Servizos de nomes de dominio

Habitualmente usamos os sistemas de nomes para acceder a recursos doutros computadores dentro da rede local ou en Internet. Un sistema de nomes permite identificar aos ordenadores e outros equipos dunha rede cun nome que poida ser fácil de lembrar polos usuarios.

Un sistema de nomes asocia cada un dos nomes de equipos dentro dunha rede cos seus correspondentes enderezos IP de tal forma que a partir do nome dun equipo pódese obter o enderezo IP que ten ese equipo na rede.

Os sistemas de nomes pódense clasificar en dous tipos:

- **Sistemas de nomes planos**: Non utilizan ningún sistema baseado nunha xerarquía. Determínase a pertenencia a subredes ou outras organizacións por calquera outra condición xerarquica. En redes Microsoft nas que non se traballa en dominio úsase un sistema de nomes plano que asigna aos ordenadores nomes como PC1, PC2, servidor que non representan unha organización xerarquizada. Este sistema de nomes chámase NetBIOS e pode usar un servidor de nomes WINS.
- **Sistemas de nomes xerarquicos**: Caracterízanse polo nome de cada equipo dunha rede que representa a pertenencia do equipo a unha organización xerarquizada ou organizada en forma de árbore. O enderezo postal é un claro exemplo (non dun sistema informático) de tipo xerárquico. En Internet úsase un sistema de nomes xerárquico para identificar ordenadores. Por exemplo www.mec.es indica o ordenador www pertencente ao dominio mec.es.

Un sistema de nomes plano non se pode usar en redes grandes como Internet, dado que non se pode repetir o nome de dous ordenadores na rede e sería difícil para os administradores buscar nomes que non se repitan. Por outra banda, a xestión do sistema de nomes planos debería estar totalmente centralizada. Cun sistema de nomes xerárquico como o usado en Internet, pódense ter moitos ordenadores con nome www sempre que pertenzan a diferentes organizacións ou dominios e a xestión dos nomes está distribuída.

Sumario

Un pouco de historia

Inicialmente, o DNS naceu da necesidade de lembrar facilmente os nomes de todos os servidores conectados a Internet. Nun inicio, SRI (agora SRI International) aloxaba un arquivo chamado HOSTS que contiña todos os nomes de dominio coñecidos . Cada sitio que tiña que resolver nomes de host na rede descargaba este único arquivo. O crecemento explosivo da rede causou que o sistema de nomes centralizado no arquivo hosts non resultase práctico.

A medida que o número de hosts de Internet creceu, o tráfico que se xeraba co proceso de actualización aumentaba, ademais do tamaño do arquivo de hosts. Fíxose necesaria a existencia dun novo sistema que ofrecese características como escalabilidad, administración descentralizada e compatibilidade con varios tipos de datos.

DNS introduciuse en 1984 e converteuse neste novo sistema...

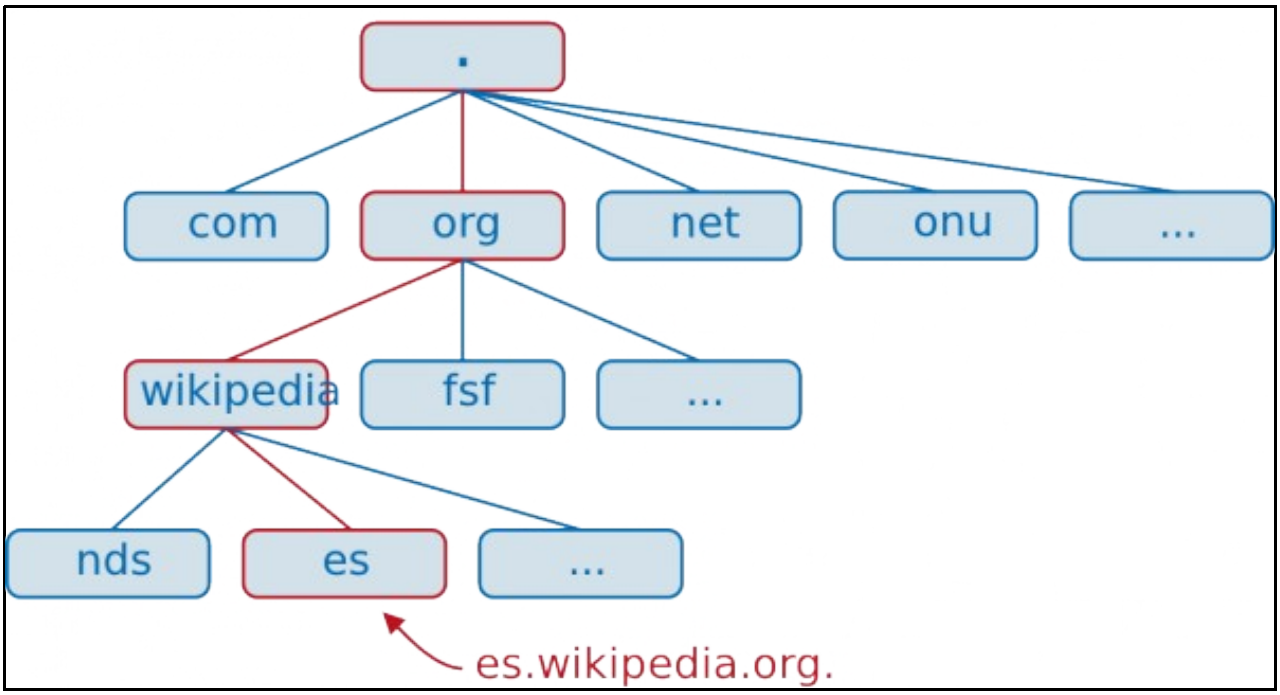
Funcionamento do servizo DNS

Os usuarios xeralmente non se comunican directamente co servidor DNS: a resolución de nomes faise de forma transparente polas aplicacións do cliente (por exemplo, navegadores, clientes de correo e outras aplicacións que usan Internet). Ao realizar unha petición que require unha procura de DNS, a petición envíase ao servidor DNS local do sistema operativo. O sistema operativo, antes de establecer algunha comunicación, comproba se a resposta atópase na memoria caché. No caso de que non se atope, a petición enviarase a un ou máis servidores DNS.

A maioría de usuarios domésticos utilizan como servidor DNS o proporcionado polo provedor de servizos de Internet. O enderezo destes servidores pode ser configurado de forma manual ou automático mediante DHCP. Noutros casos, os administradores de rede teñen configurados os seus propios servidores DNS.

En calquera caso, os servidores DNS que reciben a petición, buscan en primeiro lugar se dispoñen da resposta na memoria caché. Se é así, serven a resposta; en caso contrario, iniciarían a procura de maneira recursiva. Unha vez atopada a resposta, o servidor DNS gardará o resultado na súa memoria caché para futuros usos e devolve o resultado.

Xerarquía DNS



O espazo de nomes de dominio é unha base de datos distribuida entre múltiples servidores DNS, que almacena los nombres DNS de equipos xunto cos seus enderezos IP. É unha estrutura xerárquica organizada en forma de árbore con varios niveles de dominio. As follas e os nodos da árbore utilízanse como etiquetas dos medios. Un nome de dominio completo dun obxecto consiste na concatenación de todas as etiquetas dun camiño. As etiquetas son cadeas alfanuméricas (con '-' como único símbolo permitido), deben contar con polo menos un carácter e un máximo de 63 caracteres de lonxitude, e deberá comezar cunha letra (e non con '-') (ver a RFC 1035, sección "2.3.1. Preferencia nomee da sintaxe "). As etiquetas individuais están separadas por puntos. Un nome de dominio termina cun punto (aínda que este último punto xeralmente se omite, xa que é puramente formal). Un FQDN correcto (tamén chamado Fully Qualified Domain Name), é por exemplo: www.example.com. (Incluíndo o punto ao final)

Un nome de dominio debe incluír todos os puntos e ten unha lonxitude máxima de 255 caracteres.

Un nome de dominio escríbese sempre de dereita a esquerda. O punto no extremo dereito dun nome de dominio separa a etiqueta da raíz da xerarquía (en inglés, root). Este primeiro nivel é tamén coñecido como dominio de nivel superior (TLD).

Cada servidor DNS encárgase dunha ou varias zonas. Cada zona contén a información necesaria para resolver os nomes das máquinas de un ou máis dominios.

Os obxectos dun dominio DNS (por exemplo, o nome do equipo) rexístranse nun arquivo de zona, situado nun ou máis servidores de nomes.

Tipos de dominio

Respecto desa estrutura xerárquica, existen os seguintes tipos de dominios:

- **Dominio raíz**: deste dominio colga toda a estrutura do espazo de nomes DNS. Simbolízase cun punto. Baixo o directorio raíz hai dominios de primeiro nivel. Encárgase de xestionar a información sobre os dominios de primeiro nivel, en concreto, sobre os nomes deses dominios e sobre os servidores encargados da xestión deses dominios. O organismo que se encarga da súa xestión é ICANN.
- **Dominios de primeiro nivel**: son dominios que na estrutura do espazo de nomes DNS atópanse baixo o dominio raíz. A un dominio deste tipo tamén se lle chama TLD. Dominios deste tipo son .com, .org e .es entre outros. Baixo un TLD hai dominios de segundo nivel. Da xestión dun dominio de primeiro nivel encárgase unha determinada organización que usa varios servidores DNS. Da xestión do dominio .es encárgase Red.es. Os servidores DNS deste nivel conteñen información relativa aos servidores de dominio de segundo nivel dependentes do dominio. Por exemplo, cada servidor do dominio .es ten información sobre os servidores de dominios como mec.es e xunta.es.
- **Dominios de segundo nivel**: son os dominios que se atopan baixo os TLDs. Cada un destes dominios está rexistrado a favor dunha determinada entidade (empresa, universidade, órgano, persoa, etc.). A entidade propietaria do dominio é a encargada da xestión do dominio. Para un dominio deste tipo téñense un ou varios servidores DNS que teñen información sobre máquinas dispoñibles no dominio, sobre posibles subdominios e sobre servidores DNS do dominio e dos subdominios. Cando unha entidade desexa dispor dun dominio, debe rexistralo ante un rexistrador oficial autorizado por ICANN. Dominios de segundo nivel son wikipedia.org, mec.es, google.com e outros moitos.
- **Subdominios**: Son dominios que hai baixo un dominio de segundo nivel ou baixo outro subdominio. Un subdominio non ten que ser rexistrado como un dominio de segundo nivel. É o propietario do dominio de segundo nivel quen decide a existencia ou non de subdominios. Nun subdominio pode haber servidores encargados de toda a xestión do subdominio aínda que tamén esa xestión pódese levar a cabo desde os servidores de segundo nivel. Para cada subdominio tense información sobre as máquinas e servidores pertencentes ao subdominio.

Dominios de primeiro nivel

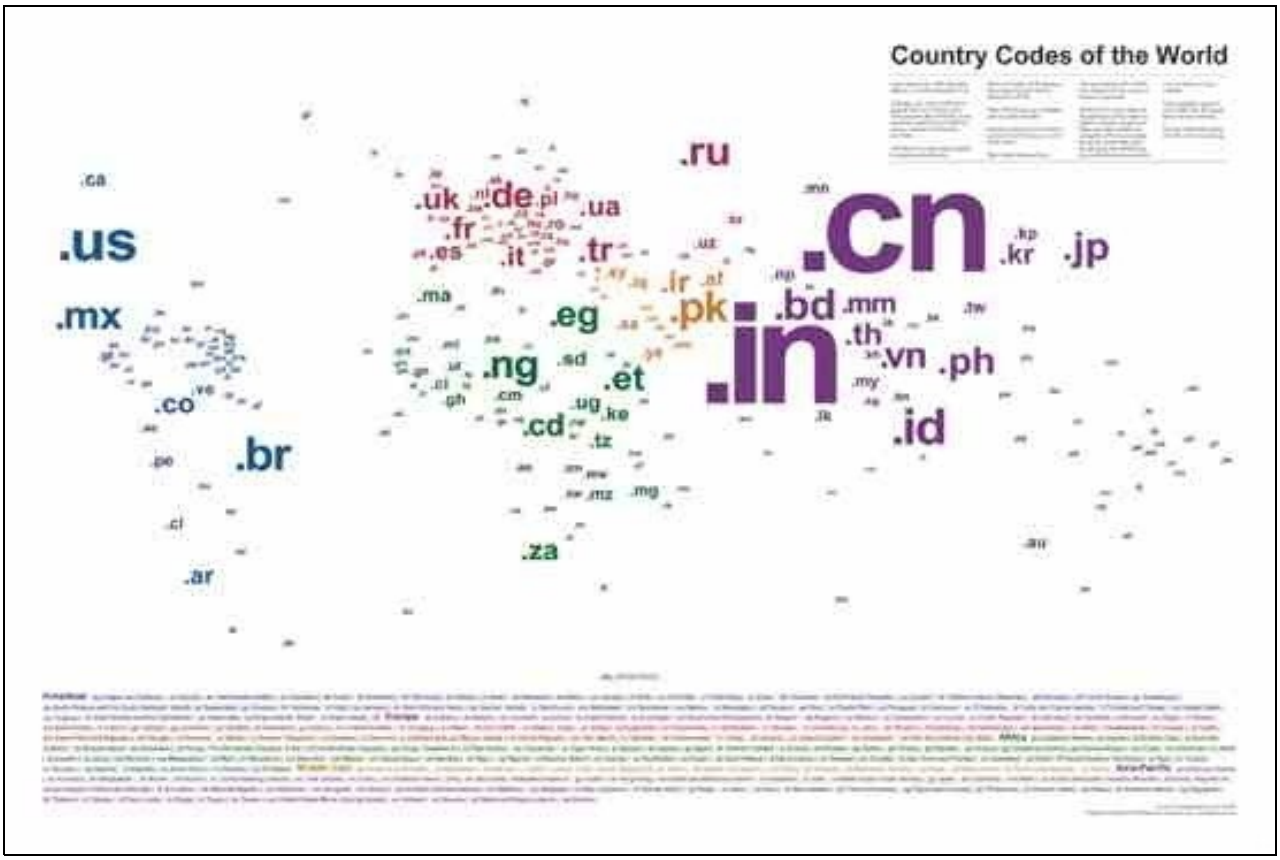
ICANN ten actualmente autorizados un gran número de dominios de primeiro nivel ou TLDs. Nun principio, estableceu dous tipos de TLDs:

- **gTLD**: Dominios de primeiro nivel xenéricos. Nun principio establecéronse seis dominios deste tipo e todos tiñan tres letras. Para que algúns dominios de segundo nivel pertenzan a algúns destes gTLDs deben cumprir unhas restricións.

Dominios de primeiro nivel xenéricos

gTLD	Funcionalidade
.com	Orientado a obxectivos comerciais.
.net	Para entidades que están relacionadas con Internet.
.org	Para organizacións.
.int	Reservado a organismos internacionais. Deben cumprir unhas restricións.
.mil	Reservado a organismos de carácter militar. Deben cumprir unhas restricións.
.edu	Reservado a institucións educativas. Deben cumprir unhas restricións.

- **ccTLD**: dominios xeográficos ou de país. Simbolízanse con dúas letras representativas do nome do país. Os dominios de segundo nivel que pertenzan a un destes dominios deben pertencer ao país correspondente. Son dominios deste tipo .es para España, .fr para Francia ou .co para Colombia. O dominio .eu non é para un país senón para a Unión Europea. Dominios como .fm non son na actualidade dominios de país aínda que teñan dúas letras (é xenérico para emisoras de radio).



Un dominio xenérico especial é .arpa que serve para realizar resolucións inversas e cuxa función a comprenderás máis adiante. Creáronse outros dominios xenéricos como .biz (para empresas), .gov (para organismos de goberno) e outros que mesmo teñen máis de tres letras como .info.

Dentro dos gTLD pódense considerar outros subtipos como:

- *sTLD*: patrocinados por fundacións independentes. Exemplos destes son .aero para aeroportos e .travel para axencias de viaxe. Adoita ser bastante caro obter dominios deste tipo.
- *lTLD*: trátase de dominios lingüísticos que están destinados a fomentar o uso dunha lingua. Por tanto, as páxinas web accesibles a través deses dominios estarán na lingua correspondente. Exemplos destes dominios son .cat para o catalán, .gal para o galego. Hai que aclarar que non é necesario que estes dominios pertenzan ao país ou rexión correspondente á lingua que fomentan. Tamén debes saber que nos dominios ccTLD pódese usar calquera lingua, por exemplo, nun dominio .es pode haber páxinas web escritas en inglés.

Resolución de nomes de dominio

Os clientes DNS realizan as súas consultas a través de resolutores. Un resolutor é un proceso que se executa a petición dun programa que usa un nome DNS para establecer unha conexión. O resolutor xestiona o proceso de consulta do nome DNS, recepción da resposta relativa á consulta e entrega do resultado. Os procesos resolutores execútanse nos clientes DNS e en servidores que deben dar respostas a clientes DNS.

Existen dous tipos de consultas que un cliente pode facer a un servidor DNS:

Iterativa

As resolucións iterativas consisten na resposta completa que o servidor de nomes poida dar. O servidor de nomes consulta os seus datos locais (incluíndo o seu caché) buscando os datos solicitados. O servidor encargado de facer a resolución realiza iterativamente preguntas á os diferentes DNS da xerarquia asociada ao nome que se desexa resolver, até descender nela até a maquina que contén a zona autoritativa para o nome que se desexa resolver.

Este tipo de consultas, sempre se dan, cando se comenza a procura a partires dos servidores raíz.

Recursiva

Nas resolucións recursivas, o servidor non ten a información nos seus datos locais, polo que busca e ponse en contacto cun reenviador (outro servidor DNS). **So admite como resposta o rexistro que está consultando**, ou a información de erro, de que non se pudo resolver o rexistro.

O servidor DNS que actúa como reenviador en caso de ser necesario repite o mesmo proceso básico (consultar a un servidor remoto e seguir á seguinte referencia) ata que obtén a mellor resposta á pregunta.

Os clientes sempre fan consultas recursivas ao servidor DNS.

Cando existe máis dun servidor autoritario para unha zona, Bind utiliza o menor valor na métrica RTT (round-trip estafe) para seleccionar o servidor. O RTT é unha medida para determinar canto tarda un servidor en responder unha consulta.

O proceso de resolución normal dáse da seguinte maneira: Queremos resolver o nome *equipo1.exemplo.org*. O noso servidor DNS é A, que ten como reenviador ao servidor DNS B. O servidor B non emprega reenviadores.

1. O cliente envia unha consulta recursiva ao servidor DNS A
2. O servidor A recibe unha consulta recursiva desde o cliente DNS.
3. O servidor A envía unha consulta recursiva a B.
4. O servidor B non ten configurados reenviadores, e comeza cunha consulta iterativa a buscar no Servidor raíz.
5. O servidor Raíz, devolve o enderezo do servidor de nomes de nivel superior (.org)
6. O servidor B, consulta ao servidor do dominio de nivel superior
7. O servidor de dominio de nivel superior, refire ao servidor DNS da zona a buscar (.exemplo)
8. O servidor B consulta ao servidor DNS da zona exemplo.org.
9. O servidor da zona exemplo.org ten o rexistro equipo1.exemplo.org e devolvelle o enderezo ao servidor B
10. O servidor B, responde ao servidor A
11. O servidor A, responde ao cliente.

Como funciona unha suxestión de raíz

Unha suxestión de raíz é un rexistro de recursos DNS almacenado nun servidor DNS que indica a IP para os servidores raíz DNS.

Cando o servidor DNS recibe unha consulta DNS, comproba o caché. Entón, o servidor DNS tenta localizar o servidor DNS autorizado para o dominio consultado. Se o servidor DNS non ten a IP do servidor DNS autorizado para o devandito dominio e se o servidor DNS está configurado coas s IP das suxestións de raíz, o servidor DNS consultará a un servidor raíz o dominio á esquerda do dominio raíz da consulta.

O servidor raíz DNS devolve entón a IP do dominio á esquerda do dominio raíz e o servidor DNS continúa analizando o nome de dominio completo até localizar o dominio autorizado.

En circunstancias normais, as suxestións de raíz indican as s IP para os servidores raíz DNS que InterNIC mantén en Internet. As suxestións de raíz tamén apuntan a un servidor DNS local. Se as suxestións de raíz apuntan a un servidor local, os únicos nomes que estarán dispoñibles para resolución son aqueles a os que o servidor DNS pode facer referencia (normalmente, só s locais). Esta configuración ás veces pode utilizarse para incrementar a seguridade, posto que nela só poden resolverse os dominios internos.

Como funcionan os reenviadores

Un reenviador é un servidor DNS que outros servidores DNS internos designan para reenviar consultas e resolver nomes de dominio DNS externos ou fóra do sitio.

Cando un servidor de nomes DNS recibe unha consulta, tenta localizar a información solicitada dentro dos arquivos da súa propia zona. Se non o consegue, ben porque o servidor non estea autorizado para o dominio solicitado ou ben porque non teña o rexistro dunha procura anterior almacenado no caché, o servidor debe comunicarse con outros servidores de nomes para resolver a solicitude. Nunha rede conectada globalmente como Internet, as consultas DNS que están fóra dunha zona local poden necesitar a interacción con servidores de nomes DNS en vínculos da rede de área extensa (WAN) fose da organización. A creación de reenviadores DNS é unha maneira de designar servidores de nomes específicos como responsables do tráfico DNS baseado en WAN.

Pódense seleccionar servidores de nomes DNS específicos para ser reenviadores, nese caso os seus servidores resolverán consultas DNS en nome doutros servidores DNS.

Os servidores de nomes que non son reenviadores poden configurarse para utilizar reenviadores. Os servidores DNS poden configurarse coa dun ou varios reenviadores.

O reenvío condicional permite a un servidor DNS utilizar un reenviador cando o servidor resolve un conxunto de dominios seleccionado. Por exemplo, o reenvío condicional permitiría a un servidor DNS reenviar solicitudes de resolución de s IP para hosts nunha organización asociada que teña unha infraestrutura DNS privada para o seu servidor DNS, mentres que todas as demais solicitudes poderían resolverse normalmente.

Resolucións directas e inversas

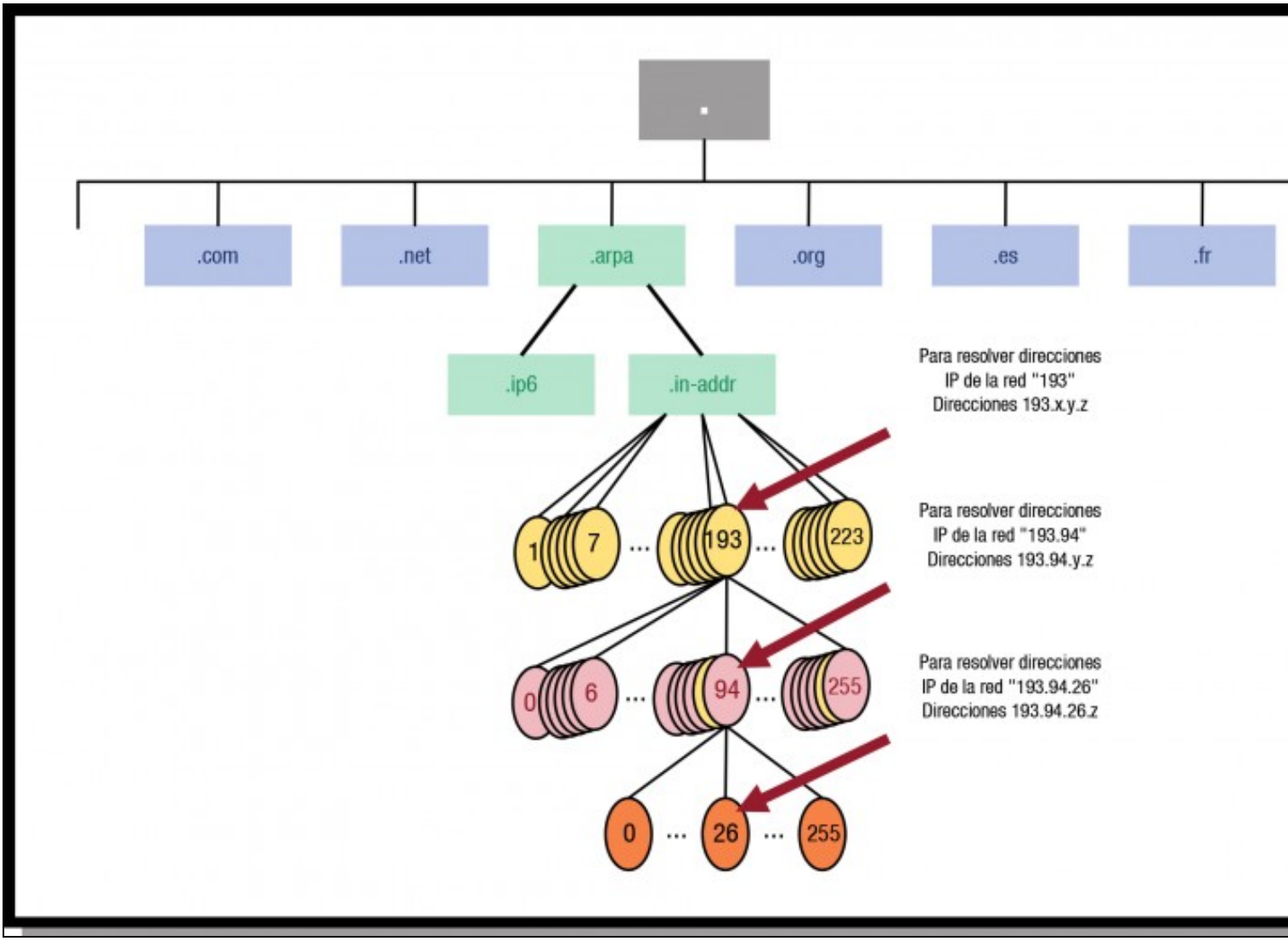
Até agora cando estivemos falando de resolución de nomes de dominio e sempre nos estivemos referindo a obter unha IP a partir dun nome de dominio. Ás resolucións que obteñen s IP a partir de nomes DNS chámaselles resolucións directas.

Preguntáchesche se se pode facer o contrario, é dicir, se se poden obter nomes DNS a partir de IP's? A resposta é se. Aínda que unha resolución deste tipo úsase con moita menos frecuencia que a oposta, pódese realizar e úsase, por exemplo, como unha medida de seguridade.

Un cliente DNS consulta o nome DNS www.mibanco.com e recibe como resposta o IP 193.5.5.5. Pode ocorrer que mediante algunha técnica enviáronnos un IP que non corresponda ao nome DNS consultado para dirixirnos a outro sitio web fraudulento. Pódese verificar que o IP 193.5.5.5 corresponde realmente a www.mibanco.com solicitando a resolución inversa desa IP.

As resolucións e consultas DNS poden ser de dous tipos:

- Directas: Cando se trata de obter a IP que corresponde a un nome DNS.
- Inversas: Cando se trata de obter o nome DNS correspondente a unha IP.



Esquema en forma de árbore que mostra desde o dominio raíz a estrutura xerárquica das zonas de resolución inversa. Dun cadro superior que representa o dominio raíz , colgan varios cadros que representan dominios de primeiro nivel, entre eles o dominio .arpa. Deste dominio colgan dous recadros que representan os dominios in-addr.arpa e ip6.arpa. Do dominio in-addr.arpa colgan múltiples círculos que representan servidores para resolver s IP que comezan por 1, 2 e así até 223. Do nodo 193 colgan igual que antes nodos con números comprendidos entre 0 e 255. Dun dos nodos anteriores, o 94, colgan outra vez múltiples nodos e sinálase especialmente o nodo 26. Un recuadro que apunta a este nodo indica que o servidor correspondente resolve s IP que comezan por 193.94.26.
Para as resolucións inversas utilízase o dominio de primeiro nivel "**.arpa**" cos seus correspondentes servidores. Dentro dese dominio tense o dominio "**in-addr.arpa**" para resolver s IPv4 e o dominio "ip6.arpa" para resolver s IPv6. Baixo eses servidores nunha estrutura xerárquica hai outros servidores que se encargan de resolver conxuntos de s IP pertencentes a unha IP de rede.

Calquera organización que teña en propiedade unha de rede debe responsabilizarse de ter servidores DNS que resolvan inversamente as s IP pertencentes á de rede. A seguinte imaxe representa como están organizados os servidores para as resolucións inversas e indícase, para algúns deles, as s IP nas que participan na súa resolución.

Cando un cliente DNS realiza unha consulta inversa dunha IPv4 debe preguntar por un nome formado polo enderezo IP escrito ao revés e seguido dun nome do dominio "**.in-addr.arpa**" e finalizado nun punto que especifica o servidor raíz.

Zonas primarias e secundarias

Os termos zona e dominio poden chegar a confundirse. Unha zona contén a información necesaria para resolver nomes pertencentes a un ou varios dominios. Unha zona non é máis que un arquivo que se almacena nun servidor DNS e que contén unha parte de toda a información do espazo de nomes DNS. Por tanto é unha parte da base de datos distribuída correspondente ao espazo de nomes DNS.

Unha zona almacénase nun servidor DNS e, nese caso, dise que o servidor ten autoridade sobre a zona ou que é un servidor autorizado da zona. Un servidor DNS pode ter autoridade sobre varias zonas. DNS permite que un espazo de nomes DNS se divida en zonas. Para cada nome de dominio DNS incluído nunha zona, a zona convértese na fonte autorizada de información acerca de devandito dominio. Os arquivos de zona mantéñense en servidores DNS. Un único servidor DNS pódese configurar para aloxar ningunha, unha ou varias zonas. Cada zona pode estar autorizada para un dominio DNS ou para máis dun sempre que sexan contiguos na árbore DNS. As zonas poden almacenarse en arquivos de texto sen formato ou na base de datos de Active Directory.

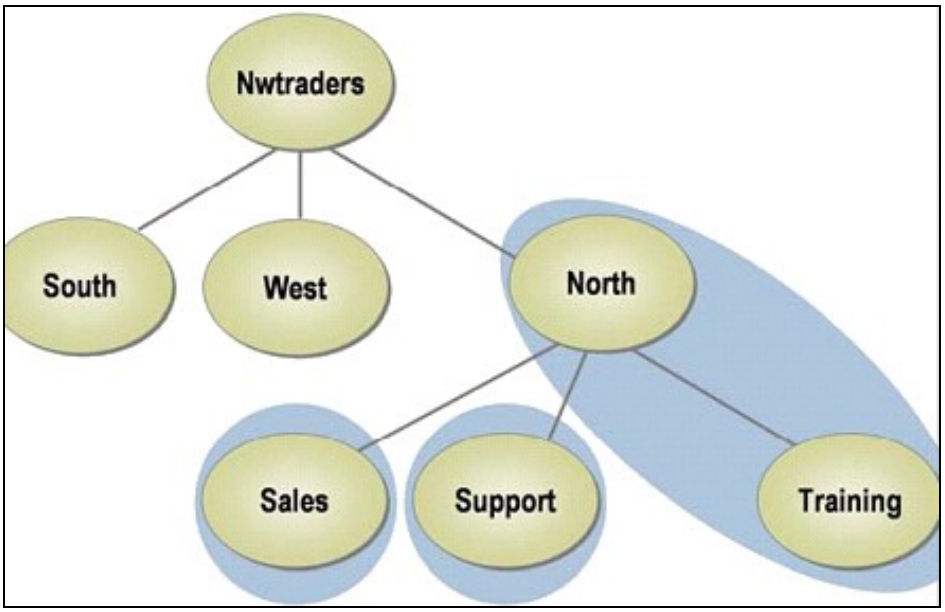
Entre as características dunha zona inclúense as seguintes:

- Unha zona é un conxunto de asignacións entre nomes de host e direccións IP para os hosts nunha parte contigua do espazo de nomes DNS.
- Os datos de zona mantéñense nun servidor DNS
- Un servidor DNS está autorizado para unha zona se aloxa os rexistros de recursos para os nomes e as direccións que os clientes solicitan no arquivo de zona.

A zona está constituída por varios rexistros. Cada rexistro serve para resolver un nome DNS ou, no seu caso, un enderezo IP. Tamén os rexistros teñen outras funcións como indicar cales son os servidores DNS da zona. Ás zonas tamén se lles chama zonas de autoridade ou zonas de autoridade no dominio.

É moi normal que unha zona resolva os nomes dun dominio e que nun dominio haxa unha zona (porque só hai un servidor DNS). Por isto pódense confundir os termos zona e dominio. Unha zona pode conter información sobre un dominio e os seus subdominios. Desde agora, lembra que o termo zona fai referencia a un arquivo para realizar resolucións.

Unha zona pode albergar os rexistros de recursos para un dominio ou os rexistros de recursos para varios dominios. Unha zona pode aloxar máis dun dominio só se os dominios son contiguos; é dicir, están conectados mediante unha relación primario-secundario directa.



Na ilustración hai tres zonas representadas:

- north.nwtraders.com
- sales.north.nwtraders.com
- support.north.nwtraders.com

A primeira zona (north.nwtraders.com) está autorizada para dous dominios contiguos (north.nwtraders.com e training.north.nwtraders.com), mentres que cada unha das outras dúas zonas (salgues.north.nwtraders.com e support.north.nwtraders.com) representan un único dominio.

Tipos de zona DNS

Ao configurar un servidor DNS, pode configuralo con varios tipos de zona ou con ningunha, segundo o tipo de función que o servidor DNS desempeñe na rede.

Hai numerosas opcións para realizar a unha configuración óptima do servidor DNS, baseadas en decisións tomadas segundo, por exemplo, a topología de rede e o tamaño do espazo de nomes. A operación normal do servidor DNS implica tres zonas:

- Zona principal
- Zona secundaria
- Zona de código auxiliar

Mediante o uso de zonas diferentes, pode configurar a solución DNS para axustarse mellor ás súas necesidades. Por exemplo, recoméndase configurar unha zona principal e unha zona secundaria en servidores DNS independentes, para proporcionar tolerancia a erros no caso de que un servidor falle. Se a zona mantense nun servidor DNS independente, pódese configurar unha zona de código auxiliar.

Unha zona principal é a copia autorizada da zona DNS, onde se crean e administran rexistros de recursos. Ao configurar servidores DNS co fin de aloxar zonas para un dominio, o servidor principal adoita estar situado onde sexa accesible para administrar o arquivo de zona.

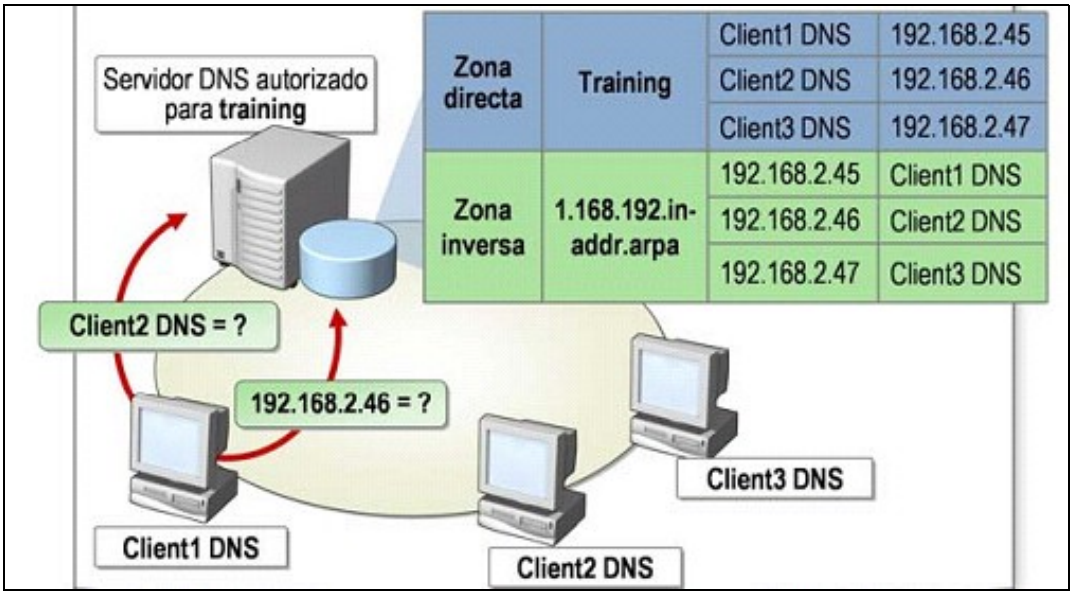
Unha zona secundaria é unha copia da zona DNS que contén a copia de só lectura da zona DNS. Os rexistros da zona secundaria non poden modificarse; os administradores só poden modificar rexistros da zona DNS principal. Normalmente, configúrase polo menos un servidor secundario con tolerancia a erros. No entanto, poderíanse configurar varios servidores secundarios noutras localizacións para que os rexistros da zona puidesen resolverse sen que a solicitude cruzase vínculos WAN.

As zonas de código auxiliar son copias dunha zona que conteñen só os rexistros de recursos necesarios para identificar o servidor DNS autorizado para a dicir zona. Unha zona de código auxiliar contén un subconjunto de datos de zona que consta dun rexistro SOA, NS e A, tamén coñecido como rexistro de adherencia. Unha zona de código auxiliar é como un marcador que simplemente apunta ao servidor DNS que está autorizado para a dicir zona.

As zonas de código auxiliar poden utilizarse onde as suxestións de raíz apuntan a un servidor DNS interno, en lugar da servidores raíz en Internet. Por razóns de seguridade, o servidor DNS está deseñado só para resolver certas zonas.

Zonas de procura directa e inversa

Unha vez que se decide se a zona é de tipo principal, secundario ou de código auxiliar, debe decidir en que tipo de zona de procura se almacenan os rexistros de recursos, que poden almacenarse en zonas de procura directa ou en zonas de procura inversa.



Unha asignación pode almacenarse como unha asignación entre un nome de host e unha dirección IP ou á inversa. Pode elixir o tipo de asignación necesario para unha zona, en función de como desexe que os clientes e servizos consulten rexistros de recursos.

En DNS, unha procura directa é un proceso de consulta no que se busca o nome para mostrar do dominio DNS dun equipo host para atopar a súa dirección IP.

No Administrador de DNS, as zonas de procura directa baséanse nos nomes de dominio DNS e adoitan aloxar rexistros de recursos de dirección de host (A).

En DNS, unha procura inversa é un proceso de consulta mediante o cal se busca a dirección IP dun equipo host para atopar o seu nome para mostrar no dominio DNS.

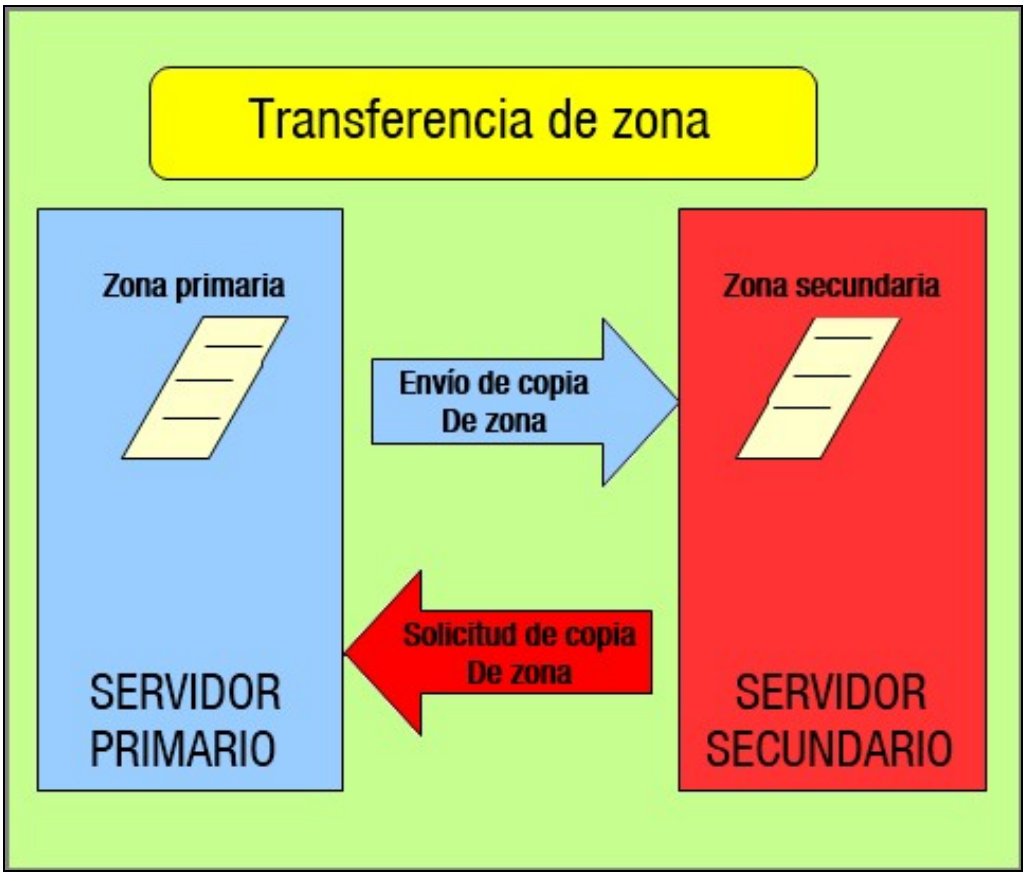
No Administrador de DNS, as zonas de procura inversa baséanse no seu nome de dominio in-addr.arpa e adoitan albergar rexistros de recursos de punteiro (PTR).

Transferencias de zona

Como se manteñen as zonas secundarias? Os servidores secundarios realizan cada certo tempo unha actualización da zona. Para iso solicitan ao servidor primario o envío dunha copia da zona primaria. Esta copia enviada actualiza os rexistros na zona secundaria.

O proceso de actualización dunha zona secundaria cunha copia da zona primaria chámase transferencia de zona.

A seguinte imaxe mostra un proceso de transferencia de zona.



Cando se inicia, un servidor secundario solicita unha transferencia de zona ao primario. No secundario pódese configurar cada canto tempo deben realizar as transferencias de zona. Especialmente para zonas que conteñen moita información, adóitanse realizar transferencias de zona incrementales nas que só se envían os datos modificados na zona desde a última transferencia.

Tipos de rexistros DNS

Un rexistro de recursos (RR) é unha estrutura de base de datos DNS estándar que contén información para procesar consultas DNS.

Unha zona é unha parte da base de datos DNS que contén os rexistros de recursos cos nomes de propietario que pertencen á parte contigua do espazo de nomes DNS.

Un arquivo de zona é o arquivo do disco duro local do servidor DNS que contén toda a información de configuración para unha zona e os rexistros de recursos contidos nela.

Unha vez instalado o servizo Servidor DNS e configuradas as propiedades do servizo DNS, xa se pode completar o servizo DNS mediante a adición de asignacións entre nomes de host e direccións IP. Estas asignacións denomínanse rexistros de recursos en DNS. Hai moitos tipos diferentes de rexistros de recursos. Os tipos de rexistros de recursos que se cren en DNS dependerán das necesidades de DNS. Para agregar rexistros de recursos, é necesario dispor dunha estrutura en DNS que poida albergalos. Estes colectores lóxicos denomínanse zonas en DNS. Cando se crea unha zona, créase un arquivo de zona para almacenar as propiedades de zona e rexistros de recursos. Hai varias configuracións diferentes de zonas en DNS e as zonas que se crearán veñen ditadas polas necesidades de DNS na contorna.

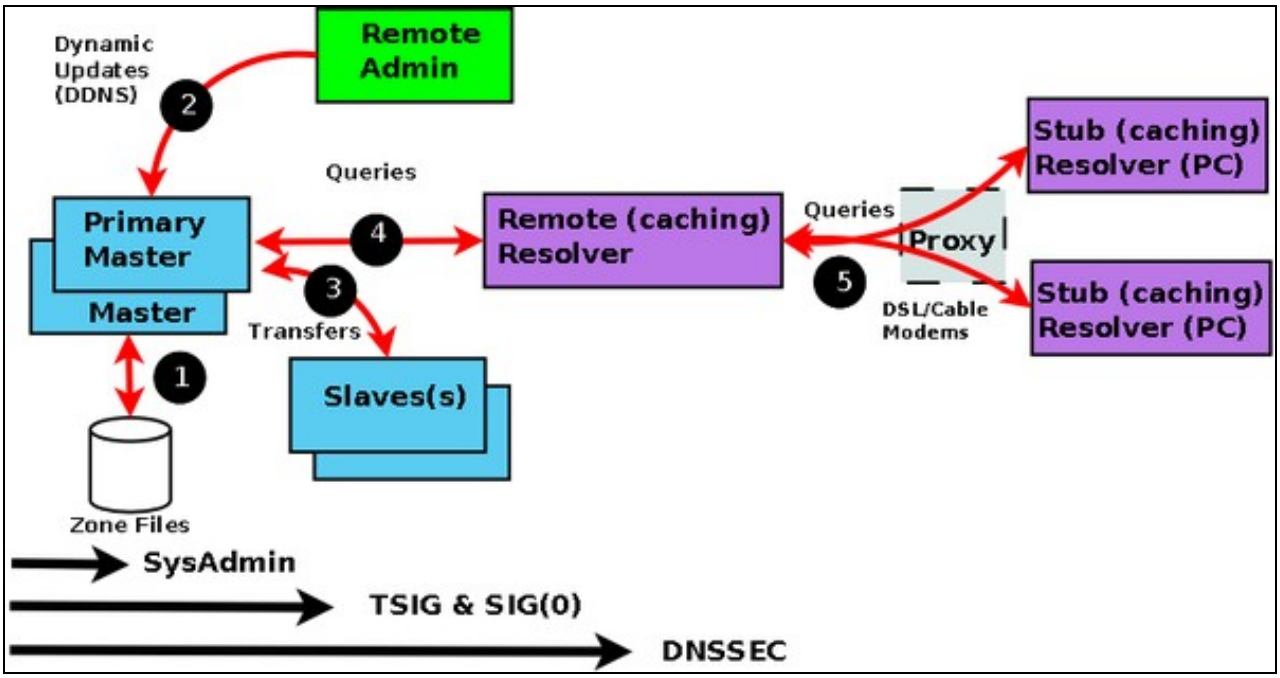
Tipos de rexistros DNS:

- **A** = Address - (Dirección) Este rexistro úsase para traducir nomes de servidores de aloxamento a direccións IPv4.
- **AAAA** = Address (Dirección) Este rexistro úsase en IPv6 para traducir nomes de hosts a direccións IPv6.
- **CNAME** = Canonical Name - (Nomee Canónico) Úsase para crear nomes de servidores de aloxamento adicionais, ou alias, para os servidores de aloxamento dun dominio. É usado cando se están correndo múltiples servizos (como ftp e servidor web) nun servidor cunha soa dirección ip. Cada servizo ten a súa propia entrada de DNS (como ftp.exemplo.com. e www.ejemplo.com.). isto tamén é usado cando corres múltiples servidores http, con diferente nomes, sobre o mesmo host.
- **NS** = Name Server - (Servidor de Nomes) Define a asociación que existe entre un nome de dominio e os servidores de nomes que almacenan a información do devandito dominio. Cada dominio pódese asociar a unha cantidade calquera de servidores de nomes.
- **MX** (rexistro) = Mail Exchange - (Rexistro de Intercambio de Correo) Asocia un nome de dominio a unha lista de servidores de intercambio de correo para ese dominio.

- **PTR** = Pointer - (Indicador) Tamén coñecido como 'rexistro inverso', funciona á inversa do rexistro A, traducindo IPs en nomes de dominio.
- **SOA** = Start of authority - (Autoridade da zona) Proporciona información sobre o servidor DNS primario da zona.
- **TXT** = TeXT - (Información textual) Permite aos dominios identificarse de modos arbitrarios.
- **SRV** = Service - Permite indicar que equipo e que porto ofrecen un servizo indicado.

Seguridade en DNS

Para ser capaz de avaliar as ameazas potenciais e poder tomar medidas é necesario, en primeiro lugar entender os fluxos de comunicación normais nun sistema de DNS. Pódese ver no seguinte esquema



Cada fluxo de dato (liña VERMELLA no esquema de enriba) é unha fonte potencial de ameazas. Utilizando os números imos analizar que ameazas e riscos podemos atopar:

Riscos nos fluxos de comunicación DNS

Número	Área	Risco
1	Ficheiros de zona	Corrupción de ficheiro (De maneira maliciosa ou accidental). Mitigado por prácticas de Administración de Sistema boas.
2	Actualizacións dinámicas	spoofing de enderezos IP] (actualizacións desde unha IP suplantada). Ameaza Server2Server. Mitigado mediante limitación de enderezos ou solucións críptográficas que empregan chaves TSIG.
3	Transferencias de zona	Spoofing de enderezos IP] (solicitudes de transferencia desde unha IP suplantada). Ataques DDoS con peticións de transferencia reiteradas. Ameaza Server2Server. Mitigado mediante limitación de enderezos ou solucións críptográficas que empregan chaves TSIG.
4	Consultas remotas	Cache poissoning] (envenamento de cache DNS) mediante IP spoofing. Interceptión de datos entre clientes e servidores. Ataques DDoS baseados en resolvedores abertos e erros de configuración. Computadores zombies ou servidores infectados con virus. Ameaza Server2Client. Mitigado mediante limitación de enderezos ou solucións críptográficas que empregan DNSSEC.
5	Consultas dos clientes	cache poissoning] (envenamento de cache DNS). Un número crecente de clientes, usan un proxy DNS que pode estar comprometido ou mal configurado. Ameaza Server2Client. Mitigado mediante limitación de enderezos ou solucións críptográficas extremo a extremo que empregan DNSSEC.

Solución Server2Server

- **Transferencias de zona**. Se temos varios servidores que fan transferencias de zona, sempre podemos emrpegar ACL's (Access Control ist) para protexer os accesos desde determinados enderezos IP.
- **Actualizacións dinámicas**. Se empregamos este servizo, que por defecto ven deshabilitado, debemos protexelo. Unha maneira sinxela é empregar ACL's, que pode non ser adecuado, se non podemos securizar os enderezos IP, por exemplo, poñendo os equipos detras fun firewall, ou actualizando os servidores desde un enderezo privado.
- **Chaves TSIG**. Se todas as demais solucións fallan, o uso de chaves TSIG prove un protocolo de autenticación que securizará as comunicacións entre servidores. É un pouco lioso pero non demasiado complicado. Como as transaccións non van ser moi frecuentes, o

protocolo depende dunha chave segreda compartida, que haberá que introducir en ámbolos dous extremos. Esa chave compartida, pode ser vulnerable a ataques de forza bruta, que podemos disminuir cabiando de forma frecuente as chaves.

Socución Server2Client

O problema cásico de envelenamento da caché DNS (cache poissoning) non é sinxelo de resolver, porque pode afectar a un número infinitamente grande de cachés DNS remotas. Non é razonable empregar chaves segredas, polo ese elevado número de actores que interveñen. Pola contra o mecanismo, descansa en solucións de chave pública/privada (cifrado asimétrico). As especificacións DNSSEC intentan dar resposta atres preguntas:

- **Autenticación**: O servidor DNS que responde é realmente o que se lle fixo a pregunta.
- **Inrtegridade**: A resposta é completa e non foi modificada.
- **Proba de non existencia**: Se un rexistro DNS non está dispoñible, podese comprobar que realmente non existe (Proof-of-non-existence - PNE).

DNSSEC

DNSSEC é unha extensión ao sistema de resolución de nomes DNS que permite aumentar a seguridade deste, evitando ataques como o envelenamento de cache (respostas falsas co fin de dirixir o tráfico a un destino diferente ao real).

Basicamente engade autenticación ás respostas DNS mediante sinatura dixital, permitindo aos clientes validar a veracidade das devanditas respostas. DNSSEC non cifra o tráfico entre clientes e/ou servidores, que segue sendo "en claro". Nin evita ataques de denegación de servizo.

Como funciona DNSSEC

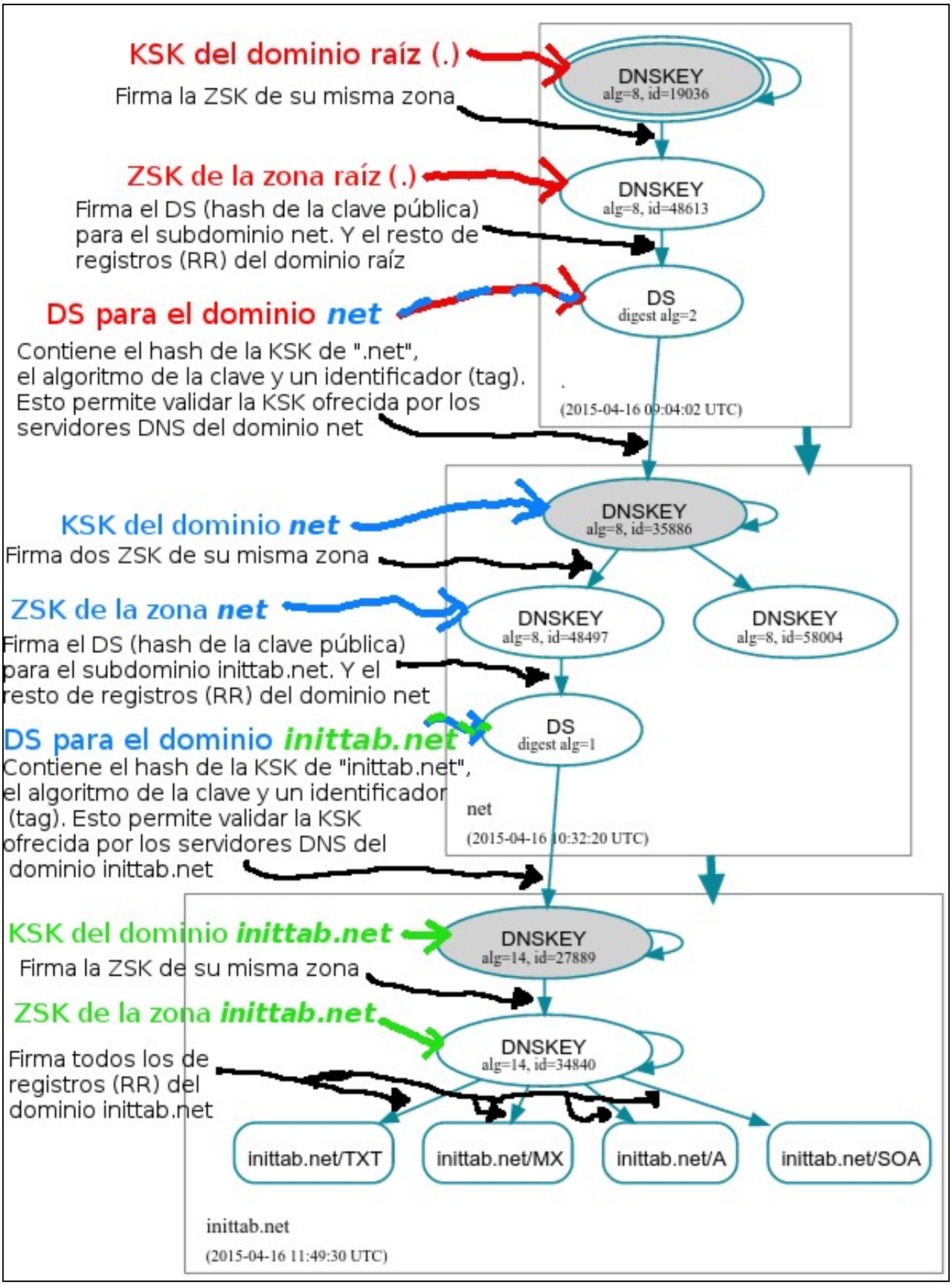
O funcionamento baséase nunha delegación de confianza entre as zonas pai e fillas e o uso de criptografía asimétrica (chave pública/privada). A zona raíz (.) está asinada cunha chave privada e a súa pública é de coñecemento global (normalmente vén incluída nos servidores DNS). Na devandita zona (.) atópase un rexistro DS (Delegation Signer) por cada zona filla (.com, .com, .org, .es,...) que contén un hash da chave pública correspondente a cada unha delas.

É dicir, na zona raíz (.) hai un rexistro DS que indica cal é a chave pública da zona .com. Na zona .com hai un rexistro DS para cada dominio (que soporte DNSSEC) que colga dela. Por exemplo, na zona .com, ademais dos servidores DNS (NS) que serven o dominio exemplo.com, tamén hai un rexistro DS que indica con que chave (pola súa hash) hai que verificar as respostas desa zona.

Cando usamos DNSSEC, as respostas a unha pregunta DNS (sexa un rexistro A, MX, DS, CNAME, ...) virán acompañadas dun rexistro "extra" de tipo RRSIG (Resource Record SIGnature) que consiste na sinatura dixital (coa chave privada da zona) do rexistro que se solicitou. Este rexistro RRSIG pode ser verificado coa chave pública de exemplo.com, que ademais pode ser validada ao ser un rexistro DS na zona pai (.com), que á súa vez está asinado pola chave privada desta,...

De forma que se solicitamos o rexistro MX do dominio exemplo.com, o proceso (que seguiría normalmente o servidor DNS que nos presta o servizo de resolución de nomes) sería:

- Solicitar aos servidores raíz a lista de DNS (rexistros NS) que serven o dominio .com. A resposta levaría devanditos rexistros (NS), ademais dos correspondentes RRSIG para validarlos. Ademais habería que solicitar o rexistro DS (hash da chave pública) do dominio .com, para poder validar a resposta que nos dean os seguintes servidores DNS. Por suposto este rexistro (DS) será verificable co seu correspondente rexistro RRSIG (sinatura creada coa chave privada do dominio raíz).
- O noso servidor DNS validaría coa chave pública da zona raíz (que xa ten, por exemplo en /etc/bind/bind.keys) que a sinatura (RRSIG) dos rexistros NS e DS é correcta e por tanto a información válida.
- O seguinte sería pedir a algún dos servidores encargados de .com a súa chave pública (rexistro DNSKEY) para poder validar as seguintes respostas que nos dea. Este rexistro debe conter unha chave cuxo hash coincida co que viña no rexistro DS que nos entregou a zona raíz e que xa validamos.
- Agora, coa chave pública (xa validada) do dominio .com, podemos pedir aos servidores DNS os rexistros NS do dominio exemplo.com e o rexistro DS co hash da súa chave pública. Por suposto as respostas a estas preguntas virán acompañadas dos correspondentes rexistros RRSIG que permitirán comprobar a validez das mesmas coa chave pública de .com.
- O proceso repetiríase cos DNS de exemplo.com. É dicir, pedimos a chave pública de exemplo.com (DNSKEY) verificamos queo seu hash coincide co rexistro validado DS que nos entregaron os servidores da zona pai (.com) e con el validaremos o resto de peticións que fagamos do dominio e que virán acompañadas dos seus correspondentes RRSIG.


KSK del dominio raíz (.)
Firma la ZSK de su misma zona
ZSK de la zona raíz (.)
Firma el DS (hash de la clave pública) para el subdominio net. Y el resto de registros (RR) del dominio raíz
DS para el dominio net
Contiene el hash de la KSK de ".net", el algoritmo de la clave y un identificador (tag). Esto permite validar la KSK ofrecida por los servidores DNS del dominio net
DNSKEY alg=8, id=19036
DNSKEY alg=8, id=48613
DS digest alg=2
.
(2015-04-16 09:04:02 UTC)
KSK del dominio net
Firma dos ZSK de su misma zona
ZSK de la zona net
Firma el DS (hash de la clave pública) para el subdominio inittab.net. Y el resto de registros (RR) del dominio net
DS para el dominio inittab.net
Contiene el hash de la KSK de "inittab.net", el algoritmo de la clave y un identificador (tag). Esto permite validar la KSK ofrecida por los servidores DNS del dominio inittab.net
DNSKEY alg=8, id=35886
DNSKEY alg=8, id=48497
DNSKEY alg=8, id=58004
DS digest alg=1
net
(2015-04-16 10:32:20 UTC)
KSK del dominio inittab.net
Firma la ZSK de su misma zona
ZSK de la zona inittab.net
Firma todos los de registros (RR) del dominio inittab.net
DNSKEY alg=14, id=27889
DNSKEY alg=14, id=34840
inittab.net/TXT
inittab.net/MX
inittab.net/A
inittab.net/SOA
inittab.net
(2015-04-16 11:49:30 UTC)

chaves de sinatura de chave e chaves de sinatura de zona (KSK vs ZSK)

Como se pode observar do proceso anteriormente descrito, as zonas pai deben conter unha referencia (DS) á chave coa que as zonas fillas asinan os seus rexistros. No caso dun dominio tradicional (p.e. exemplo.com), iso require de informar o rexistrador, xunto cos DNS que o servirán, o valor do devandito rexistro DS para o domino. Isto é un proceso manual e pouco automatizable.

Ademais a información que se asina dos rexistros dun dominio é moi pequena (un IP, un nome de máquina, un rexistro SPF, etc..), o que "facilita" a criptoanálise da chave coa que están asinados. Por iso é conveniente cambiar a chave coa que se asinan de forma periódica.

De feito os rexistros RRSIG teñen unha validez temporal (independente do TTL do dominio) e teñen que ser recreados (asinados) de forma periódica. O motivo é evitar ataques de repetición (Replay Attacks) que permitirían reutilizar unha resposta vella (asinada hai meses ou anos) por un atacante para enganar a un cliente.

Por estes motivos, e para facilitar o cambio da chave coa que se asinan os rexistros da zona, recoméndase o uso de dúas chaves: KSK e ZSK. A chave KSK (Key Signing Key) é aquela que estará "informada" como DS na zona superior. A súa función é a de asinar a chave de zona (ZSK) coa que están asinados o resto de rexistros do dominio. É dicir, a "exposición" da KSK é mínima.

Pola contra a ZSK (Zone Signing Key) é a que asina todos os rexistros da zona. Pode ser algo máis "curta" que a KSK xa que a súa rotación periódica é máis sinxela que a dunha soa chave ou a da KSK. É dicir, non hai que modificar a zona pai (cambios no rexistrador) cando se queira cambiar de chave de asinado de zona (ZSK), basta con xerar unha nova e asinala coa KSK, unicamente informando os cambios na nosa zona DNS.

Desde o punto de vista técnico non hai diferenzas (importantes) entre un tipo de chave e outro. Só é a forma na que se usan o que a diferenza. De feito pode usarse unha única chave, informando á zona pai desta, e asinando todo con ela. O problema é que o traballo de cambio de chave será máis complexo. Mentres que o de cambio dunha ZSK usando unha KSK está practicamente automatizado coas ferramentas DNSSEC que usaremos e non require de cambios no rexistrador do dominio.

Así que aínda que pareza unha solución máis complicada inicialmente, o uso dunha chave para cada función a longo prazo é máis seguro e máis sinxelo de xestionar.

- Bruno Vila Vilariño (set 2020)