

```
comp@comp:~$ sudo apt install nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 libssh2-1t64 nmap nmap-common
0 upgraded, 5 newly installed, 0 to remove and 195 not upgraded.
Need to get 6,286 kB of archives.
After this operation, 27.4 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3.12.0-3build1.1 [238 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.0+dfsg-5build1 [42.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0-4.1build2 [120 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-3build2 [4,192 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-3build2 [1,694 kB]
Fetched 6,286 kB in 10s (641 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 220430 files and directories currently installed.)
Preparing to unpack .../libblas3_3.12.0-3build1.1_amd64.deb ...

```

```
comp@comp:~$ nmap -sn 192.168.5.101/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 10:54 IST
Nmap scan report for _gateway (192.168.5.1)
Host is up (0.00079s latency).
Nmap scan report for 192.168.5.2
Host is up (0.0087s latency).
Nmap scan report for 192.168.5.3
Host is up (0.0078s latency).
Nmap scan report for 192.168.5.4
Host is up (0.0097s latency).
Nmap scan report for 192.168.5.5
Host is up (0.0097s latency).
Nmap scan report for 192.168.5.6
Host is up (0.024s latency).
Nmap scan report for 192.168.5.24
Host is up (0.0012s latency).
Nmap scan report for 192.168.5.25
Host is up (0.0019s latency).
Nmap scan report for 192.168.5.26
Host is up (0.0014s latency).
Nmap scan report for 192.168.5.27
Host is up (0.00078s latency).
Nmap scan report for 192.168.5.28
Host is up (0.0011s latency).
Nmap scan report for 192.168.5.29
Host is up (0.0012s latency).
Nmap scan report for 192.168.5.30
```

```
comp@comp:~$ sudo nmap -sS -sV -T4 192.168.5.2
```

Starting Nmap 7.94SVN (https://nmap.org) at 2025-08-11 11:03 IST

Nmap scan report for 192.168.5.2

Host is up (0.0011s latency).

All 1000 scanned ports on 192.168.5.2 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 04:DA:D2:11:E3:AA (Cisco Systems)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds

```
comp@comp:~$ sudo apt install mrtg snmp snmpd -y
```

```
comp@comp:~$ nmap -oX scan_results.xml 192.168.5.101/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:08 IST

comp@comp:~$ nmap -T4 -oX scan_results.xml 192.168.5.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:10 IST

comp@comp:~$ nmap -T4 -oX scan_results.xml 192.168.5.1-50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:12 IST

comp@comp:~$ nmap -v -T4 -oX scan_results.xml 192.168.5.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:13 IST
Initiating Ping Scan at 11:13
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 11:13, 1.90s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 69 hosts. at 11:13
Completed Parallel DNS resolution of 69 hosts. at 11:13, 0.07s elapsed
Nmap scan report for 192.168.5.0 [host down]
Nmap scan report for 192.168.5.2 [host down]
Nmap scan report for 192.168.5.3 [host down]
Nmap scan report for 192.168.5.4 [host down]
Nmap scan report for 192.168.5.5 [host down]
Nmap scan report for 192.168.5.6 [host down]
Nmap scan report for 192.168.5.7 [host down]
Nmap scan report for 192.168.5.8 [host down]
Nmap scan report for 192.168.5.9 [host down]
Nmap scan report for 192.168.5.10 [host down]
Nmap scan report for 192.168.5.11 [host down]
Nmap scan report for 192.168.5.12 [host down]
Nmap scan report for 192.168.5.13 [host down]
Nmap scan report for 192.168.5.14 [host down]
Nmap scan report for 192.168.5.15 [host down]
Nmap scan report for 192.168.5.16 [host down]
Nmap scan report for 192.168.5.17 [host down]
Nmap scan report for 192.168.5.18 [host down]
Nmap scan report for 192.168.5.19 [host down]
Nmap scan report for 192.168.5.20 [host down]
```

```
Nmap scan report for 192.168.5.27
Host is up (0.00056s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap scan report for 192.168.5.28
Host is up (0.00064s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap scan report for 192.168.5.29
Host is up (0.00079s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap scan report for 192.168.5.30
Host is up (0.00061s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap scan report for 192.168.5.33
Host is up (0.00078s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
```

```
comp@comp:~$ nmap -p 22,80,443 192.168.5.101
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:15 IST
```

```
Nmap scan report for comp (192.168.5.101)
```

```
Host is up (0.000067s latency).
```

```
PORT      STATE SERVICE
```

```
22/tcp    closed ssh
```

```
80/tcp    open  http
```

```
443/tcp   closed https
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

```
comp@comp:~$ nmap -sV 192.168.5.101
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:15 IST
```

```
Nmap scan report for comp (192.168.5.101)
```

```
Host is up (0.00011s latency).
```

```
Not shown: 999 closed tcp ports (conn-refused)
```

```
PORT      STATE SERVICE VERSION
```

```
80/tcp    open  http    Apache httpd/2.4.58 ((Ubuntu))
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

```
comp@comp:~$ sudo nmap -sV --script=vuln 192.168.5.101
[sudo] password for comp:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:18 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for comp (192.168.5.101)
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
| http-enum:
|_ /server-status/: Potentially interesting folder
| vulners:
| cpe:/a:apache:http_server:2.4.58:
|   95499236-C9FE-56A6-9D7D-E943A24B633A      10.0      https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT
*   2C119FFA-ECE0-5E14-A4A4-354A2C38071A      10.0      https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT
*   CVE-2024-38476  9.8      https://vulners.com/cve/CVE-2024-38476
```

```
--snpd:  publicc@192.168.5.101: -> Z -> trspeed = 1000000000
comp@comp:~$ sudo mrtg /etc/mrtg.cfg
-----
ERROR: Mrtg will most likely not work properly when the environment
variable LANG is set to UTF-8. Please run mrtg in an environment
where this is not the case. Try the following command to start:

env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
-----
comp@comp:~$ sudo env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
2025-08-11 11:35:20, Rateup WARNING: /usr/bin/rateup could not read the primary log file for 192.168.5.101_eno1
2025-08-11 11:35:20, Rateup WARNING: /usr/bin/rateup The backup log file for 192.168.5.101_eno1 was invalid as well
2025-08-11 11:35:20, Rateup WARNING: /usr/bin/rateup Can't rename 192.168.5.101_eno1.log to 192.168.5.101_eno1.old updating log file
comp@comp:~$ sudo env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
sudo env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
comp@comp:~$ sudo mkdir -p /var/log/mrtg
sudo chown -R www-data:www-data /var/log/mrtg
comp@comp:~$ sudo indexmaker /etc/mrtg.cfg > /var/www/html/mrtg/index.html
bash: /var/www/html/mrtg/index.html: Permission denied
comp@comp:~$ sudo bash -c 'indexmaker /etc/mrtg.cfg > /var/www/html/mrtg/index.html'
comp@comp:~$ sudo mkdir -p /var/www/html/mrtg
comp@comp:~$ sudo mkdir -p /var/www/html/mrtg
sudo bash -c 'indexmaker /etc/mrtg.cfg > /var/www/html/mrtg/index.html'
comp@comp:~$
```



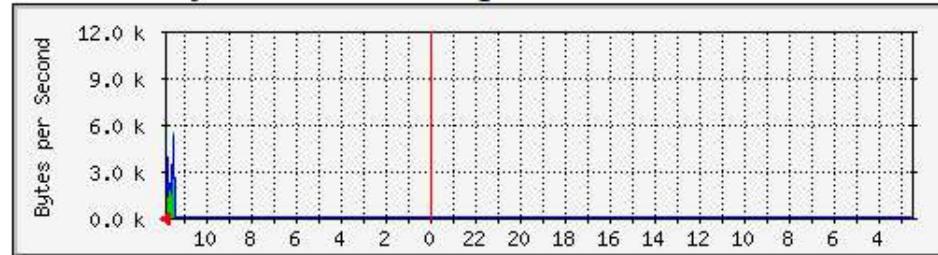
Not Secure

http://192.168.5.99/mrtg/index.html



MRTG Index Page

Traffic Analysis for eno1 -- comp



MRTG MULTI ROUTER TRAFFIC GRAPHER

version
2.17.10

Tobias Oetiker <tobi@oetiker.ch>
and Dave Rand <d1r@bungi.com>