Capa de aplicación TCP/IP

1. Servicios de mensajería

a. Simple Mail Transfer Protocol (SMTP)

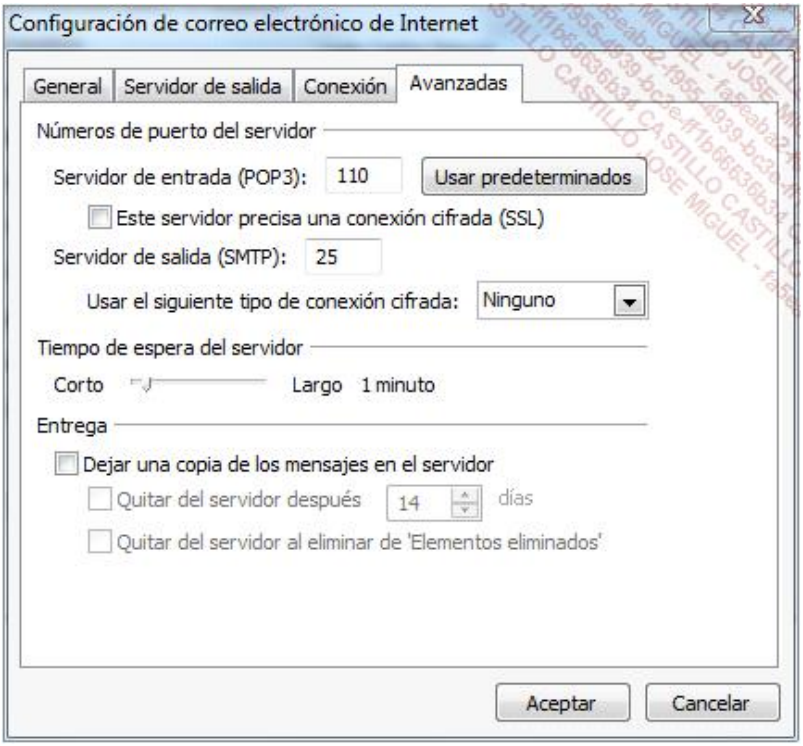
SMTP es un protocolo de transferencia simple que se utiliza en mensajería electrónica. Se basa en TCP e IP y no integra ninguna interfaz de usuario.

El objetivo de SMTP es transmitir mensajes (e-mail) hasta el buzón de correo del destinatario.

Este protocolo utiliza equipos distintos y nombrados según su función:

- MUA (*Mail User Agent*), cliente de mensajería.
- MTA (*Mail Transfer Agent*), transmisor de correo.
- MDA (*Mail Delivery Agent*), servicio de entrega de correo en los buzones de los destinatarios.

Este protocolo utiliza el puerto TCP 25 en el lado del servidor. La RFC 5321 describe el funcionamiento de este protocolo.



Configuración avanzada del correo electrónico en el cliente

Para el envío de un mensaje por SMTP, se deben identificar un emisor y un destinatario. Para ello, deben tener una dirección formada por la referencia del buzón a la izquierda del signo @, y por un nombre de dominio a la derecha.

El mensaje se divide en tres partes:

- Un sobre, que los agentes utilizan para el enrutamiento.

- Una cabecera, que incluye las direcciones y el objeto.
- El cuerpo, que contiene el mensaje.

b. Post Office Protocol 3 (POP3)

Al contrario que SMTP, que tiene el papel de transporte, POP se dedica específicamente a la publicación y al acceso remoto a un servidor de correo.

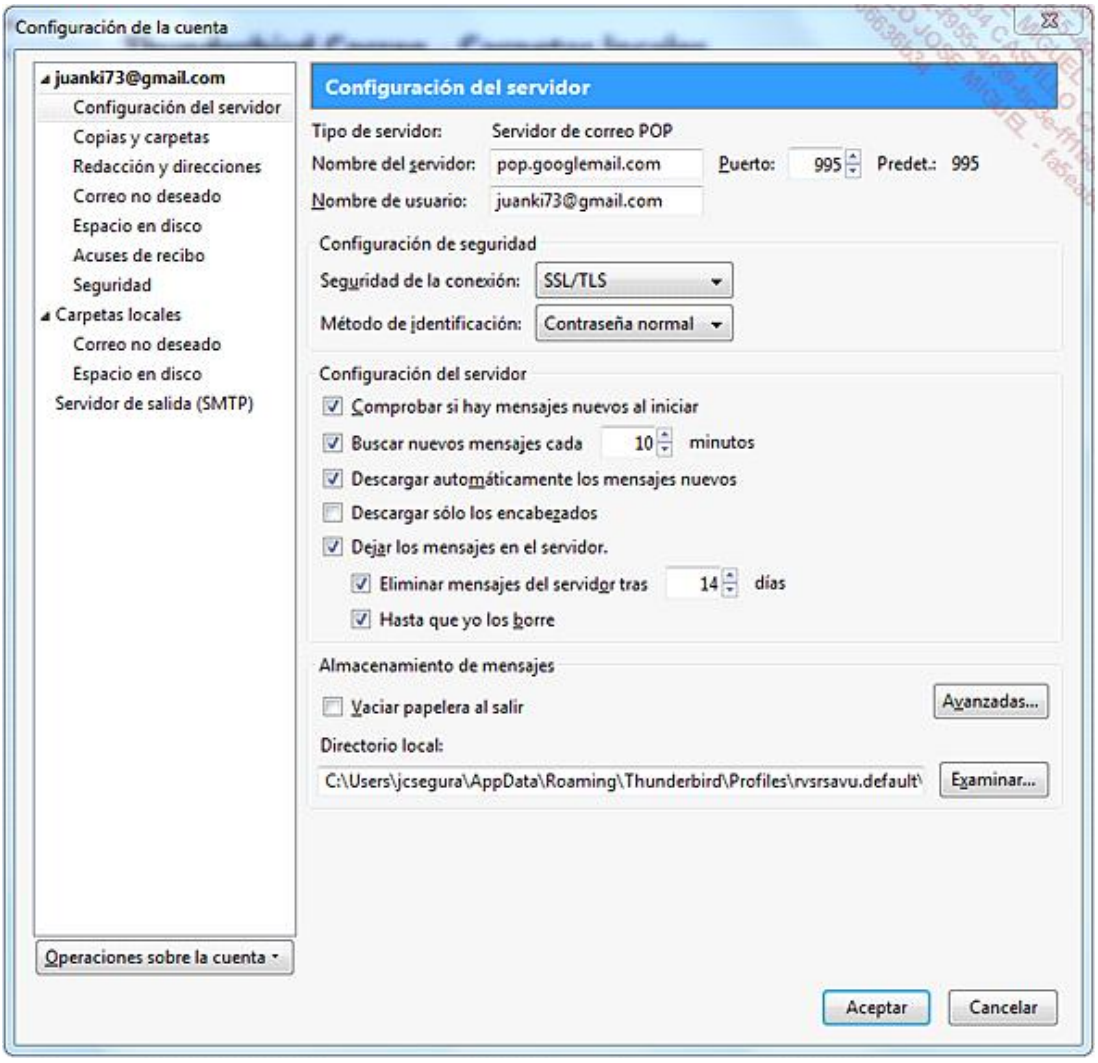
El servidor POP se comunica con el agente usuario (*User Agent*), por ejemplo Mozilla Thunderbird, a través de una conexión síncrona. El servidor transfiere al cliente los mensajes, y después los elimina a petición del cliente.

Normalmente, el servidor solo conserva los mensajes que no se han transferido al cliente.

POP 3 se define en la RFC 1939 y utiliza el puerto TCP 110 y el 995 en modo seguro.

Con POP, el cliente tiene que establecer una conexión previa con el servidor utilizando un usuario y una contraseña. Por supuesto, es el cliente de correo el que se encarga de ello. La sesión se cerrará con el comando *quit*. Una vez se ha establecido la conexión, el servidor bloquea el buzón del usuario y entra en fase de transacción.

Por defecto, con POP el nombre y la contraseña se transmiten sin cifrar. Algunos servidores POP implementan el algoritmo MD5 (*Message Digest 5*, RFC 1321) para proteger la contraseña enviada.



c. Internet Message Access Protocol (IMAP)

IMAP permite almacenar y conservar en el servidor los correos electrónicos (e-mails), en lugar de descargarlos sistemáticamente en el cliente.

De hecho, el cliente IMAP se conforma con visualizar de forma remota las cabeceras de los mensajes y permite elegir cuáles se descargan finalmente.

IMAP tiene una gran ventaja sobre POP3 y se presentó como su sucesor. De hecho, a veces se hablaba de IMAP4 para indicar este hecho. El modo de funcionamiento de IMAP podría haber sido una ventaja crucial si la descarga de mensajes se hubiera continuado haciendo por líneas analógicas lentas, que facturaban en función del tiempo.

El crecimiento de las conexiones de banda ancha fue un primer freno para el uso de IMAP en lugar de POP3. Además, la generalización de la consulta de los mensajes directamente en los sitios web (*webmail*) ha anulado las ventajas de las funcionalidades complementarias que podían ser interesantes.

Sin embargo, desde hace algunos años, IMAP ha conseguido avanzar y la mayor parte de los operadores lo ofrece y está incluido en numerosas herramientas colaborativas.

Hay numerosos comandos disponibles en IMAP. Permiten gestionar los buzones, los mensajes, efectuar búsquedas, transferencias selectivas... Con IMAP, también es posible compartir un mismo buzón de correo entre diferentes personas.

2. Servicios de transferencia de archivos

a. HyperText Transfer Protocol (HTTP)

HTTP es, sobre todo, un protocolo de transferencia de archivos. *HyperText Markup Language* (HTML) se utiliza para formatear y visualizar. Los archivos transmitidos al cliente los interpreta un software navegador (*browser*).

El protocolo HTTP es utilizado por un servidor web, que almacena la información en forma de páginas de texto (HTML), imágenes, vídeos, sonidos… Cada entidad corresponde a un archivo, dentro de una jerarquía.

La versión de HTML que actualmente está en desarrollo es la versión 5, que nació en 2006. La última versión completa, la 4.01, data de 1999.

Sin embargo, la mayor parte de los navegadores de Internet, en sus últimas versiones, incorporan las novedades ofrecidas por esta versión del protocolo (Internet Explorer, Chrome, Firefox, Safari u Opera).


La URL http://html5test.com/ permite probar las funcionalidades HTML5 que soporta su navegador.

HTML5 proviene de la colaboración entre el W3C (*World Wide Web Consortium*), que sobre todo ha trabajado en XHTML 2.0, y de WHATWG (*Web Hypertext Application Technology Group*), que se centró en los formularios y aplicaciones web.

Se han enunciado algunas nuevas reglas para esta nueva versión:

- Las nuevas funcionalidades deben basarse en HTML, CSS (*Cascading Style Sheet* u hojas de estilo en cascada), DOM (*Document Object Model*) y JavaScript.

- Se debe reducir al máximo la utilización de componentes externos (p. ej., Plugin Flash).
- Debe haber un perfecto control de errores.
- Numerosas etiquetas complementarias reemplazan a scripts.
- HTML5 debe ser independiente de los dispositivos.
- Los procesos de desarrollo deben ser accesibles al público.

En HTML5 solo hay una declaración <!DOCTYPE>.

De este modo, el documento HTML5 más pequeño posible se parecerá a este:

```
<!DOCTYPE html>
<html>
<head>
<title>Título del documento</title>
</head>

<body>
El contenido del documento...
</body>

</html>
```

Entre las nuevas funcionalidades de HTML5, se encuentran:

- El elemento `<canvas>` para el diseño 2D.
- Los elementos `<audio>` y `<video>` para las funcionalidades multimedia.
- La implementación del almacenamiento local.
- Nuevos elementos que definen nuevos contenidos, como `<article>`, `<section>`, `<nav>` o `<footer>`.

`<nav>` permite definir vínculos de navegación. `<footer>` es la firma o el pie de página de un documento.

- Nuevos formularios, como *calendar*, *date*, *time*, *email*, *search* o *url*.

Para visualizar esta información, se utilizan las URL (*Uniform Resource Locator*). Una URL requiere, en primer lugar, el protocolo (http://) y a continuación el alias del servidor web y la referencia de la entidad.

Llamada a una URL en un navegador

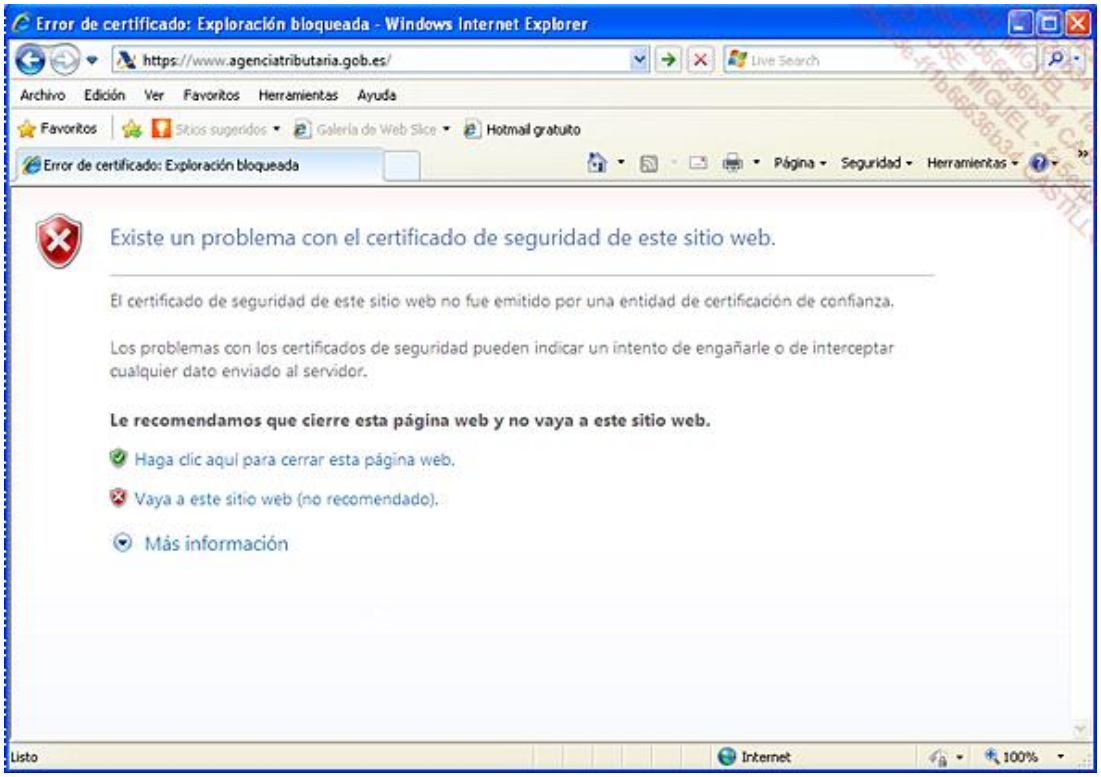
Por ejemplo, un navegador puede mostrar la página «redes.html» del directorio «Libros» llamando a la URL http://www.editions-eni.fr/libros/redes.html, que está gestionada por el servidor www.eni.fr.

Para formular las comunicaciones entre clientes y servidores, el protocolo HTTP utiliza comandos, llamados métodos, en el puerto TCP 80. Estos métodos ofrecen diferentes funciones, como la llamada a páginas (*get*), el envío de formularios (*post*)...

El protocolo que se utiliza actualmente es HTTP 1.1.

De forma predeterminada, el texto transmitido entre un cliente y un servidor se realiza sin cifrar. De esta manera es perfectamente legible por cualquiera que intercepte la conversación. Para solucionar este defecto, la versión segura del protocolo, HTTPS (TCP 443), cifra la comunicación y convierte la información en confidencial.

El protocolo HTTPS también se denomina SSL (*Secure Socket Layer*). Su versión estándar, que se puede usar con otros protocolos, es TLS (*Transport Layer Security*). Esta denominación muestra una voluntad más general de cifrar la comunicación.



Aviso de IE9 de conexión a un sitio seguro (diálogo SSL)

b. File Transfer Protocol (FTP) y Trivial FTP (TFTP)

FTP es un protocolo de transferencia de archivos basado en un método fiable e implementado en TCP. La principal ventaja de FTP es que se puede utilizar entre sistemas operativos diferentes, que se basan en sistemas de archivos heterogéneos.

El protocolo FTP ofrece dos tipos de acceso. El primero es una conexión anónima, con el identificador predeterminado anónimo. Este modo es similar a la conexión HTTP «clásica». Por el contrario, podemos querer que la descarga de archivos en un sentido o en otro sea segura. Por lo tanto, es posible solicitar la autentificación de una cuenta de usuario conocida.

Solicitud de autentificación y mensaje que detalla la prohibición de uso anónimo

El usuario podrá entonces, mediante la utilización de comandos propios de FTP, mover archivos de un directorio a otro (según los permisos de los que el usuario disponga en cada sistema).

Hay dos tipos de clientes FTP. El primero es gráfico y la mayoría de veces tiene la forma de un navegador, que ofrece funciones como tal, como Internet Explorer o Firefox.

Para los puristas en Windows o Linux, está disponible el cliente de línea de comandos, como se muestra en la siguiente captura:

Ejemplo del entorno interactivo FTP

El protocolo FTP es peculiar, ya que utiliza dos conexiones separadas para su uso:

- Un canal de comandos/control en el puerto 21 (lado servidor).
- Un canal de datos, en el puerto 20 (lado servidor).

Además, este protocolo ofrece dos modos. El primero, activo, parece un diálogo de tipo cliente/servidor, pero con la utilización de 2 canales (comandos y datos). En el siguiente esquema se puede ver su funcionamiento.

El segundo modo, pasivo, se diseñó para la transferencia de archivos entre servidores. En este caso, el canal de datos no es en el puerto 20, sino en un puerto aleatorio.

Trivial FTP (TFTP) permite descargar más rápidamente la información pero sin garantizar su integridad. Su falta de fiabilidad se basa en el hecho de que utiliza el protocolo UDP en lugar de TCP para el transporte. Este protocolo se utiliza en redes locales de diseño reciente, que podemos considerar en principio más fiables.

Se utilizará igualmente TFTP para realizar copias de seguridad de configuraciones de conmutadores o routers. Para hacer la copia de seguridad diaria de un router CISCO Router1 en un servidor TFTP, cuya dirección es 10.1.2.100, se utilizará el siguiente comando:

```
Router1#copy running-config tftp:
Address or name of remote host []? 10.1.2.100
Destination filename [router1-confg]?
Copia_de_seguridad_de_mi_router!!
1030 bytes copied in 2.489 secs (395 bytes/sec)
Router1#
```

De igual modo, para restaurar esta copia de seguridad en otro router, Router2, se puede utilizar un comando parecido:

```
Router2#copy tftp: running-config
Address or name of remote host []? 10.1.2.100
Source filename []? Copia_de_seguridad_de_mi_router
Destination filename [startup-config]?
Accessing tftp://10.1.2.100/Copia_de_seguridad_de_mi_router...
Loading Copia_de_seguridad_de_mi_router from 10.1.2.100
(via FastEthernet0/0): !
[OK - 1030 bytes]
1030 bytes copied in 9.612 secs (107 bytes/sec)
Router2#
```

c. Network File System (NFS)

Desarrollado por SUN en 1985, NFS es un sistema de archivos distribuido para entornos heterogéneos. Permite a los usuarios de ordenadores y sistemas operativos diferentes acceder a un sistema de archivos remoto, sin tener que aprender nuevos comandos.

NFS fue el primer intercambio de archivos verdaderamente operativo y constituyó un complemento indispensable del entorno de estaciones de trabajo que ofrecía SUN. La popularidad de su sistema operativo SOLARIS permitió

contribuir al éxito de NFS.

A lo largo del tiempo se han creado diferentes versiones de NFS:

NFSv2 y v3 se basan en las llamadas a procedimientos remotos o RPC (*Remote Procedure Call*) y se definen respectivamente en las RFC 1094 y 1813.

La versión 2 es más antigua y está ampliamente extendida.

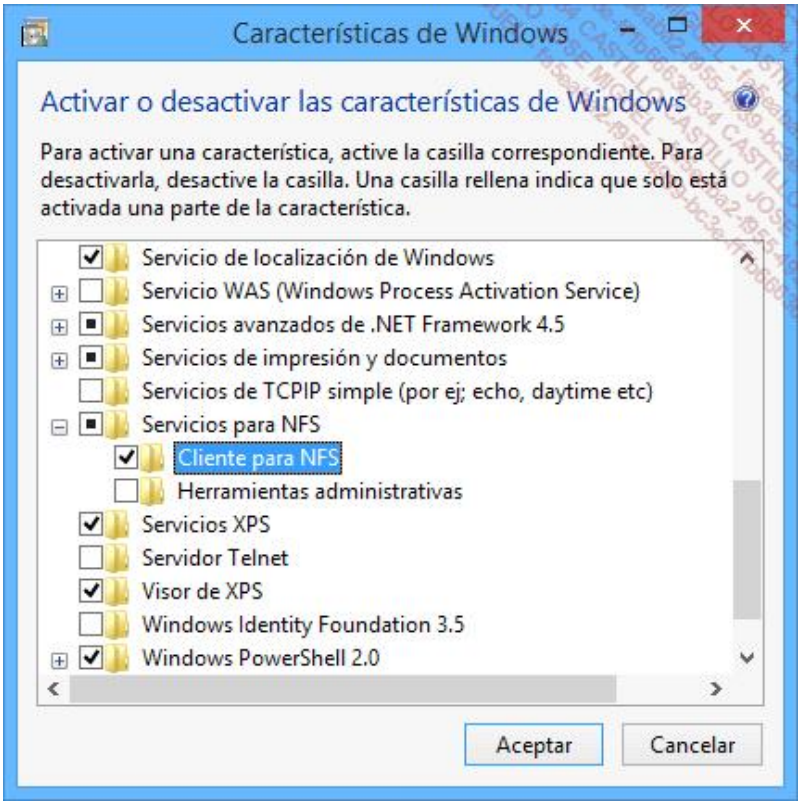
La versión 3 mejora un poco la gestión de errores y permite tratar bloques de tamaño variable, pero no es completamente compatible con la v2.

La versión 4 ya no utiliza los RPC que se basan en puertos aleatorios y que acarrean problemas de seguridad cuando se utilizan cortafuegos entre clientes y servidores.

Esta última versión, definida en la RFC 3530, implementa igualmente kerberos para la autenticación y permite gestionar listas de control de acceso (ACL o *Access Control List*) para permitir definir autorizaciones basándose en grupos de usuarios.

A pesar de su antigüedad, este protocolo de gestión de archivos en red está presente hoy en día en las empresas, en particular al lado de CIFS (*Common Internet File System* o sistema de archivos Microsoft).

Los NAS (*Network Attached Storage*) ofrecen NFS. Aparece como rol de servicio en Windows Server 2008 y 2012. En Windows, hay también un cliente NFS como componente opcional que se puede activar.



Cliente NFS en Windows 8.1

3. Servicios de administración y de gestión de red

a. Domain Name System (DNS)

Introducción

El objetivo del sistema de nombres de dominio es ofrecer una resolución basada en nombres jerárquicos y distribuidos para los huéspedes IP conectados a la red.

El sistema de nombres de dominio existe desde 1983, año en que fue creado por Paul Mockapertis (RFC 882 y 883); remplazó históricamente la gestión de un archivo *hosts* que se utilizaba al principio en Internet y que era mantenido por el *Network Information Center* del *Stanford Research Institute* (SRI).

La norma correspondiente a DNS se publicó finalmente en 1987 (RFC 1034 y 1035).

Al principio el sistema permitía solamente resolver nombres en direcciones IP, así como direcciones IP en nombres.

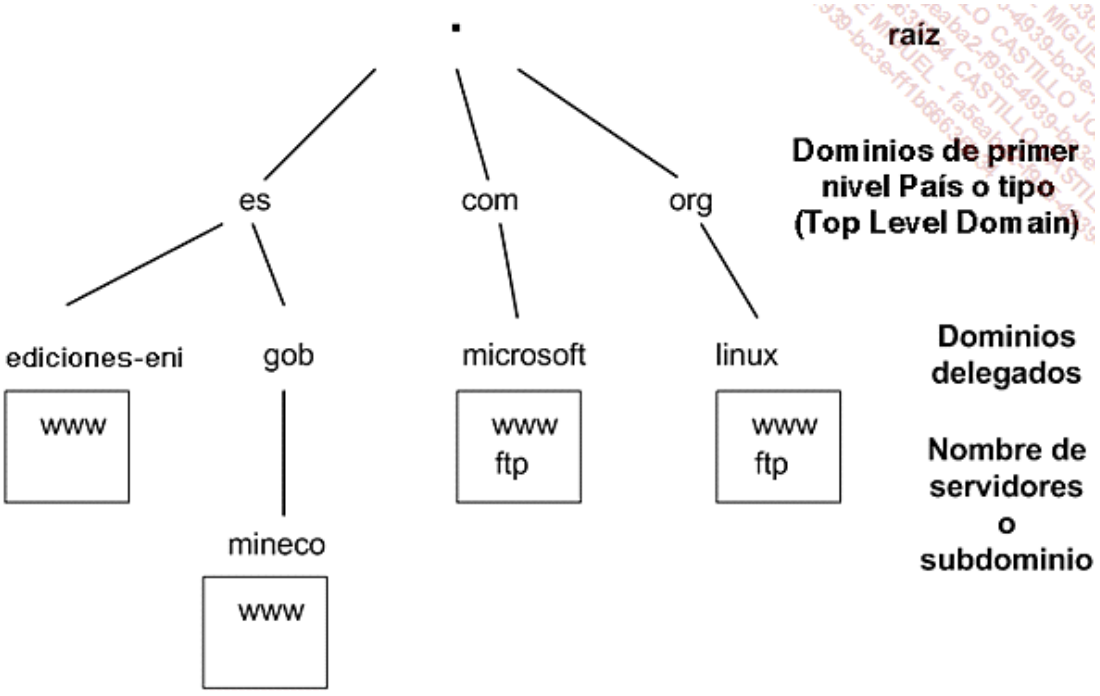
La resolución de dirección en nombre es una funcionalidad que se utiliza como una verificación de identidad y se implementa en UNIX, por ejemplo para verificar el nombre de un servidor del que se tiene que hacer una copia de seguridad cuya dirección IP es conocida o verificar los huéspedes en un entorno NFS (*Network File System*).

El sistema ha evolucionado progresivamente para actuar como un verdadero servicio de localización de recursos: de este modo, hoy en día, un ordenador puede preguntar al servicio DNS para encontrar un servicio de mensajería correspondiente a un dominio específico (registro MX o *Mail eXchanger*), encontrar un servidor Kerberos, un servidor proxy de Internet, un servidor LDAP (*Lightweight Directory Access Protocol*), un servidor SIP (*Session Initiation Protocol*) o incluso localizar un servicio de licencias Microsoft. El SRV Record o registro de servicio permite de este modo definir cualquier tipo de servicio basado en UDP o TCP.

DNS ahora implementa tanto IPv6 como IPv4 para identificar los objetos dentro de la arborescencia lógica.

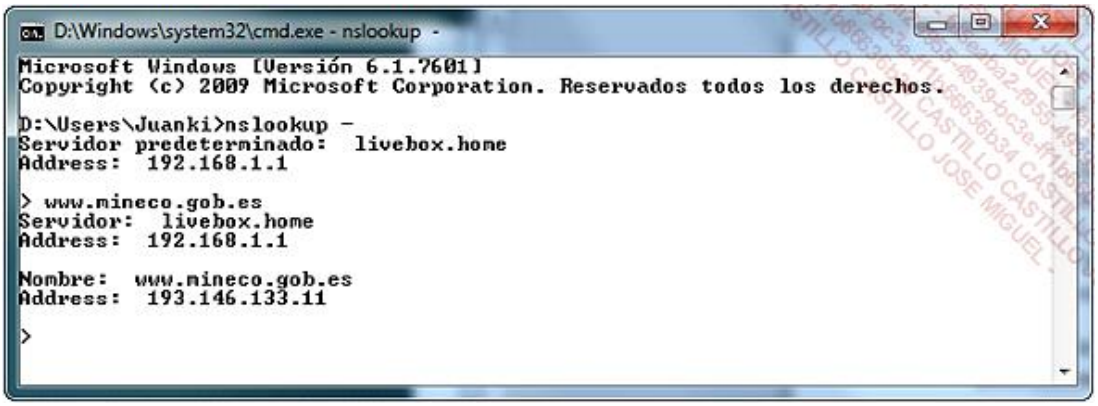
Modelo lógico

El modelo lógico es independiente de la implantación física y permite una implementación completamente distribuida a través de delegaciones y de redirecciones.



El detalle de las delegaciones realizadas al nivel del domino raíz y en favor de los dominios de primer nivel (*Top Level Domain* o TLD) está disponible en: http://www.iana.org/domains/root/db/

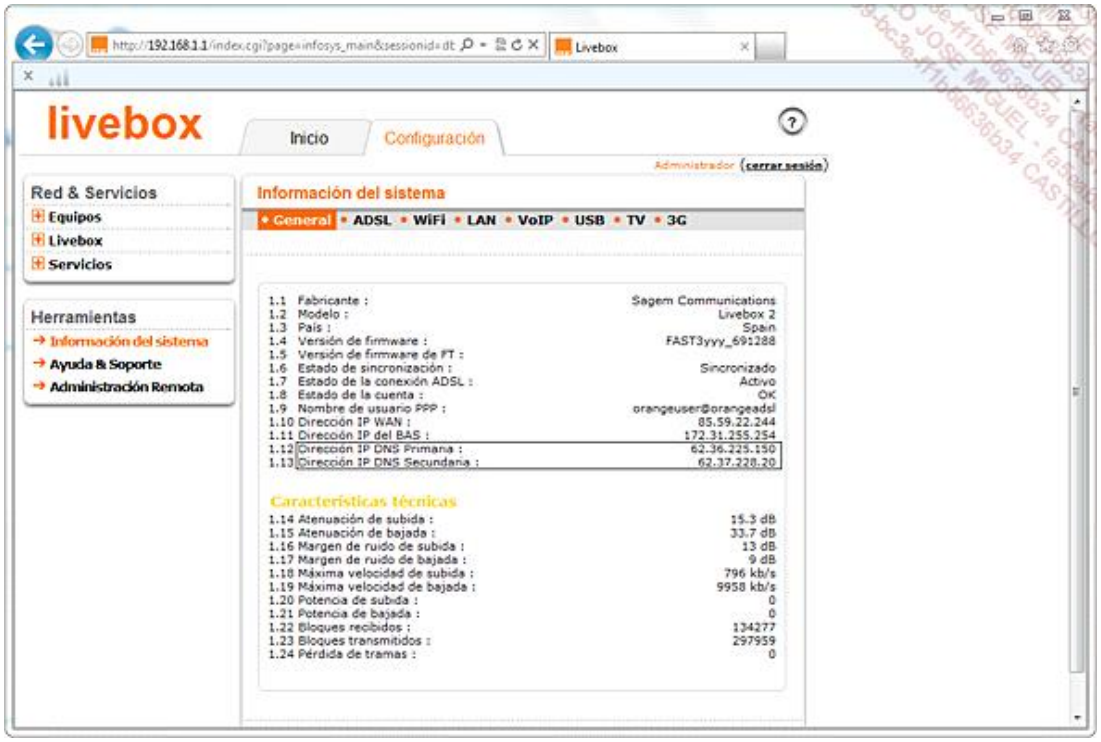
De este modo, el nombre www.mineco.gob.es corresponde a un alias DNS que resuelve en un dirección IP; en este caso se trata de 193.146.133.11.



Un alias DNS es un nombre que reenvía hacia otro nombre. A nivel DNS, se definirá como un CNAME o CANONICAL NAME.

Funcionamiento

Por ejemplo, para un particular, el ordenador obtiene una dirección IP por medio del router ADSL. Entre otras cosas, se le proporciona una dirección IP de DNS. Esta dirección IP es la dirección IP interna del router que va a actuar como proxy DNS (es decir, que va a ser cliente DNS en lugar del cliente). El router dispone igualmente de una dirección IP externa pública que conoce al menos dos direcciones IP de servidores DNS del proveedor de acceso a Internet (ISP).



Propiedad de la dirección IP pública externa de un router ADSL

De este modo, cuando el ordenador pide resolver un nombre DNS (1), como www.mineco.gob.es, el router ADSL envía esta petición al servidor del ISP (2).

El servidor DNS del ISP pregunta de inmediato a uno de los 13 servidores raíz de Internet (3), para buscar los servidores DNS que gestionan la zona **es**. El servidor raíz, que conoce el servidor que gestiona la zona es, reenvía la dirección IP del servidor DNS correspondiente.

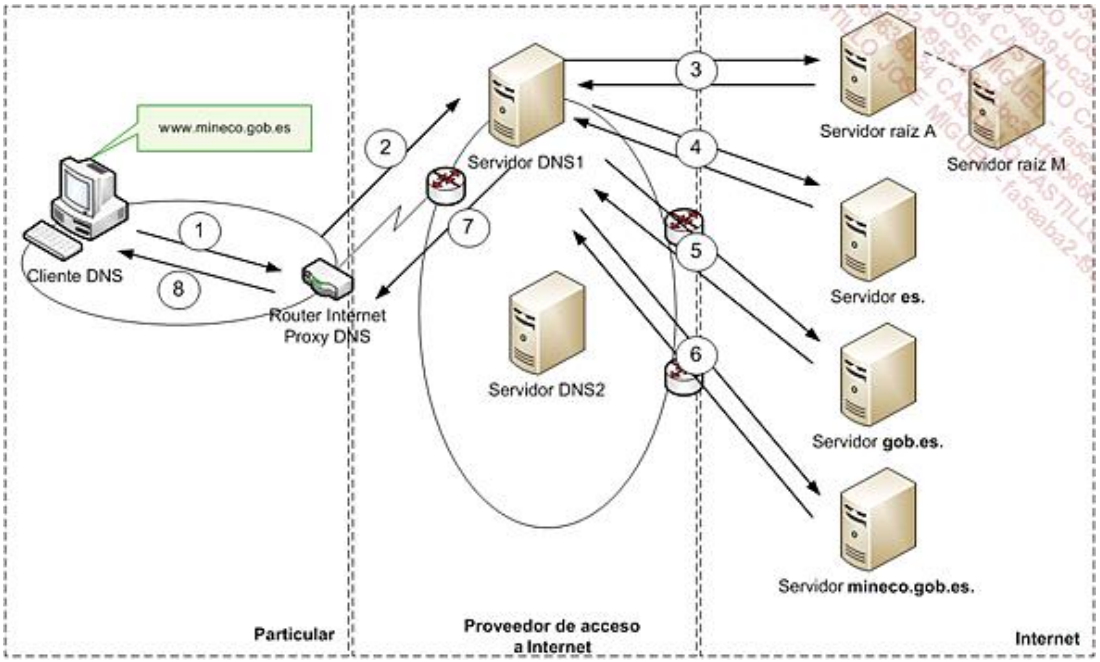
El servidor del ISP a continuación pregunta al servidor que gestiona la zona **es** (4) para encontrar quién gestiona la zona **gob.es** (5).

Y así, igualmente, hasta que se recupera la dirección IP del servidor DNS que gestiona la zona **mineco.gob.es**.

De hecho, todos los servidores disponen de una caché y puede haber un registro no autorizado (es decir, que no gestiona la zona de destino) que se haya encontrado antes de llegar al servidor autorizado.

Una vez que el servidor DNS del ISP ha obtenido la información que se le ha pedido (en este caso, la dirección IP de www.mineco.gob.es), la pone en la caché, para transmitirla al router ADSL (7).

El router reenvía finalmente la dirección del cliente DNS de la red local (8).



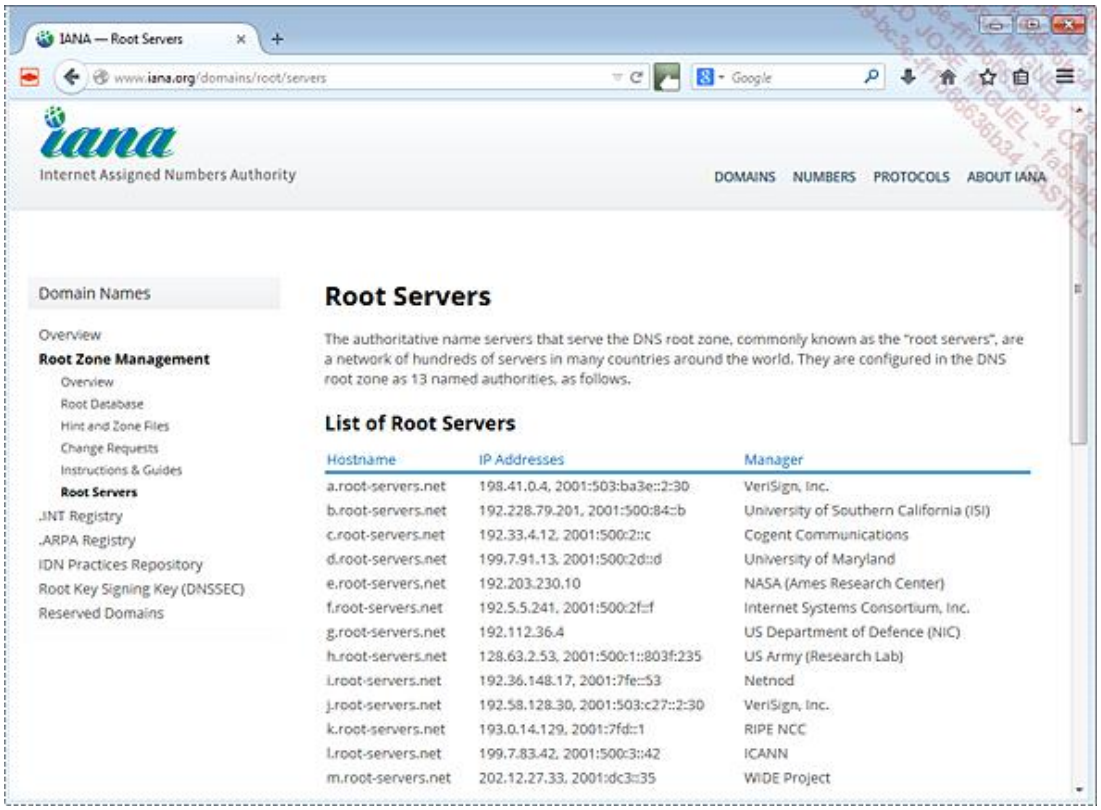
Mecanismo de resolución DNS

Existen dos tipos de peticiones: recursivas e iterativas.

Los intercambios [(1), (8)] y [(2), (7)] corresponden a peticiones recursivas.

Los intercambios (3), (4), (5) y (6) corresponden a peticiones iterativas.

Los servidores raíces que conocen todos los sufijos existentes a nivel mundial están disponibles en la URL: http://www.iana.org/domains/root/servers

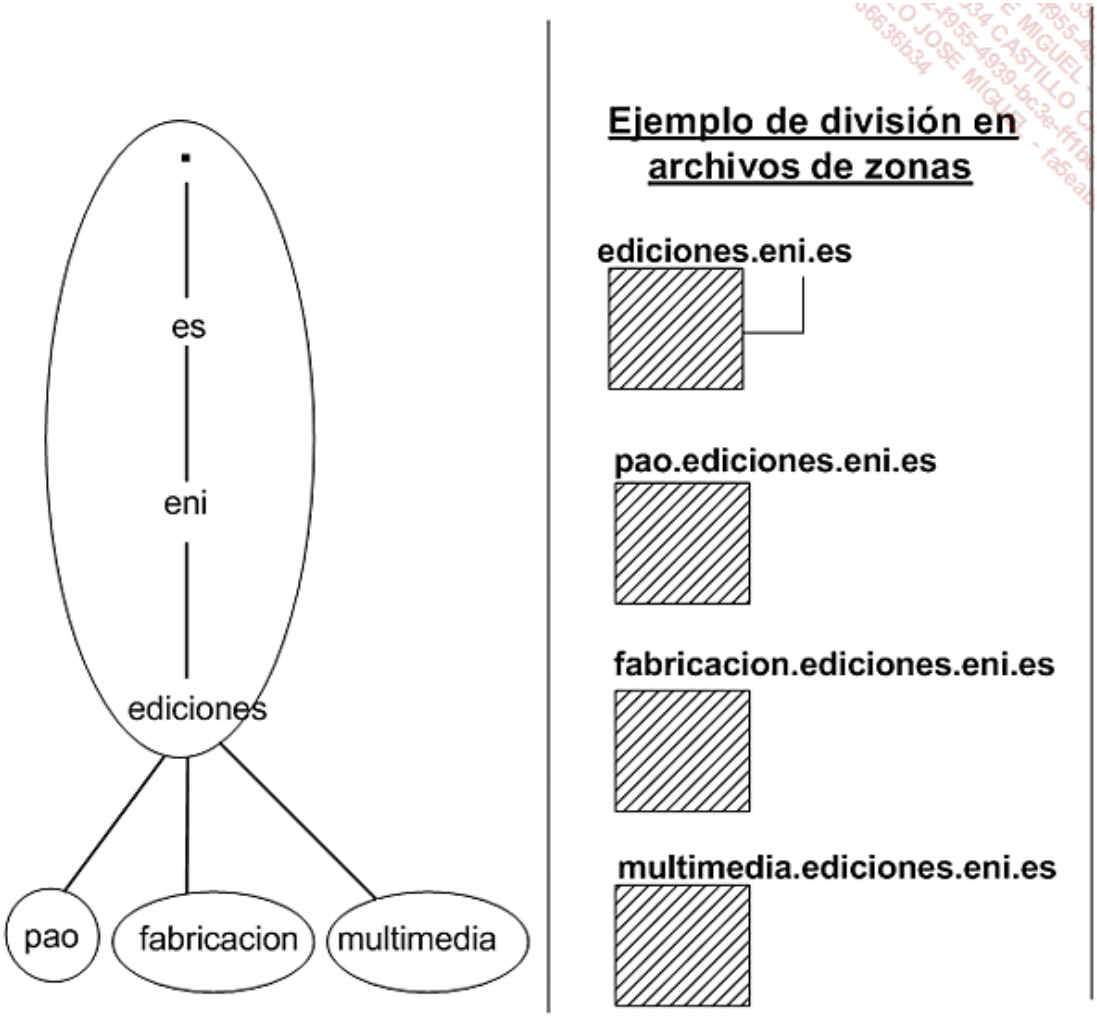


Modelo físico

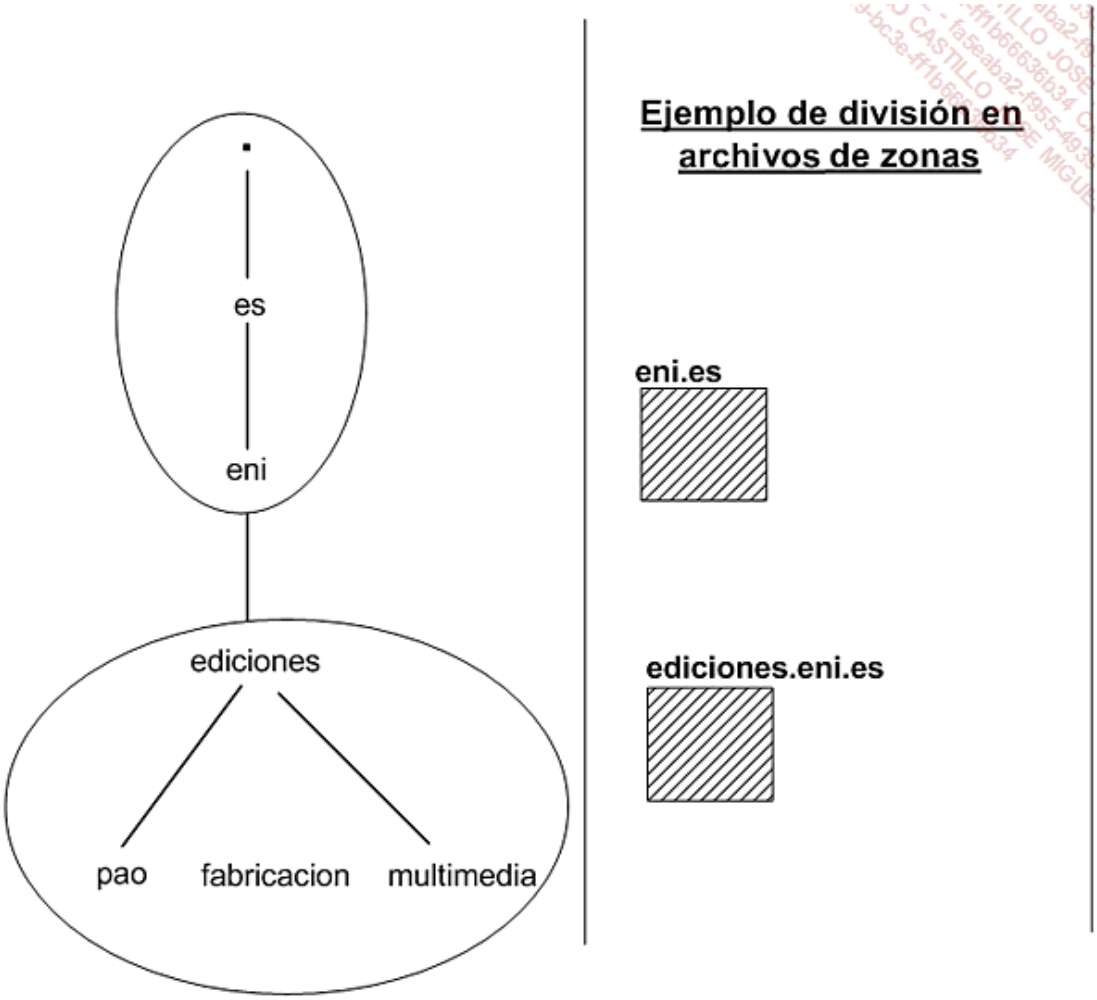
Dadas las arborescencias lógicas DNS, a continuación hay que definir la implementación física de la solución.

Se trata de definir el número de servidores físicos que se utilizarán, el número de zonas o archivos de zonas que se implementarán y la relación entre los diferentes servidores.

Una zona corresponde a un punto de anclaje de una parte de la arborescencia lógica que se materializa mediante un archivo almacenado en un servidor.



Lista de servidores raíces DNS

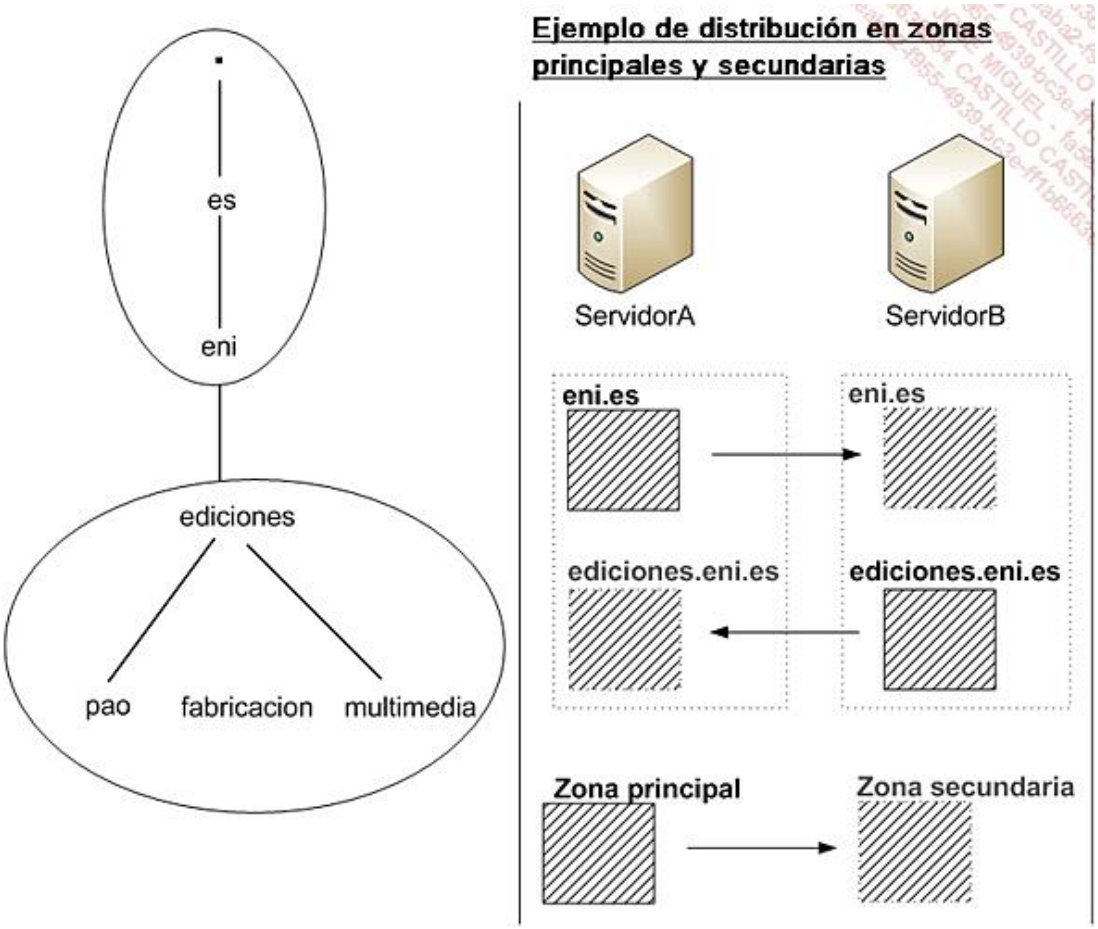


Ejemplo 2: división en zonas DNS

Servidor de nombres

Existen varios tipos de servidores de nombres. El tipo depende del origen a partir del cual el servidor obtiene su información de zona. De este modo, se hablará de **servidor DNS principal** para identificar un servidor que gestiona una zona que se puede modificar. Se calificará como **servidor secundario** aquel que gestiona una zona de solo lectura (copia de una zona principal o secundaria).

Un servidor dispondrá generalmente a la vez de zonas principales y secundarias.



Gestión de zonas principales y secundarias

Por ejemplo, en el esquema anterior, el ServidorA alberga la zona **eni.es** como zona principal. Se realiza una replicación llamada **transferencia de zona** al ServidorB para esta zona. Inversamente, el ServidorB alberga la zona **ediciones.eni.es** como zona principal. Se hace una copia de esta zona en el ServidorA como zona secundaria.

Generalmente, un servidor alberga también zonas directas, así como varias zonas indirectas (llamadas zonas inversas).

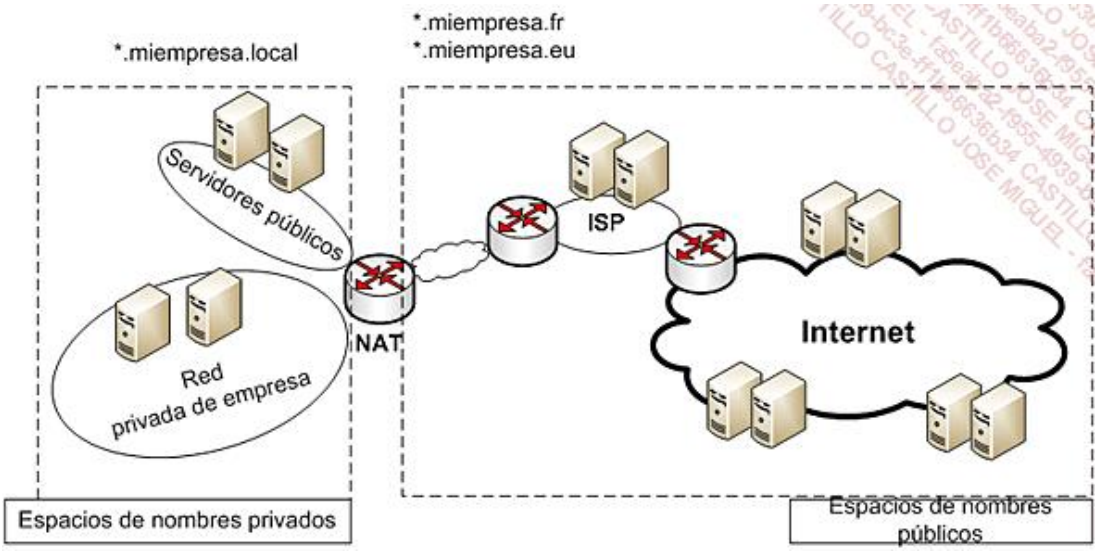
Las zonas inversas son zonas especiales que disponen de un sufijo particular predefinido, **in-addr.arpa**. Estas zonas permiten la resolución de direcciones IP en nombres.

Por ejemplo, para una red privada, se definirán zonas 10.in-addr.arpa, 172.in-addr.arpa y 192.in-addr-arpa.

Espacio de nombres privado y público

Se habla de espacios de nombres para designar los tipos de nomenclatura utilizados. De este modo, dentro de una empresa, los dispositivos y los servidores e incluso los puestos de trabajo recibirán nombres jerárquicos de acuerdo con un espacio de nombres privado. Sería ideal utilizar un sufijo que no exista en internet, por ejemplo ***.local**.

Por el contrario, para referenciar servidores que deben ser accesibles directamente desde Internet, utilizaremos sufijos oficiales, que estén reservados en Internet (por ejemplo *.es, *.eu).



Espacio de nombres públicos y privados

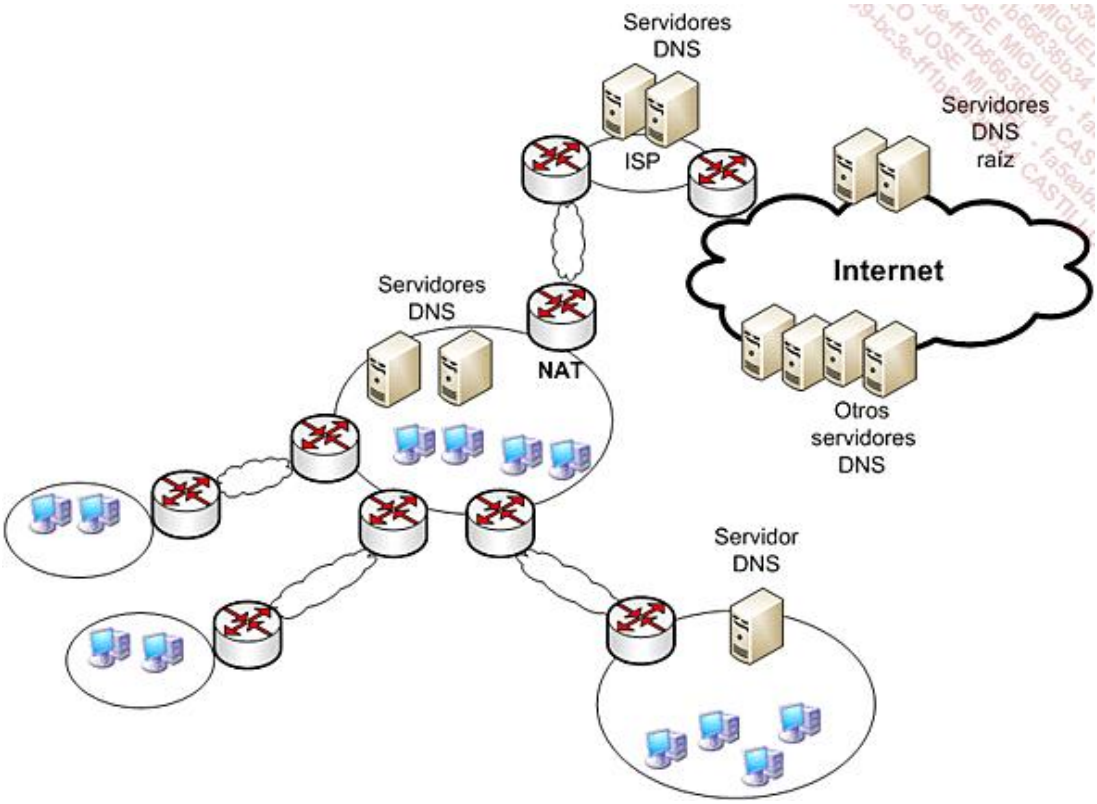
Arquitectura tipo

De manera general, la función de resolución de DNS debe estar disponible **cerca** de los clientes en términos de tiempos de respuesta. Cualquier servidor DNS integra una función de caché centralizada para los clientes. Los clientes disponen de una caché local.

Generalmente, un cliente recibe al menos dos direcciones IP de servidores DNS (para garantizar tolerancia a errores).

Lo ideal es que la configuración DNS se defina en los clientes a través de un servidor DHCP (*Dynamic Host Configuration Protocol*).

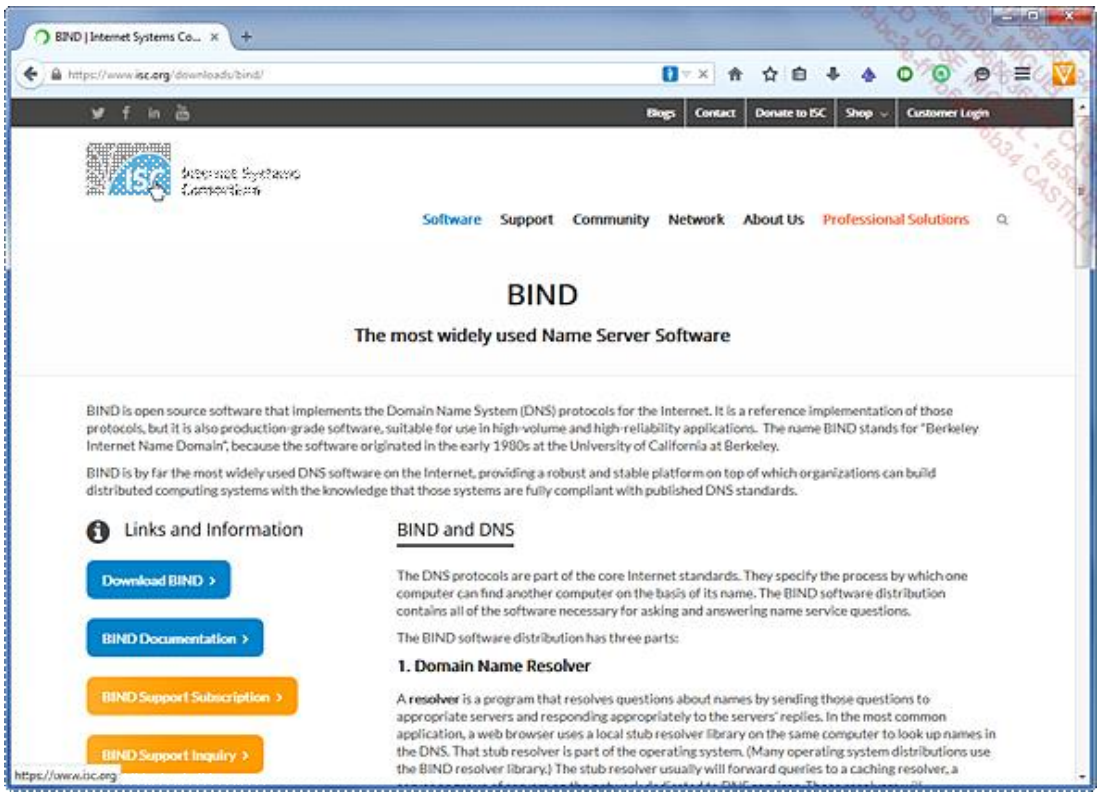
Para los servidores, la configuración DNS se realiza sobre todo manualmente, a menos que en el sistema se hayan hecho reservas DHCP para los servidores.



Arquitectura DNS

Implementaciones

Las principales implementaciones DNS son el software BIND del ISC (*Berkeley Name Domain* del *Internet Systems Consortium*, al que se puede acceder en https://www.isc.org/software/bind) y el servicio DNS de Microsoft proporcionado por los sistemas operativos de servidor.



Página de descarga BIND ISC

b. Dynamic Host Configuration Protocol v.4 (DHCPv4)

Introducción

Históricamente, el servicio DHCP apareció en 1993 como una extensión del protocolo BOOTP creado en 1985. El objetivo de BOOTP es iniciar una estación de trabajo sin disco. La configuración desplegada es personalizable basándose en la dirección MAC de la máquina y asociándole una dirección IP (se habla así de *Reverse Address Resolution Protocol*).

En efecto, el protocolo TCP/IP que se ha impuesto después de muchos años tiene una gran inconveniente: necesita definir para cada uno de los dispositivos como mínimo una dirección IP, una máscara, así como ocasionales parámetros complementarios.

El servicio DHCP permite definir de manera centralizada una configuración TCP/IP completa para el conjunto de los dispositivos de red (parámetros dinámicos o estáticos).

Diferentes RFC definen BOOTP y DHCP:

- RFC 951: BOOTP
- RFC 1497: opciones BOOTP vendor extensions
- RFC 1541: definición del protocolo DHCP
- RFC 1542: interacción entre BOOTP y DHCP
- RFC 2131: DHCP
- RFC 2132: complemento a las opciones DHCP y BOOTP vendor extensions

Puede consultar estas RFC en http://www.ietf.org/rfc/

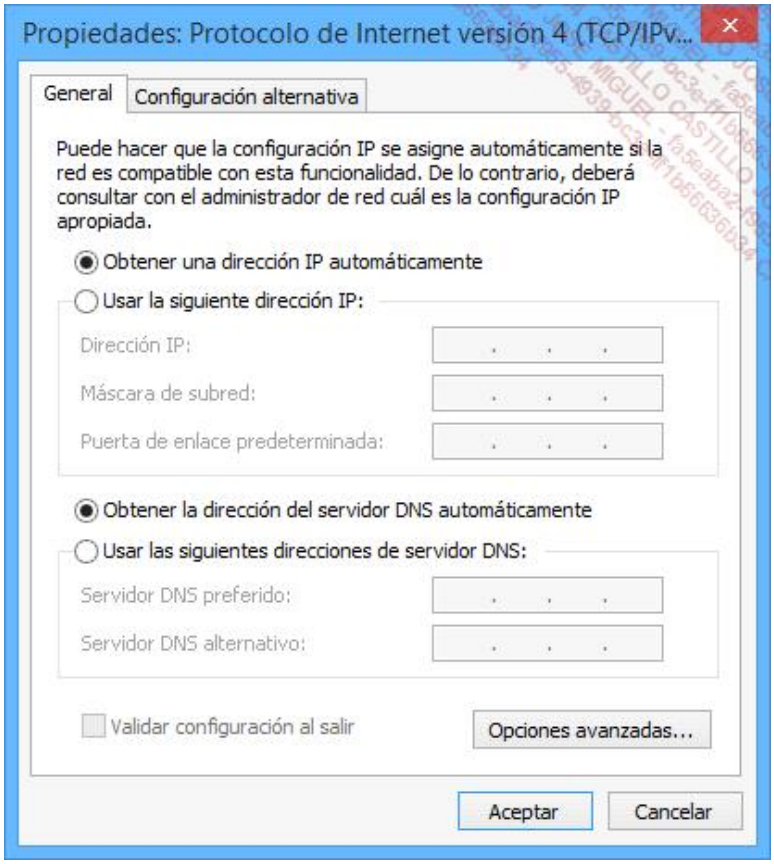
Funcionamiento en una pequeña red

Un dispositivo, un puesto de trabajo, un teléfono IP, un lector de código de barras Wi-Fi, una impresora de red, etc., ejecutan un componente cliente DHCP que les permite comunicarse con un servidor para obtener un conjunto de parámetros TCP/IP.

Se utiliza cada vez más a menudo una reserva de dirección IP asociada a una dirección MAC. Este mecanismo permite disponer de IP fijas conservando flexibilidad de gestión al definir los ordenadores como clientes DHCP.

En general, el dispositivo se configura por defecto para utilizar un servidor DHCP.

Por ejemplo, en Windows:



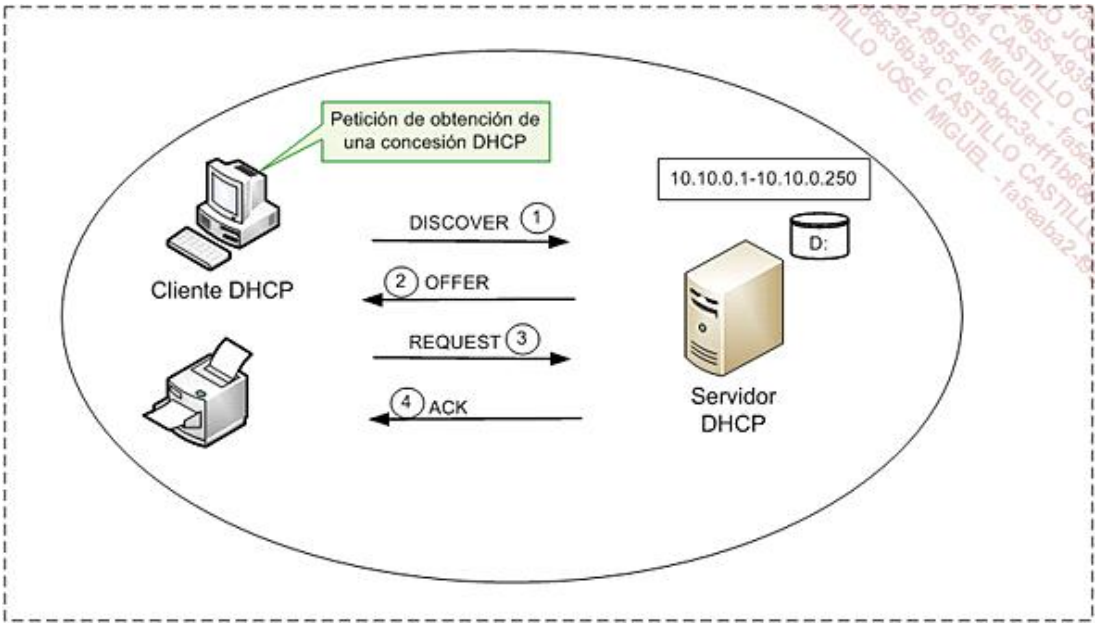
Configuración DHCP en Windows 8.1

O en Linux:

Configuración DHCP en CentOS 7

Al arrancar la primera vez, la comunicación que permite obtener la configuración se desarrolla en varias etapas:

- (1) DHCP DISCOVER: el descubrimiento de la red.
- (2) DHCP OFFER: la propuesta de parámetros por parte de uno o varios servidores.
- (3) DHCP REQUEST: la respuesta favorable del cliente a una de las propuestas.
- (4) DHCP ACK: el acuse de recibo por el servidor teniendo en cuenta la petición del cliente.

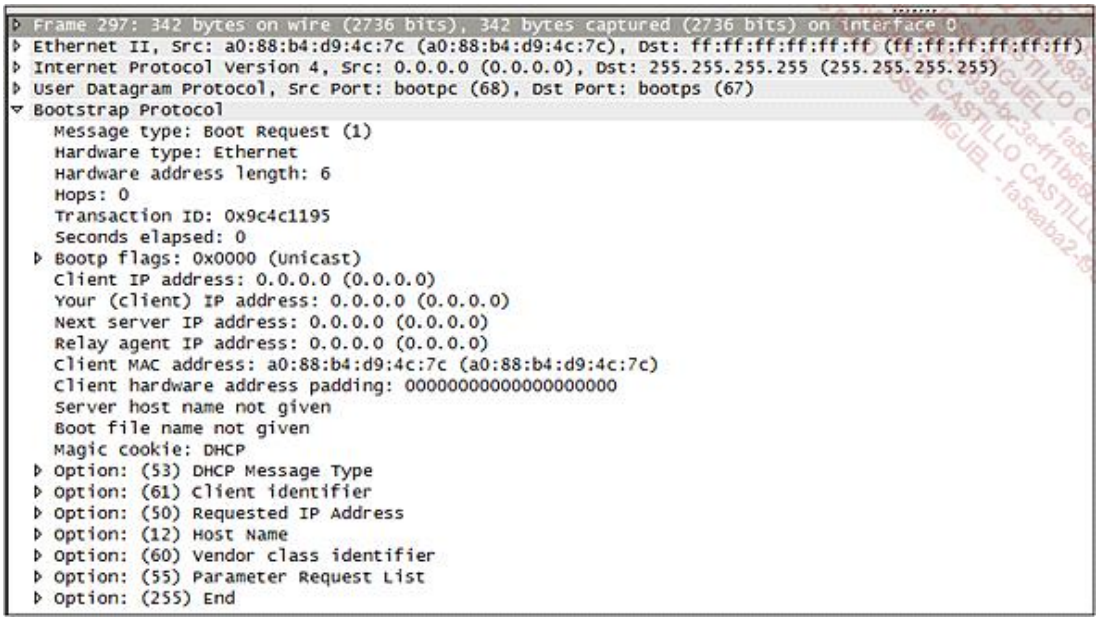


Funcionamiento de DHCP

DHCP DISCOVER

El protocolo TCP/IP se inicializa con una versión limitada (dirección IP no definida: 0.0.0.0).

Transmite en el nivel 2 a todos los ordenadores (FF.FF.FF.FF.FF.FF) una petición para obtener una concesión DHCP. Como se trata de un protocolo UDP, la dirección IP debe ser emitida por el destino. Se define como 255.255.255.255 (todo el mundo).



Análisis de una trama DHCP DISCOVER

Capa	Origen (cliente)	Destino (todo el mundo)
UDP	68	67
IP	0.0.0.0	255.255.255.255
Ethernet	a0:88:b4:d9:4c:7c	ff:ff:ff:ff:ff:ff

Si al cabo de un segundo el cliente no ha recibido ninguna respuesta, se transmite una nueva petición al cabo de 9, 13 y 16 segundos.

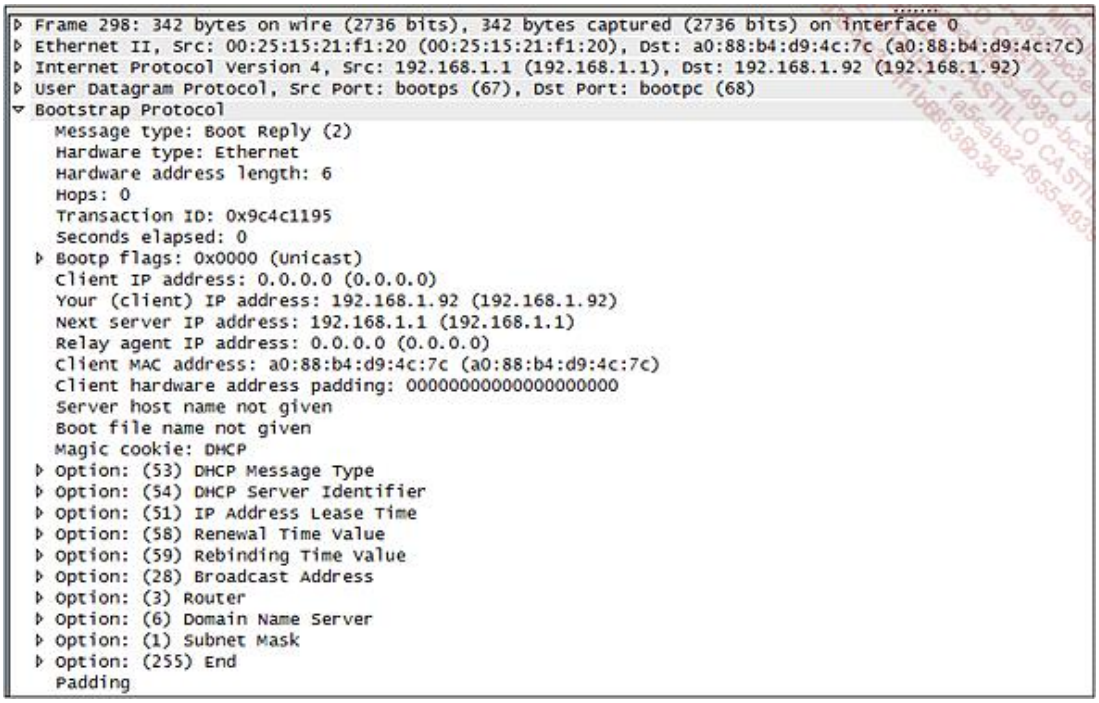
Después de estos intentos, se hará una petición cada cinco minutos.

DHCP OFFER

Algunos dispositivos que actúan como servidor DHCP (servidor, router, router ADSL) responden al cliente.

Transmiten una propuesta que tiene la siguiente información: la dirección MAC del cliente, una dirección IP, una máscara de subred, la duración de la concesión y su dirección IP.

Capa	Origen (servidor)	Destino (cliente)
UDP	67	68
IP	192.168.1.1	192.168.1.92
Ethernet	00:25:15:21:f1:20	a0:88:b4:d9:4c:7c



Análisis de una trama DHCP OFFER

El cliente selecciona una propuesta (en general, la primera que recibe).

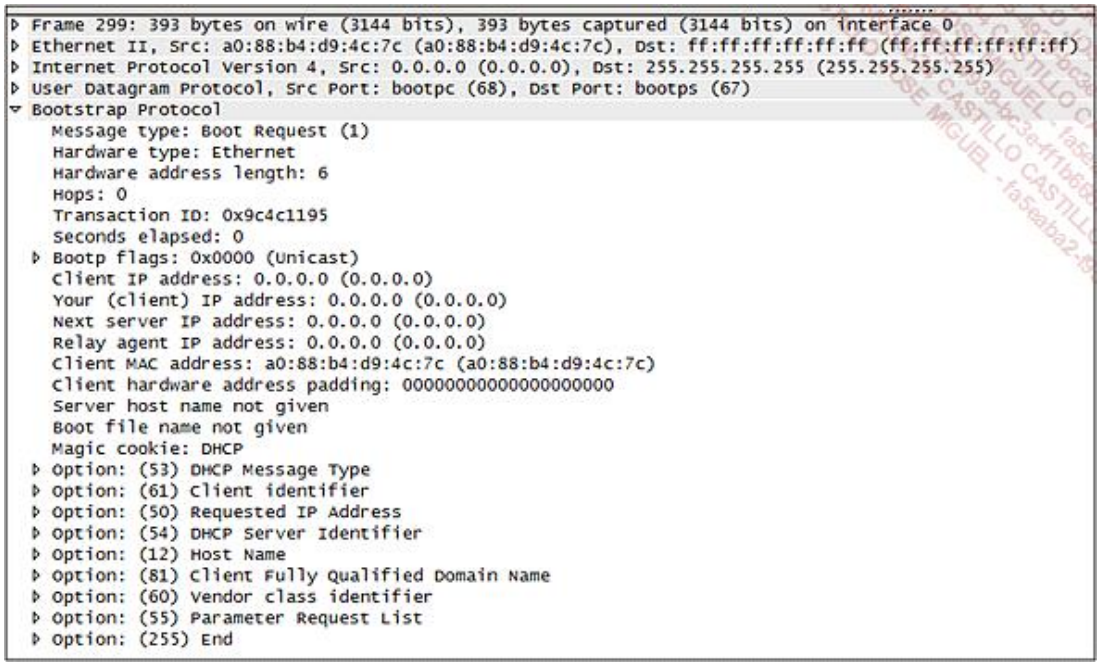
Tenga en cuenta que, después de la RFC, el servidor intenta primero un *unicast* (para encargarse de una eventual transmisión DHCP) antes de hacer una difusión.

DHCP REQUEST

Esta respuesta permite al cliente avisar a todos los servidores que se ha captado una concesión. La información relativa a la concesión está disponible al final de la trama.

Así, el resto de los servidores pueden retirar su propuesta y dejar disponible la dirección que se había reservado.

Capa	Origen (cliente)	Destino (todo el mundo)
UDP	68	67
IP	0.0.0.0	255.255.255.255
Ethernet	a0:88:b4:d9:4c:7c	ff:ff:ff:ff:ff:ff

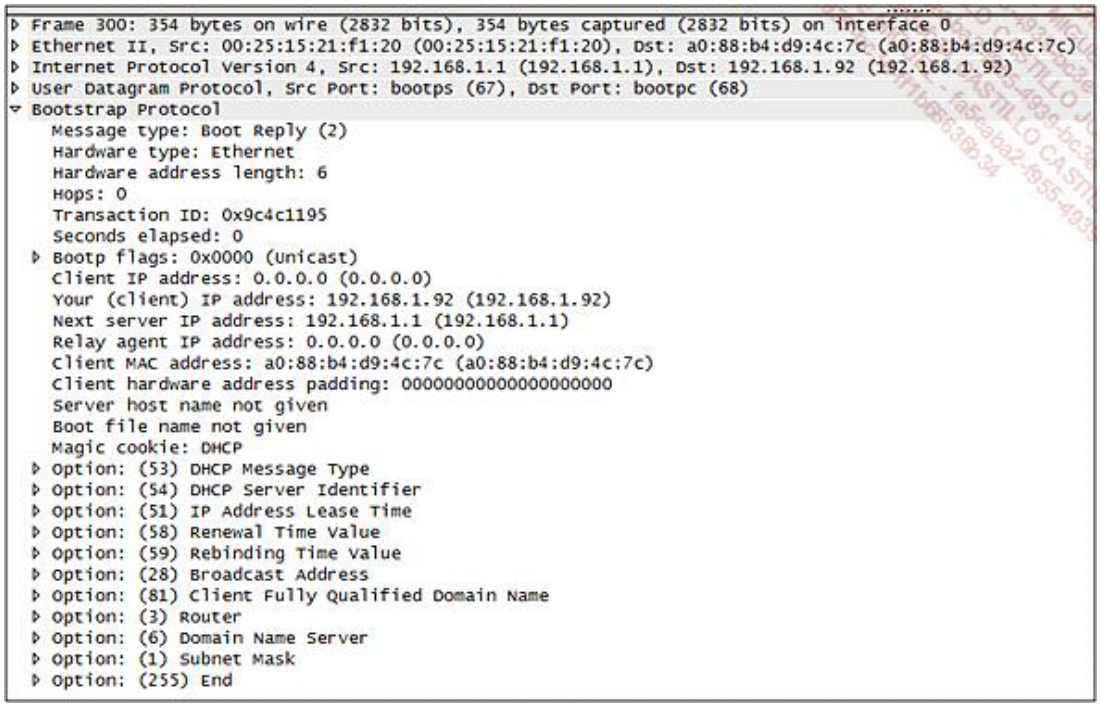


Análisis de una trama DHCP REQUEST

DHCP ACK

El servidor cuya propuesta ha sido aceptada envía una trama dirigida directamente al cliente como acuse de recibo. Se añaden otras opciones a la trama (opción 003 router, 006 Domain Name Server, 001 Subnet Mask).

Capa	Origen (servidor)	Destino (cliente)
UDP	67	68
IP	192.168.1.1	192.168.1.92
Ethernet	00:25:15:21:f1:20	a0:88:b4:d9:4c:7c



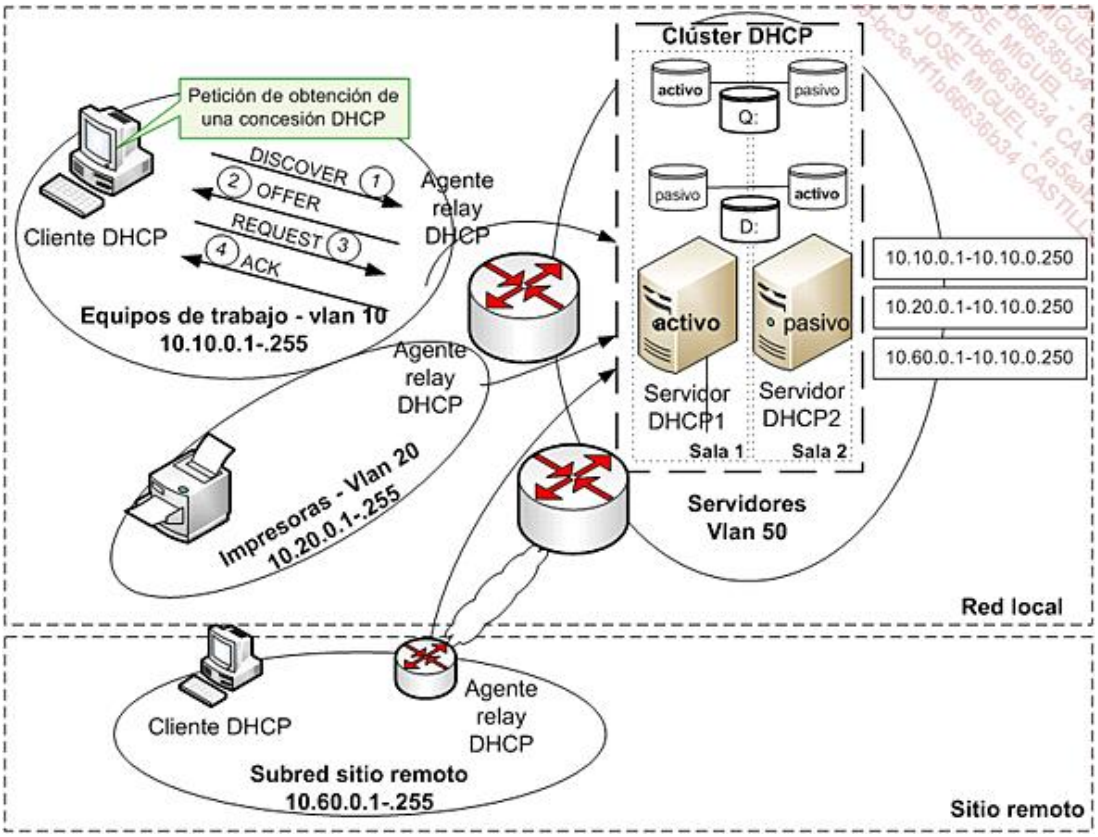
Tenga en cuenta que, en algunas implementaciones de DHCP, el ACK se puede realizar con una difusión.

Funcionamiento en una gran red

En un entorno más grande, la arquitectura es un poco más compleja. Por una parte, las subredes IP están generalmente asociadas a una descomposición en VLAN. Así, se va a asignar una VLAN por tipo de dispositivos (estación de trabajo, servidor, lector de códigos de barras) o por uso (red principal, copias de seguridad, administración de servidores).

Por otra parte, como los clientes están generalmente en subredes diferentes que los servidores DHCP, conviene implementar un mecanismo que permita transmitir las tramas DHCP a o desde los servidores DHCP designados. De hecho, los routers detienen las tramas de difusión.

El comando asociado generalmente a los routers es «ip-helper-address». Permite designar explícitamente uno o varios servidores DHCP hacia el que se transmitirá una difusión DHCP captada en la red local.



Funcionamiento DHCP en un entorno enrutado

En un entorno consecuente, el núcleo de la red está constituido generalmente por un conmutador multinivel que conoce todas las VLAN. Cada una de las interfases que corresponden a la puerta de enlace por defecto conoce la existencia del servidor al que va a redirigir las difusiones DHCP.

Clúster DHCP

El servidor DHCP se podrá ayudar de un clúster que va a ofrecer redundancia del servicio, al mismo tiempo que

redundancia de los datos:

- Un disco D: contiene la configuración del servidor DHCP cuyo servicio se ejecuta en uno de los dos servidores. El servicio DHCP del otro servidor está en *standby*.
- Un disco Q corresponde al quórum. Almacena la información de actual del clúster. En caso de problemas, el servidor que puede acceder al quórum se hace cargo.

Los recursos de disco se replican en segundo plano en modo síncrono, para permitir una recuperación en caso de fallo de un disco o de la pérdida de una sala.

La dirección IP que referencia el servicio DHCP es de hecho una dirección IP virtual, que corresponde a un recurso del clúster. Este recurso se ejecuta efectivamente en uno de los nodos del clúster.

DHCP Failover

Esta funcionalidad permite asegurar la continuidad del servicio DHCP sin necesitar un clúster para bascular. De hecho, Windows Server 2012 o ISC DHCP ofrece esta funcionalidad. De este modo, los servidores son capaces de intercambiar su información.

Agente relay DHCP

La utilización de agentes relay introduce un funcionamiento complementario.

Cuando la puerta de enlace recibe una trama DHCP que proviene de un cliente de su subred, el router transmite la trama dirigida directamente al servidor DHCP. Si la dirección IP origen identificada es 0.0.0.0, el router la sustituye por su propia dirección IP de puerta de enlace. De hecho, el servidor DHCP debe poder identificar el área de alcance DHCP para asignar una dirección IP válida al cliente.

El servidor DHCP recibe entonces la petición y examina la dirección IP de origen para asociar un rango de dirección IP adecuado.

Selecciona finalmente una dirección IP disponible para enviar una propuesta directamente a la puerta de enlace. La puerta de enlace finalmente va a transmitir la propuesta a la subred local (al destino del puesto de trabajo que hace la petición en el nivel 2 y de todo el mundo en el nivel 3).

A continuación, el router transmite el mensaje DHCP REQUEST al servidor DHCP.

Finalmente, el servidor responde un DHCP ACK al cliente.

Renovación de la concesión

El cliente obtiene los parámetros TPC/IP para una duración limitada: la concesión.

Esta concesión se debe renovar regularmente para permitir al cliente seguir utilizando sus parámetros.

La renovación se produce después de que expire la mitad de la concesión. Si la petición no obtiene resultados, se realiza un nuevo intento a 7/8 de la duración de la concesión.


Este mecanismo de renovación evita generar tráfico de difusión inútil.

Cuando un equipo arranca, se repite el proceso completo; esto permite tener en cuenta los desplazamientos de los

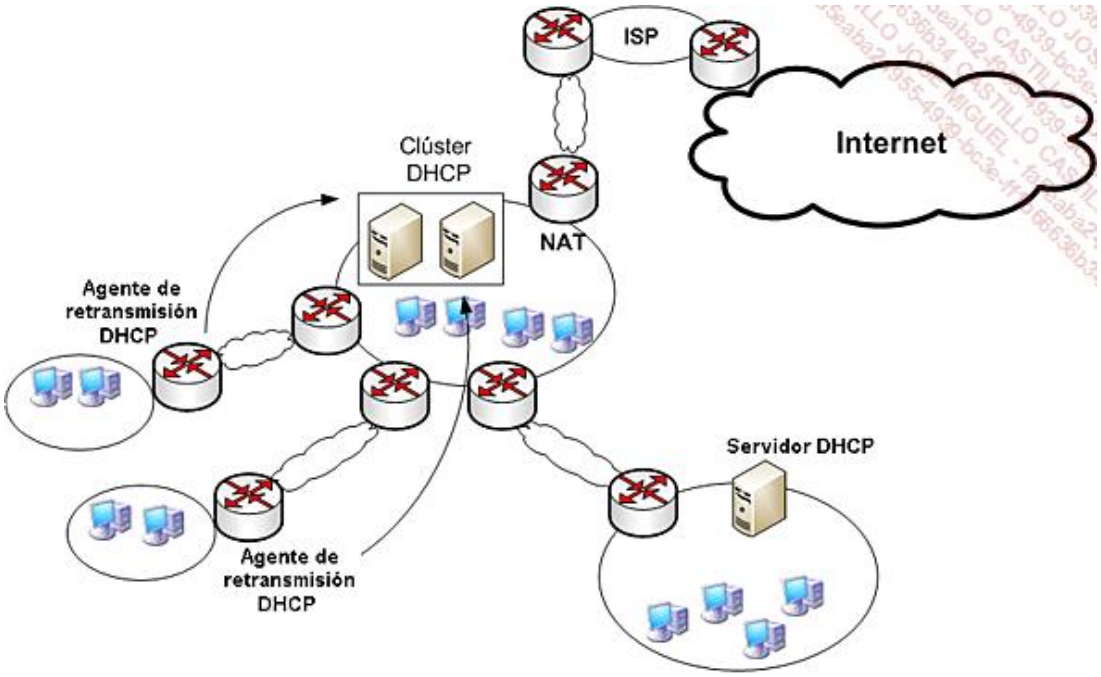
ordenadores portátiles.

El servidor también puede pedir al cliente que libere su dirección dirigiéndole un DHCP NACK.

Arquitectura tipo

Una arquitectura tipo implementa generalmente un servidor centralizado para el conjunto de la red. Por lo común, para tener en cuenta las posibles interrupciones de conexiones remotas, se configuran las concesiones para una duración lo suficientemente larga.

Igualmente es posible centralizar de forma completa la gestión de direcciones IP fijas definiendo reservas explícitas para elementos concretos (impresores, servidores).



Arquitectura DHCP estándar

Implementaciones

Entre las implementaciones existentes, encontramos aquellas integradas con los sistemas operativos de servidor:

- Microsoft DHCP.
- Internet Systems Consortium DHCP: http://www.isc.org/downloads/dhcp

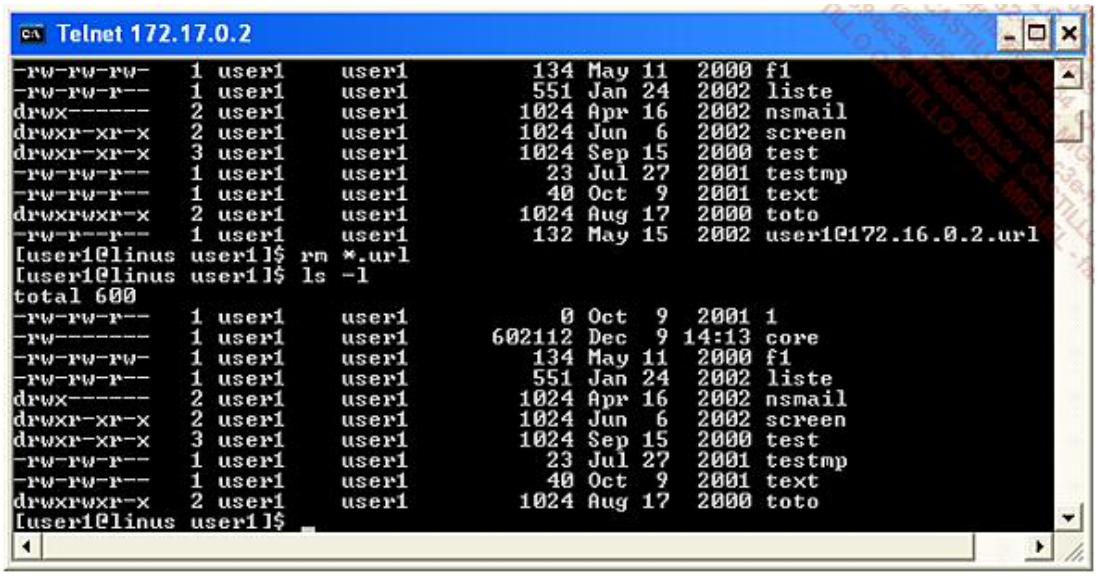
Encontramos también otras implementaciones:

- Alcatel-Lucent VitalQIP (DNS/DHCP): http://www.alcatel-lucent.com/vitalqip
- Cisco Network Registrar (DNS/DHCP) : http://www.cisco.com/

c. Telnet

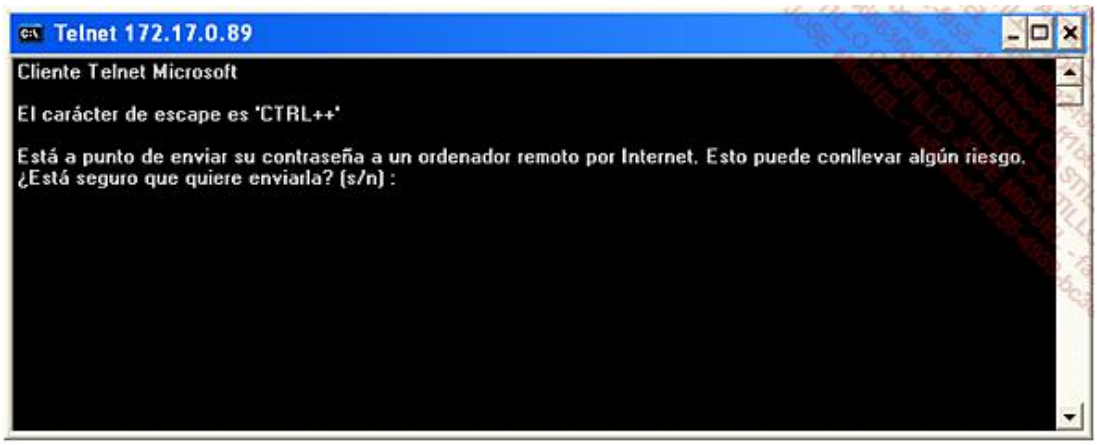
Telnet es un protocolo de emulación de terminal. Establece una sesión entre una estación de trabajo (cliente

Telnet) y una máquina remota (servidor Telnet). Se transmite cualquier comando escrito por el cliente y se ejecuta en el servidor Telnet. El eco del proceso remoto se redirige a la estación de trabajo, que ve el resultado del comando. Telnet debe conocer los comandos del sistema operativo remoto.



Este servicio utiliza el puerto TCP 23.

Los servidores (Windows, Linux...) u otros componentes administrables a distancia (conmutadores, routers...) pueden disponer de un servicio Telnet.



Por razones de seguridad, este servicio suele estar desactivado de manera predeterminada. Al tratarse de un protocolo antiguo, no es muy seguro. Por ejemplo, la contraseña se comunica de manera transparente. El protocolo SSH (*Secure Shell*) es equivalente, pero bastante más fiable a este nivel.

d. Network Time Protocol (NTP)

Introducción

El protocolo NTP o protocolo de sincronización de relojes de ordenadores en red fue propuesto en 1985 por el profesor David Mills de la Universidad de Delaware.

Han ido apareciendo diferentes versiones:

- v1, en 1988, RFC 1059.
- v2, en 1989, RFC 1199.
- v3, en 1992, RFC 1305.
- v4, en 2010, RFC 5905.

Jerarquía NTP

Al más alto nivel de organización, tenemos los relojes atómicos, que sirven de referencia a nivel mundial.

Se puede consultar la hora de estos relojes, ya sea a través de receptores que recuperan la hora atómica por diferentes medios (satélite, radio, cable), ya sea a través de servidores ubicados en el primer nivel de la jerarquía. Se habla de **capa 1** (o *stratum* 1) para designar los **servidores primarios**.

Los servidores de hora de nivel inferior serán los de **capa 2** y se dirigen a los servidores de capa 1. A partir de este nivel 2, se habla de **servidores secundarios**.

La norma prevé un máximo de 16 capas.

En general, los clientes se sitúan en los niveles 3 o 4.

A nivel mundial, la jerarquía se define a nivel de continentes, y a continuación de países.

De este modo, a nivel mundial, el nombre **pool.ntp.org** identifica un pool de servidores.

A nivel de continentes, se definen los siguientes nombres:

Continente	Nombre
Asia	asia.pool.ntp.org
Europa	europe.pool.ntp.org
América del Norte	north-america.pool.ntp.org
Oceanía	oceania.pool.ntp.org
América del Sur	south-america.pool.ntp.org

Luego, dependiendo de cada país, hay servidores NTP disponibles.

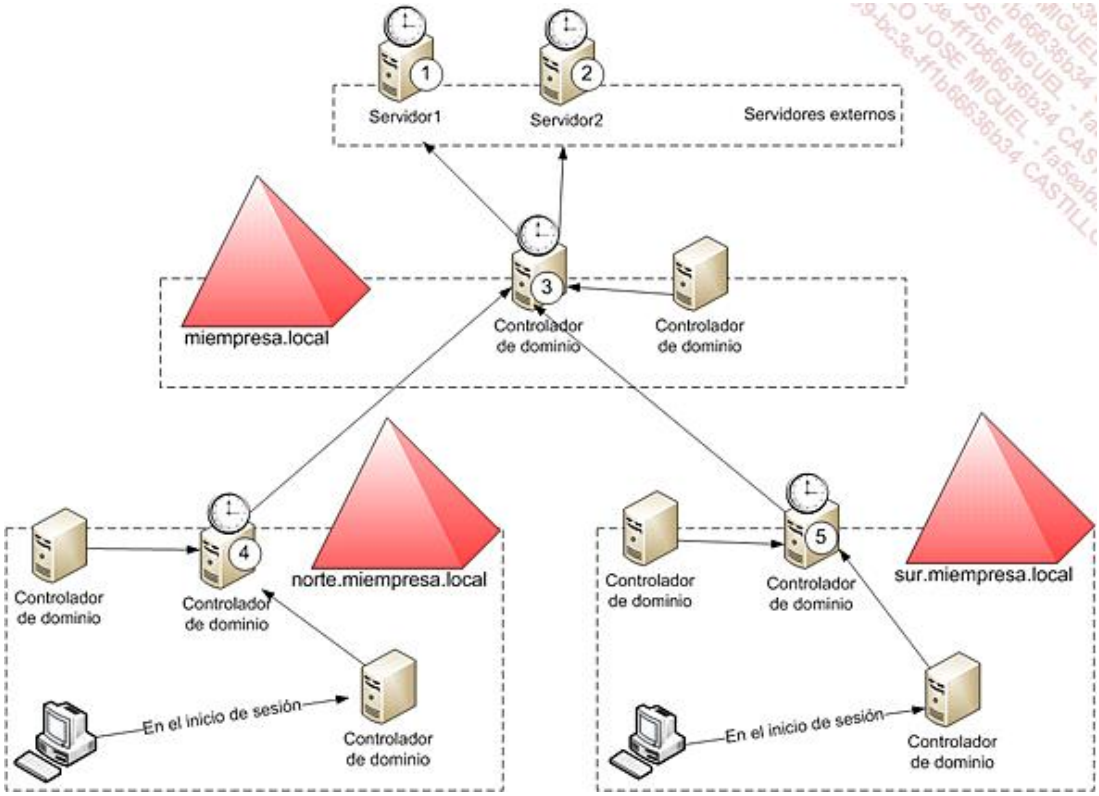
En la URL http://www.rediris.es/ntp/drafts/ hay una lista de servidores NTP españoles de diferentes capas.

Funcionamiento en un dominio Microsoft

Cuando los ordenadores están conectados a un entorno de dominio Active Directory Microsoft (directorio LDAP), el mecanismo de sincronización NTP está asegurado por defecto, sin tener que configurar los ordenadores individualmente.

De hecho, cuando se utiliza la autenticación Kerberos, es indispensable que los ordenadores estén correctamente sincronizados, ya que la autorización de acceso se da a través de testigos válidos para una duración determinada, basados en las horas de los ordenadores.

Los equipos de trabajo sincronizan su reloj en el momento de inicio de sesión con el servidor (llamado «controlador de dominio») que valida su petición.



Sincronización de ordenadores en un dominio Active Directory de Microsoft

Los controladores de dominio, a su vez, se tienen que sincronizar con el servidor, que tiene un papel que permite especialmente servir de referencia temporal: servidores (4) y (5).

A continuación, el dominio se puede organizar en diferentes niveles: se hablará de dominios hijo y de dominio raíz.

Los controladores de dominio que proporcionan hora a los equipos de trabajo de los dominios hijo (norte y sur) se tienen que sincronizar a su vez con el controlador de dominio raíz que tiene el papel de servir de referencia temporal: (3).

Por último, el servidor de referencia interno se tiene que sincronizar también con servidores externos: (1) y (2).

e. Simple Network Management Protocol (SNMP)

Introducción

Dada la complejidad de un entorno informático en red, es necesario poder supervisar y gestionar de forma centralizada tanto los componentes de hardware, conmutadores, routers, como los componentes de software, bases de datos, servidores web, servicios de red.

Este desafío, extremadamente ambicioso, es posible a condición de utilizar protocolos normalizados, como SNMP.

Lo que está en juego es importante para la empresa, pero los costes asociados a una solución de este tipo suelen ser elevados. Deben ser acordes con los riesgos de pérdida de actividad y los costes generales por una indisponibilidad del servicio.

SNMP o *Simple Network Management Protocol* es un protocolo elemental que asegura el transporte entre los equipos supervisados y administrados y la consola de administración o supervisión.

El protocolo SNMP se basa en UDP y utiliza los puertos 161 y 162.

Ha evolucionado, y actualmente ofrece su versión 3, que es más segura que las anteriores, en las que la contraseña se intercambiaba sin cifrar en las tramas de red.

Se han publicado diferentes RFC a medida que han evolucionado las versiones de SNMP. Las principales RFC son: RFC 1155 (SNMPv1), RFC 1901 (SNMPv2) y RFC 3411 (SNMPv3).

Funcionamiento

En un entorno SNMP, en los equipos supervisados están disponibles los servicios integrados. Se les llama «agentes SNMP». Permiten interactuar con el supervisor SNMP para responder a las peticiones de información (acceso de lectura) o a peticiones de actualización de configuración (acceso de escritura).

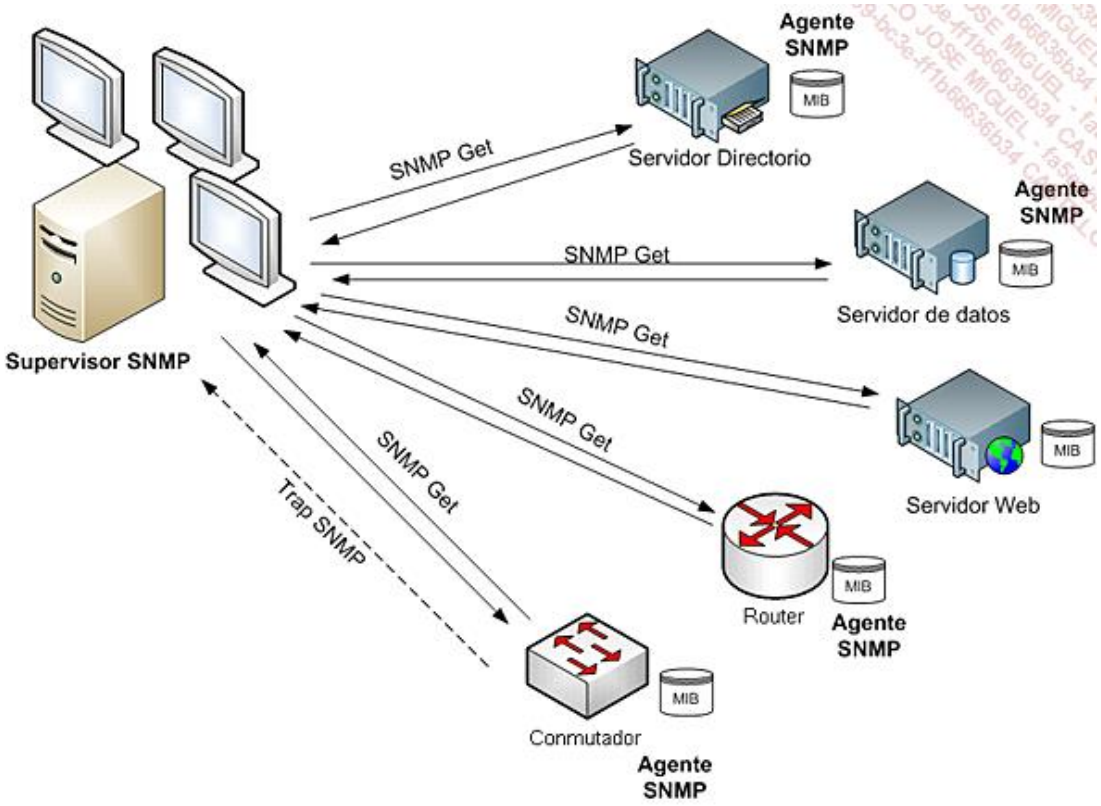
La compartimentación SNMP existe a través de comunidades que permiten definir un espacio de trabajo común; por ejemplo, la comunidad por defecto «privada» permite autorizar el acceso de escritura a los agentes, mientras que la comunidad por defecto «pública» autoriza solo acceso de lectura.

Otro mecanismo inherente a SNMP es la alerta SNMP o «trampa», que permite programar un agente para enviar un mensaje en caso de que se supere algún límite: ancho de banda WAN saturado, servicio a punto de saturarse, vínculo WAN roto, memoria o espacio en disco saturados de un servidor en concreto.

En general, el supervisor permite mostrar de forma gráfica un estado del entorno con colores que permiten identificar rápidamente cualquier anomalía.

Este mecanismo de supervisión normalmente está junto a un mecanismo de detección automática del entorno.

Además de la recogida de información, existe también un mecanismo de *polling* que permite testar la presencia de IP «sensibles» en la infraestructura (routers, servidores concretos).

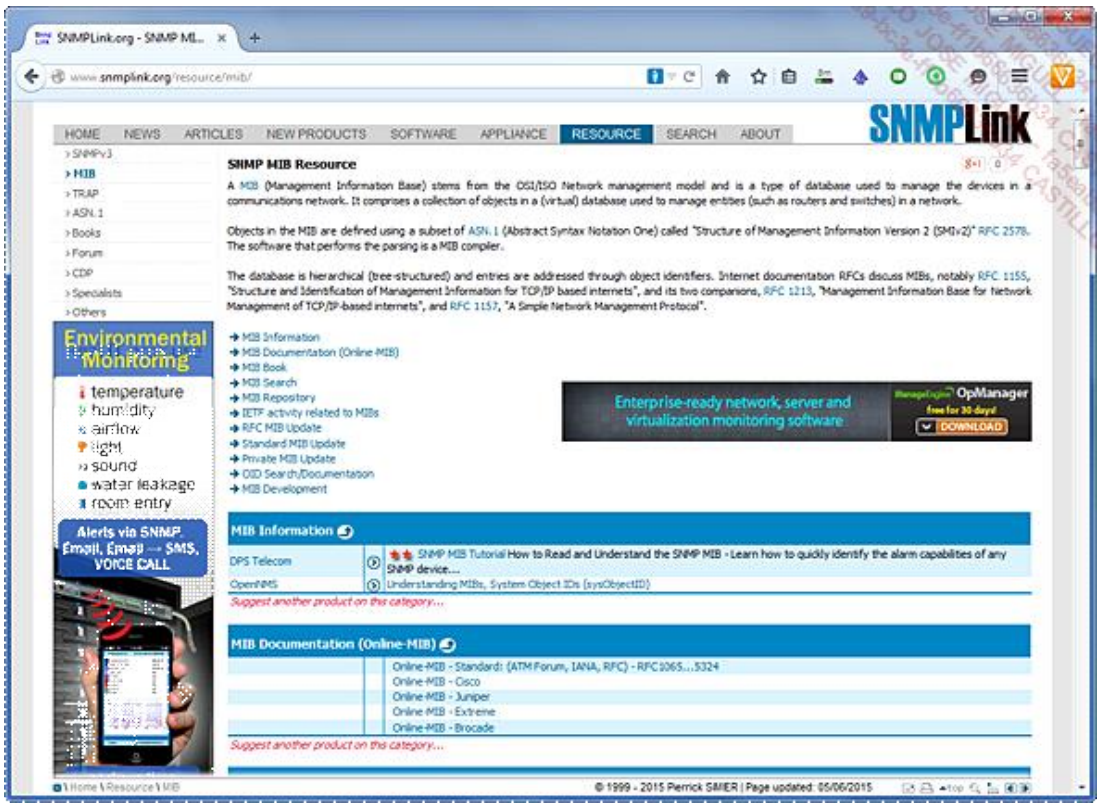


Comunicaciones SNMP supervisor - agentes

Organización de los datos SNMP

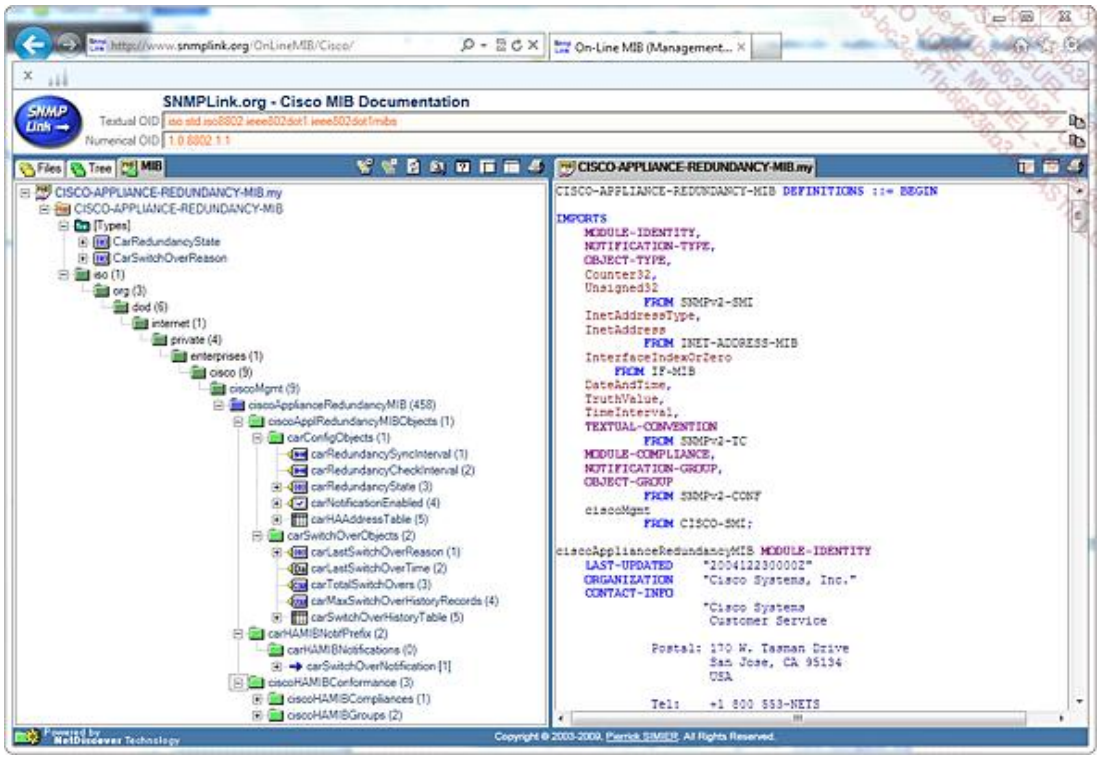
Los agentes SNMP disponen de parámetros de configuración, de estadísticas de rendimiento, de información de hardware o de software, que se organiza en una base de datos jerárquica llamada MIB (*Management Information Base*). La última versión es la MIB II.

Algunos sitios ofrecen herramientas para navegar por las MIB con objeto de buscar contadores específicos:



Obtención de información de SNMP en general: www.snmplink.org

Así, es posible identificar claramente los contadores disponibles:



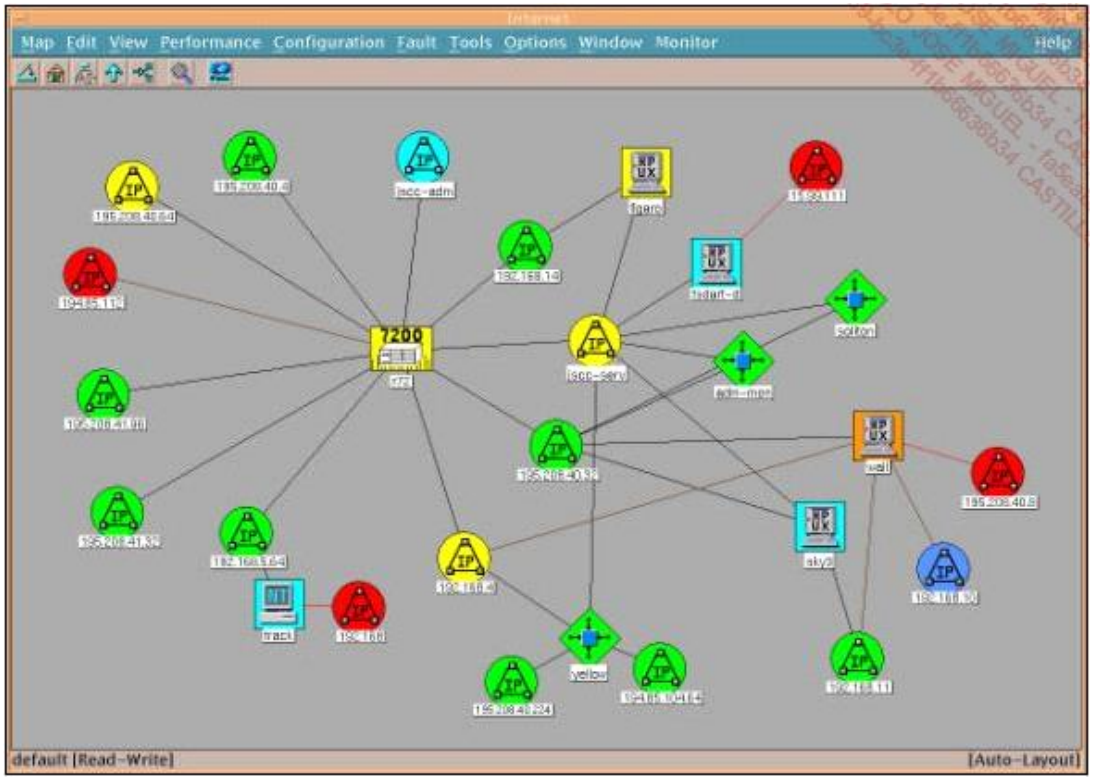
Obtención de información detallada de una MIB

Implementación

Existen numerosas soluciones que permiten cartografiar el entorno de red para supervisarlo en tiempo real.

HPOV (HP OpenView)

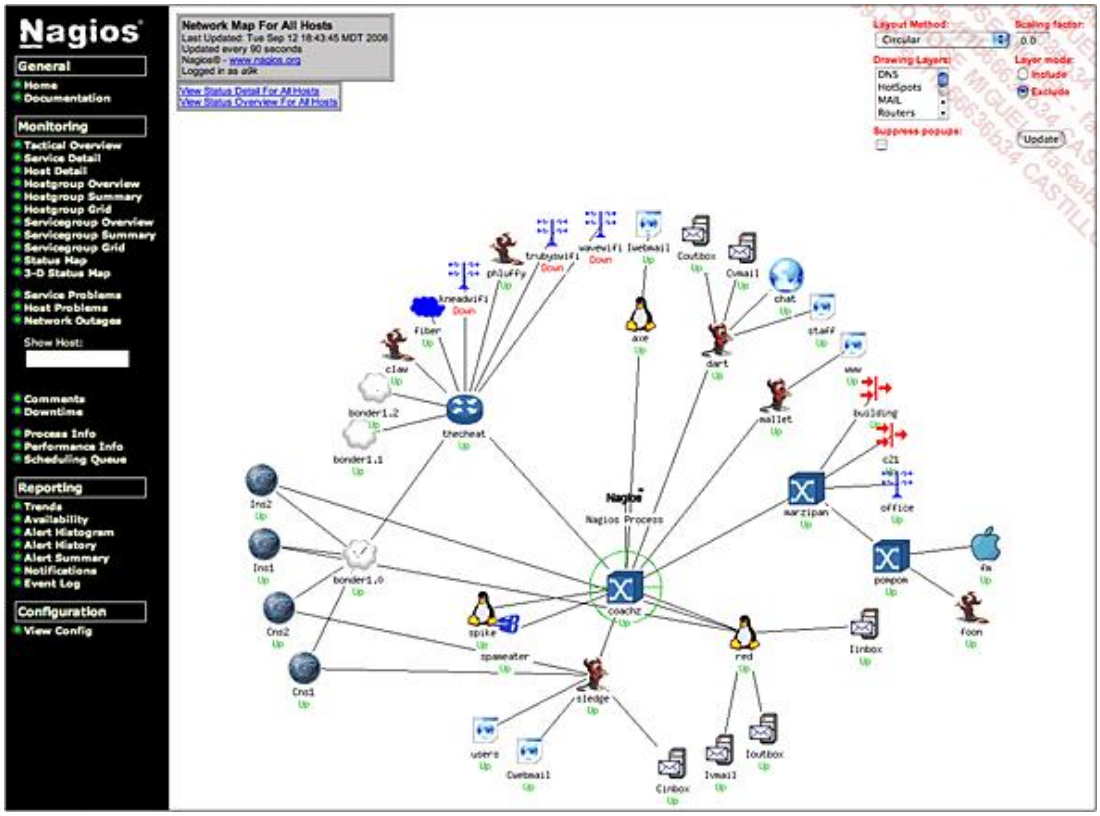
Una herramienta como HP Open View permite visualizar los equipos y los resalta con colores distintos en función de los posibles problemas que haya podido identificar. El color rojo se utiliza para advertir de que un componente se encuentra sin conexión o de que un conector de red está inactivo.



Cartografía HP Open View

Nagios

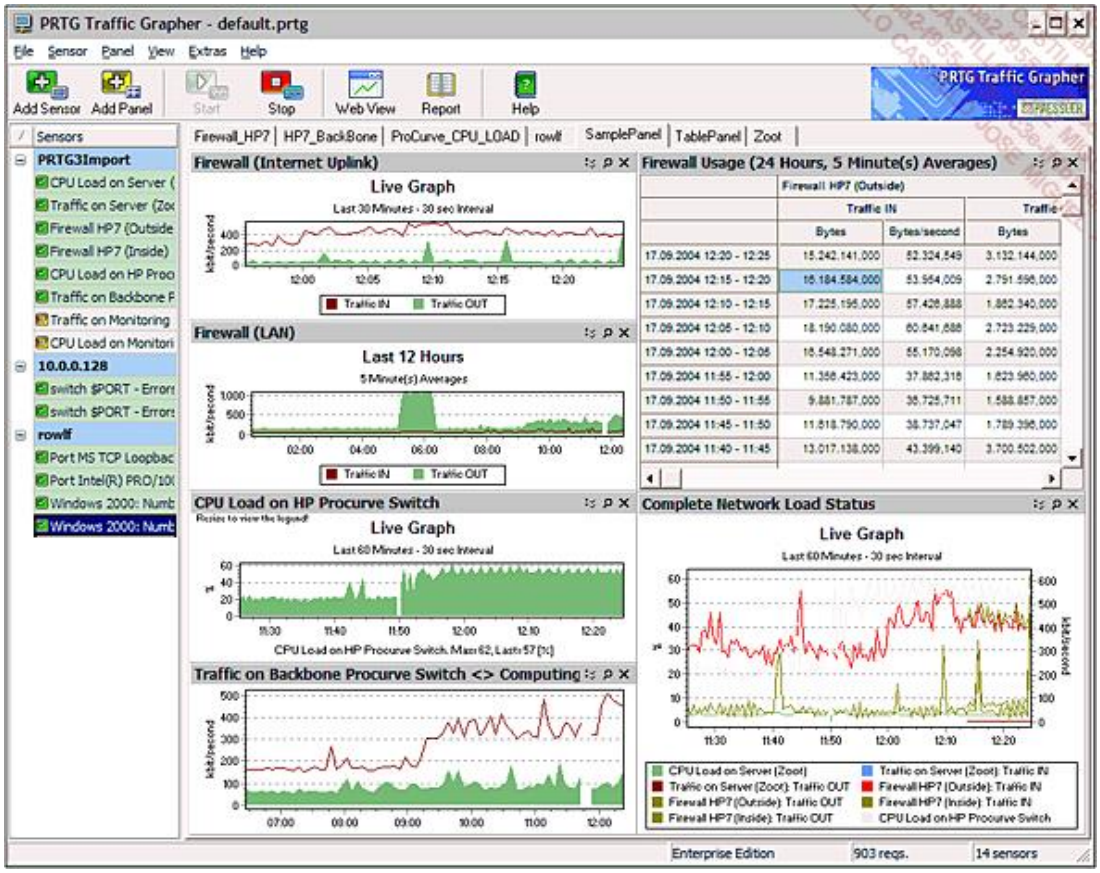
Otra solución de supervisión, llamada Nagios, se basa en componentes de código abierto. De este modo es posible, mediante la licencia libre, disponer de un conjunto de herramientas totalmente gratuito para supervisar en tiempo real el estado de todo el sistema informático.



Nagios

MRTG/PRTG (Multi Router Traffic Grapher/Paessler Router Traffic Grapher)

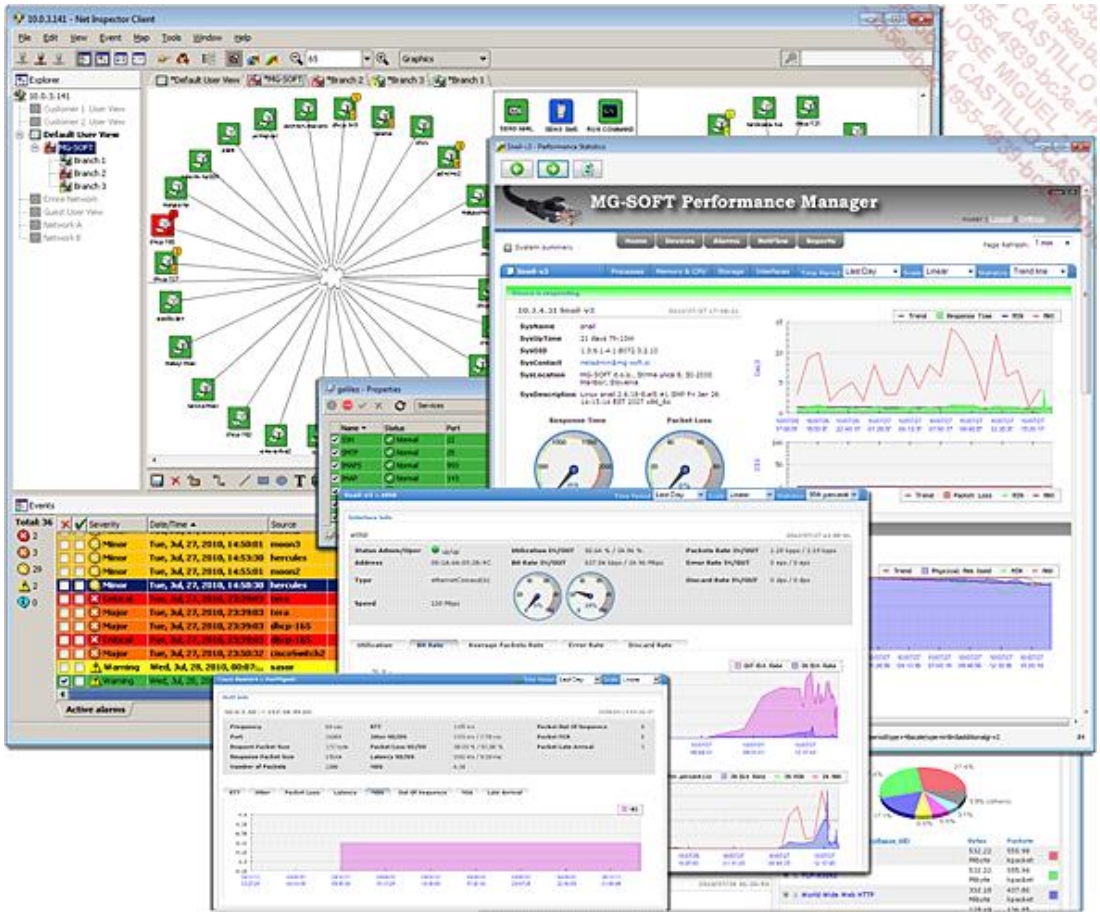
A veces, es necesario hacer un análisis profundo de los datos recogidos para poder observar anomalías. En estas situaciones, es necesario disponer de herramientas gráficas que permitan una visualización resumida de esta información. Herramientas como PRTG están especializadas en la visualización de información obtenida de los routers, conmutadores o cortafuegos.



PRTG Traffic Grapher

Net Inspector

Otras utilidades, como Net Inspector, también permiten realizar una cartografía para seguir en tiempo real el estado del entorno:



MG-SOFT Net Inspector