Trabalho Laboratorial 2

Planeamento e Gestão de Redes

Sala I321 Bancada 1

Diogo Remião & Miguel Pinheiro

Faculdade de Engenharia da Universidade do Porto
TEC

Contents

1 Introdução

Este trabalho tem como objetivo o aprofundamento dos nossos conhecimentos com ferramentas de monitorização de tráfego. As ferramentas a serem utilizadas neste trabalho são o **MRTG** e o **NTOP**. Estas duas ferramentas apresentam abordagens diferentes e trazem diferentes considerações na sua configuração. No final deste trabalho esperamos estar mais capacitados para usar estas ferramentas, assim como perceber o funcionamento da rede e do tráfego.

2 Setup

2.1 Web Server

A configuração do web server foi similar à do projecto anterior. Foi utilizado o **Apache** para dar host a um site nas porta 80 (default http) e 81. Como isto já foi analisado no trabalho anterior. não será apresentada uma análise profunda da sua configuração [1].

2.2 FTP server

A ferramenta selecionada para criar um servidor FTP foi o **Vsftpd**. Seguindo o guia de instalação [2], definimos um *username* (testuser), com uma *password*, que corresponde ao *login* para aceder ao servidor. O diretório predefinido num acesso FTP é `\home\testuser`. Para efeitos de teste, colocamos nesse diretório um ficheiro *test.txt*. De seguida, através do Firefox, onde já tínhamos o proxy configurado (Lab1), acedemos ao servidor através do endereço *ftp://172.16.1.12*, sendo que depois do login com as credenciais definidas, foi-nos possível aceder ao ficheiro. Para fazer acessos FTP dos próprios *tux*s, foi criado um script que ao ser executado, faz download do ficheiro *test.txt* presente no diretório:

```
#!/bin/sh
HOST='172.16.1.12'
USER='testuser'
PASSWD='testuser'
FILE='test'

ftp -n $HOST <<END_SCRIPT
quote USER $USER
quote PASS $PASSWD
get $file
quit
END_SCRIPT
exit 0
```

2.3 NTP Server

O serviço requere duas componentes: um servidor e um cliente. O servidor NTP irá estar sincronizado com os servidores a nível internacional, e o cliente com o

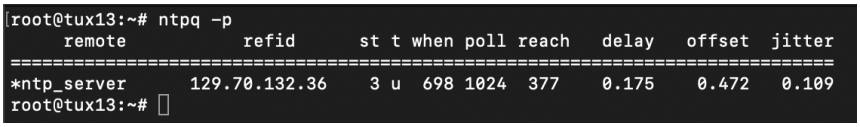


Figure 2.1: Servidor NTP do cliente

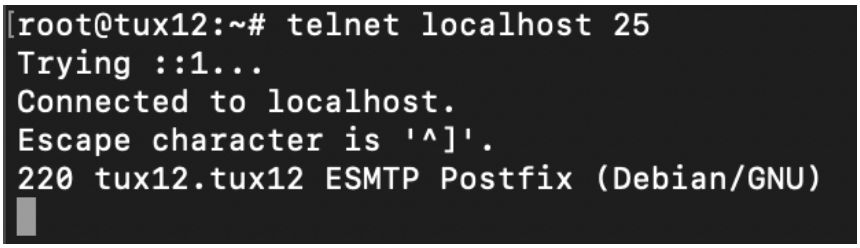


Figure 2.2: Teste telnet na porta 25

servidor NTP. Durante a configuração do NTP server [3], definimos no ficheiro de configuração com 3 servidores internacionais para sincronização, indicados em *https://support.ntp.org/bin/view/Servers/NTPPoolServers*.

Neste caso, os servidores indicados para a região de Portugal são:

- server 1.pt.pool.ntp.org
- server 0.europe.pool.ntp.org
- server 1.europe.pool.ntp.org

No cliente, no ficheiro `\etc\hosts` colocamos o IP do servidor NTP de modo a que o nome depois seja resolvido. No ficheiro de configuração do NTP, adicionamos apenas o server *NTP-server-host prefer iburst*. A sincronização desta máquina será agora feita pelo servidor NTP.

Correr o comando *ntpq -p* comprova o correto funcionamento do serviço (Fig 2.1).

2.4 Email Server

Para criar um servidor email utilizamos o **Postfix**. Esta ferramenta é o MTA (Mail Transfer Agent) predefinido do Ubuntu e a sua instalação é simples [4]. Os endereços de mail gerados pelo Postfix são *user@tux99.netlab.fe.up.pt*, onde o *user* é "netlab" e o *tux99* o "hostname" do computador.

Após a instalação do Postfix, fizemos um teste na porta 25 onde o serviço de email opera. Observamos a resposta do serviço ESMTP Postfix, garantindo que a instalação tinha sido bem sucedida (Fig 2.2).

```
root@tux12:~# mail -s "hello from tux12" netedu@tux13.netlab.fe.up.pt
Cc:
Hello World!
root@tux12:~#
```

Figure 2.3: Email enviado do tux12

```
From root@tux12  Sun Mar 28 00:33:26 2021
Return-Path: <root@tux12>
X-Original-To: netedu@tux13.netlab.fe.up.pt
Delivered-To: netedu@tux13.netlab.fe.up.pt
Received: from tux12.tux12 (ntp_server [172.16.1.12])
        by tux13.netlab.fe.up.pt (Postfix) with ESMTP id 264E512143A
        for <netedu@tux13.netlab.fe.up.pt>; Sun, 28 Mar 2021 00:33:26 +0000 (WE$
Received: by tux12.tux12 (Postfix, from userid 0)
        id 0D2361216DC; Sun, 28 Mar 2021 00:33:26 +0000 (WET)
Subject: hello from tux12
To: <netedu@tux13.netlab.fe.up.pt>
X-Mailer: mail (GNU Mailutils 3.5)
Message-Id: <20210328003326.0D2361216DC@tux12.tux12>
Date: Sun, 28 Mar 2021 00:33:26 +0000 (WET)
From: root <root@tux12>

Hello World!
```

Figure 2.4: Log do email recebido no tux13

Para verificar o funcionamento do serviço, enviamos emails dentro da rede local para o *tux13*, onde o Postfix também tinha sido configurado (Fig 2.3). Verificamos o ficheiro `\var\log\mail.log` para ver se o email tinha sido enviado com sucesso. De seguida fomos ao *tux13*, onde no ficheiro `\var\spool\mail\netedu` podemos ler o email que foi recebido ((Fig 2.4).) Desta modo, ficou garantido o funcionamento do servidor de email na rede local.

2.5 DNS Cache Server

Um servidor DNS tem como função traduzir nomes em Ip's. A funcionalidade de cache permite que essa informação possa ser guardada localmente. Desde modo, quando escrevemos um endereço, em vez de acedermos aos DNS servers do nosso ISP, temos essa informação guardada localmente, o que permite uma *query* mais rápida.

O software utilizado foi o **Bind9**, predefinido do Ubuntu [5]. Durante a configuração, foram adicionados os DNS servers do nosso ISP. Procedemos à configuração quer da *Forward Zone File* e do *Reverse Zone File*. Para testar o serviço, fez-se uso do comando `dig @localhost google.com` (Fig 2.5a).

Como se pode observar ao correr o comando a segunda vez, o query time é de 0 ms, dado que a informação ficou guardada em cache (Fig 2.5b). Passado um período de tempo predefinido no sistema, esta cache é limpa e um novo query é efetuado ao servidor DNS do ISP.

```
;; ANSWER SECTION:
google.com.             220     IN      A       142.250.184.14

;; AUTHORITY SECTION:
.                       351753  IN      NS      b.root-servers.net.
.                       351753  IN      NS      i.root-servers.net.
.                       351753  IN      NS      j.root-servers.net.
.                       351753  IN      NS      c.root-servers.net.
.                       351753  IN      NS      k.root-servers.net.
.                       351753  IN      NS      f.root-servers.net.
.                       351753  IN      NS      m.root-servers.net.
.                       351753  IN      NS      a.root-servers.net.
.                       351753  IN      NS      d.root-servers.net.
.                       351753  IN      NS      h.root-servers.net.
.                       351753  IN      NS      l.root-servers.net.
.                       351753  IN      NS      e.root-servers.net.
.                       351753  IN      NS      g.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     90156   IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3716    IN      AAAA    2001:500:200::b
c.root-servers.net.     3716    IN      AAAA    2001:500:2::c
d.root-servers.net.     90156   IN      AAAA    2001:500:2d::d
e.root-servers.net.     3716    IN      AAAA    2001:500:a8::e
f.root-servers.net.     90156   IN      AAAA    2001:500:2f::f
g.root-servers.net.     3716    IN      AAAA    2001:500:12::d0d
h.root-servers.net.     90156   IN      AAAA    2001:500:1::53
i.root-servers.net.     90156   IN      AAAA    2001:7fe::53
j.root-servers.net.     90156   IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     90156   IN      AAAA    2001:7fd::1
l.root-servers.net.     90156   IN      AAAA    2001:500:9f::42
m.root-servers.net.     90156   IN      AAAA    2001:dc3::35
a.root-servers.net.     4693    IN      A       198.41.0.4
b.root-servers.net.     90156   IN      A       199.9.14.201
c.root-servers.net.     90156   IN      A       192.33.4.12
d.root-servers.net.     90156   IN      A       199.7.91.13
e.root-servers.net.     90156   IN      A       192.203.230.10
f.root-servers.net.     90156   IN      A       192.5.5.241
g.root-servers.net.     90156   IN      A       192.112.36.4
h.root-servers.net.     90156   IN      A       198.97.190.53
i.root-servers.net.     90156   IN      A       192.36.148.17
j.root-servers.net.     90156   IN      A       192.58.128.30
k.root-servers.net.     90156   IN      A       193.0.14.129
l.root-servers.net.     90156   IN      A       199.7.83.42
m.root-servers.net.     90156   IN      A       202.12.27.33

;; Query time: 2 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun Mar 28 23:11:04 WEST 2021
;; MSG SIZE  rcvd: 866
```

(a) Primeiro DNS query a google.com

```
;; ANSWER SECTION:
google.com.             197     IN      A       142.250.184.14

;; AUTHORITY SECTION:
.                       351730  IN      NS      a.root-servers.net.
.                       351730  IN      NS      e.root-servers.net.
.                       351730  IN      NS      d.root-servers.net.
.                       351730  IN      NS      g.root-servers.net.
.                       351730  IN      NS      i.root-servers.net.
.                       351730  IN      NS      k.root-servers.net.
.                       351730  IN      NS      j.root-servers.net.
.                       351730  IN      NS      f.root-servers.net.
.                       351730  IN      NS      c.root-servers.net.
.                       351730  IN      NS      m.root-servers.net.
.                       351730  IN      NS      h.root-servers.net.
.                       351730  IN      NS      l.root-servers.net.
.                       351730  IN      NS      b.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     90133   IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3693    IN      AAAA    2001:500:200::b
c.root-servers.net.     3693    IN      AAAA    2001:500:2::c
d.root-servers.net.     90133   IN      AAAA    2001:500:2d::d
e.root-servers.net.     3693    IN      AAAA    2001:500:a8::e
f.root-servers.net.     90133   IN      AAAA    2001:500:2f::f
g.root-servers.net.     3693    IN      AAAA    2001:500:12::d0d
h.root-servers.net.     90133   IN      AAAA    2001:500:1::53
i.root-servers.net.     90133   IN      AAAA    2001:7fe::53
j.root-servers.net.     90133   IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     90133   IN      AAAA    2001:7fd::1
l.root-servers.net.     90133   IN      AAAA    2001:500:9f::42
m.root-servers.net.     90133   IN      AAAA    2001:dc3::35
a.root-servers.net.     4670    IN      A       198.41.0.4
b.root-servers.net.     90133   IN      A       199.9.14.201
c.root-servers.net.     90133   IN      A       192.33.4.12
d.root-servers.net.     90133   IN      A       199.7.91.13
e.root-servers.net.     90133   IN      A       192.203.230.10
f.root-servers.net.     90133   IN      A       192.5.5.241
g.root-servers.net.     90133   IN      A       192.112.36.4
h.root-servers.net.     90133   IN      A       198.97.190.53
i.root-servers.net.     90133   IN      A       192.36.148.17
j.root-servers.net.     90133   IN      A       192.58.128.30
k.root-servers.net.     90133   IN      A       193.0.14.129
l.root-servers.net.     90133   IN      A       199.7.83.42
m.root-servers.net.     90133   IN      A       202.12.27.33

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun Mar 28 23:11:27 WEST 2021
;; MSG SIZE  rcvd: 866
```

(b) Segunda DNS query a google.com

Figure 2.5: Dns Queries

3 Test Environment

Neste capítulo será abordada a configuração utilizada na implementação das ferramentas, assim como os procedimentos para os testar.

3.1 Proxy

Tal como no projeto anterior, o servidor de bancada funcionou como um proxy, de mode a que remotamente se tivesse acessos aos *tux*s, nomeadamente aos sites gerados pelo **MRTG** e **NTOP**. Esta configuração não será abordada neste relatório, dado que foi analisada no relatório anterior.

3.2 Serviços

Todos os serviços (Webmail, FTP, etc.) foram instalados no **tux12**. Note-se que no caso do NTP, foi preciso também instalar um cliente no **tux13**. O mesmo se verifica no caso do Webmail, sendo que foi necessário a cooperação com colegas da sala I320, onde também foram instalados Webmail servers nesses computadores. A razão pela qual foi necessária esta cooperação deve-se ao princípio de funcionamento do MRTG (Capítulo 4.1.2).

O **NTOP** foi configurado no **tux12** e o **MRTG** no **tux13**. O **tux14** não teve disponível na parte final do trabalho devido a erro durante a sua configuração que não pode ser corrigido presencialmente em tempo útil. Consequentemente, não foi utilizado.

3.3 Routing

Devido ao objetivo do trabalho, foi necessário fazer uso do router de bancada **rtr-1**. O router de bancada está ligado à mesma rede local que os *tux*s, através do switch, que por sua vez está ligado ao router de sala **firetux**. Esta informação será util durante a utilização do MRTG.

3.4 Cronjobs

De forma similar ao projeto anterior, foram configurados *cronjobs* para simular tráfego na rede. Este cronjobs estavam configurados: (Fig 3.1)

```
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repo$
#mails
0 * * * * root echo "My message" | mail -s test netedu@gnu32.netlab.fe.up.pt
30 * * * * root echo "My message" | mail -s testing netedu@tux13.netlab.fe.up.pt
45 * * * * root echo "My message" | mail -s testing netedu@gnu32.netlab.fe.up.pt
#digs
0 * * * * root dig @localhost google.com
1 * * * * root dig @locahost google.com
#
```

Figure 3.1: Exemplo dos Cronjobs no tux12

- No *tux12* e *tux13*, para gerar tráfego local
- No *gnu32*, para gerar tráfego não local que passasse pelo router

Este *cronjobs* geram tráfego especifico de cada serviço nomeadamente:

- SMTP (Simple Mail Transfer Protocol), ao enviar emails.
- FTP, ao fazer download de um ficheiro via FTP
- DNS, ao fazer queries, neste caso do *google.com*
- HTTP, ao aceder ao sites através do *wget*

O tráfego NTP é gerado automaticamente pois o computador sincroniza periodicamente com a hierarquia superior.

4 Análise de Resultados

Nesta secção serão abordadas duas ferramentas de monitorização de tráfego, o **MRTG** e o **NTOP**.

4.1 MRTG

4.1.1 Configuração

O **MRTG** é uma ferramenta capaz de monitorizar o tráfego SNMP numa rede. Através do MRTG, pode-se monitorizar o tráfego que entra e sai da nossa rede, com a informação apresentada em gráficos com diversos intervalos de tempo. Deste modo, analisa-se de uma forma visual os padrões de tráfego da nossa rede.

Durante configuração do MRTG [6], este foi configurado para que analisasse o tráfego no router de bancada (172.16.1.19). Este router foi configurado de modo a que o serviço SNMP estivesse ativo e o MRTG pudesse obter essa informação.

4.1.2 Propriedades da rede

Devido à configuração da rede no laboratório, não é obrigatório que todo o tráfego passe pelo router de bancada (Fig 4.1).

Em primeiro lugar, o **tráfego local** faz uso do **switch**, logo esse tráfego não será registado pelo MRTG dado que não passa pelo router de bancada. Isto inclui todo o tráfego entre todos os *tux*s da sala I321.

Em segundo lugar, o router de bancada faz parte da mesma rede local que os *tux*s, ligados pelo switch ao router de sala **firetux**. Deste modo, não é obrigatório que um acesso de um tux a um host externo passe pelo router de bancada. Foi preciso então configurar os *tux*s, de modo a que utilizassem o router de bancada como *default gateway* para forçar o tráfego a ir por esse caminho. O router de bancada por sua vez tem o router de sala como o seu *default gateway* (Fig 4.2). Isto só funciona para novos queries, dado que da segunda vez que fazemos um acesso, o algoritmo irá determinar automaticamente que o melhor caminho é diretamente pelo **firetux** e mais uma vez o tráfego não irá ser registado (Fig 4.3).

Para voltar a forçar o caminho, é preciso apagar o routing cache, que é feito pelo próprio sistema periodicamente.

Em terceiro lugar, é preciso notar que o tráfego que vem de host externo **nunca** passa pelo router de bancada, a menos que seja direcionado para o mesmo. Isto

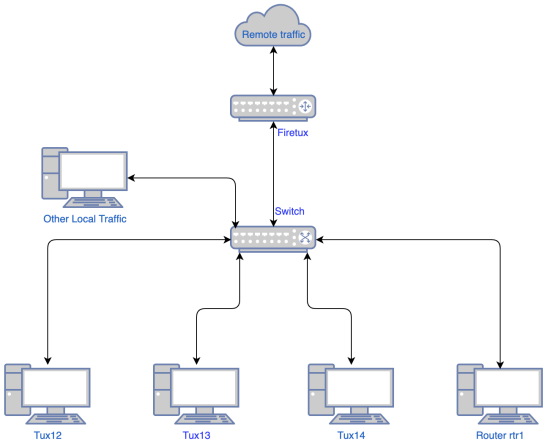


Figure 4.1: Configuração da rede neste trabalho

```
root@tux12:~# traceroute google.com
traceroute to google.com (142.250.184.14), 30 hops max, 60 byte packets
 1  tux-rtr1.netlab.fe.up.pt (172.16.1.19)  0.438 ms  0.483 ms  0.525 ms
 2  firetux.netlab.fe.up.pt (172.16.1.254)  1.121 ms  0.381 ms  0.468 ms
 3  192.168.110.253 (192.168.110.253)  6.694 ms  7.386 ms  7.531 ms
 4  gw.fe.up.pt (193.136.33.254)  2.432 ms  2.381 ms  2.440 ms
 5  193.136.25.81 (193.136.25.81)  3.341 ms  3.410 ms  3.352 ms
 6  Router22.Porto.fccn.pt (193.136.4.37)  2.773 ms Router23.Porto.fccn.pt (193.137.4.21)  2.549 ms  2.478 ms
 7  Router30.Backbone1.Lisboa.fccn.pt (193.136.1.1)  7.039 ms  7.069 ms  7.090 ms
 8  Router6.Lisboa.fccn.pt (194.210.6.105)  7.517 ms  7.305 ms  7.355 ms
 9  Google.AS15169.gigapix.pt (193.136.250.20)  6.669 ms  6.788 ms  6.856 ms
10  74.125.245.118 (74.125.245.118)  7.623 ms 74.125.245.68 (74.125.245.68)  7.412 ms 74.125.245.83 (74.125.245.83)  7.345 ms
11  142.251.55.185 (142.251.55.185)  14.637 ms 142.250.237.29 (142.250.237.29)  7.348 ms 142.251.55.149 (142.251.55.149)  15.846 ms
12  142.251.55.189 (142.251.55.189)  15.311 ms  15.613 ms 108.170.253.241 (108.170.253.241)  15.234 ms
13  142.250.214.43 (142.250.214.43)  15.497 ms  17.209 ms 142.250.214.41 (142.250.214.41)  15.977 ms
14  mad41s10-in-f14.1e100.net (142.250.184.14)  15.853 ms 142.250.214.43 (142.250.214.43)  15.598 ms  16.991 ms
root@tux12:~#
```

Figure 4.2: Primeiro traceroute de google.com

```
root@tux12:~# traceroute google.com
traceroute to google.com (142.250.184.14), 30 hops max, 60 byte packets
 1  firetux.netlab.fe.up.pt (172.16.1.254)  0.211 ms  0.286 ms  0.331 ms
 2  192.168.110.253 (192.168.110.253)  1.238 ms  1.474 ms  1.588 ms
 3  gw.fe.up.pt (193.136.33.254)  1.996 ms  1.933 ms  2.038 ms
 4  193.136.25.81 (193.136.25.81)  3.394 ms  3.137 ms  3.034 ms
 5  Router22.Porto.fccn.pt (193.136.4.37)  2.456 ms  2.405 ms  2.335 ms
 6  Router23.Porto.fccn.pt (193.137.4.21)  2.917 ms  3.378 ms  3.696 ms
 7  Router30.Backbone1.Lisboa.fccn.pt (193.136.1.1)  7.273 ms  6.789 ms  6.824 ms
 8  Router6.Lisboa.fccn.pt (194.210.6.105)  6.472 ms  6.556 ms  6.981 ms
 9  Google.AS15169.gigapix.pt (193.136.250.20)  6.637 ms  6.458 ms  6.515 ms
10  74.125.245.101 (74.125.245.101)  18.812 ms 74.125.245.84 (74.125.245.84)  7.457 ms 74.125.245.68 (74.125.245.68)  18.195 ms
11  142.250.237.29 (142.250.237.29)  6.756 ms 142.251.55.185 (142.251.55.185)  14.527 ms 172.253.76.193 (172.253.76.193)  15.821 ms
12  108.170.253.225 (108.170.253.225)  13.594 ms 216.239.47.124 (216.239.47.124)  15.242 ms 142.251.55.189 (142.251.55.189)  15.174 ms
13  108.170.253.225 (108.170.253.225)  15.114 ms 142.250.214.41 (142.250.214.41)  16.652 ms 142.250.214.43 (142.250.214.43)  16.410 ms
14  142.250.214.43 (142.250.214.43)  15.190 ms mad41s10-in-f14.1e100.net (142.250.184.14)  15.623 ms  15.368 ms
root@tux12:~#
```

Figure 4.3: Segundo traceroute de google.com

faz sentido dado que router de bancada não faz parte do caminho ótimo para os *tux*.

Levanta-se então a nível do tráfego que nos é possível monitorizar. Todo o tráfego que é gerado no sentido *Local->Remote* é monitorizado. Tráfego *Remote->Local / Local->Local* não é possível de observar. Não podemos registar, por exemplo, acessos feitos ao nosso servidor FTP, ou emails enviados para o nosso servidor email. A sincronização entre o NTP server e NTP client também não é analisado dado que é tráfego local.

Uma solução seria monitorizar o tráfego no switch, onde todo o tráfego passa obrigatoriamente. Teria por consequência ver-se no entanto também tráfego local de outras bancadas.

4.1.3 Análise temporal

O MRTG apresenta gráficos temporais do tráfego que passa pelo router, quer a entrar, quer a sair. Devido ao período de tempo em que este esteve a monitorizar, só faz sentido apresentar o gráfico diário e semanal (Fig 4.4).

Como se pode observar, o gráfico é constante e apresenta um padrão a nível de picos que está relacionado com a temporização dos cronjobs. Estes cronjobs fazem diferentes tarefas como enviar mails, fazer "digs" no DNS e aceder a servidores HTTP. Os picos maiores devem-se a testes que estavam ser executados durante a configuração o sistema, como, por exemplo, pelo envio de muitos emails num curto espaço de tempo.

Constatamos também que o tráfego que entra é praticamos igual ao tráfego que sai. Isto deve-se ao facto de muito pouco tráfego ser destinado ao próprio router, funcionando este apenas como uma *gate*.

4.2 NTOP

4.2.1 Configuração

O **NTOP** é uma ferramenta de monitorização de tráfico. Oferece uma versão comunitária grátis, assim como versões profissionais de subscrição.

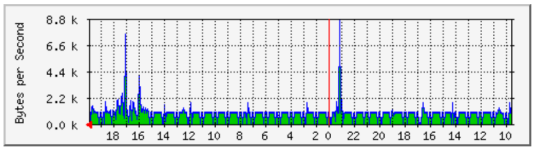
O NTOP funciona escutando o tráfego num adaptador de rede, i.e., interface. No nosso caso, é utilizada a interface *eth0*. É de notar que o NTOP consegue monitorizar várias interfaces ao mesmo tempo. Desse modo, este foi configurado para escutar essa interface [7]. A web-app do NTOP é acedida através do link `172.16.1.12:3000` e depois é efetuado o login com os dados configurados.

Traffic Analysis for 1 -- tux-rtr1

System: tux-rtr1 in
Maintainer:
Description: GigabitEthernet0/0 $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ifType: ethernetCsmacd (6)
ifName: Gi0/0
Max Speed: 125.0 MBytes/s
Ip: 172.16.1.19 (tux-rtr1.netlab.fe.up.pt)

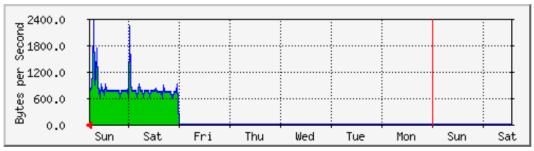
The statistics were last updated **Sunday, 28 March 2021 at 19:55**,
at which time **'tux-rtr1'** had been up for **2 days, 6:52:47**.

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	8552.0 B/s (0.0%)	825.0 B/s (0.0%)	1499.0 B/s (0.0%)
Out	8554.0 B/s (0.0%)	826.0 B/s (0.0%)	1520.0 B/s (0.0%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	2353.0 B/s (0.0%)	798.0 B/s (0.0%)	792.0 B/s (0.0%)
Out	2365.0 B/s (0.0%)	799.0 B/s (0.0%)	793.0 B/s (0.0%)

Figure 4.4: Gráficos temporais do tráfego no router MRTG

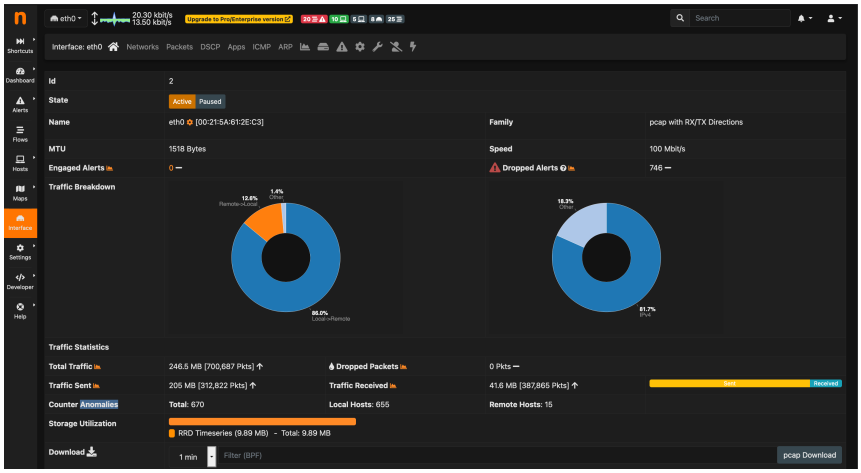


Figure 4.5: Main page da interface eth0

4.2.2 Análise global

Dentro da web-app do NTOP, após selecionar a interface desejada, é-nos apresentada uma página inicial onde se pode observar resumo do tráfego nessa interface: (Fig 4.5)

- Monitorização do tráfego em tempo real no canto superior esquerdo
- Tipo de tráfego, com 86% a ser *Local->Remote*.
- Total de tráfego registado pelo NTOP, com 205 MB enviado e 41.6 MB recebidos. Dado que estão a ser realizados acessos FTP externos, ocorre um aumento considerável do total de MB enviados pelo servidor.

4.2.3 Análise por tipologia

Na tab "Apps", são apresentados 4 piecharts contendo a distribuição do tráfego por tipologia. É apresentada uma avaliação total, assim como uma monitorização em tempo real (Fig 4.6).

O *FTP Data* corresponde a 52.4% do tráfego, com o NTOP a representar 28.2%. Isto deve-se ao facto do NTOP gerar informação em realtime, que obriga a atualização constante da informação, gerando mais tráfego. No momento em que foi tirado o print, não estava a ser detetado tráfego significativo de outros serviços, por isso o NTOP representa a maior fatia.

Conseguimos também ver a distribuição total do tráfego em valores absolutos, onde podemos observar, por exemplo, que o tráfego FTP representa a maior fatia de tráfego na interface (Fig 4.7). Conseguimos também observar tráfego dos outros

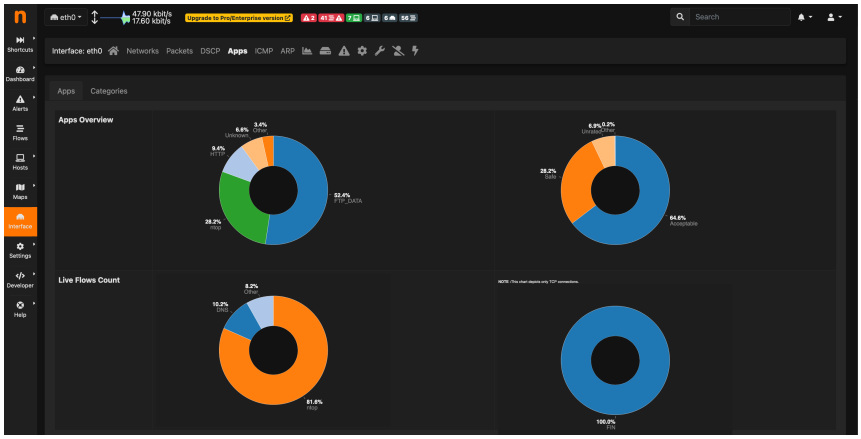


Figure 4.6: Piecharts da distribuição do tráfego por tipologia

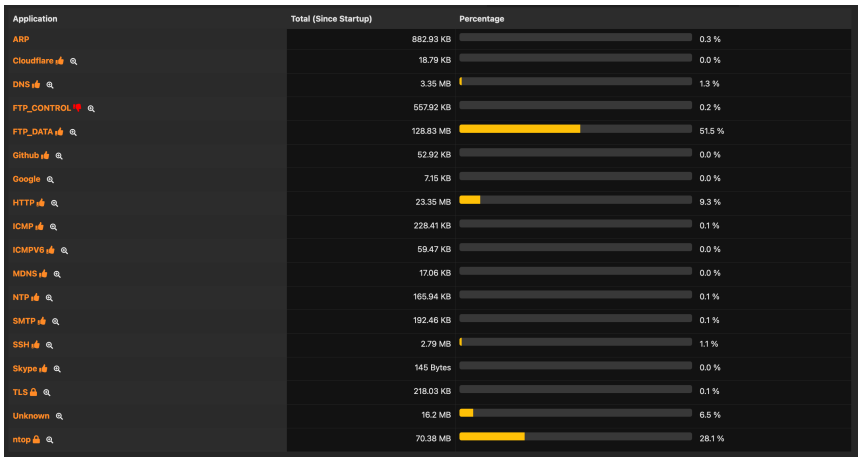


Figure 4.7: Distribuição do tráfego por tipologia

serviços instalados, nomeadamente DNS, HTTP, NTP e SMTP (Simple Mail Transfer Protocol). O FTP estava a ser acedido para fazer download de um ficheiro de 250 Kb, pelo que gera mais tráfego. O email por outro lado, era pequeno, pelo que gera menos tráfego. Outros serviços são também detetados.

4.2.4 Análise temporal

Tal como o MRTG, o NTOP também apresenta gráficos com a distribuição do tráfego a nível temporal. Podemos observar diferentes intervalos temporais, como por exemplo, o horário (Fig 4.8). Podemos constatar neste gráfico vários picos periódicos de tráfego. Estes correspondem, mais uma vez, aos pedidos FTP que geram muito mais tráfego que os restantes serviços.

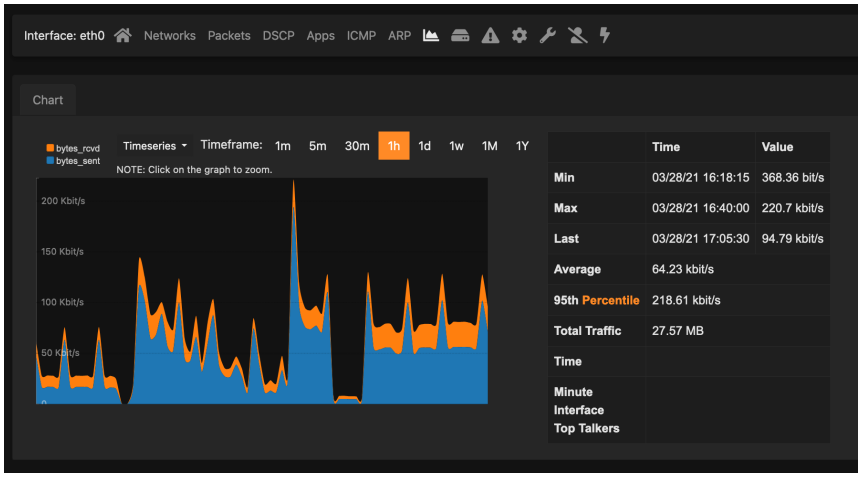


Figure 4.8: Análise horária do tráfego

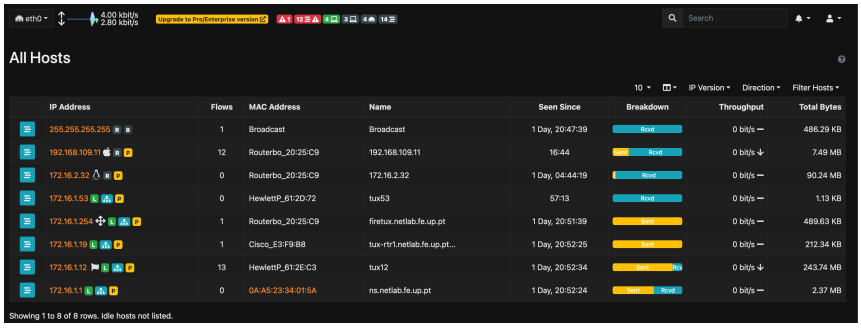


Figure 4.9: Lista dinâmica de hosts ativos

4.2.5 Análise dos Hosts

O NTOP apresenta também uma lista de hosts que utilizaram a interface para enviar/receber tráfego (Fig 4.9). Esta lista é dinâmica e apresenta apenas os hosts ativos recentemente, mas é possível fazer uma pesquisa por qualquer host que tenha utilizado a interface. Podemos constatar que o *tux12* (172.16.1.12) gerou a maior parte do tráfego (243.74 MB). Isto faz sentido dado que foi neste *tux* que se instalaram todos os serviços.

Também é possível fazer o mesmo tipos de análises que foram feitas para a interface, como a distribuição por tipologia e a distribuição temporal (Fig 4.10).

4.2.6 Análise dos recursos do Sistema

Além da análise do tráfego da interface, o NTOP apresenta também os recursos do sistema onde está instalado e o seu nível de utilização (Fig 4.11). Podemos observar gráficos de utilização do CPU do sistema para avaliar possíveis *bottlenecks*

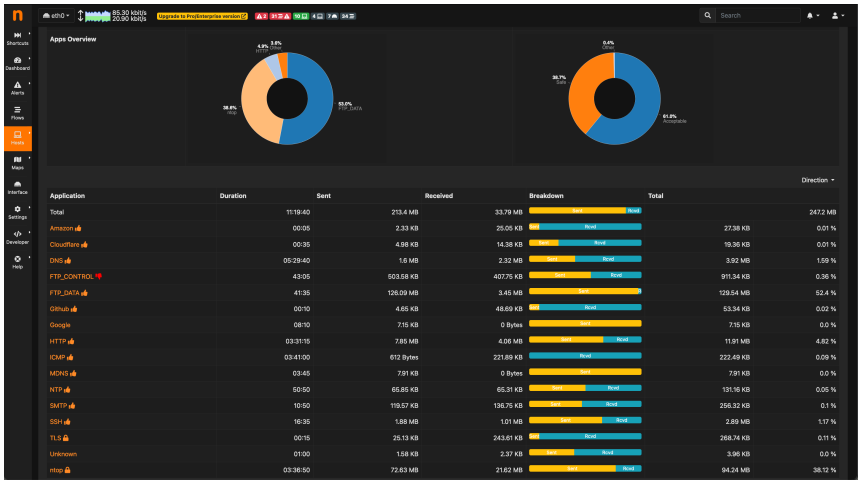


Figure 4.10: Distribuição do tráfego por tipologia no tux12

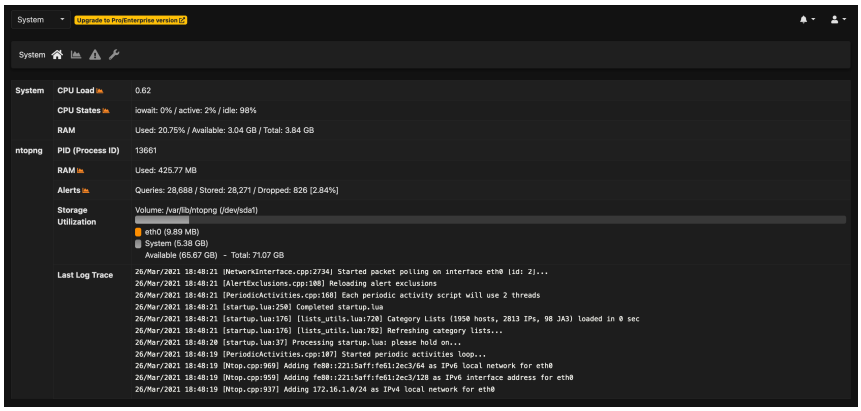


Figure 4.11: Utilização dos recursos do sistema

a nível do hardware. No nosso caso, os serviços instalados e a sua utilização não representam uma carga de utilização suficientemente grande para esta ferramenta ser útil neste projeto.

4.3 Comparação

Estas duas ferramentas e os resultados obtidos diferem em vários aspetos. Vamos analisar essas diferenças nesta secção.

4.3.1 Monitorização de tráfego

O NTOP, como mencionado anteriormente, regista todo o tráfego que usa a interface *eth0*. Esta interface é usada para praticamente todo tráfego, quer dentro da

rede local quer externo. Deste modo o NTOP é capaz de registar todo o tráfego dos serviços instalados no tux12.

O MRTG faz a monitorização do tráfego através do protocolo SNMP. Ele foi configurado para monitorizar o router de bancada onde foi ativado o SNMP. Pelas razões mencionadas na capítulo 4.1.2, o MRTG neste contexto não é capaz de ler todo o tráfego gerado pelos serviços, dado que nem todo o tráfego passa pelo router. Desde modo, não é possível fazer uma análise total da utilização do nosso serviço com dois tipos de tráfego: *Local->Local e Remote->Local*.

4.3.2 User Interface

O MRTG não faz distinção do tipo de tráfego. De uma forma simples, apresenta gráficos com a evolução do tráfego total recebido e enviado ao longo do tempo.

O NTOP faz discriminação do tráfego, assim como da origem dele. Apresenta vários gráficos e tabelas onde podemos ver o tipo de tráfego, a sua origem, e a sua evolução ao longo do tempo. Deste modo, podemos afirmar que o NTOP apresenta muita mais informação do que o MRTG.

Comparando os dois gráficos horários do NTOP (Fig 4.8) e MRTG (Fig 4.4), pode-se observar que no MRTG não estão presentes os picos de tráfego em 100kB que vemos no NTOP. Isto deve-se ao facto do tráfego FTP não estar a ser monitorizado. Estão a ser realizados acessos FTP do tipo *Remote->Local*, um tipo de tráfego que não passa pelo router de bancada. Para se poder observar tráfego FTP, seria necessário fazer ligações a servidores FTP da outra sala. Isto não foi possível realizar em tempo útil, pois à data da recolha dos dados, não havia servidores FTP na outra sala disponíveis para este teste.

4.3.3 Use Cases

O NTOP provou ser a melhor ferramenta neste contexto. No entanto, não regista o tráfego utilizado por outras interfaces de outros *tux*s. Como na nossa configuração, todos os serviços estavam instados no *tux12*, isto não foi um problema.

O MRTG é mais útil para monitorizar o tráfego de um servidor. Se estivéssemos a ler o switch, iríamos conseguir ver todo o tráfego *Local->Local / Remote->Local / Local->Remote*. Isto seria mais útil, sendo que estaríamos a ver todo o tráfego gerado por todos os hosts dentro da sala I321.

Ao ler router **firetux**, não íamos conseguir ver tráfego local.

5 Conclusão

Com a elaboração deste trabalho, atingimos os nossos objetivos de aprendizagem, nomeadamente a nível de conhecimento do funcionamento da rede e da circulação de tráfego. Analisamos também o comportamento dos hosts na rede a nível de tráfego, assim como o funcionamento do router.

Conseguimos configurar diferentes serviços nos nossos hosts, enumerando-se um servidor FTP, um web server, um servidor email, um servidor NTP e um servidor cache DNS.

Relativamente aos programas de monitorização, concluímos que de facto o MRTG e o NTOP têm dois espectros de utilização diferentes. O NTOP monitoriza a interface de comunicação, registando todo o tráfego que por ela passa. Este serviço cria uma web app com muita informação, onde podemos observar os diferentes serviços e o tráfego que geravam, assim como os hosts que estavam a utilizar a interface para comunicar.

O MRTG por outro lado monitoriza o tráfego que passava pelo router de bancada. Comprovou-se não registar todas as comunicações efetuadas dentro da rede neste caso. Apresenta uma webpage simples onde se pode ver gráficos com a evolução temporal do tráfego.

São duas ferramentas diferentes, sendo o MRTG claramente mais simples, com uma configuração mais rápida mas com menos informação disponível. O NTOP tem uma UI mais complexa, apresentando mais informação relativamente ao tráfego. É de notar que o também é capaz de monitorizar a nível do SNMP como MRTG, sendo por isso uma ferramenta mais poderosa.

Bibliografia

[1] *Apache Ubuntu*. https://ubuntu.com/tutorials/install-and-configure-apache#1-overview. [Visited 03-2021]. 2021.

[2] *How to Install And Configure FTP Server In Ubuntu*. https://www.unixmen.com/install-configure-ftp-server-ubuntu/. [Visited 03-2021]. 2020.

[3] *How to Install NTP Server and Client(s) on Ubuntu 20.04 LTS*. https://vitux.com/how-to-install-ntp-server-and-client-on-ubuntu/. [Visited 03-2021]. 2021.

[4] *Postfix Ubuntu*. https://ubuntu.com/server/docs/mail-postfix. [Visited 03-2021]. 2021.

[5] *DNS Ubuntu*. https://ubuntu.com/server/docs/service-domain-name-service-dns. [Visited 03-2021]. 2021.

[6] *How to monitor SNMP traffic on Ubuntu for free with MRTG*. https://www.techrepublic.com/article/how-to-monitor-snmp-traffic-on-ubuntu-for-free-with-mrtg/. [Visited 03-2021]. 2016.

[7] *Install Ntopng to Monitor Network Traffic on Ubuntu 20.04*. https://www.atlantic.net/vps-hosting/install-ntopng-to-monitor-network-traffic-on-ubuntu-20-04/. [Visited 03-2021]. 2020.