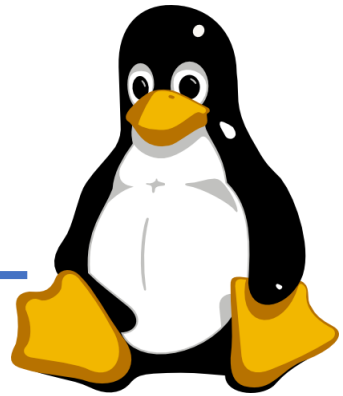
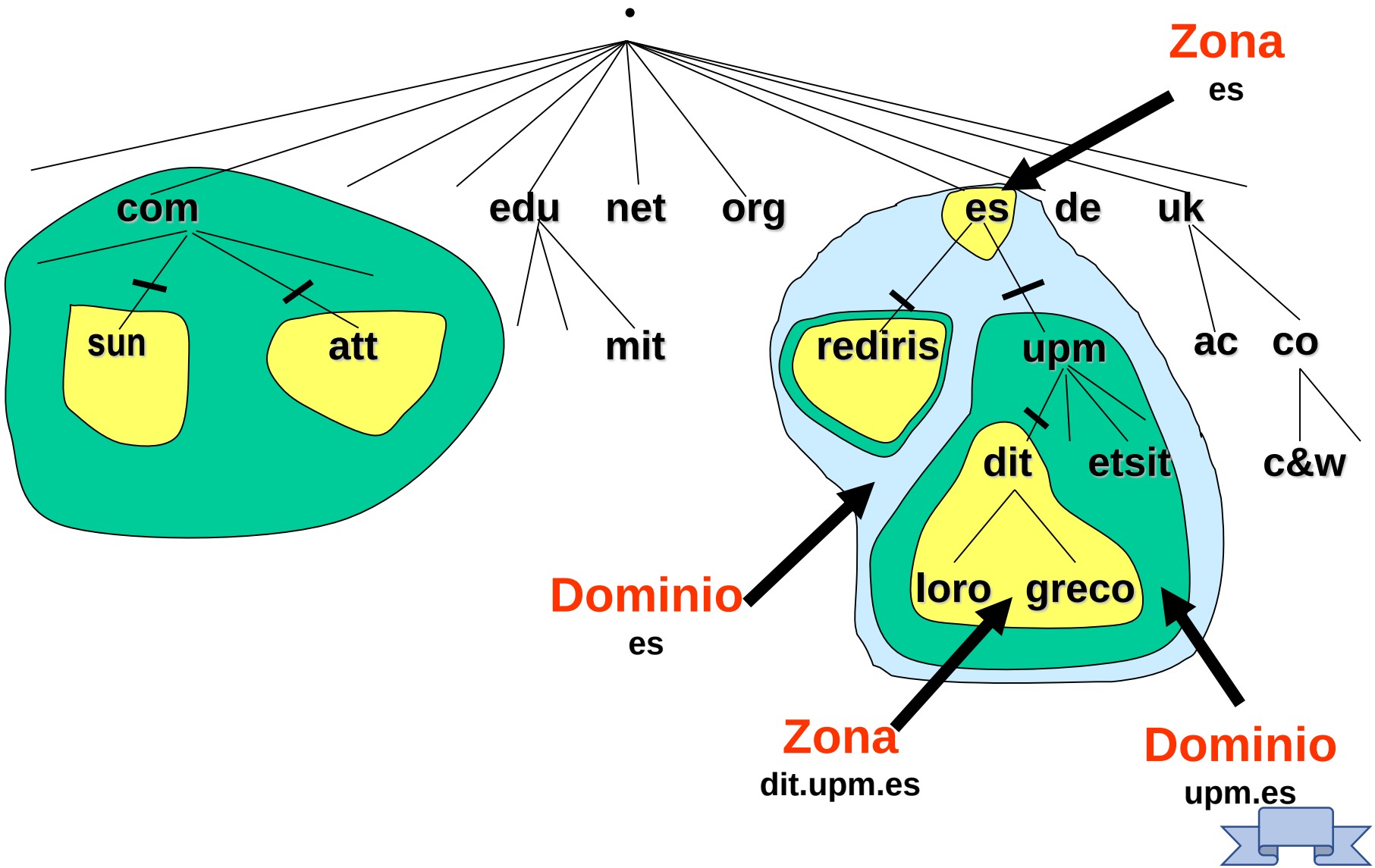
Seguridad en el protocolo DNS

Ing. Denis L. Espinoza Hernández, M.Sc.
denisjev@ct.unanleon.edu.ni



Espacio de nombres DNS

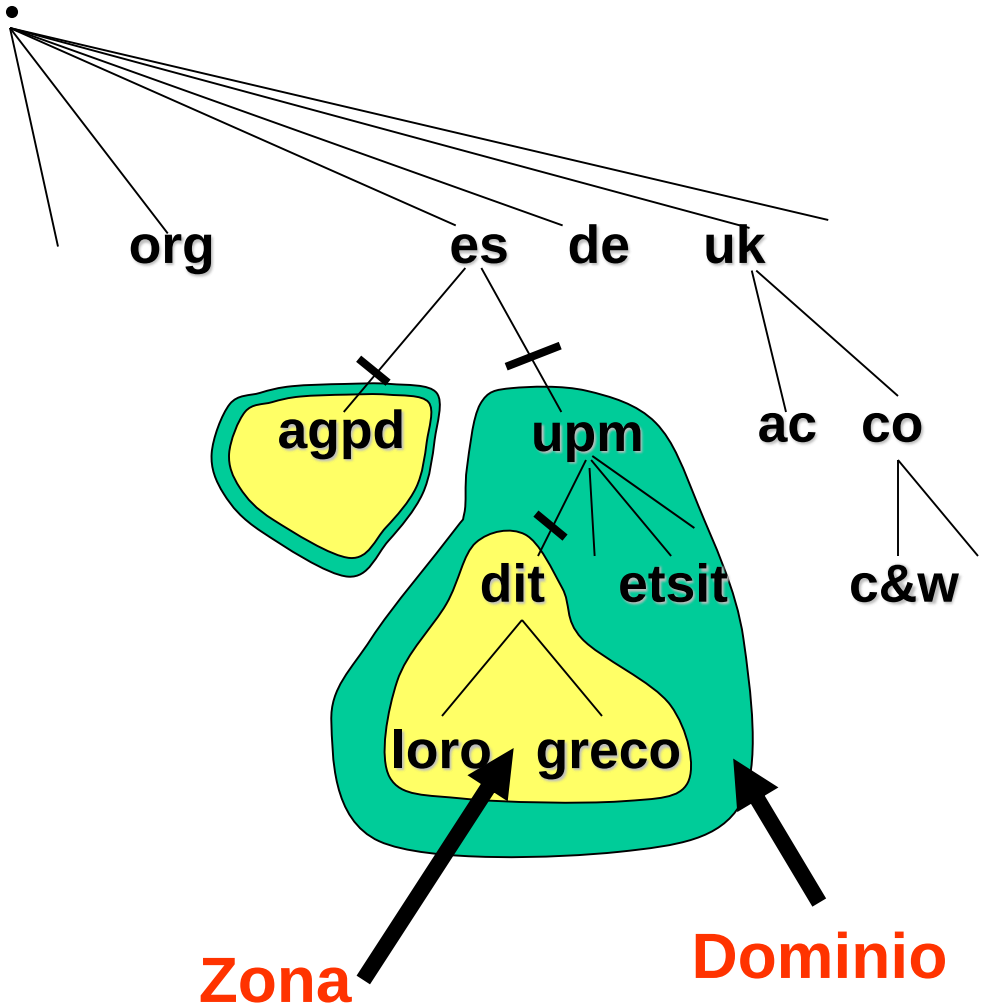


TLD (top level domains)

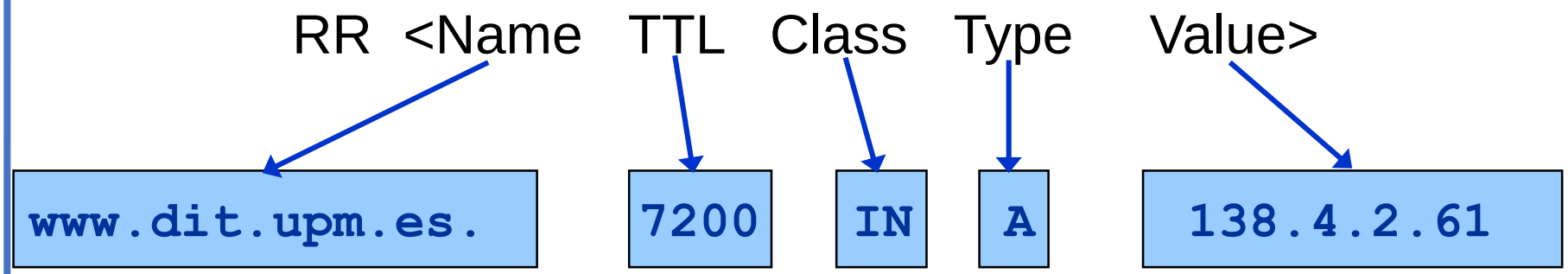
- Generic TLD (gTLD)
  - .COM, .NET, .EDU and .ORG
  - .GOV gobierno USA
  - .MIL militar USA
  - .INT organizaciones internacionales (itu.int, nato.int)
- Country Code TLD (ccTLD)
  - códigos de países ISO-3166
- 12 TLD adicionales
    - .AERO, .BIZ, .CAT, .COOP, .INFO, .JOBS, .MOBI, .MUSEUM, .NAME, .PRO, .TEL, .TRAVEL

Zonas y delegaciones

- Una zona es un límite administrativo
- El administrador de una zona es el responsable de una porción del espacio de nombres de dominio
- Se delega autoridad de padres a hijos



Registros de recursos (RR)



- ***Type***, tipo de RR

A	*IP address*
MX	*Mail eXchanger*
NS	*Name Server*
CNAME	*Canonical Name*
SOA	*Start of Authority*

- ***Value***, depende del tipo de RR

A	Dirección IP
MX	Preferencia+servidor
NS	Nombre de servidor
CNAME	Nombre de dominio
SOA	Varios campos

- ***TTL*** *(time to live)*, cuánto tiempo un RR puede estar en la copia caché antes de ser descartado (en seg.)

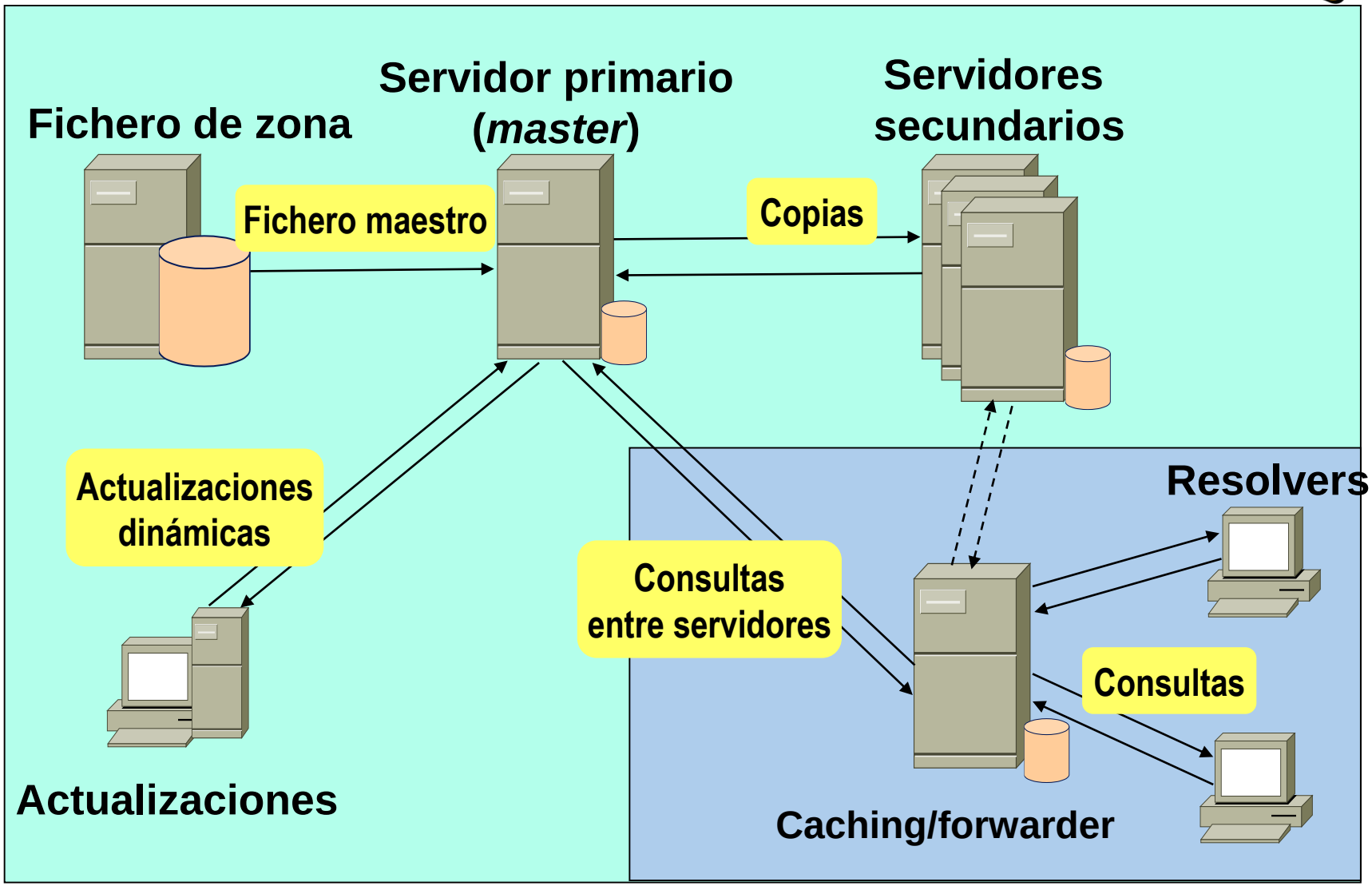
Tipos de Registros DNS

- Internos
  - Authority: NS, SOA,
    - Lista nombres de Servidores de Nombres y Start Of Authority/zona.
  - DNSSEC: DS, DNSKEY, RRSIG, NSEC
    - Usados para DNSSEC
  - Meta types: OPT, TSIG, TKEY, SIG(0)
    - Meta Types: No se almacenan en las zonas DNS se usan sólo en la transferencia de información
  - Indirectos: CNAME, DNAME
    - Aliases
- Terminales:
  - Registros de direcciones: A, AAAA,
  - Informativos: TXT, HINFO, KEY, SSHFP …
    - infomación para las aplicaciones
- No terminales: MX, SRV, PTR, KX, A6, NAPTR, AFSDB
    - contienen nombres de dominio que pueden provocar peticiones adicionales.

Servidores NS

- Responden a consultas y son los *almacenes de información*
- El árbol se distribuye en ***zonas*** y se reparte entre los servidores
  - cada organización, departamento, ISP, etc. puede tener un servidor
    - **servidor local**
- Cada zona disponible en 2 ó más servidores
  - servidor maestro (**primario**)
  - servidores con copias (**secundarios**)
    - Transferencias de zona de acuerdo a parámetros en SOA
  - con autoridad sobre los datos (**authoritative**)
- ¿Cómo se divide en zonas?
  - Cortes en nodos donde una organización quiere tomar control de un subárbol

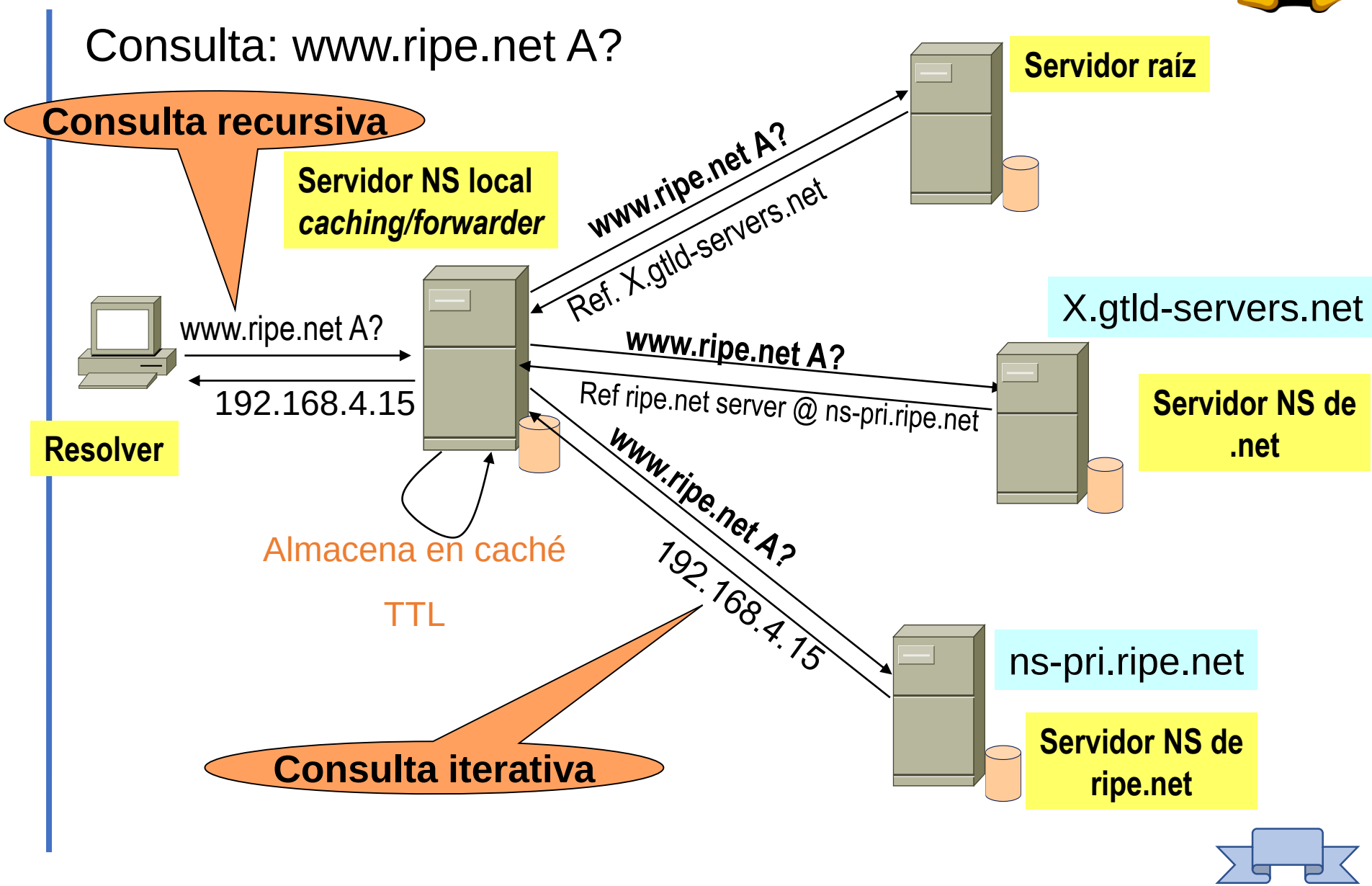
Flujos de datos



Proceso de resolución

- Un *resolver* debe conocer al menos un ***servidor local***
- Cada servidor debe conocer al menos un ***servidor raíz***
  - y a todos los servidores de los dominios jerárquicos inferiores
- *Los servidores raíz* conocen a todos los servidores de dominios de primer nivel
- El *resolver* envía una consulta al servidor
  - si el servidor no puede resolver localmente, contacta con otro servidor (**consulta recursiva**)
  - o devuelve una referencia (**consulta iterativa**)

Proceso de resolución



Protocolo DNS

Id de 16 bits para un par consulta/respuesta

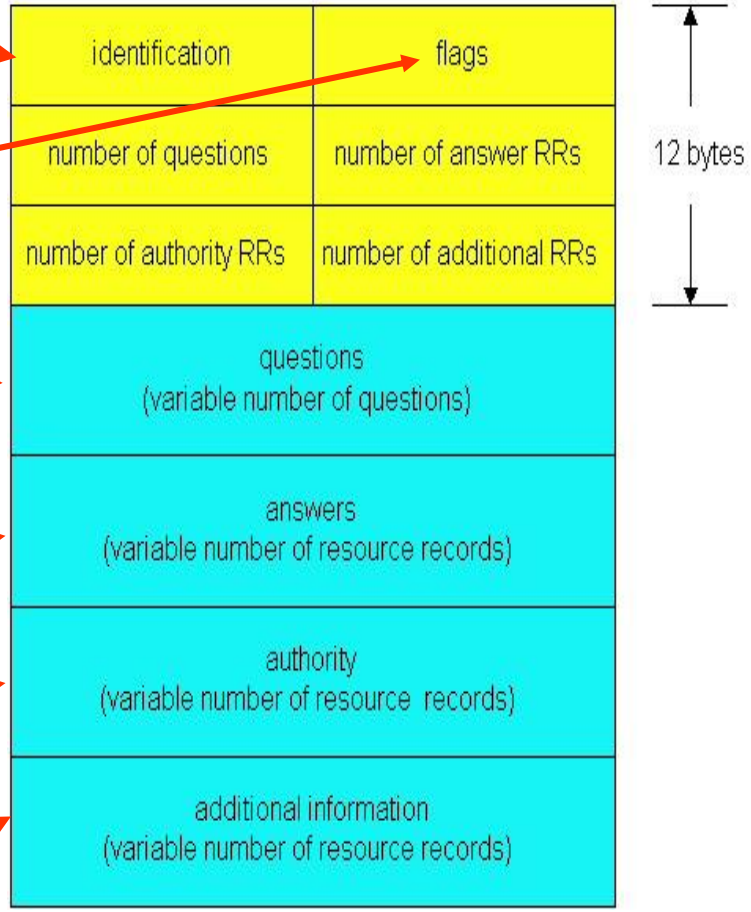
Flags: consulta/respuesta, pide recursión, recursión disponible, etc.

Tipo de consulta (Qtype: A, MX, NS, SOA, PTR, AXFR, …) y otros parámetros

RRs de respuesta

RRs de otros servidores con autoridad

RRs con información adicional sobre los RRs de la respuesta o autoridad



Protocolo DNS

- Transporte
  - UDP con carga útil de 512 octetos, alternativamente TCP
  - Negociación posible para ampliar el tamaño de la carga útil (EDNS0)
  - TSIG permitiría autenticación e integridad salto a salto
- Retransmisión
  - Timeouts y retransmisión hacia otro servidor

Soporte IPv6

- RFC3596 define:
  - Un nuevo tipo de RR (AAAA) para la correspondencia de nombre de dominio a dirección IPv6
  - Un dominio para consultas inversas
    - IP6.ARPA
      - Consulta sobre 2001:db8:1:2:3:4:567:89ab
      - b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.8.b.d.1.0.0.2.ip6.arpa
  - Modificación de consultas que realizan procesados adicionales para buscar una dirección IPv4 (se añade IPv6)
    - consultas NS, SRV, MX
- La versión IP utilizada para la consulta es independiente de la versión de protocolo de los RRs
  - cinco servidores raíz ya tienen dirección IPv6 asignada

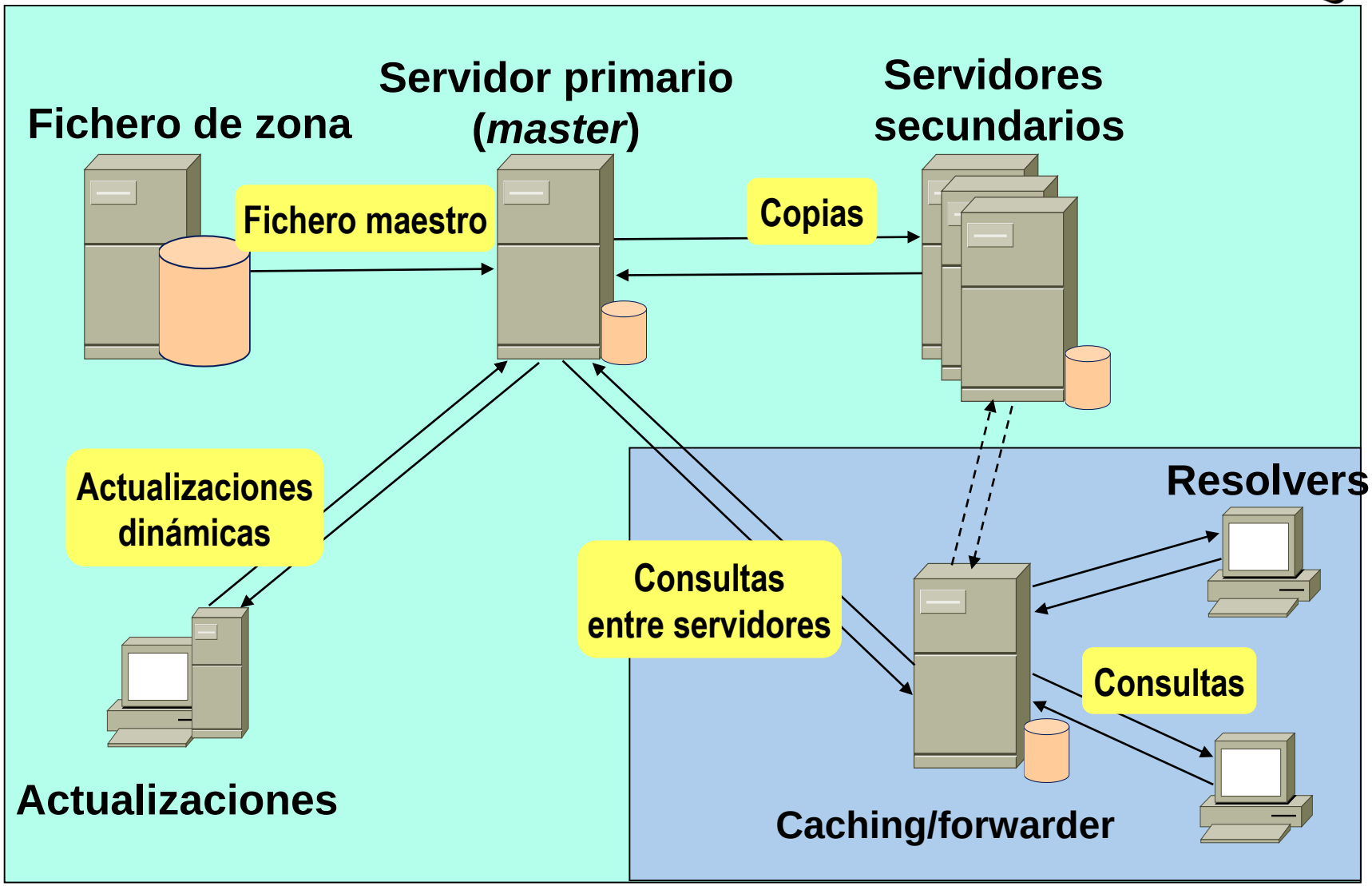
Algunos problemas de DNS

- Tamaño de paquete UDP:
  - 512 para DNS estándar, 4K+ para EDNS0
    - Posible problema con RRSets demasiado grandes
- Delegaciones
  - Padres e hijos sincronizados sobre los nombres de los servidores
  - Secundarios actualizados con los primarios.
    - posibles problemas: permisos, bloqueo del protocolo de transferencia, sincronización de relojes, renumerado del SOA
- Integridad de los datos
  - Envenenado de cachés
- Software antiguo o con errores
  - Porcentaje pequeño

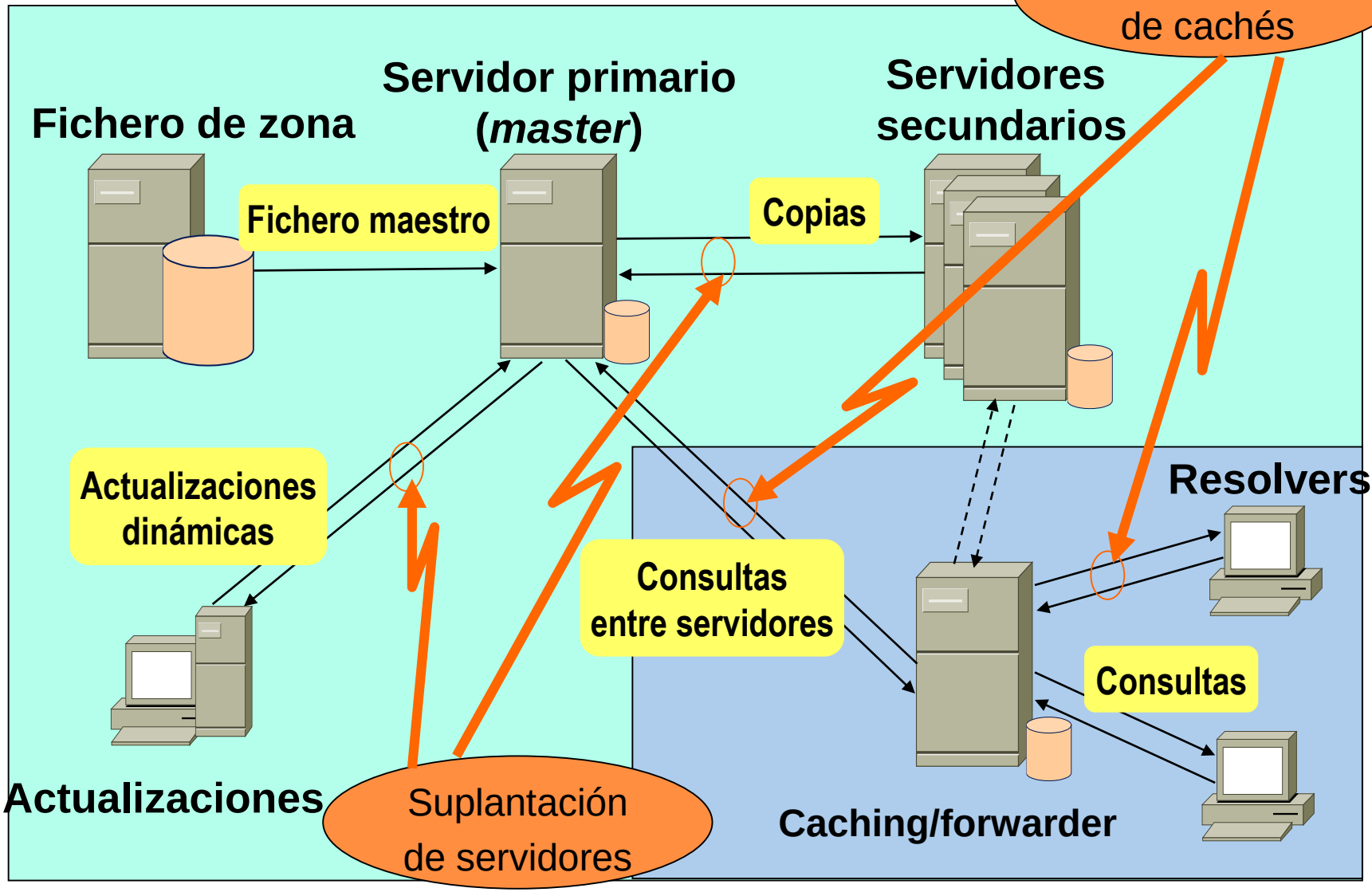
DNS es vulnerable

- Las especificaciones originales no incluyen aspectos de seguridad.
- Filosofía de diseño:
  - datos públicos
  - la restricción de acceso a la información en el espacio de nombres de DNS, no forma parte del protocolo
- Algunas versiones de software de servidor DNS permiten definir control de acceso
- **Solución**: medidas de seguridad + DNSSEC

Flujos de datos



Vulnerabilidades



Vulnerabilidades

- Existen múltiples problemas de seguridad documentados en DNS:
  - Ataques contra el software del servidor
    - Fallos en programas, configuración defectuosa
  - Divulgación de información sensible
  - Suplantación (DNS *spoofing*)
  - Envenenado de cachés
    - Redirecciones maliciosas
  - Ataques de denegación de servicio (DoS)

Divulgación de información sensible

- La operación de **transferencia de zona** (axfr) permite la actualización de los secundarios mediante descarga de información de zona desde el servidor primario.
  - Pero la lista de una zona permite identificar objetivos (servidores de correo, DNS, máquinas no protegidas, …)
    - axfr sobre zona **es (!!)**
  - Con nslookup

```
nslookup
    server sec1.apnic.net
    ls -d icann.org >> datos_zona
```

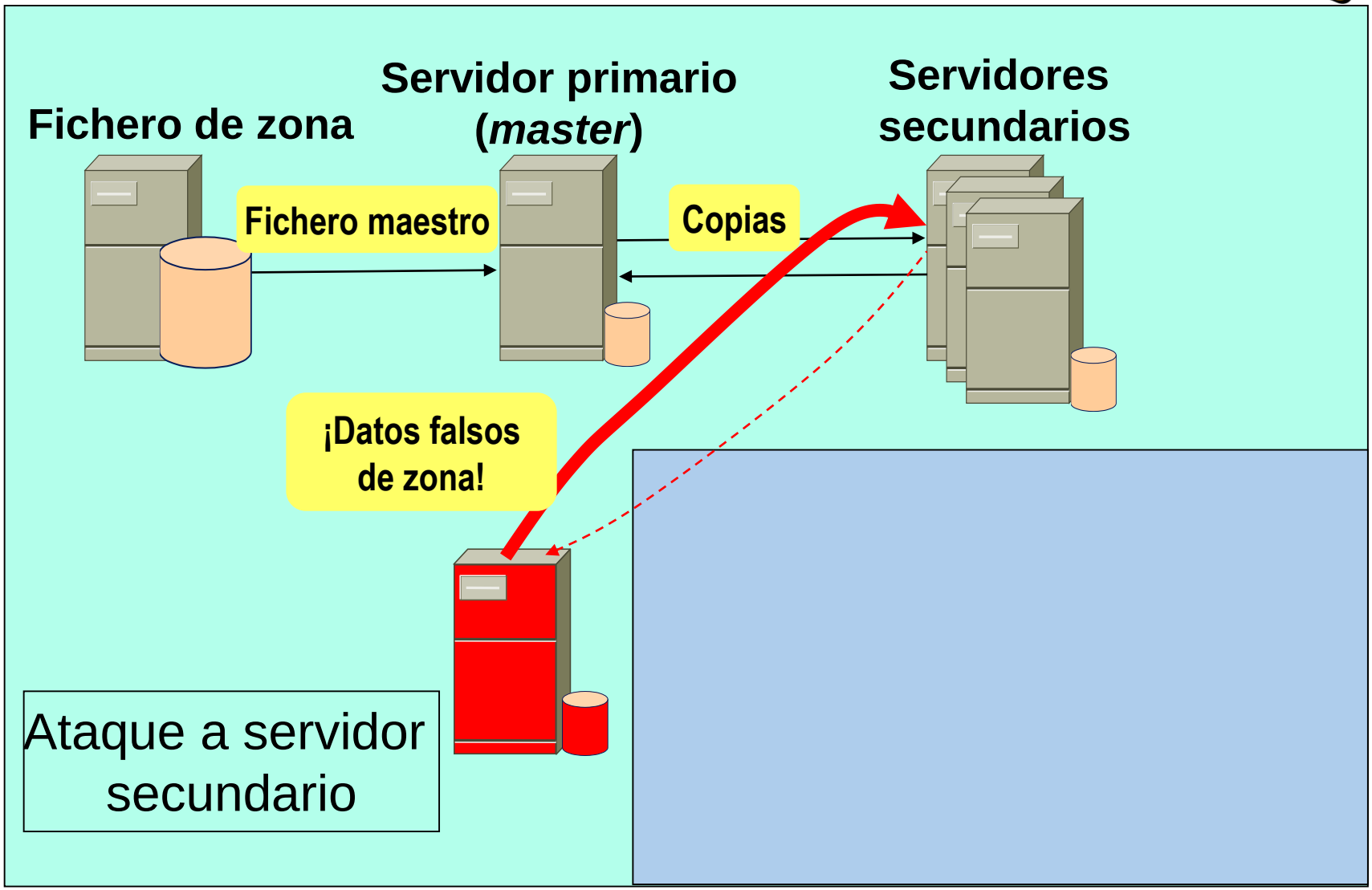
  - Con dig

```
dig @sec1.apnic.net icann.org axfr
dig @marianela.tsm.es tsm.es axfr
```

Divulgación de información sensible. Defensa

- Técnicas de prevención:
  - Restringir **transferencias de zona** (desde primario y todos los secundarios)
    - Configurar el servidor
  - Filtrar el tráfico TCP/53
    - Evita transferencias de zona, pero permite las consultas (que usan UDP)
  - Usar una configuración de servidores "*Split-Horizont DNS*"

Suplantación de primario



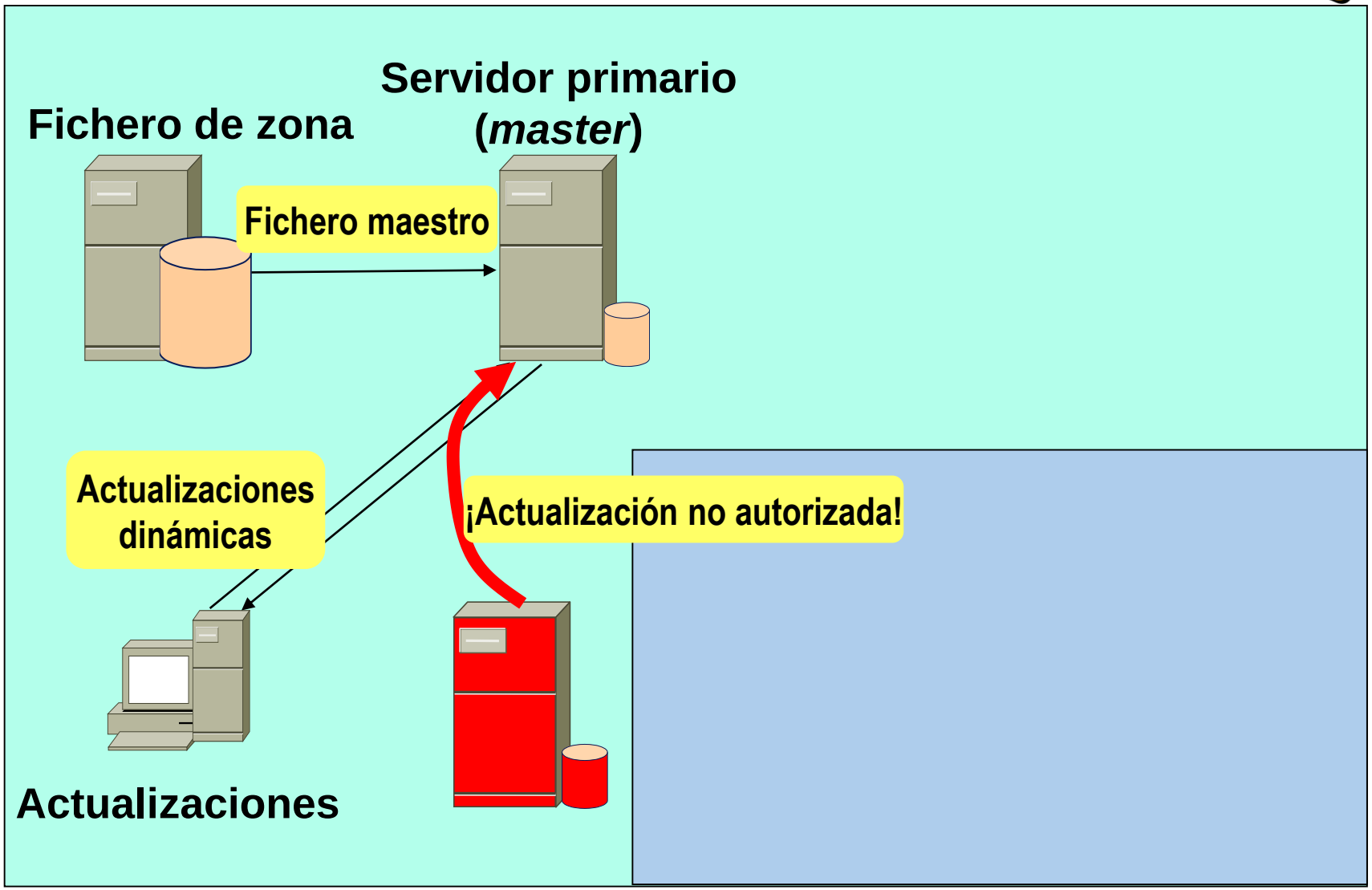
Suplantación de primario. Defensa

- Restringir **transferencias de zona**
  - Opción allow-transfer de BIND

```
zone "ejemplo.com" {
        type master;
        file "db.ejemplo.com";
        allow-transfer {192.168.4.25; };
};
```

    - Pero no protege contra posible suplantación de primario
    - ataque a datos de servidor secundario!
  - Solución: uso de **TSIG**

Suplantación de origen de actualización



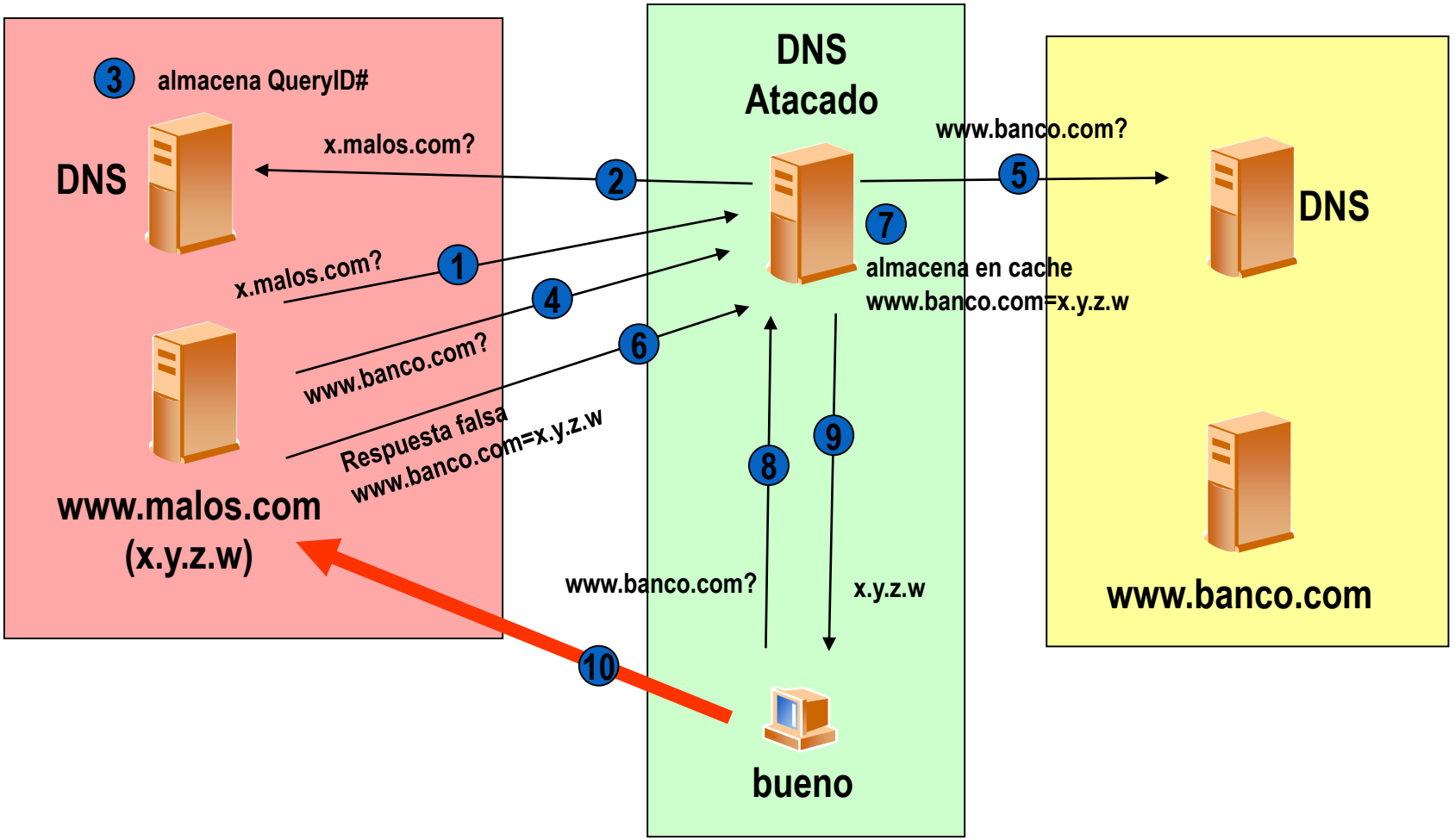
Defensa

- Restringir actualizaciones dinámicas
  - Protege, en parte, contra posible suplantación de origen de actualización
    - ataque a datos de servidor primario!
  - Prohibirlas si no son estrictamente necesarias
  - En caso de utilizarlas, restringir
    - a direcciones individuales
    - usar **TSIG**
  - Si se restringe a direcciones, la entrada de la red corporativa debe utilizar mecanismos *anti-spoofing*
    - en el router frontera
    - en el bastión
  - Otra alternativa es delegar una nueva zona con el nombre de dominio al que correspondan las actualizaciones (confinar una zona)

Envenenado de cachés (*data spoofing*)

- Ataques muy conocidos y analizados
  - datos maliciosos añadidos en los mensajes de respuesta (*additional records*) que se almacenan en la caché de la víctima
  - consultas-respuestas falsificadas
  - respuestas falsificadas
- Consecuencias:
  - Redirección de tráfico web
    - a un sitio con cierta propaganda
    - a un banco falso para capturar passwords
    - a un sitio con información manipulada
  - Posible "*man-in-the-middle*"

Ejemplo ataque: Envenenado de cachés

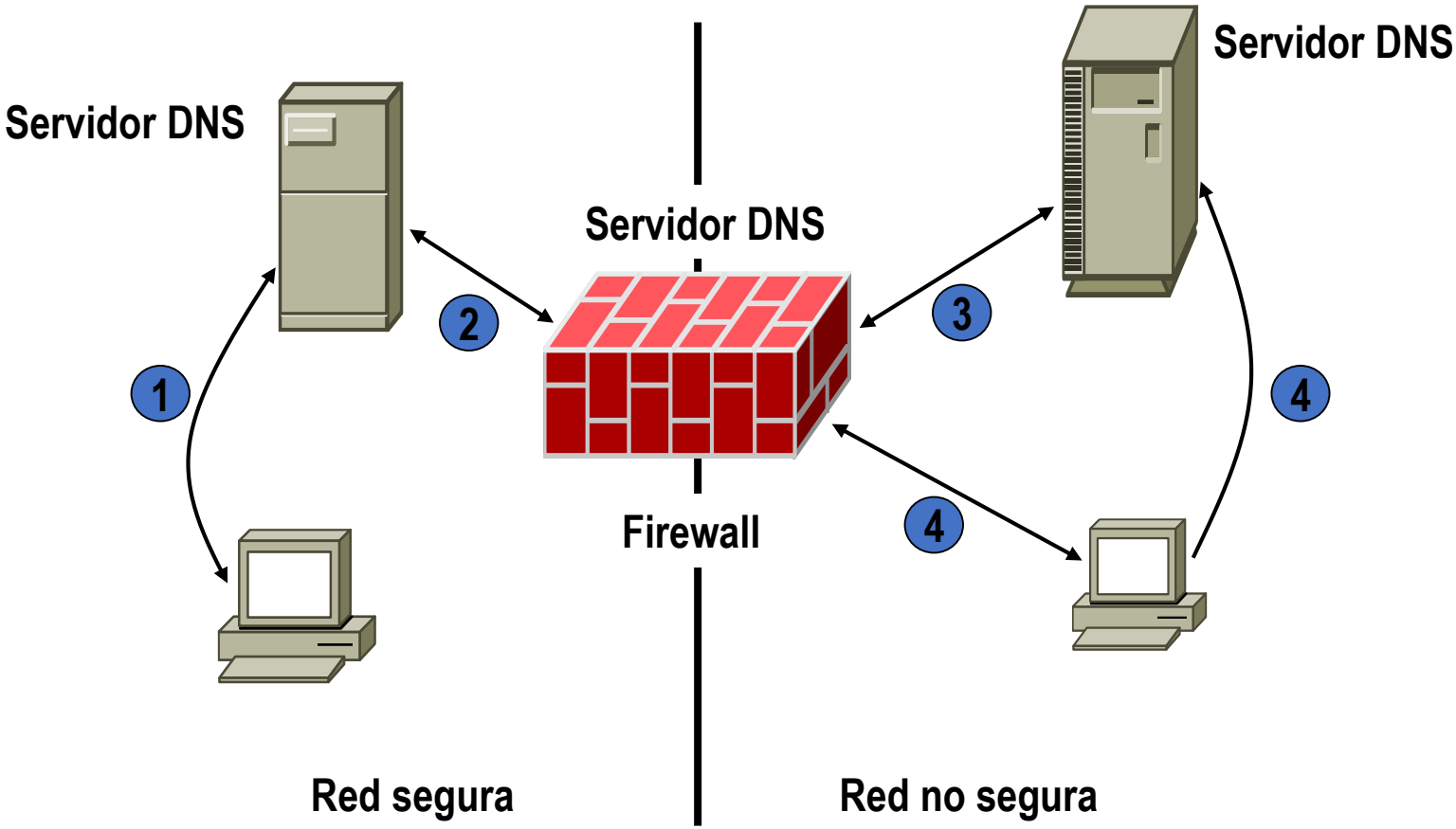


Protección contra envenenado de cachés

- Evitar que un servidor resuelva **consultas recursivas**
  - ¡Pero sí debe hacerlo para resolvers!
  - Si un servidor acepta consultas recursivas puede reenviar consultas a un servidor malicioso y recibir información contaminada
  - Si no acepta consultas recursivas, sólo devuelve referencias (NSs)
    - los servidores raíz siempre devuelven referencias

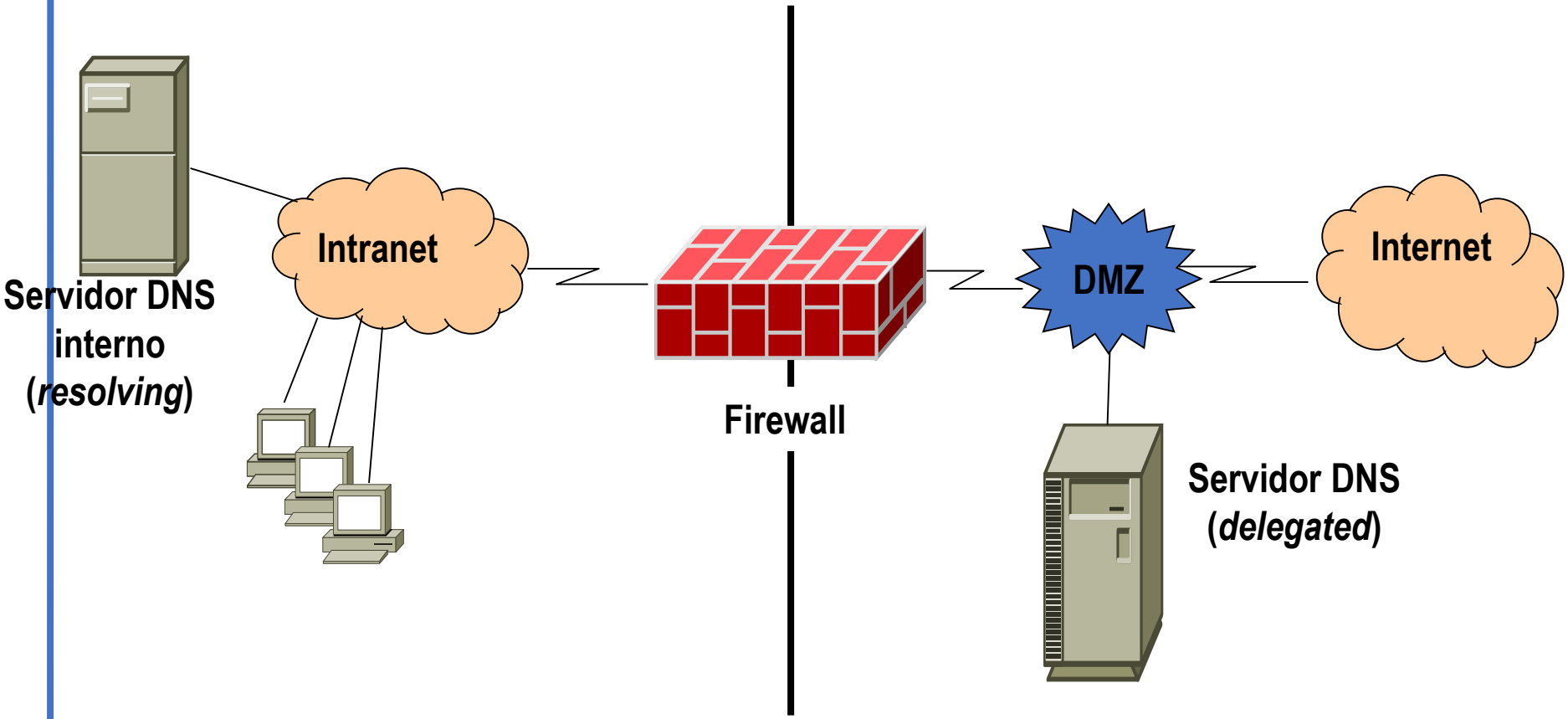
Escenarios de administración de servidores (i)

- Coexistencia de DNS con firewalls



Escenarios de administración de servidores (ii)

- Dominios internos y externos (*Split-Horizont DNS*)



Medidas generales de seguridad (i)

- Instalar la última versión del software del servidor
  - Minimiza posibilidades de ataque
  - Por ejemplo, ver vulnerabilidades y versiones en http://www.isc.org/products/BIND/bind-security.html
- Evitar puntos donde se pueda producir un fallo completo.
  - Previene el ataque por DoS y otros posibles fallos del servicio
    - Todos los servidores DNS en la misma subred… NO!
      - gestionar el mantenimiento de secundarios por terceros
    - Todos los servidores detrás del mismo router… NO!
    - Diversificar caminos físicos de acceso a la red
- Filtrar tráfico
  - Dejar pasar tráfico sólo al puerto 53 UDP

Medidas generales (ii)

- El proceso servidor (*named*) no debe ejecutarse con privilegios de root
  - puede ser un punto de ataque a la máquina si se descubre alguna vulnerabilidad en el software del servidor
- El proceso servidor debe ejecutarse confinado en un directorio particular
  - chroot()
  - no queda así expuesto todo el sistema de directorios de la máquina
- Deshabilitar el proceso en toda máquina que no sea servidor DNS.

DNSSEC

- Autenticación del origen
  - es quien dice ser
- Integridad (contenido)
  - no ha sido manipulado
- Autorización
  - comprobar derechos de acceso

→ **DNSSEC**

- Confidencialidad (contenido)
  - nadie más escucha
- No repudio

→ **Implementaciones**

Extensiones de Seguridad: DNSSEC

- Marco de seguridad
- Mecanismos para **autenticación de servidores**
  - TSIG, RFC 2845
  - Previene contra los ataques por suplantación de servidores
    - en transferencias de zona
    - en actualizaciones
- Mecanismos para **integridad de datos y autenticación**
  - RFC 4033 a 35
  - Previene contra envenenado de cachés en consultas y respuestas
  - Criptografía de clave pública, los datos intercambiados se firman digitalmente
  - Nuevos registros para
    - Mantener firmas digitales: RRSIG
    - Mantener claves públicas para verificar las firmas: DNSKEY
    - Protección sobre entradas no existentes: Registros (NSEC)

Transaction Signatures (TSIG)

- Independiente del resto de mecanismos DNSSEC
- Firma de mensajes DNS
  - Actualizaciones dinámicas
  - Transferencias de zonas
- Basado en algoritmos de clave compartida
- Utiliza HMAC-MD5: función “one-way hash” que genera resúmenes (digest) de 128 bits partiendo de una clave de 128 bits (recomendado)
- Se firma el mensaje DNS completo y otros campos adicionales:
  - Fecha y hora, para evitar ataques de tipo “replay” (necesario sincronizar relojes: NTP)

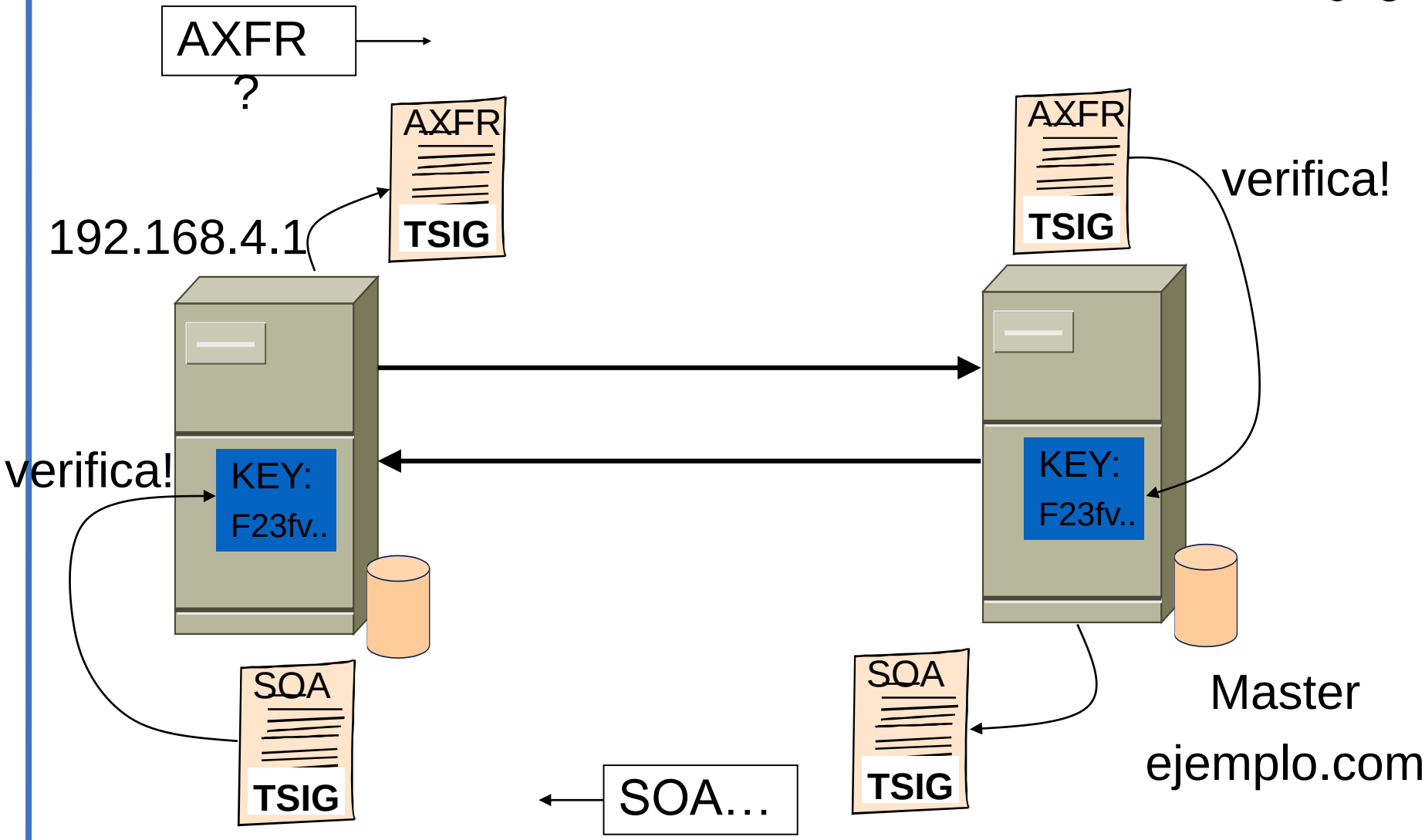
Transaction Signatures (TSIG)

- Registro TSIG. Es un meta-registro:
  - No aparece en ficheros de zona
  - No se guarda en cachés
  - Es parte de la configuración del servidor de nombres
- Por ejemplo (BIND):

```
key dns1-dns2.ejemplo.com. {//nombre de clave para dns1 y dns2
                                  // (igual para ambos extremos)
  algorithm hmac-md5;    // algoritmo
  secret "skrKc4Twy/cIgIykQu7JZA==";// clave codificada en
 base 64
};
```

- Creación de claves: utilidad dnskeygen o dnssec-keygen de BIND
- ¡¡La clave debe estar BIEN protegida!!

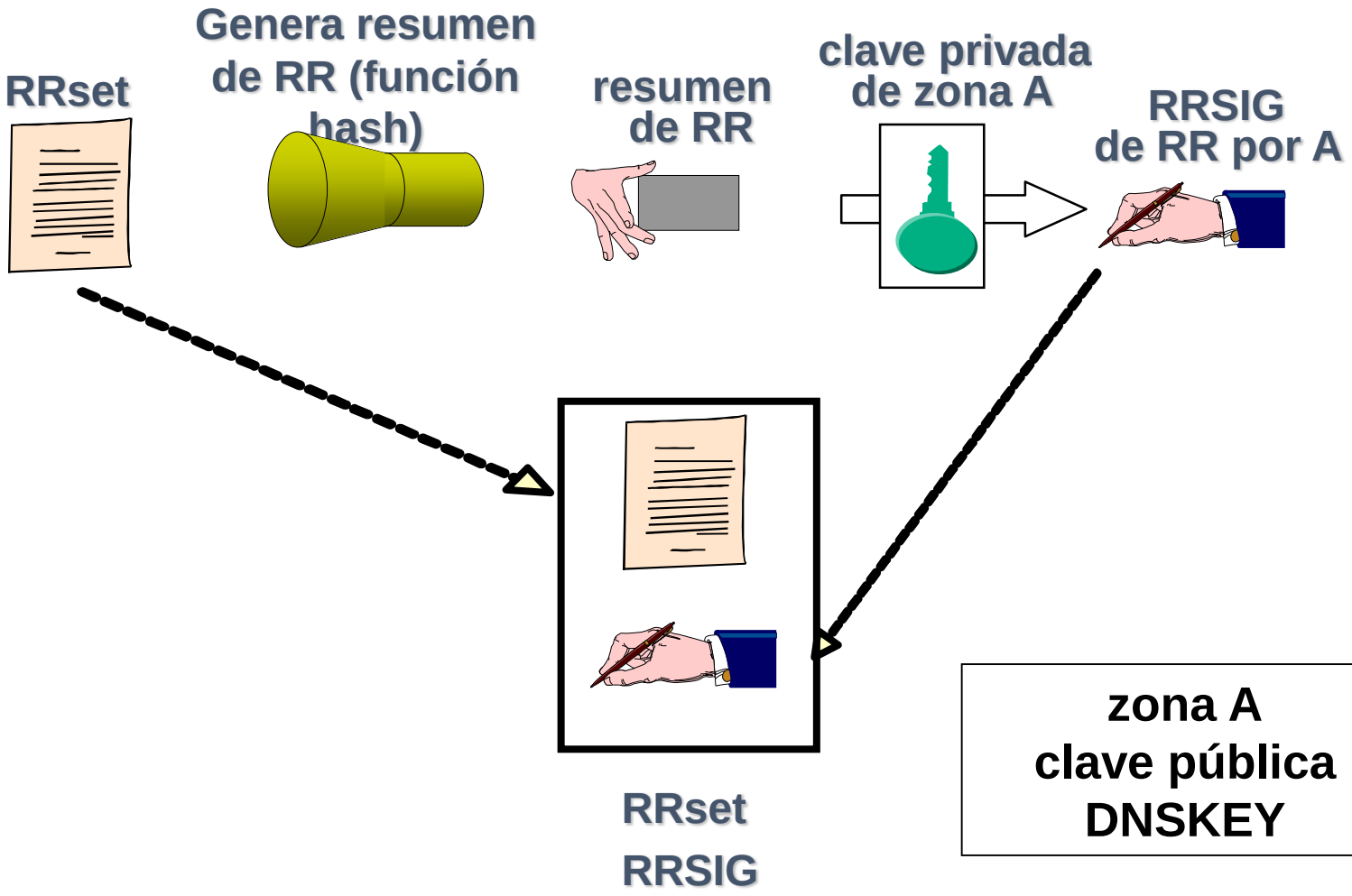
Ejemplo TSIG



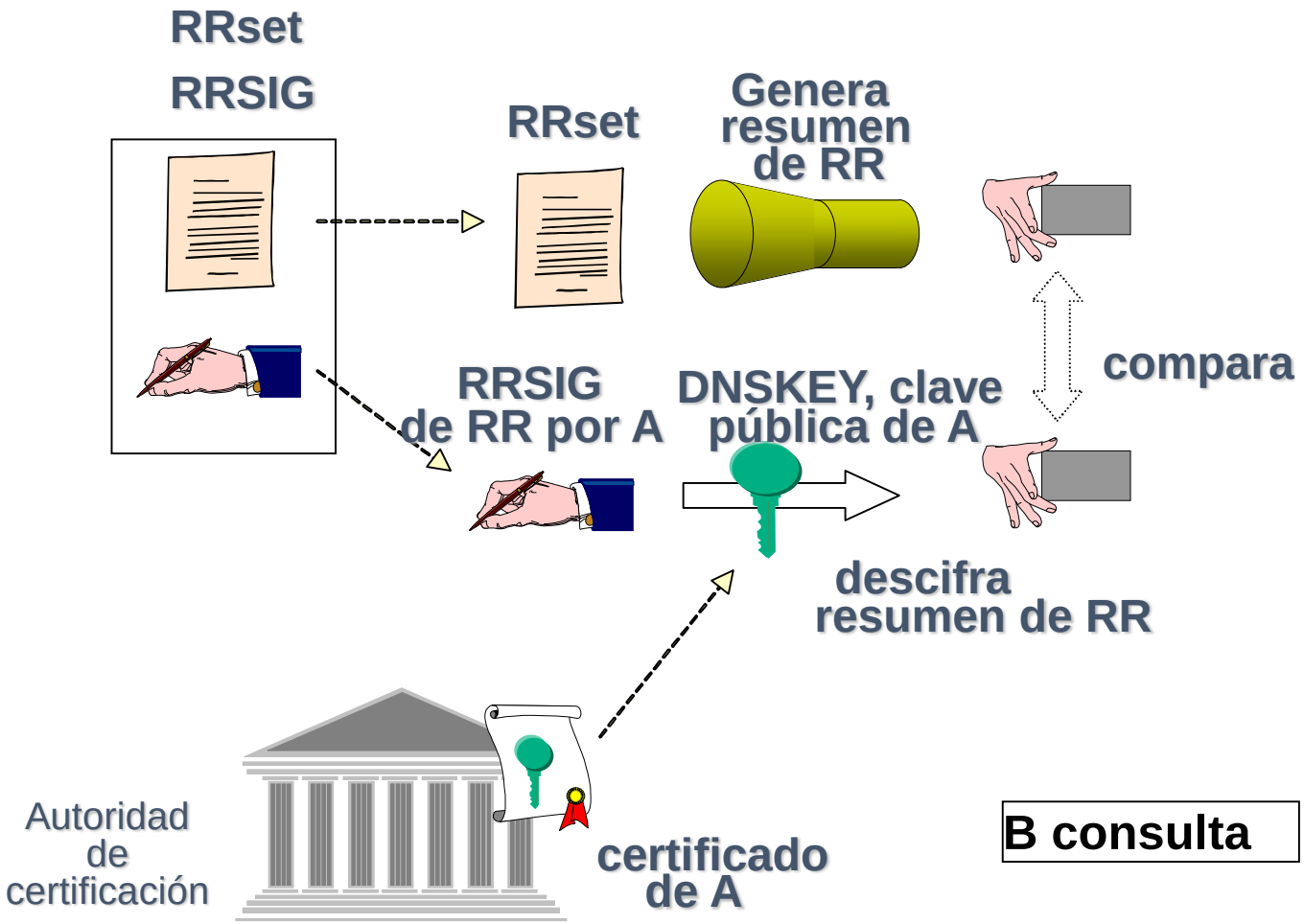
DNSSEC

- **Integridad y autenticación** mediante firmas de RRsets con claves privadas
- Para verificar la firma (RRSIG) se usan claves públicas (DNSKEY)
- Cada **subzona** firma los RRsets de la zona con su **clave privada**
  - La autenticidad de su DNSKEY se establece mediante la firma de esa clave por la zona jerárquica superior
- Idealmente, sólo la clave pública de la raíz tendría que distribuirse “manualmente”

Firmando RRsets



Verificando RRset firmado



Resumen: Nuevos Registros para Seguridad en DNS

- RRSIG
  - Mantiene la firma digital de un conjunto de datos (claves asimétricas)
- DNSKEY
  - Mantiene una clave pública de una zona
- NSEC
  - Permite certificar la inexistencia de datos en el DNS
- TSIG
  - Firma de mensajes (mediante claves simétricas para mejorar la velocidad)
  - No se almacena en el DNS

Prestaciones DNSSEC

- El uso de DNSSEC tiene una influencia importante sobre las prestaciones del DNS debido a:
  - Mayor tamaño de las bases de datos (en ficheros y en memoria ocupada por los servidores)
  - Mayor tamaño de los paquetes de respuesta (contienen registros DNSKEY y RRSIG)
    - ¡Pueden llegar a provocar el uso de TCP en vez de UDP!
  - Consultas adicionales para obtener claves de dominios superiores
    - Fácil de evitar almacenando las claves en caché
  - Capacidad de computación necesaria para verificar las firmas y validar las claves
    - Necesaria en servidores de nombres locales y resolvers

Resumen DNSSEC

- Ventajas:
  - Añade integridad y autenticación al DNS “clásico”
- Desventajas:
  - Disminuye las prestaciones debido al:
    - Mayor tamaño de los ficheros
    - Mayor tamaño de los mensajes
    - Consultas adicionales para obtener claves
    - Uso frecuente de TCP en vez de UDP
    - Mayores retardos (validación de datos)
  - Muy complejo construir la cadena de confianza