

Autor: [Pedro Daniel Gonçalves Antunes]

Data: [2025/03/27]

Curso/Disciplina: [LSIRC/PPR]

Instituição: [ESTG]

NIM:[8230068]

Ficha:[Ficha Prática 4]

1. Objetivo

O objetivo deste trabalho foi instalar e configurar ferramentas de análise de tráfego em ambiente de rede simulada (GNS3), utilizando os serviços `ntopng` e `Ganglia`, com foco na monitorização de protocolos e fluxos entre dispositivos.

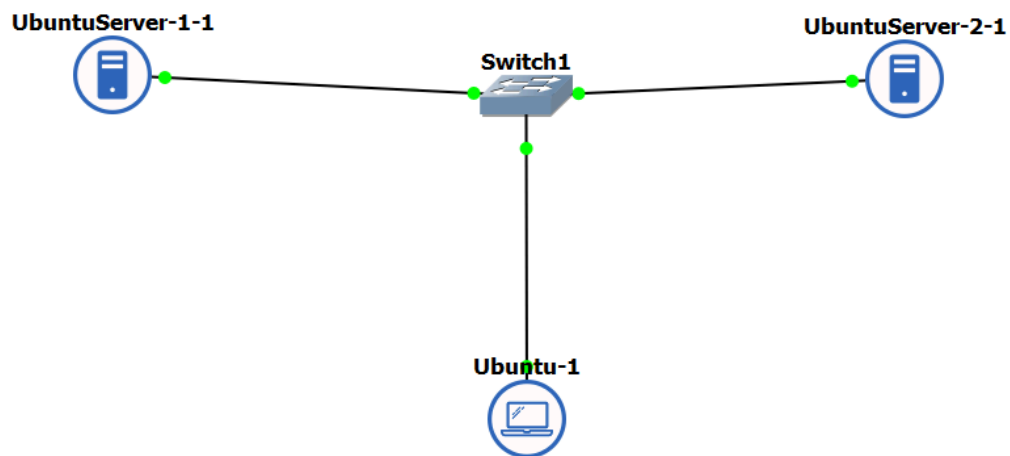
2. Topologia da Rede

A topologia da rede foi composta por:

- 1x **Ubuntu Desktop** (Laptop-PT 3) – com `ntopng` e

tentativa de Ganglia

- 2x **Ubuntu Server** (Server-PT 1 e Server-PT 2) – com serviços instalados
- Todos ligados a um switch virtual no GNS3, em rede 192.168.1.0/24



3. Configuração da Rede

Cada máquina recebeu um IP fixo:

Equipamento	IP	SO
Laptop-PT 3	192.168.1.10	Ubuntu Desktop
Server-PT 1	192.168.1.11	Ubuntu Server
Server-PT 2	192.168.1.12	Ubuntu Server

As interfaces foram configuradas manualmente com Netplan.

UbuntuServer1

```
GNU nano 7.2
network:
  version: 2
  ethernet:
    enp0s3:
      addresses:
        - 192.168.1.11/24
      dhcp4: no
```

UbuntuServer2

```
GNU nano 7.2
network:
  version: 2
  ethernet:
    enp0s3:
      addresses:
        - 192.168.1.12/24
      dhcp4: no
```

Ubuntu Desktop

```
vboxuser@Ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7d:67:fe brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
```

4. Serviços Instalados

Nos servidores:

- Apache2 (HTTP)
- OpenSSH (SSH)
- Samba (Partilhas de rede)

No Desktop:

- `ntopng`
 - `redis-server`
-

5. Testes Realizados

Tráfego foi gerado de forma realista através de comandos:

```
curl http://192.168.1.11
ssh usuario@192.168.1.12
ping 192.168.1.11
smbclient -L //192.168.1.12
```

6. Resultados - ntopng

A interface web do ntopng permitiu visualizar:

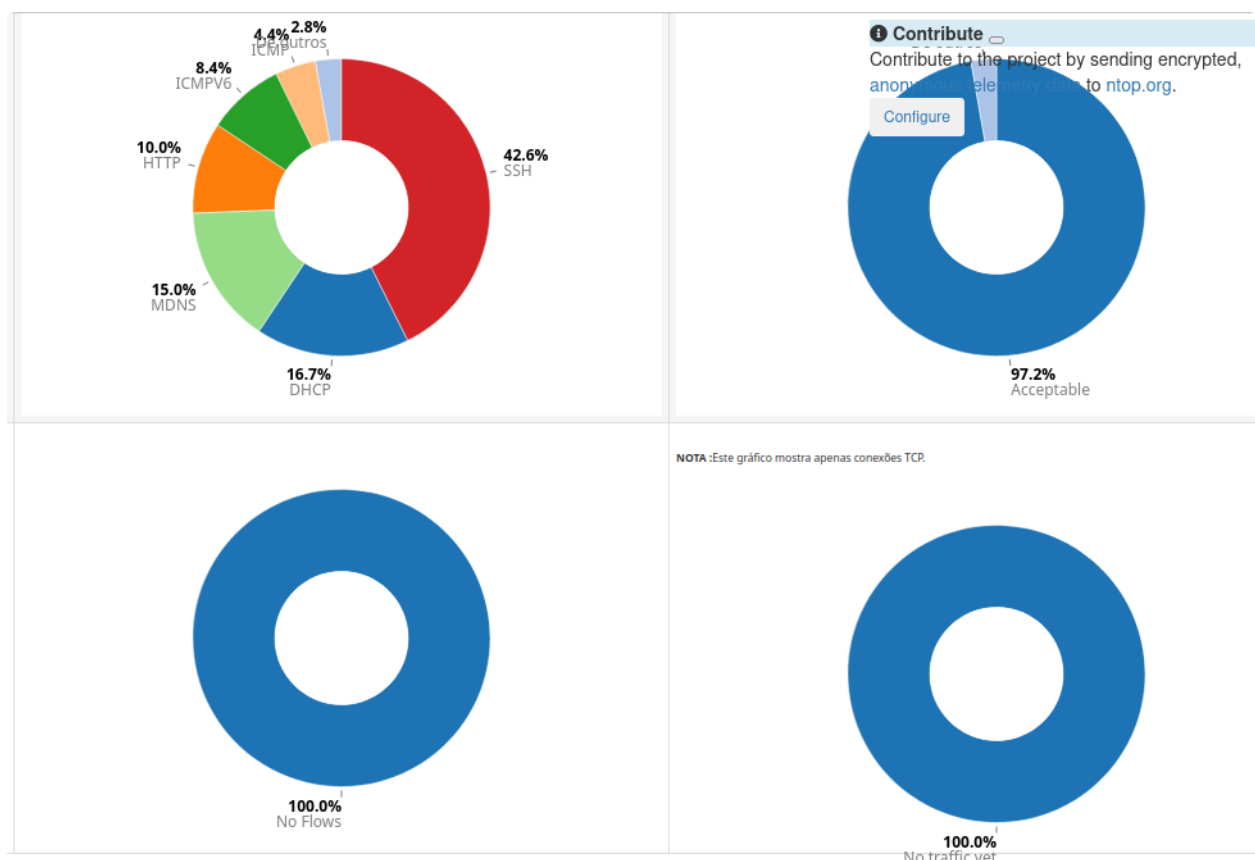
- **Protocolos identificados:** SSH, HTTP, DHCP, ICMP, ARP, mDNS, etc.

- **Gráficos de distribuição de tráfego** (local → remoto, protocolos, flows)
- **Top Talkers:** Mostra quem está a comunicar com quem

Através do painel `http://localhost:3000`, foi possível observar:

Protocolos Detetados:

- SSH: 42.6%
- HTTP: 10%
- DHCP: 16.7%
- mDNS: 15%
- ICMPv6: 8.4%
- Outros: TELNET, ARP, etc.

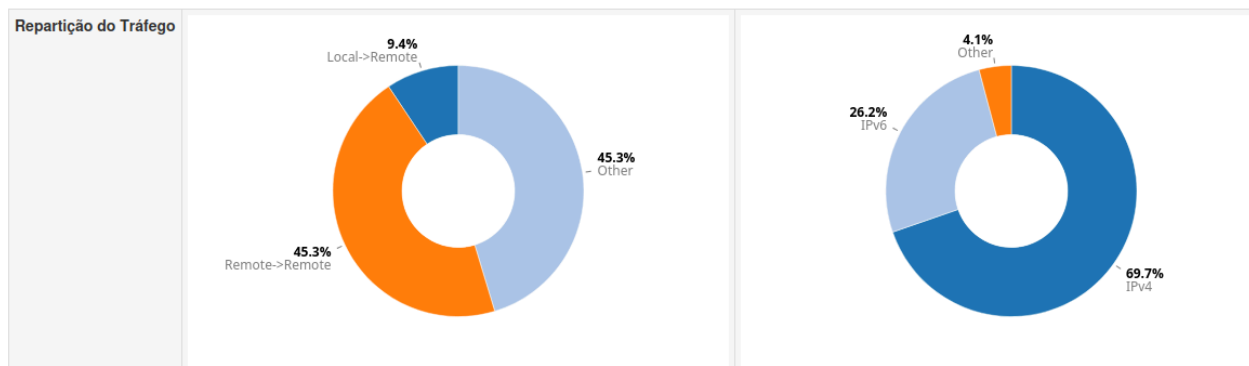


Tráfego captado:

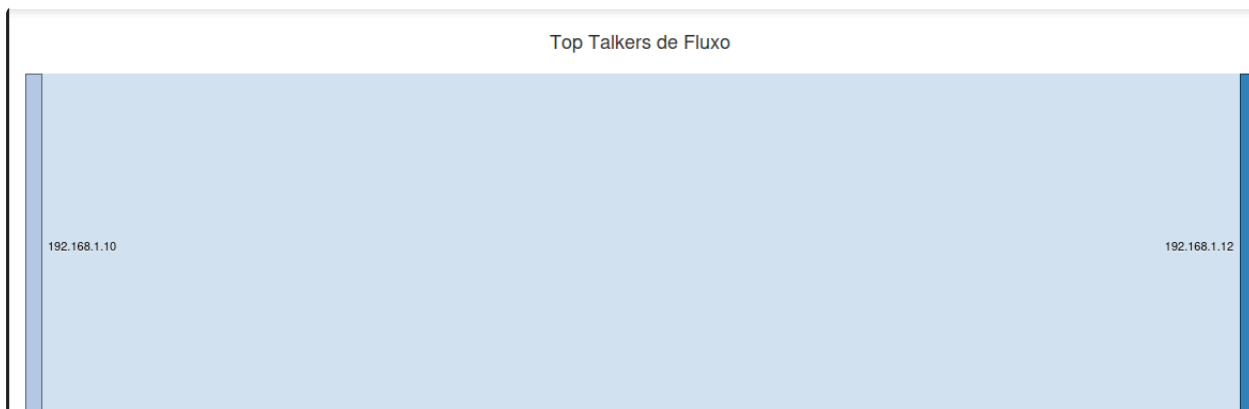
- Packets enviados: 82
- Packets recebidos: 5
- Tráfego total: ~14 KB









Prints tirados

nome	enp0s3 [08:00:27:7D:67:FE]	Familia	Contribute Contribute to the project by sending encrypted, anonymous telemetry data to ntop.org. 1 Click Configure
MTU	1518 Bytes	Rapidez	
Alertas Envolvidos	3	Dropped Alerts	



Estatísticas de tráfego				
Traffic Anomalies	Local Hosts Anomalies	0	Remote Hosts Anomalies	0
Tráfego total	14.3 KB [87 Pkts]	Pacotes Soltos	0 Pkts	
Tráfego enviado	12.9 KB [82 Pkts]	Tráfego recebido	1.4 KB [5 Pkts]	Enviar
Baixar	1 min	pcap baixar		



Aplicação	Total (Desde a inicialização)	Percentagem	Configure
ARP	1.41 KB	<div><div></div></div>	9.8 %
DHCP 	20.29 KB	<div><div></div></div>	141.5 %
HTTP 	12.1 KB	<div><div></div></div>	84.3 %
ICMP 	5.36 KB	<div><div></div></div>	37.4 %
ICMPV6 	10.18 KB	<div><div></div></div>	71.0 %
IGMP 	108 Bytes	<div><div></div></div>	0.7 %
MDNS 	18.21 KB	<div><div></div></div>	126.9 %
SSH 	51.75 KB	<div><div></div></div>	360.7 %
Unknown 	1.93 KB	<div><div></div></div>	13.5 %

Nota sobre Ganglia

Foi tentada a instalação e configuração do Ganglia, mas a interface web apresentou erros devido a incompatibilidade com o PHP 8+.

Apesar da configuração dos agentes (`ganglia-monitor`) nos servidores, não foi possível validar os dados pela interface. A análise foi concluída apenas com `ntopng` .

#7 Conclusão

Através da ferramenta `ntopng` , foi possível analisar o tráfego de rede de forma eficaz. A aplicação permitiu identificar os principais protocolos usados, visualizar fluxos de dados entre os dispositivos e confirmar a funcionalidade dos serviços instalados.

A atividade cumpriu os objetivos propostos, apesar das limitações encontradas com a ferramenta Gangleia.