Revisión	Fecha	Comentario	Autor
0	24/06/2009		Ulises Bigliati

ÍNDICE

Introducción

Mediante la presente nota, nos dirigimos a quienes necesiten incorporar conectividad de red en sus sistemas (que podrían ser embebidos o no) suponiendo que uno de sus requerimientos es que su equipo pueda ser accedido desde cualquier parte del mundo y asumiendo que el sistema en cuestión estaría conectado a una red de área local vinculada a Internet mediante un router, ya que así sucede en el común de los casos.

Conceptos necesarios

Conocimientos básicos de networking y el stack de protocolos TCP/IP.

Objetivos

- Describir el procedimiento que permitiría lograr la conectividad buscada, utilizando para esto el servicio gratuito que prestan proveedores tales como DynDNS (http://www.dyndns.com/)

Fuera de alcance

No es objeto de esta nota explicar las bases teóricas de los servicios utilizados para lograr el objetivo propuesto. Tampoco lo es la explicación de procesos administrativos relativos al manejo de las cuentas de usuario obtenidas de parte de los diferentes proveedores del servicio DDNS. Tampoco se detallan aspectos relativos a la configuración de firewalls.

Escenario

Tal como mencionábamos al comienzo, asumimos una situación similar a la siguiente:
Se dispone de un establecimiento en el cual funciona una red LAN (local area network). En dicho establecimiento, los usuarios de computadoras conectados a esa red tienen acceso a Internet. Para esto algún humano habrá contratado oportunamente los servicios de algún ISP (Internet service provider), que utilizando el medio físico correspondiente ha proporcionado una conexión sobre la cual seguramente actuará algún módem, que mediante el procedimiento adecuado (acorde a la naturaleza del servicio contratado), establecerá un enlace de red con algún punto remoto en la red de nuestro ISP. Así la LAN de nuestro hipotético establecimiento estará vinculada a la red de redes. Pero hasta ahora solo nombramos al modem, es decir que todavía no llegamos a la red local, y los usuarios están ansiosos por navegar. Para esto necesitamos un elemento adicional que distribuya la conexión tan preciada entre todos los usuarios de la red local. Por supuesto, este elemento es un router, que valiéndose de un mecanismo llamado NAT (network address translation) es capaz de multiplexar/demultiplexar una conexión entre varias terminales. Detalles mas o menos, la descripción anterior corresponde al escenario que nos servirá de ejemplo.

Fig.1

Ahora bien, siguiendo con el ejemplo, de pronto surge la necesidad de instalar un dispositivo que puede fácilmente ser conectado a la red local para ofrecer algún servicio, utilizando por ejemplo, TCP/IP como protocolos de transporte y red. Y esto es llevado a cabo sin problemas, y con tanto éxito que ahora se desea extender geográficamente hablando las prestaciones de ese servicio, es decir que se quiere acceder al sistema desde puertas afuera del establecimiento, desde la base Marambio, por ejemplo.
Y vemos que por un lado, no parece haber inconveniente, dado que la comunicación se establece vía TCP/IP, sin embargo, tenemos dos aspectos a solucionar:

a) Nuestro proveedor de internet, nos proporciona una dirección IP que no es siempre la misma, y varía periódicamente.
b) Aunque logremos el direccionamiento necesario, no hay que olvidar que nuestro dispositivo se encuentra detrás de un router, por lo tanto las comunicaciones irían dirigidas hacia la dirección IP del router, quien interpretará como propios esos paquetes y allí acabaría la cosa.

El esquema de resolución de nombres

Antes de darle solución a los dos puntos conflictivos que detectamos en el apartado anterior, conviene recordar como funciona el mecanismo de resolución de nombres en direcciones para que los recursos puedan ser accedidos en internet.
Para los humanos es fácil asociar nombres con los objetos que representan y no lo es tanto asociar números con esos objetos. Pero resulta que los sistemas de telecomunicaciones insisten en seguir usando números para el direccionamiento.
Pare resolver este conflicto de intereses, se definió el sistema de nombres de dominio (DNS) que permite realizar la asociación nombre-dirección de forma transparente. Así, cuando se solicita un recurso que reside en la red de redes utilizando un nombre de dominio, se producen una serie de pasos a partir de esa petición tendientes a traducir ese nombre en una dirección de internet, y es acá donde entra en juego el DNS:

1º) Se busca en un caché local a la aplicación que solicita el recurso (por ejemplo un browser).
2º) Si falla lo anterior, se interroga al sistema operativo que también mantiene un caché local.
3º) Si falla lo anterior, tiene lugar la consulta a los servidores del DNS de nuestro ISP.

Nuestro ISP nos asigna sus direcciones normalmente mediante DHCP en el momento de establecer el enlace de red. Es así como nuestro sistema operativo obtiene el conocimiento de las direcciones de esos servidores DNS y puede consultarlos en cualquier momento. Las consultas a servidores DNS son cursadas a través de un esquema jerárquico de servidores de nombres, así es que pueden generarse varias "interconsultas" entre servidores antes de que nuestro sistema operativo obtenga la respuesta.
Finalmente, una vez que el S.O. recibe la dirección IP buscada, esta es regresada al proceso que la pidió, y recién ahí se comienza la comunicación con el recurso de red.

DNS dinámico

Bajo el subtítulo anterior mencionamos de que manera se obtiene la dirección de un recurso de internet para interactuar con el.
Ahora, volviendo a nuestro escenario hipotético de la figura 1, recordemos que teníamos un sistema conectado a una LAN y que queremos que sea accesible desde cualquier parte del mundo.
En virtud de lo dicho, lo que necesitamos es dar de alta un nombre de dominio en un servidor DNS para que al ser consultado devuelva la dirección IP de nuestro sistema.
Sin embargo, teníamos dos problemas, y uno de ellos afecta directamente al esquema de DNS descripto, ya que, la dirección IP que nos asigna nuestro ISP cambia impredeciblemente.
Aquí es cuando entra en juego el DNS dinámico, que no es ni mas ni menos que el mismo sistema, con el agregado de un mecanismo de actualización en tiempo real de la dirección IP en el registro de asociación "nombre-IP" que mantiene el servidor de nombres en el cual nos hayamos registrado.
Este mecanismo se implementa mediante una sencilla aplicación cliente-servidor cuya parte cliente debe ejecutarse en algún host de la red local que queremos hacer accesible al mundo, y cuya parte servidor reside obviamente en las instalaciones del prestador del servicio de DNS Dinámico al cual nos estaríamos suscribiendo.

Suscripción al servicio de DNS dinámico

Llegamos al punto en el que, a pesar de no tener una IP pública fija, podemos lograr que mediante un nombre de dominio, nuestro sistema pueda ser accedido desde internet en cualquier momento. Sabemos que necesitaremos suscribirnos a un servicio de DNS dinámico, entonces debemos buscar uno que sea gratuito, y los mas reconocidos son los siguientes aunque hay muchos más:

- DynDNS www.dyndns.com
- No-IP www.no-ip.com

DynDNS es el que está siendo mayormente difundido y por lo tanto dispone de un mayor soporte entre los diferentes fabricantes de hardware, que como ya veremos será una de las alternativas a la hora de poner en marcha el servicio, (es decir, la del cliente DDNS embebido).

Los detalles de la creación de la cuenta de usuario con el proveedor elegido quedan fuera del alcance de esta nota. Lo que debemos considerar aquí es que al crear esa cuenta podremos obtener los siguientes datos que usaremos luego para poner en funcionamiento el servicio, a saber:

- Nombre de usuario: (Se establece al crear la cuenta con el proveedor de DDNS)
- Contraseña: (Se debe especificar al crear la cuenta)
- Nombre de dominio: (Nombre de host elegido en el sitio de administración del proveedor)

Una vez activada la cuenta con nuestro proveedor de DDNS, y podamos disponer de esos datos, con ellos estaremos en condiciones de acceder al servicio, es decir, podremos publicar los recursos de nuestra LAN en Internet gracias a la asociación de su dirección IP pública con el nombre de dominio especificado durante la creación de la cuenta, teniendo la seguridad de que la dirección IP vinculada a nuestro nombre de dominio siempre estará actualizada aunque nuestra dirección IP cambie permanentemente.

El cliente DDNS

Bien, hasta ahora, ya sabemos como resolver el problema de la IP fija, en consecuencia obtuvimos una cuenta en DynDNS o similar y tenemos los datos necesarios para activar el servicio, y ahora?
Hay básicamente dos opciones:

1) Correr el programa cliente DDNS provisto en forma gratuita por el proveedor.
   El programa se debe correr en forma continua en cualquiera de los hosts conectados a la red local, se le deben suministrar los datos consignados y en forma periódica o cuando ocurra algún cambio este cliente se encargará de mantener la IP pública actualizada en el servidor de nombres del proveedor DDNS.

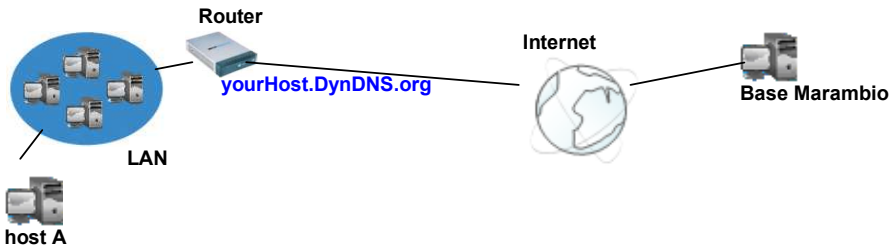
2) Si fuera posible, utilizar el cliente DDNS del router que vincula nuestra LAN a internet.
   En la actualidad, casi todos los routers poseen un cliente DynDNS embebido, e incluso de otros proveedores, si así fuera, es conveniente utilizar esta opción, por lo tanto, primero habría que verificar que clientes incorpora el router para obtener la cuenta con el proveedor correspondiente. Así que bastaría especificar los datos obtenidos al suscribirse al servicio en el propio router y así podríamos olvidarnos de correr el programa cliente en un host de la red en forma permanentemente. A modo de ejemplo, podemos ver a continuación la interfaz de configuración de DDNS en un router Linsys:

Tal como puede apreciarse la opción 2 parece ser la más apropiada para la mayoría de los casos, no obstante existen algunas configuraciones que podrían justificar la opción 1 aunque se dispusiera de un router con la funcionalidad en cuestión.

Port forwarding

Prácticamente ya tenemos la funcionalidad buscada, pero aún nos queda un problema por resolver, pues si todo salió bien, desde la Base Marambio ya pueden hacer un ping al nombre de host que definimos en la cuenta DDNS y ese ping será felizmente respondido por nuestro router (asumiendo que no hay restricciones de seguridad al respecto).

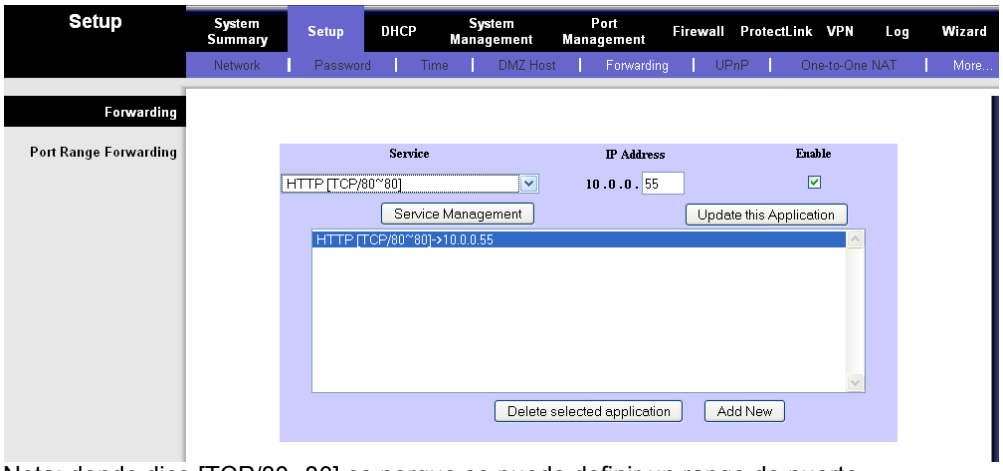
Pero en principio, nosotros no queríamos publicar servicios ofrecidos por el router, sino, por algún otro sistema residente puertas adentro, en nuestra LAN, como por ejemplo, podría ser algún sistema embebido, construido sobre la base de un módulo Rabbit, digamos, y ya que estamos digamos que ese sistema está corriendo un servidor HTTP en el puerto 80 mediante el cual se ofrece algún servicio particular.
Tal como está la cosa, cuando un ciudadano en la Base Marambio intente conectarse con un browser al recurso http://yourHost.DynDNS.org, obtendrá un error, a menos que explícitamente hayamos configurado nuestro router para que exponga su interfaz de configuración web al resto del mundo, lo cual no sería muy recomendable. Lo que necesitamos es que el ciudadano antártico invocando la dirección representada por **yourHost.DynDNS.org** llegue hasta la interfaz de red del "host A" que está conectado a la LAN y tiene acceso a internet mediante el router.



Para lograr esto, que es lo único que nos falta, debemos configurar la funcionalidad de "port forwarding" que está presente en todo router. Para ello debemos conocer:

- La dirección IP que el host utiliza en la LAN, por lo tanto aquella no debe variar y hay que definirla fija (ej. 192.168.1.100).
- El servicio o aplicación que estamos exponiendo, y en virtud de esto, el protocolo de transporte y el puerto de protocolo que utiliza (ej. HTTP, TCP, puerto 80).

Con estos datos, ingresamos en la interfaz de configuración del router y definimos:
Todo paquete IP procedente del exterior que intente ingresar a la LAN que contenga el protocolo TCP y tenga como destino el puerto 80, será "forwardeado" al host con dirección IP 192.168.1.100, puerto 80
Por ejemplo, en nuestro router Linksys, esto es:



Nota: donde dice [TCP/80 ~80] es porque se puede definir un rango de puerto.

Firewalls

Adicionalmente habrá que configurar el firewall que posiblemente esté actuando en el router para evitar que este bloquee todo tráfico proveniente desde WAN, ya que posiblemente este activado esta opción esté activada por defecto. Si el sistema que se está exponiendo a la web fuera ejecutado en PC, también habría que asegurarse de que el firewall que posiblemente esté ejecutandose en el S.O. no bloquee el puerto de protocolo en cuestión.

Resúmen

Podemos resumir lo desarrollado hasta ahora en pocas líneas:
Cuando se requiere exponer en internet un equipo conectado a una red de área local, de debe considerar que la IP que nos asigna nuestro ISP no es fija, y además, que dicho equipo estará conectados mediante un router.
La solución es crear una cuenta suscribiéndose al servicio de DNS dinámico de alguno de los proveedores que existen en el ercado y que brindan este servicio en forma gratuita, tal como puede ser DynDNS. Una vez creada la cuenta tendremos un nombre de dominio, un nombre de usuario y un password que utilizaremos para configurar un cliente DDNS, pudiendo ser el que esté embebido en el router o el software provisto por el proveedor para correr en PC. Una vez configurado el cliente, el nombre de dominio elegido podrá ser accedido desde internet, solo resta configurar el forwardeo de puertos en el router de forma adecuada según se requiera conforme al servicio publicado (HTTP => TCP/80, FTP=>TCP/21, etc.). Se debe asegurar también que el sistema a exponer en WAN posea una IP fija dentro de la LAN a fines de poder realizar el port forwarding y por supuesto que el default gateway de aquel esté apuntando al router. Por último se debe checkear que los firewalls que posiblemente estén actuando en la red no bloqueen el tráfico hacia el equipo.

Anexo: DDNS en Rabbit

Para quienes trabajan en el diseño de sistemas embebidos con Rabbit con funcionalidades basadas en TCP/IP y requieren la conexión del equipo a Internet, podría ser de interés un programa de demostración incluido en la recientemente liberada versión 10.54 de Dynamic C.
Esto es para módulos de la línea 4xxx y 5xxx y se trata de la implementación de un cliente DynDNS que podría ser muy útil si de alguna manera el módulo Rabbit se conecta a internet en forma directa, sin pasar a través de un firewall ni ser parte de una LAN en la que otros hosts pudieran correr el cliente DynDNS.