

LAB 4
GII 3º TDRC

TELEMATIC SERVICES ON INTERNET

Autor 1: Ernesto Alejo Oltra

Autor 2: Alberto Moreno Alcaraz

Autor 3: Gabriel Guirado Muñoz

Dominio: tdrc2014-emaon-ip.biz

Fecha: 30 May 2014

BACKGROUND

Objective: Deploying two services behind a NAT using DDNS.

To troubleshoot errors we have used nslookup and ping.eu.

Configured services:

- Apache (with XAMPP).
- Filezilla Server (with XAMPP too)
- Web proxy (squid3).

Software & SO:

- Elementary (Ubuntu-based).
- Apache
- Filezilla Server
- Squid
- NoIP DDNS application.

Test software: Browser, wireshark, ...


BACKGROUND

We tried to configure the UGR VPN to have an additional external network from which run the tests. This posed two problems.

The DDNS local application updated the IP while the PC was inside the VPN; redirecting the domain to the UGR routers which were not prepared to handle the request.

Then we had problems trying to reach the PC, because the service was exposed through the VPN connection, not the local network one.

CREATE Dynamic DNS Account: tdr2014-ema0.no-ip.biz



Managed **DNS** Services

Create Your No-IP Account

Username

tdrc-redes

Email

Password

Confirm Password

.noip.me

☐ Create my hostname later

That address is also available with these **Enhanced DNS** domains for only \$19.95 a year:

tdrc-redes.ddns.me

tdrc-redes.noip.us

tdrc-redes.ddns.net

tdrc-redes.hopto.me

tdrc-redes.no-ip.ca

tdrc-redes.dnsfor.me

+ view more

No thanks, I'll use **the free hostname**

Names must be 6-15 characters long and only contain a-z, 0-9, -, and _

Minimum of 6 characters.

Password Strength

Choose a hostname for your account. You can change your hostname or add more later.

Upgrading to Enhanced DNS now will save you time and money later.

For more information on the Enhanced DNS upgrade, hover over the name for an explanation of the feature.

If you have chosen an Enhanced domain, but wish to sign up for a No-IP Free account, please choose the no-ip.biz domain option **above**.




CREATE Dynamic DNS Account: tdr2014-ema. no-ip.biz

Manage Hosts

Current Hosts: 1

Need More Hosts? Enhance Your Account!

Enhance Your Account

Host	IP/URL	Action
 Hosts By Domain		
no-ip.biz		
tdr2014-ema. no-ip.biz	217.216.102.114	 Modify  Remove

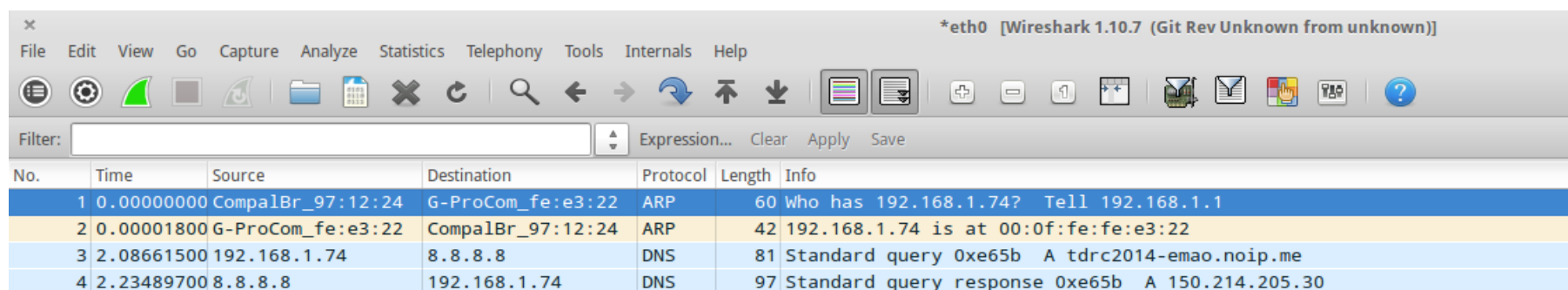
Add A Host

CHECK domain with nslookup and wireshark

```
~/Universidad/noip-duc-linux/noip-2.1.9-1  
✗ nslookup tdrc2014-emaao.no-ip.biz  
Server:          127.0.0.1  
Address:         127.0.0.1#53  
  
Non-authoritative answer:  
Name:   tdrc2014-emaao.no-ip.biz  
Address: 217.216.102.114
```

The results from the nslookup command, showing our domain pointing to the router IP.

CHECK domain with nslookup and wireshark



The screenshot shows the Wireshark interface with the following packet list:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	CompalBr_97:12:24	G-ProCom_fe:e3:22	ARP	60	Who has 192.168.1.74? Tell 192.168.1.1
2	0.00001800	G-ProCom_fe:e3:22	CompalBr_97:12:24	ARP	42	192.168.1.74 is at 00:0f:fe:fe:e3:22
3	2.08661500	192.168.1.74	8.8.8.8	DNS	81	Standard query 0xe65b A tdr2014-ema. no- ip. me
4	2.23489700	8.8.8.8	192.168.1.74	DNS	97	Standard query response 0xe65b A 150.214.205.30

Packets captured by Wireshark while the nslookup to our domain was running.

We can see the DNS request and the reply from the server.

Configure DDNS at home

```
~/Universidad/noip-duc-linux/noip-2.1.9-1
✗ sudo /usr/local/bin/noip2 -C

Auto configuration for Linux client of no-ip.com.

Please enter the login/email string for no-ip.com ernestokarim+noip@gmail.com
Please enter the password for user 'ernestokarim+noip@gmail.com' *****

Only one host [tdrc2014-ema0.no-ip.biz] is registered to this account.
It will be used.
Please enter an update interval:[30]
Do you wish to run something at successful update?[N] (y/N) ^M

New configuration file '/usr/local/etc/no-ip2.conf' created.

~/Universidad/noip-duc-linux/noip-2.1.9-1
✗ sudo /usr/local/bin/noip2 -S
1 noip2 process active.

Process 16877, started as /home/ernesto/Universidad/noip-duc-linux/noip-2.1.9-1/noip2, (version 2.1.9)
Using configuration from /usr/local/etc/no-ip2.conf
Last IP Address set 217.216.102.114
Account ernestokarim+noip@gmail.com
configured for:
    host tdr2014-ema0.no-ip.biz
Updating every 30 minutes via /dev/eth0 with NAT enabled.
```


Open ports in ADSL router

PORT FORWARDING

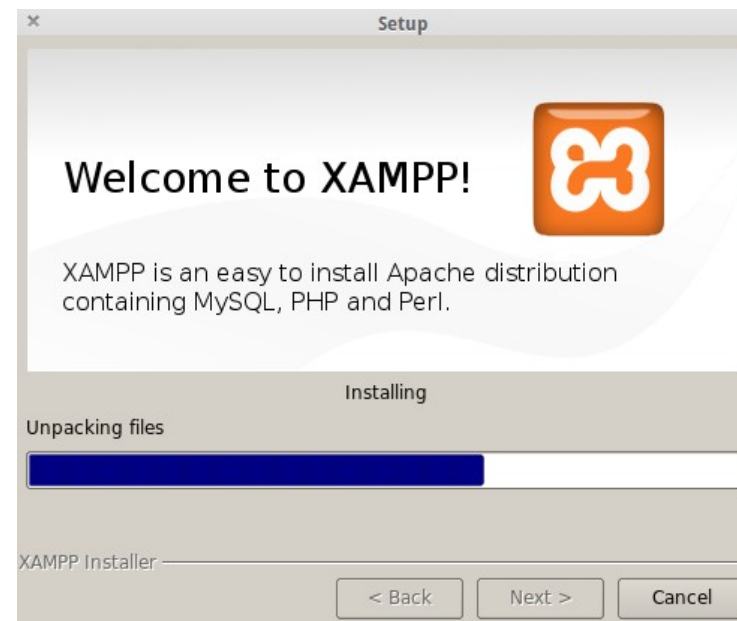
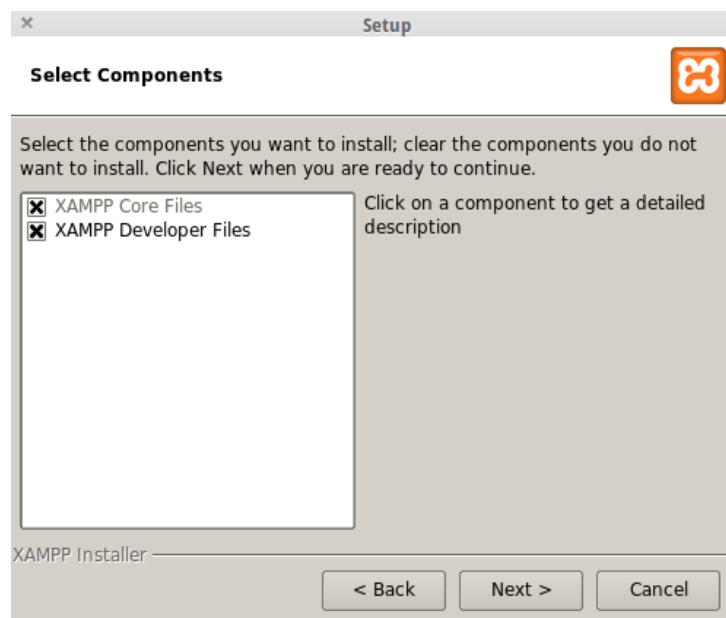
External IP Address: 217.216.102.114

Port Forwarding							
Local IP Addr	External		Internal		Protocol	Enabled	Delete
	Start Port	End Port	Start Port	End Port			
192.168.1.74	80	80	80	80	TCP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.168.1.74	3128	3128	3128	3128	Both	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.168.1.74	21	21	21	21	TCP	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add

Apply

Install service 1



Install service 1



Install service 2

```

699 # Adapt to list your (internal) IP networks from where browsing
700 # should be allowed
701 acl localnet src 0.0.0.0/0
702 #acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
703 #acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
704 #acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
705 #acl localnet src fc00::/7 # RFC 4193 local private network range

```

```

838
839 # Example rule allowing access from your local networks.
840 # Adapt localnet in the ACL section to list your (internal) IP networks
841 # from where browsing should be allowed
842 http_access allow all
843 http_access allow localnet
844

```

Install service 2

```
~/Universidad/noip-duc-linux/noip-2.1.9-1  
✗ sudo service squid3 start  
squid3 start/running, process 5536
```

```
~/Universidad/noip-duc-linux/noip-2.1.9-1  
✗ sudo service squid3 restart  
squid3 stop/waiting  
squid3 start/running, process 9428
```

Check ports in your server with netstat -a

```
~/Universidad/noip-duc-linux/noip-2.1.9-1
$ netstat -atn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80               0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:53043            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:4371           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:57621            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53             0.0.0.0:*               LISTEN
```

```
tcp        0      0 192.168.1.74:52805       192.241.190.153:443     ESTABLISHED
tcp        0    35 192.168.1.74:53043       86.147.228.238:62782    ESTABLISHED
tcp        0      0 192.168.1.74:42616       173.194.41.14:443      ESTABLISHED
tcp6       0      0 :::21                    :::*                    LISTEN
tcp6       0      0 :::1:631                  :::*                    LISTEN
tcp6       0      0 :::3128                   :::*                    LISTEN
tcp6       0      0 :::3306                   :::*                    LISTEN
```

Check ports from outside with www.ping.eu

Online service Port check



Port check – Tests if port is opened on specified IP

IP address or host name: tdr2014-ema.no-ip.biz

Port number: 80

Go

tdr2014-ema.no-ip.biz:80 port is open

Online service Port check



Port check – Tests if port is opened on specified IP

IP address or host name: tdr2014-ema.no-ip.biz

Port number: 3128

Go

tdr2014-ema.no-ip.biz:3128 port is open

Online service Port check



Port check – Tests if port is opened on specified IP

IP address or host name: tdr2014-ema.no-ip.biz

Port number: 21

Go

tdr2014-ema.no-ip.biz:21 port is open

Check ports from outside with www.ping.eu

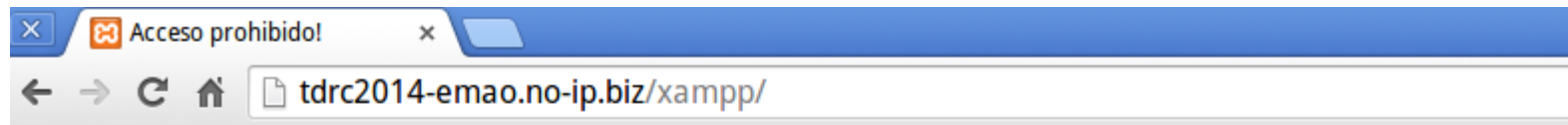
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	88.198.46.51	192.168.1.74	TCP	74	54491 > http [SYN] Seq=0 Win=7300 Len=0 MSS=1460 SACK_PERM=1 TSval=2197651435 TSecr=0 WS=256
2	0.00002900	192.168.1.74	88.198.46.51	TCP	74	http > 54491 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1085344 TSecr=2197651435 WS=128
3	0.06377100	88.198.46.51	192.168.1.74	TCP	66	54491 > http [ACK] Seq=1 Ack=1 Win=7424 Len=0 TSval=2197651451 TSecr=1085344
4	0.06471500	88.198.46.51	192.168.1.74	TCP	66	54491 > http [FIN, ACK] Seq=1 Ack=1 Win=7424 Len=0 TSval=2197651451 TSecr=1085344
5	0.06477400	192.168.1.74	88.198.46.51	TCP	66	http > 54491 [ACK] Seq=1 Ack=2 Win=14592 Len=0 TSval=1085360 TSecr=2197651451
6	0.06492600	192.168.1.74	88.198.46.51	TCP	66	http > 54491 [FIN, ACK] Seq=1 Ack=2 Win=14592 Len=0 TSval=1085360 TSecr=2197651451
7	0.12879100	88.198.46.51	192.168.1.74	TCP	66	54491 > http [ACK] Seq=2 Ack=2 Win=7424 Len=0 TSval=2197651468 TSecr=1085360

Packets received in a port check

Check connectivity to server with traceroute

```
~/Universidad/noip-duc-linux/noip-2.1.9-1
$ traceroute tdr2014-ema.no-ip.biz
traceroute to tdr2014-ema.no-ip.biz (217.216.102.114), 30 hops max, 60 byte packets
 1  vpn-i2001.ugr.es (172.20.2.1)  39.374 ms  51.004 ms  51.936 ms
 2  rfuentes205.ugr.es (150.214.205.223)  52.424 ms  52.471 ms  52.897 ms
 3  172.18.250.165 (172.18.250.165)  51.902 ms  52.023 ms  52.094 ms
 4  * * *
 5  * * *
 6  * * xe-0-3-1.sevilla01.red.cica.es (150.214.231.21)  42.877 ms
 7  GE7-0-0.cica.rt1.and.red.rediris.es (130.206.194.1)  43.796 ms  43.927 ms  47.086 ms
 8  CICA.XE0-0-2.ciemat.rt1.mad.red.rediris.es (130.206.245.37)  62.735 ms  58.615 ms  61.744 ms
 9  nttverio-1.espanix.net (193.149.1.36)  59.894 ms  57.247 ms  57.070 ms
10  ae-2.r01.mdrdsp04.es.bb.gin.ntt.net (129.250.4.105)  58.294 ms  57.949 ms  58.149 ms
11  83.231.151.210 (83.231.151.210)  63.092 ms  64.255 ms  64.412 ms
12  * * *
13  217.216.102.114.dyn.user.ono.com (217.216.102.114)  76.597 ms  * *
```

Show service 1



Acceso prohibido!

XAMPP nuevo concepto de seguridad:

Acceso a la solicitud objeto sólo está disponible desde la red local.

Este ajuste puede ser configurado en el archivo "httpd-xampp.conf".

Si usted cree que esto es un error del servidor, por favor comuníquese al [administrador del portal](#).

Error 403

tdrc2014-ema0.no-ip.biz

Apache/2.4.9 (Unix) OpenSSL/1.0.1g PHP/5.5.11 mod_perl/2.0.8-dev Perl/v5.16.3

Show service 1

Host: Username: Password: Port:

Local site:

Filename ^	Filesize	Filetype	Last modified
..			
.IntelliJldea13	Directory		25/03/14 22:31..
.Private	Directory		04/06/14 14:54..
.aptitude	Directory		24/05/14 14:58..
.atom	Directory		08/05/14 02:48..
.berkshelf	Directory		06/03/14 09:51..
.cache	Directory		03/06/14 14:49..
.cmake	Directory		06/04/14 20:35..
.compiz	Directory		07/02/14 21:30..

23 files and 62 directories. Total size: 145,2 KB

Quickconnect

Remote site:

Filename ^	Filesize	Filetype	Last modified	Permission	Ow
img		Directory	30/05/14 11...	file (0755)	0
webalizer		Directory	30/05/14 11...	file (0755)	1
xampp		Directory	30/05/14 11...	file (0755)	0
applications.html	1,5 KB	HTML do...	04/04/14 16...	adfr (06...	0
bitnami.css	2,2 KB	css-file	29/04/13 09...	adfr (06...	0
favicon.ico	30,9 KB	ico-file	11/05/07 14...	adfr (06...	0
index.php	256 B	php-file	05/02/09 22...	adfr (06...	0
tdrc.php	113 B	php-file	05/06/14 09...	adfrw (0...	0

Selected 1 file. Total size: 113 B

Show service 2

```

~/Universidad/noip-duc-linux/noip-2.1.9-1
$ sudo cat /var/log/squid3/access.log
1401444776.212 174 127.0.0.1 TCP_MISS/200 906 POST http://clients1.google.com/ocsp - DIRECT/173.194.41.6 application/ocsp-response
1401444776.576 74 127.0.0.1 TCP_MISS/200 906 POST http://clients1.google.com/ocsp - DIRECT/173.194.41.6 application/ocsp-response
1401444788.484 76 127.0.0.1 TCP_MISS/200 906 POST http://clients1.google.com/ocsp - DIRECT/173.194.41.6 application/ocsp-response
1401444788.496 73 127.0.0.1 TCP_MISS/200 906 POST http://clients1.google.com/ocsp - DIRECT/173.194.41.6 application/ocsp-response
1401444820.213 88 127.0.0.1 TCP_MISS/200 724 GET http://www.google.es/url? - DIRECT/173.194.34.247 text/html
1401444820.395 23 127.0.0.1 TCP_MISS/200 1512 GET http://www.google.es/favicon.ico - DIRECT/173.194.34.247 image/x-icon
1401444820.482 216 127.0.0.1 TCP_MISS/200 9313 GET http://www.ugr.es/ - DIRECT/150.214.204.25 text/html
1401444820.615 163 127.0.0.1 TCP_MISS/200 17565 GET http://www.ugr.es/css/8ecc84c9b2f0f8af6c9f3433bcb4f4b5.css - DIRECT/150.214.204.25 text/css
1401444820.699 239 127.0.0.1 TCP_MISS/200 49333 GET http://www.ugr.es/cjs/676152f0080a3385e8eda8822b978952.js - DIRECT/150.214.204.25 application/javascript
1401444820.709 257 127.0.0.1 TCP_MISS/200 34078 GET http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js - DIRECT/173.194.66.95 text/javascript
1401444820.761 42 127.0.0.1 TCP_MISS/200 1382 GET http://www.ugr.es/img/favicon.ico - DIRECT/150.214.204.25 image/vnd.microsoft.icon
1401444820.764 304 127.0.0.1 TCP_MISS/200 61273 GET http://ajax.googleapis.com/ajax/libs/jqueryui/1.10.3/jquery-ui.min.js - DIRECT/173.194.66.95 text/javascript
1401444821.520 42 127.0.0.1 TCP_MISS/200 807 GET http://www.ugr.es/img/general/facebook_head-off.png - DIRECT/150.214.204.25 image/png
1401444821.521 43 127.0.0.1 TCP_MISS/200 862 GET http://www.ugr.es/img/general/twitter_head-off.png - DIRECT/150.214.204.25 image/png
1401444821.566 44 127.0.0.1 TCP_MISS/200 642 GET http://www.ugr.es/img/general/destacados-cabecera_fondo.png - DIRECT/150.214.204.25 image/png
1401444821.566 88 127.0.0.1 TCP_MISS/200 1379 GET http://www.ugr.es/img/general/accesibilidad-head-off.png - DIRECT/150.214.204.25 image/png
1401444821.567 46 127.0.0.1 TCP_MISS/200 907 GET http://www.ugr.es/pages/_inicio/!/images - DIRECT/150.214.204.25 application/javascript
1401444821.571 278 127.0.0.1 TCP_MISS/200 16271 GET http://stats.g.doubleclick.net/dc.js - DIRECT/173.194.66.155 text/javascript
1401444821.576 96 127.0.0.1 TCP_MISS/200 2138 GET http://www.ugr.es/img/general/cabecera-elvira_off.png - DIRECT/150.214.204.25 image/png
1401444821.579 96 127.0.0.1 TCP_MISS/200 650 GET http://www.ugr.es/img/general/cabecera-menu_servicios-biblioteca.png - DIRECT/150.214.204.25 image/png
1401444821.580 95 127.0.0.1 TCP_MISS/200 624 GET http://www.ugr.es/img/general/menu-item_off.png - DIRECT/150.214.204.25 image/png
1401444821.580 98 127.0.0.1 TCP_MISS/200 735 GET http://www.ugr.es/img/general/cabecera-language-es_off.png - DIRECT/150.214.204.25 image/png
1401444821.583 102 127.0.0.1 TCP_MISS/200 2421 GET http://www.ugr.es/img/general/cabecera-biotic_off.png - DIRECT/150.214.204.25 image/png
1401444821.584 101 127.0.0.1 TCP_MISS/200 664 GET http://www.ugr.es/img/general/cabecera-menu_servicios-correo.png - DIRECT/150.214.204.25 image/png
1401444821.585 100 127.0.0.1 TCP_MISS/200 624 GET http://www.ugr.es/img/general/menu-otros_off.png - DIRECT/150.214.204.25 image/png
1401444821.585 101 127.0.0.1 TCP_MISS/200 648 GET http://www.ugr.es/img/general/cabecera-menu_perfiles-item_off.png - DIRECT/150.214.204.25 image/png
1401444821.589 101 127.0.0.1 TCP_MISS/301 711 GET http://www.ugr.es/pages/_banner/banner_mecenazgo/!/ - DIRECT/150.214.204.25 text/html
1401444821.590 107 127.0.0.1 TCP_MISS/200 650 GET http://www.ugr.es/img/general/cabecera-menu_servicios-acceso.png - DIRECT/150.214.204.25 image/png

```