Configuración del acceso a Internet desde una LAN.

Caso práctico

Después de estos meses de prácticas en la empresa trabajando y estudiando las redes de ordenadores, **Noiba** está convencida de que ya sabe todo cuanto necesita sobre ellas y que ahora estaría preparada para enseñar a sus compañeras algunas de sus conclusiones. Han quedado una tarde en una cafetería para comentar cómo les ha ido en el empresa para que cada una exponga sus conclusiones. Comienza **Noiba** explicando que ha sido muy positivo asentar los conocimientos teóricos con el trabajo práctico.

Naroba está de acuerdo y cree que ha sido un acierto por parte del profesorado asignarles esa empresa a las tres juntas, porque para ella ha sido una gran ayuda contar con **Jana** y **Noiba**.

Jana está de acuerdo en parte, porque dice que el buen ambiente de la empresa ha ayudado a ello, y especialmente la ayuda que les han prestado tanto **Laro** como **Vindio**. A pesar de todo ello cree que solo han practicado una pequeña parte de toda la teoría que han visto en clase y hay cosas que le gustaría practicar; NAT, WiMAX, UMTS, PAT...

Las tres están de acuerdo y han decidido planteárselo a **Laro** y **Víndio**, así que les llamarán para quedar a desayunar el sábado todos juntos y hablar del tema.

Esta última unidad del módulo profesional, la vamos a dedicar a asentar gran parte de los conocimientos adquiridos en unidades anteriores y a entender la importancia del direccionamiento en una red local, así como las posibilidades que supone. También veremos los sistemas de conexión de área extensa con tecnologías inalámbricas para una área metropolitana, especialmente para dispositivos móviles.

1.- Direccionamiento interno y direccionamiento externo.

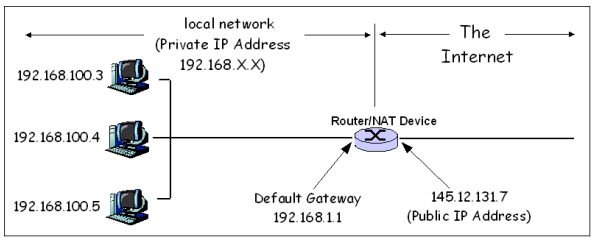
Caso práctico

Alain Bachellier (CC BY-NC-SA)

Como era de esperar **Laro** y **Vindio** están dispuestos a preparar diferentes prácticas sobre la red de la sala de formación que han montado. El primer concepto que **Vindio** quiere dejar claro es el de direccionamiento, la razón de utilizar diferentes IP y la diferencia de las direcciones IP dentro y fuera de una LAN. Esto es especialmente interesante para entender cómo se gestiona la conexión a Internet de toda la oficina, algo que también podemos llevar a casa utilizando un router. Algo que invita a hacer, aunque reconoce que muchas veces la configuración de los routers que entregan las compañías que prestan el servicio está muy limitada y siempre podemos adquirir uno propio, que no es tan caro y ofrece grandes ventajas en el hogar, pero hay que saber cuál es el más interesante.

Vindio continúa explicando los conceptos direccionamiento interno y externo, para llevarles a conocer lo que es NAT y PAT. No hay duda de que el poder compartir una misma conexión a Internet es algo muy interesante para todos, pero requiere cierto cuidado.

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).



Yangliy (Dominio público)

Para poder tener conexión a Internet se necesita hacer uso de una **dirección IP pública**, asignada por un ISP, a los que 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.

2.- NAT origen y NAT destino.

Caso práctico

Alain Bachellier (CC BY-NC-SA)

Jana tiene muy claro que esta es la situación ideal para aprender algo. Están trabajando con herramientas actuales de uso diario en la empresa, en instalaciones reales similares a las que encontrarán en cualquier situación laboral y además sus compañeros están implicados en su formación como profesionales de la informática. Y eso es algo que la empuja a aprovechar al máximo el tiempo que está con ellos, incluso está haciendo algo que no ha hecho nunca. Cuando llega a casa dedica buena parte de la tarde a llevar una especie de diario de trabajo en el que recoge todo cuanto ha aprendido y busca en Internet para ampliar conocimientos de algunos de los conceptos que han trabajado, algo que le lleva de una cosa a otra y cada vez le genera más dudas estimulando su interés por el tema.

Así lleva un buen rato intentando configurar el NAT del router, y ha descubierto que su modelo está muy limitado, no se parece en nada a los que tienen en la empresa **BK Sistemas Informáticos**.

Jana intenta entender cómo funciona el NAT desde Internet a una red y al contrario, es decir, el 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.

Netgear (Todos los derechos reservados)

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 del fordwarding 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 los siguientes vídeos podrás ver una explicación del funcionamiento de NAT y cómo se configura en los routers Cisco.

Nociones básicas de NAT (Parte 1)

Nociones básicas de NAT (Parte 2)

Nociones básicas de NAT (Parte 3)

2.1.- NAT origen y NAT destino I.

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 también DNAT (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 otro equipo.
- 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 destino 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.

Incorrecto, es insuficiente, NAT se utiliza para salir hacia Internet.

No es correcto, es insuficiente, PAT se utiliza para que los paquetes que llegan de Internet encuentren el host en la red LAN.

Correcto, aunque de manera coloquial se utiliza el término NAT para todo.

No es la opción correcta, no son términos que definan la misma técnica.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.2.- 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.

AlfBonillo. (Dominio público)

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.

Incorrecto. El mapeo cambia el puerto destino pero no puede abrir o cerrar puertos.

Correcto. El mapeo de un puerto es redireccionar hacia otro puerto, pero esto no implica que el puerto final esté abierto, eso depende del servicio que utilice ese puerto.

No es correcto. Es posible que el puerto destino esté cerrado porque en el servidor al que se intenta acceder así se haya escogido.

No es la opción correcta. El puerto destino puede estar cerrado o abierto.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

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

Caso práctico

Aprovechando que está configurando la salida a Internet de un servidor, **Naroba** pregunta a **Laro** sobre el direccionamiento que se produce al consultar desde Internet este servidor. Por ejemplo, si ella quiere acceder desde casa, cómo funciona.

Laro intenta explicar que ellos utilizan siempre un NAT dinámico, que es una gran característica de los routers, con la que permite que se utilicen diferentes correspondencias entre direcciones públicas y privadas.

Naroba dice que recuerda que habían estudiando en clase que existen diferentes tipos de NAT, pero que no tiene claro cómo funcionan y cómo se implementan de forma real.

Alain Bachellier (CC BY-NC-SA)

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.

AlfBonillo. (Dominio público)

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.

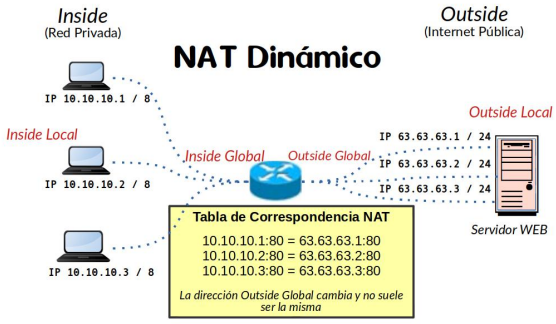
El número de direcciones privadas y públicas en este tipo de NAT debe ser diferente para asegurar que el proceso sea lo más dinámico posible, con esta configuración se establece una especie de firewall entre la red pública y la privada, ya que la única conexión que se asegura es la que va desde la LAN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

3.1.- NAT estático, dinámico y de sobrecarga (PAT).

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



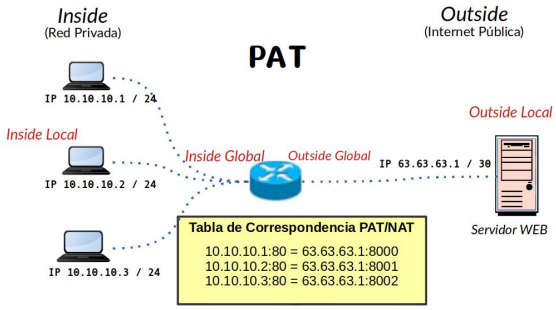
AlfBonillo. (Dominio público)

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.



AlfBonillo. (Dominio público)

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 ordenadores 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 ordenadores 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.

Incorrecta. No se puede asegurar que no tenga éxito.

Correcto. PAT solamente asegura la comunicación si se utilizan conexiones con protocolos TCP y UDP.

No es correcto. PAT se creó para mejorar el NAT dinámico, donde uno de los problemas era que las direcciones privadas fueran más que las públicas y se perdieran conexiones.

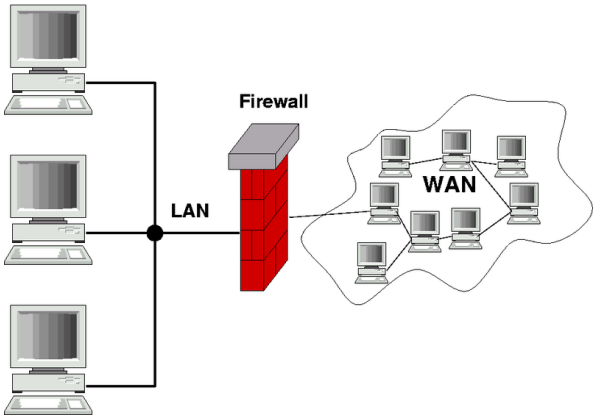
No es la opción correcta. PAT como evolución de NAT tiene como objetivo precisamente lo contrario.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

3,2.- 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, que es una variación de NAT que incluye puertos y consiste en la traducción de la dirección de red de destino.
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 red local.



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.

Incorrecto. La IP destino desde mi casa debe ser la IP pública del router del instituto.

No es correcto. Si tengo conexión a Internet, desde mi casa puedo ver cualquier IP pública.

No es la opción correcta. Si tengo conexión a Internet, no es necesario configurar NAT.

¡Muy bien! Con DNAT en el router del instituto, especifico que las peticiones que vengan al router por el puerto utilizado por Conexión a Escritorio remoto, se dirijan a la dirección privada de mi ordenador en el instituto.

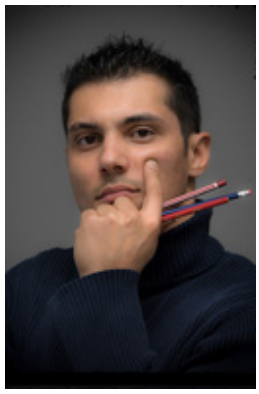
Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

4.- Configuración de NAT.

Caso práctico

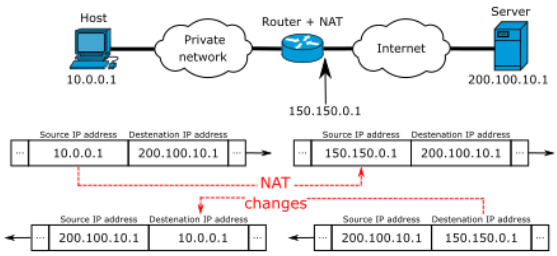
Laro explica a **Naroba** que aunque actualmente los dispositivos suelen disponer de una interfaz gráfica para su configuración a través del navegador, él prefiere hacerlo con la línea de comandos, le resulta más cómodo y se siente más seguro, aunque reconoce que en el fondo es igual porque ambos sistemas inciden sobre los mismos archivos de configuración que a la larga son los que definen el funcionamiento del dispositivo.



Alain Bachellier (CC BY-NC-SA)

En cualquier caso, y dado que está intentando que **Naroba** vea cómo funciona, le muestra ambas opciones de configuración, entrando al dispositivo mediante la interfaz gráfica del navegador y con el terminal de línea de comandos. Al final ella también prefiere esta última, porque dice que tiene la ventaja de que conociendo tres comandos, es mucho más rápido, aunque eso si, que no se te olviden, porque entonces pierdes esa ventaja de la rapidez.

La configuración de NAT en un router se puede hacer desde una interfaz gráfica o con la línea de comandos. 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.



MIchel Bakni (CC BY-SA)

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 con línea de comandos 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 la línea de comandos 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
```

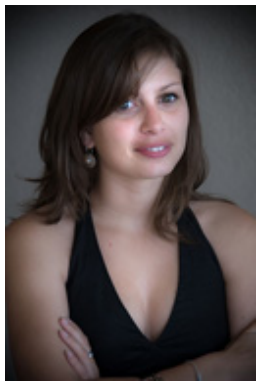
Con la configuración anterior se hacen corresponder las direcciones privadas pertenecientes a la red 192.168.1.0 con el conjunto de direcciones públicas que van desde la 195.235.113.1 a la 195.235.113.30, la red privada está conectada a la interfaz tipo FastEthernet y la red pública a la interfaz serie.

5.- Configuración de PAT.

Caso práctico

Continuando con la configuración NAT de los dispositivos de red, **Laro** explica que algunos problemas se solucionan configurando correctamente PAT, **Noiba** no tiene muy claro qué es eso del PAT. Sabe que permite que una misma dirección IP sea utilizada por varios equipos en una Intranet, pero quiere saber cómo funciona y cómo se configura de forma correcta, porque a priori, le parece una opción muy interesante para una red doméstica a la que acceder desde Internet, es decir, desde cualquier parte del mundo.

Laro enseña a sus compañeras la manera de configurar PAT utilizando la línea de comandos y les explica el proceso que se sigue y que incluye conceptos ya vistos como las listas de acceso.



Alain Bachellier (CC BY-NC-SA)

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.

AlfBonillo. (Dominio público)

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:

1.- Definir una lista de acceso que permita las direcciones privadas que se deben traducir.
2.- Establecer la traducción dinámica de origen, especificando la lista de acceso que se definió anteriormente.
3.- Establecer la dirección global como un conjunto que se usará para la sobrecarga.
4.- Establecer la traducción de sobrecarga.
5.- Especificar la interfaz interna.
6.- 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.

No es correcta. La interfaz serie está en la parte de fuera.

Correcto. La interfaz serie está en el exterior.

No es la opción correcta. El comando es nat no pat y además nos referimos a la parte de afuera.

Incorrecta. El comando es nat no pat.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

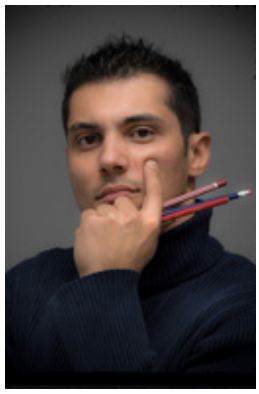
4. Incorrecto

6.- Diagnóstico de incidencias de NAT.

Caso práctico

La incidencia más habitual a la hora de configurar NAT en una red local, es que alguno de los equipos no tenga acceso a Internet. **Laro** les cuenta que en esta situación es importante tener claro cómo se realiza la correspondencia entre direcciones. Él es partidario de instalar una aplicación para compartir el escritorio de forma remota e intentar acceder a esa aplicación desde fuera de la red local, para comprobar que es posible la comunicación en la red por completo.

Pero explica a sus compañeras la utilidad del comando show, con el que comprobar esa comunicación y qué modificadores deben utilizar. Y bromea diciendo que a veces le gusta utilizar este tipo de comandos delante de los clientes para hacerse el interesante.



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.

AlfBonillo. (Dominio público)

Si se quiere ver la tabla de correspondencia 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 ejemplos del comando show ip nat así como su interpretación.

Show ip nat

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.

No es correcto.

Incorrecto. El ping hacia un host de la red privada no va a funcionar.

¡Muy bien! Respuesta correcta, si tenemos configurado PAT, todas las direcciones privadas se multiplexarán en la dirección IP pública, en este caso la WAN.

Respuesta incorrecta. Se puede utilizar para verificar la conexión entre la red local y la WAN, es una de las funciones de NAT.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

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

Caso práctico

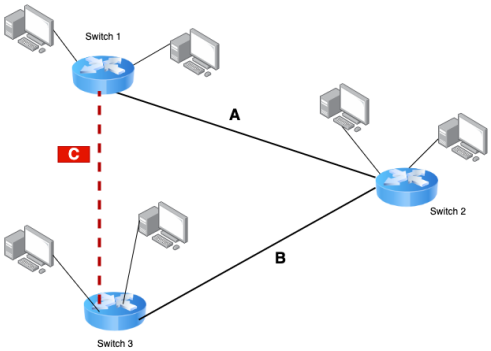
El fin de semana han quedado todos los compañeros para tomar algo juntos con algunos amigos y compañeros de clase que están realizando el módulo de FCT en otros empresas. **Jana** quería que conociesen a **Vindio** y **Laro.** Como no podía ser de otro modo, la conversación deriva en el trabajo que están realizando en BK Sistemas Informáticos y hay quienes se interesan por la evolución del uso de las tecnologías de conexión a Internet que ofertan actualmente los diferentes ISP, como han sido ADSL, RDSI o Frame Relay.

Alain Bachellier (CC BY-NC-SA)

Laro opina que, desde su punto de vista, cada vez hay más presencia de las tecnologías inalámbricas y entiende que ese va a ser uno de los aspectos que más va a evolucionar en los próximos años, especialmente en lo que a dispositivos móviles se refiere.

Jana dice que uno de sus vecinos tiene una conexión a Internet inalámbrica a través de una servicio WiMAX, que le ha preguntado cómo va ese servicio y dice que igual que con la conexión cableada anterior, pero bastante más barato.

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.



Benoît Prieur (CC BY-SA)

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.

La conmutación de paquetes es muy sencilla de entender, cuando un host quiere enviar un mensaje, lo divide en trozos (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 la conmutación de paquetes.

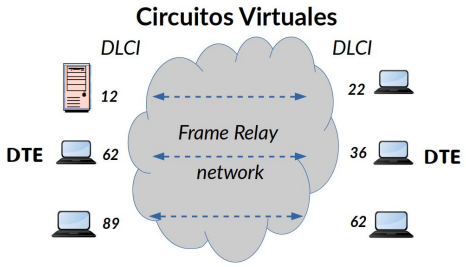
Conmutación de paquetes

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

Circuito virtual

7.1.- 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.



AlfBonillo. (Dominio público)

Esta tecnología establece un circuito virtual, permanente PVC (Circuito Virtual Permanente) o conmutado SVC (Circuito Virtual Conmutado). 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 (identificador de canal del circuito).

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.

Un parámetro importante a tener en cuenta en las transmisiones es el caudal CIR, (tasa de información comprometida), 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:

1.- Del cliente a la red.
2.- 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 (conmutación de etiquetas multiprotocolo), VPN (red privada virtual), cable módem y DSL (línea de abonado digital) hace que Frame Relay tienda a desaparecer del mercado.

Para saber más

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

Frame Relay

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.

No es correcto. La RTB no utiliza esta tecnología, no se fragmentan los mensajes.

Correcto, vas muy bien. Se preestablece el circuito antes de la comunicación.

Incorrecta. Esta técnica se utilizaba con el telégrafo.

Respuesta incorrecta. En la comunicación RTB no existe el concepto de celda.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

7.2.- 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, pero a diferencia de ésta, que solamente soporta conmutación de circuitos, soporta también conmutación de paquetes.

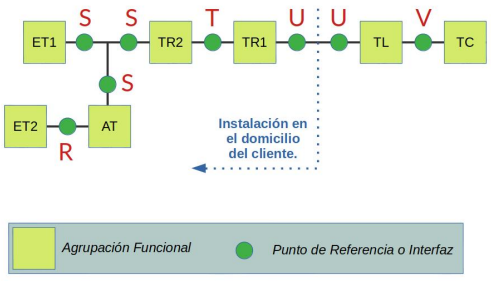
La mejora más relevante de RDSI respecto a la línea telefónica básica ,fue la capacidad para poder utilizar los servicios de Internet y de voz al tiempo, así como el aumento de velocidad.

RDSI tiene dos tipos de acceso:

1.- BRI (acceso básico).
2.- PRI (acceso primario).

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.



AlfBonillo. (Dominio público)

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 ET 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 el futuro de la tecnología RDSI.

Apagado RDSI

7.3.- ADSL.

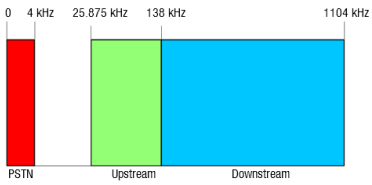
ADSL son las siglas de Línea de Abonado Digital Asimétrica. La tecnología ADSL nació en las compañías telefónicas para poder competir con otras, en la transmisión de datos utilizando las instalaciones de la red telefónica existentes. Con este objetivo, el diseño de ADSL debía cumplir los siguientes preceptos:

- 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**.

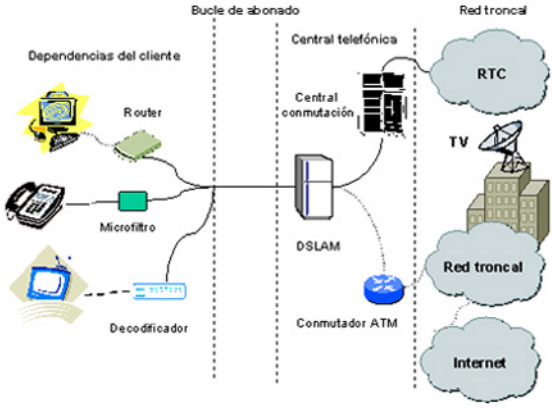


Biot (CC BY-SA)

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 televisión, 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, vídeo, música, datos) viaje por la línea de comunicaciones sin interferencias.

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.

La evolución de ADSL, pasando por ADSL2 ha desembocado en VDSL, 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.

Para saber más

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

DSLAM

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

Comparador de Fibra Óptica

Proveedores de Internet 2020

8.- Las tecnologías Wifi y Wimax.

Caso práctico

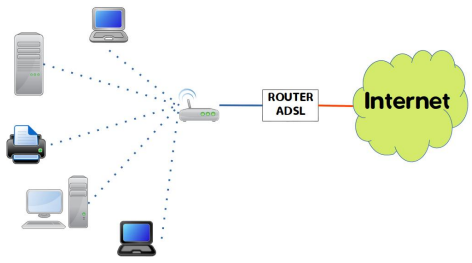
Uno de los compañeros de clase de **Jana**, **Naroba** y **Noiba**, está realizando precisamente la FCT en una empresa proveedora de servicios de Internet de forma inalámbrica con tecnología WiMAX y dice que esta tecnología es como una WiFi que funciona a nivel de toda una ciudad. Pero **Vindio** le corrige y le explica que utiliza una tecnología diferente, que no debe confundirlas porque son muy diferentes, algo similar a lo que ocurre con las diferentes tecnologías cableadas y que todos entienden con facilidad.

Alain Bachellier (CC BY-NC-SA)

Laro añade que también es necesario conocer las diferencias desde el punto de vista legal y todas las normas que rigen este tipo de tecnologías inalábricas, ya que presentan importantes diferencias a la hora de implantar el servicio en una ciudad u otra.

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).



AlfBonillo. (Dominio público)

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.

8.1.- Las tecnologías Wifi y Wimax.

La respuesta está en la tecnología Wimax, que son las siglas de 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.

Stalinas (CC BY-SA)

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.

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.

No es correcto, si se diferencian en el alcance pero Wifi utiliza ondas de radio.

Incorrecta, Wimax es más direccional, las ondas son de mayor frecuencia.

Correcto. Wimax es compatible con Wifi por las ondas de radio, pero incorpora las microondas lo que permite un mayor alcance en la comunicación.

Respuesta incorrecta. Wifi opera con ondas de radio.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Para saber más

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

OFDM

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

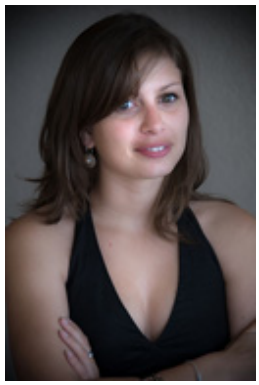
WiMax

¿Qué es y cómo funciona WiMax?

9.- Las tecnologías UMTS y HSDPA.

Caso práctico

Noiba explica que también existen otro tipo de tecnologías inalámbricas como las que utilizan actualmente los dispositivos móviles, sobre lo que alguien comenta:



Alain Bachellier (CC BY-NC-SA)

—¡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. Hay varias tecnologías, desde las más antiguas GSM, pasando por GPRS, UMTS hasta llegar a la HSDPA, 3G, 4G o 5G.

UMTS (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 .

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 ordenador, predominando las interfaces USB .

Mac (CC BY-SA)

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 ordenador.

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

Condiciones y términos de uso de los materiales

Historial de actualizaciones

Versión: 01.00.01	Fecha de actualización: 31/03/21
Actualización de materiales y correcciones menores.	
Versión: 01.00.00	**Fecha de actualización: 23/07/20**
Versión inicial de los materiales.	