

Relatório Aula Prática 4 e 5



Mestrado Integrado em Engenharia Eletrotécnica e
Computadores

Planeamento e Gestão de Redes

Francisco Fernandes Xavier de Barros – 201506338
João Nuno Barbosa Neves – 201405198

27 de Março de 2019

Introdução

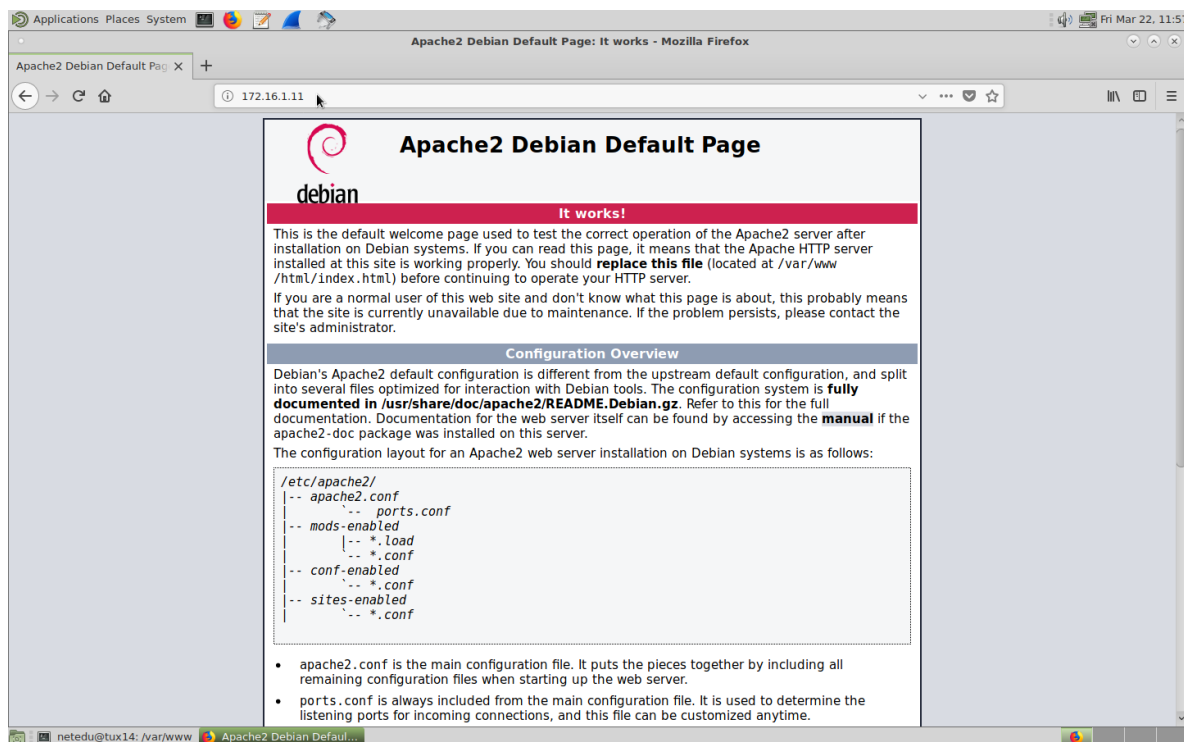
No âmbito da unidade curricular de Planeamento e Gestão de Redes foram estudadas para este trabalho duas ferramentas de monitorização de tráfego de sistemas e serviços de uma rede, sendo elas MRTG (*"The Multi Router Traffic Gapher"*) e ntop (*"Network Top"*).

Para a monitorização foram configurados, um servidor Web, um servidor FTP, um servidor NTP, um servidor de e-mail e um servidor cache de DNS, de modo a gerar tráfego.

Configuração dos Servidores

Servidor Web

Para o servidor Web foi utilizado um dos servidores criados no trabalho anterior.



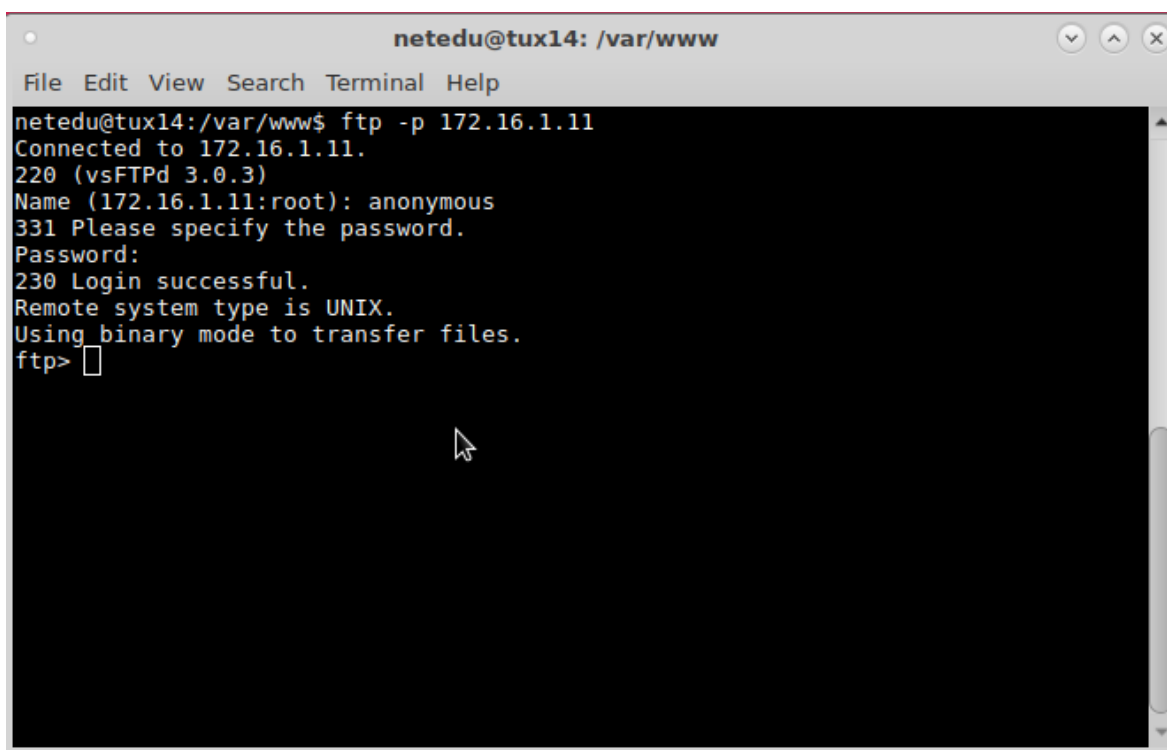
Servidor FTP

Para o servidor FTP foram executados os seguintes comandos:

- apt install vsftpd
- nano /etc/vsftpd.conf

Configurações acrescentadas:

- anonymous_enable = YES
 - anon_upload_enable = YES
 - write_enable = YES
 - anon_mkdir_write_enable = YES
- systemctl restart vsftpd
 - systemctl enable vsftpd

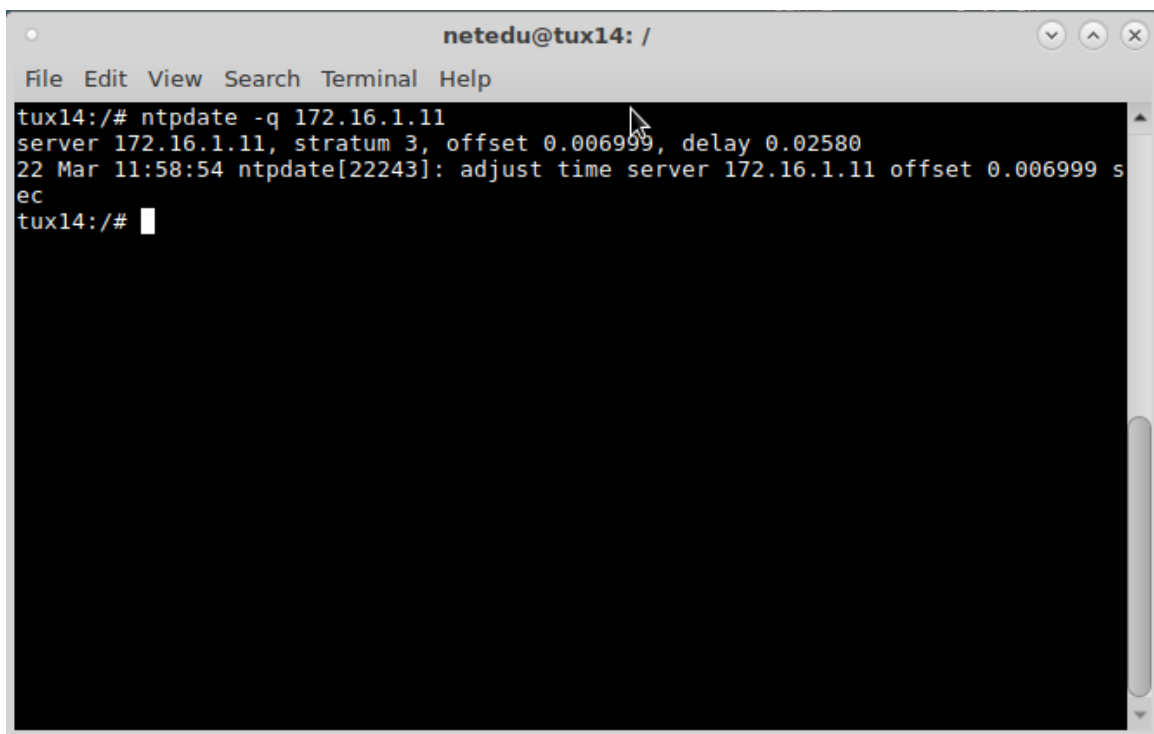
A screenshot of a terminal window titled 'netedu@tux14: /var/www'. The terminal shows the execution of the command 'ftp -p 172.16.1.11'. The output indicates a successful connection to 172.16.1.11 using vsFTPD 3.0.3. The user is prompted for a password, and the login is successful. The terminal also shows the remote system type as UNIX and that binary mode is used for file transfers. The prompt 'ftp>' is visible at the bottom.

```
netedu@tux14:/var/www$ ftp -p 172.16.1.11
Connected to 172.16.1.11.
220 (vsFTPd 3.0.3)
Name (172.16.1.11:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Servidor NTP

Para o servidor executamos estes comandos:

- apt install ntp
- systemctl restart ntp
- systemctl enable ntp

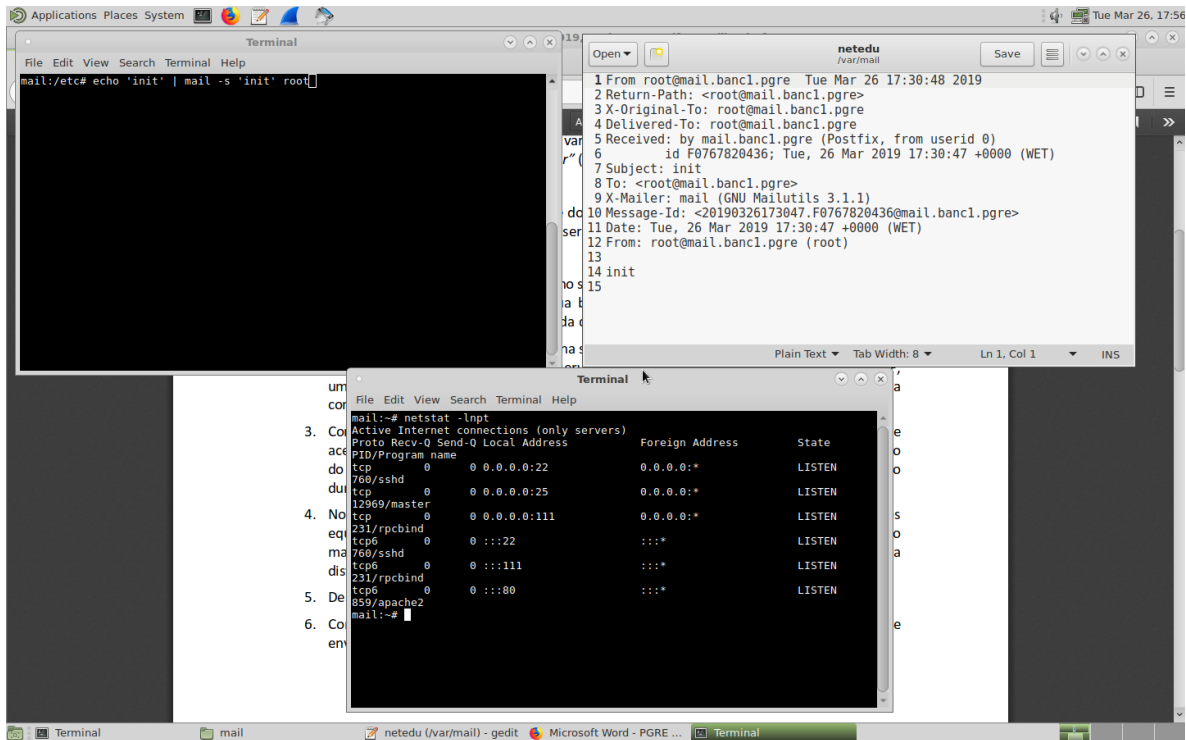
A terminal window titled 'netedu@tux14: /' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'ntpdate -q 172.16.1.11' being executed. The output is: 'server 172.16.1.11, stratum 3, offset 0.006999, delay 0.02580', '22 Mar 11:58:54 ntpdate[22243]: adjust time server 172.16.1.11 offset 0.006999 s', and 'ec'. The prompt 'tux14:/#' is followed by a cursor.

```
netedu@tux14: /
File Edit View Search Terminal Help
tux14:/# ntpdate -q 172.16.1.11
server 172.16.1.11, stratum 3, offset 0.006999, delay 0.02580
22 Mar 11:58:54 ntpdate[22243]: adjust time server 172.16.1.11 offset 0.006999 s
ec
tux14:/#
```

Servidor e-mail (Postfix)

O servidor de e-mail necessitou de um número maior de comandos, sendo eles:

- apt-get install postfix
- apt-get install mailutils
- cp /etc/postfix/main.cf{,.backup}
- nano /etc/postfix/main.cf
 - Configurações acrescentadas/modificadas
 - myhostname = mail.banc1.pgre
 - mydomain = banc1.pgre
 - mynetworks = 127.0.0.0/8, 192.168.1.0/24, 172.16.1.0/24
 - inet_protocols = ipv4
 - home_mailbox = Maildir/
- systemctl restart postfix
- systemctl enable postfix
- echo 'init' | mail -s 'init' root /* Comando para enviar mail */



Observe-se na imagem a porta 25 associada ao protocolo smtp aberta, o comando que utilizamos para o envio do mail e a receção do mesmo no ficheiro `/var/mail/netedu`. Apesar de ter sido enviado para root, a configuração no ficheiro `/etc/aliases` transporta para netedu o mail recebido.

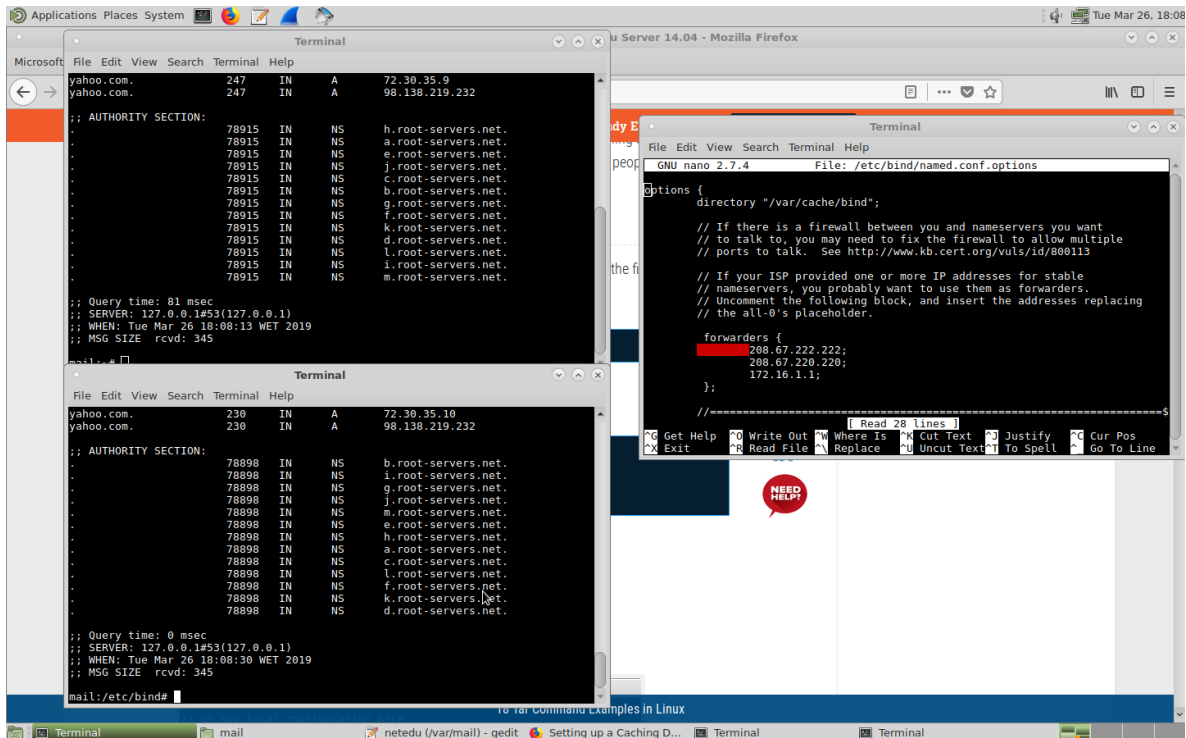
Servidor e Cliente DNS

No servidor executamos os comandos:

- `apt install bind9 bind9utils`
- `nano /etc/bind/named_conf_options`

Configurações acrescentadas/modificadas:

- `forwarders {`
- `172.16.1.1;`
- `}`



Observe-se na imagem a diferença na Query Time à primeira e segunda execução do comando dig yahoo.com.

Resultados obtidos MRTG e nTop

Para obter uma quantidade maior de informação criamos um ficheiro crontab e os servidores web, ftp, ntp e dns ficaram a correr durante um dia.

Ficheiro crontab:

```
Apache */5 * * * * curl http://172.16.1.14 >/dev/null 2>&1
FTP */5 * * * * /root/Desktop/script.sh
NTP */5 * * * * ntpdate -u 172.16.1.14 > /dev/null 2>&1
DNS */5 * * * * dig 172.16.1.14 > /dev/null 2>&1
```

No caso do servidor de e-mail criamos um script bash para correr o mesmo.

Script Bash:

```
# !bin/bash
while true
do
    echo 'init' | mail -s 'init' root
    sleep 50
done
```

MRTG:

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)

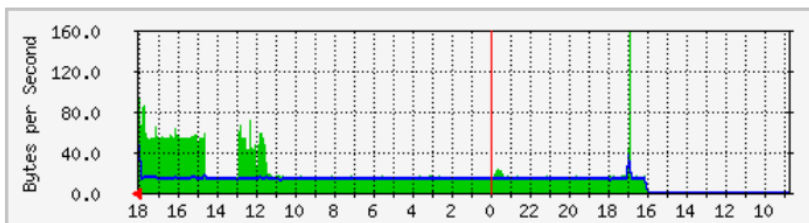
ifName: Gi0/0

Max Speed: 12.5 MBytes/s

Ip: 172.16.1.19 (tux-rtr1.netlab.fe.up.pt)

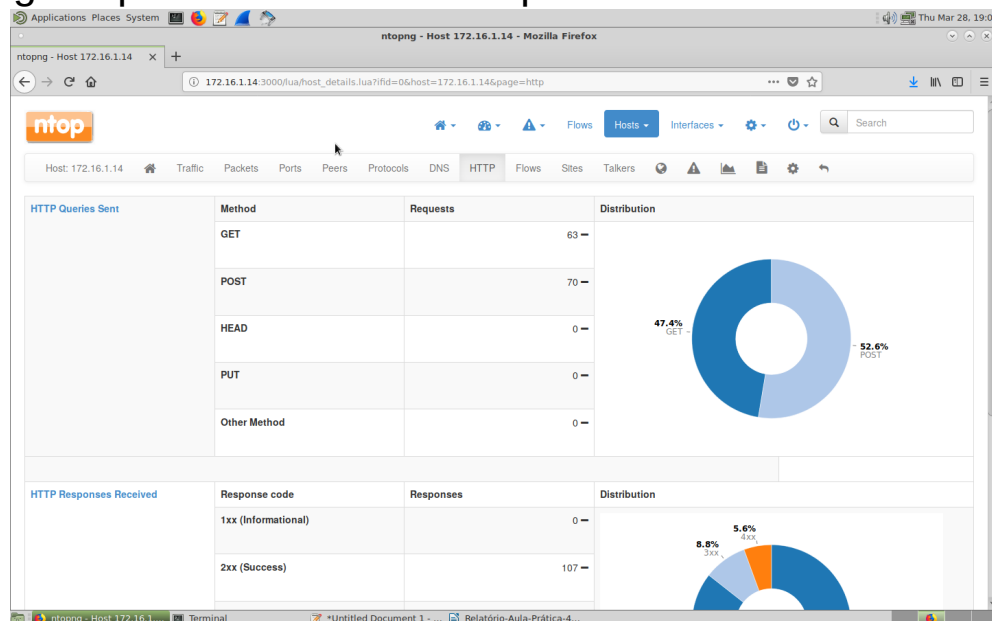
The statistics were last updated **Thursday, 28 March 2019 at 18:05**, at which time '**tux-rtr1**' had been up for **3:48:13**.

'Daily' Graph (5 Minute Average)

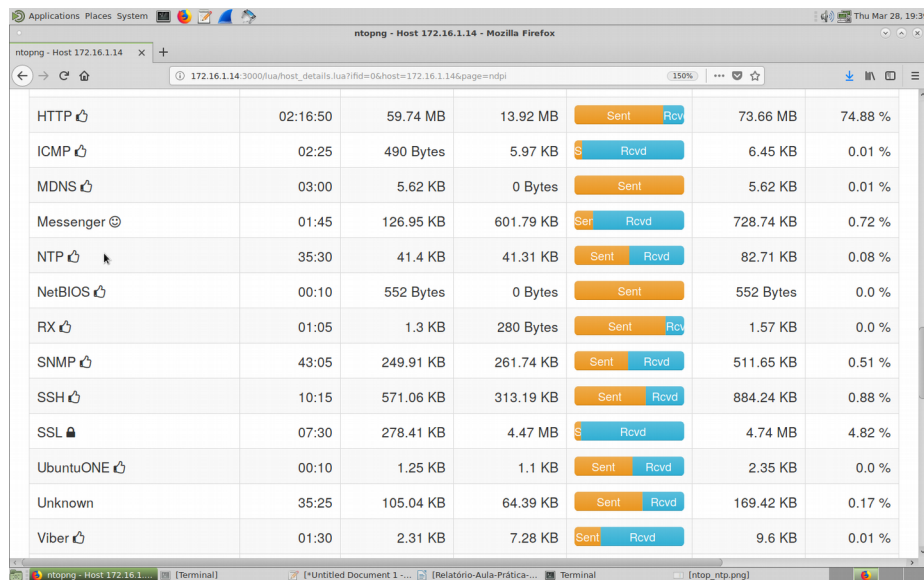


NTOP

Tráfego capturado do servidor apache:

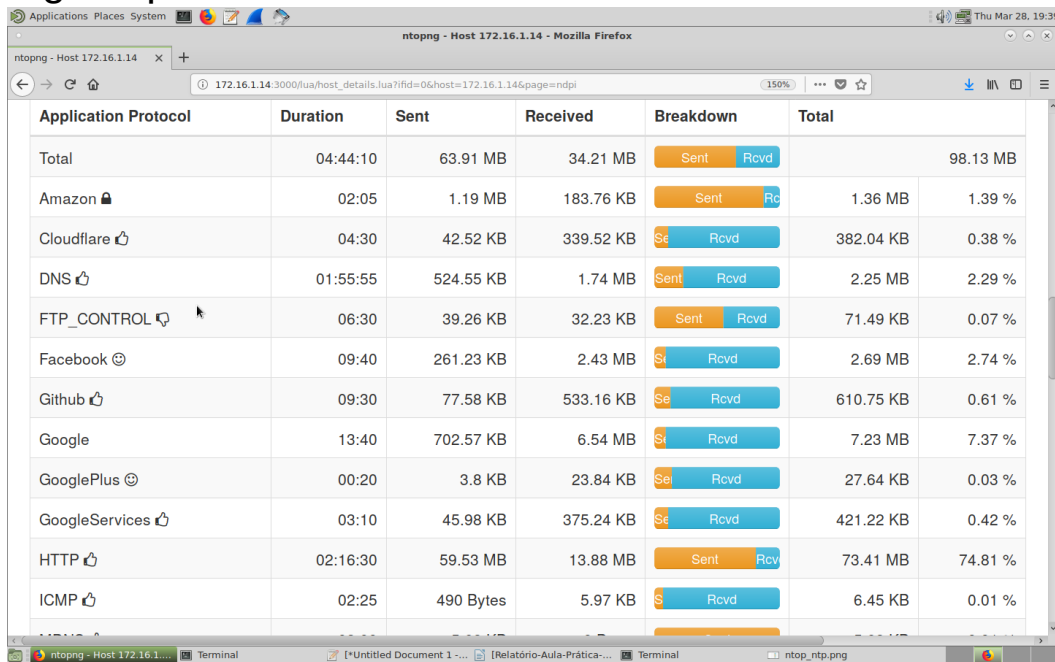


Tráfego capturado servidor ntp:



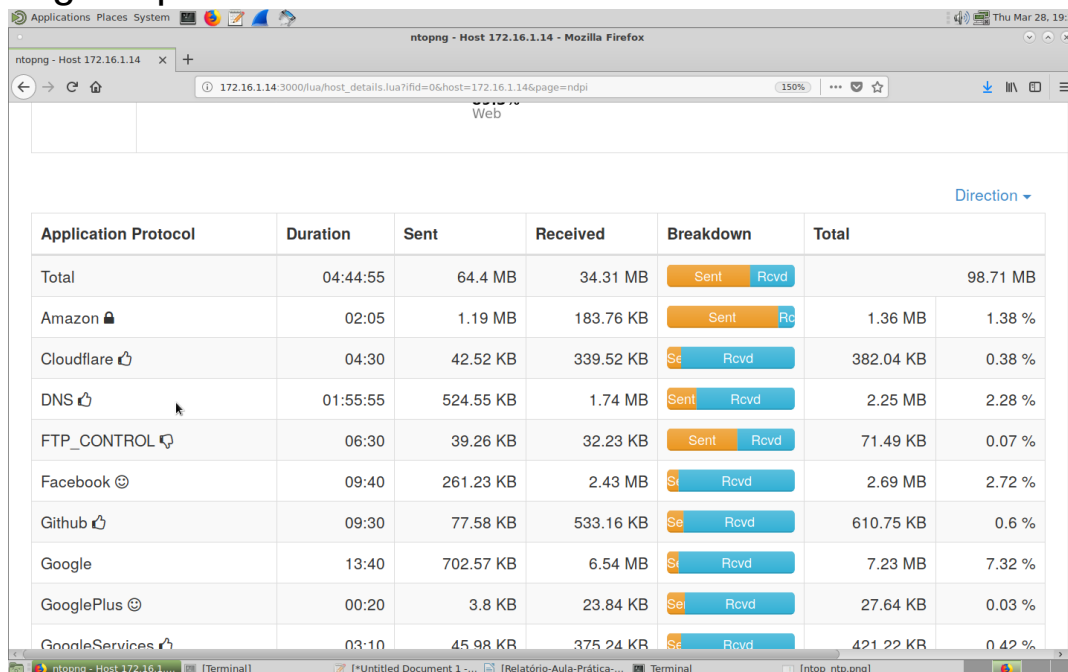
Protocol	Duration	Sent	Received	Sent (MB)	Received (KB)	Total (KB)	%
HTTP	02:16:50	59.74 MB	13.92 MB	Sent	Rcvd	73.66 MB	74.88 %
ICMP	02:25	490 Bytes	5.97 KB	Sent	Rcvd	6.45 KB	0.01 %
MDNS	03:00	5.62 KB	0 Bytes	Sent		5.62 KB	0.01 %
Messenger	01:45	126.95 KB	601.79 KB	Sent	Rcvd	728.74 KB	0.72 %
NTP	35:30	41.4 KB	41.31 KB	Sent	Rcvd	82.71 KB	0.08 %
NetBIOS	00:10	552 Bytes	0 Bytes	Sent		552 Bytes	0.0 %
RX	01:05	1.3 KB	280 Bytes	Sent	Rcvd	1.57 KB	0.0 %
SNMP	43:05	249.91 KB	261.74 KB	Sent	Rcvd	511.65 KB	0.51 %
SSH	10:15	571.06 KB	313.19 KB	Sent	Rcvd	884.24 KB	0.88 %
SSL	07:30	278.41 KB	4.47 MB	Sent	Rcvd	4.74 MB	4.82 %
UbuntuONE	00:10	1.25 KB	1.1 KB	Sent	Rcvd	2.35 KB	0.0 %
Unknown	35:25	105.04 KB	64.39 KB	Sent	Rcvd	169.42 KB	0.17 %
Viber	01:30	2.31 KB	7.28 KB	Sent	Rcvd	9.6 KB	0.01 %

Tráfego capturado servidor FTP:



Application Protocol	Duration	Sent	Received	Breakdown	Total
Total	04:44:10	63.91 MB	34.21 MB	Sent Rcvd	98.13 MB
Amazon	02:05	1.19 MB	183.76 KB	Sent Rcvd	1.36 MB 1.39 %
Cloudflare	04:30	42.52 KB	339.52 KB	Sent Rcvd	382.04 KB 0.38 %
DNS	01:55:55	524.55 KB	1.74 MB	Sent Rcvd	2.25 MB 2.29 %
FTP_CONTROL	06:30	39.26 KB	32.23 KB	Sent Rcvd	71.49 KB 0.07 %
Facebook	09:40	261.23 KB	2.43 MB	Sent Rcvd	2.69 MB 2.74 %
Github	09:30	77.58 KB	533.16 KB	Sent Rcvd	610.75 KB 0.61 %
Google	13:40	702.57 KB	6.54 MB	Sent Rcvd	7.23 MB 7.37 %
GooglePlus	00:20	3.8 KB	23.84 KB	Sent Rcvd	27.64 KB 0.03 %
GoogleServices	03:10	45.98 KB	375.24 KB	Sent Rcvd	421.22 KB 0.42 %
HTTP	02:16:30	59.53 MB	13.88 MB	Sent Rcvd	73.41 MB 74.81 %
ICMP	02:25	490 Bytes	5.97 KB	Sent Rcvd	6.45 KB 0.01 %

Tráfego capturado servidor cache dns:



Application Protocol	Duration	Sent	Received	Breakdown	Total
Total	04:44:55	64.4 MB	34.31 MB	<div>Sent Rcvd</div>	98.71 MB
Amazon	02:05	1.19 MB	183.76 KB	<div>Sent Rcvd</div>	1.36 MB 1.38 %
Cloudflare	04:30	42.52 KB	339.52 KB	<div>Sent Rcvd</div>	382.04 KB 0.38 %
DNS	01:55:55	524.55 KB	1.74 MB	<div>Sent Rcvd</div>	2.25 MB 2.28 %
FTP_CONTROL	06:30	39.26 KB	32.23 KB	<div>Sent Rcvd</div>	71.49 KB 0.07 %
Facebook	09:40	261.23 KB	2.43 MB	<div>Sent Rcvd</div>	2.69 MB 2.72 %
Github	09:30	77.58 KB	533.16 KB	<div>Sent Rcvd</div>	610.75 KB 0.6 %
Google	13:40	702.57 KB	6.54 MB	<div>Sent Rcvd</div>	7.23 MB 7.32 %
GooglePlus	00:20	3.8 KB	23.84 KB	<div>Sent Rcvd</div>	27.64 KB 0.03 %
GoogleServices	03:10	45.98 KB	375.24 KB	<div>Sent Rcvd</div>	421.22 KB 0.42 %

Quanto ao servidor de mail postfix, apesar do SPAM que tentámos forçar no servidor não nos foi possível encontrar pegadas na interface do ntop, provavelmente por não estarmos a fazer algo da melhor forma.

Comparação entre MRTG e nTop e conclusões

Após a monitorização e obtenção dos dados dos servidores através das duas ferramentas, concluímos que, embora as duas ferramentas sejam utilizadas para o mesmo fim, ambas têm as suas particularidades.

Enquanto que a MRTG consegue obter uma maior quantidade de informação relativamente ao tráfego que passa pelo router, a ferramenta nTop consegue informação mais detalhada ao nível dos protocolos associados aos pacotes que o servidor alocado na máquina consegue observar.

Ao nível da gestão de redes podemos concluir que foi positivo aprender as funcionalidades destas ferramentas devido à sua utilidade, apesar do ocupamento que ambas tem na banda.

Admitimos que o mais difícil no trabalho foi configurar os servidores pois o que encontrámos na web nem sempre se adapta a 100% aos sistemas que dispomos mas isso também nos obriga a entender melhor as máquinas que temos e o próprio sistema Linux.

Nota final

O facto dos ip's que aparecem nos prints não corresponderem com o ip do servidor que efetivamente usámos deve-se ao azar de termos aulas de outras cadeiras na mesma sala, onde pedem a execução do comando updateimage que apaga todas as configurações. Daí termos feito o trabalho em tuxes diferentes ao longo das duas semanas.

Fontes

<https://oss.oetiker.ch/mrtg/doc/mrtg-unix-guide.en.html>

<https://www.tecmint.com/install-postfix-mail-server-with-webmail-in-debian/>

<https://linuxconfig.org/how-to-configure-ftp-server-on-debian-9-stretch-linux>

<https://linuxconfig.org/how-to-setup-ntp-server-and-client-on-debian-9-stretch-linux>

<https://www.ntop.org>

<https://www.cisco.com>