Administración DNS

Tomás P. de Miguel

Dpto. de Ingeniería de Sistemas Telemáticos

Universidad Politécnica de Madrid

dit UPM

Índice

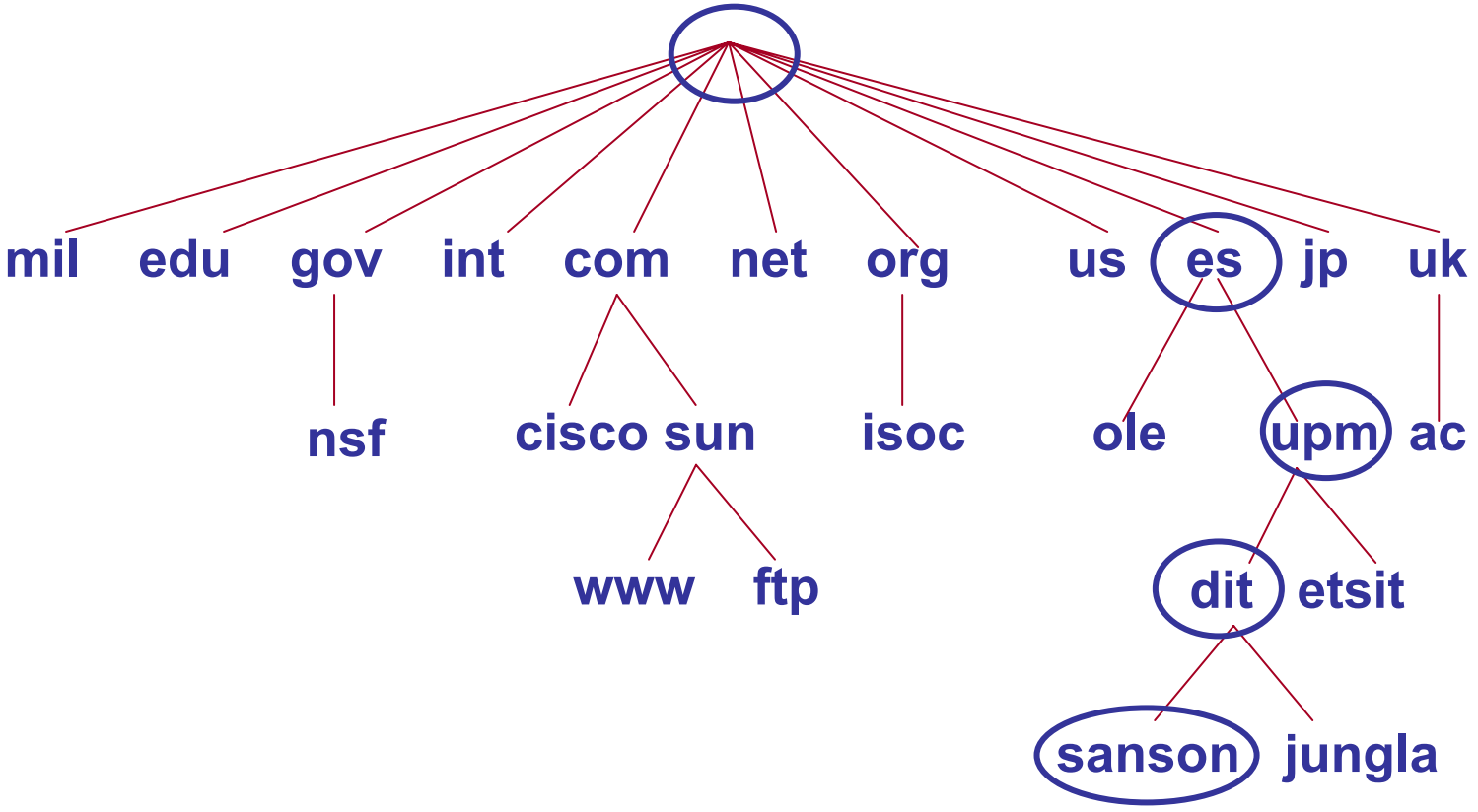
- Definición del servicio
- Configuración de un cliente
- Configuración de un servidores
- Arquitecturas de servicios de nombres
- Administración de dominios
- Facilidades avanzadas
- Aspectos de seguridad

Servicio de nombres

- DNS (Domain Name Server) (RFC1034, RFC1035)
- Establece una correspondencia entre nombres y direcciones IP.
- Consiste en una base de datos distribuida por toda la Internet.
  - se gestiona de forma descentralizada
  - el esquema de distribución es jerárquico
  - fácil de usar en las aplicaciones (gethostbyname())
  - espacio de nombres es global
- Almacena información adicional
  - se puede utilizar para otros fines
  - almacenamiento de características de máquinas
  - configuración de servicios

Modelo de información

- Jerárquico en árbol invertido
- Base de datos de información de dominios (DIB)



Registros de recursos

- Registro de recursos (RR)
  - información asociada a cada nodo
- RR: es una tupla

  <Owner Type Class TTL Value>
  - **Owner** nombre de dominio, propietario del RR
  - **Type** tipo de recurso

A	IP address
MX	Mail eXchanger
NS	Name Server
CNAME	Canonical Name
HINFO	Host description
PTR	Pointer (alias de un dominio)
SOA	Start of a zone of authority

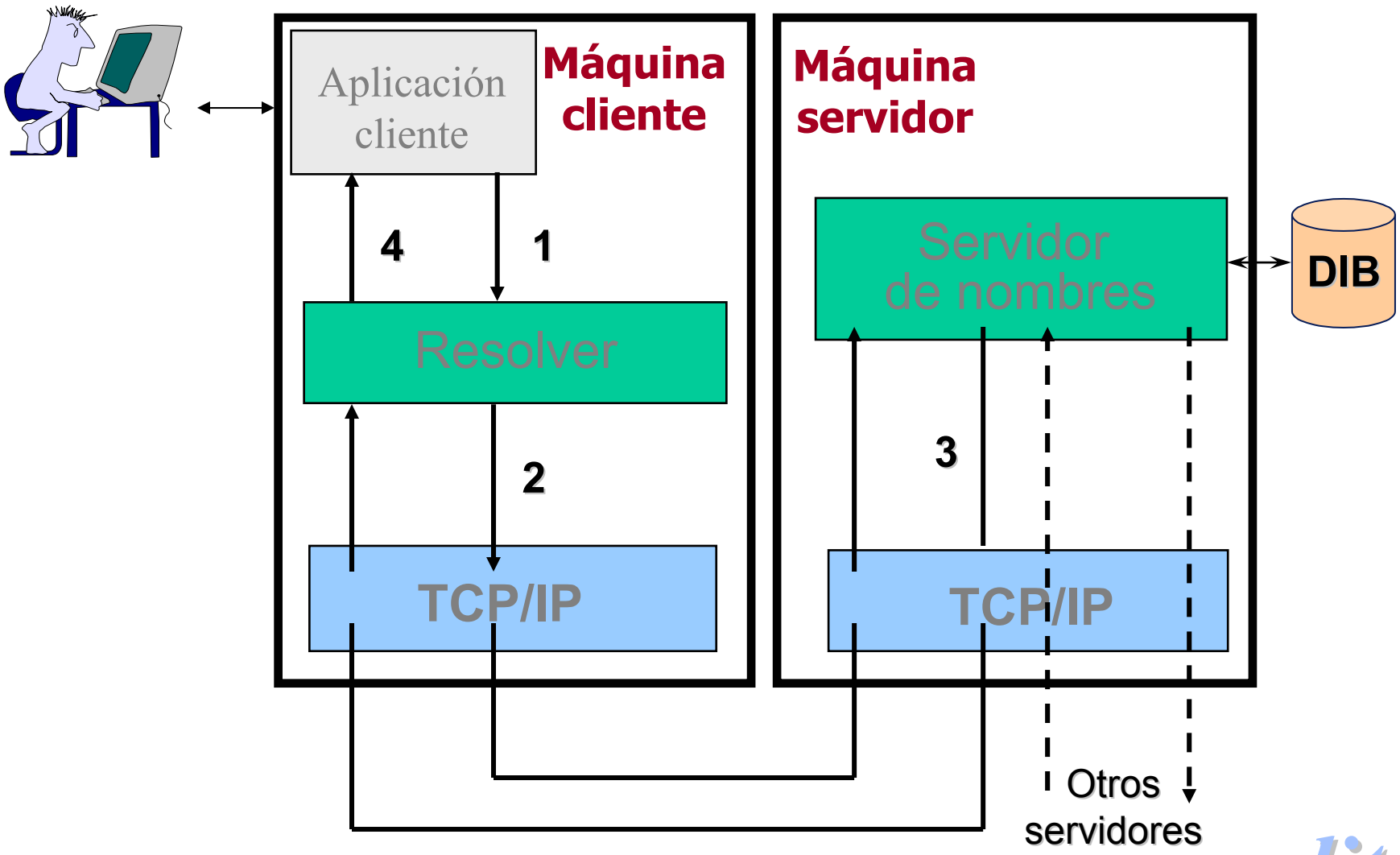
Registros de recursos

<Owner Type Class TTL Value>

- **Class** identifica a una familia de protocolos (IN en Internet)
- **TTL** *time to live,* cuánto tiempo un RR puede estar en la copia caché antes de ser descartado
- **Value** datos, depende del tipo de RR

A	Dirección IP de 32 bits
MX	Preferencia + nombre de dominio
NS	Nombre de dominio (sistema)
CNAME	Nombre de dominio
HINFO	Máquina, S.O.
PTR	Nombre de dominio
SOA	Varios campos

Resolución de nombres



Configuración y administración

- Configuración de los clientes
  - resolver
  - En las aplicaciones
  - En el sistema
    - `gethostbyname()`
    - como un gancho en el núcleo
    - como un proceso en el sistema
- Configuración de un dominio
  - Delegado en otro dominio
  - Dominio en un solo servidor
  - Dominio en varios servidores
    - arquitectura de la base de datos distribuida

Versiones

- UNIX
  - BIND 4
  - BIND 4.9
  - BIND 8
- Windows 95 y Windows 98
  - solo resolver
- Windows NT y Windows 2000
  - resolver
  - servidor de nombres
    - dominios sencillos
    - incorpora opciones avanzadas

Configuración del cliente

- Configurando el resolver se configuran todas las aplicaciones
  - `gethostbyname()`
- Orden de traducción de nombres
  - UNIX (host.conf, nsswitch.conf)
    - `/etc/hosts`
    - Páginas amarillas NIS
    - DNS
  - Windows
    - LMHOSTS
    - WINS
    - DNS

Configuración de DNS

- Consiste en configurar el resolver local de la máquina
- En UNIX está en /etc/resolv.conf
  - domain
  - search
  - nameserver
  - sortlist
  - options
- Todas las aplicaciones se comportan igual

Definición de dominio

- Para indicar el dominio por defecto
- En `.rhosts` (dominio mark)
- En `hostname` (lince.**dit.upm.es**)
- En el resolver
  - **`domain dit.upm.es`**
- Si no se indica ninguno se obtiene de la configuración general del sistema

Lista de búsqueda

- Sirve para facilitar la búsqueda de un nombre.
- Simplifica la identificación de una máquina:
  - lince
  - lince.dit.upm.es.
- El dominio por defecto determina la lista de búsqueda por defecto.
  - Sin punto se añade el dominio por defecto
  - Con punto:
    - primero se busca sin dominio
    - si falla se añade el dominio por defecto
- La lista de búsqueda permite buscar en mas de un dominio
  - **`search dit.upm.es lab.dit.upm.es`**

Servidor de nombres

- El resolver inicia las búsquedas conectando con el servidor de nombres local.
- Como no es necesario tener un servidor de nombres en todas las máquinas se debe seleccionar uno.
  - `nameserver 138.4.2.10`
- Cuando falla el acceso al servidor no se vuelve a buscar en /etc/hosts
- El resolver siempre busca en el mismo orden

Elegir entre varias respuestas

- Si la respuesta a una petición contiene varios alternativas se puede indicar cual es la preferida
- **`sortlist 138.4.2.0/255.255.255.192`**
- **`sortlist 138.4.0.0`**
- **`sortlist 138.4.2.0/255.255.255.0 138.4.22.0/255.255.255.0`**

Ejemplos

Configuración de resolvers

nslookup

utilizando el servicio DNS

nslookup

- Herramienta para consultar DNS
  - dig
  - host
- nslookup es la más extendida.
- Se puede probar el comportamiento del resolver o el de cualquier servidor.
- Solo habla con un servidor cada vez, mientras que el resolver puede dialogar con varios.

Servidor

- Siempre se trabaja con un único servidor.
- Se utiliza por defecto el primero que se indica en la configuración del resolver.
- Ajusta los mismos plazos de espera del traductor.
- No trata de optimizar plazos.
- En esta herramienta lo importante es la respuesta no el tiempo empleado en conseguirla.

Opciones

- Depuración
  - debug y d2
- Considerar un dominio por defecto
  - defname, domain o nosearch
- Realizar peticiones recursivas
  - recurse
- Ignorar paquetes erróneos
  - por defecto intenta resolver el problema utilizando TCP
- Utilizar otro puerto
  - port
- Muestra diferentes tipos de recursos
  - querytype, class
- Configuración de plazos y repeticiones
  - tiemout, retry

Ejemplos

Buscando información con nslookup

Administración de un servidor DNS

Tipos de acceso a Internet

- Sin ningún tipo de acceso
  - se pueden utilizar dominios inventados
- Acceso completo
  - hay que estar registrado en un dominio público
  - conectado con el resto de la BD mundial
- Acceso limitado por un corta-fuegos
  - se puede operar con una parte pública y otra privada

Configuración de un servidor

- Escribir la tabla de máquinas
- Traducir la tabla de máquinas a ficheros de configuración DNS
- Definir la arquitectura local
  - un servidor primario
  - varios secundarios (esclavos)
  - forwarders (cache)
- Configurar el servicio named
- Probar la configuración con nslookup

Tabla de máquinas

- Fichero /etc/hosts
- Puede incluir máquinas en una o varias redes
- La tabla de máquinas incluye:

127.0.0.1	localhost	localhost.localdomain
138.4.2.9	itaca fax news nis	itaca.dit.upm.es
138.4.2.9	mail	mail.dit.upm.es
138.4.2.10	sanson dns	sanson.dit.upm.es
138.4.2.13	yeti dns2	yeti.dit.upm.es
138.4.2.13	mail2	mail2.dit.upm.es
138.4.2.60	loro www ftp proxy hora	loro.dit.upm.es
138.4.3.171	lince	lince.dit.upm.es
138.4.23.170	cajon	cajon.dit.upm.es

Traducción de la Tabla de Máquinas

- DNS se compone de varios ficheros
  - conversión de nombres a direcciones
  - conversión de direcciones a nombres (reverse mapping)
  - Otros ficheros redundantes:
    - db.cache y db.127.0.0
- Cada red tiene una resolución inversa
- Por convenio se utilizan los siguientes nombres
  - Conversión de nombres a direcciones: db.DOMINIO
  - Conversión de dirección a nombre: db.DIRECCION-RED
- Los nombres se indican en el fichero de configuración
  - /etc/named.boot (para BIND 4)
  - /etc/named.conf (para BIND 8)

Generación de ficheros DNS

- Se puede hacer a mano, pero es peligroso si hay muchas máquinas y muchas redes
- En Windows NT se hace a través de menús
  - muy lento si hay que administrar muchas redes
  - no está conectado con otros servicios
- Hay muchas utilidades en UNIX para traducir los nombres de una BD local a la de DNS

Ficheros de registros

- En UNIX
  - dos formatos parecidos
    - BIND 4
    - BIND 8
    - src/bin/named/named-bootconf.pl (pasa de 4 a 8)
  - ficheros textuales donde no se distingue entre mayúsculas y minúsculas
- En Windows
  - Se introducen los datos por menus
  - Se registran en el Fichero oculto de Registros
  - Es posible volcar el fichero de registros a un fichero de texto
  - También se pueden añadir ficheros de texto al registro de Windows.

Ficheros de registros

- Se componen de Registros de Recursos
- Formato parcialmente libre
  - un registro por línea
- Tipos de registros
  - SOA indica la autoridad de la zona
  - NS indica un servidor de nombres de la zona
  - Aconversión nombre a dirección
  - PTR conversión dirección a nombre
  - CNAME nombre canónicos (ALIAS)
  - comentarios
    - ; es un comentario en v4
    - /* es u comentario en v8 */
    - // y este también
    - # y este también

Configuración del servidor

- Directorio con los ficheros de datos
  - directory /usr/local/named
  - options { directory “/usr/local/named”; };
- Servidor maestro primario
  - contiene una linea por cada fichero de datos
  - cada línea tiene tres campos:
    - primary (en la primera columna)
    - el nombre de dominio
    - nombre de fichero

Abreviaturas

- El nombre del servidor primario se añade a todos los nombres no completos (que no terminan en .)

```
lince.dit.upm.es.                IN A      138.4.3.171
lince                            IN A      138.4.3.171
171.3.4.138.in-addr.arpa         IN PTR lince.dit.upm.es.
171                              IN PTR lince.dit.upm.es.
```

- No olvidar el “.” en los nombres completos
  - lince.dit.upm.es IN A 138.4.3.171
  - equivale a lince dit.upm.es.dit.upm.es.

Abreviaturas de nombres

- El nombre de dominio se puede reducir
  - dit.upm.es.
  - @
- Se puede asumir en nombre anterior
  - selva IN A 138.4.2.7
  - IN A 138.4.22.1
- Los nombres no pueden incluir el _
  - Solo se puede utilizar en las direcciones de correo

Servidor de nombres secundario

- Es necesario tener al menos un servidor de nombres esclavo del primario
- Muchas veces hay mas de dos.
- Sirve además para repartir carga
- Diferencias
  - el primario tiene la información local
  - el esclavo la coge por la red (zone transfer)
- Como el loopback y la cache son iguales se pueden copiar a mano.

Configuración del correo

- La Tabla de Máquinas solo sirve para dar nombres a las máquinas.
- DNS permite encaminar el correo electrónico.
- DNS ofrece la posibilidad de indicar servidores de correo alternativos
- El registro MX sirve para indicar el servidor para
  - procesar el correo
  - distribuir correo
- Originalmente estaba dividido en dos, MD y MF.

Servidores de correo

- Se puede especificar mas de un servidor de correo
- Para evitar bucles se añade un parámetro que es la preferencia, que indica la prioridad de cada servidor.
- dit.upm.es. IN MX 10 mail.dit.upm.es.
- Cuando se dan varios se ordenan por prioridad y se evalúan en ese mismo orden:

```
selva      IN     A              138.4.22.1
           IN     MX       0     mail.dit.upm.es.
           IN     MX      10     mail2.dit.upm.es.
           IN     MX     100     selva.dit.upm.es.
```

- Se pueden dar valores de 0 a 65535
- Es recomendable indicar un registro MX para cada máquina

Características de un servidor de correo

- Tamaño
  - para manejar todo el correo
  - para encolarlo si es necesario
- Disponible
  - en funcionamiento la mayor parte del tiempo
- Conectividad
  - bien conectado con los demás servidores
- Gestión y administración
  - manteniendo la privacidad
  - que no pierde mensajes cuando se producen fallos
  - consigue una velocidad de entrega

Algoritmo de entrega de mensajes

- Se busca el servidor adecuado con mas prioridad y se entrega el mensaje a ese.
- Si no está disponible se busca el siguiente en función del orden de prioridad.
- Se deben usar siempre nombres canónicos.
  - muchos intercambiadores de correo no miran los alias (CNAME)

Entrega de mensajes

- Cuando se alcanza una máquina con baja prioridad
  - se descartan los servidores con igual o mayor prioridad
  - se intenta mandar el mensaje al de prioridad mas baja
  - si falla se encola y se prueba mas tarde.
- Si al intentar enviarlo se encuentra a si mismo
  - da un error y devuelve el mensaje
  - se puede configurar el sendmail para evitarlo

Ejemplos

Configuración de servidores

Mantenimiento de un servidor DNS

Añadir y quitar máquinas

- Actualizar siempre el primario
  - si se actualiza el secundario se pierde el cambio con la siguiente actualización
- Fichero db.DOMINIO
  - Actualizar el número de serie
  - Añadir los registros: A, CNAME, MX
- Fichero db.DIRECCION
  - Actualizar el número de serie
  - Añadir los registros: PTR
- Relanzar el servidor de nombres
  - kill -HUP `cat /etc/named.pid`

Trazas de funcionamiento

- Durante la operación se generan trazas de funcionamiento
- Como mínimo se deben volcar los errores
- Se suele enviar la información al syslog
- Hay dos categorías de mensajes
  - estadísticas
  - peticiones
- Hay dos canales donde enviar la información
  - syslog (estadísticas)
  - fichero de log (estadísticas y peticiones)

Trazas de funcionamiento

- Hay diferentes tipos de mensajes
  - critical
  - error
  - warning
  - notice
  - info
  - debug nivel
  - dynamic

- En BIND 8 es fácil definirlo

```
logging {
    channel mi_syslog {
      syslog daemon;
      severity info;
    };
    channel mi_fich {
      file “log.mens”;
      severity dynamic;
    };
    category statistics {mi_syslog;
    mi_fich;}
    category queries {mi_fich;}
};
```

Arquitecturas de DNS

- Cuantos servidores se deben instalar
  - Como mínimo un primario
  - Un secundario directamente conectado a cada subred
    - asociarlos a los servidores de ficheros
  - Poner un secundario fuera de las redes del dominio
- Factores a tener en cuenta
  - conectividad
  - versiones de software
  - homogeneidad
  - seguridad

Servidores muy cargados

- Si un servidor recibe muchas peticiones puede ser necesario
  - replicarlo en varios procesos (BIND 4)
  - limitar la carga que admite (BIND 4.9)
- Las transferencias de zonas suponen muchos mensajes de DNS sobre conexiones TCP.
  - Los sistemas tradicionales solo ponen un registro en cada mensaje DNS.

Acciones para reducir la carga

- limitar las transferencias iniciadas con un servidor
  - no traer todas las BD de golpe sino poco a poco
- limitar el número total de zonas a transferir
  - transferencias por servidor *
  - número de servidores
- limitar la duración de una transferencia de zona
  - por defecto son 2 horas
  - después de ese tiempo se considera que el servidor ha muerto
- transferencias de zona mas eficientes
  - se pueden poner varios registros en un mensaje DNS

Recursos limitados

- Limitando el tamaño del segmento de datos
  - limitar el tamaño del proceso antes de que se pare.
- Limitando el tamaño de la pila
- Limitando el tamaño del proceso
- Limitando el número de ficheros abiertos
  - ficheros que el proceso puede abrir simultáneamente

Como aumentar la capacidad

- Añadiendo mas servidores primarios maestros
- Aumentando los intervalos de refresco para que los secundarios no tengan que sondear con mucha frecuencia.
- Cargar unos secundarios de otros
- Crear servidores cache
- Crear servidores secundarios parciales

Cuando añadir un subdominio

- Cuando es necesario delegar o distribuir la gestión entre varios grupos (organizaciones)
- Cuando el tamaño del dominio es muy grande
  - al dividirlo se simplifica la gestión
  - se reduce la carga en el servidor
- Cuando es necesario distinguir las máquinas dentro de una organización por grupos

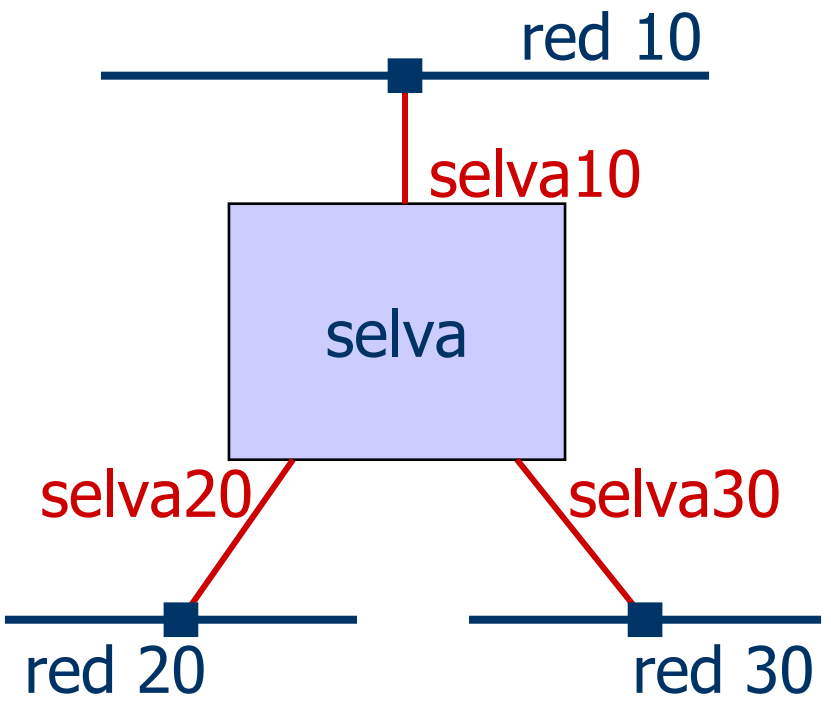
Como nombrar subdominios

- Elegir nombres que no sean susceptibles de cambios frecuentes
- Si los nombres de la organización no son estables usar nombres geográficos
- No sacrificar la legibilidad
- Utilizar nombres obvios
- No utilizar nombres de dominios existentes a nivel mundial

Mantenimiento

- Borrar entradas obsoletas
  - periódicamente se revisa la cache y se eliminan las entradas obsoletas
  - BIND 8 consume menos disco que BIND 4 donde no se limpia
- Intervalo de inspección de interfaces
  - para que el servidor atienda por todas las interfaces aunque estas se activen y desactiven.
- Intervalo entre estadísticas
  - plazo para volcar estadísticas
  - para no entorpecer el funcionamiento normal

Máquinas con varias interfaces



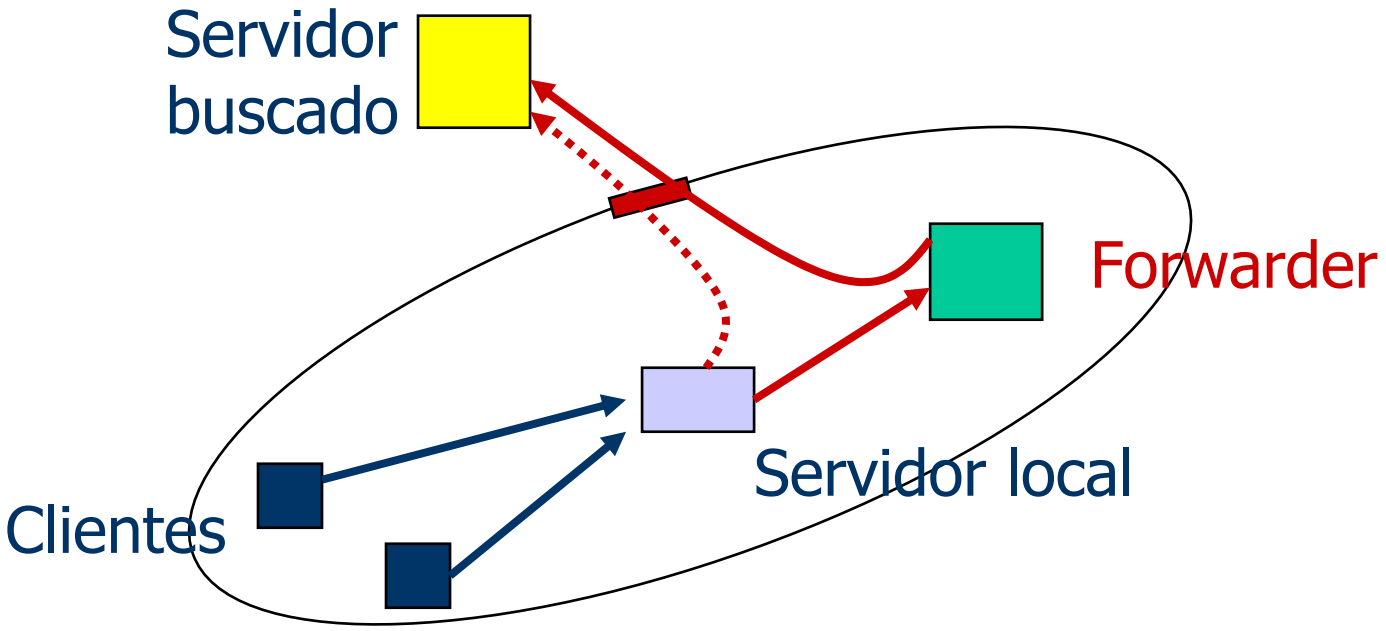
- La mayoría de los servicios mejoran si se accede a la interfaz correcta
- Si se accede al nombre (selva) se puede elegir la interfaz no deseada
- Se puede dar nombre a las interfaces físicas.

Ordenación de respuestas

- Si una máquina pregunta por otra de su misma red, se ordena la respuesta para que la dirección de esa red aparezca la primera.
- Si la máquina que pide la dirección es de otra red no conectada directamente a ninguna de las interfaces
  - no se ordena la lista
  - se puede forzar en la configuración una ordenación
    - sortlist 10.0.0.0
    - esto solo funciona con redes, no subredes
    - se puede indicar varias redes en la lista
- Se puede ordenar los servidores

Forwarders

- Cuando un sitio tiene una conexión de baja capacidad con Internet
- Interesa minimizar al máximo las peticiones fuera y mantener una cache local



Configuración

- Los clientes no tienen nada especial
- Los servidores locales deben saber que existe uno o mas forwarders
  - options { 138.4.2.10; 138.4.3.130; };
  - forwarders 138.4.2.10 138.4.3.130
- Se puede restringir la configuración aun mas
  - options { 138.4.2.10; 138.4.3.130; };
    forward-only;
  - forwarders 138.4.2.10 138.4.3.130
    slave

Servidor en grupo

- Cuando un servicio de Internet se da con mas de una máquina
- Ayudar a repartir carga entre servidores espejo
- Versiones antiguas
  - Un registro especial: Shuffle Address Record
- Versiones modernas (4.9)
  - varios registros A
    - www.foo.com. 60 IN A 192.1.1.1
    - www.foo.com. 60 IN A 192.1.1.2
    - www.foo.com. 60 IN A 192.1.1.3
  - va rotando las direcciones en las respuestas

DNS y páginas amarillas

- El orden de búsqueda es el siguiente
  - /etc/hosts
  - NIS
  - DNS
- Ignorar NIS
  - mv /etc/hosts /etc/hosts.tmp
  - touch /etc/hosts
  - (cd /var/yp; make)
  - mv /etc/hosts.tmp /etc/hosts
- En Linux se puede establecer un orden cualquiera
  - /etc/host.conf
  - /etc/nsswitch.conf

DNS y Windows 95

- Se puede configurar el resolver local
  - Dial-up networking
  - TCP/IP settings
- El orden de búsqueda es
  - LMHOSTS
  - WINS
  - DNS
- Se puede indicar
  - el nombre de la máquina
  - los servidores en los que buscar
  - dominios en los que buscar

Notificaciones de cambio

- Los esclavos se actualizan periódicamente (refresh time)
- Cuando se efectúa un cambio en el primario no se percibe hasta que vence el plazo de actualización
- DNS NOTIFY (RFC 1996)
  - el primario envía una petición NOTIFY a los esclavos
  - el esclavo asiente NOTIFY
  - el esclavo hace como se el periodo de actualización hubiera vencido
  - solo si el número de serie ha aumentado se transfiere la zona

Configuración

- Está configurado por defecto
- El servidor DNS para NT dispone de esta facilidad
- No siempre se desea que este activada
  - options { notify no; };
  - de esa forma un esclavo no notifica a otro en cascada
  - si se tienen esclavo con BIND 4 es mejor no notificar
  - se notifica a todos los servidores NS

Configuración explícita

- Se pueden añadir máquinas a mano

```
zone “acmebw.com” {
        type master;
        file “acmebd.com.db”;
        notify yes;
        also-notify 15.255.152.4;
};
```

Movilidad

- Se desea que la misma máquina se pueda conectar a varias redes
- Se puede utilizar DHCP para asignar número de IP al cliente
- Pero hay que actualizar la BD de DNS
- Actualización dinámica (RFC 2136)
- Hay que actualizarlo en el servidor

```
zone “acmebw.com” {
  type master;
  file “acmebw.com.db”;
  allow_update { 192.168.0.1; };
};
```

Actualización dinámica

- Por línea de comandos (nsupdate) o por programa
- Establecer prerequisitos antes de actualizar
  - prereg yxrrset domain name type [rdata]
  - prereg nxrrset
  - prereg yxdomain domain name
  - prereg nxdomain
- Actualizar la base de datos
  - update delete domain name [type][name]
  - update add domain name ttl [class] type rdata

Ejemplos

- Añadir una máquina
  - nsupdate
  - prereg nxdomain dit.upm.es.
  - update add lince.dit.upm.es 333 in a 138.4.23.58
- Si una máquina tiene MX borrarlo y poner otros dos en su lugar
  - nsupdate
  - prereg yxrrset yeti.dit.upm.es. in mx
  - update delete yeti.dit.upm.es. In mx
  - update add yeti.dit.upm.es. In mx 10 yeti.dit.upm.es.
  - Update add yeti.dit.upm.es. In mx 50 selva.dit.upm.es.

Aspectos de seguridad

- La mayoría de los aspectos de seguridad no son necesarios en corporaciones
- A quien contestar
- A quien ofrecer la notificación de cambios
- A quien permitir que se actualice dinámicamente

Seguridad

- Protegerse contra ataques maliciosos
  - utilizar versiones modernas protegidas
- Limitar las peticiones
  - dando una lista de acceso
- Evitar transferencias no autorizadas
- No ejecutar el servidor como root

Limitar las peticiones

- Rechazar el acceso a la información
- ofrecer nombres solo al grupo local
- options { allow-query { lista_de_acceso }; };

```
options {
        allow-query { 138.4.1.0/6; 138.4.2.64/6; }
};
```

Limitar las peticiones por zonas

- Se puede limitar la información por zonas

```
zone “hp.com” {
        type slave;
        file “db.hp”;
        masters { 15.255.152.2; };
        allow-query { “HP-NET”; };
};
```

- En BIND 4.9 se utiliza el registro secure_zone
  - limita las transferencias de zona además de las peticiones
  - secure_zone IN TXT “138.4.23.0:255.255.255.0”
  - secure_zone IN TXT “138.4.2.0:255.255.255.192”
  - secure_zone IN TXT “127.0.0.1:H”

Limitar las transferencias de zonas

- Asegurar que solo los servidores esclavos pueden transferir la zona
- Configuración
  - allow-transfer (BIND 8)
  - xfrnets (BIND 4.9)
- Configuración del primario
  - indicar las máquinas autorizadas
- Configuración del esclavo
  - prohibir la transferencia totalmente

Ejemplo (BIND 8)

- primario

```
zone “acmebw.com” {
    type master;
      file “db.acmebw”;
      allow-transfer {192.168.0.1; 192.168.1.1; };
};
```

- esclavo

```
zone “acmebw.com” {
    type slave;
      masters { 192.168.0.4; };
      allow-transfer { none; };
};
```

Reglas de seguridad

- Evitar las peticiones recursivas en los servidores de nombres delegados
  - para evitar el spoofing
- No se puede evitar la recursión en los forwarders
  - limitar las peticiones a un grupo
  - allow-query { 138.4/16; };
- Restringir la transferencia de zona a servidores conocidos