NIC.bo Bolivia

ADSIB Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

Vicepresidencia del Estado Plurinacional
Presidencia de la Asamblea Legislativa Plurinacional
Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

Curso de Configuración De DNS

Octubre, 2014

ADSIB

NIC.bo Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

Introducción

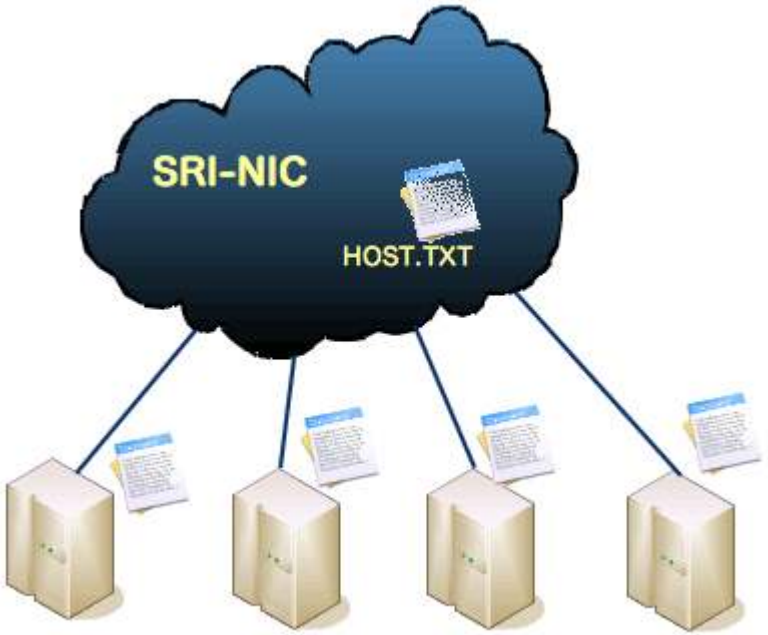
Historia de DNS

Red ARPANET en los 70

Nombre	Dirección
amaru	21
platon	23
evo	24
lapaz	20
***IP no existió como tal sino hasta 1981, anteriormente eran direcciones planas.**	

Historia de DNS

Se distribuye el archivo HOSTS.TXT, y su actualización es periódica



Historia de DNS

- Paul Mockapetris en 1983 inventa el Sistema de Nombres de Dominio y escribe la primera implementación e Internet.

- Evolución de los RFC's relacionados con el DNS.

882 – 883 ----------> 1034 – 1035 – 2181 – 2535

Por que utilizar DNS?

- Las maquinas se comunican con números (direcciones IP). Los humanos nos comunicamos con las maquinas a través de nombres.

- Y esto nos resulta más fácil.....

Como funciona el DNS

IP: 192.168.20.4
Mask: 255.255.255.0
DNS: 200.87.100.10

www.presidencia.gob.bo?

IP: 200.87.30.25

IP: 200.87.100.10
Tiene Varios nombres:
- Resolver
- Dns Recursivo
- Dns cache

www.presidencia.gob.bo?

utama.bolnet.bo
166.114.1.40

Root Servers

www.presidencia.gob.bo?

amaru.presidencia.gob.bo
200.87.30.23

utama.bolnet.bo

www.presidencia.gob.bo?

IP: 200.87.30.25 TTL: 1 dia

amaru.presidencia.gob.bo

IP: 200.87.30.25

Fully Qualified Domain Names FQDN

- Que es el nombre de dominio?

Es un conjunto de etiquetas separadas y (opcionalmente) finalizadas por el delimitador punto **“.”**.

nombre-host.second-level.top-level.

Sintaxis de los nombres

- ¿Que caracteres puede contener un nombre de dominio?

Letras, números y el guión medio “-”.

Cada etiqueta puede llevar hasta 43 caracteres, el nombre de dominio en total puede tener hasta 255 y puede haber hasta 127 niveles.

NIC.bo Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

Configuración de BIND

BIND

- **BIND** (Berkeley Internet Name Domain) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto.

Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley.

Práctica

		K= Número Asignado
Portátil IP	192.168.52.X	Donde: X=10 + K
ns1.empresaK.bolivia.	192.168.52.Z	Donde: Z=100 + X
ns2.empresaK.bolivia.	192.168.52.Y	Donde: Y=200 + X
EJEMPLO:		K=10
Portátil IP	192.168.52.20	X = 20
ns1.empresa10.bolivia.	192.168.52.120	Z = 120
ns2.empresa10.bolivia.	192.168.52.220	Y = 220

BIND

- **BIND** (Berkeley Internet Name Domain) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto.

Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley.

Práctica

El objetivo de la práctica es instalar el servidor de nombres BIND a partir del repositorio elegido en el archivo /etc/apt/sources.list

Instalar bind9 en los tres servidores:

#**apt-get install bind9 bind9utils bind9-doc**
#apt-get install dnsutils

Archivo named.conf

- El archivo named.conf es el archivo de configuración principal de BIND.
- Por lo general el archivo named.conf se encuentra en /etc/bind/

Comentarios en named.conf

Existen varias formas de comentar dentro del archivo named.conf:

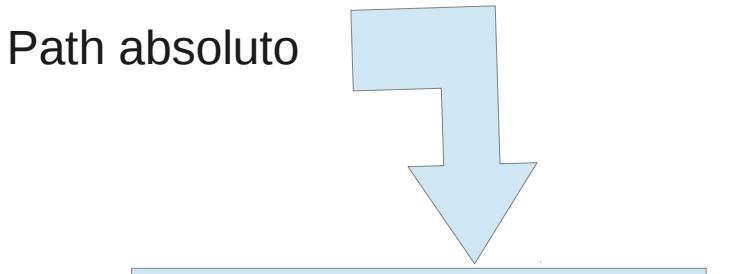
- /* Comentarios que continua a través de cambios de línea, hasta encontrar */

- // ó # Comentario para una linea

Listas en named.conf

- Para enumerar elementos en una lista el separador es un “**;**”.
- Siempre que un argumento sea una lista, este debe estar entre llaves **{192.168.4.1; 192.168.4.2;}**.
- Nombres de Dominio siempre están entre comillas dobles **“bolivia.gob.bo”**.
- El “**!**” se utiliza para negar expresiones o elementos.

Directiva options




```
options {
    directory “ Directorio de las zonas ”;
};
```

Directiva zone (tipo master)

```
zone “NOMBRE.DE.DOMINIO” {
        type master;
        file “ARCHIVO_DE_ZONA”;
};

// Indica que el servidor es autoritativo
// para el NOMBRE.DE.DOMINIO
```

Directiva zone (tipo slave)

```
zone “NOMBRE.DE.DOMINIO” {
        type slave;
        file “ARCHIVO_DE_ZONA”;
        masters {IP_addr; [IP_addr]....;};
};

# Indica que el servidor es autoritativo
# para la zona y que se debe transferir el contenido
# de alguno de los servidores listados en el masters.
```

Directiva zone (tipo hint)

```
zone “NOMBRE.DE.DOMINIO” {
        type hint;
        file “ARCHIVO_DE_ZONA”;
};

/* Indica el archivo de zona que contiene las
   direcciones de IP y los nombres de los root
   servers. */
```

NIC.bo Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

Archivos de zona de un dominio

empresa80.zone

```
$TTL 1d

@       IN      SOA     dns1.empresa80.bolivia. root.dns1.empresa80.bolivia.(
                        2014052601      ; serial
                        1d              ; Refresh Dns secundario actualiza
                        2h              ; Retry Dns secundario vuelve a intentar
                        2w              ; Expire Cuanto tiempo vive el secundario sin actulizar del primario
                        1h      )       ; Negative TTL

        IN      NS      ns1
ns1     IN      A       192.168.52.8
```

Directiva $TTL

- Indica el tiempo que debe guardar los resolver (proveedores) en cache este registro.

Formato:
$TTL <ttl>

Ejemplo:
$TTL 1d

NOTA.- Por lo general se utiliza la siguiente notación para definir el tiempo:

d = dia
w = semana
h = hora

Registro SOA

- El SOA define algunos parámetros para la zona autoritativa para la cual el servidor de nombres esta ofreciendo el servicio de dns autoritativo.

Ejemplo:

```
@       IN      SOA     dns1.empresa80.bolivia. root.dns1.empresa80.bolivia.(
                        2014052601      ; serial
                        1d              ; Refresh Dns secundario actualiza
                        2h              ; Retry Dns secundario vuelve a intentar
                        2w              ; Expire Cuanto tiempo vive el secundario sin actulizar del primario
                        1h      )       ; Negative TTL
```

Registro SOA

- **Serial.** Número de versión de la zona. Debe ser incrementado cada vez que se hace un cambio al archivo de zona de lo contrario el servidor no releerá la nueva información y por lo tanto el servidor secundario (slave) no se actualizara.

Formato sugerido:

YYYYMMDDnn

Donde:

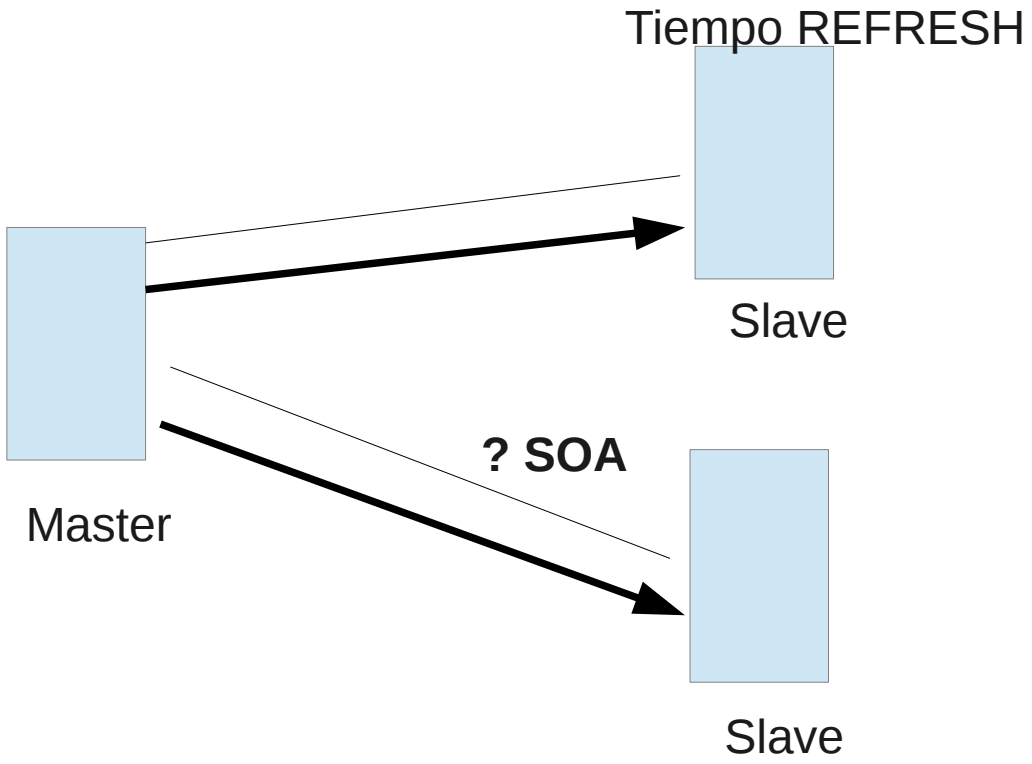
- YYYY = Año en cuatro dígitos,
- MM = Mes
- DD = Día
- nn = Versión del día

Ejemplo:

2014052810

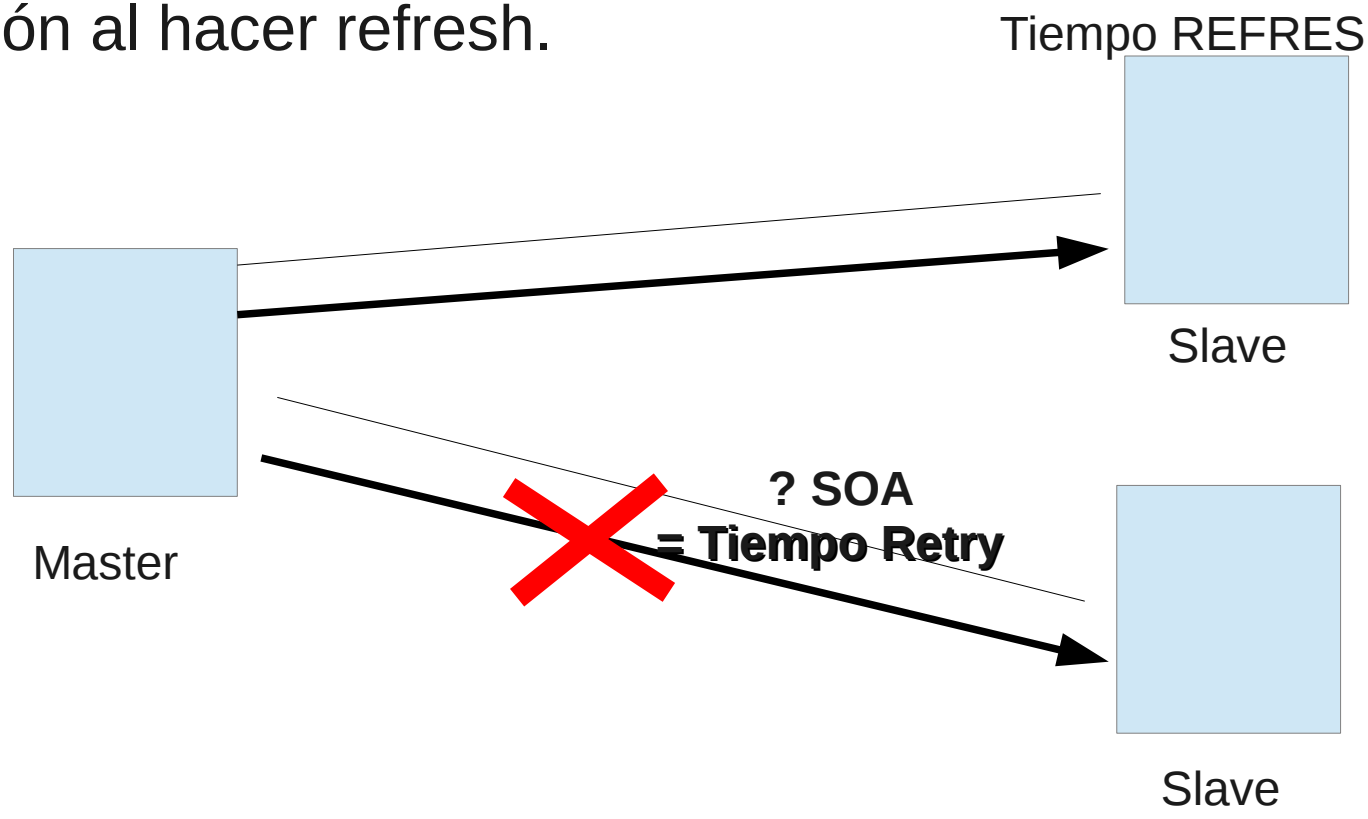
Registro SOA

- **Refresh.** Intervalo de tiempo, contado desde la última vez que se hizo la actualización del archivo de zona en el slave, al final del cual el NS slave debe copiar la zona del NS master.



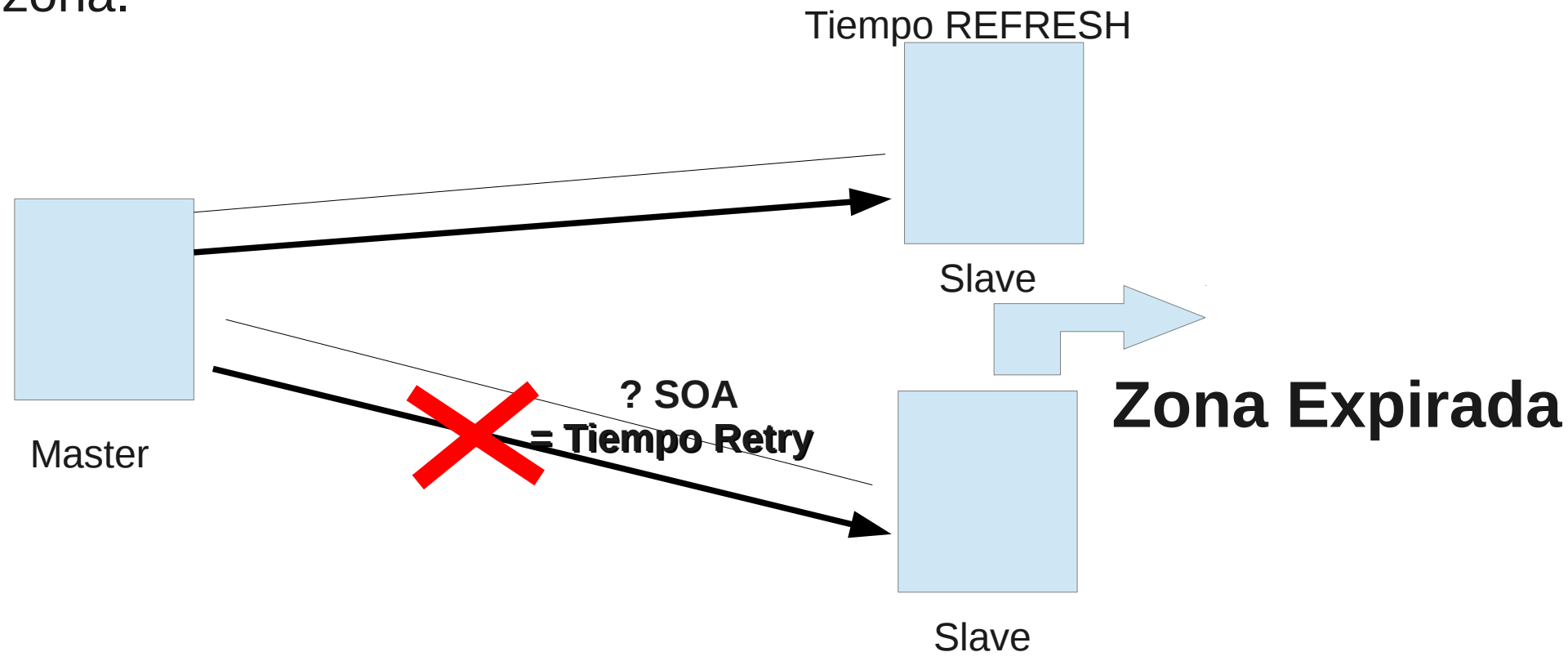
Registro SOA

- **Retry.** Tiempo que el secundario debe esperar para reintentar la actualización de la zona del NS master en caso de que falle la conexión al hacer refresh.



Registro SOA

- **Expire.** Tiempo después del cual, sino se ha logrado hacer el refresh, se desecha la zona; el NS slave deja de responder a requisiciones sobre el nombre de dominio al que se refiere la zona.



Registro SOA

- **Negative TTL.** Cuando un NS responde un query para un nombre para el que “sabe”, que no hay respuesta, envía en la respuesta este TTL para indicarle al NS que “pregunta”, por cuanto tiempo debe guardar en “cache” esta pregunta negativa (negative caching),

- **Negative caching.** Lo definimos como el almacenar el conocimiento de que algo no existe, es decir, si un servidor recibe una respuesta que dice que no hay información para un registro que solicitó, al almacenar esa respuesta, el servidor esta haciendo negative caching.

Registro NS

- Define un servidor de nombres autoritativo para un dominio.
- Formato del registro:
  [dominio] [ttl] IN NS Servidor-de -nombre
- Ejemplo:
  empresa80.gob.bo IN NS dns1.empresa80.gob.bo.

Registro A

- Define una dirección de IPv4 para un nombre de máquina.
- Formato del registro:
  [nombre-máquina] [ttl] IN A dirección.de.IP
- Ejemplo:
  dns1.empresa80.gob.bo. IN A 200.87.10.22

Registro CNAME

- Define un ALIAS para una máquina.

- Formato del registro:
  [alias-máquina] [ttl] IN A nombre-máquina

- Ejemplo:
  ftp.empresa80.gob.bo. IN CNAME ww.empresa80.gob.bo.

Registro TXT

- Define información para una máquina.
- Formato del registro:
  [nombre-máquina] [ttl] IN TXT “información”
- Ejemplo:
  dns1.empresa80.gob.bo. IN TXT “Servidor secundario”

Registro TXT

- Define información para una máquina.
- Formato del registro:
  [nombre-máquina] [ttl] IN TXT “información”
- Ejemplo:
  dns1.empresa80.gob.bo. IN TXT “Servidor secundario”

Registro TXT

- Define información para una máquina.
- Formato del registro:
  [nombre-máquina] [ttl] IN TXT “información”
- Ejemplo:
  dns1.empresa80.gob.bo. IN TXT “Servidor secundario”

Registro MX

- Define un mail exchange para un dominio y un nivel de preferencia.

- Formato del registro:

  [nombre-dominio] [ttl] IN MX prioridad Servidor

- Ejemplo:

```
empresa80.gob.bo.    IN  MX  0   mail.empresa80.gob.bo.

empresa80.gob.bo.    IN  MX  10  mail2.empresa80.gob.bo.
```

NIC.bo Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

Seguridad Básica

Seguridad Básica de transferencia

- Existen algunos pasos simples que se pueden tomar en cuenta para hacer un servidor más seguro y potencialmente reducir su carga.

Práctica

		K= Número Asignado
prueba	192.168.52.M	Donde: M =150 + K
EJEMPLO:		K=10
Portátil IP	192.168.52.20	X = 20
ns1.empresa10.bolivia.	192.168.52.120	Z = 120
ns2.empresa10.bolivia.	192.168.52.220	Y = 220
prueba	**192.168.52.160**	**M = 160**

allow-transfer

- **allow-transfer** Especifica los servidores esclavos que están autorizados para pedir una transferencia de información de la zona. Por defecto, todas las peticiones se autorizan.

```
zone “empresa80.bolivia ” {
                type master;
                file “empresa80.zone”;
                allow-transfer {192.168.52.9; 127.0.0.1;};
                };
  // Los valores puede ser “any;” “none;” “nombre-acl” “IPv4;”
```

allow-query

- **allow-query**. Especifica los clientes que se autorizan para pedir información sobre una zona. Por defecto, todas las peticiones de información son autorizadas.

```
zone “empresa80.bolivia ” {
        type master;
        file “empresa80.zone”;
        allow-query {192.168.52.9; 127.0.0.1;};
        };

// Los valores puede ser “any;” “none;” “nombre-acl” “IPv4;”
```

notify

- **notify**. Controla si named notifica a los servidores esclavos cuando una zona es actualizada. Esta directiva sólo acepta las opciones:

  yes: Notifica a los servidores esclavos.

  no: No notifica a los servidores esclavos.

  Explicit: Solamente notifica a los servidores esclavos especificos en una lista de **also-notify** dentro de la declaración de una zona.

```
zone “empresa80.bolivia ” {
        type master;
        file “empresa80.zone”;
        notify yes;
        also-notify {192.168.52.9;};
        };
```

Lista de control de Acceso (acl)

- **Lista de control de acceso** (ACL, del inglés, Access Control List) define grupos de hosts a los que se les puede permitir o negar el acceso al servidor de nombres.

```
acl “nombre_elegido ” {
                    IP_addr;
                    [IP_addr;]
                    .
                    .
                    .
                  };
```

NIC.bo Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

Seguridad Avanzada

Transferencia segura de zonas

- TSIG (Transaction SIGnature, RFC 2845) es un método para firmar las transacciones y mensajes de DNS mediante el uso de claves simétricas (secretas) compartidas.

- TSIG opera con cifrado simétrico, es decir, los servidores implicados en la transacción comparten una misma clave. Esto permite restringir quién puede transferir las zonas DNS entre servidores.

Configuración de TSIG

La utilidad **dnssec-keygen** incluida en bind9, genera claves.

dnssec-keygen -a **algoritmo** -b **longitud_clave** -n HOST **keyname**

Donde:

Algoritmo: HMAC-MD5 | HMAC-SHA1 | HMAC-SHA224 | HMAC-SHA256 | HMAC-SHA384 | HMAC-SHA512

Longitud_clave: Longitud de la clave (o el número de bits).

Keyname: Nombre de Clave

Configuración de TSIG Servidor

En la maquina master se deberá añadir lo siguiente:

key “**nombre_key** ” {
algorithm **nombre_algoritmo**;
secret “**CLAVE_GENERADO**”;
};

server IP_ESCLAVO {
keys {
nombre_key;
};
};

Configuración de TSIG Servidor

```
zone “empresa80.bolivia ” {
        type master;
        file “empresa80.zone”;
        allow-transfer {key nombre_key; };
        };
```

Configuración de TSIG Secundario

En la maquina secundario se deberá añadir lo siguiente:

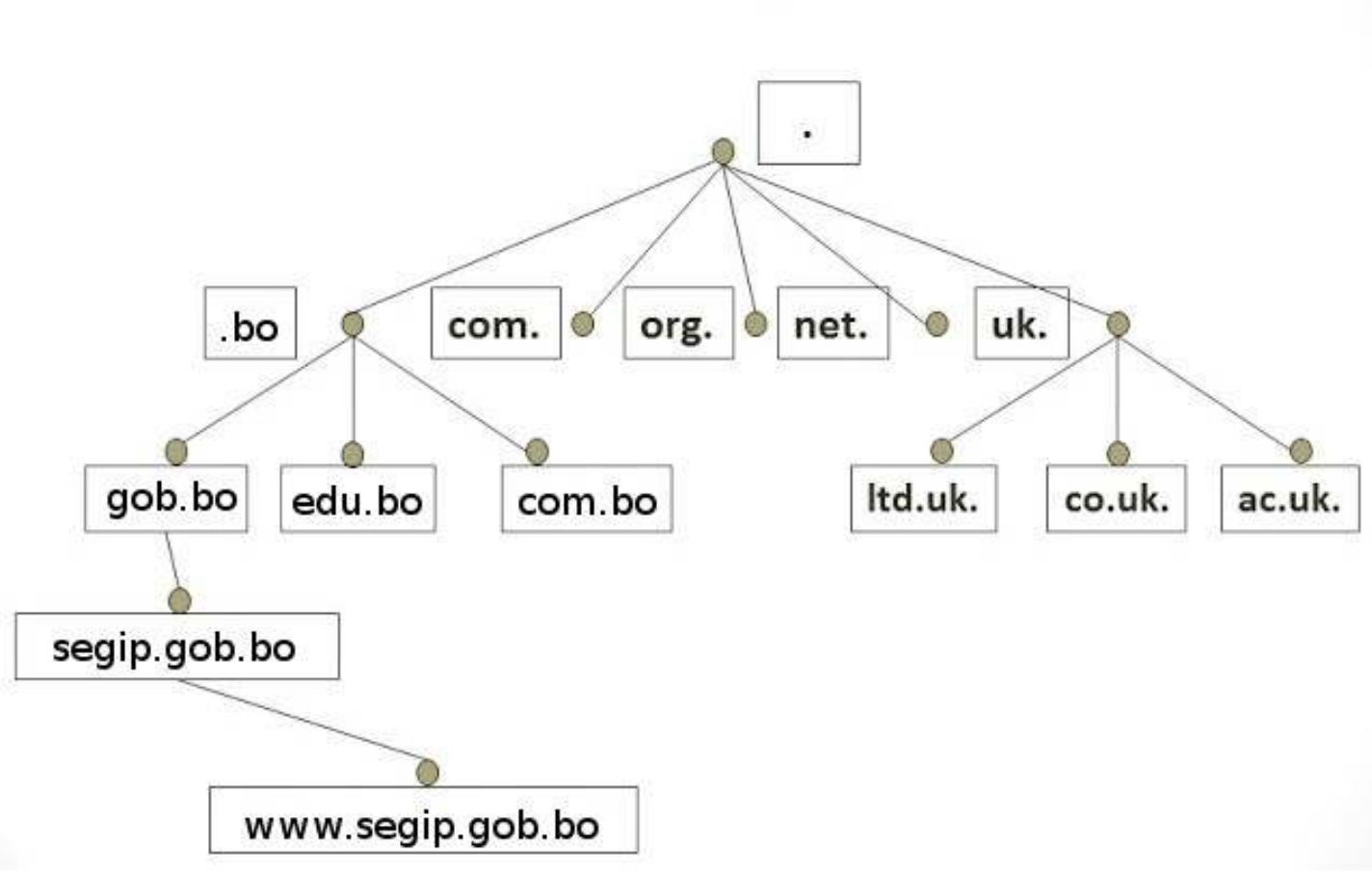
```
key “nombre_key ” {
        algorithm nombre_algoritmo;
        secret “CLAVE_GENERADO”;
        };

server IP_MASTER {
        keys {
                nombre_key;
        };
        };
```

NIC.bo Bolivia

Sistema de Nombres de Dominio (DNS/BIND)

DNS RECURSIVO

Estructura Jerárquica



Tipos de consultas al DNS

- **Recursivas.**
  El cliente le solicita al servidor la respuesta final sobre un nombre de dominio. El servidor debe buscar la información que se le solicita con otros servidores si no la tiene.

- **No Recursivas**
  El cliente le solicita al servidor la mejor referencia que tenga respecto a un nombre de dominio. El servidor le responde al cliente con la información que tiene en memoria, no la busca en otros servidores.

Tipos de Consultas al DNS

- **Recursivas**

  El cliente le solicita al servidor la respuesta final sobre un nombre de dominio. El servidor debe buscar la información que se le solicita con otros servidores si no la tiene.

- **No Recursivas**

  El cliente le solicita al servidor la mejor referencia que tenga respecto a un nombre de dominio. El servidor le responde al cliente con la información que tiene en memoria, no la busca en otros servidores.

Servidor de DNS autoritativo

- Un servidor autoritativo responde con información que obtiene de sus archivos de zona.

- Un servidor autoritativo tiene una copia completa de la zona para la cual es autoritativo.

- Un servidor autoritativo realiza un simple proceso de búsqueda en las zonas configuradas y ofrece una respuesta en caso de encontrar la información..

Servidor de DNS recursivo

- Un servidor recursivo o de cache busca una respuesta en el DNS a la petición que recibe de cliente.

- Un servidor recursivo es mucho mas complejo en su funcionamiento que un servidor autoritativo por que es capaz de recorrer el DNS hasta encontrar la respuesta.

- **Cache**

Es el área de memoria temporal del proceso servidor de DNS recursivo en el que va acumulando todos los registros de DNS que éste obtiene de otros servidores, durante el proceso de resolución de nombres de dominio. El cache es utilizado para minimizar la cantidad de preguntas que se realizan en el DNS.

Servidor de DNS recursivo

- Un host que requiere utilizar el DNS debe tener configurado un servidor recursivo.

- El sistema operativo permite la configuración de uno o más servidores recursivos y una lista de nombres de dominio que son agregados por omisión a una pregunta.

- EDHCP y otros protocolos de auto configuración de parámetros de red permiten configurar de forma automática el servidor de DNS recursivo.

Configuración del DNS recursivo

```
# Archivo de configuración del resolver
# /etc/resolv.conf

search    segip.gob.bo.
nameserver  192.168.52.10
```

NIC.bo Bolivia

ADSIB Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

Vicepresidencia del Estado Plurinacional
Presidencia de la Asamblea Legislativa Plurinacional
Bolivia

GRACIAS .....

soporte@softwarelibre.gob.bo