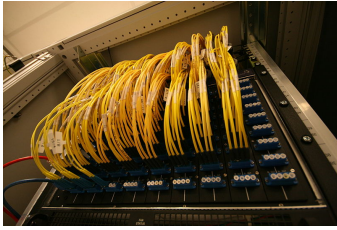


Caso práctico



María tiene curiosidad por saber más acerca de su instalación de red, habla con Blanca, una amiga suya que es Técnico de Sistemas Microinformáticos y Redes, y le pregunta si una vez están todos los equipos y dispositivos conectados se ha finalizado el trabajo y se puede funcionar con los equipos.

Blanca le comenta, que aún no, que falta configurar los equipos y dispositivos para que puedan comunicarse entre ellos y tengan acceso a Internet. Además, hay que tener en cuenta las limitaciones de acceso a los usuarios para que no puedan acceder a cualquier dato en la red.



[Ministerio de Educación y Formación Profesional](#), (Dominio público)

Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

[Aviso Legal](#)

1.- Introducción

En este tema veremos la configuración de dispositivos, más concretamente, el principal aspecto de configuración hoy en día es el enfocado a la conexión a internet y la conexión a redes inalámbricas.

2.- Tecnologías de acceso a la WAN

Una red de área amplia, o WAN, por las siglas de (wide area network en inglés), es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales, llamadas LAN, por lo que sus miembros no están todos en una misma ubicación física.

Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de internet (ISP) para proveer conexión a sus clientes.

Para acceder a la WAN podemos hacer una clasificación sencilla:

- Acceso cableado
- Acceso inalámbrico

2.1.- Acceso cableado

Dentro de los accesos más conocidos:

- RTC (Red Telefónica Conmutada), ya anticuada, consiste en aprovechar el cable de cobre y transportar datos informáticos binarios a través de la red telefónica de voz mediante un módem. El módem modula los datos binarios en una señal analógica en el origen y demodula la señal analógica a datos binarios en el destino.
- RDSI (Red digital de servicios integrados), se trata de una línea telefónica, pero digital (en vez de analógica) de extremo a extremo. En vez de un módem, este tipo de conexión emplea un adaptador de red que traduce las tramas generadas por el ordenador a señales digitales.
- ADSL (Asymmetric Digital Subscriber Line) une las ventajas de la RTB y de la RDSI, por lo que se convirtió pronto en el tipo de conexión favorito de hogares y empresas. La ADSL aprovecha el cableado de la RTB para la transmisión de voz y datos, que puede hacerse de forma conjunta (como en la RDSI), para ello establece tres canales independientes sobre la misma línea telefónica estándar: 1 canal de envío de datos, 1 canal de recepción de datos y 1 canal de voz. El nombre de "asimétrica" que lleva la ADSL se debe a que el ancho de banda de cada uno de los canales de datos es diferente, reflejando el hecho de que la mayor parte del tráfico entre un usuario y la Internet son descargas de la red.
- BPL (Broadband over Power Lines), es el uso de las redes eléctricas para dar cobertura de internet, es decir, es la utilización de la tecnología PLC para acceso a internet. No ha tenido mucho éxito porque se ha visto superada por otras tecnologías y por problemas de interferencias que produce.
- FTTH (Fiber to the Home), FTTB (Fiber to the Building) y en general las tecnologías FTTx, son acceso a internet a través de fibra óptica, estas tecnologías se están expandiendo actualmente. La tecnología FTTH propone la utilización de fibra óptica hasta la casa del usuario o cliente de fibra (usuario final). La red de acceso entre el abonado y el último nodo de distribución puede realizarse con una o dos fibras ópticas dedicadas a cada usuario (una conexión punto-punto que resulta en una topología en estrella) o una red óptica pasiva (del inglés Passive Optical Network, PON) que usa una estructura arborescente con una fibra en el lado de la red y varias fibras en el lado usuario
- Cable coaxial, utiliza la instalación típica de televisión por cable para recibir internet por el mismo medio.

Debes conocer

Este video comenta las diferentes formas de acceder a internet:

https://www.youtube.com/watch?v=6BtpH7zYu_I&t=2s

2.2.- Acceso inalámbrico

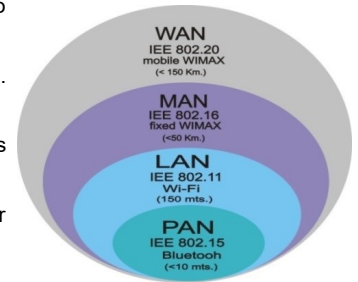
Podemos dividir las redes inalámbricas en 4 categorías tomando como criterio el alcance:

WPAN: redes inalámbricas de área personal. Se emplean dentro del denominado "espacio operativo personal", es decir, el espacio que rodea a una persona. (Por ejemplo Bluetooth).

WLAN: Alcance de varios centenares de metros. Comprenden el espacio de una oficina o un edificio. (Por ejemplo WiFi).




WMAN: Se utilizan para comunicar distintas ubicaciones dentro de un área metropolitana, entre varios edificios. (Por ejemplo WiMAX)

WWAN: Llamadas redes inalámbricas globales. Pueden cubrir todo un país o incluso varios países. (Por ejemplo HSDPA).



2.2.1.- Acceso inalámbrico WPAN

Además de las tecnologías anteriores utilizadas para el acceso a la WAN hay otra serie de tecnologías que permiten intercambio de información dentro de lo que se denomina PAN (Redes de Área Personal):

- Bluetooth, se utiliza para la comunicación entre dispositivos. Tiene poco alcance y capacidad y se utiliza para conectar dispositivos informáticos entre sí y transmitir pequeñas cantidades de información 
- NFC es una plataforma abierta pensada desde el inicio para teléfonos y dispositivos móviles. Su tasa de transferencia puede alcanzar los 424 kbit/s por lo que está pensada para comunicación instantánea, es decir, identificación y validación de equipos/personas. La velocidad de comunicación es casi instantánea sin necesidad de emparejamiento previo, el alcance es máximo 20 cm. 
- ZigBee utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y bajo consumo eléctrico. 
- Infrarrojos, esta tecnología óptica tiene un alcance corto, pero tiene un bajo consumo y bajo costo. La principal desventaja de la tecnología infrarroja es que requiere la misma línea de visión directa entre los dispositivos de una PAN. Sin embargo, la tecnología infrarroja ha existido desde hace varios años y es poco probable que desaparezca pronto.
- HomeRF es también una especificación que permite la interconexión de dispositivos (ordenadores, teléfonos, electrodomésticos, ...) en una área pequeña

Para saber más

Internet de las cosas (Internet of Things) es un concepto que se refiere a la conexión de objetos domésticos con internet y que está en pleno auge, en este video podrás saber un poco más acerca de ello:

<https://www.youtube.com/watch?v=gV7I2YOSOQ4>

2.2.2.- Acceso inalámbrico WLAN

Aunque en esta categoría esta también Hiperlan sin duda alguna la más extendida es la WI-FI (Wireless Fidelity). Es un paso más en lo que eran las redes cableadas Ethernet.



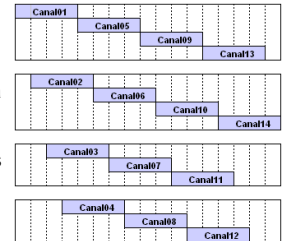
La tecnología Wi-Fi permite mediante radio frecuencia conectarse a una red local o acceder a internet.

Dentro de los estándares más conocidos tenemos 802.11b, 802.11g, 802.11n, 802.11ac y entre los últimos desarrollados están 802.11ad (WiGig), 802.11ah (HaLow) y en desarrollo aún 802.11ax. Para que podemos conectar dispositivos en los diferentes estándares el punto de acceso debe trabajar en modo mixto.

Principales conceptos sobre WIFI

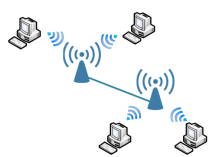
SSID (Identificador de servicio compartido) es un identificador único que utilizan los dispositivos cliente para distinguir entre múltiples redes inalámbricas cercanas.

Canal, el rango de frecuencias legalmente permitidas para la emisión de señales WIFI se divide en 14 canales para la banda de 2.4 Ghz según se muestra:



En redes inalámbricas existen tres topologías:

- **BSS**. Conjunto de servicio básico. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). Un dispositivo, punto de acceso, centraliza toda la comunicación. Todos los dispositivos que estén al alcance del AP, lo utilizan para poder comunicarse entre sí o para acceder a otra red a través de él.
- **IBSS**. Conjunto de servicio básico independiente, es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Enlaces punto a punto entre dispositivos que estén en el mismo rango, los dispositivos se conectan entre sí sin que exista un nodo central (AP)
- **ESS**. Conjunto de servicio extendido. Varias BSS interconectadas. Cuando un usuario itinerante va desde un BSS a otro mientras se mueve dentro del ESS, el adaptador de la red inalámbrica de su equipo puede cambiarse de punto de acceso (roaming).



El estándar 802.11 define dos modos operativos:

- El modo de infraestructura en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso (nodo central). Éste es por lo general el modo predeterminado.
- El modo ad-hoc en el que los clientes se conectan entre sí sin ningún punto de acceso.

WDS (Wireless Distribution System). La función WDS es un estándar que permite que dos puntos de acceso que soporten WDS se comuniquen entre sí, además estos puntos de acceso siguen desempeñando también su función habitual de dar acceso a equipos

Modos de seguridad:

- Abiertas: Las redes Wi-Fi abiertas no tienen contraseña, por lo que queda claro que no se aconseja de ninguna forma.
- WEP (Wired Equivalent Privacy) de 64: El viejo estándar de encriptación WEP es vulnerable y no se debe utilizar
- WEP de 128: un cifrado de mayor tamaño, pero igual inseguro.
- WPA (Wi-Fi Protected Access) adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida (PSK, Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red. Tampoco es seguro.
- WPA2 (Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA
- WPA3 corrige problemas de seguridad que se detectaron en WPA2, aunque el protocolo ya está disponible, se necesitarán unos años para una implantación completa, hay que tener en cuenta que hay que cambiar muchos dispositivos para hacerlos compatibles o actualizar sus firmwares. WPA3 introduce un cifrado individual de forma que cada conexión se cifra separada de las demás y evita los ataques por fuerza bruta.

Encriptación, hay dos mecanismos de encriptación: Protocolo de integridad de clave temporal (TKIP) y Estándar de encriptación avanzada (AES).

En conclusión, las medidas de seguridad recomendadas son:

- Camuflaje SSID - Deshabilite los broadcasts SSID de los puntos de acceso
- Filtrado de direcciones MAC
- Implementación de la seguridad WPA3 o WPA2
- Evitar el uso de parámetros predeterminados.

Además de estas medidas siempre es recomendable tomar todas las precauciones que podamos como apagar el router cuando no vayamos a usar la red en un periodo largo, vigilar los accesos a la red a través de los menús del router, etc.

Para saber más

Normalmente el canal WIFI lo selecciona automáticamente nuestro router o punto de acceso pero nos interesa saber algo más acerca de estos canales, puedes informarte en este [link](#) para configurarlos correctamente.

2.2.3.- LIFI

Light Fidelity, es una tecnología inalámbrica, que en vez de usar ondas de radio, utiliza pulsos de luz. Aunque la velocidad es muy superior a WIFI tiene el inconveniente de no poder atravesar paredes.

Una de las principales ventajas de la novedosa tecnología, que está llamada a sustituir o al menos complementar a las redes WiFi actuales, es que ayudaría a desaturar el espacio radio eléctrico. Al utilizar la luz visible, no interfiere con otras frecuencias por lo que podría ser utilizado sin problema, por ejemplo, en aviones.

Para saber más

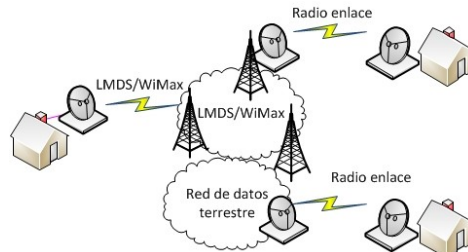
En el siguiente [video](#) se explica el funcionamiento de la tecnología LIFI

2.2.4.- Acceso inalámbrico WMAN

En esta categoría se trata WiMax (aunque también la podemos incluir en la categoría WWAN, las fronteras de estas categorías no están claramente definidos).

[WiMax](#) (Worldwide Interoperability for Microwave Access) un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, transmite mediante una red de estaciones base. Cada estación base conecta con múltiples usuarios situados a grandes distancias a través de pequeños paneles situados en el exterior de los edificios.

WiMAX está pensado para construir una infraestructura de red cuando el entorno o distancia no es favorable para una red cableada (por ejemplo zonas rurales de difícil acceso). Es una alternativa más rápida y barata que tener que instalar cables. También se está usando actualmente para conexiones entre empresas, o entre sedes e Internet.



También podemos encontrar dentro de esta categoría otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service), es un medio de transmisión de altas frecuencias y dado que las altas frecuencias son más proclives a los accidentes de terrenos (no atraviesan obstáculos) se requiere una visibilidad en línea directa con la antena emisora. LMDS es una tecnología más antigua y con costes de adquisición más elevados.

El radio enlace es un medio de comunicación complementario que funciona a muy altas frecuencias (de hecho son micro ondas). El receptor en casa del usuario requiere visibilidad directa con la antena emisora. Se emplea para conectar una delegación que no está en la zona de cobertura de WiMax (por eso hace de enlace hacia WiMax) o para conectar una delegación remota a la red de fibra del operador.

2.2.5.- Acceso inalámbrico WWAN



Dentro de los más conocidos tenemos:

- GSM (Global System for Mobile Communications) Sistema Global para las comunicaciones Móviles. GSM se considera, por su velocidad de transmisión y otras características, un estándar de segunda generación (2G):
 - GSM – CSD (Circuit Switched Data), 2G: hasta 9'6 kbps en subida y bajada, ya no se usa.
 - GSM – GPRS (General Packet Radio Service), 2'5G: hasta 80 kbps en bajada y 20 kbps en subida
 - GSM - EDGE (Enhanced Data Rates for GSM Evolution), 2'75G: hasta 236 kbps en bajada y 59 kbps en subida
- UMTS (Universal Mobile Telecommunications System), la tercera generación de sistemas para móviles (3G). Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de email, y mensajería instantánea). Permite velocidades de conexión de hasta 2 Mbps en condiciones óptimas.
- HSDPA (High Speed Downlink Packet Access), 3.5G, 3G+ o Turbo3G, es la optimización de la tecnología espectral UMTS/WCDMA, pudiendo alcanzar velocidades de bajada de hasta 14 Mbps en teoría en condiciones óptimas.
- HSUPA (High-Speed Uplink Packet Access), H+ es un protocolo de acceso de datos para redes de telefonía móvil con alta tasa de transferencia de subida (de hasta 7.2 Mbit/s). Calificado como generación 3.75 (3.75G) o 3.5G Plus, es una evolución de HSDPA, como una tecnología que ofrece una mejora sustancial en la velocidad para el tramo de subida, desde el terminal hacia la red.
- LTE (Long Term Evolution), 4G, con LTE, el caudal de velocidad llega hasta los 100Mbps (descarga) y 50Mbps (subida), e incluso llegar a 1Gbps para usuarios que precisen de poca movilidad. Por su parte, la evolución de WiMax (también considerada una red 4G) puede alcanzar los 128Mbps (descarga) y los 56Mbps (subida).
- 5G, el primer estándar (Release 15). Se implantará en los próximos años, tienen unas velocidades de 20 Gbps, ahorro de energía, conectividad masiva y una latencia muy baja (establecimiento de la conexión muy rápido que permitirá mayor fiabilidad en vehículos autónomos, trabajo remoto, ...).
- Satélite: la conexión se realiza a través de una antena parabólica que capta la señal de satélites de comunicación.

Debes conocer

[Video explicativo sobre 5G](#)

2.3.- Redes mixtas. Integración de la red inalámbrica en la red cableada

Lo habitual en el diseño de red es empezar realizando la estructura cableada y después dar acceso a los clientes inalámbricos. No es necesario más que un punto de acceso o un router Wi-Fi, que será el único dispositivo que tenga una conexión física, y una tarjeta Wi-Fi en el equipo que queramos conectar. De esta manera se puede acceder a la red local de alguna entidad o conectar varios ordenadores de una casa a Internet evitando tanto cableado. En la actualidad la mayoría de los equipos que salen a la venta llevan la tarjeta Wi-Fi incorporada

Los clientes se conectan de manera inalámbrica al AP (punto de acceso) y este lo hace por cable a dispositivos que nos facilitan la conexión al exterior.

Actualmente lo más normal es que el punto de acceso esté dentro de la misma "caja" que el router que da acceso al exterior, el ejemplo típico son los routers-ADSL que hay en gran cantidad de hogares.

Dispositivos	Modo	Topología
Sin puntos de acceso	Ad hoc	IBSS
1 punto de acceso	Infraestructura	BSS
Varios puntos de acceso	Infraestructura	ESS

3.- NAT

El agotamiento del espacio de direcciones IPv4 por la expansión de Internet ha provocado la adopción de diferentes técnicas para un mejor reparto de las direcciones. En un primer momento se introdujeron las CIDR para evitar que las direcciones se asignaran por clases y, así, poder ajustar más la concesión de IPs al tamaño de la red solicitada.

Otra técnica que se implantó fue NAT. El uso *más habitual* de la traducción de direcciones de red (NAT, Network Address Translation) es compartir una IP pública para muchos dispositivos, para ello, se traducen las IPs privadas por una IP pública.

La ventaja de las IPs privadas es que cualquiera puede utilizar estos rangos, la desventaja es que no se pueden usar en internet porque están reservadas para uso privado. Las IPs públicas, en cambio, pueden ser usadas en internet pero el inconveniente es que al ser únicas en el mundo deben ser asignadas por el organismo competente y esto tiene un coste.

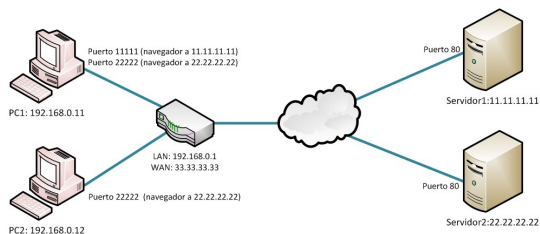
Un uso más frecuente de la técnica NAT lo encontramos en nuestros routers caseros, estos reciben una única IP pública del proveedor de internet y, usando NAT consiguen compartir esta IP pública para que la usen todos los dispositivos de nuestra red privada.

¿Cómo funciona en un router DSL-fibra la NAT?

Muchos de nosotros tenemos las IPs típicas en casa IP 192.168.0..... Por tanto, es imposible que cuando solicitemos una página web desde una IP privada a un servidor web este sepa a quien responder de entre todos nosotros. Con NAT, cuando solicitamos la página web desde nuestro equipo con IP privada, al atravesar esta petición nuestro router, se sustituye nuestra IP privada por la IP pública que nos facilita nuestro proveedor de internet (ISP) y se envía la petición al exterior (internet). Así el servidor web sabrá a quien responder porque la petición le llega de una IP única en el mundo (nuestra IP pública).

Si tenemos varios equipos y todos quieren visitar la misma página web el router construye una tabla (tabla NAT) donde anota todas las salidas al exterior de forma que cuando llega la respuesta busca en esta tabla y envía la respuesta al equipo que solicitó la web. Supongamos el siguiente ejemplo:

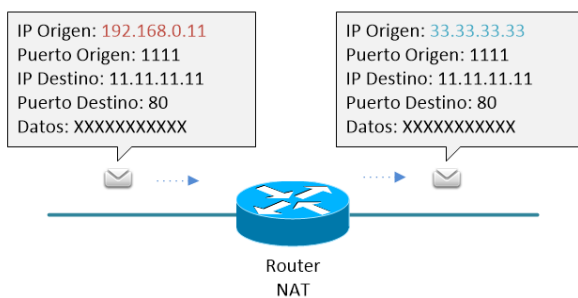
En una pequeña red local hay dos PC, el primero tiene abierto 2 navegadores (que usan los puertos 11111 y 22222) visitando respectivamente las web 11.11.11.11 y 22.22.22.22, el segundo PC solo tiene abierto un navegador (que usa el puerto 22222) visitando la web 22.22.22.22. El router DSL tiene la IP privada 192.168.0.1 en su interfaz LAN y la IP pública 33.33.33.33 en su interfaz WAN.



Las traducciones de direcciones realizadas por nuestro router DSL podrían ser similares a las siguientes:

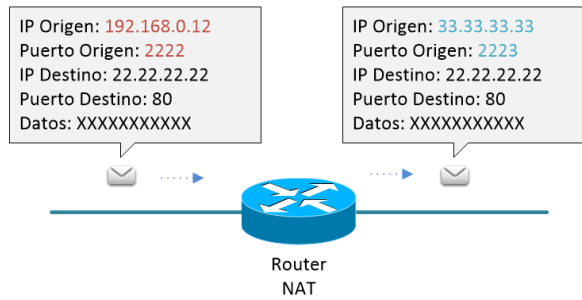
Paquetes llegados al router de la LAN				Paquetes enviados por el router al exterior			
IP origen	Puerto origen	IP destino	Puerto destino	IP origen	Puerto origen	IP destino	Puerto destino
192.168.0.11	11111	11.11.11.11	80	33.33.33.33	11111	11.11.11.11	80
192.168.0.11	22222	22.22.22.22	80	33.33.33.33	22222	22.22.22.22	80
192.168.0.12	22222	22.22.22.22	80	33.33.33.33	22223	22.22.22.22	80

Cuando el PC1 quiere visitar la página 11.11.11.11 envía una solicitud a nuestro router, este elimina la IP privada y la sustituye por la pública, además anota que el puerto que hace la petición es el 11111, cuando llegue una respuesta a nuestra IP pública con destino el puerto 11111 nuestro router sabrá que la petición es para el navegador 1 del PC 1 y se la enviará a este haciendo el cambio contrario, es decir, quitando la IP 33.33.33.33 como destino y poniendo la IP privada.



Pero como el PC1 hay 2 aplicaciones abiertas hay, por tanto, dos puertos en uso. Cuando el navegador 2 visita la web 22.22.22.22 se produce el mismo proceso, el router sustituye la IP privada por la IP pública y envía al exterior la solicitud, cuando llega la respuesta busca en su tabla NAT y hace el cambio inverso.

En el PC 2 hay un navegador abierto usando el puerto 22222, cuando solicita una web, el router sustituye la IP privada por la IP pública, pero en este caso, la combinación IP pública + 22222 ya está asociada en la tabla al navegador 2 del PC1, por tanto el router tiene que buscar un puerto libre (supongamos 22223) y en esta ocasión debe cambiar la IP y el puerto privados por una combinación pública que no esté en uso en la tabla NAT (es decir, se ha traducido dirección y puerto privados por dirección y puertos públicos).



Reflexiona

Imaginemos una centralita telefónica interna en una empresa, los empleados se llamarán a los números internos (extensión 22, extensión 23, ...) pero estos números no tienen sentido en el exterior. Pueden existir estas mismas extensiones en otra telefonía interna de otra empresa. Estas son los equivalentes a las IPs privadas, números que no tienen validez en el exterior.

Supongamos que el número de teléfono público (999999999) admite hasta 3 líneas (conversaciones simultáneas) Cuando algún empleado necesita hablar con el exterior coge una de las tres líneas, al destinatario le aparece que le están llamando desde 999999999. El equivalente al número de teléfono es nuestra IP pública y las 3 líneas son los puertos públicos disponibles.

Pregunta de Elección Múltiple

En un centro educativo disponen de una línea DSL típica ¿Cuántos alumnos podrían estar navegando a la vez como máximo si cada uno solo puede abrir un navegador?

- Todos los que quieran
- Ninguno
- 65536
- 256

Incorrecto, podremos tener tantas como puertos públicos existan.

Incorrecto, podremos tener tantas como puertos públicos existan.

Efectivamente, una vez estén en uso todos los puertos públicos (2^{16}) no podrán asignarse nuevas conexiones.

Incorrecto, podremos tener tantas como puertos públicos existan.

Solución

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

3.1.- NAT inversa (o Abrir puertos)

La expresión "abrir puertos" tiene muchas acepciones, en principio el uso correcto es el equivalente a "escuchar por un puerto", es decir, ejecutar aplicaciones que usan un determinado puerto y tener ese puerto activo y listo para para enviar o recibir datos.

Otro uso de la expresión "abrir puertos" para, en un firewall (encargado de permitir, denegar y custodiar las conexiones), conceder permisos para que cierto puerto destino u origen pueda salir o entrar de la red local.

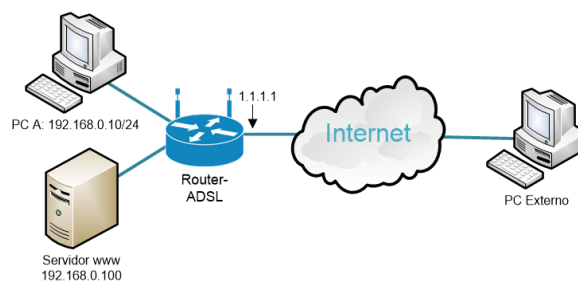
Pero en cuanto al tema que tratamos, la traducción de direcciones y puertos, hablamos de "abrir puertos", o NAT inversa (Port Forwarding o Virtual Server en muchos menús de router domésticos) para permitir entrar en una LAN desde Internet, sin que previamente se haya producido una petición desde la LAN.

Como se ha visto en el apartado anterior, los paquetes que entran en LAN corresponden a respuestas de peticiones previas realizadas desde dentro de la LAN. Para entrar en LAN sin que haya una solicitud previa es necesario "abrir los puertos", es decir, hay que incluir una traducción en la tabla NAT fija, no dinámica producida por un paquete que ha salido.

La finalidad de abrir los puertos es tener servicios (servidor web, servidor base de datos, etc.) instalados en una red local y que se puedan acceder desde cualquier lugar exterior.

Ejemplo de NAT inversa o apertura de puertos

En el esquema hay un servidor web en una red local, para acceder a este servidor web desde el exterior solo es necesario poner en el navegador del equipo externo <http://1.1.1.1>



¿Qué contenido tendrá la tabla NAT antes de abrir el puerto?

Antes de abrir el puerto la tabla NAT estará vacía, o si algún equipo local ha enviado alguna petición al exterior el router habrá anotado esa salida, es decir, anotaciones dinámicas asociadas a las salidas de datos al exterior.

Dinámica/Fija	Protocolo	IP interna		IP externa	
		IP	Puerto	IP	Puerto
Dinámica
....					
Dinámica

¿Qué contenido tendrá la tabla NAT después de abrir el puerto?

La tabla NAT tendrá una entrada fija, indicando que todas las peticiones con destino al puerto 80 (servicio web) la atenderá el servidor www

Dinámica/Fija	Protocolo	IP interna		IP externa	
		IP	Puerto	IP	Puerto
Fija	TCP	192.168.0.100	80	1.1.1.1	80
Dinámica
....					
Dinámica

Como se puede observar no hay datos relativos a la IP externa, la razón es que las peticiones pueden venir de cualquier IP externa. Cuando llegue un paquete con destino a 1.1.1.1:80, el router aplicará la traducción fija y lo enviará a 192.168.0.100:80

¿Podríamos tener dos servidores web funcionando en la red local?

Pues sí, pero el puerto 80 está abierto hacia 192.168.0.100, es decir, el puerto 80 está asociado al equipo 192.168.0.100, por tanto, será necesario utilizar otro puerto, por ejemplo el 81 para el segundo servidor:

Dinámica/Fija	Protocolo	IP interna	IP externa
---------------	-----------	------------	------------

		IP	Puerto	IP	Puerto
Fija	TCP	192.168.0.100	80	1.1.1.1	80
Fija	TCP	192.168.0.200	80	1.1.1.1	81
Dinámica

Cuando un paquete llegue al router con destino puerto 81, el router aplicará la segunda traducción y enviará al puerto 80 del equipo 192.168.0.200 el paquete. Para visitar esta segunda web desde el exterior habrá que indicar <http://1.1.1.1:81>

Autoevaluación

¿Puedo abrir el mismo puerto hacia 2 dispositivos diferentes?

Verdadero Falso

Falso

No, cuando abrimos un puerto lo que hacemos es que cada vez que venga una petición del exterior a nuestro router y a ese puerto en concreto se la enviamos a un equipo interno que atenderá la petición. Solo un equipo puede atender la petición.

3.2.- NAT Masivo

El NAT masivo o a gran escala (Carrier Grade NAT ó large-scale NAT) es usado por los proveedores de internet para compartir un grupo de IPs públicas entre muchos usuarios. Esta traducción es realizada dentro de la red del ISP. Las NAT anteriores (traducción de direcciones, de puertos y con sobrecarga) son conocidas como NAT44 porque hacen una traducción de IPv4 a IPv4. El NAT masivo se conoce también como NAT444 porque realiza una doble traducción de IPv4 a IPv4 a IPv4.

En un principio, hasta los 90, el proveedor de internet disponía de un bloque de IPs públicas que iba asignando a los clientes a medida que estos se conectaban a internet, cuando se desconectaban el proveedor reutilizaba la IP pública para otro cliente. Pero el cliente pasó a estar conectado constantemente, con lo cual nunca liberaba la IP asignada, como solución surgió el NAT masivo.

El cálculo es más o menos así: supongamos un ISP con 10 IPs públicas, este las reparte entre 12 abonados (utiliza una técnica de overbooking, presupone que no habrá de esos 12 más de 10 conectados simultáneamente). Pero realmente lo que necesita un abonado son varias conexiones (cada IP+puerto sería una aplicación conectada), pues bien si en vez de asignar IPs asigna combinaciones de IP+puerto tiene para 10×65536 conexiones, si asignará hasta 1000 conexiones por usuario tendría para 655 usuarios.

El problema que surge para el usuario es que hay una traducción de direcciones que se realiza por el proveedor y que no controlará. Los ISP pueden ofrecer control a través de páginas web limitadas para el usuario o con protocolos como PCP (Protocolo de control de puertos)

El IANA ha asignado el rango 100.64.0.0/10 para CGNAT, este bloque no se puede usar ni en redes privadas ni en Internet (Curioso, porque puede haber redes privadas más grandes como 10.0.0.0/8)

Reflexiona

¿Puedo abrir puertos si mi ISP me tiene dentro de NAT masivo?

Mostrar retroalimentación

No dependerá de nosotros, la manipulación de puertos y traducciones NAT se realiza en los dispositivos del ISP y será a quien le tengamos que solicitar la apertura de puertos.


4.- Configuración de red en equipos Windows y Linux

Todos los sistemas operativos existentes hoy en día incluyen soporte para conexión en red, a la hora de la instalación y configuración del equipo lo único que hay que añadir son los controladores o drivers correspondientes a la tarjeta de red.

Una vez tengamos activa la tarjeta de red está se configurará por defecto en modo IP automática porque lo habitual es tener un router doméstico o algún dispositivo que asigne la configuración a nuestros equipos. Pero si no es así necesitamos acceder a la configuración de los parámetros de red.

En el caso de Windows:

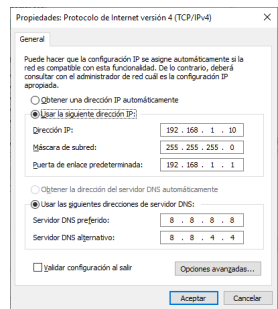
Accedemos a Configuración  Red e Internet  Red e Internet Wi-Fi, modo avión, VPN Si es cableada tendremos un icono Ethernet  Ethernet

y si es inalámbrica tendremos un icono Wi-Fi  Wi-Fi .

Desde aquí podemos acceder a “Estado” “Cambiar las opciones del adaptador”, y entramos con un clic en el botón derecho en las propiedades, en protocolo de internet IPv4:

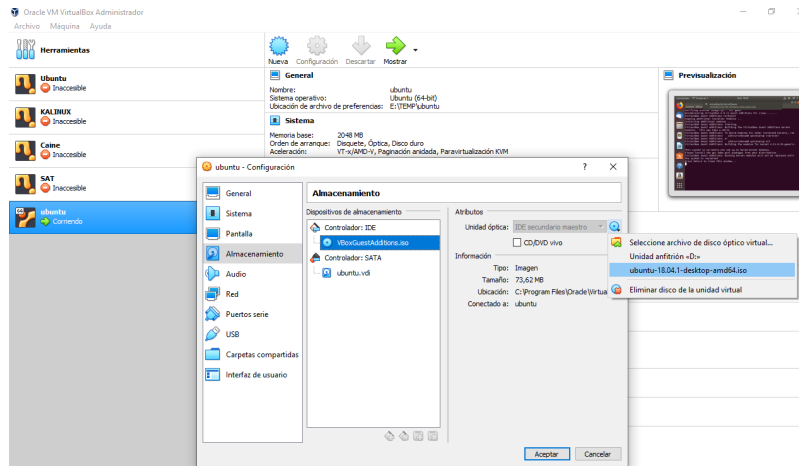
Aunque lo más cómodo es una configuración automática de los parámetros de red, en determinados casos (en muchas ocasiones para resolver problemas en nuestra red) debemos configurar manualmente los parámetros de nuestra conexión a internet. Estos son:


- Dirección IP, deber ser única en la nuestra red.
- Máscara de red: determina el tamaño de nuestra red.
- Puerta de enlace predeterminada: la IP del dispositivo de nuestra red por el que accedemos al exterior. Evidentemente un router que es el dispositivo que separa redes.
- DNS: IP del dispositivo (habitualmente fuera de nuestra red) o dispositivos, que nos permiten escribir direcciones web sin necesidad de conocer la IP.

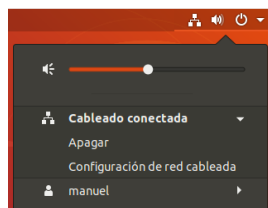


En el caso de Linux (Ubuntu 18):

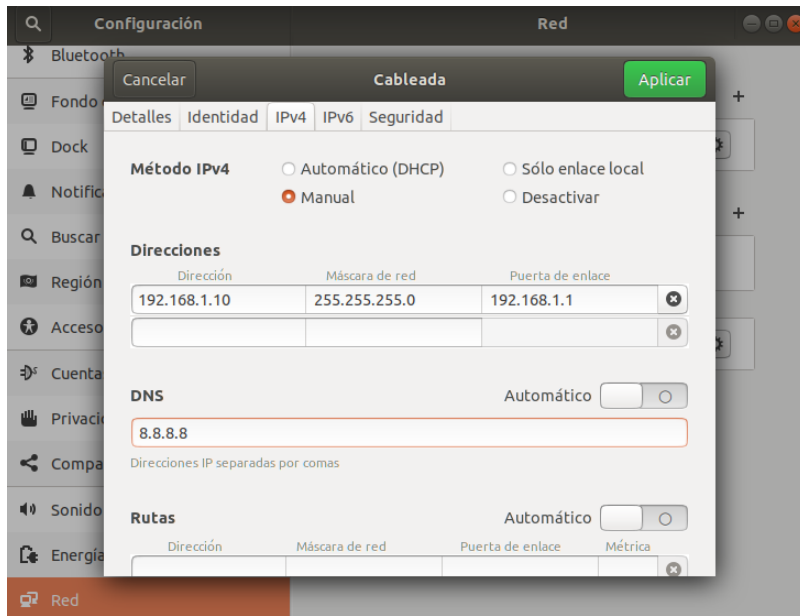
Si tenemos un equipo Windows podemos descargar e instalar [VirtualBox](#), después creamos una máquina virtual (un equipo ficticio) y descargamos e instalamos [Ubuntu](#) para ello en almacenamiento indicamos la iso de Ubuntu descargada y arrancamos nuestro equipo ficticio desde el DVD ficticio con Ubuntu.



En la esquina superior derecha tenemos un icono de red (), si accedemos a Configuración de red cableada:



Dentro de “Configuración” accedemos a “Red”, en la solapa “IPv4”, el método por defecto viene establecido en automático (DHCP) pero si queremos establecer la IP de forma manual podemos seleccionar la opción automática e indicar los parámetros habituales (IP, máscara, puerta de enlace y DNS):



5.- Configuración de routers

La configuración de router por vía web está basada en las páginas web que cada fabricante diseña, evidentemente cada fabricante plantea los menús, los parámetros, etc. como le parece conveniente. La única ventaja es que cada fabricante suele usar diseños muy similares para los diferentes dispositivos, con lo cual los dispositivos que tenemos son de una sola marca o de muy pocas solo tendremos que aprender a manejar unas pocas páginas web.

Para mostrar las configuraciones usaremos dd-wrt, es un firmware que podemos instalar de diferentes dispositivos y que tienen bastante auge.

Para cambiar el nombre del router basta con acceder a la configuración básica y escribir en la casilla nombre del router:

The screenshot shows the dd-wrt control panel interface. The top navigation bar includes 'Configuración', 'Inalámbrico', 'Servicios', 'Seguridad', 'Restricciones de Acceso', 'NAT / QoS', 'Administración', and 'Estado'. The 'Configuración' section is active, with sub-tabs for 'Config Básica', 'DDNS', 'Clonar Dirección MAC', 'Ruteo Avanzado', 'Redes', and 'Túnel EoIP'. The 'Config Internet' section is expanded, showing 'Tipo de Conexión' set to 'IP Estática'. Below this, there are input fields for 'Dirección IP de Internet' (172.23.160.210), 'Máscara de Subred' (255.255.255.0), 'Puerta de Enlace' (172.23.160.15), and three 'DNS Estática' fields (80.58.61.250, 80.58.61.254, and 0.0.0.0). The 'Config Opcional' section is also expanded, showing 'Nombre del Router' set to 'router-asir1', 'Nombre del Host' set to 'asir1', 'Nombre del Dominio' (empty), 'MTU' set to 1500, and 'STP' set to 'Desactivar'. A right-hand sidebar contains 'Ayuda más...' and 'Configuración Automática - DHCP?' with explanatory text.

Cambio de contraseña, se haría en la opción de administración, este entorno, como la mayoría de los routers domésticos solo hay un tipo de usuario que tiene acceso a la configuración completa del router.

The screenshot shows the dd-wrt control panel interface with the 'Administración' section active. The top navigation bar includes 'Configuración', 'Inalámbrico', 'Servicios', 'Seguridad', 'Restricciones de Acceso', 'NAT / QoS', 'Administración', and 'Estado'. The 'Administración Router' section is expanded, showing 'Clave del Router' with three password input fields (User, Router, Re-introducir Clave). Below this, the 'Acceso Web' section is expanded, showing 'Protocolo' with 'HTTP' selected and 'HTTPS' unselected, 'Auto-Refresco (en segs)' set to 3, and 'Activar la página Info' set to 'Activar'. A right-hand sidebar contains 'Ayuda más...' and 'Auto-Refresco:' with explanatory text.

En el caso de router domésticos la configuración de las interfaces se realiza vía web, los tipos más habituales son:

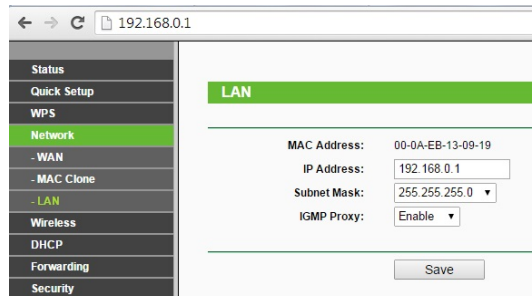
- Ethernet, las cuales no suelen admitir más configuración que la relacionada con la dirección IP.
- Inalámbricas, donde podemos configurar el nombre de la WIFI, los parámetros de seguridad, etc.

The screenshot shows the dd-wrt control panel interface with the 'Inalámbrico' section active. The top navigation bar includes 'Configuración', 'Inalámbrico', 'Servicios', 'Seguridad', 'Restricciones de Acceso', 'NAT / QoS', 'Administración', and 'Estado'. The 'Configuración' section is active, with sub-tabs for 'Config Básica', 'SuperChannel', 'Seguridad Inalámbrica', 'Filtrado MAC', and 'WDS'. The 'Interfaz física WIFI ath0 [2.4 GHz]' section is expanded, showing 'Modo Inalámbrico' set to 'AP', 'Modo de Red WIFI' set to 'Desactivado', 'Anchura de canal' set to 'Completo (20 MHz)', 'Nombre de Red WIFI (SSID)' set to 'redwifi', and 'Broadcast SSID Inalámbrico' set to 'Desactivar'. Below this, the 'Interfaz virtual' section is expanded, showing an 'Añadir' button. At the bottom, there are buttons for 'Guardar Config.', 'Aplicar Configuración', and 'Cancelar Cambios'. A right-hand sidebar contains 'Ayuda más...' and 'Modo de Red WIFI:' with explanatory text.

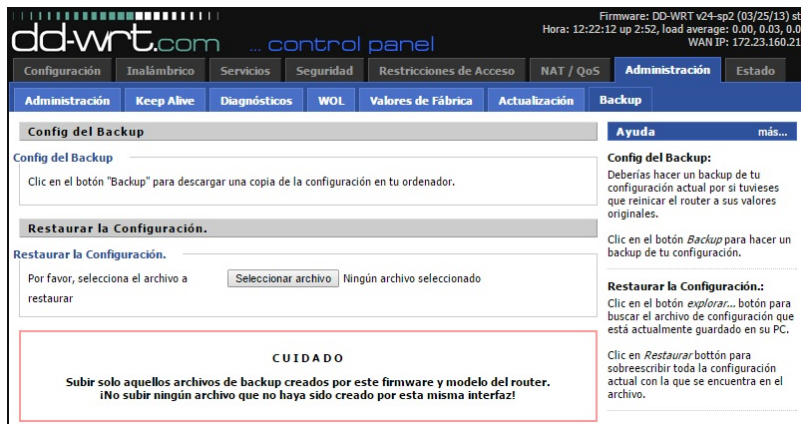
- PPP, es usado en varios tipos de redes físicas como cable serial, línea telefónica, telefonía móvil. PPP también es usado en las conexiones de acceso a internet. Los ISP han usado PPP para que accedan a internet los usuarios de línea telefónica:

WAN Configuration			
Interface	VPI/VCI	Encap	Protocol
vc0	8/32	LLC	rt1483

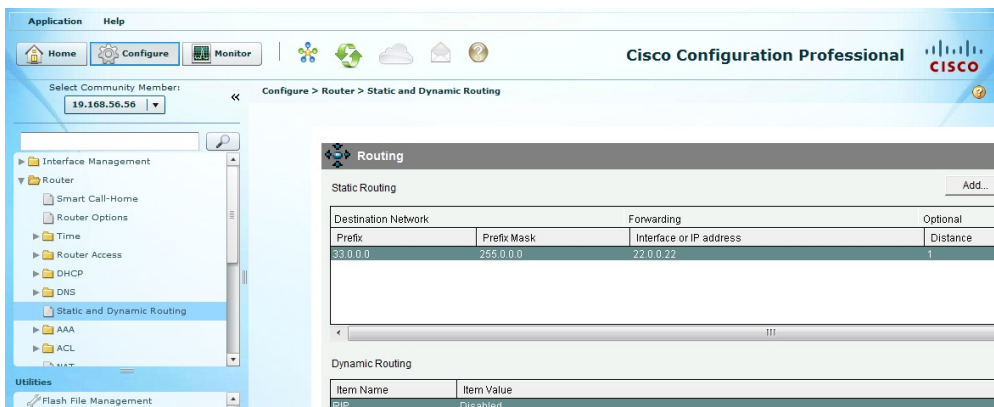
En el caso de router domésticos, la interfaz LAN suele traer una configuración de fábrica (habitualmente una IP 192.168.x.x) y la interfaz WAN suele venir configurada en IP dinámica con todos los parámetros necesarios. No obstante, si deseamos podemos cambiar la configuración de estos parámetros a través del entorno gráfico:



Hacer una copia de seguridad de la configuración:

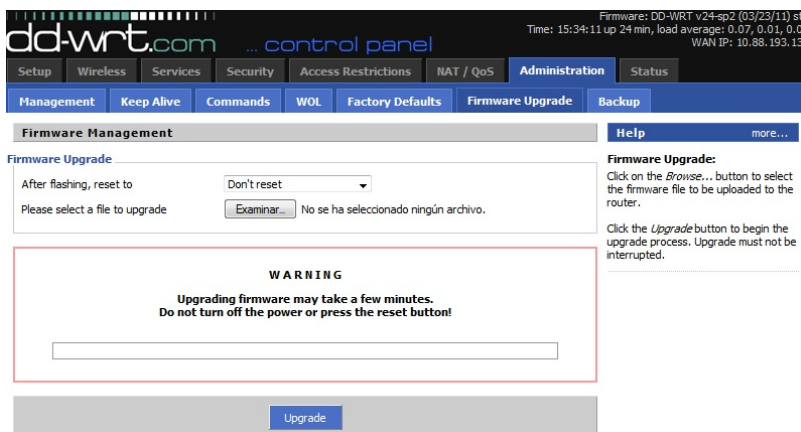


Mostrar la tabla de enrutamiento en Cisco Configuration Professional:



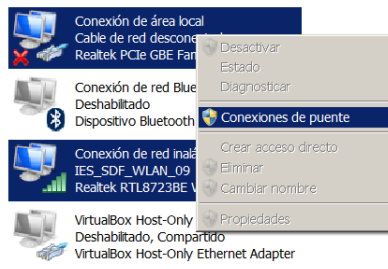
Actualización del firmware:

En el caso de routers domésticos, el firmware o software que maneja el dispositivo se actualiza normalmente a través de una pantalla web, pero cuidado, **no actualizar nunca desde una conexión WIFI** porque podemos perder la conexión en mitad de la subida del nuevo firmware y averiar el dispositivo:



6.- PC como switch

Nos vamos a "Conexiones de red", marcamos las dos tarjetas que formarán nuestro "switch" y marcamos conexiones de puente



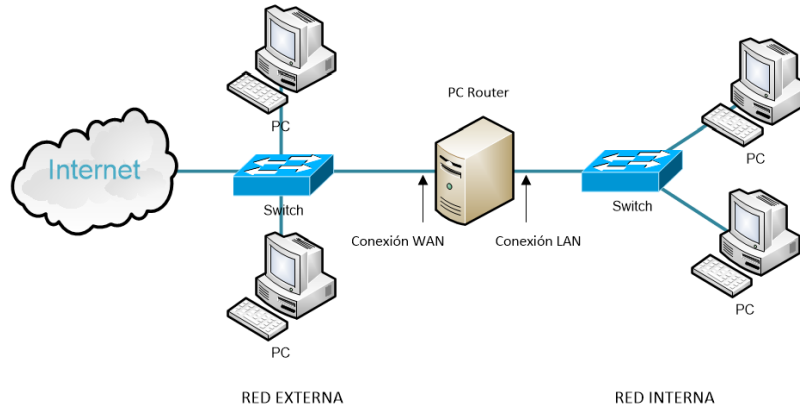
7.- PC como router

Para cambiar un poco este aspecto lo trataremos desde un sistema Linux.

Para que un equipo haga de router lo más básico es que tenga acceso a dos redes diferentes y, para ello, lo más sencillo es disponer de un PC con 2 tarjetas de red, en cada tarjeta de red estará conectada una red diferente.

Utilizaremos una máquina virtual Ubuntu con dos tarjetas de red, una tarjeta conectada a la red interna y una tarjeta conectada hacia la salida a internet.

Un esquema lógico podría ser el siguiente:



El primer paso para que nuestro equipo Linux permita la comunicación entre las redes es descomentar la línea `net.ipv4.ip_forward=1` en `/etc/sysctl.conf` y reiniciar el equipo:

```
root@manuel-VirtualBox: /
GNU nano 2.5.3 Archivo: /etc/sysctl.conf
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Como las dos redes están conectadas directamente enrutaría el tráfico entre ellas perfectamente, pero si queremos que realice las funciones del típico router casero tendríamos que activar el NAT:

```
iptables -t nat -A POSTROUTING -o WAN -j MASQUERADE
```

OJO, al configurar la conexión interna **no se debe poner puerta de enlace** puesto que esto crearía una ruta por defecto hacia la red interna que interferiría con la salida al exterior, es decir, buscaría la salida a internet por la red interna. Solo una ruta default y hacia el exterior, la tabla de enrutamiento sería similar a:

```
root@manuel-VirtualBox:/home/manuel# ip route
default via 192.168.1.1 dev WAN proto static metric 100
169.254.0.0/16 dev WAN scope link metric 1000
172.16.0.0/16 dev LAN proto kernel scope link src 172.16.0.1 metric 100
192.168.1.0/24 dev WAN proto kernel scope link src 192.168.1.2 metric 100
```

Anexo. Licencia de Recursos

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: Fabienne Serriere Licencia: CC BY-SA 3.0 Procedencia: https://es.m.wikipedia.org/wiki/Archivo:AMS-IX_optical_patch_panel.jpg		Autoría: Mariela Morales Licencia: Dominio público Procedencia: http://marielamoralesramirez.blog/2015/05/05/la-clasificacion-de-las-redes-de-telecomunicaciones/
	Autoría: Desconocido Licencia: CC BY-SA 3.0 Procedencia: https://es.wikipedia.org/wiki/Bluetooth		Autoría: Desconocido Licencia: Dominio público Procedencia: https://zigbeeallia.org/
	Autoría: Desconocido Licencia: CC BY-SA 3.0 Procedencia: http://s322749716.mialojamiento.es/triquet/index.php/es/ssoluciones/red-de-datos/181-diferencia-entre-wimax-y-lmids.html		Autoría: Desconocido Licencia: Dominio público Procedencia: https://www.wi-fi.org/
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Manuel Castaño Guillén Licencia: CC BY
	Autoría: Manuel Castaño Guillén Licencia: CC BY		Autoría: Captura pantalla Manuel Castaño Guillén Licencia: CC BY