



Universidad
de Oviedo

REDES



***TEMA 6B: CREACION DE REDES PRIVADAS Y CONEXIÓN A
INTERNET***



INDICE TEMA 6B

1. CREACIÓN DE REDES TCP/IP PRIVADAS	1
1.1 DIRECCIONAMIENTO.....	1
1.1.1 <i>Ventajas y Desventajas del Espacio de Direcciones Privado</i>	2
1.1.2 <i>Aspectos Operacionales</i>	3
1.2 DIVISIÓN EN SUBREDES	4
1.2.1 <i>Uso de Máscaras de Red</i>	5
1.3 SERVICIOS DE RED EN LA RED PRIVADA.....	5
1.3.1 <i>Servicios Básicos en Windows</i>	6
1.3.2 <i>Servicios Básicos en Unix</i>	6
1.4 CONFIGURACIÓN DE REDES MEDIANTE DHCP.....	7
1.4.1 <i>Funcionamiento de DHCP</i>	7
2. CONEXIÓN DE LA RED CON INTERNET	8
2.1 ACCESO AL SERVICIO.....	9
2.2 NAT.....	10
2.3 SERVIDORES PROXY.....	11



1. CREACIÓN DE REDES TCP/IP PRIVADAS

La arquitectura TCP/IP está íntimamente asociada a Internet, hasta el punto de ambas cosas pueden parecer lo mismo. En realidad, Internet es una unión de redes que se basan en la arquitectura TCP/IP, pero es un posible crear otras redes utilizando estos mismos protocolos. De hecho, existen muchas redes privadas que emplean esta arquitectura de red para resolver sus necesidades de comunicación. El calificativo “privadas” alude al hecho de que dichas redes no son accesibles desde fuera de la propia organización que las utiliza, e incluso es posible que desde dicha red tampoco sean alcanzables nodos fuera de la propia organización.

Son muchas las situaciones en las que sólo es necesario mantener la conectividad entre los nodos de una misma empresa. En otros casos, puede ser necesario el acceso al exterior para algunos servicios (por ejemplo el correo electrónico), sin que sea necesario que todos los nodos tengan un acceso directo al exterior. En el caso más general, lo habitual es que sólo un número reducido de nodos necesiten estar conectados con el exterior. Algunos ejemplos de estos casos son:

1. El sistema de pantallas de un aeropuerto puede estar basado en una red TCP/IP en la que cada pantalla es direccionable de forma individual, sin embargo no parece necesario (ni siquiera deseable) que dichos nodos puedan ser accedidos desde fuera del propio aeropuerto.
2. Un gran centro comercial puede disponer de terminales de venta que acceden a una base de datos mediante TCP/IP para consultar el precio del producto a partir de su código de barras, hacer reservas para los clientes o consultar si hay existencias de una determinada mercancía. En este caso, también resulta evidente que la conexión de todos estos equipos con el exterior resulta innecesaria.
3. Aún en empresas que si necesitan una conexión con el exterior, por ejemplo para el intercambio de correo electrónico con usuarios fuera de la propia empresa, es deseable que aquellos equipos que contienen información importante estén ocultos al exterior y sean solamente accesibles desde dentro de la organización.

Esta falta de conectividad con el exterior no impide que la red privada ofrezca a sus usuarios servicios de mensajería, servidores web o compartir de ficheros.

1.1 Direccionamiento.

La red de una empresa no necesariamente tiene que estar estructurada como una red local en la que todos los usuarios tienen acceso a toda la red. El número de equipos existentes en la red, la necesidad de restringir la visibilidad de los equipos o mejorar la eficiencia de la red son motivos suficientes para la creación de diferentes subredes (dominios), necesitando por tanto el uso de routers que encaminen el tráfico entre las distintas subredes.

Si la red privada nunca va a estar conectada al exterior, no es necesario preocuparse de que ninguna otra máquina a nivel mundial tenga reservada dicha dirección. Sin embargo, en caso de que nuestra red terminase por conectarse al exterior, el uso de direcciones cualesquiera podría terminar causando problemas de encaminamiento que nos obligarían a cambiar todas las direcciones de nuestros equipos. Para estos casos, la Internet



Assigned Numbers Authority (IANA) ha reservado tres bloques del espacio de direcciones IP para su uso en redes privadas (RFC 1918):

1. 10.0.0.0 a 10.255.255.255 (10/8 en notación CIDR): bloque de 24 bits
2. 172.16.0.0 a 172.31.255.255 (176.16/12): bloque de 20 bits
3. 192.168.0.0 a 192.168.255.255 (192.168/16): bloque de 16 bits

El primer de los bloques se corresponde con una dirección de red de clase A. El segundo está formado por 16 subredes contiguas de clase B, comenzando en la 172.16.0.0. Por último, el tercero corresponde a 256 subredes contiguas de clase C que comienzan con la 192.168.0.0.

No es necesario pedir permisos para el uso de estos rangos de direcciones. Estas direcciones sólo serán únicas dentro de la red privada de la empresa o empresas que decidan colaborar en una red privada conjunta.

Los nodos de la red que necesiten conectividad directa a nivel IP con Internet, deberán tener asignada una dirección pública válida. Dicha dirección debe ser obtenida a través de la autoridad competente. Ningún nodo público de Internet podrá tener asignada una dirección perteneciente a los bloques reservados para las redes privadas.

Para utilizar correctamente el espacio de direcciones privado, el primer paso será determinar que nodos no necesitan tener conectividad a nivel de la capa de red con nodos externos a la propia empresa en un futuro cercano y, por tanto, pueden ser clasificados claramente como nodos privados. Las direcciones para dichos nodos se seleccionarán de entre los grupos descritos anteriormente. Un nodo privado podrá comunicarse con cualquier otro nodo privado de la empresa, bien sea público o privado. Sin embargo, no podrán tener conectividad IP con nodos externos. El acceso de estos nodos a servicios de comunicaciones externos deberá realizarse a través de pasarelas correctamente configuradas.

Los nodos que no hayan sido clasificados como privados, serán públicos, y deberán tener asignada una dirección IP pública válida. Podrán comunicarse directamente (a nivel de red) con cualquier otro nodo público y con los nodos privados de la propia empresa. Nunca podrán acceder a nodos privados de otras organizaciones.

Convertir un nodo privado en un nodo público, o viceversa, implica necesariamente un cambio en su dirección IP, así como cambios en las entradas DNS correspondientes, y en los ficheros de configuración de cualquier máquina que referencia a dicho nodo por su dirección IP.

Dado que las redes privadas no tienen significado a nivel global, la información de encaminamiento sobre el interior de la red no debe ser propagada hacia el exterior. De la misma forma, datagramas IP con origen o destino en este tipo de nodos tampoco pueden viajar a través de la red. Para conseguir estas condiciones será necesaria la correcta configuración de los routers.

1.1.1 Ventajas y Desventajas del Espacio de Direcciones Privado

La principal ventaja del uso del espacio de direcciones privadas lo obtiene el conjunto de la comunidad en Internet, al permitir conservar un espacio de direcciones únicas global para todos los nodos públicos, al no usar direcciones públicas válidas cuando no es necesario.

Desde el punto de vista de la organización que utiliza este espacio de direccionamiento, la principal ventaja es el aumento de flexibilidad en el diseño de la red



privada, al disponer de un espacio de direcciones mucho mayor del que normalmente se podría disponer mediante la reserva de direcciones públicas. De esta forma se pueden usar esquemas de direccionamiento que faciliten el uso y la administración de la red, así como su posterior ampliación.

Si bien es cierto que es necesario cambiar las direcciones de aquellos nodos que pasasen de la red privada a la pública, el uso previo de direcciones privadas disminuye el riesgo de sufrir problemas de encaminamiento derivados de un encaminamiento ambiguo.

Un inconveniente asociado al uso del espacio de direcciones privadas es que en el caso de interconectar dos redes privadas diferentes, puede ser necesario reenumerar una de ellas. Este riesgo existe siempre, pero es minimizado si la dirección de la subred se elige al azar de entre todas las posibles. Para disminuir el impacto que puede provocar los cambios de direcciones, es aconsejable el uso de servidores DHCP (Dynamic Host Configuration Protocol) que permitan la configuración automática de los nodos al arrancar.

1.1.2 Aspectos Operacionales

Una posible estrategia es diseñar primero la parte privada de la red, y asignar direcciones pertenecientes al espacio de direcciones privado en todos los nodos internos de la misma. En una segunda fase se planearán las subredes públicas y su conexión con el exterior.

El diseño puede ser modificado posteriormente si algún nodo es trasladado de la parte pública a la privada o viceversa. Normalmente será suficiente con reconfigurar su direccionamiento y cambiar su cableado físico. Aunque es posible, no resulta conveniente que distintas subredes compartan el mismo medio físico, ya que esta situación complica la administración de la red.

Resulta necesario un correcto diseño del esquema de división en subredes. Si el equipo disponible lo soporta, es aconsejable utilizar el bloque de direcciones de 24-bits del espacio de direccionamiento privado para obtener un esquema de direccionamiento que facilite el crecimiento futuro de la red. De no ser posible el uso de estas direcciones, se emplearía el bloque de 20-bits o el de 16.

Es muy aconsejable que los equipos que conecten la red con el exterior se configuren adecuadamente para que filtren el tráfico y la información de encaminamiento de forma correcta. Se debe evitar que el tráfico externo penetre en la red privada y viceversa. Además también debe evitarse se propague información sobre rutas privadas hacia el exterior.

Con un diseño adecuado, es posible que dos empresas con un esquema de direccionamiento coordinado se comuniquen entre sí mediante el uso de los enlaces punto a punto adecuados. Otra posibilidad es que lo hagan a través de la red pública. Para ello, es necesario que los puntos de frontera entre la red pública y las redes privadas dispongan de los medios hardware/software adecuado para encapsular datagramas IP de la red privada en paquetes capaces de viajar por la red pública.

Se deberá prestar especial atención en la configuración de los servicios de red para evitar conflictos entre las zonas pública y privada. Por ejemplo, si se configura un servidor DNS para resolver las direcciones IP en la zona privada, sus entradas nunca deberían propagarse hacia el exterior de la red.



1.2 División en Subredes

En general, Internet es vista como una jerarquía con dos niveles. En el nivel superior Internet como conjunto, y el nivel inferior las distintas redes que la componen cada una con su dirección de red propia. Con esta visión, cada nodo ve su red como una única entidad. Aunque este modelo es útil, en determinados casos es interesante introducir un nivel más, de modo que cada red se encuentre dividida a su vez en un conjunto de subredes. En este caso, cada nodo pertenece a una subred y no tendrá acceso a nodos de otras subredes si no se proporciona la información de encaminamiento adecuada.

Esta jerarquía de tres capas es útil para describir aquellas redes privadas formadas por varias redes locales diferentes (es decir, que no comparten el mismo medio físico). Son varias las razones por las que una organización puede tener varias redes locales diferentes:

- Uso de diferentes tecnologías: Ethernet, Token Ring, etc.
- Limitaciones de la tecnología usada: En general, las tecnologías LAN imponen limitaciones basadas en las características eléctricas del medio físico, el número de nodos conectados al mismo o la longitud total máxima del medio.
- Congestión de la red: Las características del tráfico de la red local puede hacer necesario su compartimentación en subredes formadas por aquellos nodos entre los que las comunicaciones son más frecuentes, para evitar así la degradación del comportamiento de la red.
- Existencia de enlaces punto-a-punto: En algunos casos, la red local está formada por grupos de nodos separados una distancia considerable. Ambos grupos pueden ser conectados mediante un enlace punto a punto de alta velocidad.

El problema asociado a la existencia de varias redes locales diferentes es que la comunicación entre nodos de diferentes redes obliga a la utilización de software y hardware de red que permita encaminar los mensajes entre las diferentes LAN. Utilizando la familia de protocolos TCP/IP, existen tres posibles soluciones:

1. Utilizar un identificador de red diferente para cada LAN.
2. Usar un único identificador de red y asignar las direcciones a los nodos de forma independiente de la red local en la que se encuentran.
3. Usar un único identificador de red y repartir el rango de identificadores de host mediante la asignación explícita de identificadores de subred.

Cada una de estas estrategias tiene sus propios inconvenientes. En el primer caso, aunque no se requieran nuevos protocolos, puede provocar un gran incremento en las tablas de rutas. Dichas tablas reflejarán la estructura interna de nuestra red.

En el segundo caso, será necesario usar algún protocolo que haga que las distintas redes LAN parezcan una sola. Si por ejemplo se utilizan redes LAN en las que está implementado el protocolo de resolución de direcciones (ARP), puede lograrse el objetivo anterior si los puentes entre las distintas subredes son capaces de capturar las peticiones ARP para nodos que estén en una LAN distinta. Además, el puente debe ser capaz de averiguar a que LAN pertenece el destino de la pregunta ARP mediante un algoritmo que permita difundir, en modo broadcast, la petición ARP hacia todas las redes LAN a las que está conectado. A medida que crece el número de redes LAN, la complejidad asociada a este método aumenta enormemente.

La tercera solución consiste en proporcionar un soporte explícito para las subredes. Para poder usar esta solución basta con que la implementación de la capa IP sea capaz de manejar máscaras de red, algo común en las implementaciones actuales.

1.2.1 Uso de Máscaras de Red.

La división de una red en subredes se hace mediante la definición de una máscara para la dirección IP, que permita separar la parte asignada a la subred y la parte asignada al identificador de host dentro de la subred. Este esquema permite fácilmente conmutar entre el empleo estándar de las direcciones IP y la creación de subredes. Además ofrece una gran flexibilidad a la hora de determinar el número de subredes que necesitan distinguirse.

De esta forma, la dirección IP de un nodo se interpretará de la siguiente forma:

<identificador de red> <identificador de subred> <identificador de host>

donde el identificador de red es el definido por la clase de direccionamiento IP a la que pertenezca la dirección, el identificador de host posee al menos 1 bit, y la longitud del identificador de subred es constante para una red dada. Si la longitud de este último campo es cero, entonces la red no está dividida en subredes. Por ejemplo, una dirección de clase B con 6 bits para el identificador de subred tendría la estructura:

1																2																3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1						
1										2										3																											
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1						
1	0	ID. DE RED										ID. SUBRED										ID. DE HOST																									

Como los bits que especifican la subred están indicados por la máscara, no es necesario que sean contiguos. Sin embargo, la práctica recomendada es que sean contiguos y ocupen los bits más significativos del identificador de host. En cualquier caso, deben respetarse las direcciones especiales. Es decir, el identificador cero hará referencia a “este”, y el identificador formado por todos los bits a 1 hará referencia a “todos”. Así, en el ejemplo anterior podrían distinguirse hasta 62 subredes, ya que los identificadores 0 y 63 se emplearían para distinguir la subred a la que pertenece un host, y todas las subredes respectivamente.

Para permitir el tráfico entre subredes, deberán configurarse los correspondientes gateways con las tablas de encaminamiento adecuadas.

1.3 Servicios de Red en la Red Privada.

Una vez configurados los distintos nodos de la red, sus gateways y/o routers, el tráfico se encaminará de un nodo origen hacia otro sin problemas. Sobre dicha plataforma será posible instalar servidores y clientes de cualquier tipo, siempre y cuando estén basados en redes TCP/IP. Algunos servicios como servidores de nombres, o servidores DHCP pueden ser muy deseables para facilitar la operación y mantenimiento de la red. Cualquier otro servicio también podrá ser instalado y accedido desde la red. Evidentemente dichos servicios serán locales. Por ejemplo, si se instala un servidor de correo SMTP, se podrá ofertar correo electrónico a los usuarios de la red con la única restricción de que sólo podrán intercambiar correos con otros usuarios de la red privada.



1.3.1 Servicios Básicos en Windows

Windows incluye varios clientes TCP/IP, pero ninguna posibilidad de ofertar servicios a otras plataformas. En la instalación por defecto de Windows, al instalar el protocolo TCP/IP, se instalan también las siguientes aplicaciones:

- cliente ftp
- cliente telnet
- navegador web (Internet Explorer)
- cliente POP3/IMAP (Outlook/Outlook Express)
- ping: solicitud de eco
- netstat: permite comprobar el estado de las conexiones TCP/UDP
- ipconfig: permite consultar/modificar la configuración de los diferentes adaptadores de red instalados y asociados a la pila de protocolos TCP/IP
- traceroute: permite analizar las rutas hasta un determinado destino
- arp: permite editar la tabla creada por el protocolo ARP
- route: permite editar la tabla de rutas

Estas aplicaciones configuran un buen conjunto de herramientas para una estación que actúe como cliente de servicios de red. La instalación de servidores depende fundamentalmente de otros vendedores de software, aunque las últimas versiones de Windows suelen permitir la instalación de pequeños servidores proxy o web, y capacidad de encaminamiento automático con filtrado por puertos y direcciones.

Para compartir archivos se utiliza SMB. SMB es un servidor de archivos propietario de Windows que puede ejecutarse sobre TCP/IP o sobre el protocolo de transporte NetBIOS. En plataformas UNIX existen clientes y servidores compatibles con SMB (SAMBA). Sin embargo, es difícil disponer de servidores y/o clientes NTFS para plataformas Windows a pesar de que sea un protocolo TCP/IP estándar.

En caso montar una red Windows sobre TCP/IP que se extienda más allá de una red local, será necesario instalar un servidor WINS o editar convenientemente el fichero LMHOSTS en el directorio de instalación de windows. Dicho fichero cumple una tarea similar a la del fichero hosts de los sistemas Unix. El fichero sirve para asociar un nombre de recurso con una dirección.

1.3.2 Servicios Básicos en Unix

El desarrollo de los protocolos TCP/IP está íntimamente ligado a los sistemas Unix, básicamente porque la mayor parte de las aplicaciones se implementaron inicialmente sobre este tipo de sistemas operativos dada su amplia difusión en las universidades de Estados Unidos. Quizá por ello, la práctica totalidad de distribuciones de dicho sistema operativo incluyen todo tipo de servidores y clientes. Lo más habitual era que la configuración de los mismos se hiciese editando manualmente los ficheros correspondientes. Sin embargo, las nuevas distribuciones de estos sistemas suelen incorporar aplicaciones que nos guiarán en la configuración de dichos ficheros. Estos equipos pueden trabajar como servidores y/o clientes. Tanto en la documentación del sistema operativo como en la amplia literatura disponible se puede encontrar la información suficiente para instalar, configurar y administrar todos estos servicios. Como indicación de la gran variedad de servicios disponibles, basta decir que las distribuciones habituales de Linux incluyen software para la implementación de Firewalls.



1.4 Configuración de Redes Mediante DHCP

El protocolo DHCP está descrito en las RFC 1541, 2131 y 2132. Es un protocolo que permite la configuración automática de los nodos de una red. Funciona con un esquema cliente-servidor. El cliente se ejecuta en cada nodo que desea configurar su pila de protocolos TCP/IP de forma automática. El servidor deberá realizar la reserva de direcciones IP y distribuir al cliente los parámetros necesarios para la configuración de su interfaz TCP/IP.

El uso de servidores DHCP proporciona al administrador de la red la capacidad de ajustar remotamente la configuración de las máquinas cliente. DHCP proporciona dos ventajas principales:

- No es necesaria ninguna configuración por parte del usuario final.
- Tampoco es necesario mantener una voluminosa base de datos con las direcciones IP y los nombres de todas las máquinas que componen la red.

De esta forma, DHCP libera al administrador de realizar un conjunto de tareas poco productivas y que exigen mucha dedicación. Sin embargo, también puede limitar su capacidad para resolver los problemas de los usuarios individuales. Las direcciones se actualizan según una unidad de tiempo, denominada duración de la *asignación DHCP*. Cuando la asignación caduca, la dirección puede reasignarse a la misma máquina o otra diferente. Es responsabilidad del cliente la renovación de la licencia de la dirección IP asignada, cuando haya transcurrido la mitad del tiempo de asignación. Por lo general, la dirección se puede renovar indefinidamente. Si una asignación llega a caducar, es posible que el servidor DHCP asigne una configuración IP diferente a la misma máquina. Esta acción origina el que el administrador de la red no tenga ninguna forma adecuada de saber quién tiene una determinada dirección en un determinado instante de tiempo y, en su lugar, lo único que posee es una lista de direcciones IP y las direcciones hardware a las que están asignadas.

1.4.1 Funcionamiento de DHCP

Debido a que, cuando una máquina se está configurando, todavía no dispone de dirección IP, el servidor DHCP debe ser capaz de comunicarse con ella utilizando la dirección hardware. El primer paso consiste en que el cliente envíe una solicitud DHCP a la red. Este paquete se difunde mediante una trama broadcast que será reconocida como una consulta DHCP por el nodo en el que está corriendo el servidor. Tras recibir la solicitud, el servidor DHCP ofrecerá una dirección a la computadora cliente mediante el envío de un paquete a la dirección hardware que emitió la petición. Dicho paquete contiene una dirección IP libre que puede ser utilizada por el cliente. El cliente deberá responder a dicho ofrecimiento con una solicitud de utilización de la dirección ofrecida. Previamente el cliente habrá asignado la dirección ofrecida a su dispositivo de red. El servidor DHCP dispondrá de la posibilidad de aceptar o rechazar la solicitud de utilización. Si la solicitud es denegada, el proceso deberá comenzar de nuevo.

El protocolo DHCP deriva del protocolo BOOTP (Protocolo de Arranque), de hecho es un ampliación del mismo. Como principal ventaja, DHCP se puede ejecutar desde un único servidor a través de diferentes subredes.



2. CONEXIÓN DE LA RED CON INTERNET

La forma de conectar una red privada a Internet dependerá mucho de las necesidades de comunicación que se tengan: ancho de banda, número de puntos de acceso, calidad de servicio, periodos de utilización, etc. El sistema de conexión puede llegar a ser muy sofisticado, pero el esquema es similar independientemente del tipo de tecnología utilizado.

Como norma general, accederemos a Internet gracias a la formación de algún tipo de contrato con un proveedor de servicios de Internet (ISP). En ese contrato se fijarán las condiciones del acceso:

- Ancho de banda.
- Tarifas.
- Uso de direcciones IP fijas, y en su caso, número de direcciones asignadas.
- Tipos de servicios prestados.
- Capacidad para disponer de servidores propios, etc.

En los siguientes apartados se citarán las formas más habituales de conexión y como poder extender el uso de ciertos servicios de comunicaciones a nodos de la red privada.

A la hora de proporcionar un acceso a Internet a los usuarios de una red privada, se deben abordar dos cuestiones clave. La primera es elegir el tipo de conexión y la segunda el nivel de seguridad que se desea obtener. Una vez decididos ambos aspectos se podrá diseñar e implementar la solución más adecuada.

Hoy en día existe una gran variedad de opciones para conectarse a Internet, aunque la disponibilidad real variará en función de la localización geográfica. Así por ejemplo, una conexión a través de la red telefónica básica es prácticamente universal, lo que no sucede con las conexiones de banda ancha. Por eso, siempre será necesario consultar con los proveedores cuáles son los servicios realmente disponibles. Los puntos clave a considerar serán:

- **Tipo acceso:** Hoy en día los tipos de acceso preferido son el cable, XDSL, o los accesos de banda ancha (Líneas T1) debido a su alta velocidad, su capacidad para soportar múltiples usuarios sobre una única conexión y el establecimiento permanente de la conexión. Las alternativas más habituales son:
 1. **Conexiones vía módem:** Las conexiones vía módem a través de la línea telefónica son una opción muy extendida (sobre todo entre usuarios particulares) debido a su gran disponibilidad. Con los módem existentes en la actualidad, pueden alcanzarse velocidades de hasta 56Kbps en función de la negociación de opciones efectuada entre ambos extremos de la conexión. En la práctica, las velocidades máximas que se alcanzan son 53Kbps para descargas y 13Kbps para envíos. Aparte de las consideraciones de velocidad, un inconveniente asociado a la conexión vía módem es que la línea telefónica queda bloqueada para llamadas.
 2. **Líneas RDSI:** La conexión RDSI básica proporciona un canal a 64Kbps a la vez que permite mantener disponible una línea de voz. También es posible acceder a velocidades mayores (múltiplos de 64K) en función del tipo de contrato.
 3. **Cable Módem:** Con velocidades que alcanzan los 2 Mbps, las conexiones a través de proveedores de cable son una alternativa razonable para la conexión permanente a Internet. Su disponibilidad depende de la zona y del proveedor elegido. Al ser una conexión permanente, se elimina todo el procedimiento de establecimiento de conexión mediante llamadas, y la facturación depende de la



calidad de servicio demanda. La conexión permanente también implica un mayor riesgo a ataques procedentes del exterior, por lo que es aconsejable la instalación de algún tipo de firewall. Las conexiones por cable son un medio compartido, por lo que se pueden experimentar reducciones en el ancho de banda disponible en función del tráfico generado por otros usuarios de la misma zona.

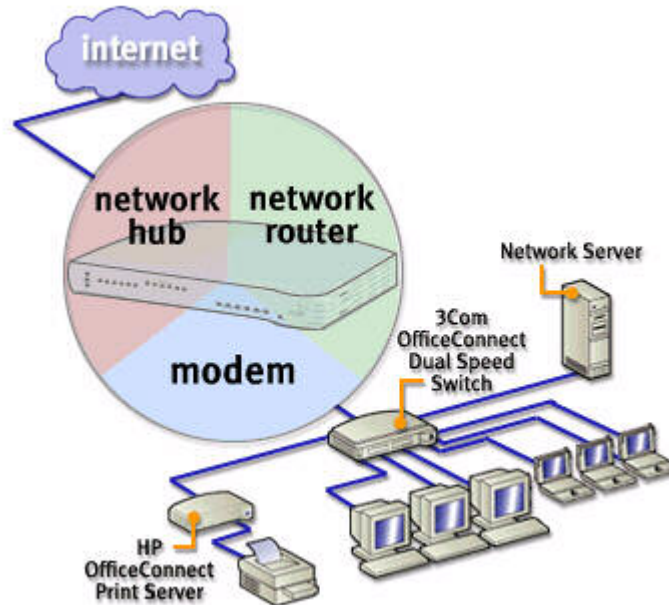
4. Conexiones XDSL: Los distintos tipos de líneas DSL (ADSL son las más comunes) permiten mezclar voz y datos sobre una misma línea telefónica convencional. Sin embargo, la prestación del servicio dependerá de las características de la central telefónica a la que esté conectada nuestra línea, es decir, no todas las líneas telefónicas permiten el uso de DSL. Como ya se comentó, ADSL es el servicio DSL disponible con más facilidad, soportando velocidades de hasta 8Mbps, aunque lo más habitual es disponer de conexiones a 1.5Mbps. Conviene tener en cuenta que estas velocidades son para la descarga, mientras que las velocidades de envío suelen ser casi de un orden de magnitud inferiores. Las líneas SDSL solucionan dicho problema, ofreciendo un comportamiento simétrico para ambos sentidos del tráfico, con velocidades de hasta 1.5 Mbps. SHDSL es una variante de SDSL que permite alcanzar mayores velocidades en función del número de hilos usados en la conexión. Las conexiones XDSL son permanentes, por lo que se evita el establecimiento y liberación de las conexiones. La conexión XDSL entre nuestro punto de acceso y el proveedor es una conexión dedicada, por lo que las características del enlace contratado permanecen inalterables.
5. Otras conexiones: Dependiendo de la ubicación geográfica y del proveedor, puede ser posible acceder a líneas de gran ancho de banda, como por ejemplo conexiones T1 o T3. Su uso sólo se justifica si las demandas de comunicaciones de la empresa son realmente elevadas. Este tipo de conexiones es permanente y pueden incluir tanto líneas de voz como de datos. Al igual que en los casos anteriores, será necesario establecer firewalls que eleven el nivel de seguridad.
 - **Tipo de uso**: Debe considerarse el nivel de tráfico que se generará, teniendo en cuenta el número de usuarios que pueden estar accediendo simultáneamente, la frecuencia de acceso, la duración de las conexiones y el volumen de información transmitido. También deberán tenerse en cuenta las características de la información: texto, gráficos,.... En cualquier caso, debe establecerse un balance entre el ancho de banda demandado, su coste, y los beneficios que comporta.
 - **Crecimiento**: La contratación de un determinado tipo de acceso a Internet supone una serie de costes fijos que dificultarán el cambio a otros tipos de conexión, por ello, debe prestarse atención a las expectativas de crecimiento; número de usuarios, tipo de servicios demandados, etc.

2.1 Acceso al servicio

El tipo de dispositivo usado para acceder a Internet depende del tipo de enlace seleccionado. Sin embargo, en cualquier acceso compartido existen tres funcionalidades básicas necesarias para que la solución funcione: módem, router de red y hub (o switch).

La parte del router de acceso correspondiente al módem es la que proporciona la conexión física al ISP. En este caso, el concepto módem debe ser entendido en sentido amplio, y su tecnología variará en función del tipo de conexión utilizada: línea telefónica básica, RDSI, cable, ADSL, ...

El router de acceso también ejercerá funciones de router, de forma que encaminará la información saliente hacia su destino. Además permitirá la conexión de varios usuarios internos hacia el exterior a través de una única cuenta de acceso a Internet, mediante la tecnología NAT (Network Address Translation). No todo el hardware utilizado para la conexión a Internet dispone de esta funcionalidad. En esos casos, deberá suplirse mediante la compra de hardware/software adicional que proporcione esta función.



La función de concentrador (o switch) permite la conexión de la red interna con el router de acceso a Internet. Al igual que en el caso anterior, no todos los equipos para la conexión a Internet proporcionan esta funcionalidad, por lo que será necesario incorporar equipos adicionales.

Habitualmente, los equipos utilizados para la conexión a servicios de banda ancha suelen incorporar las tres funcionalidades. En esos casos suele hablarse propiamente de un router de acceso propiamente dicho. El punto de acceso es visto como un nodo más de la red interna y será el que realice las funciones de gateway, encaminando el tráfico saliente y entrante. A su vez puede ser considerado como un firewall básico que oculta al exterior la estructura de nuestra red interna.

En otros casos, el proveedor ISP sólo proporciona las funcionalidades correspondientes al módem. En ese caso, será el propio usuario el que deberá implementar la funcionalidad del gateway mediante la adquisición del hardware y el software apropiado. Estos equipos pueden ser desde equipos específicos hasta un ordenador personal de la red interna ejecutando el software adecuado.

2.2 NAT

NAT (Network Address Translation) es similar a la técnica denominada “enmascaramiento IP” y en ocasiones ambos términos se emplean indistintamente. NAT constituye una técnica muy rápida y eficaz para conectar una red local TCP/IP con Internet. La mejor parte del uso de NAT es que es totalmente transparente para la red interna. Las computadoras cliente pueden usar todos los protocolos que quieran para conectarse con el mundo exterior sin necesidad de modificaciones. Para la red interna parecerá que todos los nodos estuviesen directamente conectados a Internet, mientras que desde el exterior sólo



será visible el router de acceso. Todas las conexiones con el exterior parecerán provenir del único nodo que tiene una IP válida. Es la tecnología NAT la que reenvía las contestaciones recibidas hacia el interlocutor interno que inició la comunicación. La principal desventaja es que, sin una configuración especial, no hay forma de proporcionar servicios al exterior desde una computadora de la red privada. De esta forma, todos los servicios que se ofrezcan deberán ejecutarse en el nodo que esté ejecutando NAT.

NAT funciona de forma similar al modo en que se traducen las direcciones de hardware en direcciones IP en los encaminadores y puentes. Las computadoras cliente están configuradas para ver el servidor NAT como pasarela. Cuando se envía un paquete desde un cliente, llega a la pasarela, la cual coloca su propia información IP en el paquete, sustituyendo la dirección IP original. Dado que este nodo tiene conexión directa con Internet, enviará el paquete hacia su destino a través del router que tenga configurado para su dirección IP pública. Cuando llega un paquete de respuesta, la pasarela sustituye la dirección de destino con la dirección de la computadora que envió el paquete original y encamina el nuevo paquete hacia la red interna. Además de traducir la dirección, NAT también debe modificar la información de encabezado y sumas de comprobación del paquete.

La diferencia principal entre NAT y el enmascaramiento IP es el número de máquinas que puede servir el software. NAT permite un número de clientes ilimitado mientras que el enmascaramiento IP no.

Si se desea proporcionar servicios en Internet desde un nodo de la red privada, lo primero que debe tenerse en cuenta es si el contrato firmado con el proveedor nos permite ofrecer dicho servicio. Además se deberá configurar NAT de modo que acepte conexiones entrantes en un determinado puerto como peticiones dirigidas a un determinado nodo de la red interna en el que realmente se está ejecutando el servidor. De esta forma, el gateway dirigirá todo el tráfico entrante a través de dicho puerto hacia una misma dirección interna.

2.3 Servidores Proxy

Otra forma de compartir una conexión a Internet consiste en ejecutar los llamados servidores proxy en el nodo que esté conectado directamente a la red. Los servidores proxy actúan de forma similar a los routers, pero a nivel de aplicación. Así por ejemplo, si desde un nodo de la red interna se desea acceder a una página web, la petición se dirigirá al proxy correspondiente. Este redirigirá la petición al exterior, y una vez recibida la respuesta, la enviará a la máquina que le hizo la petición inicial. El software de proxy suele mantener una caché con las páginas recibidas de modo que posteriores peticiones de una misma página se podrían atender sin volver a descargarla. Esta solución mejora los retardos si diversos usuarios acceden a las mismas páginas. Sin embargo, implica problemas tales como la caducidad de la información almacenada o el espacio ocupado.

Un inconveniente adicional asociado a los servidores proxy, consiste en que es necesario activar una pasarela por cada servicio que se quiera compartir. Además, los clientes deberán ser configurados específicamente para acceder al servicio a través del proxy, por lo que las aplicaciones seleccionadas (y en ocasiones los propios protocolos) necesitan estar preparadas para soportar este tipo de funcionamiento.