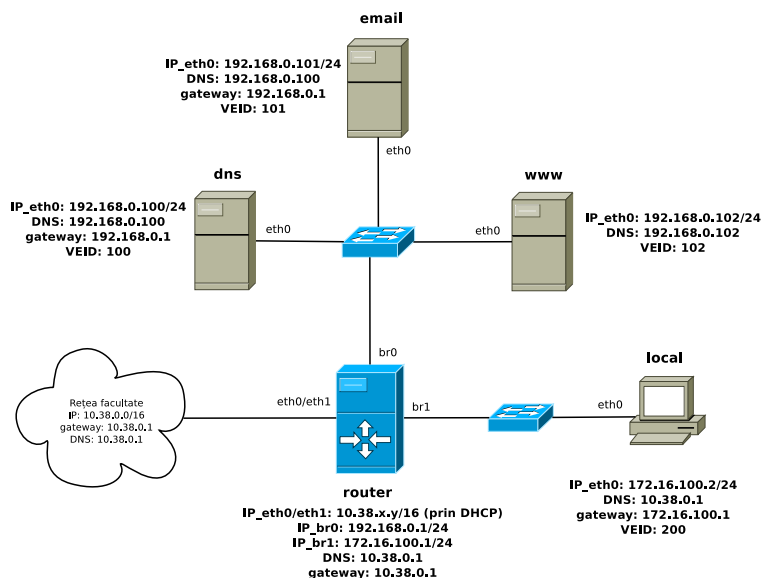


Test Practic RL – Simulare Varianta B, 12 decembrie 2010 Rezolvări



1. Rezolvare:

```
dns:/# ip a add 192.168.0.100/24 dev eth0
dns:/# ip r add 0.0.0.0/0 via 192.168.0.1
dns:/# echo "nameserver 192.168.0.100" > /etc/resolv.conf
email:/# ip a add 192.168.0.101/24 dev eth0
email:/# ip r add 0.0.0.0/0 via 192.168.0.1
email:/# echo "nameserver 192.168.0.100" > /etc/resolv.conf
www:/# ip a add 192.168.0.102/24 dev eth0
www:/# echo "nameserver 192.168.0.100" > /etc/resolv.conf
```

• Verificare:

```
ping (pentru a testa conectivitatea)
ip r show (pentru a vedea default gateway)
host -a test.ro (pe dns, www, email pentru a testa că a fost adăugat corect dns-ul)
nu trebuie folosit \texttt{host -a test.ro 192.168.0.100}
```

• Troubleshooting:

- Ping nu merge
 - Verificați interfețele eth0 să fie \texttt{up}
 - Nu dați /etc/init.d/networking restart pe stația \texttt{router}, interfețele br0 și br1 vor pica automat. Va trebui să le porniți în caz că acest lucru se întâmplă
 - Verificați adresele să nu fie ip/32 sau acestea să fie corect puse.
- Nu este setată bine default gateway în tabela de rutare
Ruta trebuie să arate ca și 'default via \$ip dev \$interfață'
- Nu merge interogarea serverului dns
 - Verificați configurarea din /etc/resolv.conf
 - Testați conectivitatea

2. Rezolvare:

```
sysctl -w net.ipv4.ip_forward=1
ip route add 172.16.100.0/24 via 192.168.0.1
```

- Verificare:


```
ip route list
ping 172.16.100.2
```
 - Troubleshooting:

Verificați conectivitatea între rețea_locală și router (Layer 2 & 3)
 Verificați conectivitatea între www și router (Layer 2 & 3)
 Verificați că este activată rutarea pe router
 Când adăugați o rută țineți minte că parametrul după add
 trebuie să fie un ip al unei stații(mască implicită /32) sau ip-ul unei subrețele
3. • Rezolvare:
- a)
- ```
router:/home/student# iptables -t nat -A POSTROUTING -o eth0
-j SNAT --to-source 10.38.217.63
router:/home/student# vim /etc/sysctl.conf
router:/home/student# sysctl -p
net.ipv4.ip_forward = 1

retea_locala:/# ip r a 0.0.0.0/0 via 172.16.100.1
```
- b)
- ```
router:/home/student# iptables -t nat -A PREROUTING -i eth0
-d 10.38.217.63 -p tcp --dport 25
-j DNAT --to-destination 192.168.0.101:25
```
- Verificare:

a)

```
retea_locala:/# ip r s
172.16.100.0/24 dev eth0 proto kernel scope link src 172.16.100.2
default via 172.16.100.1 dev eth0
retea_locala:/# ping google.com
merge
```

b)

```
router:/# iptables -t nat -nL
router:/# telnet 10.38.217.63 25
```
 - Troubleshooting:

a)

Verificați dacă interfețele sunt pornite pe stațiile router și rețea locală
 Verificați dacă aveți rutarea activată și că pe rețea locală aveți ca default
 gateway ip-ul de pe interfața br1, de pe stația router
 Regula adăugată trebuie să fie în tabela nat pe lanțul POSTROUTING, ca interfață
 de output eth0, iar ip-ul translatat să fie cel de pe interfața eth0

b)

Verificați conectivitatea cu stația email.
 Verificați pe stația email că serverul postfix ascultă pe portul 25.

```
email:/# netstat -tlnp | grep 25
```
4. • Rezolvare:
- a)
- ```
router:/home/student# iptables -t filter -A FORWARD -p icmp
-s 192.168.0.100 -d 172.16.100.2 --icmp-type 8
-j ACCEPT
router:/home/student# iptables -t filter -A FORWARD -p icmp
-d 192.168.0.100 -s 172.16.100.2 --icmp-type 0
-j ACCEPT
router:/home/student# iptables -t filter -P FORWARD -j DROP
```
- b)
- ```
router:/home/student# iptables -t mangle -A FORWARD -p icmp
-s 172.16.100.2 -d 192.168.0.100 --icmp-type 0
-j TTL --ttl-inc 20
```

- Verificare:

```
a)
dns:/# ping $ip_rețea_locală
merge
rețea_locala:/# ping $ip_dns
nu merge
b)
dns:/# ping $ip_rețea_locală
ttl se modifică la valoare + 20
```

- Troubleshooting:

```
a)
Regula trebuie pusă în tabela filter pe lanțul FORWARD
Grijă mare la pachetele icmp (0 - echo request și 8 - echo reply)
b)
Folosiți tabelul mangle pentru orice modificări aduse informațiilor din pachetele IP
--ttl-inc și nu --ttl-set, în enunț se specifică "...incrementați valoarea câmpului TTL..."
```

5. • Rezolvare:

```
dns:/# vim /etc/bind/external/db.192.168.0
$ORIGIN 0.168.192.in-addr.arpa.
$TTL 604800
@ IN SOA lab.edu. lab.edu. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS lab.edu.

1 IN PTR gw.lab.edu.
100 IN PTR ns.lab.edu.
101 IN PTR mail.lab.edu.
102 IN PTR www.lab.edu.
```

```
dns:/# vim /etc/bind/named.conf.local
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/external/db.192.168.0";
};
```

- Verificare:

```
host -t PTR 192.168.0.100 $ip_dns
host -t PTR 192.168.0.101 $ip_dns
host -t PTR 192.168.0.102 $ip_dns
host -t PTR 192.168.0.1 $ip_dns
```

- Troubleshooting:

```
Nu merge host:
a) A fost repornit serviciul după configurări?
b) dns:/# named-checkconf /etc/bind/named.conf
- Verificare dacă fișierele de configurare sunt corecte,
named.conf conține named.conf.local și named.conf.options
c) dns:/# named-checkzone 0.168.192.in-addr.arpa /etc/bind/db.192.168.0
- Verificare dacă zona pretest.edu este configurată corect
d) Verificați fișierele named.conf.local, poate ați pus incorect calea
pentru fișierul de zonă sau numele zonei este incorect
```

6. • Rezolvare:

```
dns:/# vim /etc/bind/named.conf.local
zone "rumble.org" IN {
```

```
type forward;
forwarders { 192.168.0.102; };
};
```

- Verificare:

```
email:/# host -t A ftp.rumble.org
```

- Troubleshooting:

```
Verificați conectivitatea între router, dns, email, www.
Verificați dacă există setat bine nameserver-ul pe stația
de pe care dați comanda host, în caz că nu ați dat ca și
parametru serverul de interogare
dns:/# named-checkconf /etc/bind/named.conf
```

7. • Rezolvare:

```
email:/# vim /etc/postfix/main.cf
mydestination = email, localhost.localdomain, localhost, rumble.org
home_mailbox = Maildir/
```

```
email:/# adduser corina
corina@email:~$ maildirmake Maildir/
email:/# chown -R mailbox:mail /home/corina/Maildir/
```

- Verificare:

```
email:/# mailx -s test corina@rumble.org
corina@email:~/Maildir/new$ cat fisier_mail
```

- Troubleshooting:

```
Nu se primește mail:
a) Serviciul a fost restartat după realizarea configurărilor?
b) Fișierul /etc/postfix/main.cf conține erori?
c) Nu există drepturi setate bine pe /home/$username/Maildir
```

8. • Rezolvare:

```
a)
router:/home/student/# adduser paul
router:/home/student/# adduser roxana
router:/home/student/# adduser tudor
router:/home/student/# adduser sorina
```

```
b)
retea_locala:/# su student
student@retea_locala:/$ ssh-keygen
```

```
student@retea_locala:/$ ssh-copy-id -i ~/.ssh/id_rsa.pub paul@172.16.100.1
student@retea_locala:/$ ssh-copy-id -i ~/.ssh/id_rsa.pub roxana@172.16.100.1
student@retea_locala:/$ ssh-copy-id -i ~/.ssh/id_rsa.pub tudor@172.16.100.1
student@retea_locala:/$ ssh-copy-id -i ~/.ssh/id_rsa.pub sorina@172.16.100.1
```

```
c)
router:/# vim /etc/ssh/sshd_config
DenyUsers sorina
DenyUsers tudor
```

- Verificare:

```
a)
ls /home/
b)
paul@retea_locala:/$ ssh student@172.16.100.1
..
```

```
c)
sorina@retea_locala:/$ ssh student@172.16.100.1
nu merge
tudor@retea_locala:/$ ssh student@172.16.100.1
nu merge
```

- Troubleshooting:

```
b)
Rulează serviciul ssh pe 172.16.100.1:
router:/# netstat -tlnp | grep 22 ?
c)
Rulează serviciul ssh pe 172.16.100.1:
router:/# netstat -tlnp | grep 22 ?
Verificare fișier configurare dacă a fost adăugată
câte o directivă DenyUsers pentru sorina și tudor
```

9. • Rezolvare:

```
a)
vim /etc/ssh/sshd_config
Port 2222

b)
student@router:$ ssh-keygen -t dsa
student@router:$ scp /.ssh/*.pub student@$ip_router:
student@router:$ ssh student@$ip_router
student@dns:$ mkdir .ssh
student@dns:$ touch .ssh/authorized_keys
student@dns:$ cat id_dsa.pub >> .ssh/authorized_keys

sau

ssh-copy-id -i /student/.ssh/id_dsa.pub student@$ip_router
```

- Verificare:

```
a) netstat -tlnp
b) student@router:$ ssh student@$ip_dns -p 2222 -i /.ssh/id_dsa
```

- Troubleshooting:

```
a)
Ați restartat serviciul după modificări?
Rulează serviciul ssh pe 172.16.100.1:
router:/# netstat -tlnp | grep 22 ?
b)
Ați generat o cheie DSA, nu una RSA?
Conectați-vă la server folosind portul de curând modificat (2222)
```

10. • Rezolvare:

```
a) netstat -ulnp
b) ip route show
c) ip neigh show
d) iptables -t filter -nL
```

- Verificare:

```
a) netstat -ulnp
b) ip route show
c) ip neigh show
d) iptables -t filter -nL
```

- Troubleshooting:

```
man :)?
```