Using tcpdump for Network Monitoring

Introduction to tcpdump

tcpdump is a command-line utility that allows you to capture and analyze network packets. It is widely used for network troubleshooting and security monitoring.

Installing tcpdump

On Ubuntu, install tcpdump with the following command:

```
sudo apt install tcpdump
```

Basic Command Structure

The basic syntax for tcpdump:

```
sudo tcpdump [options] [filter-expression]
```

Capturing Packets

To start capturing packets on a specific interface:

```
sudo tcpdump -i eth0
```

Replace `eth0` with the appropriate network interface.

Writing Captures to a File

To save captured packets to a file:

```
sudo tcpdump -i eth0 -w capture_file.pcap
```

Reading from a Capture File

To read packets from a saved file:

```
tcpdump -r capture_file.pcap
```

Filtering Traffic

Examples of common filters:

- Capture only TCP traffic:

```
sudo tcpdump tcp
```

- Capture traffic on a specific port:

```
sudo tcpdump port 80
```

- Capture traffic from or to a specific IP:

```
sudo tcpdump host 192.168.1.1
```

Combining Filters

Combine multiple filters to refine results:

```
sudo tcpdump 'tcp port 80 and src host 192.168.1.1'
```