CONFIGURAZIONE DNS by Daniele Veratti (danielev83@yahoo.it)

si specificano i nameserver di un client all'interno del file /etc/resolv.conf

```
search dominiolocale.it #se non si ha un FQDN cerco nei domini
              #locali (max 6)
nameserver 128.138.243.51 # max 3 nameserver
nameserver 128.138.204.4  #
nameserver 128.138.240.1   #
```

Server dns: il file /etc/named.conf

```
options {
     directory “/var/named”; #dove si trovano i file di zona
     pid-file “/var/named/named.pid”; # dove porre il pid-file
     # se devo interrogare altri name server uso la clausola forwarders
     forwarders {          # inoltro le query (se non so risp) un altro
          128.138.243.151; # nameserver e faccio il caching della risposta
     };                    # posso aggiungere altri ns (no più di 2?)
     forward first; # solo nel caso il master non risponde posso
                    # risolvere con i dati che posseggo
     query-source adrress * port 53;# accetto query da qualsiasi indirizzo
                                    # ma solo sulla porta 53 (DEFAULT)
     allow-transfer { # indico verso quale server mandare i miei dati
          none;       # none indica nessun server
     };               # WARNING: se sono un master sono obbligato ad avere
                      # uno slave DNS!!!
     also-notify 192.108.21.2; # indico un'altra macchina a cui mandare i
                               # file di zona oltre ai miei slave
};

zone “.” {
     type hint;
     file “named.cache”;
};

zone “127.in-addr.arpa” {
     type master;
     file “localhost”;
     notify no; # non vado a trasferire agli slave questo file di zona
};
...
zone “cs.colorado.edu” {
     type slave;
     file “forward/cs.colorado.edu”;
     masters { 128.138.243.151; } # è accettato solo 1 master no lista!
};

zone “250.138.128.in-addr.arpa” {
     type slave;
     file “reverse/250.138.128”;
     masters {128.138.243.151; }
};

zone “xor.com” {
     type master;
     file “forward/zor.com”;
};
zone “21.108.192.in-addr.arpa” {
     type master;
     file “reverse/xor.com”;
```

```
};
```

Se sto dietro un NAT per cui il mio DNS deve rispondere diversamente in base a chi fa una query allora posso renderelo uno split DNS:

```
     view “internal” {
          match-clients { 192.168.1.0/24; }
          recursion yes;

          zone “example.com” {
               type master;
               file “internal/example.com.fwd”;
          };
    zone “1.168.192.in-addr.arpa” {
               ...
          };
     };

     view “external” {
          match-clients {any;};
          recursion no;

          zone “example.com” {
               type master;
               file “external/example.com.fwd”;
          };
          zone “128.175.203.in-addr.arpa” {
               ....
          };
     };
```

Configurazione dei file di zona:

```
@    IN   SOA  ns.cs.colorado.edu. admin.cs.colorado.edu. (
     1999121501; numero di serie del file
     21600     ; refresh,quanto spesso gli slave interrogano il master
               ; per vedere se il numero di serie è cambiato e aggiornarsi
               ; (6 ore)
     1800      ; retry,se un server slave interroga il master per avere gli
               ; aggiornamenti e il master non risp. questo è il tempo che
               ; lo slave deve aspettare prima di riprovare (30 min)
     1209600   ; expire,se il master non è più disponibile, gli slave
               ; continuano a fornire dati authoritative per questo tempo
               ; (2 settimane)
     432000    ; minimum,definisce per quanto tempo il dns fa caching di
               ; una risposta negativa (5 giorni)
     )
     IN   NS   <dnsserver>

     IN   NS   ns
     IN   NS   anchor
     IN   NS   ns.dicom.uninsubria.it.

     IN   MX   <priority> <host>
     IN   MX   10   mail
     IN   MX   20   mail.otherdomain.com.

ns   IN   A    128.138.243.100
```

```
     IN   A    128.138.243.101 ; in questo caso la macchina ns ha 2 IP
anchor    IN   A    128.138.243.105
www  IN   CNAME anchor   ;definisco un alias, vietato per i DNS!!!
```
nel file reverse al posto dei record A si usa PTR
```
100  IN   PTR  ns.cs.colorado.edu. ; il nome dell'host deve essere un FQDN
```

Il trucco del CNAME per le reti CIDR
Per i file forward non ci sono problemi, ma come gestire, nei file reverse, una sottorete la cui maschera non cade nel limite del byte? (il problema più che altro è dell'isp che ci fornisce gli indirizzi)

L'ISP nel file della zona 243.138.128.in-addr.arpa (rete 128.138.243.0/24)
deve scrivere per avere 4 sottoreti di tipo /26:

```
@ IN SOA ... ( ... )

                     ; sono indirizzi relativi, quindi completi sarebbero
1    IN CNAME 1.0-63 ; e.g. 1.0-63.243.138.128.in-addr.arpa.
2    IN CNAME 2.0-63
     ...
63   IN CNAME 63.0-63
64   IN CNAME 64.64-127
65   IN CNAME 65.64-127 ; 1.64-127.243.138.128.in-addr.arpa.
     ...
```
e così via dichiarando poi i dns a cui cediamo l'autorità:
```
0-63      IN NS ns.sottorete1.com.
64-127    IN NS ns.sottorete2.com. (eccetera)
```

Per abbreviare esiste la macro $GENERATE. Ad esempio la rete .0/26 può essere dichiarata dall'ISP con:

```
$GENERATE 0-63 $    CNAME $.0-63
$GENERATE 64-127 $  CNAME $.64-127
$GENERATE 128-191 $ CNAME $.128-191
$GENERATE 192-255 $ CNAME $.192-255

e continuare con le dichiarazioni dei DNS:
0-63      IN NS ns.sottorete1.com.
0-63      IN NS ns2.sottorete1.com.
64-127    IN NS ns.sottorete2.com. (eccetera)
```

I file di zona delle macchine ns.sottorete1.com non presenta particolarità. Hanno regolari record 65 IN PTR ....
Il problema dei glue records: per delegare una sottozona dns bisogna che l'ISP tenga traccia dell'indirizzo ip del server dns che gestice la sottozona. Per questo è importante mantenere costante l'indirizzo IP del server DNS.
