Hardware Model: OptiPlex Tower 7020
Firmware Version: 1.20.0
    Firmware Date: Thu 2025-09-04
    Firmware Age: 5month
dell@dell-OptiPlex-Tower-7020:~$
```

Observation: The hostnamectl command shows system identification and operating system details. The output displays the system hostname, OS version, kernel, architecture, and hardware information, confirming successful system configuration.

4. Use SNMP: snmpwalk -v2c -c public <IP\_address> system

```
dell@dell-OptiPlex-Tower-7020:~$ snmpwalk -v2c -c public 127.0.0.1
iso.3.6.1.2.1.1.1.0 = STRING: "Linux dell-OptiPlex-Tower-7020 6.14.0-34-generic #34-24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Tue Sep 23 15:35:20 UTC 2 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (3498) 0:00:34.98
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "dell-OptiPlex-Tower-7020"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (546549) 1:31:05.49
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 EA 02 03 0E 33 2E 08 2B 05 1E
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/boot/vmlinuz-6.14.0-34-generic root=UUID=ccf035e8-3293-48c8-afa2-757955d2aa61 ro quiet splash vt.handoff=7"
```

Observation: The snmpwalk -v2c -c public 127.0.0.1 command retrieves SNMP Management Information Base (MIB) data from the local system.

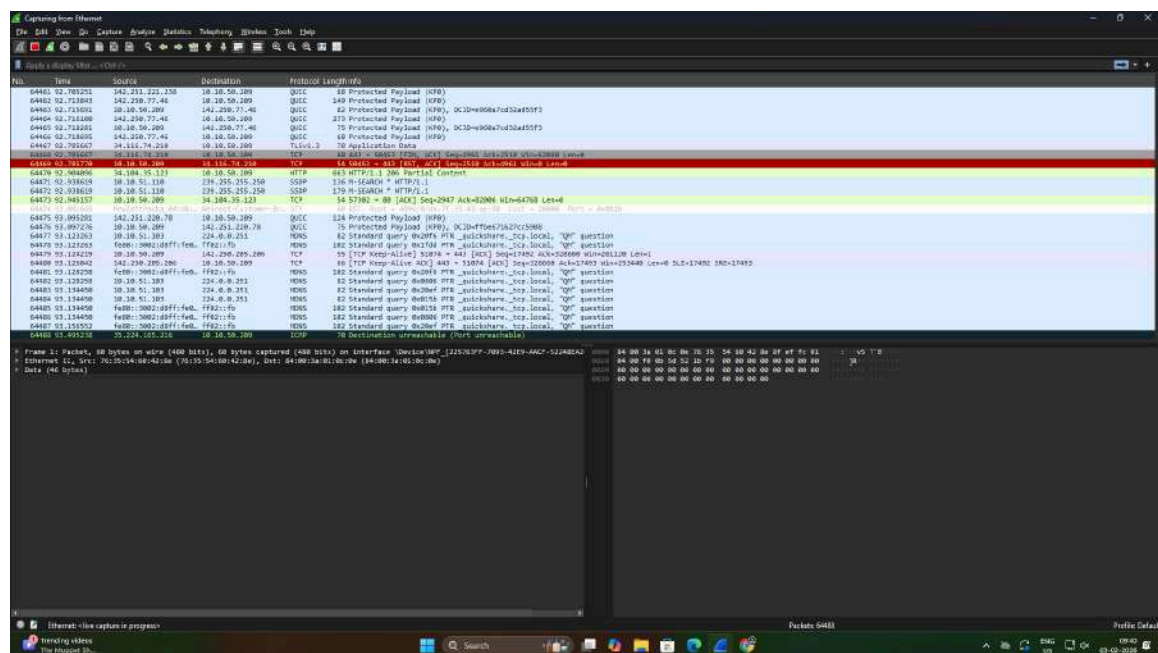
The output lists system details such as OS version, hostname, uptime, and SNMP modules, indicating that the SNMP service is active and responding correctly.

### 3. Accounting Management

Objective: To monitor network usage.

#### Windows Steps

1. Launch Wireshark.
2. Select active network interface.
3. Start capture and generate network traffic.



Observation: The screenshot shows live network traffic captured using Wireshark. Different protocols such as TCP, UDP, DNS, and QUIC are visible along with source/destination IPs, indicating real-time packet flow and communication analysis.

4. Use Statistics → Protocol Hierarchy to analyze usage.

The screenshot shows the 'Protocol Hierarchy Statistics - Ethernet' window in Wireshark. It provides a summary of the captured traffic by protocol, including the percentage of packets and bytes, and the count of packets and bytes. The data is organized into a table with columns for Protocol, Percent Packets, Packets, Percent Bytes, Bytes, Bits/s, End Packets, End Bytes, End Bits/s, and Pkts/s.

| Protocol                              | Percent Packets | Packets | Percent Bytes | Bytes    | Bits/s | End Packets | End Bytes | End Bits/s | Pkts/s |
|---------------------------------------|-----------------|---------|---------------|----------|--------|-------------|-----------|------------|--------|
| Ethernet                              | 100.0           | 66635   | 100.0         | 57527208 | 4144 k | 0           | 0         | 0          | 66635  |
| Logical-Link Control                  | 0.1             | 69      | 0.0           | 220      | 15     | 0           | 0         | 0          | 69     |
| Spanning Tree Protocol                | 0.1             | 33      | 0.0           | 1080     | 142    | 33          | 1080      | 142        | 33     |
| Logical-Link Control Basic Format XID | 0.0             | 1       | 0.0           | 3        | 0      | 1           | 3         | 0          | 1      |
| Link Layer Discovery Protocol         | 0.0             | 4       | 0.0           | 1020     | 73     | 4           | 1020      | 73         | 4      |
| Internet Protocol Version 6           | 1.1             | 737     | 0.1           | 30262    | 2204   | 0           | 0         | 0          | 737    |
| Use Datagram Protocol                 | 1.1             | 701     | 0.0           | 5608     | 404    | 0           | 0         | 0          | 701    |
| Simple Service Discovery Protocol     | 0.4             | 238     | 0.2           | 116848   | 8418   | 238         | 116848    | 8418       | 238    |
| Multicast Domain Name System          | 0.6             | 429     | 0.1           | 40439    | 2913   | 429         | 40439     | 2913       | 429    |
| Link-local Multicast Name Resolution  | 0.0             | 20      | 0.0           | 544      | 39     | 20          | 544       | 39         | 20     |
| DNS                                   | 0.0             | 14      | 0.0           | 760      | 56     | 14          | 760       | 56         | 14     |
| Internet Control Message Protocol v6  | 0.1             | 56      | 0.0           | 1644     | 118    | 56          | 1644      | 118        | 56     |
| Internet Protocol Version 4           | 96.1            | 63395   | 2.3           | 1308068  | 94 k   | 0           | 0         | 0          | 63395  |
| Use Datagram Protocol                 | 71.5            | 47664   | 0.7           | 387312   | 27 k   | 0           | 0         | 0          | 47664  |
| Simple Service Discovery Protocol     | 0.4             | 279     | 0.2           | 130808   | 9411   | 279         | 130808    | 9411       | 279    |
| OSPF                                  | 99.9            | 66603   | 99.8          | 39570510 | 2851 k | 49603       | 39570510  | 2781 k     | 49603  |
| Network Time Protocol                 | 0.0             | 2       | 0.0           | 96       | 6      | 2           | 96        | 6          | 2      |
| NetBIOS Name Service                  | 0.0             | 21      | 0.0           | 1374     | 98     | 21          | 1374      | 98         | 21     |
| NetBIOS Datagram Service              | 0.0             | 2       | 0.0           | 164      | 11     | 0           | 0         | 0          | 2      |
| SMB (Server Message Block Protocol)   | 0.0             | 2       | 0.0           | 238      | 17     | 0           | 0         | 0          | 2      |
| SMB MailSlot Protocol                 | 0.0             | 2       | 0.0           | 50       | 3      | 0           | 0         | 0          | 2      |
| Microsoft Windows Browser Protocol    | 0.0             | 2       | 0.0           | 66       | 4      | 2           | 66        | 4          | 2      |
| Multicast Domain Name System          | 0.6             | 420     | 0.1           | 34290    | 2482   | 420         | 34290     | 2482       | 420    |
| Link-local Multicast Name Resolution  | 0.0             | 9       | 0.0           | 232      | 18     | 9           | 232       | 18         | 9      |
| Dynamic Host Configuration Protocol   | 0.1             | 43      | 0.0           | 13806    | 942    | 43          | 13806     | 942        | 43     |
| Domain Name System                    | 0.3             | 229     | 0.0           | 15043    | 1086   | 229         | 15043     | 1086       | 229    |
| Transmission Control Protocol         | 28.5            | 17083   | 0.7           | 294404   | 21 k   | 9008        | 222452    | 16 k       | 17083  |
| Transport Layer Security              | 12.6            | 8190    | 24.3          | 13807639 | 1008 k | 8190        | 13244451  | 954 k      | 8190   |
| Hypertext Transfer Protocol           | 0.1             | 47      | 0.0           | 10803    | 1432   | 30          | 12117     | 874        | 47     |
| JavaScript Object Notation            | 0.0             | 1       | 0.0           | 0        | 0      | 0           | 0         | 0          | 1      |
| Line-based text data                  | 0.0             | 1       | 0.0           | 80       | 5      | 1           | 80        | 5          | 1      |
| Internet Group Management Protocol    | 0.1             | 42      | 0.0           | 368      | 26     | 42          | 368       | 26         | 42     |
| Internet Control Message Protocol     | 0.0             | 6       | 0.0           | 216      | 15     | 6           | 216       | 15         | 6      |
| Data                                  | 0.5             | 349     | 0.4           | 217362   | 15 k   | 349         | 217362    | 15 k       | 349    |
| Audio Instant AP Protocol             | 0.2             | 119     | 0.0           | 5474     | 394    | 119         | 5474      | 394        | 119    |
| Address Resolution Protocol           | 0.3             | 201     | 0.0           | 5628     | 405    | 201         | 5628      | 405        | 201    |

Observation: This summarizes captured traffic based on protocol distribution. The output shows the percentage and packet count for each protocol, helping analyze network usage patterns and dominant protocols in the captured data.

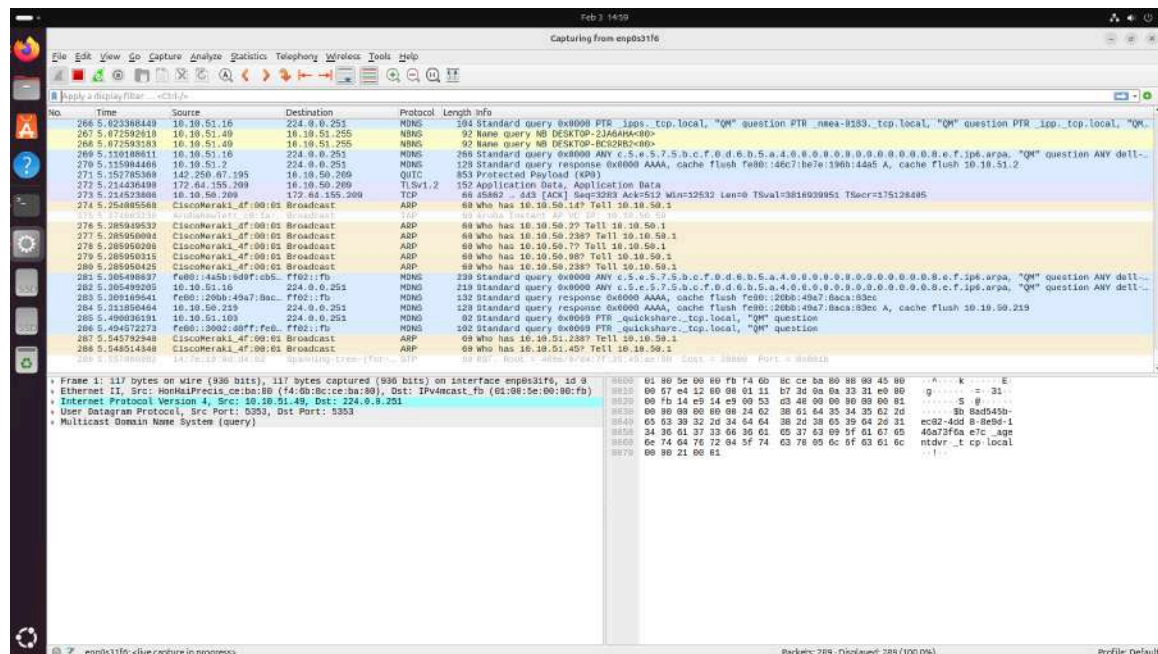


## Ubuntu Steps

### 1. Start Wireshark with sudo privileges.

```
dell@dell-OptiPlex-Tower-7020:~$ sudo wireshark
[sudo] password for dell:
** (wireshark:4763) 14:59:35.949127 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME
E_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:4763) 14:59:40.133190 [Capture MESSAGE] -- Capture Start ...
** (wireshark:4763) 14:59:40.186481 [Capture MESSAGE] -- Capture started
** (wireshark:4763) 14:59:40.186540 [Capture MESSAGE] -- File: "/tmp/wireshark_
enp0s31f64507J3.pcapng"
** (wireshark:4763) 15:01:41.764104 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:4763) 15:01:41.785440 [Capture MESSAGE] -- Capture stopped.
** (wireshark:4763) 15:01:41.785498 [Capture WARNING] ./ui/capture.c:722 -- cap
ture_input_closed():
```

### 2. Capture packets on active interface.



Observation : The screenshot shows packet capture containing DNS queries, ARP requests, and responses. This indicates normal name resolution and address mapping activity occurring within the local network.

### 3. Apply filters such as tcp, udp.



Wireshark - Conversations - emp03316

| Address A       | Port A | Address B       | Port B | Packets | Bytes     | Stream ID | Total Packets | Percent Filtered | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration |
|-----------------|--------|-----------------|--------|---------|-----------|-----------|---------------|------------------|---------------|-------------|---------------|-------------|-----------|----------|
| 10.10.50.209    | 54122  | 34.36.137.203   | 443    | 4       | 342 bytes | 2         | 4             | 100.00%          | 2             | 171 bytes   | 2             | 171 bytes   | 23.196594 | 0.0351   |
| 10.10.50.209    | 37992  | 142.250.194.229 | 443    | 17      | 7 kB      | 6         | 17            | 100.00%          | 9             | 4 kB        | 8             | 2 kB        | 51.771301 | 3.9635   |
| 10.10.50.209    | 42636  | 151.101.129.91  | 443    | 4       | 342 bytes | 3         | 4             | 100.00%          | 2             | 171 bytes   | 2             | 171 bytes   | 24.243246 | 0.0667   |
| 10.10.50.209    | 45662  | 172.04.155.209  | 443    | 44      | 13 kB     | 0         | 44            | 100.00%          | 25            | 9 kB        | 19            | 4 kB        | 46.811981 | 36.5406  |
| 54.47.296.11    | 3323   | 10.10.51.132    | 63348  | 2       | 132 bytes | 4         | 2             | 100.00%          | 2             | 132 bytes   | 0             | 0 bytes     | 26.944932 | 30.2122  |
| 199.232.210.172 | 80     | 10.10.51.130    | 56816  | 1       | 60 bytes  | 1         | 1             | 100.00%          | 1             | 60 bytes    | 0             | 0 bytes     | 7.273846  | 0.0000   |
| 199.232.210.172 | 80     | 10.10.51.130    | 56812  | 1       | 60 bytes  | 3         | 1             | 100.00%          | 1             | 60 bytes    | 0             | 0 bytes     | 31.293373 | 0.0000   |

Wireshark - Conversations - emp03316

| Address A    | Port A | Address B       | Port B | Packets | Bytes     | Stream ID | Total Packets | Percent Filtered | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start  | C   |
|--------------|--------|-----------------|--------|---------|-----------|-----------|---------------|------------------|---------------|-------------|---------------|-------------|------------|-----|
| 0.0.0.0      | 68     | 255.255.255.255 | 67     | 6       | 2 kB      | 32        | 6             | 100.00%          | 6             | 2 kB        | 0             | 0 bytes     | 4.712789   | 41  |
| 10.10.50.1   | 67     | 255.255.255.255 | 68     | 1       | 345 bytes | 194       | 1             | 100.00%          | 1             | 345 bytes   | 0             | 0 bytes     | 113.667548 | 0.1 |
| 10.10.50.32  | 5353   | 224.0.0.251     | 5353   | 5       | 940 bytes | 171       | 5             | 100.00%          | 5             | 940 bytes   | 0             | 0 bytes     | 11.271213  | 0.1 |
| 10.10.50.56  | 5353   | 224.0.0.251     | 5353   | 18      | 2 kB      | 81        | 18            | 100.00%          | 18            | 2 kB        | 0             | 0 bytes     | 18.324265  | 162 |
| 10.10.50.70  | 5353   | 224.0.0.251     | 5353   | 18      | 2 kB      | 82        | 18            | 100.00%          | 18            | 2 kB        | 0             | 0 bytes     | 18.324438  | 162 |
| 10.10.50.85  | 60576  | 10.10.51.255    | 3490   | 1       | 594 bytes | 54        | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 3.180638   | 0.1 |
| 10.10.50.85  | 60510  | 10.10.51.255    | 3490   | 1       | 594 bytes | 154       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 59.166187  | 0.1 |
| 10.10.50.85  | 60829  | 10.10.51.255    | 3490   | 1       | 594 bytes | 86        | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 15.182627  | 0.1 |
| 10.10.50.85  | 61118  | 10.10.51.255    | 3490   | 1       | 594 bytes | 335       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 49.160030  | 0.1 |
| 10.10.50.85  | 61508  | 10.10.51.255    | 3490   | 1       | 594 bytes | 199       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 119.116189 | 0.1 |
| 10.10.50.85  | 61303  | 10.10.51.255    | 3490   | 1       | 594 bytes | 190       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 109.113648 | 0.1 |
| 10.10.50.85  | 63461  | 10.10.51.255    | 3490   | 1       | 594 bytes | 175       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 78.111826  | 0.1 |
| 10.10.50.85  | 63537  | 10.10.51.255    | 3490   | 1       | 594 bytes | 179       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 89.112383  | 0.1 |
| 10.10.50.85  | 63700  | 10.10.51.255    | 3490   | 1       | 594 bytes | 168       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 95.109805  | 0.1 |
| 10.10.50.85  | 64699  | 10.10.51.255    | 3490   | 1       | 594 bytes | 113       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 29.104315  | 0.1 |
| 10.10.50.85  | 64881  | 10.10.51.255    | 3490   | 1       | 594 bytes | 186       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 99.112041  | 0.1 |
| 10.10.50.85  | 65355  | 10.10.51.255    | 3490   | 1       | 594 bytes | 130       | 1             | 100.00%          | 1             | 594 bytes   | 0             | 0 bytes     | 39.105234  | 0.1 |
| 10.10.50.121 | 137    | 10.10.51.255    | 137    | 2       | 184 bytes | 187       | 2             | 100.00%          | 2             | 184 bytes   | 0             | 0 bytes     | 100.787671 | 0.1 |
| 10.10.50.135 | 5353   | 224.0.0.251     | 5353   | 1       | 120 bytes | 150       | 1             | 100.00%          | 1             | 120 bytes   | 0             | 0 bytes     | 56.103151  | 0.1 |
| 10.10.50.140 | 38267  | 239.255.255.250 | 1900   | 1       | 179 bytes | 82        | 1             | 100.00%          | 1             | 179 bytes   | 0             | 0 bytes     | 19.792082  | 0.1 |
| 10.10.50.171 | 5353   | 224.0.0.251     | 5353   | 6       | 714 bytes | 12        | 6             | 100.00%          | 6             | 714 bytes   | 0             | 0 bytes     | 11.983762  | 100 |
| 10.10.50.189 | 5353   | 224.0.0.251     | 5353   | 10      | 3 kB      | 173       | 10            | 100.00%          | 10            | 3 kB        | 0             | 0 bytes     | 78.831047  | 32  |
| 10.10.50.194 | 5353   | 224.0.0.251     | 5353   | 7       | 833 bytes | 4         | 7             | 100.00%          | 7             | 833 bytes   | 0             | 0 bytes     | 6.497890   | 126 |
| 10.10.50.197 | 5353   | 224.0.0.251     | 5353   | 2       | 238 bytes | 56        | 2             | 100.00%          | 2             | 238 bytes   | 0             | 0 bytes     | 6.412491   | 41  |
| 10.10.50.200 | 5353   | 224.0.0.251     | 5353   | 3       | 416 bytes | 44        | 3             | 100.00%          | 3             | 416 bytes   | 0             | 0 bytes     | 7.418288   | 41  |
| 10.10.50.201 | 5353   | 224.0.0.251     | 5353   | 20      | 2 kB      | 38        | 20            | 100.00%          | 20            | 2 kB        | 0             | 0 bytes     | 6.097826   | 134 |
| 10.10.50.202 | 5353   | 224.0.0.251     | 5353   | 1       | 291 bytes | 47        | 1             | 100.00%          | 1             | 291 bytes   | 0             | 0 bytes     | 7.960325   | 0.1 |
| 10.10.50.208 | 5353   | 224.0.0.251     | 5353   | 2       | 236 bytes | 86        | 2             | 100.00%          | 2             | 236 bytes   | 0             | 0 bytes     | 11.414745  | 41  |
| 10.10.50.209 | 40935  | 142.250.67.174  | 443    | 192     | 115 kB    | 9         | 192           | 100.00%          | 133           | 100 kB      | 59            | 15 kB       | 1.0070471  | 168 |
| 10.10.50.209 | 55269  | 142.250.67.195  | 443    | 32      | 24 kB     | 104       | 32            | 100.00%          | 8             | 7 kB        | 24            | 17 kB       | 25.752324  | 23  |
| 10.10.50.209 | 52946  | 142.250.67.195  | 443    | 31      | 23 kB     | 103       | 31            | 100.00%          | 8             | 7 kB        | 23            | 16 kB       | 25.770984  | 23  |
| 10.10.50.209 | 53377  | 142.250.70.42   | 443    | 37      | 23 kB     | 22        | 37            | 100.00%          | 12            | 9 kB        | 25            | 14 kB       | 30.104687  | 23  |
| 10.10.50.209 | 46089  | 142.250.194.227 | 443    | 56      | 26 kB     | 153       | 56            | 100.00%          | 21            | 9 kB        | 35            | 18 kB       | 50.221586  | 66  |
| 10.10.50.209 | 43657  | 142.250.195.74  | 443    | 24      | 2 kB      | 67        | 24            | 100.00%          | 12            | 870 bytes   | 12            | 1 kB        | 11.605668  | 106 |
| 10.10.50.209 | 52182  | 142.250.206.174 | 443    | 131     | 59 kB     | 70        | 131           | 100.00%          | 84            | 49 kB       | 47            | 11 kB       | 12.425669  | 106 |

Observation : This displays active IPv4 conversations between source and destination IP addresses. It summarizes packet counts and data volume exchanged, helping identify major communication pairs.

#### 4. Performance Management

Objective: To evaluate network performance.

#### Windows Steps

1. Install iPerf.
2. Run server: iperf -s
3. On another system, run: iperf -c <server\_IP>
4. Note throughput values.

```

PS C:\Users\Admin\Downloads\iperf3.20_64\iperf3.20> .\iperf3.exe -s
-----
Server listening on 5201 (test #1)
-----
Accepted connection from 10.10.51.136, port 56358
[ 5] local 10.10.51.139 port 5201 connected to 10.10.51.136 port 56359
[ ID] Interval            Transfer       Bitrate
[ 5]  0.00-1.01      sec    92.8 MBytes    774 Mbits/sec
[ 5]  1.01-2.01      sec    94.6 MBytes    794 Mbits/sec
[ 5]  2.01-3.00      sec    95.1 MBytes    799 Mbits/sec
[ 5]  3.00-4.00      sec    94.5 MBytes    794 Mbits/sec
[ 5]  4.00-5.00      sec    94.0 MBytes    790 Mbits/sec
[ 5]  5.00-6.00      sec    94.9 MBytes    796 Mbits/sec
[ 5]  6.00-7.01      sec    96.2 MBytes    797 Mbits/sec
[ 5]  7.01-8.01      sec    95.5 MBytes    802 Mbits/sec
[ 5]  8.01-9.01      sec    95.2 MBytes    801 Mbits/sec
[ 5]  9.01-10.01     sec    94.8 MBytes    794 Mbits/sec
[ 5] 10.01-10.01     sec     128 KBytes    700 Mbits/sec
-----
[ ID] Interval            Transfer       Bitrate
[ 5]  0.00-10.01     sec    948 MBytes    794 Mbits/sec
-----
Server listening on 5201 (test #2)
-----
|

```

Observation : The iperf3 -s command starts the system in server mode to measure network performance. The output shows successful client connections and high throughput values, indicating efficient data transfer over the network.

```

PS C:\Users\Admin\Downloads\iperf3.20_64\iperf3.20> .\iperf3.exe -c 10.10.51.136
Connecting to host 10.10.51.136, port 5201
[ 5] local 10.10.51.139 port 49092 connected to 10.10.51.136 port 5201
[ ID] Interval            Transfer       Bitrate
[ 5]  0.00-1.01      sec    78.2 MBytes    648 Mbits/sec
[ 5]  1.01-2.01      sec    77.0 MBytes    648 Mbits/sec
[ 5]  2.01-3.01      sec    76.5 MBytes    643 Mbits/sec
[ 5]  3.01-4.01      sec    77.2 MBytes    650 Mbits/sec
[ 5]  4.01-5.00      sec    75.2 MBytes    634 Mbits/sec
[ 5]  5.00-6.01      sec    77.9 MBytes    645 Mbits/sec
[ 5]  6.01-7.01      sec    75.2 MBytes    633 Mbits/sec
[ 5]  7.01-8.01      sec    76.1 MBytes    642 Mbits/sec
[ 5]  8.01-9.01      sec    77.2 MBytes    646 Mbits/sec
[ 5]  9.01-10.01     sec    72.8 MBytes    612 Mbits/sec
-----
[ ID] Interval            Transfer       Bitrate
[ 5]  0.00-10.01     sec    764 MBytes    640 Mbits/sec
[ 5]  0.00-10.01     sec    763 MBytes    640 Mbits/sec
-----
iperf Done.
PS C:\Users\Admin\Downloads\iperf3.20_64\iperf3.20> |

```

Observation: The iperf3 -c <IP> command initiates a bandwidth test toward the server.



The results display per-interval transfer and bitrate, confirming stable and consistent network performance.

#### Ubuntu Steps

1. Install iPerf: `sudo apt install iperf`
2. Run server: `iperf -s`

```
dell@dell-OptiPlex-Tower-7020:~$ iperf -s
-----
-
Server listening on TCP port 5001
TCP window size: 128 KByte (default)
-----
-
[ 1] local 10.10.50.209 port 5001 connected with 10.10.50.
219 port 46678 (icwnd/mss/irrtt=14/1448/898)
[ ID] Interval          Transfer      Bandwidth
[ 1] 0.0000-10.0176 sec  1.09 GBytes  934 Mbits/sec
[ 2] local 10.10.50.209 port 5001 connected with 10.10.50.
200 port 38138 (icwnd/mss/irrtt=14/1448/889)
```

Observation : The `iperf -s` command runs the system as a TCP performance measurement server. The output shows active connections with high bandwidth values, demonstrating good link capacity.

3. Run client: `iperf -c <server_IP>`

```
dell@dell-OptiPlex-Tower-7020:~$ iperf -c 10.10.50.200
-----
-
Client connecting to 10.10.50.200, TCP port 5001
TCP window size: 16.0 KByte (default)
-----
-
[ 1] local 10.10.50.209 port 60248 connected with 10.10.50.
200 port 5001 (icwnd/mss/irrtt=14/1448/746)
[ ID] Interval          Transfer      Bandwidth
[ 1] 0.0000-10.0234 sec  1.09 GBytes  933 Mbits/sec
dell@dell-OptiPlex-Tower-7020:~$
```

Observation : The screenshot displays configured inbound firewall rules in Windows Defender Firewall. It shows allowed and blocked rules based on protocol, port, and profile, indicating how incoming network traffic is controlled.



## Ubuntu Steps

### 1. Scan open ports: nmap <IP\_address>

```
dell@dell-OptiPlex-Tower-7020:~$ nmap 10.10.50.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-03 14:10 IST
Nmap scan report for dell-OptiPlex-Tower-7020 (10.10.50.209)
Host is up (0.00015s latency).
All 1000 scanned ports on dell-OptiPlex-Tower-7020 (10.10.50.209) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Observation : The nmap 10.10.50.209 command scans the local system for open TCP ports. The output shows all scanned ports are closed or filtered, indicating no active services are exposed.

```
dell@dell-OptiPlex-Tower-7020:~$ nmap 8.8.8.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-03 14:12 IST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0026s latency).
Not shown: 993 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
53/tcp    open  domain
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
```

Observation : The nmap 8.8.8.8 command scans a public DNS server for open services. The results show specific open ports such as 53 and 443, indicating accessible DNS and HTTPS services.

### 2. Enable firewall: sudo ufw enable

```
dell@dell-OptiPlex-Tower-7020:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

Observation : The sudo ufw enable command activates the Uncomplicated Firewall on the system. The output confirms that the firewall is enabled and will start automatically on system boot.



3. Block unused ports: `sudo ufw deny <port>`
4. Re-scan to verify security.

```
dell@dell-OptiPlex-Tower-7020:~$ sudo ufw allow 22/tcp
Rule updated
Rule updated (v6)
dell@dell-OptiPlex-Tower-7020:~$ sudo ufw status
Status: active

To Action From
--
53 DENY Anywhere
22/tcp ALLOW Anywhere
53 (v6) DENY Anywhere (v6)
22/tcp (v6) ALLOW Anywhere (v6)

dell@dell-OptiPlex-Tower-7020:~$ sudo ufw deny 22/tcp
Rule updated
Rule updated (v6)
dell@dell-OptiPlex-Tower-7020:~$ sudo ufw status
Status: active

To Action From
--
53 DENY Anywhere
22/tcp DENY Anywhere
53 (v6) DENY Anywhere (v6)
22/tcp (v6) DENY Anywhere (v6)

dell@dell-OptiPlex-Tower-7020:~$
```

Observation : UFW rules are added to allow and then deny TCP port 22, followed by checking firewall status. The final status output confirms that SSH traffic is blocked, demonstrating effective firewall rule enforcement.

**Conclusion :** This lab successfully demonstrated the practical implementation of network management concepts based on the FCAPS model. Fault-related activities were observed through connectivity and reachability testing using commands like ping and traceroute. Configuration management was validated by examining system and network settings using ipconfig, ifconfig, hostnamectl, and firewall rule configuration.

Accounting and performance aspects were analyzed using tools such as iperf, snmpwalk, and Wireshark statistics to measure bandwidth usage and traffic distribution. Security management was demonstrated through port scanning with nmap and enforcing access control using Windows Defender Firewall and UFW. Overall, the experiment provided a comprehensive understanding of how FCAPS-based network management tools are applied in real-world systems.