Department of Computer Science and Engineering

Lab9A:Installation and configuration of network traffic analyzer NTOP

Name of student: Shrihari Prashant Joshi
UCID: 2022600019
Branch: AIML Date: 20-04-2024
Sem: 4

Objectives:

1. To generate the traffic from a remote machine and analyse that traffic on the server.
2. To analyse protocol distribution.
3. To get the detailed information about the hosts.

Outcomes:

1. Understanding Network Traffic Monitoring: Students will learn the fundamentals of network traffic monitoring, including the different layers of network protocols and how ntopng utilizes both layer 2 and layer 3 information to provide a comprehensive view of network activity.

2. Utilizing ntopng Features: Participants will gain hands-on experience with ntopng's various features, including its interactive mode for real-time network status display, web mode for generating HTML reports, and its ability to emit and collect NetFlow/sFlow data.

3. Analyzing Network Protocols: Through practical exercises, students will analyze and interpret protocol-wise distribution of traffic, including UDP, TCP, DNS, HTTP, and other protocols, using ntopng's capabilities to gain insights into network usage patterns and potential security risks.

4. Implementing Monitoring Solutions: By working with ntopng's HTTP-based client interface and RRD for persistently storing traffic statistics, participants will learn how to develop custom monitoring applications tailored to specific network monitoring needs, enhancing their skills in network management and optimization.

System Requirements:

1. Computers with Wireshark installed (can be Windows, macOS, or Linux).
2. ntop latest edition

Introduction to ntop:

ntop is the best tool to see network usage in a way similar to what top command does for processes i.e. it is network traffic monitoring software. You can see network status, protocol wise distribution of traffic for UDP, TCP, DNS, HTTP and other protocols.
ntop is a hybrid layer 2 / layer 3 network monitor, that is by default it uses the layer 2 Media Access Control (MAC) addresses AND the layer 3 tcp/ip addresses. ntop is capable of associating the two, so that ip and non-ip traffic (e.g. arp, rarp) are combined for a complete

picture of network activity.
ntop is a network probe that shows interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a Web server, creating a HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, a HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.Network Load Statistics.

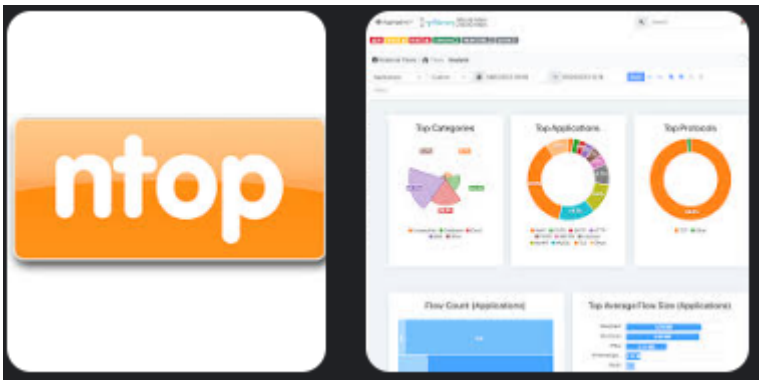


Figure-1: ntop

ntop shows the current network usage. It displays a list of hosts that are currently using the network and reports information concerning the IP (Internet Protocol) and Fibre Channel (FC) traffic generated by each host. The traffic is sorted according to host and protocol. Protocols (user configurable) include:

- TCP/UDP/ICMP
- (R)ARP
- DLC
- IPsec
- Netbios
- TCP/UDP
  - 1. FTP
  - 2. HTTP
  - 3. DNS
  - 4. Telnet
  - 5. SMTP/POP/IMAP
  - 6. SNMP
  - 7. NFS
  - 8. X11
- Fibre Channel
  - 9. Control Traffic - SW2,GS3,ELS
  - 10. SCSI

ntop's author strongly believes in open source software and encourages everyone to modify, improve and extend **ntop** in the interest of the whole Internet community according to the enclosed licence.

Procedure:

Method-1:

Step-1: Check your Ubuntu OS version

$cat /etc/issue

OR

$lsb_release -a

Step-2: Install ntop

For Ubuntu 22.04, refer [1] online

Install Ntopng on Ubuntu 22.04 LTS Jammy Jellyfish

$sudo apt update

$sudo apt upgrade

$sudo apt install gnupg ca-certificates apt-transport-https software-properties-common

Installing Ntopng on Ubuntu 22.04.

$sudo apt install ntopng

Step-3: Configure ntopng

You need to open the Ntopng configuration file with your favorite text editor:

$sudo nano /etc/ntopng.conf

Find the -w directive and uncomment it:

-w=3000

Save and close the file, then restart Ntopng to take change the effect:

$sudo systemctl restart ntopng

Step 4. Configure Firewall.

Ubuntu 22.04 has ufw a firewall running by default. Make sure to open port 3000 for server Ntopng using the following command below:

sudo ufw allow 3000

sudo ufw enable

sudo ufw status

Step 5. Accessing the Ntopng Web Interface.

Once successfully installed, open your web browser and type the URL **https://your-server-ip-address:3000.**

You will be redirected to the Ntopng dashboard interface, The default username, and password as admin/admin:

Method-2:

Step-1. Install ntop under Linux (Ubuntu):

Type the following commands, enter:

$ sudo apt-get update

$ sudo apt-get install ntop

Step-2.Set ntop admin user password

Type the following command to set password, enter:

 # /usr/sbin/ntop -A

OR

$ sudo /usr/sbin/ntop -A

Step-3. Restart ntop service

Type the following command, enter:

 # /etc/init.d/ntop restart

Verify ntop is working, enter:

 # netstat -tulpn | grep :3000

ntop by default use 3000 port to display network usage via webbrowser.

Step-4. View network usage stats:

Type the url:

http://localhost:3000/

OR

http://server-ip:3000/

Method-3:

Using ntop Applications with Docker and OpenStack, refer [3]

Step-1: Install docker and docker-compose

$sudo apt-get install docker.io docker-compose

Step-2: Install it

$sudo docker pull lucaderi/ntopng-docker

Step-3: Run it

$sudo docker run --net=host --name ntopng -t -i lucaderi/ntopng-docker ntopng -v

Questionnaire:

1. How do you track your network usage (network usage monitoring) and protocol wise

distribution of traffic ?

=> To track network usage, network monitoring tools like Wireshark or SolarWinds can be used. These tools capture and analyze network traffic, showing you which protocols are being used and how much data is being transferred. Wireshark can dissect and display traffic by protocol, making it easy to see the distribution of different types of traffic on your network.

2. How do you get a complete picture of network activity?

=> Tools like Wireshark, SNMP (Simple Network Management Protocol), and NetFlow can be used in combination. Wireshark captures and analyzes individual packets, SNMP collects data on network devices and performance, and NetFlow provides flow-based data to show overall traffic patterns.

3. What is traffic load monitoring?

=> Traffic load monitoring is the process of tracking and analyzing the amount of data flowing through a network over a specific period of time. It helps to understand how much network resources are being used at any given moment and can be used to identify potential congestion or performance issues.

Skills:
The skills acquired through this ntopng laboratory session include:
1. Network Traffic Monitoring: Participants develop the ability to monitor and analyze network traffic effectively using ntopng, gaining proficiency in understanding network activity patterns and identifying potential issues.

2. Protocol Analysis: Students learn to interpret and analyze various network protocols, such as UDP, TCP, DNS, and HTTP, enhancing their ability to recognize different types of traffic and their significance.

3. Data Interpretation: Through hands-on experience with ntopng's features, participants develop skills in interpreting and making sense of complex network traffic data, enabling them to extract meaningful insights for decision-making and troubleshooting.

4.Tool Proficiency: By working with ntopng's interactive mode, web mode, and other features, learners gain proficiency in using network monitoring tools, which is essential for network management and optimization tasks in real-world scenarios.

Conclusion: (Write in your own words-two paragraphs)

In conclusion, the utilization of network monitoring tools like Wireshark, and ntopng provides students with a comprehensive understanding of network usage and traffic distribution. By leveraging these tools, students can accurately track the flow of data within a network, identifying the protocols being utilized and the volume of data transferred. This insight is invaluable for network administrators in maintaining network performance and identifying potential bottlenecks or security threats.

Moreover, the acquisition of skills in protocol analysis further enhances students' ability to interpret and dissect network traffic. Through hands-on experience with protocols such as UDP, TCP, DNS, and HTTP, students develop a understanding of different types of network communication and their implications. This proficiency not only aids in troubleshooting network issues but also in optimizing network performance and ensuring the overall security and reliability of the network infrastructure.

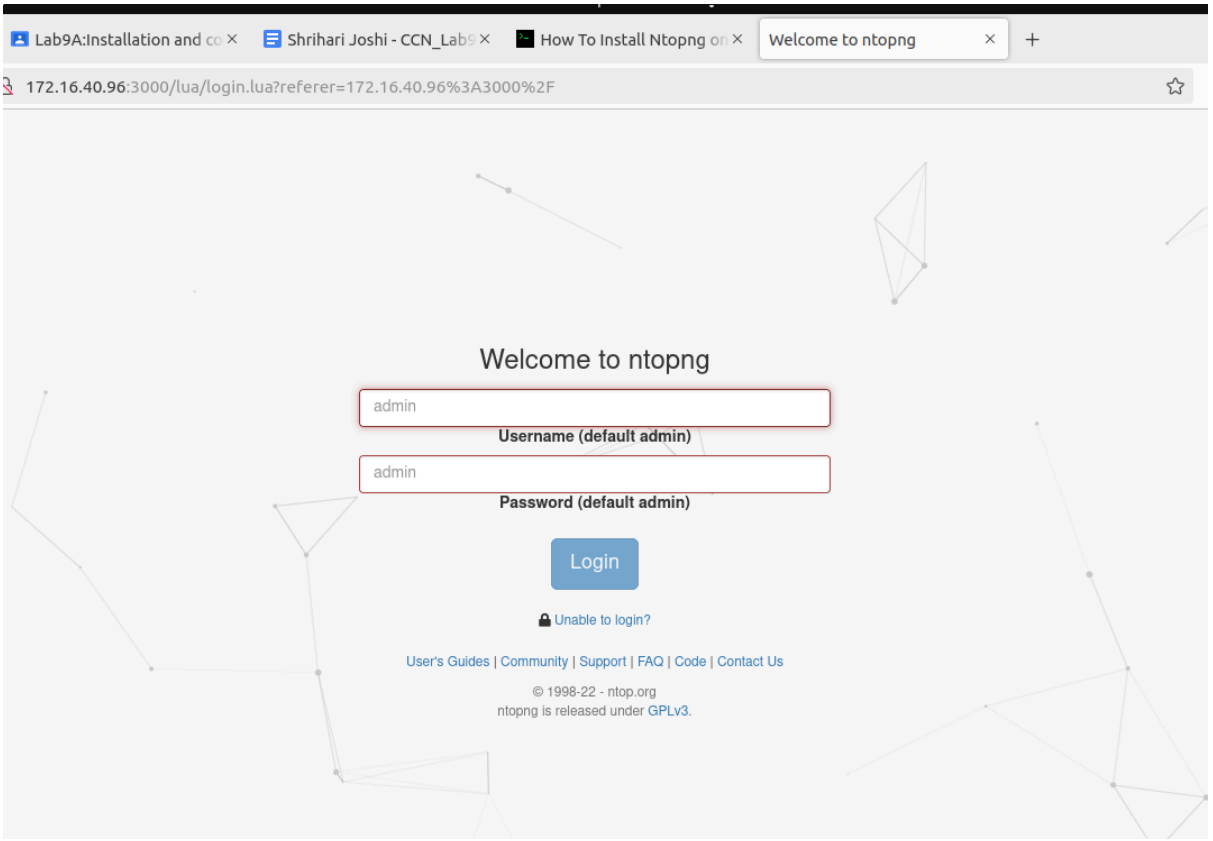
Department of Computer Science and Engineering

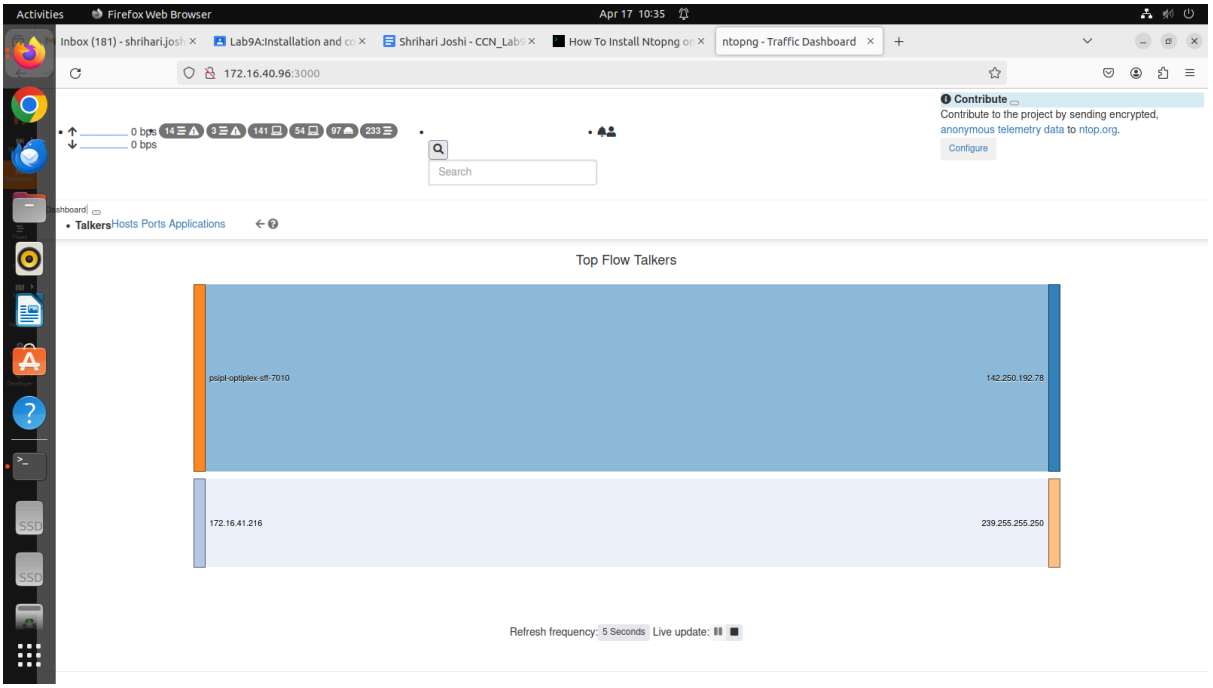
```
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo apt update
[sudo] password for shrihari:
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:4 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:5 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:6 https://packages.microsoft.com/repos/code stable/main amd64 Packages [16.9 kB]
Get:7 https://packages.microsoft.com/repos/code stable/main armhf Packages [17.2 kB]
Get:8 https://packages.microsoft.com/repos/code stable/main arm64 Packages [17.3 kB]
Get:9 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,063 B]
Hit:10 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:11 http://dell.archive.canonical.com jammy InRelease
Hit:12 http://oem.archive.canonical.com jammy InRelease
Hit:13 https://ppa.launchpadcontent.net/ansible/ansible/ubuntu jammy InRelease
Get:14 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [445 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,562 kB]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1,346 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [611 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [298 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [699 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,075 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [237 kB]
Get:22 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [600 kB]
Get:23 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [852 kB]
Fetched 8,013 kB in 12s (653 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
139 packages can be upgraded. Run 'apt list --upgradable' to see them.
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  cifs-utils dmraid gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 kbuild keyutils
  kpartx kpartx-boot libdebian-installer4 libdmraid1.0.0.rc16 libgsoap-2.8.117
  libllvm13 liblzf1 libtimezonemap-data libtimezonemap1 libwpe-1.0-1
  libwpebackend-fdo-1.0-1 linux-headers-oem-22.04c linux-image-oem-22.04c
  module-assistant python3-icu python3-pam rdate user-setup virtualbox-source
Use 'sudo apt autoremove' to remove them.
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libmaven3-core-java node-ip traceroute
Learn more about Ubuntu Pro at https://ubuntu.com/pro
```

```
Memtest86+ needs a 16-bit boot, that is not available on EFI, exiting
Warning: os-prober will be executed to detect other bootable partitions.
Its output will be used to detect bootable binaries on them and create new boot entries.
Found Windows Boot Manager on /dev/nvme0n1p1@/EFI/Microsoft/Boot/bootmgfw.efi
Adding boot menu entry for UEFI Firmware Settings ...
done
Processing triggers for initramfs-tools (0.140ubuntu13.4) ...
update-initramfs: Generating /boot/initrd.img-6.5.0-1019-oem
I: The initramfs will attempt to resume from /dev/nvme0n1p8
I: (UUID=23c6a97e-e306-45af-a360-86cf744a917b)
I: Set the RESUME variable to override this.
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
shrihari@psipl-OptiPlex-SFF-7010:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:74:3e:fc:91  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.40.96  netmask 255.255.255.0  broadcast 172.16.40.255
        inet6 fe80::e76:313c:bf02:7e90  prefixlen 64  scopeid 0x20<link>
        ether cc:96:e5:46:36:6e  txqueuelen 1000  (Ethernet)
        RX packets 10891  bytes 2697227 (2.6 MB)
        RX errors 0  dropped 34  overruns 0  frame 0
        TX packets 3740  bytes 808209 (808.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x70600000-70620000

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 25014  bytes 3242051 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25014  bytes 3242051 (3.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

shrihari@psipl-OptiPlex-SFF-7010:~$ cat /etc/issue
Ubuntu 22.04.4 LTS \n \l

shrihari@psipl-OptiPlex-SFF-7010:~$ sudo apt install gnupg ca-certificates apt-transport-https software-properties-common
[sudo] password for shrihari:
```

```
shrihari@psipl-OptiPlex-SFF-7010:~$ cat /etc/issue
Ubuntu 22.04.4 LTS \n \l

shrihari@psipl-OptiPlex-SFF-7010:~$ sudo apt install gnupg ca-certificates apt-transport-https software-properties-common
[sudo] password for shrihari:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ca-certificates is already the newest version (20230311ubuntu0.22.04.1).
gnupg is already the newest version (2.2.27-3ubuntu2.1).
gnupg set to manually installed.
software-properties-common is already the newest version (0.99.22.9).
apt-transport-https is already the newest version (2.4.12).
The following packages were automatically installed and are no longer required:
  cifs-utils dmraid gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 kbuild keyutils kpartx kpartx-boot libdebian-installer4 libdmraid1.0.0.rc16 libgsoap-2.8.117 libllvm13
  liblzf1 libtimezonemap-data libtimezonemap1 libwpe-1.0-1 libwpebackend-fdo-1.0-1 linux-headers-6.1.0-1035-oem linux-headers-oem-22.04c linux-image-6.1.0-1035-oem
  linux-image-oem-22.04c linux-modules-6.1.0-1035-oem linux-oem-6.1-headers-6.1.0-1035 module-assistant python3-icu python3-pam rdate user-setup virtualbox-source
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo apt install ntopng
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cifs-utils dmraid gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 kbuild keyutils kpartx kpartx-boot libdebian-installer4 libdmraid1.0.0.rc16 libgsoap-2.8.117 libllvm13
  libtimezonemap-data libtimezonemap1 libwpe-1.0-1 libwpebackend-fdo-1.0-1 linux-headers-6.1.0-1035-oem linux-headers-oem-22.04c linux-image-6.1.0-1035-oem
  linux-image-oem-22.04c linux-modules-6.1.0-1035-oem linux-oem-6.1-headers-6.1.0-1035 module-assistant python3-icu python3-pam rdate user-setup virtualbox-source
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  fonts-font-awesome fonts-glyphicons-halflings libdbi1 libhiredis0.14 libjemalloc2 libjs-bootstrap libjs-d3 libjs-jquery-form libjs-jquery-metadata
  libjs-jquery-tablesorter libjs-jquery-ui libjs-rickshaw liblua5.1-0 libmysqlclient21 libndpi4.2 libnorm1 libpgm-5.3-0 librrd8 libzmq5 lua-bitop lua-cjson
  mysql-common node-html5shiv ntopng-data redis-server redis-tools
Suggested packages:
  libjs-jquery-ui-docs ruby-redis
The following NEW packages will be installed:
  fonts-font-awesome fonts-glyphicons-halflings libdbi1 libhiredis0.14 libjemalloc2 libjs-bootstrap libjs-d3 libjs-jquery-form libjs-jquery-metadata
  libjs-jquery-tablesorter libjs-jquery-ui libjs-rickshaw liblua5.1-0 libmysqlclient21 libndpi4.2 libnorm1 libpgm-5.3-0 librrd8 libzmq5 lua-bitop lua-cjson
  mysql-common node-html5shiv ntopng ntopng-data redis-server redis-tools
0 upgraded, 27 newly installed, 0 to remove and 5 not upgraded.
Need to get 16.5 MB of archives.
After this operation, 77.8 MB of additional disk space will be used.
```

```
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo nano /etc/ntopng.conf
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo systemctl restart ntopng
^C
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo systemctl status ntopng
● ntopng.service - ntopng - High-Speed Web-based Traffic Analysis and Flow Collection Tool
     Loaded: loaded (/lib/systemd/system/ntopng.service; enabled; vendor preset: enabled)
     Active: deactivating (stop-sigterm) since Wed 2024-04-17 10:02:48 IST; 1min 20s ago
       Docs: man:ntopng(8)
             file:/usr/share/doc/ntopng/README.Debian
             file:/usr/share/doc/ntopng/UserGuide.pdf.gz
    Process: 52077 ExecStart=/usr/sbin/ntopng /etc/ntopng.conf (code=exited, status=0/SUCCESS)
   Main PID: 52137 (3/flow_checks)
      Tasks: 9 (limit: 18718)
     Memory: 144.3M
        CPU: 1.466s
     CGroup: /system.slice/ntopng.service
             └─52137 /usr/sbin/ntopng /etc/ntopng.conf

Apr 17 10:01:57 psipl-OptiPlex-SFF-7010 systemd[1]: Starting ntopng - High-Speed Web-based Traffic Analysis and Flow Collection Tool...
Apr 17 10:01:57 psipl-OptiPlex-SFF-7010 ntopng[52077]: 17/Apr/2024 10:01:57 [Ntop.cpp:3258] Added Local Network 127.0.0.0/8
Apr 17 10:01:57 psipl-OptiPlex-SFF-7010 ntopng[52077]: 17/Apr/2024 10:01:57 [Ntop.cpp:3258] Added Local Network fe80::/10
Apr 17 10:01:57 psipl-OptiPlex-SFF-7010 ntopng[52077]: 17/Apr/2024 10:01:57 [Redis.cpp:157] Successfully connected to redis 127.0.0.1:6379@0
Apr 17 10:01:57 psipl-OptiPlex-SFF-7010 ntopng[52077]: 17/Apr/2024 10:01:57 [Redis.cpp:157] Successfully connected to redis 127.0.0.1:6379@0
Apr 17 10:01:58 psipl-OptiPlex-SFF-7010 ntopng[52077]: 17/Apr/2024 10:01:58 [NetworkInterface.cpp:3226] Cleanup interface dummy
Apr 17 10:01:58 psipl-OptiPlex-SFF-7010 ntopng[52077]: 17/Apr/2024 10:01:58 [Ntop.cpp:2365] Parent process is exiting (this is normal)
Apr 17 10:01:58 psipl-OptiPlex-SFF-7010 systemd[1]: Started ntopng - High-Speed Web-based Traffic Analysis and Flow Collection Tool.
Apr 17 10:02:48 psipl-OptiPlex-SFF-7010 systemd[1]: Stopping ntopng - High-Speed Web-based Traffic Analysis and Flow Collection Tool...
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo systemctl stop ntopng
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo systemctl start ntopng
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo ufw allow 3000
Rules updated
Rules updated (v6)
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo ufw enable
Firewall is active and enabled on system startup
shrihari@psipl-OptiPlex-SFF-7010:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
3000                       ALLOW       Anywhere
3000 (v6)                  ALLOW       Anywhere (v6)

shrihari@psipl-OptiPlex-SFF-7010:~$ ifconfig
```





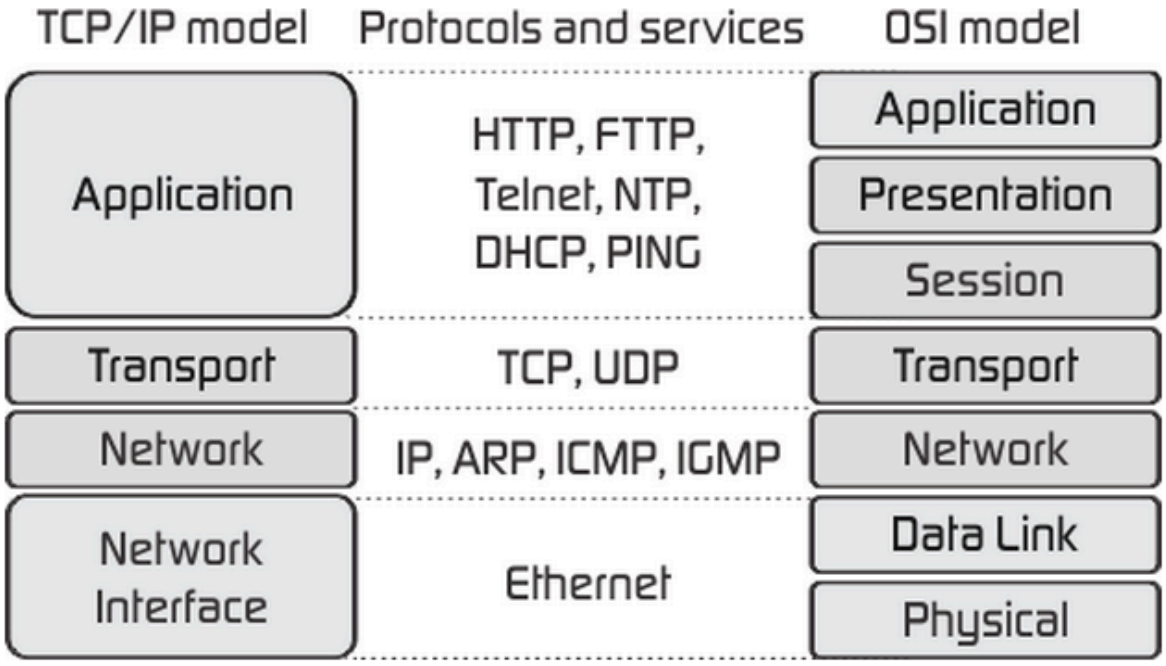
References:

[1]How To Install Ntopng on Ubuntu 22.04 LTS by r00t
https://idroot.us/install-ntopng-ubuntu-22-04/

[2] ntopng official document
https://www.ntop.org/guides/ntopng/

[3] Using ntop Applications with Docker and OpenStack
https://www.ntop.org/ntopng/using-ntop-applications-with-docker-and-openstack/

TCP/IP Fundamentals:
Transmission Control Protocol/Internet Protocol (TCP/IP) is the foundational suite of protocols that governs communication on the internet and most local area networks. Here are the fundamental aspects of TCP/IP:



Source: Google image

Overview:
TCP/IP is a suite of communication protocols that allows computers to communicate over networks. It provides the foundation for the internet and is widely used for local network communication.
Protocols:
Transmission Control Protocol (TCP): Ensures reliable, ordered, and error-checked delivery of data between applications.
Internet Protocol (IP): Handles the addressing and routing of data packets so they can travel across networks and arrive at the correct destination.
Layered Architecture:
TCP/IP follows a layered architecture, with four main layers: Link, Internet, Transport, and Application. Each layer has specific responsibilities, and data is passed down through the layers for processing.

Addressing:
IP addresses are used to uniquely identify devices on a network. IPv4 (32-bit address) and IPv6 (128-bit address) are the two versions of IP addresses. IPv6 is gradually being adopted to address the limitations of IPv4.

Subnetting:
Subnetting is the process of dividing a larger IP network into smaller sub-networks to improve performance and security. It involves creating subnets with their own unique IP address ranges.

Routing:
Routers use IP addresses to determine the best path for data packets to travel from the source to the destination across multiple networks. Routing protocols, such as RIP, OSPF, and BGP, facilitate this process.

Transport Layer:
The Transport layer is responsible for end-to-end communication between devices. TCP provides reliable, connection-oriented communication, while UDP (User Datagram Protocol) offers faster, connectionless communication.

Application Layer:
The top layer in the TCP/IP model, the Application layer, includes various protocols for specific applications and services. Common protocols include HTTP for web browsing, FTP for file transfer, SMTP for email, and DNS for domain name resolution.
DNS (Domain Name System):
DNS translates human-readable domain names into IP addresses. It is crucial for locating resources on the internet using familiar names rather than numerical IP addresses.

DHCP (Dynamic Host Configuration Protocol):
DHCP automates the assignment of IP addresses and related network configuration information to devices on a network. It simplifies network administration by dynamically managing IP addresses.

TCP/IP Tools:
Tools like Ping (to test connectivity), Traceroute (to trace the route packets take), and Netstat (to display network connections and statistics) are commonly used for troubleshooting and diagnostics.