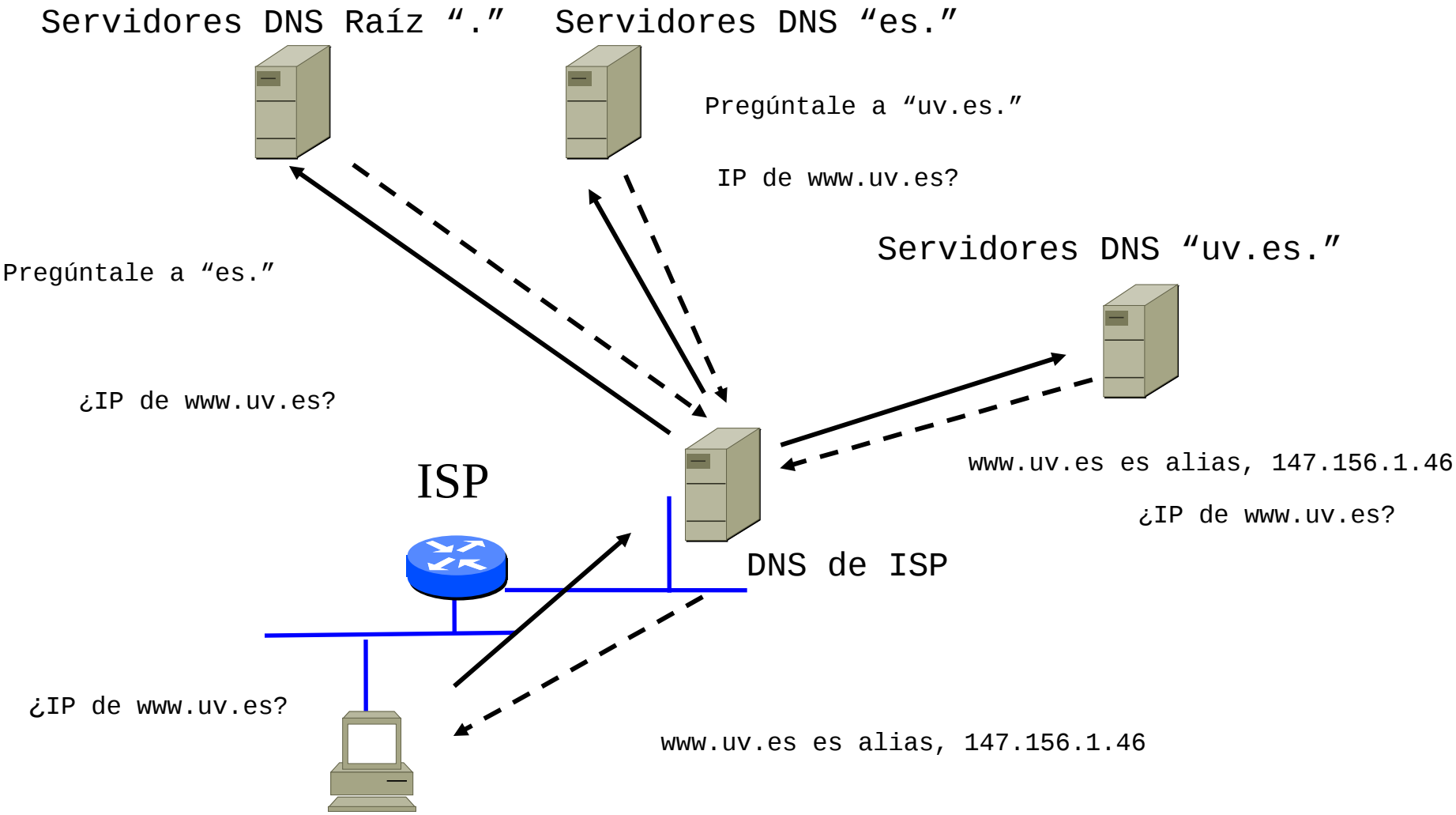
Introducción

- En Internet todos los paquetes viajan en función de su dirección IP en la red.
- Nosotros usamos nombres para identificar los ordenadores:
- Necesitamos traducir nombres en direcciones IP.
  - Inicialmente era un fichero host.txt que administraba el DoD-NIC de EE.UU.
  - Con el crecimiento se hizo necesario sustituir ese fichero por un sistema descentralizado: Domain Name Server.

Funcionamiento del servicio de DNS



El cliente DNS (I)

- Todo ordenador conectado a Internet es un cliente de DNS.
- La configuración se basa en tres ficheros:
  - /etc/hosts.
  - /etc/host.conf.
  - /etc/resolv.conf.

El cliente DNS (II)

- El fichero /etc/hosts:
  - Contiene la relación entre nombres y direcciones IP necesarias para el arranque.
  - Pueden añadirse todas las relaciones nombre-IP que se deseen (a modo del primitivo host.txt).

```
127.0.0.1 localhost localhost.localdomain localhost4
::1       localhost localhost.localdomain localhost6
147.156.222.65 glup.uv.es glup.irobot.uv.es glup
```

  - La línea 127.0.0.1 es siempre necesaria (dirección de loopback).

El cliente DNS (III)

- El fichero /etc/host.conf:
  - Contiene como principal opción, el orden en que deben utilizarse las posibilidades de resolución de nombres existentes:
    - hosts: Fichero /etc/hosts.
    - bind: Servidor de nombre.
    - nis: Servicio de información en red.
  - La entrada más común es:

```
order hosts,bind
```

El cliente DNS (IV)

- El fichero /etc/host.conf:
  - Otra entrada que suele aparecer es:

```
multi on
```

  - Que indica que si el nombre se corresponde con más de una entrada en /etc/hosts se devuelvan todas las entradas.

El cliente DNS (IV)

- El fichero /etc/resolv.conf:
  - Indica:
    - Dominio o dominios de búsqueda.
    - Servidores de nombres a los que consultar.
  - La entrada domain indica un dominio de búsqueda, generalmente el dominio del ordenador.
  - La entrada search indica hasta seis dominios de búsqueda con un tamaño máximo total de 256 caracteres.
  - La entrada nameserver indica las direcciones IP de los servidores de nombres.

El cliente DNS (V)

- Ejemplo de /etc/resolv.conf:

```
domain    uv.es
nameserver  147.156.222.65
nameserver  147.156.1.1
nameserver  147.156.1.3
```

Consulta de un cliente DNS a un servidor DNS

- La consulta se puede realizar directamente mediante con el comando host. Ejemplo:

```
host glup.irobot.uv.es
host 147.156.222.65
```

- Si preguntamos por: `host glup`
  - Obtenemos respuesta si en el fichero /etc/resolv.conf la línea domain o search contiene el dominio uv.es.
- Si preguntamos por: `host glup.`
  - ! No obtenemos respuesta, pues el . impide añadir dominios !.

El servidor DNS (I)

- Todo dominio de Internet debe disponer de dos DNS como mínimo.
- Los servidores de DNS se clasifican en cuatro conjuntos no disjuntos:
  - Servidor primario: Contiene los ficheros.
  - Servidor secundario: Contiene copia de los ficheros.
  - Servidor maestro: Permite obtener copias de los ficheros.
  - Servidor esclavo: Obtiene de otro copia de los ficheros mediante la “transferencia de zona”.

El servidor DNS (II)

- El servidor es /usr/sbin/named.
- Es un servicio UDP que utiliza el puerto 53 para resolver las consultas.
- Utiliza el puerto 53 TCP para la transferencia de zona.
- Las principales opciones son:
  - -u: Usuario como el que se ejecuta el demonio.
  - -t: Directorio donde se “encierra” la ejecución del demonio. Por defecto es /var/named/chroot.
    - Cualquier opción de configuración altera su valor anteponiendo este directorio.

Tipos de registros

- Existen los siguientes tipos de registros:

Registro	Descripción
SOA	Start Of Authority. Servidor valido para este dominio.
NS	Name Server. Servidor de nombres de un dominio.
PTR	Pointer To Register. Relaciona una dirección IPv4 o IPv6 con su nombre.
A	Address. Relaciona un nombre con su dirección IPv4.
AAAA	Address. Relaciona un nombre con su dirección IPv6.
CNAME	Canonical NAME. Nombre alternativo (alias) de un ordenador.
MX	Mail eXchanger. Intercambiador de correo para el ordenador.

Configuración del servidor DNS (I)

- La configuración se realiza en dos ficheros:
  - /etc/sysconfig/named
  - /etc/named.conf

Configuración del servidor DNS (II)

- /etc/sysconfig/named:
  - Contiene las opciones que se pasan al demonio named en su arranque.
  - La opción -u, para especificar el usuario con el que se ejecuta named, se encuentra actualmente en el script de arranque.
  - La opción -t, para especificar si el demonio es encerrado en un directorio se indica en el script:

```
systemctl start named.service
systemctl start named-chroot.service
```

Configuración del servidor DNS (III)

- /etc/named.conf:
  - Secciones de configuración del servidor.
    - options: Configuración global.
    - logging: Configuración del log del servidor
  - Zona o zonas de las que es servidor DNS.

Configuración del servidor DNS (IV)

```
options {
   listen-on port 53 { 127.0.0.1; };
   listen-on-v6 port 53 { ::1; };
   directory  "/var/named";
   dump-file   "/var/named/data/cache_dump.db";
   statistics-file "/var/named/data/named_stats.txt";
   memstatistics-file "/var/named/data/named_mem_stats.txt";
   allow-query     { localhost; };
   recursion yes;

   dnssec-enable yes;
   dnssec-validation yes;
   dnssec-lookaside auto;

   /* Path to ISC DLV key */

   bindkeys-file "/etc/named.iscdlv.key";

   managed-keys-directory "/var/named/dynamic";

   Pid-file "/run/named/named.pid";

};
```

Configuración del servidor DNS (V)

- listen-on y listen-on-v6: Puerto UDP e interfaces de red de escucha.
- directory: Directorio de ejecución.
  - /var/named si no se ha indicado nada en ROOTDIR
  - <ROOTDIR>/var/named si ROOTDIR <> /
- dump-file: Fichero donde almacenar la cache.
- statistics-file y memstatistics-file: Ficheros donde almacenar estadísticas de uso y memoria.

Configuración del servidor DNS (VI)

- allow-query: IPs que pueden usar este DNS.
- recursion { yes | no }: Recursividad de las consultas.
- Opciones de autenticación de seguridad del servidor DNS (DNSSEC):
  - dnssec-enable.
  - dnssec-validation.
  - dnssec-lookaside.
  - bindkeys-files.
  - managed-keys-directory.

Configuración del servidor DNS (VII)

- pid-file: Fichero donde se guardará el PID del servidor.

```
logging {
   channel default_debug {
      file "data/named.run";
      severity dynamic;
   };
};
```

Tipo de log, fichero donde almacenar el log, etc.

  – Si no existe esta sección el log se guarda en el fichero por defecto del sistema. Generalmente /var/log/messages.

Configuración del servidor DNS (VIII)

- Las zonas de las que es servidor un DNS se especifican con la sintaxis:

```
zone "<nombre de la zona>" IN {
    type <tipo>;
    file "fichero";
    allow-update { <direcciones IP>; };
    masters { <direcciones IP>; };
};
```

Zonas obligatorias de un servidor DNS (I)

```
zone "." IN {
   type hint;
   file "named.ca";
};

zone "localhost.localdomain" IN {
   type master;
   file "named.localhost";
   allow-update { none; };
};

zone "localhost" IN {
   type master;
   file "named.localhost";
   allow-update { none; };
};
```

Zonas obligatorias de un servidor DNS (II)

```
zone
   "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
   .0.0.0.ip6.arpa" IN {
   type master;
   file "master.loopback";
   allow-update{ none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
   type master;
   file "master.loopback";
   allow-update{ none; };
};

zone "0.in-addr.arpa" IN {
    type master;
    file "named.empty";
    allow-update { none; };
};
```

El fichero named.ca

- Contiene la relación de los servidores raíz de Internet.

```
.                       3600000    NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000    A       198.41.0.4
A.ROOT-SERVERS.NET.     3600000    AAAA    2001:503:BA3E::2:30
.                       3600000    NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000    A       192.228.79.201
...
.                       3600000    NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000    A       202.12.27.33
M.ROOT-SERVERS.NET.     3600000    AAAA    2001:DC3::35
```

- Donde puede comprobarse que actualmente algunos servidores ya tienen IPv6 y otros no.

Servidor DNS maestro de la UV

- Un servidor maestro del dominio uv.es debería tener las zonas:

```
zone "156.147.in-addr.arpa" IN {
   type master;
   file "master.147.156";
   allow-update { none; };
};
zone "4.1.0.1.0.2.7.0.1.0.0.2.ip6.arpa" IN {
   type master;
   file "master.2001:720:1014";
   allow-update { none; };
};
zone "uv.es" IN {
   type master
   file "master.uv.es";
   allow-update { none; };
};
```

El fichero master.147.156

- Relación entre IPv4 y los nombres.

```
$TTL 600    ; 10 minutos
@           IN SOA glup.irobot.uv.es. root.glup.irobot.uv.es. (
                        2010110310; Número de serie.
                        86400; Validez 1 día.
                        7200; Reintentar cada 2 horas.
                        1209600; Los datos son validos 14 días.
                        7200; Las consultas en la cache son validas 2 horas.
                    )
            NS      glup.irobot.uv.es.
            NS      amparo.irobot.uv.es.
...
$ORIGIN 222.156.147.in-addr.arpa.
34          PTR     amparo.irobot.uv.es.
65          PTR     glup.irobot.uv.es.
...
$ORIGIN 223.156.147.in-addr.arpa.
157         PTR     mirror.irobot.uv.es.
...
```

El fichero master.2001:720:1014

- Relación entre IPv6 y los nombres.

```
$TTL 600     ; 10 minutos
@            IN SOA glup.irobot.uv.es. root.glup.irobot.uv.es. (
                        2010110310; Número de serie.
                        86400; Validez 1 día.
                        7200; Reintentar cada 2 horas.
                        1209600; Los datos son validos 14 días.
                        7200; Las consultas en la cache son validas 2 horas.
                    )
             NS      glup.irobot.uv.es.
             NS      amparo.irobot.uv.es.
...
$ORIGIN 2.2.2.0.4.1.0.1.0.2.7.0.1.0.0.2.ip6.arpa.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0   PTR mirror.ipv6.uv.es.
...
```

El fichero master.uv.es (I)

- Relación entre nombres e IPv4 e IPv6.

```
$TTL 600        ; 10 minutos
@       IN SOA glup.irobot.uv.es. root.glup.irobot.uv.es. (
                2010110300; Número de serie.
                86400; Validez 1 día.
                7200; Reintentar cada 2 horas.
                2592000; Los datos son validos 14 días.
                7200; Las consultas en la cache son validas 2 horas.
                )
                NS          glup.irobot.uv.es.
                NS          amparo.irobot.uv.es.
...
$ORIGIN uv.es.
robotica        CNAME       glup.irobot
irtic           CNAME       glup.irobot
autismo         CNAME       glup.irobot
...
amparo          CNAME       amparo.irobot
glup            CNAME       glup.irobot
mirror          CNAME       mirror.irobot
...
```

El fichero master.uv.es (II)

```
...
$ORIGIN irobot.uv.es.
amparo   A  147.156.222.34
         MX 10 amparo
         MX 20 postin.uv.es.
glup     A  147.156.222.65
         MX 10 glup
         MX 20 postin.uv.es.
mirror   A  147.156.223.157
         AAAA  2001:720:1024:222::2
         MX 10 mirror
         MX 20 postin.uv.es
...
$ORIGIN ipv6.uv.es.
mirror   AAAA  2001:720:1024:222::2
...
```

Servidor esclavo DNS de la UV

- Un servidor esclavo de DNS de la UV debería, aparte de las zonas obligatorias, incluir en su fichero de configuración de zonas:

```
zone "156.147.in-addr.arpa" IN {
   type slave;
   file "slaves/db.147.156";
   masters { 147.156.1.1; };
};
zone "4.1.0.1.0.2.7.0.1.0.0.2.ip6.arpa" IN {
   type slave;
   file "slaves/db.2001:720:1024";
   masters { 147.156.1.1; };
zone "uv.es" IN {
   type slave;
   file "slaves/db.uv.es";
   masters { 147.156.1.1; };
};
```

El número de serie

- El número de serie se construye como aaaammdd##
  - Los dos últimos valores permiten 100 modificaciones diarias.
- Minimizan las transferencias de zona.
  - El servidor esclavo pregunta al maestro por el número de serie.
    - Si el número de serie es igual termina.
    - Si el número de serie es mayor pide la transferencia de zona.

El programa rndc (I)

- Permite enviar ordenes al servidor named.
- Su fichero de configuración es /etc/rndc.conf.
- Posee unicamente tres secciones:
  - options:
    - Solo puede existir una sección.
    - Especifica valores por defecto.
  - server <servidor>:
    - Indica el nombre o dirección IP del servidor al que se aplican las opciones de esta entrada.
  - key <nombre>:
    - Identificación de una clave de autenticación.

El programa rndc (II)

- options:
  - default-server: Servidor al que se envían los comandos por defecto.
  - default-key: Clave a utilizar por defecto.
  - port: Puerto a utilizar por defecto. Si no se indica nada es el 953 TCP.
- server <servidor>:
  - default-key: Clave a utilizar por defecto para este servidor.
  - port: Puerto a utilizar por defecto por este servidor.
- key <nombre>:
  - algorithm hmac-md5
  - secret "Clave secreta codificada en base 64"

El programa rndc (III)

```
options {
   default-server localhost;
   default-key "rndckey";
};
server localhost {
   key "rndckey";
};
include "/etc/rndckey";

key "rndckey" {
   algorithm hmac-md5;
   secret "Clave secreta codificada en base
  64";
};
```

El programa rndc (IV)

Opción	Descripción	Valor por defecto
-b	Utilizar la dirección indicada para conectarse al servidor.	Dirección IP por defecto.
-c	Utilizar el fichero de configuración indicado en lugar del fichero por defecto.	/etc/rndc.conf
-k	Utilizar el fichero con las llaves indicado en lugar del por defecto.	/etc/rndc.key
-s	Servidor al que se enviará el comando.	El servidor indicado en la opción por defecto de /etc/rndc.conf.
-p	Puerto al que se enviará el comando.	953 TCP
-V	Habilitar modo de depuración.	No habilitado.
-y	Clave a utilizar de las existentes en el fichero de configuración.	Clave por defecto especificada para el servidor indicado, o si no existe una clave para ese servidor, clave por defecto.

El programa rndc (V)

Comando	Descripción
`reload`	Releer los ficheros de configuración y las zonas.
`reload <zona>`	Releer la zona especificada.
`refresh <zona>`	Refrescar para mantenimiento la zona especificada.
`freeze`	Suspender la actualización de todas las zonas.
`freeze <zona>`	Suspender la actualización de una zona.
`thaw`	Habilitar la actualización de todas las zonas y releerlas.
`thaw <zona>`	Habilitar la actualización de una zona y releerla.
`reconfig`	Releer el fichero de configuración y las nuevas zonas.
`stats`	Escribir las estadísticas del servidor en el fichero de estadísticas.
`querylog`	Activar el log.
`dumpdb`	Volcar el estado de la cache al fichero named_dump.db.
`stop`	Salvar las actualizaciones pendientes de los ficheros maestros y detener el servidor.
`halt`	Detener el servidor sin salvar las actualizaciones pendientes.
`trace`	Incrementar en una unidad el valor de debug.
`trace <nivel>`	Cambiar el nivel de debug al especificado.
`notrace`	Cambiar el nivel de debug a cero (no debug).
`flush`	Volcar todas las caches de los servidores.
`status`	Mostrar el estado de un servidor.

El programa rndc (VI)

```
rndc status

number of zones: 10
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF: 0
server is up and running
```