Facultad de Ciencias Sociales y de la Administración

Diplomatura en Gestión y Administración Pública

Asignatura de:

Redes de datos

Tema XIII:

Internet (anexo)

(Transparencias de clase)

DEPARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS

Curso: 2008/2009
Profesor: Manuel Fernández Barcell

e-mail: manuel.barcell@uca.es

Índice de contenido

Glosario internet - la jerga de la red....3
HISTORIA....7
Instalación de un servidor WEB....10
Instalación....10
Configuración....11
Administración....13
Conexión al servidor mediante el software cliente....16

Glosario internet - la jerga de la red

No se asuste si al leer sobre Internet comienza a oír hablar del Ciberespacio, de la WWW, el HTML 3.0 o los URL y el TCP/IP. Son algunas de las palabras y acrónimos de uso común que hay que conocer para adentrarse en este nuevo mundo. Aquí están recogidos los términos más importantes por orden alfabético, y podrán servirle como referencia. En ocasiones verá que algunas definiciones usan otros términos de la jerga... de modo que tendrá que repasarlas todas para hacerse una idea global.

Archie - Es un servicio de Internet que sirve para localizar archivos públicos que están disponibles a través de servidores FTP.

Autopista de la información (*Information Highway*) - Término acuñado por Al Gore, vicepresidente de los Estados Unidos, en 1991, para definir una estructura de comunicación del futuro, en principio, para mantener a los Estados Unidos competitivos, que integra todo tipo de medios y servicios a alta velocidad. Internet no es la Autopista de la información (que todavía no es una realidad), pero sí lo más parecido que existe hasta el momento.

Browser (Navegador) - Programa para acceder a diversos servicios de Internet, como la WWW, los servidores de FTP, los grupos de noticias o el correo. Son una solución "todo en uno" muy fácil de usar.

Ciberespacio - Término acuñado por William Gibson en su novela de ciencia ficción "Neuromante" (1984) para describir un mundo de redes de información. Se utiliza en la actualidad para referirse al conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el que casi todo lo que contiene información o puede transmitirla puede considerarse incluido.

DNS - (*Domain Name Server*, Servidor de Nombres de Dominio). Cualquiera de los servidores automáticos de Internet que convierten nombres fáciles de entender (como www.miempresa.com) a números IP (como 192.555.26.11).

e-mail - Es el nombre en inglés del correo electrónico.

FAQ (*Frequently Asked Questions*, Documentos de Preguntas Frecuentes). Documentos recopilatorios para usuarios principiantes, que contienen las preguntas más frecuentes sobre un tema determinado. Son la mejor forma de comenzar a aprender cosas sobre Internet.

FTP (*File Transfer Protocol*, Protocolo de Transmisión de Ficheros) - Método mediante el cual se pueden transferir archivos por Internet. Está asociado con los servidores FTP, directorios normalmente públicos de archivos de todo tipo.

Gopher - Sistema de búsqueda de información en Internet a base de menús, que permite navegar por directorios FTP y bases de datos.

HTML (*HyperText Markup Language*, Lenguaje de Marcas de Hipertexto) - Lenguaje usado para crear páginas de hipertexto y gráficos que forman los contenidos de la World Wide Web.

HTTP (*HyperText Transport Protocol*, Protocolo de Transferencia de Hipertexto).
El protocolo usado en la WWW para transmitir las páginas de información entre el programa navegador y el servidor.

Internet - Conjunto que aglutina las redes de datos e todo mundo, uniendo miles de ellas mediante el protocolo TCP/IP. O, expresado como idea, el mayor conjunto que existe de de información, personas, ordenadores y software funcionando de forma cooperativa. La i mayúscula la diferencia de una internet convencional, que simplemente une varias redes. Al ser única se la conoce también simplemente por "la Red".

IP (*Internet Protocol*, Protocolo Internet) - Suele hacer referencia a un "número IP", una serie de números específicos (cuatro grupos de valores entre 0 y 255) que se asignan a cada máquina que está conectada a la Red. Un DNS convierte los números IP a nombres comunes.

IRC (*Internet Chat Relay*, Sistema de Charla en Internet) - Es un sistema de charla en tiempo real, basado en canales temáticos a los que cualquiera se puede conectar y participar en vivo, desde cualquier lugar del mundo.

MUD (**Multi-User Dungeon/Dimension**, Dimensión/Mazmorra Multi-Usuario) - Entorno de realidad virtual, basado en texto o gráficos, en el que los usuarios conversan o interpretan diferentes papeles como diversión.
Newsgroup (Grupo de noticias) - Grupo de noticias de Usenet, en el que los usuarios pueden participar enviando y contestando mensajes en público sobre un tema específico.
Servidor - Máquina que está conectada a Internet y que ofrece acceso o algún tipo de servicios: acceso a páginas Web, directorios de FTP, correo, etc.
TCP/IP (*Transmission Control Protocol/Internet Protocol, Protocolo Internet*/Protocolo de Control de Transmisión) - Es la forma de comunicación básica de Internet. Hace que la información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan, siguiendo cualquier ruta posible.
Telnet - Servicio de Internet para conectarse de forma remota a otro ordenador, como si se hiciera desde un terminal local.
URL (*Uniform Resource Locator*, Localizador Universal de Recurso) - Es el nombre que reciben las diversas cosas e información que se pueden encontrar en la Red:

Páginas Web (http), archivos (ftp) o grupos de noticias (mail). Al escribir el nombre completo de un recurso en este formato, se accede a él, normalmente desde un programa navegador o *software* específico.

Usenet - Red que transmite miles de grupos de noticias, en forma de foros de charla globales y públicos sobre muchos temas distintos. Actualmente Usenet transmite más de 14.000 grupos de noticias sobre los más diversos temas.
WWW (*World Wide Web*, la telaraña mundial) - Es una red mundial de páginas de información hipertexto, por la que se puede circular mediante un navegador Web.
Cliente: cualquier estación de trabajo de una Intranet que solicita servicios a un servidor de cualquier naturaleza.
Estación de trabajo: cualquier ordenador conectado a la red. Antiguamente sólo se llamaba estación de trabajo a los ordenadores más potentes, en la actualidad no es así. Evidentemente todas las estaciones de trabajo deben incorporar su tarjeta de red; esto no impide que la estación pueda trabajar de forma independiente y utilizar los servicios de la Intranet cuando le sea necesario.
Nodo: cualquier estación de trabajo, terminal, ordenador personal, impresora o cualquier otro dispositivo conectado a la Intranet. Por lo tanto, este término engloba al anterior. Los dispositivos pueden conectarse a la Intranet a través de un ordenador, o bien directamente si éstos son capaces de soportar una tarjeta de red.
Servidor: se trata de una estación de trabajo que gestiona algún tipo de dispositivo de la Intranet, como pueden ser impresoras, faxes, modems, discos duros, etc., dando servicio al resto de las estaciones, no siendo necesario que dichos dispositivos estén conectados de forma directa a esta estación. Por tanto, se puede hablar de servidor de impresión, servidor de comunicaciones, servidor de ficheros, etc. Estos servidores pueden ser dedicados, cuando no pueden utilizarse para otra cosa, o no dedicados, cuando funcionan como un ordenador más de la Intranet, además de prestar servicios como servidor de algún elemento.
Medio de transmisión: se trata de cualquier medio físico, incluso el aire (como por ejemplo en las comunicaciones inalámbricas o por radio), que pueda transportar información en forma de señales electromagnéticas. El medio de transmisión es el soporte de toda la Intranet: si no tenemos medio de transmisión, no tenemos Intranet. Existen diferentes medios de transmisión: cable coaxial, fibra óptica, par trenzado, microondas, ondas de radio, infrarrojos, láser, etc. La elección del medio de transmisión para una red no se hace de forma aleatoria; existen un serie de factores que lo determinan: la velocidad que queramos en la red, la arquitectura, el ruido e interferencias que va a tener que soportar, la distancia, etc.
Método de acceso al medio: una vez que se tiene seleccionado el medio de transmisión que se va a utilizar para implementar la red, se debe elegir el método que los diferentes nodos de la red van a

emplear para acceder a dicho medio. En un principio se podría obviar esta cuestión, pero si el lector se detiene un momento a pensar en el siguiente ejemplo, se dará cuenta de la necesidad de esta política. El ejemplo es el siguiente: Imagine, que tiene dos ordenadores de su Intranet que quieren utilizar la red para enviar información en un instante determinado. Si los dos ordenadores colocan en el medio físico, sin más, la información, puede ser que ambos paquetes de información "choquen" y de deterioren, no llegando ninguno de ellos a su destino. Obviamente, cuando varios dispositivos están compartiendo un medio común, es necesaria la implantación de una política de uso de dicho medio: se trata de un método de acceso al medio. Se podrían citar como medios más comunes el paso de testigo, acceso múltiple por detección de portadora con y sin detección de colisiones, polling, contención simple, etc. En cada topología de red se utiliza el más conveniente de estos métodos; por ejemplo, cuando se tiene una red en anillo, el método de acceso al medio utilizado es el paso de testigo, mientras que si tenemos una topología en bus, los métodos de contención son lo más adecuados. Los métodos de control de acceso al medio se encuentran dentro del nivel de enlace de la torre OSI, por lo que en realidad pueden entenderse como protocolos de red.

Protocolos de red: ya se ha establecido cómo van a acceder los diferentes nodos a la red y ahora es necesario especificar cómo van a comunicarse entre sí. Los protocolos de red definen las diferentes reglas y normas que rigen el intercambio de información entre nodos de la red. Los protocolos establecen reglas a muchos niveles: desde cómo acceder al medio, hasta cómo encaminar información desde origen hasta su destino, pasando por la descripción de las normas de funcionamiento de todos y cada uno de los niveles del modelo OSI de la ISO. Por citar algunos ejemplos de protocolos, nombraremos varios: TCP (protocolo de control de transmisión), IP (protocolo Internet), FTP (protocolo para transferencia de ficheros), X.25, etc.

ISO (International Organization for Standardization): Se trata de una organización reconocida mundialmente de normalización. Su objetivo es el de promover y desarrollar normas para el intercambio internacional. Establece normas de estandarización en muchísimos campos, estableciendo modelos a seguir para todos y cada uno de ellos. Abarca campos tan dispares como el diámetro de algunos tipos de conectores, el paso de rosca de tornillos, el grosor de un modelo concreto de cable, etc. En cuanto al campo de las comunicaciones, la ISO ha desarrollado un modelo, al que llamó OSI. Sus normas fomentan los entornos abiertos de conexión de red, que permiten a sistemas de diferentes casas comerciales comunicarse entre sí mediante el uso de protocolos.

OSI (Open System Interconnection): se trata de un modelo elaborado por la ISO que define los protocolos de comunicación en siete niveles diferentes. Estos niveles son los siguientes: aplicación, presentación, sesión, transporte, red, enlace y físico. Cada nivel se encarga de una parte en el proceso de transmisión (en el proceso de elaboración de la información a transmitir), apoyándose en los servicios que le ofrece el nivel inferior y dando servicios a niveles superiores.

Cada nivel tiene funciones muy definidas, que se interrelacionan con las funciones de niveles contiguos. Los niveles inferiores definen el medio físico, conectores y componentes que proporcionan comunicaciones de red, mientras que los niveles superiores definen cómo acceden las aplicaciones a los servicios de comunicación.

Paquete: un paquete es básicamente el conjunto de información a transmitir entre dos nodos. Cuando una aplicación quiera enviar información a otra aplicación de otro nodo, lo que hace es empaquetar dicha información, añadiendo datos de control como la dirección de la máquina que envía la información (dirección origen) y la dirección de la máquina a la que va destinada la información (dirección destino). Por tanto, cuando se habla de empaquetamiento, se hace referencia al proceso de guardar dentro de un paquete la información que se quiere transmitir.

Dirección: todos los nodos de la Intranet deben tener una dirección que los identifique dentro de la Intranet de forma única, al igual que todos tenemos una dirección postal para poder recibir correo. La dirección de un nodo depende del protocolo IP (de la familia de protocolos TCP/IP) y en general

codifican la Intranet (recordamos que podemos interconectar distintas Intranets) y también codifican el nodo dentro de la Intranet. El número asignado a cada una de estas partes depende del tipo de Intranet que tengamos.

Ahora ya estamos en condiciones de entender cosas como "direccionamiento IP" (no es más que enviar un paquete a otro nodo utilizando para ello direcciones con el formato que el protocolo IP impone).

TCP/IP: se ha puesto muy de moda hablar de TCP/IP, ¿pero qué es TCP/IP? TCP/IP son dos protocolos de comunicaciónes: el protocolo TCP (Protocolo de control de transmisión) que se establece a nivel de transporte del modelo OSI y el protocolo IP (Internet Protocolo), que pertenece al nivel de red. En realidad, cuando se utiliza el término TCP/IP se hace referencia a una familia muy amplia de protocolos representada por ambos. Estos protocolos son lo que utiliza Internet para la interconexión de nodos. Sobre ellos se establecen otros protocolos a niveles superiores hasta llegar al nivel de aplicación (el más cercano al usuario), en el que se encuentran protocolos tan conocidos como FTP (Protocolo para transferencia de ficheros) y que todo aquel que se haya conectado vía TCP/IP a otro nodo habrá utilizado para poder traerse ficheros.

Interconexión de Intranets: a veces se plantea la necesidad de interconectar dos o más Intranets, por ejemplo por necesidades de compartir recursos; y otras veces se necesita la división en dos subIntranets de una Intranet para mejorar el rendimiento de ésta, por ejemplo. En ambos casos es necesaria la presencia de un dispositivo, que puede ser un hubs, un bridges, un routers, etc. Cada uno de estos dispositivos está diseñado para interconectar Intranets; la diferencia estriba en el nivel en el que es necesario interconectarlas: no es lo mismo interconectar dos Intranets con la misma arquitectura que dos Intranets de arquitecturas diferentes y con diferentes protocolos.

Hubs (concentradores): dispositivo que centraliza la conexión de los cables procedentes de la estaciones de trabajo. Existen dos tipos de concentradores: pasivos y activos. Los concentradores pasivos son simplemente cajas que disponen de unos puertos a los que se conectan las estaciones de trabajo dentro de una configuración en forma de estrella. Únicamente se trata de un cuadro de uniones.

Un concentrador activo es un concentrador que dispone de más puertos que un concentrador pasivo para la conexión de estaciones y que realiza más tareas, como puede ser la de amplificación de la señal recibida antes de su retransmisión. A veces se utilizan para estructurar la topología de una Intranet, permitiendo mayor flexibilidad en la modificación de ésta.

Bridges (puentes): nos permiten dos cosas: primero, conectar dos o más Intranets entre sí, aun teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red, y segundo, segmentar una Intranet en otras menores. Los puentes trabajan en el nivel de enlace del modelo OSI de la ISO. Algunos de los motivos que nos pueden inducir a instalar un puente son ampliar la extensión de una Intranet y/o el número de nodos que la componen; reducir el cuello de botella del tráfico causado por un número excesivo de nodos unidos o unir Intranets de topologías similares como bus y anillo. Los puentes se pueden crear incorporando dos tarjetas de red (una de cada una de las Intranets a interconectar) dentro del mismo servidor (conectado obviamente a ambas redes), siempre que el sistema operativo de red de dicho servidor sea capaz de gestionarlo. Existe dos tipos de puentes: locales y remotos. Los puentes locales sirven para segmentar una Intranet y para interconectar Intranets que se encuentren en un espacio físico pequeño, mientras que los puentes remotos sirven para interconectar redes lejanas.

Routers (encaminadores): se trata de dispositivos que interconectan Intranets a nivel de red del modelo OSI de la ISO. Realizan funciones de control de tráfico y encaminamiento de paquetes por el camino más eficiente en cada momento. La diferencia fundamental con los bridges es que éstos no son capaces de realizar tareas de encaminamiento en tiempo real, es decir, una vez tienen asignado un camino entre un nodo origen y uno destino siempre lo utilizan, aunque esté saturado de tráfico, mientras que los routers son capaces de modificar el camino establecido entre dos nodos dependiendo del tráfico de la red y otros factores.

internet (anexo)

Gateways (pasarelas): se trata de ordenadores que trabajan a nivel de aplicación del modelo OSI de la ISO. Es el más potente de todos los dispositivos de interconexión de Intranets. Nos permiten interconectar Intranets de diferentes arquitecturas; es decir, de diferentes topologías y protocolos; no sólo realiza funciones de encaminamiento como los routers, sino que también realiza conversiones de protocolos, modificando el empaquetamiento de la información para adaptarla a cada Intranet.

HISTORIA

Para evitar que un ataque nuclear pudiera dejar aisladas a las instituciones militares y universidades, en 1969 el ARPA (*Advanced Research Projects Agency*), una agencia subsidiaria del departamento de defensa de los Estados Unidos, desarrolló una red denominada ARPAnet basada en el protocolo de intercambio de paquetes.

Un protocolo de intercambio de paquetes es un sistema que divide la información en partes y las envía una por una al ordenador de destino con un código de comprobación. Si el código de comprobación no es correcto se solicita al ordenadorde destino que vuelva a enviar los paquetes corruptos.

La ventaja de este sistema de transmisión es principalmente su fiabilidad de los datos, independientemente de la calidad de la línea utilizada. Los datos llegan incluso si no funcionan o son destruidos parte de los nodos de la red, factor que influyó decisivamente para su adopción por parte del gobierno norteamericano.

Otra ventaja es que este tipo de sistemas permite distribuir más fácilmente los datos, ya que cada paquete incluye toda la información necesaria para llegar a su destino, por lo que paquetes con distinto objetivo pueden compartir un mismo canal.

Además es posible comprimir cada paquete para aumentar la capacidad de transmisión o encriptar su contenido para asegurar la confidencialidad de los datos. Estas virtudes han asegurado la supervivencia de los protocolos desde las primeras pruebas realizadas en 1968 por el Laboratorio Nacional de Física del Reino Unido hasta nuestros días.

El primer protocolo utilizado por **ARPAnet** fue el denominado **NCP** (*Network Control Protocol*), que se empleó en la red hasta 1982, año en el que se adoptó el protocolo **TCP/IP** procedente de los sistemas Unix que empezaban a ejercer un silencioso dominio dentro de ARPAnet.

El protocolo **TCP/IP** (*Transmission Control Protocol/InternetProtocol*) proporciona un sistema independiente de intercambio de datos entre ordenadores y redes locales de distinto origen,conservando todas las ventajas que hemos mencionado de los protocolos de transmisión de paquetes. Este protocolo ha evolucionado hasta nuestros tiempos a pesar de que han aparecido otros como el **ATM** (*Asynchronous Transfer Mode*), que han demostrado ser más potentes pero menos difundidos.

El **TCP/IP** permite asignar un identificador numérico de cuatro números (del 0 al 255) a cualquier ordenador conectado a la red (en el caso de Internet a cualquier ordenador del mundo), proporcionando una dirección única a cada sistema, lo que permite un intercambio fiable de datos sea cual sea la línea que utilicemos.

Uno de los inconvenientes de estas direcciones **IP** es su complicada memorización por parte de los usuarios. Para solucionarlo, se adoptó una tabla denominada «nombre de dominio» que traducía las direcciones **IP** a una serie de códigos más comprensibles.

De esta manera una dirección **IP** como «129.89.200.102» puede traducirse mediante la tabla de dominios en «merlin.nasa.gov». La primera parte del dominio indica el nombre de la máquina a quien corresponde la dirección **IP**; después viene el nombre de la organización a la que pertenece el servidor (en este caso la **NASA**); mientras que en tercer lugar podemos encontrar un código que puede referirse al tipo de organización a la que pertence el sistema o al país donde resíde. Así, tenemos códigos como «.gov» (organismo gubernamental), «.edu» (universidades o centros educativos), «.com» (redes comerciales pertenecientes a empresas) o códigos de países como «.it» para Italia o «.es» para España.

En 1969 el **ARPA** instaló el primer servidor de información en un ordenador Honeywell 516 que incorporaba nada menos que 12 Kbytes de memoria. Pronto se añadirían otros servidores por parte del instituto de investigación de Stanford (**SRI**), de la **UCSB** (Universidad de California en Santa Barbara) y de la universidad de Utah que formaron los primeros nodos de

internet (anexo)

ARPAnet.

Sin embargo, la red Internet como «red de redes» no comenzó a funcionar hasta después de la primera conferencia de comunicaciones por ordenador en octubre de 1972. En esta convención **ARPAnet** presentaba una red de 40 nodos y se propuso su conexión con otras redes internacionales. Representantes de varios países formaron así el **INWG** (*Inter Network Working Group*) para establecer un protocolo común con el **ARPA**,empezando a dar forma lo que hoy en día conocemos por Internet.

Con el tiempo **ARPAnet** fue sustituida por **NSFnet**, la red de la fundación nacional para la ciencia de **EEUU**, como organismo coordinador de la red central de Internet que en breve también será sustituida quizás por un organismo privado.

Desde los primeros pasos de **ARPAnet** hasta hoy en día la red ha sufrido pocos cambios comparado, por ejemplo, con los avancesde la informática. Los cambios más drásticos se han producidoen la infraestructura de la red, aumentando la velocidad de transmisión hasta permitir el funcionamiento de aplicaciones multimedia y la transmisión de vídeo o sonido en tiempo real.

También han sufrido cambios el tipo de servicios ofrecidos por Internet, ya que si bien las utilidades en modo texto han sobrevivido con dignidad hasta nuestros días, la verdadera estrella de la Red actualmente es la World Wide Web, un servicio de consulta de documentos hipertextuales que ha logrado una inmensa popularidad tanto entre expertos como entre profanos.

Cronología de internet

1968-70	La agencia norteamericana ARPA, dependiente del Ministerio de Defensa, crea ARPANET
1971	23 nodos. Participan las universidades de Utah, Stanford, UCLA, Harvard y CMU
1974	Cerf y Kahn publican las especificaciones definitivas del protocolo TCP/IP
1981	Se crean las redes BITNET (Because Its Time NETwork) y CSNET (Computer Science NETwork) para dar servicio a la comunidad científica no directamente relacionada con ARPANET. Francia inagura la red de videotex Minitel.
1982	ARPANET adopta TCP/IP como estándard.
1983	Se crea la EARN (European Academic and Research Network) para dar servicio a las universidades y centros de investigación europeos.
1984	Se instauran los servicios de denominación simbólica DNS (Domain Name Server).
1986	Se crea la red de alta velocidad NFSNet de la National Science Foundation que comunica a cinco grandes ordenadores.

1987	NFSNet se amplia para dar acceso a las universidades norteamericanas. Gestionan esta red: Merit, MCI e IBM.
1989	Se crea RIPE (Resource IP European) para gestionar la interconectividad de las redes IP europeas.
1990	Desaparece ARPANET. Mitch Kapor crea la Electronic Frontier Foundation.
1991	Aparece la asociación Commercial Internet eXange (CIX) y los primeros servidores WAIS y GOPHER.
1992	Se crea la InterNet SOCiety (ISOC) como un organismo encargado de supervisar la evolución de la red. Tim Barnes-Lee crea el *World-Wide-Web*.
1993	Las empresas y los medios de comunicación empiezan a interesarse por InterNet. La Casa Blanca, la ONU y el Banco Mundial se conectan. Al Gore difunde el informe US National Information Infraestructure Act, que motivará la expansión de InterNet.
1994	Empiezan a aparecer, en InterNet, las operaciones masivas de márqueting y las primeras transacciones comerciales.
1995	Desaparece NFSNet. Es superado, por vez primera, el número de redes de los EEUU respecto a otros paises. NetScape Inc. inicia su cotización en la Bolsa de Nueva York. Telefónica crea en España la red privada InfoVía.

Instalación de un servidor WEB

El *Servidor Personal de Web* de Microsoft nos permitirá acceder a páginas Web dentro de nuestra red local (*Intranet*) sin estar conectados a Internet. También podremos realizar transferencias de ficheros (FTP) entre las que se incluyen la publicación de páginas web en dicho servidor. Se instalará en un equipo destinado para ese fin el cual **no** tendremos conectado a Internet. Deberemos también tener un navegador instalado previamente en el equipo (IE o Navigator) pues será necesario para la administración del servidor.

El Servidor personal de Web se incluye como un servicio dentro de la versión OSR2 de Windows 95 . Si no tenemos esa versión podemos bajar el programa de instalación del servidor desde la web de Microsoft en la dirección http://www.microsoft.com/spain/descarga/#server .

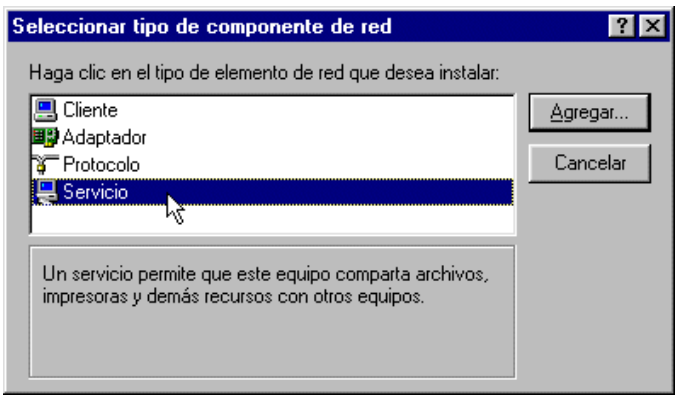
Instalación

NOTA IMPORTANTE: Antes de instalar el Servidor personal de Web, **quitar** el servicio ***Compartir impresoras y archivos para redes Microsoft*** si se encuentra instalado. Además necesitaremos tener instalado un software de navegación (por ejemplo, Netscape Navigator o Internet Explorer).

Para instalar el Servidor Personal de Web en versiones anteriores a la OSR2 hacer doble clic sobre el programa de instalación **Espwss1.exe** con lo que se añadirá automáticamente como servicio dentro del icono ***Red*** del ***Panel de control***.

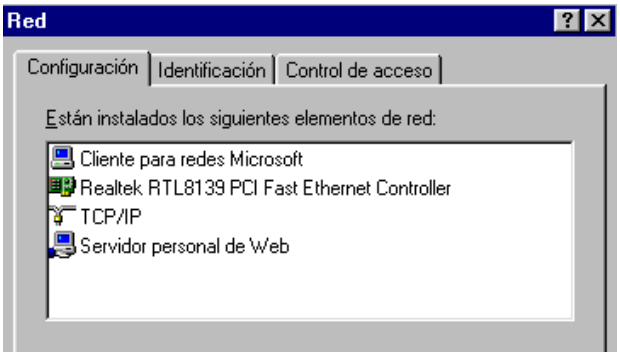
Para la versión OSR2:

- Acceder al icono ***Red*** dentro del ***Panel de control*** y en el cuadro de diálogo ***Red*** hacer clic sobre el botón ***Agregar***.
- En el cuadro de diálogo ***Seleccionar tipo de componente de red*** hacer doble clic sobre el icono ***Servicio***.



En el cuadro de diálogo ***Seleccione Servicio de Red***, seleccionar ***Microsoft*** de la lista de fabricantes y luego hacer doble clic sobre el icono ***Servidor personal de Web*** en la lista de Servicios de red.

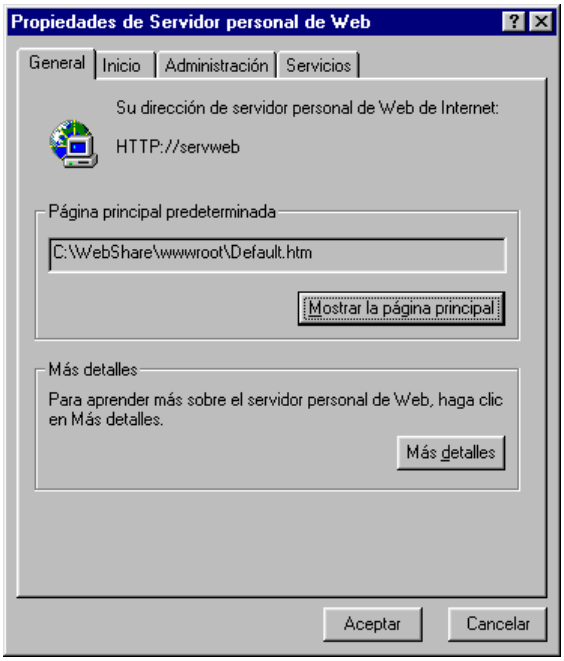
Hacer clic sobre el botón ***Aceptar*** en el cuadro de diálogo anterior, con lo que aparecerá en el cuadro de diálogo ***Red*** el ***Servidor personal de Web*** dentro de la lista de componentes instalados:



Hacer clic sobre el botón ***Aceptar***. Insertemos los disquetes o el CD-Rom de instalación de Windows 95 cuando se nos lo solicite y haremos clic sobre el botón ***Si*** cuando se nos pregunte si deseamos reiniciar el equipo.

Configuración

Una vez instalado el servidor, aparecerán sendos iconos en el ***Panel de control*** y en la ***Barra de tareas*** que nos permitirán configurarlo. Si hacemos doble clic sobre uno de esos iconos aparecerá el cuadro de diálogo ***Propiedades de Servidor personal de Web*** con la ficha ***General*** activada:



Las opciones presentes en las fichas de este cuadro de diálogo controlan la forma en que se ejecuta la aplicación y los dos servicios presentes (HTTP y FTP) y también nos conducen a páginas web que administran cada servicio.

Ficha general. En la sección ***Página principal predeterminada*** se muestra la ruta de acceso local a la página que verán los usuarios de la red cuando se conecten a nuestro servidor. Por ejemplo, si un usuario de la red teclea en su navegador la URL *http://servweb*, le aparecerá

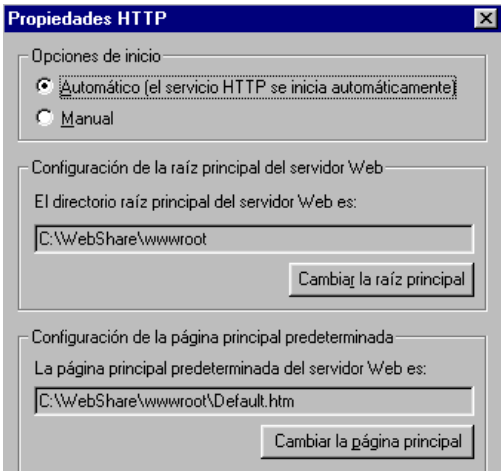
esa página. Es posible cambiar tanto la localización como la página (ya veremos cómo). Dicha página puede visualizarse haciendo clic sobre el botón adjunto.

Ficha Inicio. Los botones ***Inicio*** y ***Detener*** controlan la ejecución del servidor. En la sección

Opciones, mediante las casillas de verificación correspondientes, podemos hacer que el servidor se ejecute o no automáticamente al iniciar el equipo y que se muestre o no su icono en la Barra de tareas. En caso de que desactivemos la última opción, la única forma de acceder al cuadro de diálogo de propiedades será a través del Panel de control.

Ficha Administración. Haciendo clic sobre el botón ***Administración*** se nos conducirá a una página web que permite la administración de los servicios WWW y FTP y que estudiaremos más adelante.

Ficha Servicios. Los botones ***Inicio*** y ***Detener*** permiten iniciar o detener el servicio que hayamos seleccionado previamente con el ratón. Por otra parte, seleccionando un servicio y haciendo clic sobre el botón ***Propiedades***, se presentará el cuadro de diálogo ***Propiedades de 'Servicio'***. A través de dicho cuadro de diálogo es posible controlar la ejecución del servicio: ***automática***, si queremos que se ejecute cada vez que se inicie el servidor personal o ***manual***, si queremos iniciarlo nosotros. El cuadro de diálogo *Propiedades de 'Servicio'* también permite cambiar el directorio raiz de ambos servicios y la página principal predeterminada en el caso de HTTP como veremos en el siguiente apartado.



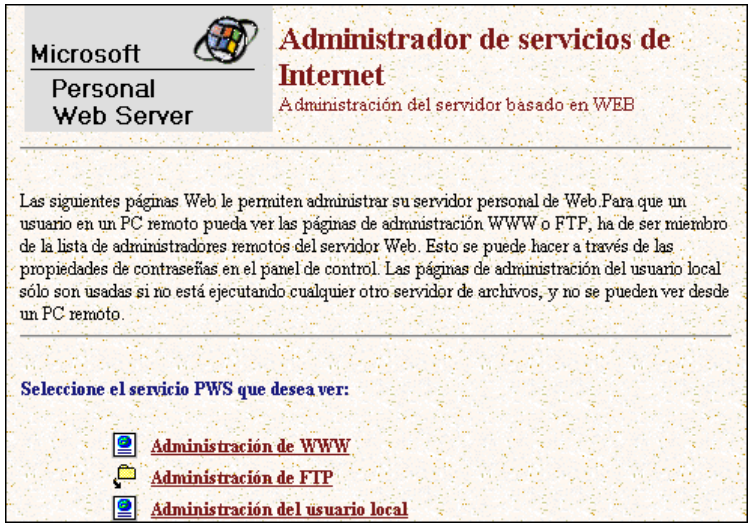
Administración

Como se comentó en la introducción, el Servidor Personal de Web permitirá que otros usuarios puedan acceder a páginas web a nivel de nuestra red local (Intranet) sin necesidad de estar conectados a Internet. Las páginas se encontrarán almacenadas en el servidor y el acceso a las mismas será exactamente igual que en Internet, a través de sus URL´s, pero con la ventaja de tener velocidades de carga mucho más rápidas. Como administradores del sistema que somos, deberemos encargarnos tanto de preparar una serie de páginas que sirvan de presentación de nuestro servidor, como de facilitar que otros usuarios de la red puedan publicar sus propias páginas en el mismo (vía FTP). La creación y publicación de páginas (transferencia de las mismas a un servidor web) se tratará en el capítulo 6: Diseño de Páginas Web. En este apartado veremos como configurar nuestro servidor para permitir lo anterior. Dicha configuración incluye:

- La habilitación de carpetas en el servidor para almacenar las páginas y que estas sean visualizadas (administración WWW).
- La habilitación del servicio FTP para determinadas carpetas en las que el administrador y otros usuarios (por ejemplo, el alumnado) puedan publicar sus páginas (administración FTP).
- La creación de nombres de usuarios y contraseñas para que solamente usuarios registrados puedan modificar las páginas publicadas o publicar nuevas páginas (administración del usuario local).

La administración de los servicios WWW, FTP y Administración del usuario local del servidor personal de Web se realiza a través de una página web. Accederemos a dicha página haciendo clic sobre el botón ***Administración*** dentro de la ficha ***Administración*** del cuadro de diálogo ***Propiedades de Servidor personal de Web***. La página se cargará con el navegador al que estén asociados los documentos HTML (en nuestro caso IE):

internet (anexo)



Como puede apreciarse, la página anterior posee tres enlaces. Veamos la finalidad de cada uno de ellos:

Administración de WWW

Haciendo clic sobre la ficha ***Directorios***, accederemos a una página que permite definir cual va a ser la carpeta raíz del servidor y su página de inicio.

La **carpeta raíz** es a la que se conectará el navegador de un ordenador cliente cuando se escriba la dirección del servidor web (en nuestro caso ***http://servweb***). Dicha carpeta es por defecto ***C:\WebShare\wwwroot***. La dejaremos como está. Toda la estructura de páginas web que queramos publicar para los usuarios de nuestra intranet (páginas principales y subcarpetas) se copiará dentro de dicha carpeta. El método de copia dependerá de donde tengamos esas páginas: lo más cómodo será tener instalado en el mismo equipo servidor un editor de páginas web con lo que podremos guardarlas directamente como archivos (ver capítulo 6) en carpetas creadas con el Explorador de Windows. También podemos guardarlas vía FTP si las hemos creado en otro ordenador de la red.

Por otra parte, la **página de inicio**, que debe encontrarse dentro de la carpeta C:\WebShare\wwwroot, será la página que visualice el navegador del ordenador cliente (por defecto, ***Default.htm***) cuando escriba la dirección de nuestro servidor. Podemos crear nuestra propia página con ese nombre y luego guardarla ahí, o bien escribir el nombre de una que ya tengamos creada en el cuadro de texto Documento predeterminado (por ejemplo *iesgrana.htm*).

Administración de FTP

Haciendo clic sobre la ficha ***Directorios*** aparecerá una página en la que podemos observar en primer lugar la carpeta raíz del servicio (que por defecto es ***C:\Webshare\ftproot***). Cuando un usuario anónimo se conecte a nuestro servidor, su carpeta raíz será esa carpeta. La podemos dejar como está.

Es posible definir carpetas adicionales para el servidor ftp haciendo uso del enlace ***Agregar*** en la parte inferior de la página. Dichas carpetas (o directorios) se llaman **directorios virtuales** y no tienen por qué ser subcarpetas físicas de la carpeta raíz. En nuestro caso las usaremos para conexiones no anónimas al servidor ftp (esto es, usuarios que se conectan usando un nombre registrado y una contraseña). Cuando un usuario se conecte de esta forma, su programa ftp cliente le llevará directamente a una de dichas carpetas en la que tendrá acceso total. Esto nos servirá para que los usuarios de nuestra Intranet publiquen su páginas web en esas carpetas. En el ejemplo que se muestra a continuación hemos habilitado dos carpetas virtuales ***alumno1*** y ***alumno2*** dentro de la subcarpeta ***alumnos*** de c:\Wevshare\wwwroot:

Para crear o habilitar (si ya se ha creado la carpeta con el explorador de Windows) una carpeta virtual, hacer clic sobre el enlace ***Agregar*** de la ficha ***Directorios***:

A través del botón ***Examinar*** explorararemos el arbol de carpetas de nuestro disco duro para seleccionar la carpeta deseada o incluso crear una nueva.

Activaremos el botón de elección ***Directorio virtual*** y escribiremos el alias para la carpeta en el cuadro de texto adjunto. El alias será el nombre con el que verán la carpeta los usuarios remotos (por ejemplo, podrían conectarse usando la URL ***ftp://servweb/alumno3***). El alias no tiene porqué coincidir con el nombre original de la carpeta.

Por último, activar las casillas de verificación ***Leer*** y ***Escribir*** para que los usuarios tengan acceso total sobre el contenido de la carpeta creada. Más adelante (en administración de usuarios)

deberemos limitar el acceso a la carpeta al usuario que vaya a hacer uso de ella para publicar las páginas. En caso contrario, todos los usuarios (incluidos los anónimos) podrían tener acceso total a esa carpeta vía ftp.

NOTA: Es posible crear subcarpetas del directorio raíz *C:\Webshare\ftproot* sin definirlas como virtuales (lo podemos hacer con el Explorador de Windows). En este caso serán visibles para cualquier usuario que se conecte a nuestro servidor (incluyendo los anónimos) como subdirectorios del directorio raíz. Además heredarán los derechos de acceso a este (que son por defecto de sólo lectura para todos los usuarios). Mediante este sistema podemos crear por ejemplo una carpeta llamada ***pub*** (esto es, ***C:\Webshare\ftproot\pub***) donde nosotros, como administradores copiaremos ficheros para distribuirlos por la Intranet vía ftp. Las conexiones anónimas a nuestro servidor localizarán fácilmente esta carpeta y podrán bajarse ficheros de todo tipo (por ejemplo, ejecutables de instalación de aplicaciones).

Administración del usuario local

Para restringir el acceso a las carpetas virtuales creadas para ftp a determinados usuarios, es necesario registrar primero a dichos usuarios dentro de nuestro sistema. Para ello usaremos el enlace ***Administración del usuario local*** presente en la página de administración del servidor que conducirá a la página siguiente:

Para **agregar un nuevo usuario**, bastará hacer clic sobre el botón correspondiente. Aparecerá la página siguiente, donde deberemos escribir un nombre y una contraseña para el mismo y luego hacer clic sobre el botón ***Agregar***:

Restricción del acceso a las carpetas de los usuarios

Una vez definidos los usuarios, deberemos quitar los permisos por defecto en las carpetas virtuales creadas y asignar permisos sólo a los usuarios de dichas carpetas. Esto se debe hacer con el ***Explorador de Windows*** a través del comando ***Compartir*** de cada carpeta.

Por ejemplo, hemos definido con anterioridad una carpeta virtual llamada ***alumno3***. Localizaremos dicha carpeta a través del ***Explorador de Windows*** y luego escogeremos la opción ***Compartir*** de su menú contextual, con lo que aparecerá el cuadro de diálogo ***Propiedades de alumno3***:

En dicho cuadro de diálogo hay que:

- Seleccionar el usuario ***El Mundo*** y hacer clic sobre el botón ***Quitar***.
- Hacer clic sobre el botón ***Agregar*** y añadir el usuario propietario de la carpeta (en nuestro caso ***Alumno3***) con derechos de ***Acceso Total***.
- Hacer clic sobre el botón ***Aceptar*** para validar los cambios efectuados.

Conexión al servidor mediante el software cliente

Conexión al servidor WWW

Ya sea con IE o con Navigator, escribiremos la URL ***http://servweb*** dentro del cuadro de diálogo ***Abrir*** del navegador. Recordemos que hemos definido una página de inicio para nuestro servidor WWW (***iesgrana.htm***) por lo que no hará falta indicar página alguna en la URL anterior. Luego nos moveremos simplemente por los enlaces de esa página.

Conexión al servidor FTP

Una vez configurado nuestro servidor ftp podremos conectarnos al mismo usando cualquier cliente FTP del mercado (por ejemplo el WS_FTP). Recordemos que para FTP existen dos tipos de acceso: *anónimo* y para *usuarios registrados* y esto se lo deberemos indicar al programa cliente. Tal como hemos diseñado nuestro servidor, accederemos anónimamente cuando queramos bajarnos software

de la carpeta "*pub*" definida anteriormente, mientras que si lo que queremos es transferir las páginas web que hayamos creado, lo haremos como usuarios registrados. A continuación se muestra un ejemplo de como configurar el acceso al servidor con el WS_FTP cuando queremos conectarnos como usuarios registrados:

internet (anexo)

DOCUMENTOS RFC (Request For Comments)

Network Working Group — Y. Rekhter
Request for Comments: 1918 — Cisco Systems
Obsoletes: 1627, 1597 — B. Moskowitz
BCP: 5 — Chrysler Corp.
Categoría: Mejor Práctica Actual — D. Karrenberg
RIPE NCC
G. J. de Groot
RIPE NCC
E. Lear
Silicon Graphics, Inc.
Febrero 1996

Asignación de direcciones para Internet privadas

Status de este memorándum

Este documento especifica unas "Mejores Prácticas Actuales", Best Current Practices (BCP), para la comunidad Internet, y solicita su discusión y sugerencias para mejorarlas. La distribución de este memorándum es ilimitada.

1. Introducción

Para los propósitos de este documento, una empresa es una entidad que maneja de manera autónoma una red usando TCP/IP y en particular, que determina el plan de direccionamiento y las asignaciones de direcciones dentro de esa red.

Este documento describe la asignación de direcciones en las redes privadas. La asignación permite la completa conectividad de nivel de red entre todas las máquinas de la empresa así como entre todas las máquinas públicas de diferentes empresas. El coste de usar un espacio privado de direcciones de Internet es el coste potencial del esfuerzo de reasignar las direcciones de las máquinas y redes de públicos a privados.

2. Motivación

Con la proliferación mundial de la tecnología TCP/IP, incluso fuera de la propia Internet, un creciente número de empresas no conectadas usan esta tecnología y sus capacidades de direccionamiento únicamente para las comunicaciones internas, sin intención alguna de en algún momento conectarse directamente a otras empresas o a la propia Internet.

Internet ha crecido más allá de todas las previsiones. El continuo crecimiento exponencial continúa presentando nuevos retos. Uno de los retos es la constancia dentro de la comunidad de que el espacio de direcciones globalmente únicas se agotará. Un asunto distinto y bastante más acuciante es que la sobrecarga de encaminamiento crecerá más allá de las capacidades de los "Proveedores de Servicios de Internet", Internet Service Providers (ISP). Dentro de la comunidad existen iniciativas en curso para encontrar soluciones duraderas para ambos problemas. Mientras tanto es necesario reconsiderar los procedimientos de asignación de direcciones, y su impacto en el sistema de encaminamiento de Internet.

Para contener el aumento en la sobrecarga de encaminamiento, un proveedor de Internet obtiene un bloque de espacio de direcciones de un registro de direcciones, y entonces asigna a sus clientes direcciones de ese bloque según las necesidades de cada cliente. El resultado de este proceso es que las rutas hacia muchos clientes pueden ser agrupadas, y aparecerán a los demás proveedores como una sola ruta [RFC1518], [RFC1519]. Para que esta agregación de rutas sea efectiva, los proveedores de Internet animarán a los clientes que se unan a su red a usar el bloque de direcciones del proveedor, y en consecuencia a renumerar sus máquinas. En el futuro, lo que ahora es una recomendación podría convertirse en una obligación.

Con el actual tamaño de Internet y su ritmo de crecimiento ya no es realista asumir que por el hecho de obtener una dirección IP globalmente única de un registro de Internet, la organización que consiga dicha dirección dispondrá de conectividad IP en todo Internet una vez dicha organización se conecte a Internet. Todo lo contrario, es bastante probable que cuando la organización se conecte a Internet para alcanzar conectividad IP global en Internet la organización tenga que cambiar las direcciones IP (renumerar) todas sus máquinas públicas (las máquinas que necesitan conectividad IP global en Internet), independientemente de si las direcciones inicialmente usadas por la organización eran globalmente únicas o no.

Ha sido típico asignar direcciones globalmente únicas a todas las máquinas que usan TCP/IP. Para prolongar la vida del espacio de direcciones IPv4, los registros de direcciones solicitan más justificaciones que nunca, haciendo más difícil que las organizaciones obtengan espacios de direcciones adicionales [RFC1466].

Se pueden dividir en tres categorías las máquinas que usan IP dentro de las empresas:

Categoría 1: máquinas que no necesitan acceder a máquinas en otras empresas, o Internet en general; las máquinas dentro de esta categoría pueden usar direcciones IP que sean

únicas dentro de la empresa, pero que pueden no ser únicas entre empresas.

Categoría 2: máquinas que necesitan acceso a un conjunto reducido de servicios externos (por ejemplo, e-mail, FTP, news, login remoto) que pueden ser gestionados por pasarelas intermedias (por ejemplo, pasarelas de nivel de aplicación). Para muchas máquinas en esta categoría, un acceso sin restricciones al exterior (el proporcionado por la conectividad IP) puede ser innecesario e incluso no deseable por razones de seguridad y/o privacidad. Como en el caso de las máquinas en la primera categoría, tales máquinas pueden usar direcciones IP que sean únicas dentro de la empresa, pero que puedan ser ambiguas entre empresas distintas.

Categoría 3: máquinas que necesitan acceso de nivel de red hacia el exterior de la empresa (proporcionado mediante la conectividad IP); las máquinas en esta última categoría necesitan direcciones IP que sean globalmente únicas.

Nos referiremos a las máquinas en la primera y segunda categorías como "privadas". Nos referiremos a las máquinas en la tercera categoría como "públicas".

Muchas aplicaciones necesitan conectividad sólo dentro de una empresa y no necesitan conectividad externa (fuera de la empresa) para la mayoría de las máquinas internas. En frecuente que en las grandes empresas sea sencillo identificar un considerable número de máquinas usando TCP/IP que no necesitan conectividad de nivel de red fuera de la empresa.

Algunos ejemplos donde la conectividad externa podría no ser necesaria son:

- Un gran aeropuerto que tiene sus pantallas de llegadas y salidas direccionables individualmente mediante TCP/IP. Es muy improbable que estas pantallas necesiten ser directamente accesibles desde otras redes.

- Grandes organizaciones como bancos y cadenas de pequeños comercios que estén cambiando a TCP/IP para sus comunicaciones internas. El elevado número de puestos locales tales como cajas registradoras, dispensadores de efectivo, y equipamiento en otros puestos raramente necesitan disponer de tal conectividad.

- Por razones de seguridad, muchas empresas usan pasarelas de nivel de aplicación para conectar sus redes internas a

Internet. A menudo las redes internas no tienen acceso directo a Internet, y sólo una o más pasarelas son visibles desde Internet. En este caso, la red interna puede usar números de red IP no únicos.

- Las interfaces de los encaminadores en una red interna a menudo no necesitan ser directamente accesibles desde fuera de la empresa.

3. Espacio de direcciones privado

La "Autoridad de Números Asignados en Internet", Internet Assigned Numbers Authority (IANA), ha reservado los tres siguientes bloques de direcciones IP para el uso en internets privadas:

10.0.0.0 - 10.255.255.255 (prefijo 10/8)
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

Nos referiremos al primer bloque como "bloque de 24 bits", al segundo como "bloque de 20 bits" y al tercero como "bloque de 16 bits". Dese cuenta que (en la notación anterior a CIDR) el primer bloque no es más que un único número de red de clase A, mientras que el segundo bloque es un conjunto de 16 números de red de clase B contiguos, y el tercer bloque es un conjunto de 256 números de red de clase C contiguos.

Una empresa que decida usar direcciones IP del espacio de direcciones definido en este documento puede hacerlo sin tener que coordinarse con la IANA o con un registro de Internet. De esta manera el espacio de direcciones puede ser usado por muchas empresas. Las direcciones de este espacio de direcciones privado sólo serán únicas dentro de la empresa, o el conjunto de empresas que elijan colaborar sobre este espacio para que puedan comunicarse con las demás en su propia internet privada.

Como antes, cualquier empresa que necesite espacio de direcciones globalmente único necesita obtener tales direcciones de un registro de Internet. Una empresa que solicite direcciones IP para su conectividad externa nunca recibirá direcciones de los bloques definidos arriba.

Para usar el espacio de direcciones privado, una empresa necesita determinar qué máquinas no necesitan disponer de conectividad de nivel de red hacia el exterior de la empresa en un futuro previsible y así poder clasificarlas como privadas. Tales máquinas usarán el espacio de direcciones privado definido anteriormente. Las máquinas privadas pueden comunicarse con el resto de máquinas de la empresa, tanto públicas como privadas. Sin embargo, no pueden tener conectividad IP a ninguna máquina fuera de la empresa. Aunque no

dispongan de conectividad IP externa (fuera de la empresa), las máquinas privadas aún pueden tener acceso a servicios externos mediante el uso de pasarelas (por ejemplo, pasarelas de nivel de aplicación).

El resto de máquinas serán públicas y usarán espacio de direcciones globalmente únicas asignadas por un registro de Internet. Las máquinas públicas pueden comunicarse con otras máquinas dentro de la empresa, tanto públicas como privadas, y pueden tener conectividad IP con máquinas públicas fuera de la empresa. Las máquinas públicas no tienen conectividad con las máquinas privadas de otras empresas.

Cambiar una máquina de privada a pública o viceversa implica un cambio de dirección IP, cambios en las entradas DNS correspondientes, y cambios en los ficheros de configuración de otras máquinas que referencien a la máquina por su dirección IP.

Puesto que las direcciones privadas no tienen significado global, la información de encaminamiento acerca de las redes privadas no se propagará en los enlaces entre empresas, y los paquetes con direcciones origen o destino privadas no deberían ser reenviados por dichos enlaces. Se supone que los encaminadores en las redes que no usen espacio de direcciones privados, especialmente aquéllos situados en los proveedores de servicios de Internet, estarán configurados para rechazar (filtrar) la información de encaminamiento acerca de redes privadas. Si uno de estos encaminadores recibe tal información, el rechazo no será tratado como un error en el protocolo de encaminamiento.

Las referencias indirectas a tales direcciones deberán quedar limitadas a los límites de la empresa. Ejemplos significativos de estas referencias son los "Registros de Recursos DNS", DNS Resource Records, y otra información importante acerca de las direcciones privadas internas. En particular, los proveedores de servicios de Internet deberían tomar medidas para evitar dichas fugas de información.

4. Ventajas y desventajas de usar espacio de direcciones privado

La ventaja obvia de usar espacio de direccionamiento privado de manera global es conservar el espacio de direcciones globalmente únicas no usando estas direcciones donde no sea necesaria esta unicidad.

Las propias empresas también obtendrán ciertas ventajas por el uso del espacio de direccionamiento privado: ganan gran flexibilidad en el diseño de la red al tener más espacio de direcciones a su disposición del que dispondrían obteniendo direcciones globalmente únicas. Esto permite esquemas de direccionamiento operacional y administrativamente provechosos, así como una sencilla escalabilidad.

Por diversas razones, en Internet se han dados casos en los que una empresa que no está conectada a Internet ha usado direcciones IP para sus máquinas sin haberlas solicitado previamente a la IANA. En algunos casos este espacio de direcciones ya ha sido asignado a otras empresas. Si posteriormente tal empresa se conecta a Internet, esto podría potencialmente crear problemas muy graves, puesto que el encaminamiento IP no puede funcionar correctamente en presencia de direccionamiento ambiguo. Aunque en principio los proveedores de servicios de Internet deberían protegerse de tales errores mediante el uso de filtros de rutas, en la práctica no siempre sucede así. El uso del espacio de direcciones privado proporciona una elección segura para tales empresas, evitando conflictos cuando sea necesaria la conectividad externa.

Uno de los principales inconvenientes del uso de direcciones privadas es que puede reducir la flexibilidad de la empresa para salir a Internet. Cuando se compromete a usar direcciones privadas, se está comprometiendo a renumerar parte o toda la empresa, si se decidiera a proporcionar conectividad IP entre esa parte (o toda la empresa) e Internet. A menudo el coste de renumerar puede medirse contando el número de máquinas que deben pasar de privado a público. Sin embargo, como se discutió previamente, incluso si una red usa direcciones globalmente únicas, aún puede ser necesario tener que renumerar para lograr conectividad IP hacia todo Internet.

Otro perjuicio de usar espacio de direcciones privado es que puede obligar a renumerar cuando se unan varias redes privadas en una única red física privada. Si revisamos los ejemplos enumerados en la sección 2, nos daremos cuenta que las compañías tienden a unirse. Si previamente a la unión dichas compañías mantuviesen sus propias redes usando direccionamiento privado, entonces si después de la unión estas redes se combinasen en una sola, algunas direcciones dentro de la red combinada podrían no ser únicas. Como resultado, las máquinas con dichas direcciones deberían ser renumeradas.

El coste de la renumeración también puede ser reducido por el desarrollo y despliegue de herramientas que faciliten la renumeración (por ejemplo, "Protocolo de Configuración Dinámica de Máquinas", Dynamic Host Configuration Protocol (DHCP)). Cuando se esté planteando si usar direcciones privadas, recomendamos consultar a los fabricantes de hardware y software sobre la disponibilidad de dichas herramientas. Un esfuerzo separado del IETF (PIER Working Group) está intentando documentar completamente los requisitos y procedimientos para la renumeración.

5. Consideraciones operacionales

Una estrategia posible es diseñar primero la parte privada de la red y usar el espacio de direcciones privado para todos los enlaces

internos. Entonces, planificar las subredes públicas en las localizaciones necesarias y diseñar la conectividad externa.

Este diseño no tiene porqué ser indefinidamente fijo. Si posteriormente un grupo de una o más máquinas necesita cambiar su status (de privado a público, o viceversa), esto se puede hacer renumerando sólo las máquinas involucradas, y cambiando la conectividad física en caso necesario. En localizaciones donde dichos cambios sean previsibles (salas de ordenadores, etc.), es aconsejable configurar medios físicos separados para las subredes pública y privada, y así facilitar tales cambios. Para evitar intervenciones de importancia en la red, es aconsejable agrupar en sus propias subredes máquinas con similares necesidades de conectividad.

Si se puede diseñar un adecuado esquema de división en subredes que esté soportado por el equipamiento implicado, es aconsejable usar el espacio privado de direcciones del bloque de 24 bits (red de clase A) y diseñar un plan de direccionamiento con un buen camino de crecimiento. Si el hacer las subredes es problemático se puede usar el espacio de direcciones del bloque de 16 bits (redes de clase C) o del bloque de 20 bits (redes de clase B).

Se podría estar tentado de tener tanto direcciones públicas como privadas en el mismo medio físico. Aunque es posible, existen riesgos en tales diseños (dese cuenta que los riesgos no tienen nada que ver con el uso de direcciones privadas, sino que son debidos a la presencia de múltiples subredes IP en una misma subred física de datos). Aconsejamos prudencia cuando se trabaje en estos supuestos.

Se recomienda encarecidamente que los encaminadores que conectan las empresas a las redes externas se configuren con los filtros de paquetes y rutas adecuados en ambos extremos del enlace para evitar fugas de paquetes e información de encaminamiento. Una empresa también debería aislar a cualquier red privada de la información de encaminamiento entrante para protegerse a sí misma de situaciones de encaminamiento ambiguas que pueden presentarse si las rutas hacia el espacio de direcciones privadas apunta hacia fuera de la empresa.

Es posible que ambos sitios, que coordinan sus respectivos espacios de direcciones privadas, se comuniquen con el otro sobre una red pública. Para hacer esto deben usar algún método de encapsulamiento en sus fronteras con la red pública, manteniendo privadas sus direcciones privadas.

Si dos (o más) organizaciones implementan la asignación de direcciones especificada en este documento y más tarde desean establecer conectividad IP con las demás, existe el riesgo de que la unicidad en las direcciones pueda violarse. Para minimizar el riesgo es altamente recomendable que una organización que use direcciones IP privadas elija aleatoriamente de la lista de direcciones privadas,

cuando asigne sub-bloques en su asignación interna.

Si una empresa usa espacio de direcciones privado, o una mezcla de espacios de direcciones privado y públicos, entonces los clientes DNS externos a la empresa no deberían ver direcciones en el espacio de direcciones privado usado por la empresa, puesto que estas direcciones serían ambiguas. Una manera de asegurarse de esto es disponer de dos servidores de nombres autorizados para cada zona DNS que contengan las direcciones tanto públicas como privadas de las máquinas. Un servidor sería visible desde el espacio de direcciones público y contendría sólo el subconjunto de direcciones de la empresa alcanzables mediante direcciones públicas. El otro servidor sería alcanzable sólo desde la red privada y contendría el conjunto completo de datos, incluyendo las direcciones privadas y cualesquiera otras direcciones públicas alcanzables desde la red privada. Para asegurar la consistencia, ambos servidores deberían configurarse a partir de los mismos datos, de los cuales la zona públicamente visible sólo contiene una versión filtrada. Hay cierto grado de complejidad adicional asociada con la provisión de estas capacidades.

6. Consideraciones de seguridad

Las consideraciones de seguridad no se tratan en este memorándum.

7. Conclusión

Con el esquema descrito muchas grandes empresas sólo necesitarán un bloque relativamente pequeño de direcciones del espacio de direcciones IP globalmente únicas. Todo Internet se beneficia del ahorro del espacio de direcciones globalmente únicas que tendrá como efecto el aumento en la vida del espacio de direcciones IP. Las empresas se benefician de la flexibilidad adicional proporcionada por un espacio de direcciones privadas relativamente grande. Sin embargo, el uso de direccionamiento privado requiere que una organización renumere parte o la totalidad de su red empresarial, puesto que sus necesidades de conectividad cambian con el tiempo.

8. Reconocimientos

Nos gustaría agradecer a Tony Bates (MCI), Jordan Becker (ANS), Hans-Werner Braun (SDSC), Ross Callon (BayNetworks), John Curran (BBN Planet), Vince Fuller (BBN Planet), Tony Li (cisco Systems), Anne Lord (RIPE NCC), Milo Medin (NSI), Marten Terpstra (BayNetworks), Geza Turchanyi (RIPE NCC), Christophe Wolfhugel (Pasteur Institute), Andy Linton (connect.com.au), Brian Carpenter (CERN), Randy Bush (PSG), Erik Fair (Apple Computer), Dave Crocker (Brandenburg Consulting), Tom Kessler (SGI), Dave Piscitello (Core Competence), Matt Crawford (FNAL), Michael Patton (BBN), y a Paul Vixie (Internet Software Consortium) su revisión y comentarios constructivos acerca del documento.

9. Referencias

[1] [RFC1466] Gerich, E., "Guidelines for Management of IP Address Space", RFC 1466, Merit Network, Inc., Mayo 1993.

[2] [RFC1518] Rekhter, Y., and T. Li, "An Architecture for IP Address Allocation with CIDR", RFC 1518, Septiembre 1993.

[3] [RFC1519] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Class less Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, Septiembre 1993.

10. Direcciones de los autores

Yakov Rekhter
Cisco systems
170 West Tasman Drive
San Jose, CA, USA
Phone: +1 914 528 0090
Fax: +1 408 526-4952
EMail: yakov@cisco.com

Robert G Moskowitz
Chrysler Corporation
CIMS: 424-73-00
25999 Lawrence Ave
Center Line, MI 48015
Phone: +1 810 758 8212
Fax: +1 810 758 8173
EMail: rgm3@is.chrysler.com

Daniel Karrenberg
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam, the Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090
EMail: Daniel.Karrenberg@ripe.net

Geert Jan de Groot
RIPE Network Coordination Centre
Kruislaan 409
1098 SJ Amsterdam, the Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090

EMail: GeertJan.deGroot@ripe.net

Eliot Lear
Mail Stop 15-730
Silicon Graphics, Inc.
2011 N. Shoreline Blvd.
Mountain View, CA 94043-1389
Phone: +1 415 960 1980
Fax: +1 415 961 9584
EMail: lear@sgi.com

Traducción al castellano:

José Luis Domingo López
c/ Cruz del Sur 22
28007 Madrid - España

EMail: jdomingo@internautas.org
