Configuración del acceso a Internet desde una LAN.

Caso práctico

Después de tantos meses estudiando las redes de ordenadores, **Tomás** ha decidido que **ya sabe todo lo necesario** sobre ellas y que ahora **puede enseñárselo a sus compañeros de oficina** para que puedan solucionar sus propios problemas. Los ha reunido para informarles de la idea que ha tenido.

—Hola a todos, como sabéis, este año he estado estudiando informática y me parece una buena idea que os transmita lo que he aprendido, para que de ahora en adelante nuestra red funcione correctamente y no tengamos problemas en nuestro trabajo diario.

—¿Qué nos vas a enseñar?

—**Os enseñare todo lo relativo a las redes de ordenadores**, yo creo que podemos empezar con 1 hora cada dos días y luego ya veremos.

—¡Muy bien! Siempre he querido saber cómo funciona nuestra red y cuáles son los mecanismos utilizados para conectarnos a Internet.

—¡Yo también quiero saber eso de los routers, el NAT y todas esas palabras raras!

—¿Has aprendido algo sobre Wimax y las tecnologías UMTS? ¿Cuándo empezamos?

—¡Y no te olvides de contarnos lo de PAT! Me iba a apuntar a un curso pero como te has ofrecido tú pues mejor todavía.

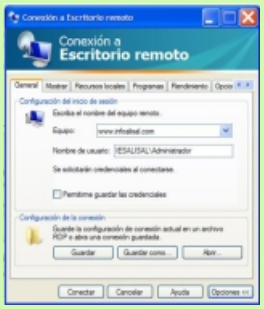
Tomás acaba de meter la pata hasta el fondo.

—¿Por qué no habré estado callado? ¿Quién me mandaría meterme en este lío?

Después de pensar cuál será su estrategia ha decidido explicarles, en la medida de lo posible, todo lo que es necesario saber sobre la configuración desde una LAN para acceder a Internet.

Direccionamiento interno y direccionamiento externo.

Caso práctico



El primer concepto que Tomás quiere dejar claro a sus compañeros el concepto de **direccionamiento**, la razón de utilizar diferentes IP y la diferencia de las direcciones IP dentro y fuera de una LAN. Esto les va a interesar mucho porque comprenderán por qué en la oficina todos pueden conectarse a Internet pagando una sola conexión y en su casa en la mayoría de los casos solamente pueden conectarse con 1 ordenador si no tienen unrouter.

—O sea, que con el router puedo hacer que nos conectemos todos con el mismo cablemódem.

—Claro, tiene la capacidad de enmascarar a los ordenadores que están en la red privada.

—¡Pues yo vivo pared con pared con mi hermano, seguro que comprando un router podemos tener una sola conexión para los dos!

—Pues sí, eso se debe a la propiedad de NAT y PAT que tienen los routers.

—¿Y las direcciones **IP**?

—Se utilizan de dos tipos, **públicas y privadas**, son dos tipos de direccionamiento.

Tomás explicará el concepto direccionamiento interno y externo a sus compañeros y les introducirá a conocer lo que es NAT y PAT. No hay duda de que el poder compartir una misma conexión a Internet es algo muy atractivo para todos.

El objetivo final del direccionamiento es identificar los elementos que forman parte de una red. En una LAN, aunque no es imprescindible, el objetivo de hoy en día es **conectarse a Internet compartiendo una sola conexión** (pagando una sola conexión). Para poder conseguir esto se necesita de las técnicas de direccionamiento y otras que oculten las direcciones interiores a las exteriores (NAT).

Para poder tener conexión a Internet se necesita hacer uso de una **dirección IP pública**, asignada por un ISP, a los ISP se les permite utilizar a su vez un número limitado de direcciones, direccionamiento externo, debido a esta limitación en la asignación, los administradores deben buscar formas de compartir el acceso a los servicios de Internet sin otorgar las limitadas direcciones IP públicas a todos los nodos en la LAN. El uso de direcciones IP privadas es la forma común de permitir a todos los nodos en una LAN acceder a los servicios de redes internos y externos. Las IP privadas se utilizan para construir un esquema de direccionamiento interno y no pueden ser utilizadas para el tráfico de Internet.

Para saber más

Puedes encontrar más información sobre las direcciones privadas en este enlace.

Direcciones privadas.

El **direccionamiento externo** se basa en técnicas que permitan encaminar los paquetes entre los routers que comunican las diferentes redes, ocultando las tecnologías de las redes LAN, en este tipo de direccionamiento se utilizan las direcciones públicas. Las direcciones IP públicas son las responsables del número de conexiones posibles en Internet, son asignadas por IANA y debido a que nunca se sospechó el brutal crecimiento de nodos conectados a la Red, siempre ha sido una preocupación su agotamiento.

Para saber más

En el siguiente enlace puedes leer un artículo que trata sobre el agotamiento de las direcciones IP.

Direcciones IP.

El router debe ser capaz de enrutar a y desde Internet, en lugar de aprender todas las rutas de Internet utilizando un protocolo de enrutamiento, puede utilizar una ruta predeterminada que lleve todos los paquetes que salen de la LAN al router del ISP y este se encargará de encontrar su destino. La principal labor del router de conexión a Internet de una LAN es simular que todos los hosts locales están usando la IP registrada públicamente, para ello se utiliza la técnica NAT y PAT (Port Address Traslation).

NAT origen y NAT destino.

Caso práctico

—Pero, ¿por qué yo puedo acceder al servidor de la oficina desde mi casa y desde la oficina no puedo acceder al ordenador de mi casa?

—¿Tienes router o directamente cablemódem?

—Tengo un router y he activado el acceso a escritorio remoto de mi equipo.

—Ya pero necesitas configurar el NAT del router para que deje pasar desde el puerto WAN al puerto LAN la comunicación por el puerto 3389.

—¿Debo configurar el NAT en el router o en el ordenador?

—En el router debes especificar que todo lo que llegue al puerto 3389 lo reenvié a la dirección IP que tiene tu equipo en tu casa.

—¿Y qué IP pongo como destino aquí en la oficina?

—Debes poner la IP del puerto WAN de tu router.

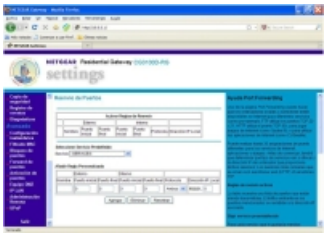
—¿Y cómo sabe el router que debe mandar la comunicación a mi ordenador?

—Por el NAT, ya verás en qué consiste.

Tomás explicará cómo funciona el NAT desde Internet a una LAN y desde la LAN a Internet, lo que formalmente se denomina NAT origen y NAT destino.

El **NAT en origen** tiene como función principal cambiar la dirección IP de origen por otra IP utilizable en el exterior de la red, al otro lado del router, se denomina también SNAT (Source NAT).

El NAT en origen se da cuando un equipo con una IP privada se comunica con otro equipo que está en Internet. Para poder solventar esto existe otro equipo de la red LAN (el que figura como puerta de enlace), que se encarga de cambiar la IP privada por la IP pública. El equipo que tiene la propiedad de cambiar las direcciones para poder "saltar" desde la parte LAN a la parte WAN suele ser un router, aunque también puede serlo un ordenador configurado adecuadamente.



La propiedad NAT se puede configurar en la práctica totalidad de los routers actuales, en la imagen anterior se puede ver la interfaz de configuración delfordwarding de un router donde se han de especificar los puertos, las direcciones y el servicio que nos interesa que atraviese el router.

Para saber más

En el siguiente vídeo podrás ver una explicación del funcionamiento de NAT.
Nociones básicas de NAT

se ha podido cargar el compleme

Resumen textual alternativo

NAT origen y NAT destino.

Una configuración posible de esta tabla podría ser la siguiente:

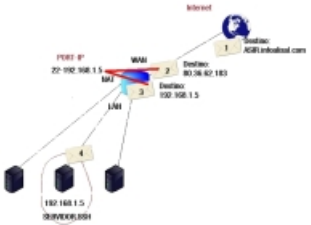
Tabla NAT

Dirección privada	Puerto privado	Dirección externa	Puerto externo	Puerto NAT	Protocolo
192.168.1.2	2045	198.235.112.1	80	14003	TCP
192.168.1.24	386	198.235.112.1	14010	80	TCP
192.168.2.1	25500	80.68.98.2	14007	21	TCP
192.168.1.254	184	180.129.33.4	14002	23	TCP

En la tabla se pueden ver diferentes campos, hay que destacar el campo **Puerto NAT**, este se utiliza para evitar que haya conexiones simultáneas a un host con todos los valores iguales (IP, puerto). Esto se puede producir cuando desde un host se hacen conexiones a un mismo servidor, al introducir el puerto NAT, evita que haya dos conexiones con valores iguales en el origen (IP, puerto) y en el destino (IP, puerto). Este proceso se conoce como **mapeo de puertos**. Esta técnica de mapeo también puede utilizarse como medida de seguridad, escogiendo como puerto destino uno que esté cerrado, y así impidiendo que la aplicación que entra no encuentre una salida, es como redirigir algo hacia un precipicio o un camino sin salida.

El NAT en destino tiene como función principal llevar hasta el equipo de la red LAN el paquete que llega a la puerta WAN del router, se denomina tambiénDNAT (Destination NAT).

La situación en la que se da **NAT en destino** es aquella en la que se tiene algún servidor en una máquina detrás de un dispositivo NAT. También se denomina fordwarding.



Un ejemplo de NAT origen y NAT destino.

El proceso sería el siguiente:

- **Un equipo de Internet (209.85.201.105) inicia una conexión solicitando una conexión vía ssh por el puerto 22 con el equipo ASIR.infoalisal.com.**
- **Consulta el DNS y obtiene como respuesta la dirección 80.36.62.183.**
- **Se establece la conexión con esta IP en el puerto 22, pero resulta que es un router con NAT y no ofrece este servicio.**
- **En el router se tendrá que crear una regla de fordwarding que obligue a que todas las peticiones hechas para ese puerto 22, se redireccionen a una IP de la red LAN donde se ofrezca ese servicio.**
- **El equipo elegido es el 192.168.1.5, por ejemplo, el router cambia la dirección destino del paquete por la 192.168.1.5.**
- **El host ASIR.infoalisal.com responde y emite un paquete cuya dirección origen es la 192.168.1.5 y la dirección de destino es la del equipo de Internet.**
- **El router recibe el paquete del equipo de la LAN y cambia en el paquete la dirección origen por su dirección pública.**

Autoevaluación

Para que los ordenadores de una red local puedan comunicarse de manera bidireccional con un servidor web alojado en Internet, el router que les da acceso a Internet debe configurarse:

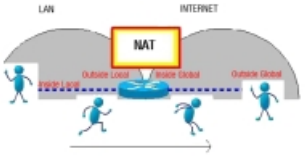
- Con NAT.
- Con PAT.
- Con PAT y NAT.
- Solamente con NAT porque es lo mismo que PAT.

Direcciones inside y outside, local y global

NAT es una tecnología que transforma las direcciones de un nodo de la red de acuerdo a la red, LAN o WAN, en la que éstas actúen, para que pueda haber comunicación. Hace corresponder una dirección privada con una pública y viceversa.

Las direcciones que intervienen en el proceso NAT, dependiendo del punto de la red desde el que se identifican, se denominan con los siguientes nombres:

- **Inside local.**
- **Inside global.**
- **Outside local.**
- **Outside global.**



Se denomina dirección inside local a la dirección que tiene el equipo en la red local (dirección privada), y la dirección inside global es la dirección pública que la red WAN ve como dirección IP de nuestro host local. La dirección outside local es la dirección que el host de la LAN ve como dirección del host remoto y la outside global es la dirección pública del host remoto.

Autoevaluación

¿Mapear un puerto es abrir un puerto?

- Sí, porque es redireccionar un servicio hacia otro puerto.
- No, el puerto destino del mapeo puede estar cerrado.
- Sí, siempre.
- No, el puerto destino de un mapeo siempre está cerrado.

NAT estático, dinámico, de sobrecarga (PAT) e inverso.

Caso práctico

—¿Y eso de PAT es lo mismo que NAT?

—Es una variante de NAT, aunque coloquialmente casi nadie lo nombra como PAT.

—¿Se utiliza mucho?

—Pues sí, de todas maneras, no es la única variante de NAT.

—¿Hay más tipos?

—Si, verás, generalmente depende de las necesidades se puede configurar uno u otro.

Tomás hablará a su compañero de los distintos **tipos de NAT, estático, dinámico, de sobrecarga e inverso.**

La diferencia entre los distintos tipos de NAT viene determinada por las correspondencias posibles entre las direcciones privadas y públicas.

Tipos de NAT

TIPO DE NAT	DIRECCIONES PRIVADAS	DIRECCIONES PUBLICAS
Estático	1	1
Dinámico	Varias	Varias
Sobrecarga	Varias	1

El tipo de NAT más sencillo, es el **NAT estático**, una dirección privada se traduce a una dirección IP pública, esta dirección pública siempre es la misma. Este NAT permite que un host tenga una dirección IP privada y sea visible en Internet.

La situación en la que es útil es aquella en la que tenemos un servidor (Web, DNS, correo) en una red local y queremos que sea accesible desde cualquier punto de Internet.

En la imagen se puede observar una situación en la que es conveniente tener esta configuración NAT.

Siempre que alguien desde Internet envía un correo al servidor mail local se utilizará la misma dirección IP que hará que llegué al servidor de correo local la petición.

Puesto que el NAT estático solamente hace posible la correspondencia 1:1 entre direcciones privadas y públicas, para mejorar el funcionamiento se diseñó el **NAT dinámico**, el fundamento es el mismo que en el caso del NAT estático pero en este caso, en lugar de una sola dirección pública, se utilizan varias direcciones públicas que están almacenadas en una tabla.

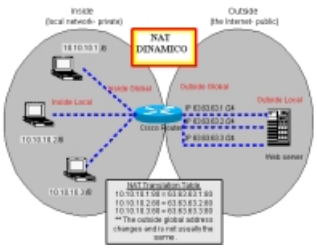
En esta tabla el router tiene una relación de posibles combinaciones entre direcciones privadas y públicas. En cada momento es posible escoger la combinación más adecuada.

El número de direcciones privadas y públicas en este tipo de NAT debe ser diferente para asegurar que el proceso sea lo más dinámico posible, con esta configuración se establece una especie de firewall entre la red pública y la privada, ya que la única conexión que se asegura es la que va desde la LAN a Internet.

La ventaja del NAT dinámico frente al estático es que se pueden tener más direcciones privadas que públicas, aunque no siempre todas las privadas podrán traducirse al tiempo en caso de que haya más direcciones privadas que públicas.

En el NAT dinámico las direcciones públicas se asignan por demanda de las privadas mientras que en el NAT estático esa asignación se hace de manera predeterminada.

NAT estático, dinámico y de sobrecarga (PAT).

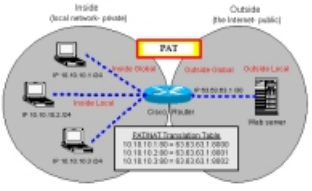


En la imagen se puede ver como se tienen 3 direcciones privadas y 3 públicas.

Se muestra la tabla de correspondencia entre direcciones privadas y públicas, esta correspondencia en un momento posterior puede variar, al contrario de lo que ocurría en el caso del NAT estático.

Para mejorar el rendimiento del NAT dinámico, se diseñó **el NAT de sobrecarga (overload)** o también denominado **PAT**. Este tipo de NAT asocia múltiples direcciones IP privadas y las traduce a una única IP pública utilizando diferentes puertos.

Este NAT, se conoce también como **NAT de única dirección** o **NAT multiplex pública**, es capaz de evitar que algún equipo de la red privada pueda quedar excluido de utilizar una IP pública, caso que se podía dar en el NAT dinámico cuando las direcciones IP privadas y las IP dinámicas no coincidían en número. Un inconveniente de esta técnica es que sólo la soportan conexiones TCP y UDP, y además las conexiones entrantes no están permitidas.



En la imagen se puede apreciar como hay más direcciones privadas que públicas, esto implicaría que solamente una de las direcciones privadas tendría conexión en la red WAN.

Para solucionar el problema, la configuración PAT utiliza distintos puertos para una misma dirección IP, con esto se consigue distinguir cada una de las conexiones requeridas por las IP privadas hacia la dirección única pública.

Para saber más

En el siguiente enlace podrás aprender más cosas sobre PAT.

PAT.

Autoevaluación

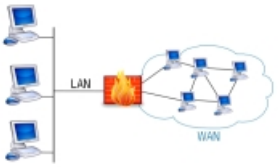
Se tiene un router, configurado con PAT que comunica una red LAN con Internet. En la parte LAN hay 4 PCs unidos directamente al router por sus puertos Ethernet y se tiene contratada una dirección IP pública con un ISP para poder navegar en Internet. Se hace un ping desde uno de los PC a la dirección http://www.infoalisal.com.

- El ping no tiene éxito porque hay más direcciones privadas que públicas.
- El ping puede que no tenga éxito porque utiliza el protocolo ICMP.
- El ping tiene éxito seguro porque es un NAT dinámico.
- Es imposible una comunicación con más direcciones privadas que públicas.

NAT Inverso.

Este tipo **funciona a la inversa de un NAT convencional**, se utiliza para poder **entrar en una LAN desde una red WAN** como Internet. Define en una tabla que a través de un determinado puerto y dirección se pueda acceder a un determinado dispositivo, también se denomina DNAT (Destination Network Address Translation).

Cuando se configura este tipo de NAT, un usuario de Internet puede alcanzar una red privada LAN desde el exterior a través de un router o firewall donde está habilitado NAT. Es útil para poder publicar en Internet servicios internos de una LAN.



Como se puede apreciar en la figura, cuando la dirección IP pública 192.0.2.1 quiere acceder al servidor instalado al otro lado del dispositivo NAT en la dirección privada 10.10.10.1, solamente lo podrá conseguir si se tiene configurado el NAT inverso (DNAT). Para las peticiones inversas, desde la red privada hacía la red pública bastará con un tipo de NAT en origen (SNAT).

Al configurar DNAT se asegura que, cuando llegue un paquete a la puerta WAN del dispositivo NAT, haya una referencia en la tabla NAT para la petición hecha desde Internet hacía la LAN y así el paquete no se descarte. En los casos en los que sí está definido NAT pero no así DNAT, la comunicación es unidireccional desde la LAN a la WAN.

Autoevaluación

Desde mi casa donde tengo instalado un router que me da acceso a Internet y quiero acceder utilizando "Conexión a Escritorio" al ordenador de mi puesto de trabajo en la red LAN del instituto:

- Debo configurar mi router con NAT y utilizar como IP destino de mi conexión la IP privada del router del instituto.
- Configuro DNAT en el router del instituto y utilizo la IP pública de la conexión de mi casa como destino de mi conexión, ya que es la única que puedo ver, la Outside Global.
- Configuro NAT en el router de mi casa y DNAT en el router del instituto.
- Configuro DNAT en el router del instituto, especificando la dirección privada de mi equipo en la LAN del instituto, junto con el puerto que soporta la petición de Conexión a Escritorio remoto.

Configuración de NAT.

Caso práctico

—¿Y esto del NAT dónde se hace?

—Pues en el router.

—¿En todos los routers?

—En los actuales se puede hacer de manera interactiva vía web y además tienen ayuda para la configuración.

—¿Y por comandos?

—También, te enseñaré como hacerlo. Verás, lo importante es que hayas comprendido como funciona.

—Creo que sí, espero que lo de los comandos sea fácil.

Tomás mostrará a su compañero como se configura NAT con comandos CLI, para que se dé cuenta de que no es algo imposible, ni para gente demasiado experta. Solamente es necesario comprender el funcionamiento porque los comandos se pueden consultar.

La configuración de NAT en un router se puede hacer desde una interfaz gráfica o con comandos CLI. Un NAT también se puede configurar en un

ordenador que esté conectado a Internet, convirtiéndolo en un router. Esta era una solución casera para poder compartir la conexión a Internet cuando los routers no eran tan accesibles como ahora.

La configuración con el interfaz web es muy intuitiva y siempre viene acompañada de ayuda en la que nos informa de como rellenar la tabla NAT.

En la configuración CLI se utiliza el comando **ip nat** añadiéndole modificadores para especificar las direcciones públicas y privadas.

La configuración de **NAT estático** tendrá que especificar una correspondencia entre una dirección IP privada y una única dirección IP pública, un ejemplo de configuración de este tipo mediante comandos CLI sería la siguiente:

```
PAR07(config)# ip nat inside source static 192.168.1.1 195.235.113.3
PAR07(config)# interface FastEthernet 0/0
PAR07(config-if)# ip nat inside
PAR07(config)# interface Serial 0/0
PAR07(config-if)# ip nat outside
```

Con la configuración anterior se hace corresponder al equipo con dirección IP privada 192.168.1.1 conectado a la interfaz Fast Ethernet 0, con la dirección IP pública 195.235.113.3 en la interfaz serie 0.

En el caso en el que haya varias direcciones privadas y públicas, se puede configurar el **NAT dinámico**, puesto que esta técnica asigna direcciones públicas según se las vayan pidiendo las direcciones privadas, deberá especificar el rango de las direcciones con las que trabaja, tanto privadas como públicas. Para especificar el rango se introduce en el comando el modificador **pool**.

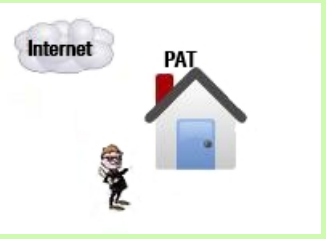
```
PAR07(config)#ip nat pool name PUBLIC 195.235.113.1 195.235.113.30 netmask 255.255.255.0
PAR07(config)#access-list 10 permit 192.168.1.0 0.0.0.255
PAR07(config)#ip nat inside source list 10 pool PUBLIC
PAR07(config)#interface FastEthernet 0/0
PAR07(config-if)#ip nat inside
PAR07(config)#interface serial 0/0
PAR07(config-if)#ip nat outside
```

Con la configuración anterior se hacen corresponder las direcciones privadas pertenecientes a la red 192.168.1.0 con el conjunto de direcciones públicas que van desde la 195.235.113.1 a la 195.235.113.30, la red privada está conectada a la interfaz tipo FastEthernet y la red pública a la interfaz serie.

Configuración de PAT.

Caso práctico

—y en nuestras casas, ¿qué tipo de NAT tenemos?



—Lo normal es la configuración PAT.

—Es decir, solamente tenemos una dirección IP pública.

—Claro, solamente pagas por una conexión.

—Pero yo miro la IP pública de mi cable módem y cambia cada cierto tiempo. ¿No sería un NAT dinámico?

—No, bueno habría que verlo para asegurarse, pero eso tiene toda la pinta de que tu dirección con el ISP es dinámica. El ISP te asigna una cada cierto tiempo pero tú solamente tienes una.

—Entonces, es posible que un NAT dinámico lo tenga configurado el ISP.

—Puede ser, pero eso es otra historia.

—Verás como configurar el PAT por línea de comandos.

Tomás enseñará a sus compañeros la manera de configurar PAT utilizando comandos CLI y les explicará el proceso que se sigue y que incluye conceptos ya vistos como las listas de acceso.

Para evitar los problemas que pudieran surgir con el NAT dinámico se puede configurar PAT. Esta técnica es la más usada por los usuarios porque permite contratar una sola dirección pública y dar servicio de conexión a varias direcciones privadas. Aparte del ahorro que supone para el usuario final, contribuye al ahorro de direcciones IP públicas.

Una configuración típica de PAT podría ser:

```
PAR07(config)# access-list 10 permit 192.168.1.0 0.0.0.255
PAR07(config)# ip nat inside source list 10 interface serial 0/0 overload
PAR07(config)#ip nat pool 1 195.235.113.1 netmask 255.255.255.0
PAR07(config)#ip nat inside source list pool 1 overload
PAR07(config)# interface FastEthernet 0/0
PAR07(config-if)# ip nat inside
PAR07(config)# interface serial 0/0
PAR07(config-if)# ip nat outside
```

Los pasos en esta configuración son:

a. Definir una lista de acceso que permita las direcciones privadas que se deben traducir.
b. Establecer la traducción dinámica de origen, especificando la lista de acceso que se definió anteriormente.
c. Establecer la dirección global como un conjunto que se usará para la sobrecarga.
d. Establecer la traducción de sobrecarga.
e. Especificar la interfaz interna.
f. Especificar la interfaz externa.

Autoevaluación

En un router en el que la interfaz de salida a Internet es la interfaz serie 0 y la interfaz que está dentro de la LAN es la ethernet 0. ¿Qué sentencia es la correcta?

- ip nat inside.
- ip nat outside
- ip pat inside.
- ip pat outside.

Diagnóstico de incidencias de NAT.

Caso práctico

—¿Y cómo se sabe si funciona el NAT?

—Para la mayor parte de los casos es fácil de comprobar, si tienes varios ordenadores en tu LAN y todos se pueden conectar a Internet, seguro que funciona correctamente.

—¿Y en los casos más complejos? ¿Servidores y accesos hacia la LAN?

—Pues los casos en los que pretendemos acceder a la LAN desde la WAN también se pueden comprobar probando, por ejemplo, un "Escritorio remoto".

—¿Hay comandos para verificar el funcionamiento?

S—i, el de siempre, el comando show.

—¿Se utiliza para todo o qué?

Bueno, lo que realmente cambia son los modificadores que lleva, en esta caso sería show ip nat.

Tomás explicará ahora a su compañero como utilizar el comando show para verificar de una manera sencilla la configuración NAT en el router con el comando show.

El resultado de una mala configuración de NAT puede comprobarse de inmediato. Por ejemplo, si no se tiene conexión a Internet desde una LAN, o puede ser un poco más laborioso, si la correspondencia entre direcciones privadas y públicas no es la deseada. En este último caso se debería usar el comando show ip nat con distintos modificadores que nos ayuden a detectar el problema.

Si se quiere ver la tabla de traducción que se tiene configurada se empleará:

```
PAR07# show ip nat translations
```

El resultado de este comando es una tabla donde se especifican las direcciones locales y globales de dentro y fuera. Para ver más estadísticas de NAT se empleará:

```
PAR07# show ip nat statistics
```

El resultado de este comando muestra las interfaces que intervienen en el NAT, las que son internas, las externas y las traducciones activas en ese momento.

Para saber más

En el siguiente enlace podrás ver un ejemplo de la salida del comando show ip nat statistics así como su interpretación.

Show ip nat statistics.

Autoevaluación

¿Se puede utilizar el comando ping para verificar el funcionamiento NAT?

- Nunca, porque utiliza el protocolo ICMP.
- En un NAT estático se puede hacer un ping desde el puerto WAN al host de la LAN.
- En un PAT se puede hacer ping desde cualquier host de la LAN a la dirección WAN del router.
- Nunca porque solamente verifica la conexión entre dos direcciones IP.

Introducción a las tecnologías WAN: Frame Relay, RDSI, ADSL.

Caso práctico

—Pues yo tengo más o menos claro cómo funciona la red LAN, pero como funciona Internet no.

—¿A qué te refieres?

—Pues que sé que en la LAN Ethernet todos los equipos compiten por el ancho de banda y que esto se soluciona con conmutadores y routers, pero no sé qué técnicas se usan en la WAN.

—ADSL, RDSI o Frame Relay son las más importantes.

—¿Qué las diferencia? ¿Se puede escoger entre una u otra?

—Bueno, puedes escoger entre lo que te ofrezcan los ISP.

Tomás explicará a su compañero las características más relevantes de las técnicas que se utilizan en las redes WAN.

Una red WAN es una red que opera fuera de una red LAN y está formada por miles de líneas de comunicación, cada una de ellas unida por routers. Si un router quiere comunicarse con otro que no está directamente accesible, debe hacerlo a través de routers intermedios. Los routers intermedios tienen la capacidad de almacenar la información de manera temporal y esperar hasta que la línea que desean utilizar esté disponible para enviar la información.

La red que funciona de acuerdo al mecanismo descrito se denomina de **almacenamiento y reenvío** o de **conmutación de paquetes**. Casi todas las redes WAN, excepto las que utilizan satélites funcionan con este mecanismo.

Para saber más

En el siguiente enlace encontrarás más información sobre la conmutación de paquetes.

Conmutación de paquetes.

La conmutación de paquetes es muy sencilla de entender, cuando un host quiere enviar un mensaje, lo divide en pedazos (paquetes) y les asigna un número para poder identificarlos. Los paquetes viajan por la red y al llegar al receptor se reorganizan de acuerdo al número que se les asignó. Estos paquetes no tienen por qué seguir la misma ruta aunque pertenezcan al mismo mensaje, esta es una de las diferencias con la técnica de conmutación de circuitos, que establece el circuito de comunicación antes de la comunicación. Dentro de la técnica de conmutación de paquetes existe la variante de circuito virtual, en la que los paquetes viajan todos por el mismo camino.

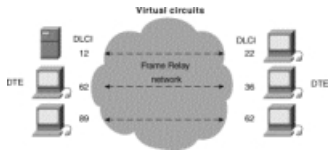
Para saber más

En el siguiente enlace encontrarás más información sobre los circuitos virtuales.

Circuito virtual.

Frame Relay.

Se diseñó como un protocolo destinado a utilizarse con las interfaces RDSI. Una red **Frame Relay** tiene como características principales que es orientada a la conexión y no tiene control de errores, ni de flujo. Estas características hacen de ella que se comporte como una especie de LAN de área



amplia, su objetivo es comunicar redes LAN utilizando la WAN, es una tunelización de la comunicación.

Esta tecnología establece un circuito virtual, permanente PVC o conmutado SVC. Después de establecer el circuito, la información se fragmenta y se le añade un identificador que sirve para marcar el circuito que debe seguir el paquete, este número se denomina DLCI (Data Link Connection Identifier).

En cada nodo se asocia cada DLCI de entrada a un puerto de salida y un nuevo DLCI hasta que los paquetes alcanzan su destino. Los números DLCI no son direcciones finales de usuarios sino referencias que determinan la ruta que deben seguir en cada nodo.

Para saber más

En el siguiente enlace encontrarás más información sobre la tecnología Frame Relay.

Frame Relay.

Un parámetro importante a tener en cuenta en las transmisiones es el caudal CIR, Committed Information Rate, que es una medida de la cantidad de información asegurada que se puede transmitir. También se denomina **caudal comprometido**. Se suele medir en bits por segundo, y es la velocidad a la que la red acuerda transferir información sobre un CVP bajo condiciones normales. Cada CVP tiene dos valores CIR independientes.

a. Del cliente a la red.
b. De la red al cliente.

En general el caudal es asimétrico, mayor en el sentido de la red al cliente, aunque existen posibilidades para que sea simétrico en las líneas como SDSL.

La llegada de otras tecnologías como MPLS, VPN, cable módem y DSL hace que Frame Relay tienda a desaparecer del mercado aunque como puedes ver en el siguiente enlace las compañías de telefonía siguen ofreciendo sus servicios.

Para saber más

En el siguiente enlace encontrarás información sobre la tecnología Frame Relay en la actualidad.

Frame Relay en los ISP actuales.

Autoevaluación

Una llamada de teléfono RTB es una comunicación:

- Por conmutación de paquetes.
- Por conmutación de circuitos.
- Por conmutación de mensajes.
- Por conmutación de celdas.

RDSI.

Red Digital de Servicios Integrados, también se denomina ISDN (término anglosajón). Es una tecnología que proporciona conectividad digital extremo a extremo, proviene de RDI (Red Digital Integrada), pero a diferencia de ésta, que solamente soporta conmutación de circuitos, soporta también conmutación de paquetes.

La mejora más relevante de RDSI respecto a la línea telefónica básica ,fue la capacidad para poder utilizar los servicios de Internet y de voz al tiempo, así como el aumento de velocidad.

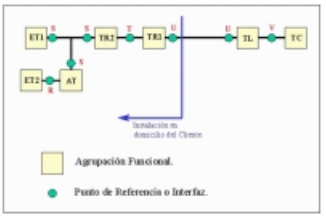
RDSI tiene dos tipos de acceso:

a. BRI.
b. PRI.

El acceso tipo BRI se compone de dos canales B y uno D (2B+D) y el acceso tipo PRI se compone en Europa de 30B+D y en Estados Unidos de 20B+D.

- **Cada canal B puede transmitir 64 Kbps.**
- **Cada canal D puede transmitir 16 Kbps.**

El acceso tipo BRI se compone de dos canales B y uno D (2B+D) y el acceso tipo PRI se compone en Europa de 30B+D y en Estados Unidos de 20B+D.



Los elementos básicos de una instalación RDSI son los que aparecen en la figura:

- **TC**: Terminación de Central, situada en la Central de Conmutación. Realiza la conexión de canales, soporta la señalización del usuario y el envío de información en modo paquete.
- **TL**: Terminación de Línea, situada en la Central, se encarga de los aspectos de transmisión. Convierte el código binario al código de línea empleado.
- **TR1**: Terminación de Red nº 1, es el primer elemento en el domicilio del Cliente lo proporciona el ISP.
- **TR2**: Terminal de red. Centralita digital que adapta los ETs a la Terminal de red (TR1). Sólo para accesos primarios donde existe una conexión física única entre cada ET y la TR2.
- **ET1**: Equipo Terminal nº 1, es el Equipo Terminal RDSI, dispositivos que soporta la conexión RDSI (teléfono RDSI).
- **AT**: Adaptador de Terminales. Convierte señales que no son RDSI en señales RDSI.
- **ET2**: Equipos que no son RDSI, a los que se les acopla un dispositivo AT para que soporten la comunicación RDSI.

Para saber más

En el siguiente enlace encontrarás más información sobre la tecnología RDSI en la actualidad.

RDSI en la actualidad.

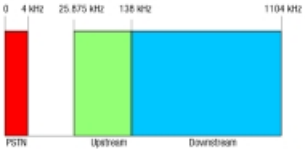
ADSL.

ADSL son las siglas de Línea de Abonado Digital Asimétrica (Asymmetric Digital Subscriber Line). La tecnología ADSL nació en las compañías telefónicas para poder competir con otras, en la transmisión de datos utilizando las instalaciones de la red telefónica existentes. Con este objetivo, el diseño de ADSL debía cumplir los siguientes preceptos:

- **Los servicios ofrecidos deberían funcionar sobre los circuitos locales existentes de par trenzado.**
- **Los servicios de fax y teléfono de los clientes no se verían afectados.**
- **La velocidad de transmisión debería ser bastante superior a los 56 Kbps.**
- **La tarificación podría ser mensual.**

La tecnología ADSL se basa en utilizar el canal disponible discriminando para diferentes servicios, se podría resumir de la manera siguiente:

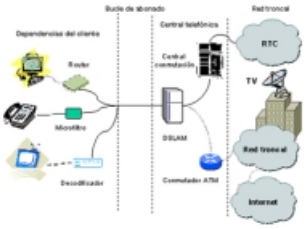
- **Dividir el espectro disponible en canales.**
- **Utilizar el canal 0 para telefonía.**
- **No utilizar los canales 1 al 5 para evitar interferencias.**
- **Utilizar un canal para el control de flujo ascendente y otro para el control de flujo descendente.**
- **Utilizar canales restantes para la transmisión de datos.**



Los ISP pueden utilizar el mismo número de canales en sentido ascendente que en sentido descendente, pero el tráfico de los usuarios es mayor en sentido descendente por lo que suelen utilizar aproximadamente el 80% de los canales para el sentido descendente y el resto para el sentido ascendente. Por eso la velocidad de bajada, (que nunca coincide con la contratada), es mucho mayor que la de subida y de ahí el nombre de **línea asimétrica**.

En la imagen se puede ver una representación de las frecuencias utilizadas en la tecnología ADSL. En rojo el ancho dedicado a la telefonía, en verde la frecuencia utilizada para el canal de subida y en azul el ancho de banda reservado en el canal para el sentido descendente desde la línea ADSL al cliente.

En la cobertura ADSL, el factor más importante es la cercanía a la central del ISP que nos ofrece el servicio, y las centrales instaladas por los ISP dependen de la demanda que haya de los usuarios, puesto que tiene unos costes muy altos cuando los usuarios son pocos. Por lo tanto, las zonas despobladas tienen mayor dificultad para poder utilizar este servicio que las zonas más densas.



En una instalación ADSL, como se muestra en la figura debe haber un dispositivo utilizado para la conexión a Internet (router), otro dispositivo para discriminar la transmisión telefónica (microfiltro) y además, si se transmite TV, un decodificador.

Toda la información viaja por el mismo canal hasta la central del ISP y allí el elemento más importante es el DSLAM.

DSLAM es el dispositivo encargado de multiplexar los datos que viajan por la línea ADSL. Es decir, es capaz de hacer que información de diferente naturaleza (voz, video, música, datos) viaje por la línea de comunicaciones sin interferencias.

Para saber más

En el siguiente enlace encontrarás más información sobre DSLAM y su importancia en la transmisión ADSL.

DSLAM.

La oferta ADSL en la actualidad es muy variada y se incluye además de conexión a Internet, televisión y teléfono, con diversas tarifas. Las velocidades ofrecidas por los operadores ADSL son, por regla general, inferiores a las ofrecidas para los operadores de cable.

Para saber más

En los siguientes enlaces podrás ver una comparativa entre los distintos operadores, incluyendo tarifas.

Operadores de ADSL y cable.

Operadores de ADSL y cable (para comparar).

La evolución de ADSL, pasando por ADSL2 ha desembocado en VDSL (Very High bit-rate Digital Subscriber Line), que permite una mayor tasa de transferencia en sentido ascendente y descendente. VDSL multiplica por dos los canales dedicados a la transmisión de datos por lo que aumenta la velocidad respecto a la ofrecida por ADSL, utiliza dos bandas de frecuencia para la subida y otras dos para la bajada, en el caso de ADSL era una banda de frecuencia para cada proceso.

En la imagen se puede ver una representación de las bandas de frecuencia utilizadas por las distintas versiones de XDSL.

VDSL actúa en unión con la tecnología de fibra óptica, reduciéndose el uso del cable de cobre casi al bucle de abonado (cientos de metros). El aumento de la fibra óptica es realmente el causante del aumento de capacidad de transmisión. El acercamiento de la fibra óptica hasta el edificio se conoce como FTTB y por lo tanto a esta tecnología se la suele denominar VDSL-FTTB.

Las tecnologías Wifi y Wimax.

Caso práctico

—¿Por qué en la oficina nos podemos conectar todos a la red inalámbrica?

—Porque tenemos montada una red Wifi.

—¿Y no se puede tener una red Wifi para toda la ciudad y así tener Internet todos?

—Sí, eso ya lo han instalado en alguna población utilizando la tecnología Wimax.

—¿Es lo mismo que Wifi?

—No exactamente, aunque es compatible.

—Pues yo creo que los políticos deberían favorecer este tipo de tecnología y que el acceso a Internet fuese gratuito.

—Bueno, por el momento se han creado redes Wifi en sitios públicos y todos los que estén en su radio de acción pueden utilizarlas.

—¿Qué diferencia hay con Wimax para que haya problemas en su instalación?

Tomás explicará a sus compañeros la diferencia entre Wifi y Wimax y las características más relevantes de ambas.

Wifi es la abreviatura de Wireless Fidelity (fidelidad inalámbrica) y es una de las tecnologías más utilizadas hoy en día para acceder a Internet a través de una LAN.

Esta tecnología está definida por el estándar IEEE 802.11 y entre sus características más importantes está la **transmisión omnidireccional**, lo que la hace ideal para que sea una tecnología capaz de recoger y enviar las transmisiones de los equipos en un radio determinado de acción. Una red Wifi está unida, por regla general, a una red de cable (la que tiene acceso a Internet).

La disposición de la figura es una disposición típica del uso de la tecnología Wifi. Se puede ver como hay una conexión a Internet (cable o DSL módem) y un dispositivo donde se agrupan todos los equipos de la red LAN (router o switch wireless).

Tanto los equipos de la red Ethernet como los que utilizan 802.11 acceden a Internet utilizando el mismo dispositivo y este lo hace por cable hasta el cable o DSL Módem.

Las tecnologías más usadas son 802.11a, 802.11b, 802.11g y 802.11n, siendo compatibles entre sí.

Las redes WiFi operan sin necesidad de licencia en las bandas de radio de 2,4 y 5 GHz, con una velocidad de transmisión de datos de 11 Mbps (802.11b) o 54 Mbps (802.11a) o con productos que contengan las dos bandas (banda dual). Pueden proporcionar un rendimiento similar a las redes cableadas 10BaseT o Ethernet.

Cualquier dispositivo al alcance del dispositivo inalámbrico de conexión (punto de acceso, switch o router inalámbrico), puede disfrutar de la conexión a Internet, esto está llevando a que esta tecnología tenga muchos usuarios, incluso en muchas ciudades ya se ofrece conexión gratuita en las inmediaciones de edificios públicos.

¿Qué pasaría si hubiera una tecnología inalámbrica capaz de emitir en un radio de acción del orden de Km? La respuesta a esta pregunta sería que todos los usuarios podrían tener acceso a Internet a través de una misma conexión, se estaría creando una especie de red local inalámbrica con las dimensiones de una MAN.

Las tecnologías Wifi y Wimax.

La respuesta está en la tecnología Wimax, que son las siglas de Worldwide Interoperability for Microwave Access, (interoperabilidad mundial de acceso por microondas). Es una tecnología que permite la recepción de datos por microondas y retransmisión por ondas de radio, basada en OFDM.

Para saber más

En el siguiente enlace puedes ver más información sobre la modulación OFDM.

OFDM.

El protocolo que caracteriza esta tecnología es el IEEE 802.16. Las microondas son ondas direccionales por lo que se necesita una visión directa entre repetidores, por otra parte el alcance con esta tecnología puede ser hasta de 80 Km. Este estándar además es compatible con Wifi aunque mucho más rápido, con velocidades del orden de la banda ancha.

La topología de una red que utilice Wimax podría ser como la que se muestra en la figura. La transmisión depende de las microondas (ondas direccionales), por lo que todos los nodos que utilicen 802.16 deberán tener visión directa con cada estación de repetición, aunque se puede dar el caso de que haya objetos que se interpongan en el camino.

Cuando hay objetos que se interponen entre la antena y el receptor, se opera con bajas frecuencias (entre los 2 y los 11 GHz), para así no sufrir interferencias por la presencia de objetos. Esto hace que el ancho de banda disponible sea menor. Las antenas para este servicio tendrán una cobertura de unos 605 Km2. Cuando no hay nada que se interponga y hay contacto visual directo, se opera a muy altas frecuencias, del orden de 66 GHz, disponiendo de un gran ancho de banda, las antenas para este servicio tendrán una cobertura de hasta 9300 Km2.

Cada estación base conecta con múltiples usuarios situados a grandes distancias a través de pequeños paneles situados en el exterior de los edificios. La instalación del panel se asemeja a la instalación de una antena parabólica. **Wimax está diseñada para operar en bandas de frecuencia con licencia**, por lo que esto si supone un impedimento para su desarrollo.

Para saber más

En el siguiente enlace puedes ver el mapa de redes Wimax en el mundo.

Wimax.

Lo último relativo a Wimax es el estándar 802.16m (Wimax2), que podría alcanzar los 300 Mbps, a pesar de que en sus inicios prometía transferencias de hasta 1 Gbps.

Autoevaluación

La diferencia entre Wifi y Wimax es:

- El alcance, debido a que Wifi utiliza microondas y Wimax ondas de radio.
- La frecuencia en la que actúan, Wimax actúa en una frecuencia más baja.
- Wimax opera con ondas de radio y microondas y Wifi solamente lo hace con ondas de radio.
- Wifi opera con infrarrojos y Wimax con microondas.

Para saber más

En el siguiente vídeo podrás ver un video sobre Wimax en una ciudad española.

Wimax en la ciudad de Sevilla.

se ha podido cargar el compleme

Resumen textual del vídeo

Las tecnologías UMTS y HSDPA.

Caso práctico

—¡A mí me gustaría saber qué sistema utiliza mi móvil para navegar por Internet!

—Pues depende de cómo sea tu móvil.

—¿Me puedo conectar a la red de la oficina para navegar?

—Sí, pero la velocidad dependerá de la tecnología de tu móvil.

—A mí me dijeron que era 3G. ¿Es bueno?

—Hay varias tecnologías, desde las más antiguas GSM, pasando por GPRS, UMTS hasta llegar a la HSDPA.

Tomás explicará las tecnologías más usadas para las comunicaciones móviles en la actualidad, tanto para los móviles como para el acceso a Internet.

UMTS (Universal Mobile Telecomunications System), Sistema Universal de Telecomunicaciones Móviles, es el sistema sucesor de las tecnologías GSM y GPRS, pertenece a la tecnología de móviles 3G (tercera generación, también llamado W-CDMA) y está perdiendo terreno respecto a su sucesor HSDPA(High Speed Downlink Packet Access).

La principal ventaja de UMTS sobre la segunda generación móvil (2G), es la capacidad de soportar altas velocidades de transmisión de datos que puede llegar a los 7,2 Mbps, aunque HSDPA puede llegar hasta los 14 Mbps.

El avance que supuso GPRS respecto a GSM, fue la posibilidad de transferir los datos en forma de paquetes en lugar de utilizar un circuito dedicado durante toda la comunicación (modo circuito), sistema empleado por los teléfonos. El paso hacia adelante que da UMTS es incorporar un subsistema de radio más avanzado que permite mayores velocidades de transmisión.

En un entorno ideal las velocidades de estas tecnologías son:

- **GPRS: 171 kbps.**
- **EDGE: 384 kbps.**
- **UMTS (3G): 2 Mbps.**
- **HSDPA: 14 Mbps.**

Donde EDGE es la conexión que tienen Blackberry y el iPhone, ideal sobre todo para descargar correos electrónicos. Para trabajar con vídeos o contenidos con mucha carga de gráficos funciona mejor UMTS o HSDPA.

Aunque estas tecnologías se diseñaron para la comunicación con teléfonos móviles, en los últimos años ha aumentado de manera significativa la movilidad en las comunicaciones, y con ello la aparición de los router-módem para comunicaciones vía Router 3G con HSDPA, UMTS, EGPRS y GPRS, estos módems tienen varios formatos y conexiones con el PC, predominando las interfaces USB.

En la imagen se puede ver el aspecto que tienen los módems que permiten el acceso a las redes móviles, en este caso se corresponde a un módem compatible con la red HSDPA y conexión USB con el PC.

Con HSDPA navegar con un portátil desde cualquier sitio utilizando estos módems debe ser similar a utilizar una conexión ADSL por cable.