Sistema de nombres de dominio - Wikipedia, la enciclopedia libre

HTML Content

Sistema de nombres de dominio

Este artículo o sección necesita **referencias** que aparezcan en una publicación acreditada. Este aviso fue puesto el 30 de agosto de 2016.
Puedes añadirlas o avisar al autor principal del artículo en su página de discusión pegando:
`{{sust:Aviso referencias|Sistema de nombres de dominio}} ~~~~`

El **sistema de nombres de dominio**[1] (DNS, por sus siglas en inglés, *Domain Name System*) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Domain Name System (DNS)

Familia	Familia de protocolos de Internet
Función	Resolución de nombres de dominio
Puertos	53/UDP, 53/TCP

Ubicación en la pila de protocolos

Aplicación	**DNS**
Transporte	TCP o UDP
Red	IP (IPv4, IPv6)

Estándares

RFC 1034 (1987)
RFC 1035 (1987)

[editar datos en Wikidata]

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio Google es 216.58.210.163, la mayoría de la gente llega a este equipo especificando `www.google.es` y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable.[2] La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre tan solo la IP del sitio web.

Índice [ocultar]

Historia [editar]

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado *HOSTS* que contenía todos los nombres de dominio conocidos. [3]

El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul Mockapetris y Jon Postel publican los RFC 882 y RFC 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno (estos RFC fueron reemplazados en 1987 con los RFC 1034 y RFC 1035).[4]

De no existir los servidores DNS los usuarios tendrían que escribir la dirección IP del sitio web en lugar de escribir la URL de este lo cual generaría confusiones y la navegación en internet se tornaría muy complicada para los usuarios.

En esta etapa, la mejor forma de proveer "continuidad" era tener múltiples servidores contestando múltiples consultas. Un servidor era el *maestro* y los demás eran *esclavos*. Cada uno de los esclavos debía revisar con el maestro periódicamente que los datos no hubieran cambiado.

Unos 10 años después, se hicieron algunos ajustes mayores al protocolo DNS. Esto era una forma más dinámica de mantener los servidores al día, utilizando NOTIFY (en inglés *notificar*) y las transferencias incrementales de zona (IXFR).[5]

NOTIFY fue un cambio clave. En vez de esperar a que un esclavo revisara, el maestro podía mandar mensajes NOTIFY a los esclavos, instándolos a adquirir los nuevos datos. Por su parte, IXFR significó un cambio en la forma en que la data se comunicaba. Si cambiaba solamente uno de entre cientos de registros, la especificación original enviaría cientos de mensajes. IXFR cambió el sistema, permitiendo que el envío fuera de los registros que cambiaron solamente.[5]

La siguiente evolución de DNS vino cuando se definieron cambios dinámicos en RFC 2136 . Esto permitió que los administradores de los servidores pudieran hacer cambios en los registros de mejor forma. Más tarde, en el RFC 2671 se definieron mecanismos de extensión de DNS (EDNS) que modernizó aún más el sistema.[5]

El interés por expandir los posibles nombres de los dominios para incluir caracteres de otros idiomas se reflejó en los nombres de dominio internacionalizados como fueron definidos en los RFC 5890 y RFC 5891 en 2010.

Componentes [editar]

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

Los **Clientes fase 1**: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS *(Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?);*

Los **Servidores DNS**: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada; y

Las **Zonas de autoridad**, es una parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS, que puede tener autoridad sobre varias zonas. (Por ejemplo : subdominio .ORG, .COM, etc).

Entendiendo las partes de un nombre de dominio [editar]

Un nombre de dominio usualmente consiste en dos o más partes (técnicamente «etiquetas»), separadas por puntos cuando se las escribe en forma de texto. Por ejemplo, `www.ejemplo.com` o `es.wikipedia.org`

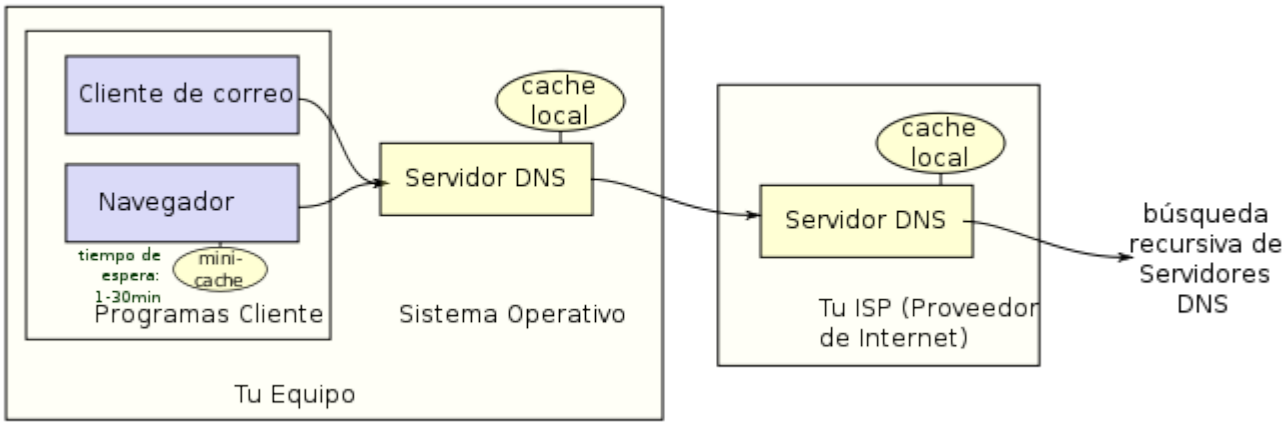
> A la etiqueta ubicada más a la derecha se le llama **dominio de nivel superior** (en inglés *top level domain*). Como `com` en `www.ejemplo.com` u `org` en `es.wikipedia.org`
>
> Cada etiqueta a la izquierda especifica una subdivisión o **subdominio**. Nótese que "subdominio" expresa dependencia relativa, no dependencia absoluta. En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.
>
> Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (en inglés *hostname*). El resto del nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida. Por ejemplo, el dominio `es.wikipedia.org` tendría el nombre de la máquina "es", aunque en este caso no se refiere a una máquina física en particular.

El DNS consiste en un conjunto jerárquico de servidores DNS. Cada dominio o subdominio tiene una o más **zonas de autoridad** que publican la información acerca del dominio y los nombres de servicios de cualquier dominio incluido. La jerarquía de las zonas de autoridad coincide con la jerarquía de los dominios. Al inicio de esa jerarquía se encuentra los servidores raíz: los servidores que responden cuando se busca resolver un dominio de primer y segundo nivel.

DNS en el mundo real [editar]

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS,[6] el usuario puede utilizar los servidores propios de su ISP, puede usar un servicio gratuito de resolución de dominios o contratar un servicio avanzado de pago que por lo general son servicios contratados por empresas por su rapidez y la seguridad que estos ofrecen.

La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet salvo quienes personalizan sus equipos o enrutadores para servidores públicos determinados. La dirección de estos servidores puede ser configurada de forma manual o automática mediante DHCP (IP dinámica). En otros casos, los administradores de red tienen configurados sus propios servidores DNS.



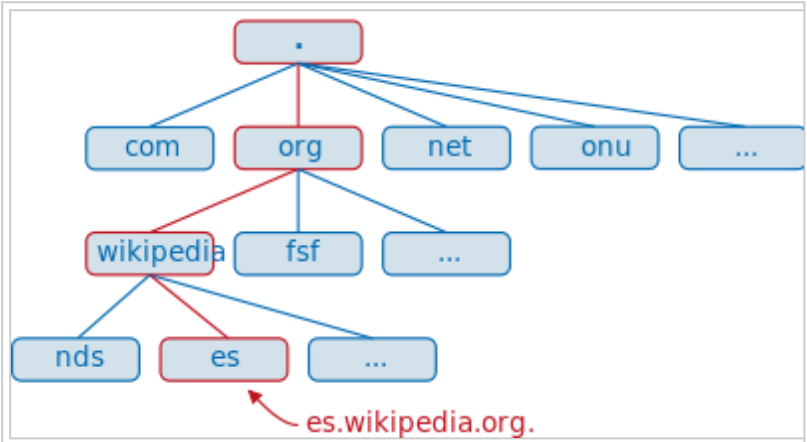
En cualquier caso, los servidores DNS que reciben la petición, buscan en primer lugar si disponen de la

respuesta en la memoria caché. Si es así, sirven la respuesta; en caso contrario, iniciarían la búsqueda de manera recursiva. Una vez encontrada la respuesta, el servidor DNS guardará el resultado en su memoria caché para futuros usos y devuelve el resultado.[6]

Típicamente el protocolo DNS transporta las peticiones y respuestas entre cliente y servidor usando el protocolo UDP, ya que es mucho más rápido. Las ocasiones donde se usa el protocolo TCP son: cuando se necesitan transportar respuestas mayores de 512 bytes de longitud (por ejemplo al usar DNSSEC) y cuando se intercambia información entre servidores (por ejemplo al hacer una transferencia de zona), por razones de fiabilidad.[7]

Jerarquía DNS [editar]

El espacio de nombres de dominio tiene una estructura arborescente. Las hojas y los nodos del árbol se utilizan como etiquetas de los medios. Un nombre de dominio completo de un objeto consiste en la concatenación de todas las etiquetas de un camino. Las etiquetas son cadenas alfanuméricas (con '-' como único símbolo permitido), deben contar con al menos un carácter y un máximo de 63 caracteres de longitud, y deberá comenzar con una letra (y no con '-').[8] Las etiquetas individuales están separadas por puntos. Un nombre de dominio termina con un punto (aunque este último punto generalmente se omite, ya que es puramente formal). Un nombre de dominio correctamente formado (FQDN, por sus siglas en inglés), es por ejemplo este: www.ejemplo.com. (incluyendo el punto al final).



Árbol DNS

Un nombre de dominio debe incluir todos los puntos y tiene una longitud máxima de 255 caracteres.

Un nombre de dominio se escribe siempre de derecha a izquierda. El punto en el extremo derecho de un nombre de dominio separa la etiqueta raíz de la jerarquía. Este primer nivel es también conocido como dominio de nivel superior (TLD, por sus siglas en inglés).

Los objetos de un dominio DNS (por ejemplo, el nombre del equipo) se registran en un archivo de zona, ubicado en uno o más servidores de nombres.

Tipos de servidores DNS [editar]

Estos son los tipos de servidores de acuerdo a su función:[6]

Primarios o maestros: guardan los datos de un espacio de nombres en sus ficheros.
Secundarios o esclavos: obtienen los datos de los servidores primarios a través de una transferencia de zona.
Locales o caché: funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres. Cuando se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.

Tipos de resolución de nombres de dominio [editar]

Existen dos tipos de consultas que un cliente puede hacer a un servidor DNS, la iterativa y la recursiva. [*cita requerida*]

Resolución iterativa [editar]

Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.

Resolución recursiva [editar]

En las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.

Cuando existe más de un servidor autoritario para una zona, BIND utiliza el menor valor en la métrica RTT (tiempo de ida y vuelta) para seleccionar el servidor. El RTT es una medida para determinar cuánto tarda un servidor en responder una consulta.

El proceso de resolución normal se da de la siguiente manera:

El servidor A recibe una consulta iterativa desde el cliente DNS.
El servidor A envía una consulta iterativa a B.
El servidor B refiere a A otro servidor de nombres, incluyendo a C.
El servidor A envía una consulta iterativa a C.
El servidor C refiere a A otro servidor de nombres, incluyendo a D.
El servidor A envía una consulta iterativa a D.
El servidor D responde.
El servidor A regresa la respuesta al resolver.
El servidor entrega la resolución al programa que solicitó la información.

Temas de Seguridad [editar]

Originalmente, las preocupaciones de seguridad no fueron consideraciones importantes para el diseño en el software DNS o de cualquier otro software para despliegue en la Internet temprana, ya que la red no estaba abierta a la participación del público general. Sin embargo, la expansión de Internet en el sector comercial en los 90s cambió los requisitos de las medidas de seguridad para proteger la integridad de los datos y la autenticación de los usuarios.

Muchos temas de vulnerabilidades fueron descubiertos y explotados por usuarios maliciosos. Uno de esos temas es el envenenamiento de caché DNS, en la cual los datos son distribuidos a los resolvedores de caché bajo el pretexto de ser un servidor de autoridad de origen, contaminando así el almacenamiento de datos con información potencialmente falsa y largos tiempos de expiración (time-to-live). Subsecuentemente, las solicitudes legítimas de las aplicaciones pueden ser redirigidas a equipos de red operados con contenidos maliciosos.

Las respuestas DNS tradicionalmente no están firmadas criptográficamente, permitiendo muchas posibilidades de ataque; las extensiones de seguridad del DNS (DNSSEC) modifican el DNS para agregar la posibilidad de tener respuestas firmadas criptográficamente. DNSCurve ha sido propuesto como una alternativa a DNSSEC. Otras extensiones, como TSIG, agregan soporte para autenticación criptográfica entre pares de confianza y se usan comúnmente para autorizar transferencias de zona u operaciones dinámicas de actualización.

Algunos nombres de dominio pueden ser usados para conseguir efectos de engaño. Por ejemplo, paypal.com y paypa1.com son nombres diferentes, pero puede que los usuarios no puedan distinguir la diferencia

dependiendo del tipo de letra que estén usando. En muchos tipos de letras la letra *l* y el numeral *1* se ven muy similares o hasta idénticos. Este problema es grave en sistemas que permiten nombres de dominio internacionalizados, ya que muchos caracteres en ISO 10646 pueden aparecer idénticos en las pantallas típicas de computador. Esta vulnerabilidad se explota ocasionalmente en phishing.[9]

Técnicas como el FDNS inverso con confirmación adelantada pueden también usarse para validar los resultados de DNS.

Tipos de registros DNS [editar]

Artículo principal: Anexo:Listado de tipos de registros DNS

Los tipos de registros más utilizados son:

A = Dirección (*address*). Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.
AAAA = Dirección (*address*). Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
CNAME = Nombre canónico (*canonical Name*). Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como `ftp.ejemplo.com.` y `www.ejemplo.com.`). Esto también es usado cuando corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real. Ej. `Ejemplo1 IN CNAME ejemplo2`
NS = Servidor de nombres (*name server*). Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.
MX = Intercambio de correo (*mail exchange*). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
PTR = Indicador (*pointer*). También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa.
SOA = Autoridad de la zona (*start of authority*). Proporciona información sobre el servidor DNS primario de la zona.
ANY = Toda la información de todos los tipos que exista.

Estándares de Internet [editar]

Los siguientes documentos definen el Sistema de Nombres de Dominio:

RFC 920 , *Domain Requirements* – Especificaba los dominios de nivel superior originales
RFC 1032 , *Domain Administrators Guide*
RFC 1033 , *Domain Administrators Operations Guide*
RFC 1034 , *Domain Names - Concepts and Facilities*
RFC 1035 , *Domain Names - Implementation and Specification*
RFC 1101 , *DNS Encodings of Network Names and Other Types*
RFC 1123 , *Requirements for Internet Hosts—Application and Support*
RFC 1178 , *Choosing a Name for Your Computer* (FYI 5)
RFC 1183 , *New DNS RR Definitions*
RFC 1591 , *Domain Name System Structure and Delegation* (Informational)
RFC 1912 , *Common DNS Operational and Configuration Errors*
RFC 1995 , *Incremental Zone Transfer in DNS*

RFC 1996 , *A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)*
RFC 2100 , *The Naming of Hosts* (Informational)
RFC 2136 , *Dynamic Updates in the domain name system (DNS UPDATE)*
RFC 2181 , *Clarifications to the DNS Specification*
RFC 2182 , *Selection and Operation of Secondary DNS Servers*
RFC 2308 , *Negative Caching of DNS Queries (DNS NCACHE)*
RFC 2317 , *Classless IN-ADDR.ARPA delegation* (BCP 20)
RFC 2671 , *Extension Mechanisms for DNS (EDNS0)*
RFC 2672 , *Non-Terminal DNS Name Redirection*
RFC 2845 , *Secret Key Transaction Authentication for DNS (TSIG)*
RFC 3225 , *Indicating Resolver Support of DNSSEC*
RFC 3226 , *DNSSEC and IPv6 A6 aware server/resolver message size requirements*
RFC 3597 , *Handling of Unknown DNS Resource Record (RR) Types*
RFC 3696 , *Application Techniques for Checking and Transformation of Names* (Informational)
RFC 4343 , *Domain Name System (DNS) Case Insensitivity Clarification*
RFC 4592 , *The Role of Wildcards in the Domain Name System*
RFC 4635 , *HMAC SHA TSIG Algorithm Identifiers*
RFC 4892 , *Requirements for a Mechanism Identifying a Name Server Instance* (Informational)
RFC 5001 , *DNS Name Server Identifier (NSID) Option*
RFC 5452 , *Measures for Making DNS More Resilient against Forged Answers*
RFC 5625 , *DNS Proxy Implementation Guidelines* (BCP 152)
RFC 5890 , *Internationalized Domain Names for Applications (IDNA):Definitions and Document Framework*
RFC 5891 , *Internationalized Domain Names in Applications (IDNA): Protocol*
RFC 5892 , *The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)*
RFC 5893 , *Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)*
RFC 5894 , *Internationalized Domain Names for Applications (IDNA):Background, Explanation, and Rationale* (Informacional)
RFC 5895 , *Mapping Characters for Internationalized Domain Names in Applications (IDNA) 2008* (Informacional)
RFC 5966 , *DNS Transport over TCP - Implementation Requirements*
RFC 6195 , *Domain Name System (DNS) IANA Considerations* (BCP 42)

Seguridad [editar]

RFC 4033 , *DNS Security Introduction and Requirements*
RFC 4034 , *Resource Records for the DNS Security Extensions*
RFC 4035 , *Protocol Modifications for the DNS Security Extensions*
RFC 4509 , *Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records*
RFC 4470 , *Minimally Covering NSEC Records and DNSSEC On-line Signing*
RFC 5011 , *Automated Updates of DNS Security (DNSSEC) Trust Anchors*
RFC 5155 , *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*
RFC 5702 , *Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC*
RFC 5910 , *Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)*
RFC 5933 , *Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC*

Véase también [editar]

Apoyo: listado de tipos de registros DNS
Ataques

Anexo:Listado de tipos de registros DNS
Archivo hosts
DNS dinámico
Nombre de dominio internacionalizado
Servidor raíz
Mecanismos de extension de DNS
Domain Name System Security Extensions
Servidor de agujero negro
Búsqueda DNS inversa
Transferencia de zona DNS

Ataques

DNS cache poisoning
DNS rebinding

Referencias [editar]

1. ↑ «Sistema de nombres de dominio» . *technet.microsoft.com*. Consultado el 21 de septiembre de 2016.
2. ↑ «Consulta DNS desde CMD» . Consultado el 26 de noviembre de 2015.
3. ↑ Stewart, William (2015). «Domain Name System (DNS) History» (en inglés). Consultado el 28 de febrero de 2016.
4. ↑ «History of DNS» . *CyberTelecom* (en inglés). Consultado el 28 de febrero de 2016.
5. ↑ **a b c** Lewis, Edward (2 de mayo de 2013). «The History & Evolution of DNS – Starting from the Beginning» (en inglés). Consultado el 28 de febrero de 2016.
6. ↑ **a b c** «6.2. Cómo funciona el DNS» . *Guía de Administración de Redes con Linux*. Consultado el 28 de febrero de 2016.
7. ↑ Sharma, Nirmal (31 de octubre de 2009). «Why DNS Works On Both TCP and UDP» . *windowsnetworking.com* (en inglés). Consultado el 28 de febrero de 2016.
8. ↑ Ver RFC 1035 , sección "2.3.1. Preferencia nombre de la sintaxis"
9. ↑ APWG. "Global Phishing Survey: Domain Name Use and Trends in 1H2010." 15/19/2010 apwg.org (en inglés)

Enlaces externos [editar]

Dónde se encuentran los servidores raíz
DNS de las principales operadoras

Categorías: Domain Name System | Redes informáticas | Protocolos de nivel de aplicación