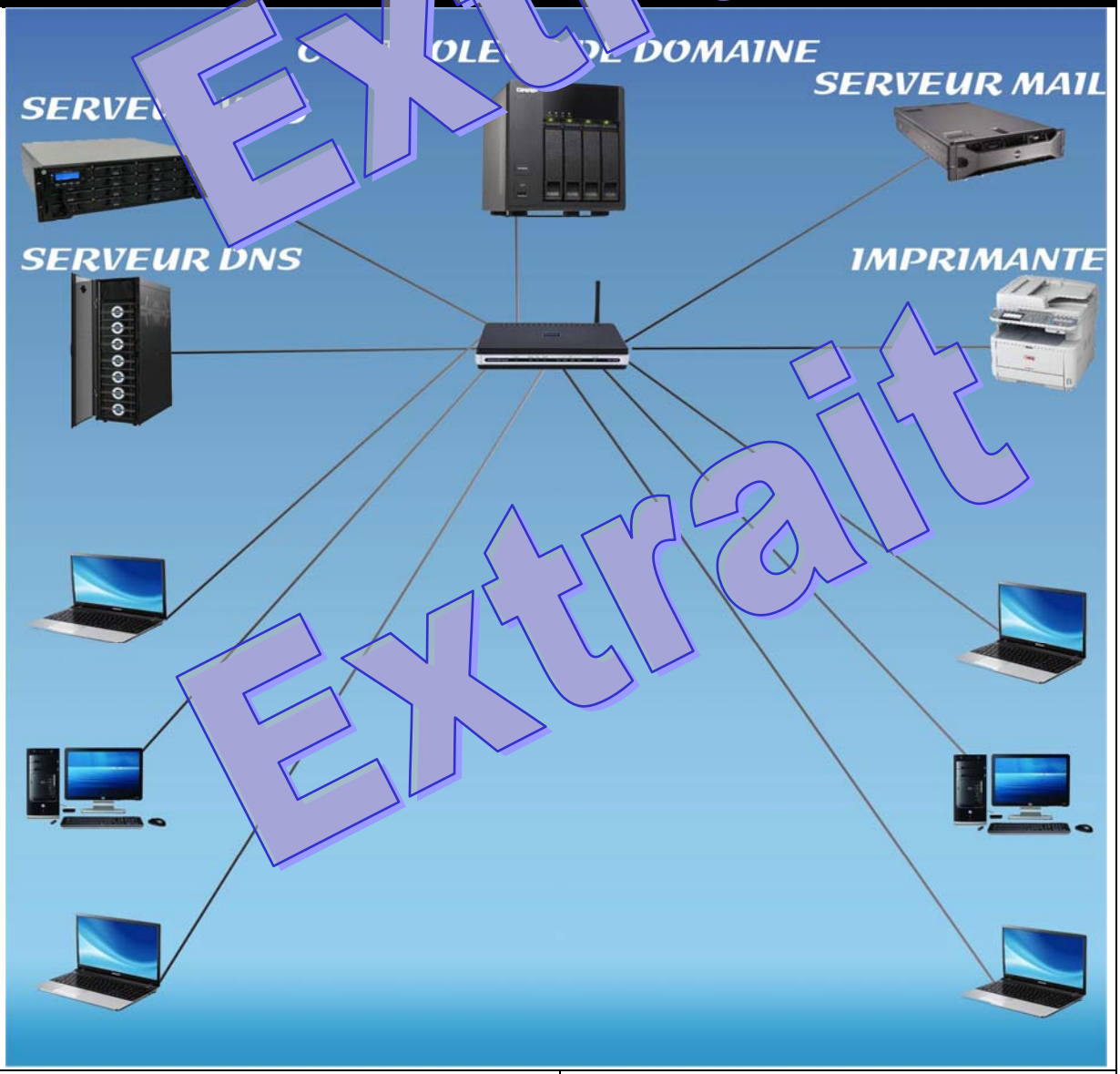
didalab
GÉNIE ÉLECTRIQUE

Projet Réseau DID@VDI+

- Contrôleur de domaine
- Résolution DNS
- Serveur Mail



Pré requis :

- Connaissance réseau (configuration carte, Switch, routeur). IP et Mask
- Notion client / serveur. Connexion ssh.
- Structure de Debian.
- Edition de fichiers (nano, vi, cat,…)

Matériel nécessaire :

- Laboratoire DIDAVDI+
- Station étudiante complète

Durée : 24 heures

Sommaire

8 TP3 : Mise en œuvre du serveur DNS

8.1.1 Named.conf

```
cd /etc/bind/
nano named.conf
```

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in
/etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

8.1.2 Named.options

```
nano /etc/bind/named.conf.options
```

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================$
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================$
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };

        #ecoute sur le port 53
        query-source address * port 53;
        #toutes les IPV4
        listen-on { any; };

};
```

8.1.3 Named.conf.local

```
nano /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if th are  use  your
// organization
//include "/etc/bind/zones.rfc1918";


//Zone DNS directe
zone "DIDAVDI.COM"  {
type mast ;
file "  ind/  DI  VDI.C
};

//Z
zone  .192.in-  .arpa" {
type  er;
file "  .DIDAVDI.COM.inv";
//allow  { key rndc-key; };
};
```

8.1.4 Fichier Zone Directe

```
 nano /etc/bind/db.DIDAVDI.COM
```

```
;
; BIND data file for local loopback interface
;
$TTL    60 ;MAJ mn
$ORIGIN DIDAVDI.COM.
@       IN      SOA     DI AVDI.CO  root    DI    M. (
                                2          Se
                                3          resh
                                0          ; Retry
                             2419          ; Expire
                              6048         ; Negative Cache TTL
;
@               NS      D AVDI.COM.             ; Notre domaine
; Service il gere  omatiquement pop/smtp/imap
@       IN              10 mx1.DIDAVDI.COM.
@       IN      A       192.168.1.91                ;Notre IP
mx1     IN      A       192.168.1.91                ;IP du service
mail

;**Service supplémentaires
www     IN      A       192.168.1.91 ; Apache, site web

;**PCs client
ServeurEtudiant IN      A       192.168.1.91
PCClientDidaVDI IN      A       192.168.1.2
ge-labo2        IN      A       192.168.1.21
ge-labo-2       IN      A       192.168.1.66
ge-labo         IN      A       192.168
```

8.1.5 Fichier Zone Inverse

nano /etc/bind/db.DIDAVDI.COM.inv

```
;
; BIND reverse data file for local loopback interface
;
$TTL 60
;$ORIGIN 1.168.192.in-addr.arpa.
@       IN      SOA     DIDAVDI.COM. root.DIDAVDI.[illegible]    (
                              1         ; [illegible]
                            900         ; [illegible] (15
                             60         ; Retry [illegible]n)
                           604800       ; Expire [illegible] semaine)
                           4[illegible] ; Negative Cache TTL (12 heures)


@       [illegible]     NS      [illegible]DAVDI.[illegible]M.
91      PTR     [illegible]DAVDI.[illegible]


;** Apach[illegible]
91      PT[illegible]      [illegible]DIDAVDI.COM.

;**mail
91      PTR     mail.DIDAVDI.COM.
91      PTR     pop.DIDAVDI.COM.
91      PTR     imap.DIDAVDI.COM.
91      PTR     smtp.DIDAVDI.COM.

;**Poste client
91      PTR     ServeurEtudiant.DIDAVDI.COM.
211     PTR     PCClientDidaVDI.DIDAVDI.COM.
21      PTR     ge-labo2.DIDAVDI.COM.
66      PTR     ge-labo-2.DIDAVDI.COM.
65      PTR     ge-labo.DIDAVDI.COM.
```

8.1.6 Redémarrage de bind9

```
=============== Verification des fichiers conf ================
root@ServeurEtudiant:~# named-checkconf  /etc/bind/named.conf
root@ServeurEtudiant:~# named-checkconf  /etc/bind/named.conf.local
root@ServeurEtudiant:~# named-checkconf
/etc/bind/named.conf.options
root@ServeurEtudiant:~#

=============== Verification des fichiers zone ================
root@ServeurEtudiant:~# named-checkzone DIDAVDI /etc/bind/db.DIDAVDI.COM
zone DIDAVDI.COM/IN: loaded serial
OK
root@ServeurEtudiant:~# named-checkzone DIDAVDI /etc/bind/db.DIDAVDI.COM.inv
zone DIDAVDI/IN: loaded serial 1
OK
root@ServeurEtudiant:~#

============ Verification fichier resolv.conf =============== coté serveur et
client
root@ServeurEtudiant:~# chattr -i /etc/resolv.conf
root@ServeurEtudiant:~# nano /etc/resolv.conf
               search DIDAVDI.COM
               nameserver 127.0.0.1
               nameserver 192.168.1.91
               #nameserver 80.1.168.192.246.2
               #nameserver 212.27.40.241
root@ServeurEtudiant:~# chattr +i /etc/resolv.conf

=============== Démarrage de bind9 ================
root@ServeurEtudiant:~# /etc/init.d/bind restart
[....] Stopping domain name service... bind9 (pid 3742) waiting for pid 3742 to
die
. ok
[ ok ] Starting domain name service... : bind9.

=============== vérification du fichier de log ==============
root@ServeurEtudiant:~# tail -10 /var/log/syslog
Oct  9 17:01:44 ServeurEtudiant named[4860]: command channel listening on 127.0.0.1#953
Oct  9 17:01:44 ServeurEtudiant named[4860]: command channel listening on ::1#953
Oct  9 17:01:44 ServeurEtudiant named[4860]: zone 0.in-addr.arpa/IN: loaded serial 1
Oct  9 17:01:44 ServeurEtudiant named[4860]: zone 1.168.192.in-addr.arpa/IN: loaded serial 1
Oct  9 17:01:44 ServeurEtudiant named[4860]: zone 127.in-addr.arpa/IN: loaded serial 1
Oct  9 17:01:44 ServeurEtudiant named[4860]: zone 255.in-addr.arpa/IN: loaded serial 1
Oct  9 17:01:44 ServeurEtudiant named[4860]: zone DIDAVDI.COM/IN: loaded serial 1
Oct  9 17:01:44 ServeurEtudiant named[4860]: zone localhost/IN: loaded serial 2
Oct  9 17:01:44 ServeurEtudiant named[4860]: managed-keys-zone ./IN: loaded serial 5
Oct  9 17:01:44 ServeurEtudiant named[4860]: running
root@ServeurEtudiant:~#
```

8.2 Vérification

8.2.1 Requêtes DIG

```
# Test sur une zone
root@ServeurEtudiant:/etc/bind# dig any DIDAVDI.COM
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> any DIDAVDI.CO
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, A
;; QUESTION SECTION:
;DIDAVDI.COM.                   NY

;; ANSWER SECTION:
DIDAVDI.COM
604800 6
DIDAV
DIDAVD
DIDAVDI.                        IN      A       192.168.1.91

;; ADDITI
DIDAVDI.CO              86400   IN      A       192.168.1.91
mx1.DIDAVDI             86400   IN      A       192.168.1.91

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Oct 11 10:33:17 2013
;; MSG SIZE  rcvd: 152
```

```
# Récupération de l'enregistrement SOA d'une zone
root@ServeurEtudiant:/etc/bind# dig soa DIDAVDI.COM
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> soa DIDAVDI.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, A
;; QUESTION SECTION:
;DIDAVDI.COM.                   IN      A

;; ANSWER SECTION:
DIDAVDI.COM.
604800 864
;; A
DIDAV
;; ADDI
DIDAVDI.                86400   IN      A       192.168.1.91

;; Query t
;; SERVER:
;; WHEN: Fri Oct 11 10:33:31 2013
;; MSG SIZE  rcvd: 100
```

```
#Vérification de la résolution de nom sur notre zone
root@ServeurEtudiant:/etc/bind# dig www.DIDAVDI.COM

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.DIDAVDI.COM
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 609
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDI    L: 1

;; QUESTION SECTION:
;www.DIDAVDI.COM.               IN      A

;; ANSWER SECTION:
www.DIDAVDI.COM.        86400   IN      A       192.168.1.91

;; AUTHORITY SECTION:
DIDAVDI.COM.            8640    IN      NS      DIDAVDI.COM.

;; ADDITIONAL SECTION:
DIDAVDI.COM.            86400   IN      A       192.168.1.91

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 15 15:17:17 2013
;; MSG SIZE  rcvd: 58
```



```
# Vérification de la résolution de nom inverse.

root@ServeurEtudiant:/etc/bind# dig ptr 211.1.168.192.in-addr.arpa

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> ptr 211.1.168.192.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48928
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
211.1.168.192.in-addr.arpa. 604800 IN   PTR     PC-ClientDidaVDI.DIDAVDI.COM.

;; AUTHORITY SECTION:
1.168.192.in-addr.arpa.         604800  IN      NS      DIDAVDI.COM.

;; ADDITIONAL SECTION:
DIDAVDI.COM.            86400   IN      A       192.168.1.91

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 15 15:36.40 2013
;; MSG SIZE  rcvd: 111
```


Toutes les requêtes dig ont abouties

`;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48928`

Et on visualise le serveur qui nous a répondu (`;; ANSWER SECTION:`) ainsi que le serveur maitre de la zone (`;; AUTHORITY SECTION:`) qui est bien celui mis en place par nos soins puisqu'il s'agit de l'IP de notre serveur DIDAVDI.COM

8.2.2 Requêtes nslookup

```
root@PCClientDidaVDI:~# nslookup
> DIDAVDI.COM
Server:         192.168.1.91
Address:        192.168.1.91#53

Name:   DIDAVDI.COM
Address: 192.168.1.91
> 192.168.1.1
Server:         192.168.1.91
Address:        192.168.1.91#53

1.1.168.192.in-addr.arpa        name = www.DIDAVDI.COM.
1.1.168.192.in-addr.arpa        name = imap.DIDAVDI.COM.
1.1.168.192.in-addr.arpa        name = mail.DIDAVDI.COM.
1.1.168.192.in-addr.arpa        name = smtp.DIDAVDI.COM.
1.1.168.192.in-addr.arpa        name = DIDAVDI.COM.
1.1.168.192.in-addr.arpa        name = ServeurEtudiant.DIDAVDI.COM.
1.1.168.192.in-addr.arpa        name = pop.DIDAVDI.COM.
> 192.168.1.211
Server:         192.168.1.91
Address:        192.168.1.91#53

24.1.168.192.in-addr.arpa       name = PCClientDidaVDI.DIDAVDI.COM.
> ServeurEtudiant
Server:         192.168.1.91
Address:        192.168.1.91#53

Name:   ServeurEtudiant.DIDAVDI.COM
Address: 192.168.1.91
> PCClientDidaVDI
Server:         192.168.1.91
Address:        192.168.1.91#53

Name:   PCClientDidaVDI.DIDAVDI.COM
Address: 192.168.1.211
> exit

root@PCClientDidaVDI:~#
```


Le PCClient a bien pris en compte notre serveur DNS puisque nslookup nous retrace directement les noms des machines par leur IP.

8.2.3 Requêtes ping

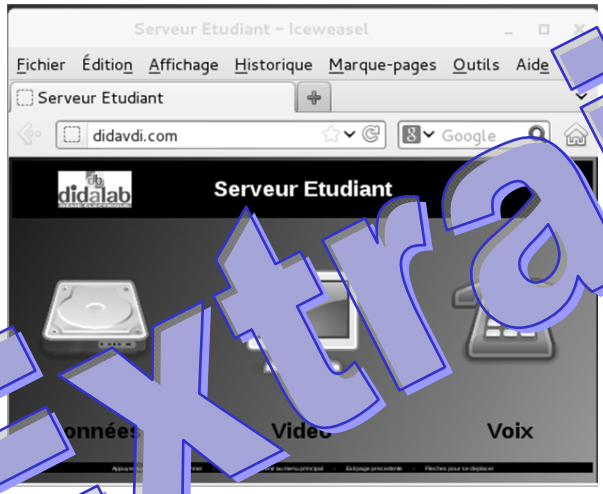
```
root@PCClientDidaVDI:~# ping ServeurEtudiant
PING ServeurEtudiant.DIDAVDI.COM (192.168.1.91) 56(84) bytes of data.
64 bytes from www.DIDAVDI.COM (192.168.1.91): icmp_req=1 ttl=64 time=  150 ms
64 bytes from imap.DIDAVDI.COM (192.168.1.91): icmp_req=2 ttl=64 tim    142 ms
^C
--- ServeurEtudiant.DIDAVDI.COM ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.142/0.146/0.150/0.004 ms
root@PCClientDidaVDI:~#
```

```
root@ServeurEtudiant:/etc/bind# ping P   ient    DI
PING PCClientDidaVDI.DIDAVDI.COM (192.   .24)  84)   data.
64 bytes from PCClientDidaVDI.DIDAVDI   192.   1.24)   p_req=1 ttl=64
time=0.130ms
^C
--- PCClientDi   DAVDI.   stati   ---
1 packets trans   ed,  1   eceiv   packet   oss, time 0ms
rtt min/avg/max/   0/0.1   0.000 ms
root@ServeurEtudi   c/bind#
```


Les requêtes dig et nslo issant, il est évidant que les requêtes puis via les noms de machines soient fonctio .

8.2.4 Connexion IceWeasel

Avec IceWeasel, les url ServeurEtudiant et DIDAVDI.COM nous renvoie sur la page d'accueil de notre serveur (192.168.1.91)



Ceci est réalisé grâce au es suivantes du fichier /etc/bind/db.DIDAVDI.COM :

```
@          IN        NS         DIDAVDI.COM.
@          IN        A        192.168.1.91
www        IN        A        192.168.1.91
```

8.3 Blocage de sites

named.conf.options

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block and insert the addresses replacing
        // the all-0's placeholder.
        // forwarders {
        //      0.0.0.0;
        // };
        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };

        #ecoute sur le port 53
        query-source address * port 53;
        #toutes les IPV4
        listen-on { any; };
        //Création d'une zone "policiere"
        response-policy { zone "site.interdit"; };
};
```

named.conf.local

```
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are used in your
// organization
//include "/etc/bind/zones.rfc1918";

//================== Zone DNS DIDAVDI.COM ======================
zone "DIDAVDI.COM" {
type master;
file "/etc/bind/db.DIDAVDI.COM";
};
//================== Zone Inverse ==================
zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/DAVDI.COM.inv";
};

//==================== Sites Interdits ==============
zone "site.interdit"  {
type master;
file "/etc/bind/db.site.interdit";
};
```

db.site.interdit

```
;
; BIND data file for local loopback interface
;
$TTL    60 ; TTL descendu à 1mn pour palier à un éventuel contournement
$ORIGIN site.interdit.
@       IN      SOA     site.interdit. root.site.interdit. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative
;
@       IN      NS      site.interd                ;No          ine
@       IN      A       192.168.1.                 ;    e T

;================= Sercive         les    ires    =====

www     IN                  .91 ;          site web

;===========          Interd          ===============
www.youtube.c              A       192.168.1.91
www.eurosport.                     192.168.1.91
www.facebook.co                    192.168.1.91
*.be                       A       192.168.1.91 ; Blocage sites belges
```

Le but étant de bloquer l'accès à certain site, nous n'auront pas besoin de zone inverse. De plus si nous en déclarons une, celle-ci sera en conflit avec notre zone DIDAVDI.COM.

8.4 Améliorations

Bind s'appuie sur des DNS publiques (type google) pour accéder aux sites internet. ... ux-ci ne sont pas toujours fiables. Il est donc préférable de renseigner le fichier named ... f.o ... ons avec les DNS de notre FAI.

```
forwarders {
        80.10  46.2
        80.1(     1
};
```

Le protocole DNS n'est ... risé ... e pou ... attaq ... arp vu précédemment, il est possible d'envoyer ... sses réponses ... omme ... logiciel arp-sk).
Pour plus d'informat ... DNS Sp ... ://serom.no-ip.org/index.php/Dns_spoofing)


Extrait


Extrait