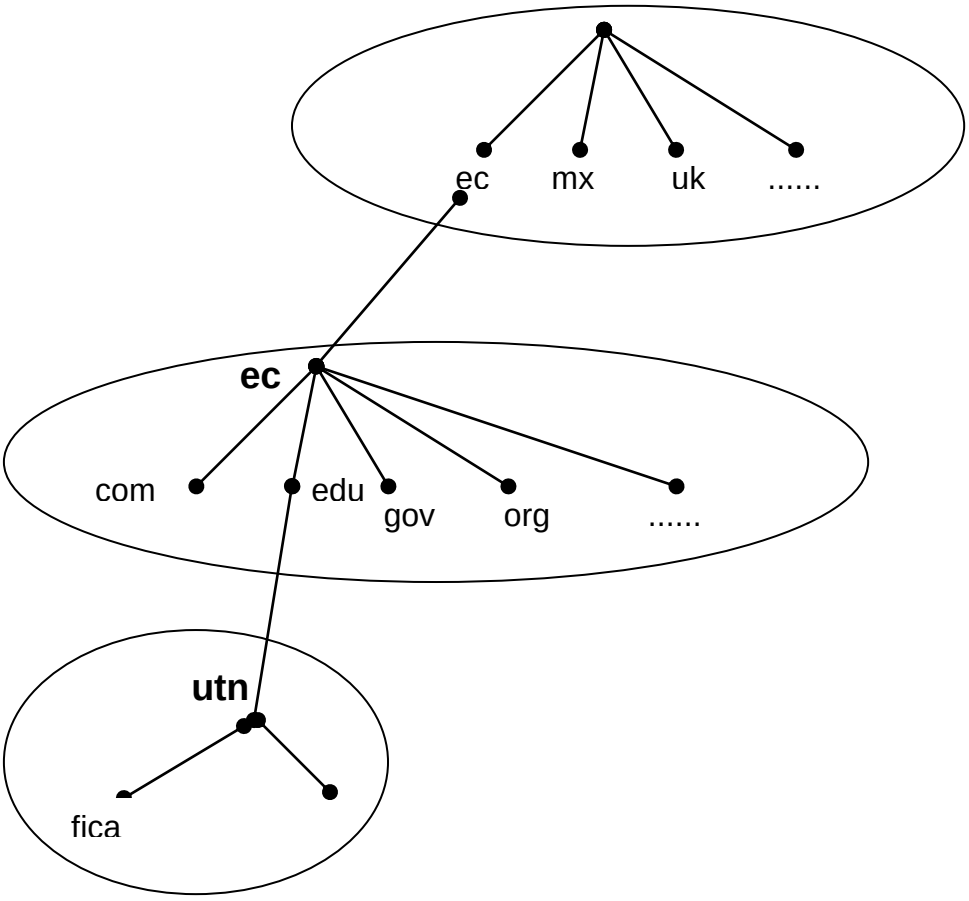
CAPÍTULO III
El DNS



3.1. Introducción

El DNS (*Domain Name Service*) es un sistema de nombres que permite traducir de nombre de host a dirección IP y viceversa. Aunque Internet sólo funciona sobre la base de direcciones IP, el DNS permite que los humanos usemos nombres de equipos que son bastante más simples de recordar que las direcciones numéricas (pero que también pueden causar muchos conflictos, puesto que los nombres son activos valiosos en algunos casos). Un ejemplo se muestra en la Tabla 3.1:

Direcciones de Internet	Números IP que les corresponden
www.fica.utn.edu.ec	192.168.1.200
www.utn.edu.ec	192.168.1.1 (interno) 64.46.79.57 (externo)
www.altavista.com	209.73.164.91 209.73.164.92 209.73.164.93 209.73.164.94 209.73.164.95 209.73.164.96 209.73.164.97 209.73.164.98 209.73.164.99

Tabla 3. 1: Direcciones de Internet con su IP correspondiente

El Sistema de Nombres de Dominios en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallas. Aunque parece muy difícil lograr todos esos objetivos, la solución no es tan compleja en realidad. El punto central se basa en un árbol que define la jerarquía entre los dominios y los subdominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda. Por ejemplo, en ***utn.edu.ec***, el dominio más alto es ***ec***. Para que exista una raíz del árbol, se puede ver como si existiera un punto al final del nombre: ***utn.edu.ec***., y todos los dominios están bajo esa raíz (también llamada “punto”).

Usando los términos de Internet, las computadoras denominadas servidores de nombres proporcionan servicios que mantienen asociaciones de nombre a dirección IP. Estos servidores de nombres DNS proporcionan esta

información a las computadoras y programas de clientes que necesitan conectarse a otras computadoras de la red.

Cuando un usuario escribe un URL (Localizador Uniforme de Recursos) en un visualizador de Internet, el visualizador contacta primero con un servidor de nombres de dominio para asociar la porción del URL referente al host y nombre de dominio a una dirección IP. Después de que el servidor de nombres DNS devuelve la asociación de nombre a dirección IP, el visualizador puede conectarse con la computadora remota utilizando la dirección IP (ver Figura 3.1).

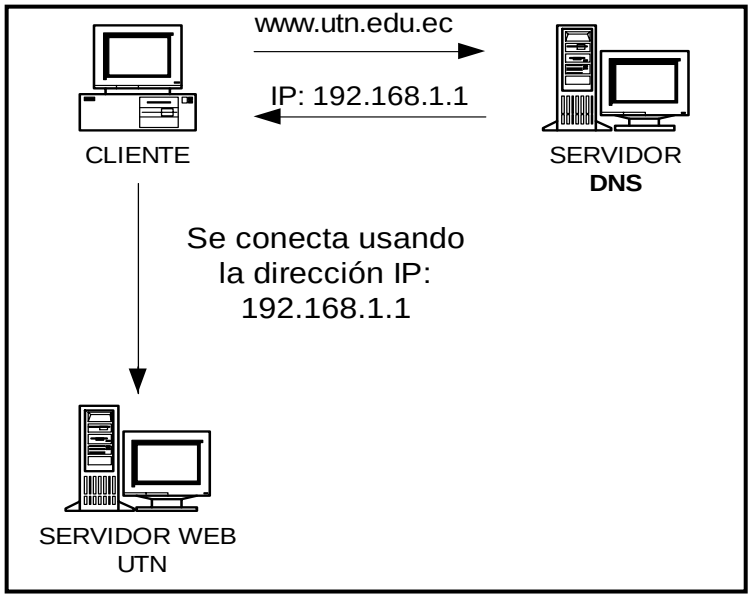


Figura 3. 1: Funcionamiento básico del DNS

Como se puede ver en la figura anterior en el lado del cliente se escribe el siguiente URL, http://www.utn.edu.ec, luego de este paso el cliente va a buscar en el servidor DNS que dirección le corresponde al URL que ingresó, el servidor DNS le devuelve el número IP que le corresponde a la Dirección que ingresó, posteriormente el cliente se enlaza con el sitio que estaba buscando. Todo este proceso parece complejo pero toma solo varios milisegundos.

Para poder garantizar que siempre este en funcionamiento el DNS cada componente del dominio (y también la raíz) tiene un servidor primario y varios servidores secundarios. Todos estos servidores tienen la misma

autoridad para responder por ese dominio, pero el primario es el único con derecho para hacer modificaciones en él. Por ello, el primario tiene la copia maestra y los secundarios copian la información desde él. El servidor de nombres es un programa que típicamente es una versión de BIND (*Berkeley Internet Name Daemon*). En general es mucho mejor traer la última versión desde Internet (www.isc.org) que usar la que viene con el Sistema Operativo, porque es un servidor que ha cambiado mucho a lo largo del tiempo.

La raíz del sistema de dominios es asistida por algunos servidores “bien conocidos". Todo servidor de nombres debe ser configurado con la lista de los servidores raíz bien conocidos (en general lo vienen de fábrica). Estos servidores dicen qué dominios de primer nivel existen y cuales son sus servidores de nombres. Recursivamente, los servidores de esos dominios dicen qué subdominios existen y cuales son sus servidores.

Si existe un conflicto de competencia entre el servidor de un dominio y el de un subdominio: ambos deben saber cuales son los servidores de nombres del subdominio. En un inicio, estarán de acuerdo, pero con el tiempo los servidores pueden ir cambiando, y las versiones de ambos pueden ser inconsistentes. Actualmente, el que manda es el servidor del subdominio, y su información es la más importante.

En general, la regla ideal es que la lista de servidores que figura en el dominio sea un subconjunto de la lista que figura en el subdominio.

La implementación del DNS en Internet, encarga la responsabilidad de mantener las asociaciones de nombre a direcciones IP entre los servidores de nombres DNS localizados por toda Internet. Cada servidor de nombres DNS de Internet gestiona solo una parte del espacio de nombres de dominios y se le denomina autoritario sólo para esa parte que gestiona. En otras palabras, cada servidor de nombres DNS sólo mantiene datos DNS para el dominio para el cual es autoritario y para ningún otro.

Cuando otros servidores de nombres de Internet necesitan asociar nombres a direcciones IP que no gestionan, contactan con el servidor de nombres autoritario que gestiona dichas asociaciones. Este proceso permite que los datos DNS y la gestión de dichos datos sean distribuidos a través de Internet.

3.1.1. Estructura del DNS de Internet

El DNS de Internet es como un directorio del disco duro de una computadora, si lo consideramos de esta manera cada dominio tiene un nombre, es así como podemos a cada dominio dividirlo y tener subdominios, en la Figura 3.2 colocamos una ilustración de cómo se encuentra estructurado el DNS de Internet.

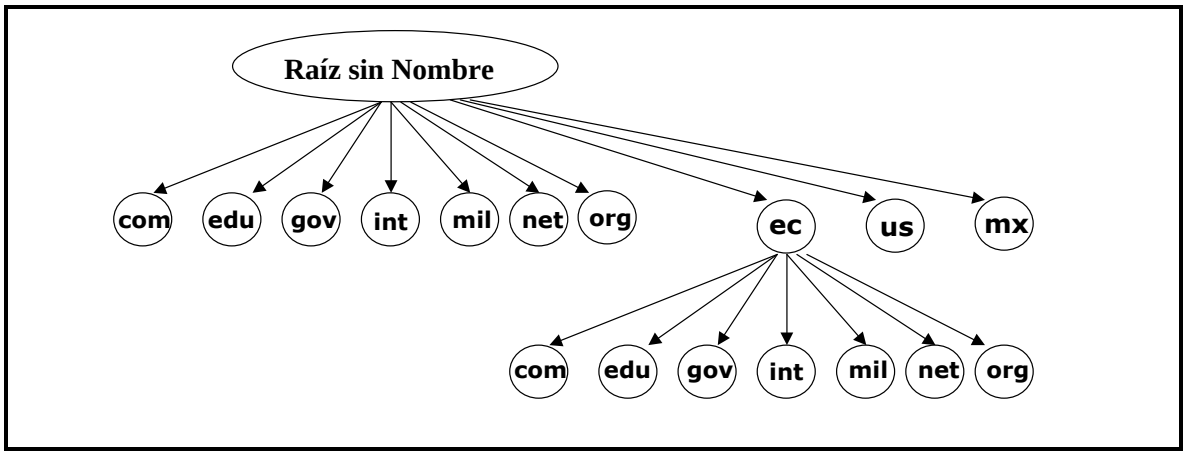


Figura 3. 2: Estructura Jerárquica del DNS de Internet

3.1.2. Categorías Básicas de Grupos de Dominios de Internet

Internet divide en siete categorías básicas de grupos de Dominios, los que detallamos en la Tabla 3.2:

Dominio	Descripción
Com	Organizaciones comerciales, como negocios
Edu	Organizaciones educativas, como universidades
Gov	Organizaciones gubernamentales
Int	Organizaciones internacionales
Mil	Organizaciones militares
Net	Una red que no encuadre en ninguna de las otras categorías de dominio de organizaciones
Org	Una organización que no encuadre en ninguna de las otras categorías de dominio de organizaciones

Tabla 3. 2: Tabla de Categorias Básicas de grupos de Dominios

Ahora además existen dominios agrupados por países, los cuales se identifican con dos iniciales, algunos ejemplos los anotamos en la Tabla 3.3:

ar Argentina	**Cu** Cuba	**in** India
au Australia	**De** Alemania	**Jp** Japón
be Bélgica	**Ec** Ecuador,	**Mx** México,
br Brasil	**Es** España	**Pa** Panamá
ca Canada	**Fr** Francia	**Pe** Peru .
cl Chile,	**Gr** Grecia	**Py** Paraguay
co Colombia,	**Gt** Guatemala	**Uy** Uruguay
cr Costa Rica	**Hn** Honduras,	**Uk** Gran Bretaña

Tabla 3. 3: Tabla de dominios por países

Si no tienen las iniciales del país significa que el dominio se encuentra en los Estados Unidos; país por el cual circula la mayor parte del tráfico de Internet.

3.1.3. Estructura del DNS en la Intranet

El modelo del DNS en Internet se lo puede aplicar perfectamente a una Intranet, en donde la raíz sería el nombre de la institución en la cual se va a aplicar la Intranet y los subdominios serían los departamentos existentes dentro de la organización.

3.2. Servidores de nombres DNS primarios y secundarios

Antes de explicar que son DNS primarios y secundarios es necesario explicar que es una zona. Las zonas son las agrupaciones administrativas principales. Por ejemplo una zona es una porción administrativa (en pequeñas empresas puede ser toda la agrupación) de un dominio DNS, denominado raíz de la zona.

Cada zona debe ser gestionada empleando al menos un servidor de nombres DNS primario y otro secundario. Un servidor de nombres *primario* contiene las asociaciones de nombre a dirección IP originales en un archivo de zona localizado en la computadora local. Un servidor de nombres *secundario* contiene una copia de las asociaciones de nombre a dirección IP de la zona. Recibe esta copia de un servidor de nombres maestro, bien sea el servidor principal o algún otro servidor DNS secundario.

El empleo de ambos servidores, primario y secundario, es necesario para proporcionar redundancia de base de datos y un grado de tolerancia a fallos. Proporcionar un servidor de nombres DNS primario y uno secundario es un requisito para el registro de dominios en InterNIC[1].

Si se establece un nodo en Internet y se registra la empresa en InterNIC, se debe proporcionar información acerca de ambos servidores de nombres, primario y secundario. InterNIC establece este requisito para asegurar que los dominios registrados siempre puedan proporcionar las asociaciones de nombre a dirección IP necesarias para la conectividad Internet.

3.2.1. InterNIC

InterNIC es el Centro de Información de Red de Internet (*InterNIC, Internet Network Information Center*), la misma que se encarga de manejar las nomenclaturas de dominio. InterNIC delega responsabilidad de asignar nomenclaturas a diferentes organizaciones y cada una de estas se encarga de una parte específica de la estructura del árbol DNS, estas áreas de responsabilidad se las denomina *zonas*, por lo que se puede decir que InterNIC encarga la responsabilidad de asignar nombres dentro de una zona a organizaciones específicas. Las organizaciones responsables de la zona pueden subdividir y transferir responsabilidades.

3.3. Servidores de nombres DNS Locales y Globales

Los Servidores de nombres **Globales** tienen la particularidad de pertenecer a instituciones encargadas o preparadas para brindar los servicios de Internet, es decir que en cada una de estas organizaciones se encuentran uno o varios servidores cuyo papel fundamental es procesar las consultas remotas, por lo que se puede decir que un servidor DNS Global es un servidor raíz que tiene una base de datos primaria de traducción de nombres, cuyo listado se duplica en uno o varios servidores raíz.

Los Servidores de nombres **Locales** pueden ser servidores principales o secundarios que tienen como papel fundamental atender peticiones de

[1] InterNIC administra la cesión de nombres de dominios a organizaciones, empresas e instituciones

traducción de nombres de las direcciones de un grupo de equipos en un área local, es decir que en un servidor de este tipo almacena una lista de direcciones de una red de área local.

3.4. Configuración del Servidor

Un servidor de nombres cumple dos roles: ayudar a los resolvers locales a resolver nombres y a servir con autoridad como primario y secundario de algunos dominios. En las organizaciones muy grandes, puede ser una buena idea separar estos dos roles, teniendo servidores para resolver y servidores para el dominio local. Tenerlos juntos es también razonable en todo caso, porque la mayoría de las consultas son dentro del dominio local, que típicamente servimos.

Para funcionar bien, se debe tener un servidor de nombres y configurarlo de modo que ubique los servidores raíz, que tenga los dominios para los que es primario y conozca para cuales debe actuar como secundario. El archivo que contiene toda la información sobre un dominio se conoce como una *zona*. Dentro de la zona se especifican valores asociados al dominio propiamente, Los servidores de nombres del dominio (records NS), los nombres de las máquinas que existen bajo él y su dirección IP (records A), los nombres de sus subdominios (si existen) y sus servidores de nombres (records NS), servidores de correo (records MX), etc. Un servidor de nombres que tiene autoridad sobre un dominio debe tener localmente una copia de la zona que lo define: si es primario tiene la versión modificable, si es secundario debe tener una copia obtenida desde el primario.

3.5. El Resolver

El DNS es un servidor con clientes un poco especiales. En general no existe un cliente propiamente como tal, sino que múltiples clientes, ya que la traducción de nombre a IP se presenta en general como una función de biblioteca.

La mayoría de los sistemas operativos ofrecen múltiples formas de hacer esa traducción, con archivos de hosts, servicios de red local y DNS. Este

capitulo se centra en el DNS, pero la existencia de otros servicios a veces causa problemas.

La operación del *resolver* comienza cuando recibe un nombre y debe traducirlo. Existen dos tipos de nombres en Internet: los nombres totalmente calificados (**fica.utn.edu.ec**) y los nombres parciales (**fica**). Es ilegal usar nombres intermedios (como **fica.utn**) porque si existiera el dominio de primer nivel **.utn** ese nombre sería ambiguo.

Para comenzar, el resolver debe conocer uno o más servidores de nombres a quienes enviarles la consulta. Esta información se configura en cada máquina, colocando la dirección IP del servidor (por supuesto, no es posible usar el nombre en este lugar). La traducción completa se le pide al servidor local.

Para resolver una consulta, un servidor de nombres debe conocer a lo menos a los servidores raíz. De ese modo, si nunca ha oído hablar de ninguno de los dominios del nombre, puede preguntarle a un servidor raíz. Por lo menos, el servidor raíz tiene que conocer la lista de servidores del dominio de primer nivel del nombre (o sabe que no existe). Si sabe más que eso (por ejemplo, si es secundario del dominio de primer nivel) responde lo más posible. Las respuestas son de dos tipos: una lista de servidores de nombres que saben más que él (servidores del dominio o del sub-dominio) o una lista de direcciones IP que corresponden a la máquina buscada.

Además de los primarios y secundarios, los otros servidores pueden responder consultas sobre un dominio si ellos preguntaron hace poco y almacenaron la respuesta. Esta respuesta queda en un cache, y se marca como sin autoridad y se acompaña de la lista de servidores que saben más que él. El resolver elige si la acepta o no.

3.6. Diseño de la Base de Datos de un Servidor de Nombres

Para el caso de tener una organización pequeña, la información se la puede estructurar como una base de datos única. Forma que no es la más

adecuada para organizaciones que se encuentran distribuidas en diferentes lugares geográficos y a largas distancias, para lo cual se considera que es un mejor modelo, delegar la gestión del árbol de nombres de la organización en cada uno de esos lugares, por lo que se hace necesario poner en funcionamiento servidores de nombres independientes en cada uno de esos lugares.

3.6.1. Zonas

Un servidor de nombres DNS puede gestionar un dominio completo o uno o más subdominios mediante agrupaciones administrativas denominadas zonas. Una zona es una agrupación de bases de datos administrativas y de servidores DNS empleada para gestionar todo o parte de un dominio de empresa. Si el dominio es grande (contiene muchos subdominios y computadoras), el servidor de nombres autoritario del dominio puede delegar la gestión de partes del dominio a uno o más servidores de dominios DNS.

3.6.2. Ubicación de los servidores de nombres de dominio

Para la mayoría de instituciones es más fácil tener un solo grupo de servidores primarios y secundarios en la red institucional, inclusive en el caso de que los datos se encuentren distribuidos en varias zonas, es aceptable la utilización de un servidor para varias zonas e incluso para varios dominios. Los datos de cada zona se almacenan en un archivo diferente, por lo que cada uno de estos se puede actualizar independientemente, dependiendo exclusivamente del administrador.

3.6.3. Transferencia de zona

Para poder mantener una copia de la información sobre una o más zonas se hace necesario instalar un servidor secundario. Este adquiere la información de un servidor primario de la zona mediante la ***transferencia de zona***, este procedimiento facilita la administración de las direcciones.

Dependiendo de la configuración un servidor secundario puede obtener la información de varios servidores primarios. Un servidor puede actuar como primario para algunas zonas y secundario para otras.

3.6.4. Datos que requiere el DNS

Un DNS para realizar su trabajo necesita al menos los siguientes datos:

- Una lista de servidores *raíz* locales y mundiales para determinar a donde realizará las consultas externas.
- Una lista de nombres con sus direcciones correspondientes
- Una lista de direcciones con sus nombres correspondientes

3.6.5. Registros que deben estar presentes en el DNS

Tipo de Registro	Descripción
SOA	Inicio de Autoridad (*start of Authority*): Identifica el dominio o la zona y fija una serie de parámetros.
NS	Hace corresponder el nombre de dominio con el nombre de una computadora de confianza para el dominio
A	Hace corresponder el nombre de un sistema con su dirección. Si un sistema, por ejemplo, un encaminador, tiene varias direcciones, habrá un registro diferente para cada una de ellas.
CNAME	Hace corresponder un alias con el nombre canónico, verdadero.
MX	Intercambiador de correo (Mail Exchanger). Identifica a los sistemas que transmiten correo en la organización.
TXT	Proporciona una forma de añadir comentarios de texto a la base de datos, es decir que un registro txt podría hacer corresponder una dirección estándar con el nombre, dirección, número de teléfono de una organización.
WKS	Servicios públicos (*Well-Known Services)*. Puede listar los servicios de las aplicaciones disponibles en el host. Se usa muy poco o nada.
HINFO	Información del host *(Host Information)*, como el modelo y tipo de computadora. Raramente usado.
PTR	Hace corresponder una dirección de IP con el nombre de un sistema. Usado en archivos dirección-nombre.

Tabla 3. 4: Tabla de Registros del DNS

El registro SOA: El primer registro es muy importante. Se trata del registro de inicio de autoridad. En este registro se encontrara información como valores de temporización, si el servidor es primario o secundario para determinado dominio.

Los servidores secundarios copiaran esta información y trabajarán con las ordenes que el servidor primario disponga o haya sido dispuesta para cada uno de los servidores como ejemplo se podría decir que un servidor secundario debe conectarse a las 2 de la tarde y otro servidor debe conectarse al primario a las 24 horas, es decir que en el registro SOA se almacena la información que permitirá el funcionamiento de permisos de una red.

Registros de servidores de nombres (NS): Los servidores *(NS-Name Server)* indican los servidores de nombres del dominio. En el caso de existir subzonas se necesitaran direcciones a estas de tal forma que el servidor de más alto nivel pueda facilitar el ingreso o la comunicación con los servidores de más bajo nivel, para realizar el acceso a estos servidores se necesita de registros de dirección los mismos que se denominan registros de *asociación*.

El administrador del servidor padre debe preocuparse por mantener actualizado la lista de nombres y direcciones así como también de mantenerse en contacto con los administradores hijo. Por lo que se puede decir que no necesariamente un servidor de nivel superior debe ser de confianza de los servidores hijo en vista de que cada uno de estos puede tener un administrador diferente.

Registros de direcciones: Los registros de direcciones, simplemente hacen corresponder un nombre con una dirección. Así la dirección de *srvfica* es 192.168.1.200.

Registros CNAME: En el caso de que en la misma máquina se ejecuten varios servicios, los registros de nombres canónicos *(CNAME – Canonical Name)* definen los alias de los host y permiten a los usuarios teclear *www.fica, ftp.fica, gopher.fica.*

Registros de intercambio de correo: Estos registros permiten a los servidores de intercambio de *correo (MX- Mail Exchanger)* realizar el reenvio de correo electrónico entre redes.

Registros TXT: Estos registros permiten al administrador incluir comentarios en las bases de datos, ya que estos registros no poseen una función real.

Registros HINFO: Estos registros permiten al usuario identificar el tipo de hardware y sistema operativo que está utilizando un sistema.

BIBLIOGRAFIA:

Ambegaonkar Prakash. Kit de Recursos de Intranet
Editorial Osborne / McGraw-Hill primera edición

Feit TCP/IP
Editorial McGraw-Hill, primera edición 1998

Greer Tyson.- Así son las Intranets
Editorial Microsoft Press primera edición 1997

Kris Jamsa / Ken Cope. Programación en Internet (Curso sobre TCP/IP)
Editorial McGraw-Hill primera edición 1996

http://www.w3c.org W3 Consortium Organization.