

## Lab 10. Servei DNS

### Objectiu:

- Aplicar el disseny de les xarxes de les practiques anteriors amb un servidor DNS.
- Configurar un servidor primari responsable de varies zones.

### Que farem:

- Configurarem un servidor DNS a la maquina que fa de Router, de manera que a cap maquina ja no caldrà mai més modificar el fitxer /etc/hosts
- Adequarem la configuració del servidor DHCP per a que proporcioni als seus clients la informació del nou servei.

### Lliurament:

- A la tasca del moodle hi penjarem un fitxer anomenat `gsx9_cognom1a_cognom1b.tgz` que contingui:
  - o Un pdf amb els scripts amb la sintaxi en color, els fitxers de configuració principals en color i les sortides txt de les proves realitzades.
  - o Els scripts
  - o Tots els fitxers de configuració

### Anem a per feina:

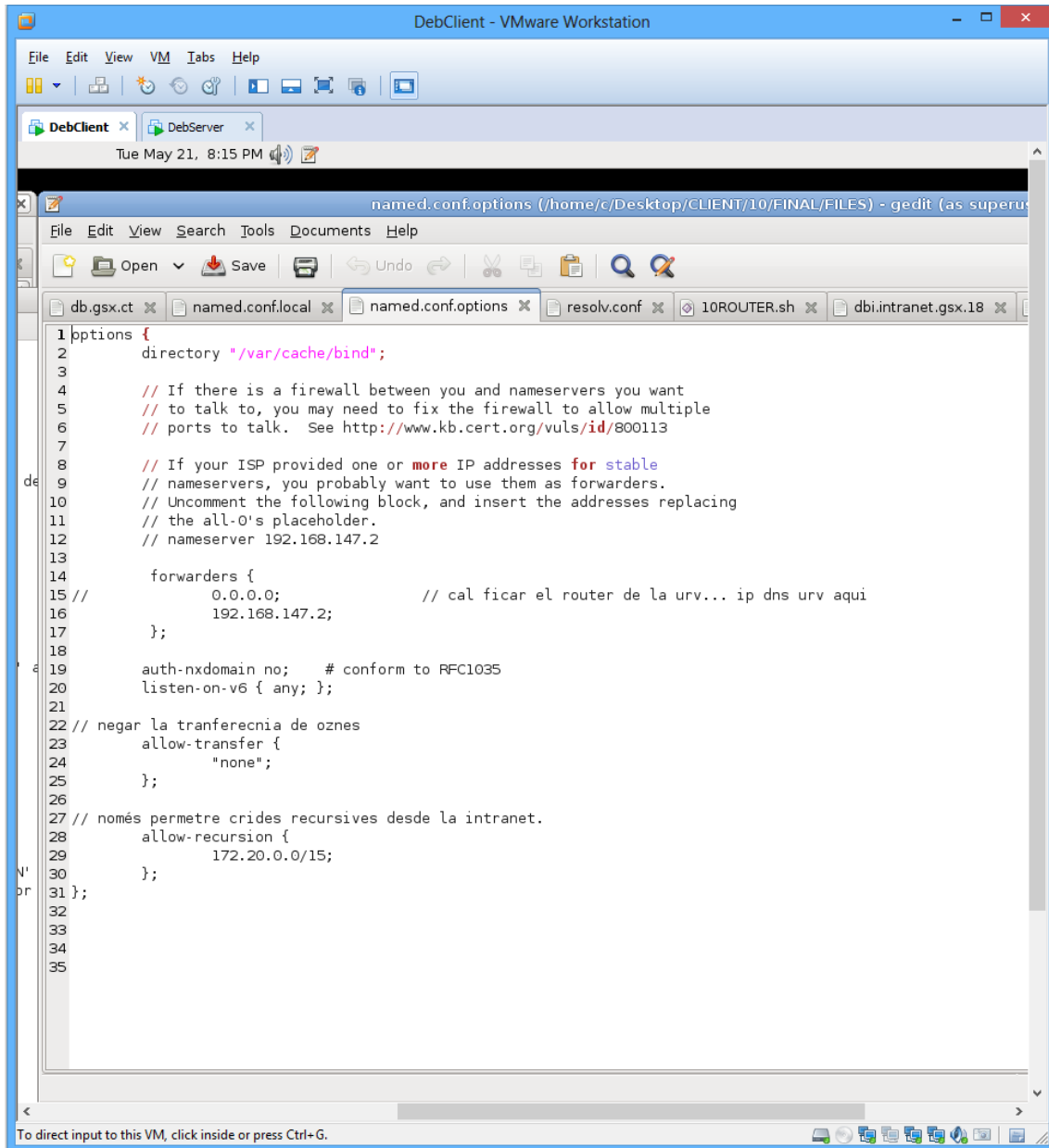
- Continuem amb la mateixa topologia que la pràctica 9.

## ROUTER

- Matem la configuració automàtica per a que no ens sobreescrigui la nostra.
- Activem el Routing, la SNAT, la DNAT i el DHCP al PC de l'esquerra.
- Comprovem que tenim els paquets bind9, bind9-doc i dnsutils.
- Configurem els servidors DNS:
  - o Editem el fitxer /etc/bind/Named.conf.local
  - o Hi afegim dues zones, una per gsx.ct i una per intranet.gsx
    - Db.gsx.general
    - Dbi.gsx.general
  - o Hi afegim 3 zones inverses.
    - Db.intranet.gsx
    - Dbi.intranet.gsx.20
    - Dbi.intranet.gsx.18

```
10
11 ///////////////////////////////////////////////////////////////////
12 // zona per la DMZ // ZONA 1 //
13 // ZONA DMZ
14 zone "gsx.ct" {
15     type master;
16     file "/etc/bind/db.gsx.ct";
17 };
18 // ZONA DMZ REVERSE
19 zone "1.168.192.in-addr.arpa" {
20     type master;
21     file "/etc/bind/dbi.gsx.general";
22 };
23
24
25
26
27 ///////////////////////////////////////////////////////////////////
28 // zona per les INTRANETS // ZONA 2 //
29 // ZONA INTRANET
30 zone "intranet.gsx" {
31     type master;
32     file "/etc/bind/db.intranet.gsx";
33 };
34
35 // ZONA INTRANET REVERSE
36 zone "20.172.in-addr-arpa" {
37     type master;
38     file "/etc/bind/dbi.intranet.gsx.20";
39 };
40 // ZONA INTRANET REVERSE
41 zone "18.172.in-addr-arpa" {
42     type master;
43     file "/etc/bind/dbi.intranet.gsx.18";
44 };
45 //
46 //Resposta: Perquè a la intranet hem fet subnetting i el Bind no li va bé el subnetting que no estigui alineat.
47 //màscares: /8 /16 i /24).
48 //Al nostre cas, les dues màquines:
```

- Editem el fitxer d'opcions globals, posant el forwarding dels quèries desconeguts cap al servidor DNS del ISP (URV), no permetem les transferències de zona i sols permetem els quèries recursius des de la intranet dels usuaris.



```
1 options {
2     directory "/var/cache/bind";
3
4     // If there is a firewall between you and nameservers you want
5     // to talk to, you may need to fix the firewall to allow multiple
6     // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
7
8     // If your ISP provided one or more IP addresses for stable
9     // nameservers, you probably want to use them as forwarders.
10    // Uncomment the following block, and insert the addresses replacing
11    // the all-0's placeholder.
12    // nameserver 192.168.147.2
13
14    forwarders {
15        // 0.0.0.0;           // cal ficar el router de la urv... ip dns urv aqui
16        192.168.147.2;
17    };
18
19    auth-nxdomain no;    # conform to RFC1035
20    listen-on-v6 { any; };
21
22    // negar la tranferencia de zones
23    allow-transfer {
24        "none";
25    };
26
27    // només permetre crides recursives desde la intranet.
28    allow-recursion {
29        172.20.0.0/15;
30    };
31 };
32
33
34
35
```

- Editem els fitxers de zona:
  - o Cada zona ha de definir un RR NS amb la IP que té el Router en aquella zona.
  - o Per a les webs visibles des de l'exterior s'ha de retornar la IP externa del Router (d'acord amb la DNAT).
  - o Per a la intranet poseu diverses maquines fictícies (per exemple PC3.intranet.gsx.ct).
  - o Afegiu uns servidors de correu fictícies
    - RR MX correu.gsx.ct
    - Smtip i pop3 com a alies
      - No funciona.
- Comprovar les sintaxis amb les eines
  - o Named-checkzone
  - o Named-checkconf

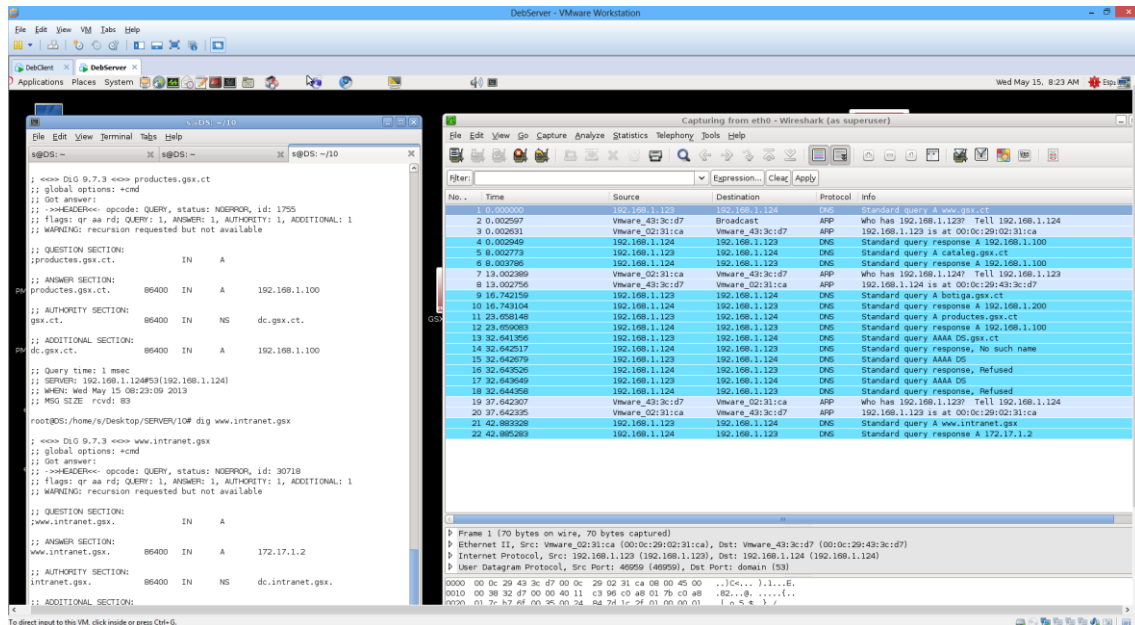
```

c@dc: ~/10/FINAL
File Edit View Terminal Help
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): ncache_message
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): clone_results
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): cancelquery
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): done
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): stopeverything
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): cancelqueries
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): sendevents
1-May-2013 20:22:56.645 fctx 0x7ff722cc5430(dc/AAAA'): destroyfctx
c@dc: /etc/bind
File Edit View Terminal Tabs Help
c@dc: /etc/bind
root@dc:/etc/bind# named-checkzone www.gsx.ct db.gsx.ct
zone www.gsx.ct/IN: loaded serial 2405201301
OK
root@dc:/etc/bind# named-checkzone cataleg.gsx.ct db.gsx.ct
zone cataleg.gsx.ct/IN: loaded serial 2405201301
OK
root@dc:/etc/bind# named-checkzone www.intranet.gsx db.intranet.gsx
zone www.intranet.gsx/IN: loaded serial 2405201303
OK
root@dc:/etc/bind# named-checkconf -z named.conf.local
zone gsx.ct/IN: loaded serial 2405201301
zone 1.168.192.in-addr.arpa/IN: loaded serial 2405201304
zone intranet.gsx/IN: loaded serial 2405201303
zone 20.172.in-addr.arpa/IN: loaded serial 2405201308
zone 18.172.in-addr.arpa/IN: loaded serial 2405201306
root@dc:/etc/bind#
  
```

To direct input to this VM, click inside or press Ctrl+G.

- Engueuem el servei, però no com a dimoni, sino per a depurar-lo.
  - o Named -u bind -4 -f -g -d 3

- Comprovem la sortida ( que carregui bé totes les zones ) i provem alguns quèries.
- Ara sí, engeguem el servei com a daemon, i mirem els logs.
- Engueguem el Wireshark per a capturar els paquets DNS.



## CLIENTS/INTRANET/DMZ/SERVIDOR

- Re-configurar el servei DHCP per a que proporcioni la informació de nom, domini i l'adreça del servidor de noms per a cada subxarxa.
- Re-enguegem els clients (per DHCP)

```
root@DI:/home/i/Desktop/INTRANET/10# host cataleg.gsx.ct
cataleg.gsx.ct has address 192.168.1.100
root@DI:/home/i/Desktop/INTRANET/10# w3m www.gsx.ct
root@DI:/home/i/Desktop/INTRANET/10# w3m 192.18.1.100

[4]+  Stopped                  w3m 192.168.1.100
root@DI:/home/i/Desktop/INTRANET/10# w3m 192.168.1.200

[5]+  Stopped                  w3m 192.168.1.200
root@DI:/home/i/Desktop/INTRANET/10# more /etc/resolv.conf
domain intranet-client.ct
search intranet-client.ct
nameserver 172.20.0.2
root@DI:/home/i/Desktop/INTRANET/10# more /etc/hosts
127.0.0.1      localhost
127.0.1.1      DI
# 172.18.1.100 www.gsx.ct

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

No.	Time	Source	Destination	Protocol	Details
17641	4092.55164700	192.18.3.100	172.20.3.123	TCP	60 http > 51569 [RST, ACK]
17642	4095.37328900	172.20.3.123	192.168.1.100	TCP	74 49400 > http [SYN] Seq=0
17643	4095.37438600	192.168.1.100	172.20.3.123	TCP	74 http > 49400 [SYN, ACK] Seq=0
17644	4095.37460300	172.20.3.123	192.168.1.100	TCP	66 49400 > http [ACK] Seq=1
17645	4095.37478200	172.20.3.123	192.168.1.100	HTTP	307 GET / HTTP/1.0
17646	4095.37546500	192.168.1.100	172.20.3.123	TCP	66 http > 49400 [ACK] Seq=1
17647	4095.37674100	192.168.1.100	172.20.3.123	HTTP	448 HTTP/1.1 200 OK (text/html)
17648	4095.37681400	172.20.3.123	192.168.1.100	TCP	66 49400 > http [ACK] Seq=2
17649	4095.37689400	192.168.1.100	172.20.3.123	TCP	66 http > 49400 [FIN, ACK] Seq=1
17650	4095.37890900	172.20.3.123	192.168.1.100	TCP	66 49400 > http [FIN, ACK] Seq=1
17651	4095.37990500	192.168.1.100	172.20.3.123	TCP	66 http > 49400 [ACK] Seq=3
17652	4103.86926400	172.20.3.123	192.168.1.200	TCP	74 53421 > http [SYN] Seq=0
17653	4103.87481200	192.168.1.200	172.20.3.123	TCP	74 http > 53421 [SYN, ACK] Seq=0
17654	4103.87522800	172.20.3.123	192.168.1.200	TCP	66 53421 > http [ACK] Seq=1
17655	4103.87543800	172.20.3.123	192.168.1.200	HTTP	307 GET / HTTP/1.0
17656	4103.87625600	192.168.1.200	172.20.3.123	TCP	66 http > 53421 [ACK] Seq=1
17657	4103.87763700	192.168.1.200	172.20.3.123	HTTP	448 HTTP/1.1 200 OK (text/html)

## PROVES

- Comprovem que des de les tres màquines diferents( Router, intranet, DMZ i desde l'exterior ) que es serveixen:
  - o Els quèries directes locals i remots correctament

```
DeblIntranet - VMware Workstation
File Edit View VM Tabs Help
Applications Places
10INTRANET.sh (/home/i/Desktop/INTRANET/10) - gedit (as superuser)
File Edit View Search Tools Documents Help
i@DI: ~
File Edit View Search Terminal Help
;; Query time: 116 msec
;; SERVER: 172.20.0.2#53(172.20.0.2)
;; WHEN: Mon May 27 20:50:00 2013
;; MSG SIZE rcvd: 118
root@DI:/home/i/Desktop/INTRANET/10# dig www.gsx.ct
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.gsx.ct
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 42681
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.gsx.ct. IN A
;; ANSWER SECTION:
www.gsx.ct. 86400 IN A 192.168.1.100
;; AUTHORITY SECTION:
gsx.ct. 86400 IN NS dc.gsx.ct.
;; ADDITIONAL SECTION:
dc.gsx.ct. 86400 IN A 192.168.1.100
;; Query time: 1 msec
;; SERVER: 172.20.0.2#53(172.20.0.2)
;; WHEN: Mon May 27 20:50:56 2013
;; MSG SIZE rcvd: 77
root@DI:/home/i/Desktop/INTRANET/10#
17664 4233.3414170K 172.20.3.123 172.20.0.2 DNS 86 Standard query 0x68fd P
17665 4233.3427590K 172.20.0.2 172.20.3.123 DNS 197 Standard query response
17666 4238.3419210K VMware_43:3c:f5 VMware_89:95:28 ARP 60 Who has 172.20.3.123? T
17667 4238.3419540K VMware_89:95:28 VMware_43:3c:f5 ARP 42 172.20.3.123 is at 00:0c
17668 4346.0530000K 172.20.3.123 172.20.0.2 DNS 83 Standard query 0x0f5d P
17669 4346.1687060K 172.20.0.2 172.20.3.123 DNS 160 Standard query response
```



- Els quèries inversos locals i remots correctament

```
10INTRANET.sh (/home/i/Desktop/INTRANET/10) - gedit (as superuser)
File Edit View Search Tools Documents Help
Open Save Undo Redo
i@DI: ~
File Edit View Search Terminal Help
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@DI:/home/i/Desktop/INTRANET/10# nslookup
> qy^Z
[6]+ Stopped nslookup
root@DI:/home/i/Desktop/INTRANET/10# dig -x 192.168.1.100

;; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> -x 192.168.1.100
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 26877
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;100.1.168.192.in-addr.arpa. IN PTR

;; ANSWER SECTION:
100.1.168.192.in-addr.arpa. 86400 IN PTR www.productes.gsx.ct.
100.1.168.192.in-addr.arpa. 86400 IN PTR dc.gsx.ct.
100.1.168.192.in-addr.arpa. 86400 IN PTR www.gsx.ct.
100.1.168.192.in-addr.arpa. 86400 IN PTR www.cataleg.gsx.ct.

;; AUTHORITY SECTION:
1.168.192.in-addr.arpa. 86400 IN NS dc.

;; Query time: 2 msec
;; SERVER: 172.20.0.2#53(172.20.0.2)
;; WHEN: Mon May 27 20:48:07 2013
;; MSG SIZE rcvd: 155

root@DI:/home/i/Desktop/INTRANET/10#
```

17656 4103.87625600 192.168.1.200 172.20.3.123 TCP 66 http > 53421 [ACK] Seq=1

17657 4103.87763700 192.168.1.200 172.20.3.123 HTTP 448 HTTP/1.1 200 OK (text/h

17658 4103.87773600 192.168.1.200 172.20.3.123 TCP 66 http > 53421 [FIN, ACK] :

17659 4103.87781400 172.20.3.123 192.168.1.200 TCP 66 53421 > http [ACK] Seq=2

17660 4103.88025300 172.20.3.123 192.168.1.200 TCP 66 53421 > http [FIN, ACK] :

17661 4103.88143300 192.168.1.200 172.20.3.123 TCP 66 http > 53421 [ACK] Seq=2

- Sols es fan les transferències de zona des de loopback
  - Dig gsx.ct AXFR
- Sols es fan queris recursius des de la intranet
  - En el servidor no hi ha internet i en la intranet si.

The screenshot shows a VMware Workstation window with a single virtual machine named 'DebClient'. The VM is running a Linux operating system. The terminal window displays the following commands and output:

```

root@dc: ~/10/FINAL
[6]+ Stopped
root@dc:/home/c/Desktop:
bind9 is running.
root@dc:/home/c/Desktop:
Stopping domain name se
Starting domain name se
root@dc:/home/c/Desktop:

```

The file manager window shows the contents of the file '/home/c/Desktop/CLIENT/10/FINAL/named.conf.options'. The file contains the following configuration:

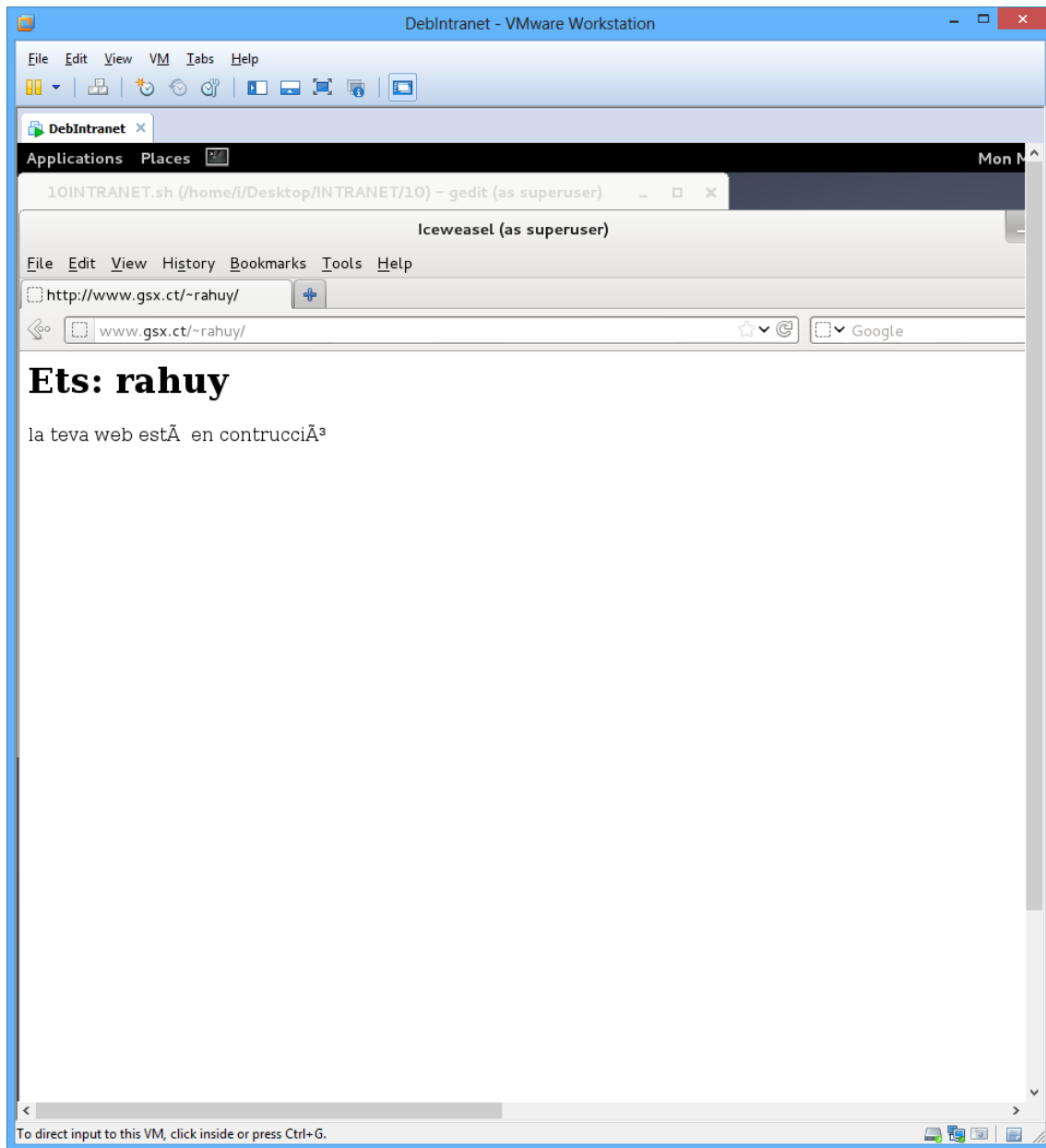
```

1 options {
2     directory "/var/cache/bind";
3
4     // If there is a firewall between you and nameservers you want
5     // to talk to, you may need to fix the firewall to allow multiple
6     // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
7
8     // If your ISP provided one or more IP addresses for stable
9     // nameservers, you probably want to use them as forwarders.
10    // Uncomment the following block, and insert the addresses replacing
11    // the all-0's placeholder.
12    // nameserver 192.168.147.2
13
14    forwarders {
15        0.0.0.0;           // cal ficar el router de la urv... ip dns urv
16        192.168.147.2;
17    };
18
19    auth-nxdomain no;      # conform to RFC1035
20    listen-on-v6 { any; };
21
22    // negar la tranferencia de oznes
23    allow-transfer {
24        "none";
25    };
26
27    // només permetre crides recursives desde la intranet.
28    allow-recursion {
29        172.20.0.0/15;
30    };
31 };
32
33
34
35

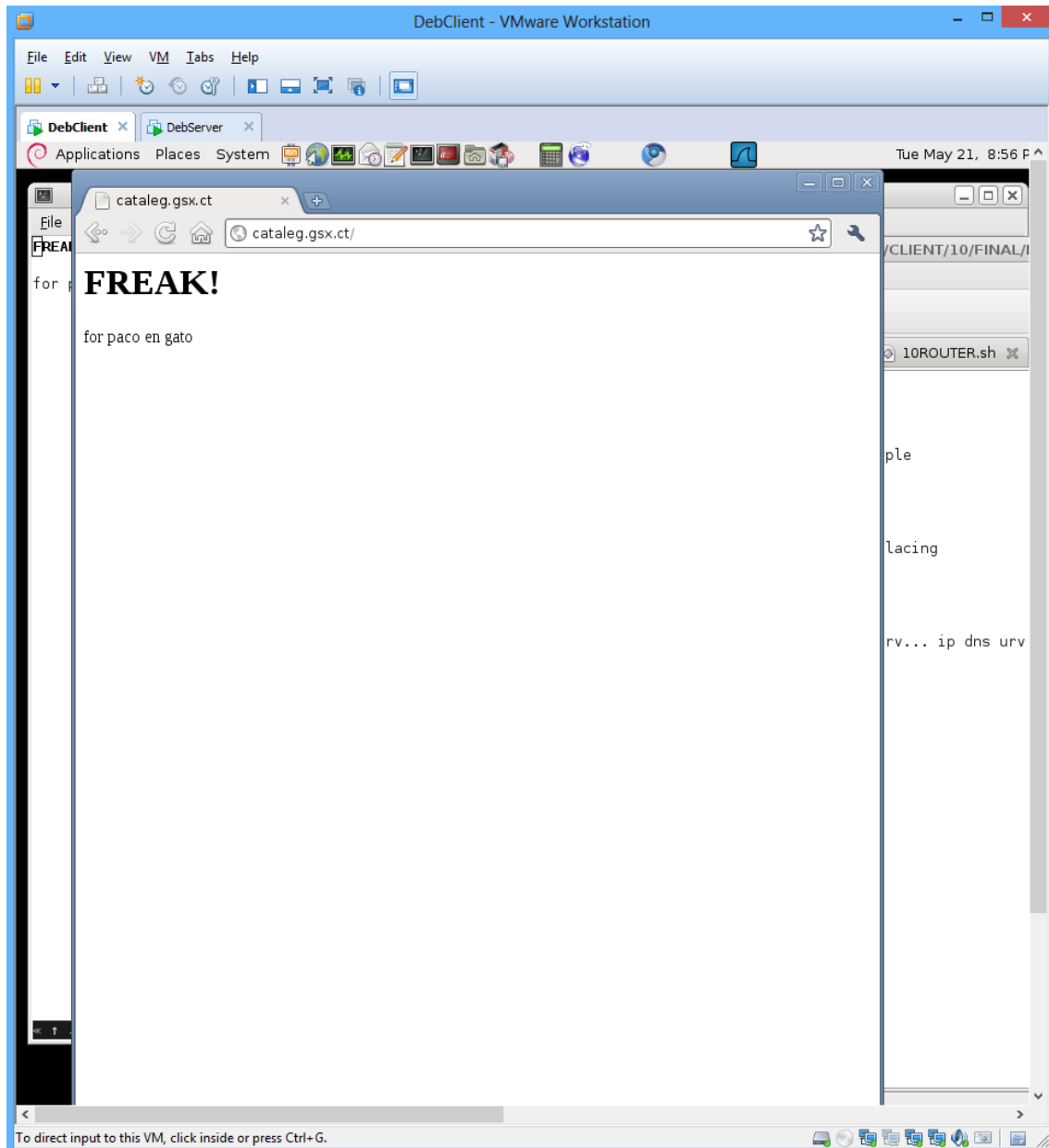
```

- Comprovem que els servidors web continuen operatius.

Desde la intranet:

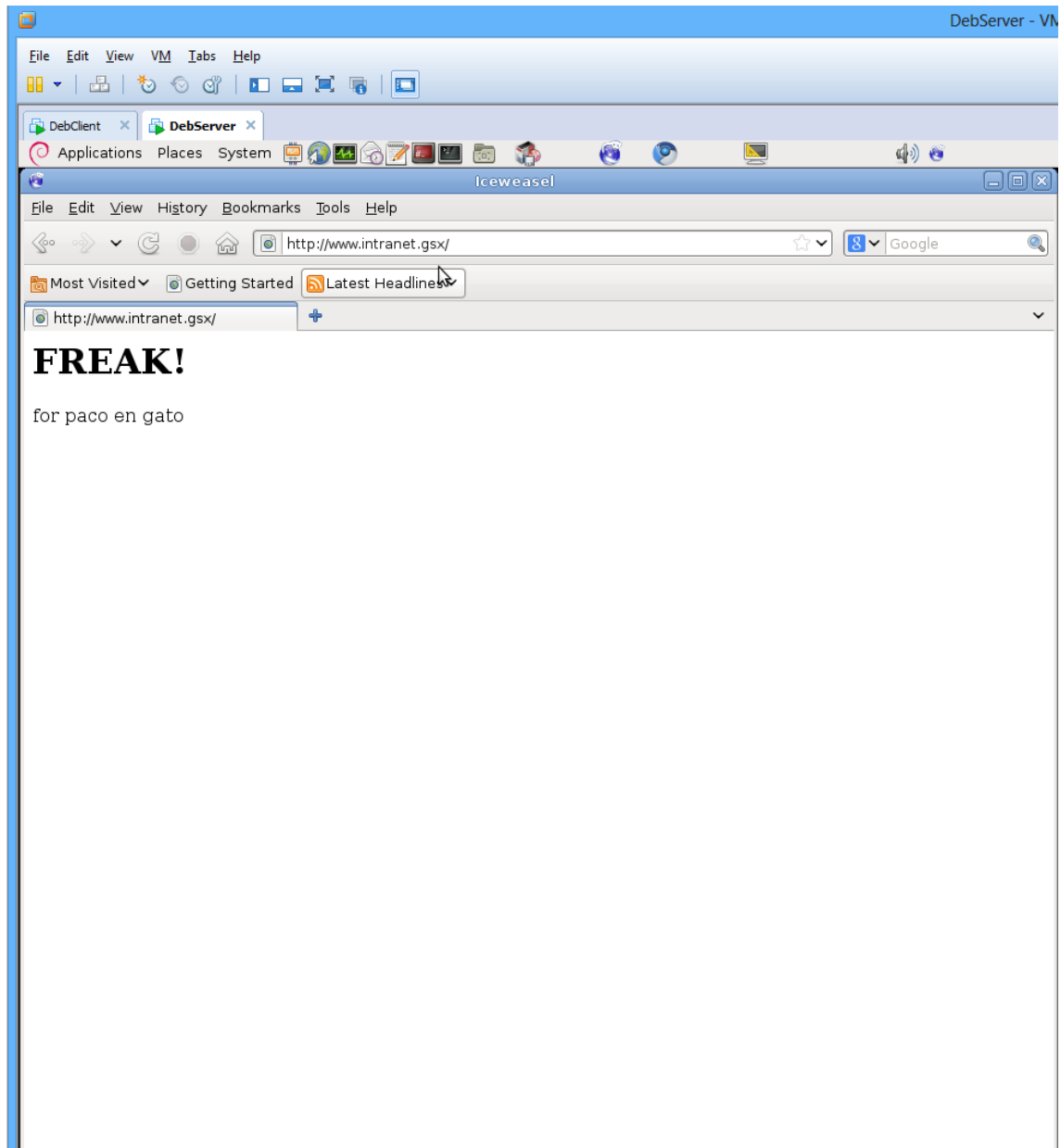


Desde el Router:



Sempre mostra la mateixa pàgina amb el mateix ip, hem tingut problemes de configuració per hosts per noms en la pràctica 8.

Desde el servidor:



Lo que queda per implementar:

- Mecànicament:
  - Pegar els scripts i fitxers de configuració and sintaxi color en aquest pdf
  - Adjuntar els fitxers de configuració principal amb un tar
  - Adjuntar el script en un amb el pdf i fitxers de configuració