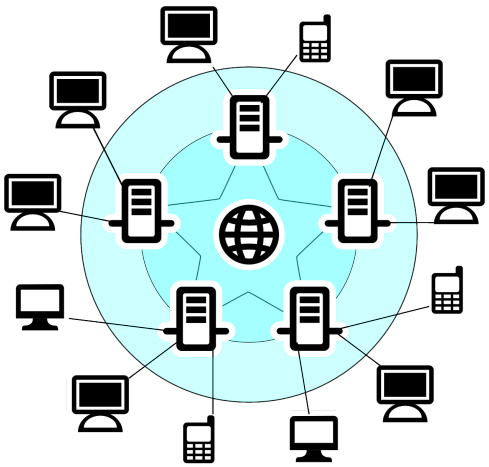
Redes Locales - 1º SMR
Tema 4: Interconexión de redes locales

por Fernando Albert y Javier Carrasco

4.1. Introducción



Hasta este punto se han estudiado los elementos básicos de conexión a nivel físico y lo concerniente a la parte lógica. En este tema trataremos las diferentes maneras que disponemos para poder interconectar equipos y segmentos de red.

Se abordará la creación de redes de área local virtuales, herramienta que nos permitirá aumentar la flexibilidad del sistema de cableado, independientemente de la ubicación geográfica.

Por lo general, muchos servicios son proporcionados por equipos dentro de la misma red local, pero en ocasiones, deberemos ir más allá, salvando así la distancia geográfica que los separa. Para ello, estudiaremos las tecnologías utilizadas para conseguir un acceso remoto.

Comenzaremos viendo los distintos dispositivos o herramientas desde el interior de la red hacia fuera, de forma que se irá aumentado la complejidad de éstos. También haremos distinción entre interconexión de redes cableadas y redes inalámbricas.

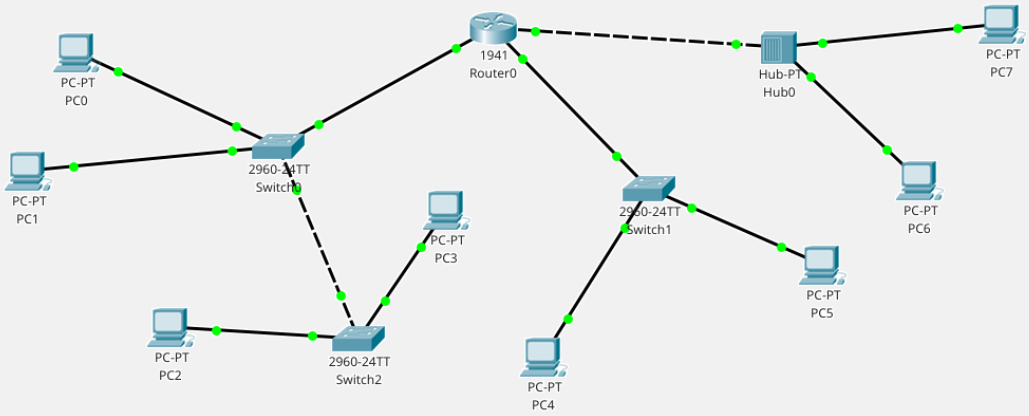
Antes de comenzar a tratar en profundidad el tema, existen dos conceptos con los que deberemos familiarizarnos.

- **Colisión:** estas se producen cuando dos hosts transmiten tramas de forma simultánea. Al producirse una colisión, las tramas pueden dañarse o destruirse, deteniéndose la transmisión por un periodo aleatorio de tiempo.
- **Broadcast:** es un paquete de datos que se envía a todos los nodos de una red. Estos paquetes se identifican por su dirección de broadcast.
- **Dominio de colisión:** es la porción de la red en la que dos nodos pueden colisionar. Dos nodos de la red pertenecen al mismo dominio de colisión si sus tramas pueden interferir entre sí. Dominio de colisión es, por tanto, un subconjunto físico de la red donde es posible que las tramas de red de un nodo puedan colisionar o interferir con las de otro, provocando la necesidad de retransmisiones y una pérdida del rendimiento de la red.
- **Dominio de broadcast:** es el área lógica de una red, en la que cualquier equipo conectado a ella puede retransmitir sin necesidad de un dispositivo de encaminamiento, ya que comparten la misma subred y puerta de enlace al encontrarse en la misma LAN.

Dispositivos de interconexión y su relación con los diferentes tipos de dominio	
Repetidores y *hubs*	Un sólo dominio de colisión Un sólo dominio de *broadcast*
Switches	Segmenta el dominio de colisión Un sólo dominio de *broadcast*
Routers	Segmenta el dominio de colisión Segmenta el dominio de *broadcast*

Ejercicios propuestos

4.1.1. Identifica en el siguiente esquema los dominios de colisión y *broadcast* que consideres



4.2. Dispositivos de interconexión de redes

Como ya se ha comentado al inicio del tema, los dispositivos que van a detallarse a continuación nos permitirán la interconexión entre equipos de red y entre segmentos de red.

4.2.1. Repetidores

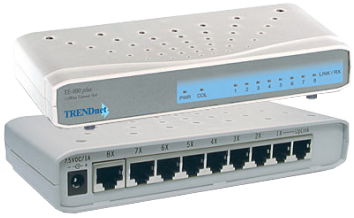
De todos es sabido que las instalaciones cableadas tienen la limitación de la distancia, siendo muy recomendable no sobrepasar segmentos de más de 100 metros, aún así, se produce pérdida de señal y generación de ruido.

Los repetidores son dispositivos electrónicos que conectan dos segmentos de una misma red, pasando el tráfico de un extremo al otro. El repetidor evita los problemas de distancia reconstruyendo y amplificando la señal y eliminando los ruidos.

Los repetidores trabajan a nivel físico o capa 1 del modelo OSI ya que trabajan con señales. Esto permite que sean dispositivos de red muy rápidos, pero no pueden procesar los datos. Esto puede ser un problema en determinados casos, ya que al no discriminar el tráfico de la red, pueden producirse colisiones en los segmentos de red.

Podemos encontrar diferentes tipos de repetidores, existen repetidores que se pueden utilizar para convertir la señal de un tipo de cableado a otro tipo. Por ejemplo, se podría cambiar una señal de entrada 10Base2 (coaxial) a una señal de salida 10BaseT (par trenzado).

4.2.2. Concentradores



También conocidos como *hub*, tienen varios puertos de conexión por los que se retransmiten cada uno de los paquetes que se reciben por uno de los puertos. Los *hub* básicamente extienden la funcionalidad de la red cableada, alcanzando así mayor distancia, por lo que podríamos considerarlos un repetidor. Los *hubs* transmiten los paquetes a todos sus puertos, por lo que todos los equipos conectados a esos puertos recibirán la misma información.

Se utilizan para implementar redes con topología en estrella y para la ampliación de la red LAN, por lo que los *hubs* trabajan en el **nivel físico** o capa 1 del modelo OSI.

Los *hubs* se limitan a copiar los datos de un segmento de red a otro, no atienden a direcciones de red, protocolos o servicios, por lo que no requieren configuración alguna. Por contra, no aísla los problemas del tráfico generado en cada uno de los segmentos, por ejemplo, si se produce una colisión en uno de los segmentos, ésta se propagará a todos los demás.

4.2.3. Puentes

En inglés conocidos como *bridges*, permiten conectar dos segmentos de red al igual que los repetidores y los *hub*. La diferencia radica en que los puentes son capaces de seleccionar el tráfico que pasa de un segmento a otro, de esta forma, únicamente el tráfico que debe ir de un segmento a otro pasará a través del *bridge*, reduciendo así el tráfico.

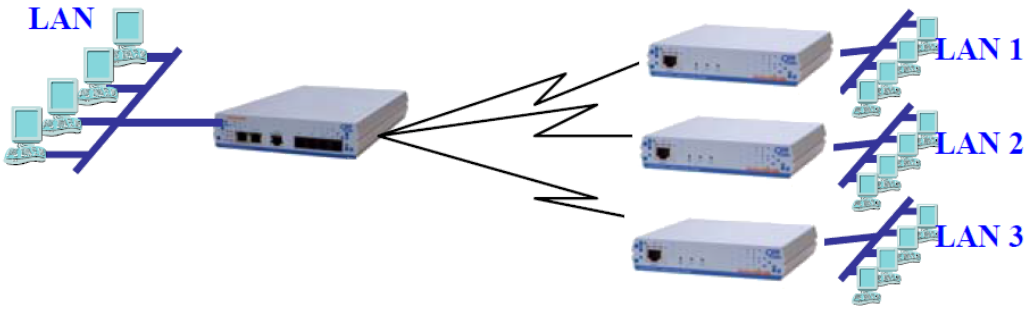
El *bridge* comprueba donde se encuentra la dirección destino y hace la copia de los datos hacia el segmento en el que se encuentre dicha dirección. Los *bridges* trabajan en el **nivel de enlace** o capa 2 del modelo OSI. Al trabajar en este nivel, son capaces de comprobar el campo de control de errores para asegurar la integridad de la trama y, en caso de encontrar un error, la eliminaría de la red. Gracias a esta comprobación tramas erróneas o incompletas no pasarían la frontera del segmento de red donde se produjo el fallo.

Las redes conectadas mediante *bridges*, en apariencia, son una única red, esto es debido a que la función de estos dispositivos es totalmente transparente.

Los *bridges* son capaces de interconectar redes de distintas topologías, cuando esto ocurre, deben encargarse de traducir las tramas de una topología a otra.

Se pueden distinguir dos tipos de puentes:

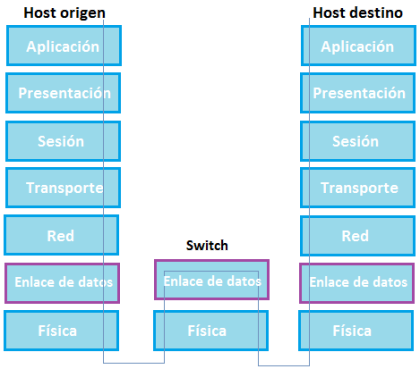
- **Locales:** se utilizan para enlazar dos redes físicamente cercanas.
- **Remotos:** estos se conectan en parejas, enlazan dos o más redes locales creando así una red de área extensa mediante líneas telefónicas.



4.2.4. Conmutadores

Los conmutadores, o *switches*, permiten conectar dos o más segmentos de red, o varios *hosts*, pasando entre los segmentos de red los datos según la dirección de control de acceso al medio (MAC) destino. Esto significa que son multipuerto, además, los *switches* son dispositivos locales.

Para realizar dicha función, disponen de una pequeña memoria asociativa que almacena las direcciones físicas de los dispositivos conectados a sus puertos. Estos dispositivos trabajan en el **nivel de enlace** o capa 2 del modelo OSI, actuando como si de filtros se tratasen.



Las funciones de los *switches* y los *bridges* son las mismas, pero a diferencia de los bridges, los *switches* pueden interconectar más de dos segmentos de red.

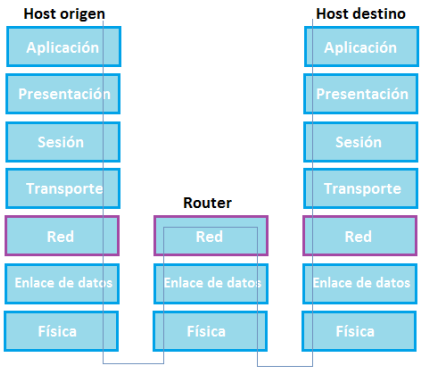
Podemos considerar un *switch* como un hub pero más inteligente, el *switch* reconocerá las direcciones MAC que le llegan por cada uno de sus puertos y enviará la información por el que considere más adecuado, de esta forma se reduce la carga en la red.

Existen *switches* profesionales, éstos también se conocen como *"gestionables"*. Dicha gestión se realizará mediante los protocolos típicos de gestión de red (SNMP, RMON, etc). Cuando la eficacia de una red depende de este tipo de conmutadores, es necesaria una vigilancia estrecha.

4.2.5. Encaminadores o enrutadores

También conocidos como *routers*, estos dispositivos trabajan entre redes de área local aisladas que utilizan las mismas direcciones y protocolos y/o se encargan de encaminar la información según la ruta más conveniente posible. También son capaces de convertir paquetes de red LAN en paquetes capaces de ser enviados a redes de área extensa.

La primera función que debe realizar un *router*, es saber si el destinatario de la información está en la misma red de la que proviene o en otra diferente. Para saberlo, el *router* utiliza la máscara de subred. La máscara de subred determina a que red pertenece un equipo en concreto. Si la máscara de subred de un paquete de información enviado no corresponde a la subred de la que proviene, el *router* determinará que el destino de



dicho paquete será otro segmento de red diferente o debe salir a otra red (WAN). Los *routers* trabajan a nivel de **capa de red** o nivel 3 del modelo OSI.

El rendimiento de los encaminadores es menor que el que podemos encontrar en los switches, ya que gastan tiempo en analizar los paquetes del nivel de red, pero, ofrecen mayor flexibilidad en la organización de la interconexión de redes.

Los *routers* encaminan uno o más protocolos, pero, no todos los protocolos son enrutables. Los protocolos de nivel 3 enrutables más utilizados son IP, IPX, AppleTalk, DECnet, XNS, etc.

Las características fundamentales de los *routers* las podemos resumir en los siguientes puntos:

- Interpretan direcciones lógicas en lugar de direcciones MAC.
- Son capaces de cambiar el formato de las tramas.
- Poseen inteligencia y pueden manejar distintos protocolos.
- Añaden seguridad, ya que se pueden configurar para restringir accesos.
- Reducen la congestión del tráfico y los dominios de colisión de las distintas subredes.

4.2.5.1. Tipos de encaminadores

Podemos clasificar los enrutadores de varias maneras, pero vamos a quedarnos con las dos siguientes clasificaciones, según el lugar que ocupen, y según el protocolo de encaminamiento utilizado.

Según su ubicación en la red

Esta clasificación se hace según el tipo de servicio que proporcionan a la red.

- ***Router* de interior**, será un encaminador instalado en una LAN para ofrecer servicio de encaminamiento en la misma red LAN, dando a los paquetes de red la posibilidad de saltar de unos segmentos a otros.
- ***Router* de exterior**, en este caso, el encaminador comunica nodos y redes con el exterior de la LAN. Generalmente, estos *routers* operan como núcleo de Internet y son utilizados por los operadores de Internet para comunicarse con ellos.
- ***Router* de borde** o **frontera**, estos *routers* se encargan de conectar *routers* interiores con *routers* exteriores. Por ejemplo, pueden interconectar una LAN a Internet a través del proveedor de servicios de Internet (ISP, Internet Service Provider).

Según el tipo de algoritmo de encaminamiento

Los routers crean tablas de enrutamiento donde registran que nodos y redes son alcanzables por cada uno de sus puertos. Se puede decir que esta tabla registra la topología de la red. Según la forma de confeccionar dicha tabla, podemos obtener la siguiente clasificación.

- Algoritmos de **encaminamiento estático** (*static routing*), en este caso, la tabla de rutas debes quedar establecida o programada por el administrador de red. No tienen la capacidad de aprender la topología

de la red por sí mismos. Cualquier cambio en la red requiere la intervención del administrador para modificar la tabla.

- Algoritmos de **encaminamiento adaptativo** (*dynamic routing*), aprenden por sí mismos la topología de la red. Son más flexibles, aunque el rendimiento es menor ya que deben intercambiar información con otros routers para confeccionar las tablas de encaminamiento.

4.2.5.2. Protocolos de encaminamiento

Los protocolos de encaminamiento son los utilizados por los *routers* para conseguir el **mejor camino** (*best path*) que les separa del destino. El mejor camino será aquel que represente la ruta más eficiente que deben seguir los paquetes, desde que sale de un host origen hasta llegar al host destino.

El mejor camino dependerá de la actividad que haya en la red, de si hay enlaces fuera de servicio, de la velocidad de transmisión de los enlaces, de la topología de la red y otros muchos factores. Por tanto, un enlace de alta velocidad representará un camino mejor que otro semejante de menor velocidad.

El **coste de la ruta** (*route cost*) es un valor numérico que representa cómo de bueno es el camino, a menor coste, mejor camino.

Los protocolos de encaminamiento tienen una propiedad conocida como **tiempo de convergencia**, ésta indica el tiempo que tardará el *router* en encontrar el mejor camino cuando se produzca una alteración en la topología de la red, exigiendo un re-cálculo de las rutas para adaptarse a la nueva situación. Cuanto mejor sea el tiempo de convergencia, más eficiente será el protocolo.

A los protocolos de enrutamiento utilizados por los *routers* de interior se les llama **IGP** (*Interior Gateway Protocol*), y a los utilizados por los *routers* de exterior se le conoce como **EGP** (*Exterior Gateway Protocol*).

4.2.5.3. Configuración del enrutamiento

Cada uno de los de nodos de una red IP debe tener configurados una serie de parámetros de red, entre ellos, uno de los más importantes es la puerta por defecto.

Cuando tenemos que un emisor y un receptor se encuentran en la misma red lógica, no tenemos problemas de comunicación, ya que el emisor sabe que el receptor se encuentra en su misma red mediante el uso de paquetes ARP[1]. El problema viene cuando emisor y receptor no se encuentran en la misma subred, puede que el emisor no sepa que debe hacer para que llegue el paquete al receptor.

Una **ruta de encaminamiento**, o **ruta**, es la dirección IP de un nodo (*router*) con la suficiente inteligencia (algoritmos de encaminamiento) para saber que debe hacer con un paquete IP recibido de un nodo con el objetivo de que llegue a su destino, o al menos, saber a quien debe enviárselo para que llegue al destino. Por lo tanto, la ruta es la dirección IP que apunta al *router*. El *router* deberá decir que puerto es el más adecuado para alcanzar su destino.

Cuando se utiliza este servicio de **ruta por defecto**[2] y la dirección destino del paquete no puede ser alcanzada, el *router* devolverá un mensaje al nodo emisor indicando que el nodo destino es inalcanzable.

Las rutas de cualquier nodo, especialmente las de un *router*, son recogidas en una o varias tablas de encaminamiento, éstas tablas son utilizadas por el servicio de enrutamiento de la red para determinar los caminos que deben seguir los paquetes IP para alcanzar su destino. Las rutas registradas en estas tablas pueden tener una serie de atributos como si son dinámicas, persistentes, estáticas, si se crean durante el arranque, etc.

Configuración de la tabla de rutas

Veamos a continuación los datos que aparecen en una tabla de rutas sobre un cliente Windows, analicemos cada uno de los datos que aparecen.

Debemos tener en cuenta que no todas las tablas de rutas son iguales, dependerán del sistema operativo sobre el que trabajen, aunque la mayoría contiene los datos que veremos.

- **Destino de red.** Es el nombre de la red que se quiere alcanzar.
- **Máscara de red.** Es la máscara de red del destino. La máscara, junto con el destino de red definen el conjunto de nodos de red a los que se dirige la ruta.
- **Puerta de acceso o de enlace.** Es la dirección IP del router (*gateway* o puerta de acceso) que debe ser capaz de resolver el destino de los paquetes. Si la puerta de enlace coincide con la propia red local, el destino se alcanzará inmediatamente.
- **Interfaz.** Es la dirección IP, o el nombre de la interfaz de red que posee el nodo, por la que saldrán los paquetes que deben alcanzar la puerta de enlace.
- **Métrica.** Este parámetro define la medida del coste telemático que supone enviar el paquete a la red destino a través de la puerta de acceso.

Para obtener la tabla de rutas, en Windows se utiliza el comando **ROUTE** desde el símbolo de sistema. En Linux podemos obtenerla utilizando diferentes comandos desde un terminal, **ROUTE**, **IP ROUTE**.

Si trabajamos desde Windows, los comandos para gestionar la tabla de rutas son **ROUTE ADD** para añadir rutas y **ROUTE DELETE** para borrarlas. Además, podemos añadir el atributo **-P** al crear la ruta para que ésta sea permanente, de esta forma, la ruta no se borrará al reiniciar el sistema.

Al crear una ruta, se deberá especificar la dirección de red destino, su máscara de red y la puerta de enlace. Éste último dato será la dirección IP del router que aceptará las peticiones hacia esa red.

Supongamos que un nodo local tiene como dirección IP 192.168.1.10, y la puerta de enlace de la subred es 192.168.1.254. Desde este nodo no se puede acceder a la subred 192.168.200.0, ya que no forman parte de la misma red lógica. Para que el nodo local pueda acceder a dicha subred deberemos añadir la siguiente ruta.

```
ROUTE ADD –P 192.168.200.0 MASK 255.255.255.0 192.168.1.254
```

De esta forma, se crea una ruta persistente y se le indica al nodo hacia donde debe enviar los paquetes para que lleguen a la subred 192.168.200.0.

Si en la especificación de la red destino hubiese sido 0.0.0.0, estaríamos añadiendo una ruta que se correspondería con la ruta por defecto.

Esta misma declaración en Linux sería como sigue, si nos fijamos es muy similar a la utilizada en Windows, ya que los datos necesarios son los mismos.

```
route add –net 192.168.200.0[/24] gw 192.168.1.254 dev eth0
```

De esta forma quedaría la ruta declarada sobre la interfaz *eth0* de Linux.

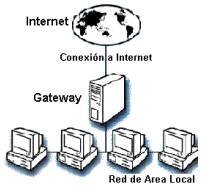
4.2.5.4. Función NAT de enmascaramiento IP

Ya se vio con más detalle en el tema 3, pero no está mal recordarlo. El enmascaramiento IP o IP Masquerading es la función de red que permite a los miembros de una red compartir la conexión a Internet que tiene la máquina que soporta la función de enmascaramiento. Para poder utilizar esta función se utiliza el protocolo NAT[3] (*Network Address Translation*) que actualmente incorporan la gran mayoría de los *routers*. De esta forma, todos los equipos de la red acceden a Internet a través de un mismo *router*.

Ventajas que ofrece el uso de NAT.

- Ahorro de dirección IPv4 públicas.
- Mejora la seguridad de la LAN al ocultar las direcciones IP privadas.
- Permite a los administradores de la red establecer su propio sistema de direccionamiento IP interno.

4.2.6. Pasarelas

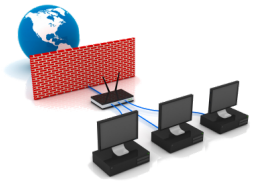


El concepto de pasarela, o *gateway* (puerta de enlace), puede resultar algo abstracto, pero la teoría es muy sencilla. Entenderemos este concepto como un elemento software o hardware que permite interconectar dos redes que utilizan arquitecturas diferentes, cuya finalidad será el intercambio de información.

Por lo general, las pasarelas suelen ser un equipo dedicado o un router, conectados en una red local, ofreciendo así una salida hacia el exterior a los equipos de ésta. Estos dispositivos suelen realizar tareas de traducción de direcciones (NAT).

Estos tipo de dispositivos suelen utilizar las primeras direcciones IP de los rangos en las redes locales, del tipo 192.168.0.1, 192.168.1.1, etc.

4.2.7. Cortafuegos



Cuando se abre una red de área local mundo exterior, a Internet, quedamos expuestos a accesos indebidos, desde la simple curiosidad al espionaje por parte de la competencia o simplemente para hacer daño. Por este motivo, es necesario restringir los accesos desde el exterior.

Un cortafuegos (*firewall*) se instala en el perímetro de la red, éste es un nodo que se encargará de limitar los accesos en ambas direcciones, haciendo así la red invisible desde el exterior y/o restringiendo accesos desde dentro hacia afuera.

En definitiva, un cortafuegos debe ofrecer seguridad en los accesos y transparencia en el envío de datos.

Existen diferentes tipos de cortafuegos según el nivel de la arquitectura OSI en el que operen. Los cortafuegos que trabajan en los niveles inferiores serán más fáciles de configurar, pero menos flexibles. Por ejemplo, una vez establecida una conexión permitida, el cortafuegos deja de trabajar pasado ese punto. Otros, los que operan en niveles más altos, permiten abrir paquetes de datos para comprobar el contenido, esto los hace más lentos, pero son muy flexibles.

Los cortafuegos se configuran mediante el uso de reglas o políticas que se establecen según sea el origen, destino y protocolo que se utilice. Por defecto, todos los cortafuegos cierran toda comunicación, siendo el administrador de la red quien abra los distintos puertos de comunicación y, habilite flujos de transporte permitidos según se requieran.

Cuando un equipo pierde la conexión, lo primero que se hace es comprobar el cableado. Si éste está bien, debe mirarse si el cortafuegos está impidiendo las conexiones.

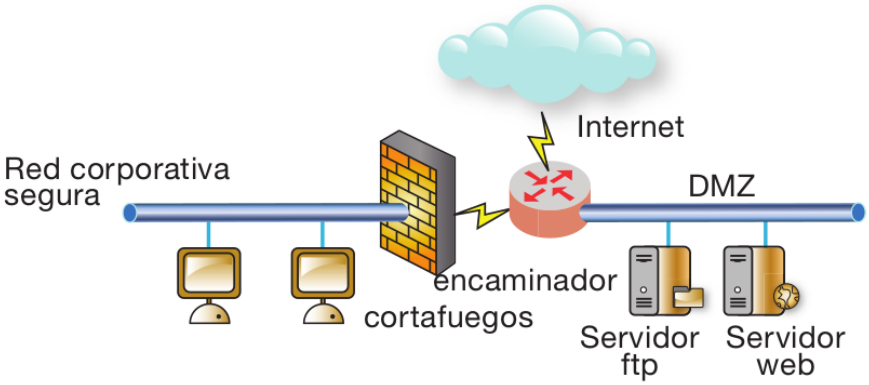
4.2.7.1. Zonas desmilitarizadas

Las zonas desmilitarizadas o DMZ (Demilitarized Zone) son redes formadas por uno o más ordenadores que se encuentran ubicados entre la red corporativa, supuestamente segura, e Internet, que es insegura. Los servicios que se suelen ubicar en las DMZ son los servicios web, FTP, correo electrónico y DNS. Es muy habitual referirse a las DMZ como redes perimetrales, ya que se encuentran ubicadas a las afueras de la red corporativa.

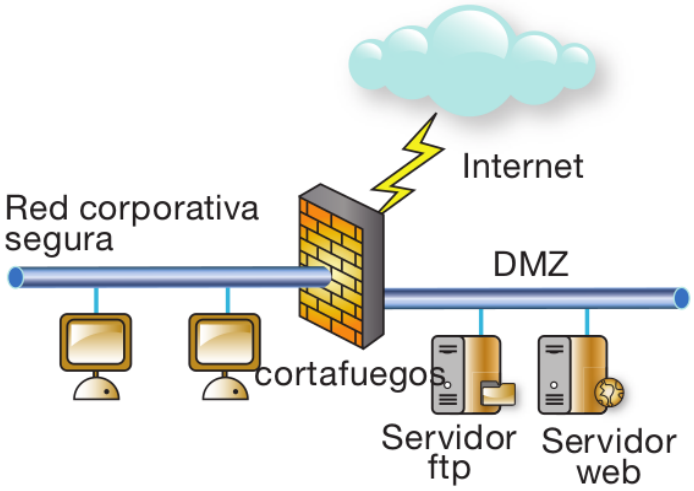
Existen muchas maneras de construir una DMZ, pero el objetivo principal de éstas es ofrecer servicios públicos a Internet sin comprometer la seguridad de la red corporativa.

Veamos a continuación unos cuantos modelos para formar una DMZ, como ya se ha comentado, existen muchas más formas.

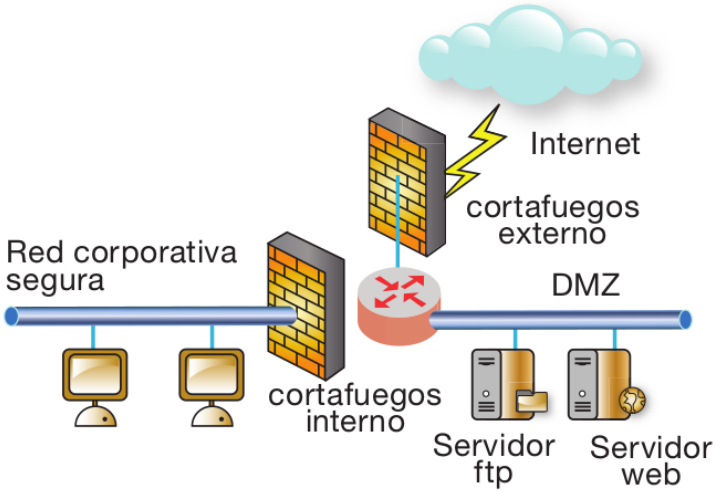
- Este primer modelo es un DMZ expuesto, en este caso, la red corporativa y la DMZ se conectan a Internet a través de un router. De esta manera, la protección de la DMZ queda para cada uno de los servidores y el filtrado que haga el router. La red corporativa, además se encuentra tras la protección de un cortafuegos, por lo que ninguna conexión desde Internet la puede alcanzar.



- En el segundo modelo de DMZ, tanto la red corporativa como la DMZ quedan protegidas por un cortafuegos. Ésta es la protección más utilizada, el cortafuegos dispondrá de una tercera red para el DMZ. El filtrado de restricciones será mucho más estricto en la red corporativa que en la DMZ.



- El tercer modelo es mucho más seguro, pero también es más costoso. La DMZ queda encerrada entre dos cortafuegos, y la red corporativa queda tras el segundo.



La configuración de una DMZ dependerá de su arquitectura y de su relación con Internet y la red corporativa. Por ello, los cortafuegos que hacen de frontera entre la DMZ, la red corporativa e Internet deben establecer tres tipos de políticas de comunicación.

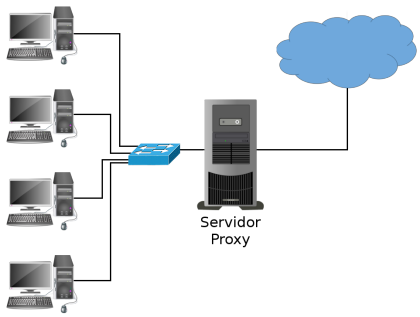
1. **Políticas de relación LAN con Internet:** configuran el acceso de los usuarios de la LAN a Internet, como la navegación por ejemplo.

2. **Políticas de relación LAN con la DMZ:** se configura como los usuarios de la LAN pueden hacer uso de los servicios ofrecidos en la DMZ, por ejemplo, actualizar contenidos. También aquí pueden configurarse como los servidores de la DMZ pueden hacer uso de los servicios ofrecidos por la LAN.

3. **Políticas de relación DMZ con Internet:** mediante estas políticas se configura como los usuarios de Internet, supuestamente anónimos, pueden hacer uso de los servidores de la DMZ.

4.2.8. Servidores Proxy

Los servidores Proxy son máquinas, estaciones, que emplean un software determinado para realizar una serie de funciones.



Básicamente, podemos definir servidor Proxy como el intermediario entre el cliente que solicita un servicio y el servidor que lo ofrece. El cliente solicitará el servicio al Proxy, y éste se encargará de gestionar la petición en su nombre al servidor destino.

Debemos tener en cuenta que pueden haber servidores Proxy de muchos tipos, según el servicio que ofrezcan estos ofrezcan (DNS, FTP, etc.), pero el más común y la vez, más utilizado, cuando se habla de Proxy es el **webproxy**. Éste tipo de servidores permiten el uso de reglas o políticas de acceso, estableciendo así restricciones de uso, por ejemplo, páginas web que no queramos que se puedan visitar, limitaciones horarias, de tráfico, etc.

Podemos encontrar diferentes varios tipos de Proxy como se ha mencionado.

- **Proxy Caché:** permite conservar el contenido que solicitan los usuarios para resolver peticiones futuras de manera más rápida. Habitualmente se trata de peticiones HTTP/HTTPS. El Proxy ofrece la versión actual de la que disponga, comprobando si existen nuevas versiones durante el proceso, ofreciendo así al usuario la más actual.
- **Proxy Web:** permite el acceso a servicios HTTP y HTTPS, y ocasionalmente FTP. Es habitual que este tipo de Proxy también implemente la función caché.

Ventajas de utilizar servidores Proxy.

- **Mejoran la velocidad:** aumentan los tiempos de respuesta gracias al uso de la caché.
- **Reducen el tráfico:** gracias a la caché, las peticiones se hacen al servidor, no directamente hacia Internet, por lo que el tráfico se ve aligerado y se reciben menos respuestas desde los servidores destino.

Los servidores Proxy más utilizados dentro de los Proxy web son los que se mencionan a continuación.

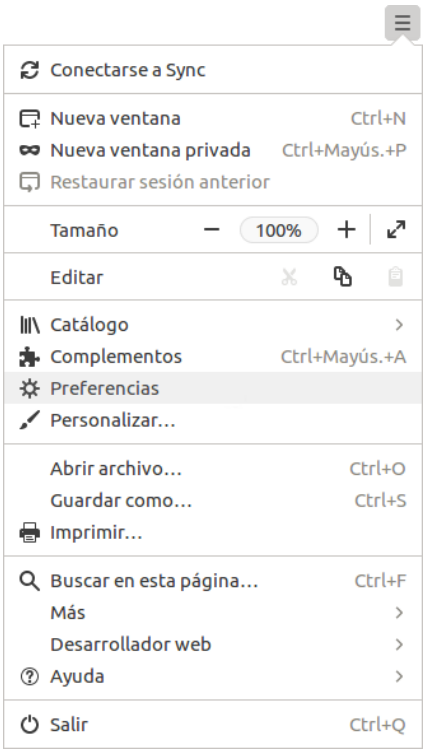
- **Proxy transparente:** por lo general, el uso de un Proxy Web o NAT no es transparente al cliente, debiendo éste configurarlo manualmente. El **Proxy transparente** es una combinación de proxy y cortafuegos, de esta forma, las peticiones son capturadas y desviadas hacia el proxy sin necesidad de que el cliente deba configurar nada, de esta forma, el cliente desconoce su existencia. Este tipo de proxies es muy utilizado por las empresas que proporcionan acceso a Internet.

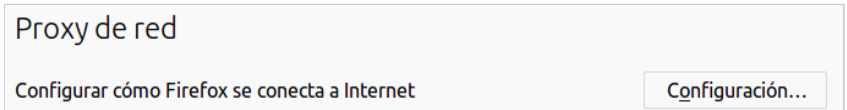
- **Proxy inverso:** (*reverse proxy*) es un servidor alojado en la parte destino, generalmente un alojamiento de un o varios servidores web. Éste servidor recoge el tráfico entrante de Internet con objeto de alcanzar alguno de los servidores alojados. El uso de este tipo de proxies es por motivos de seguridad, ya que añade capacidad de defensa, cifrado SSL, distribución de la carga y uso de una caché para contenido estático.
- **Proxy NAT:** realiza las mismas funciones que el enmascaramiento IP. Ofrece las mismas ventajas que el uso de NAT.

4.2.8.1. Configuración de un servidor Proxy en el cliente

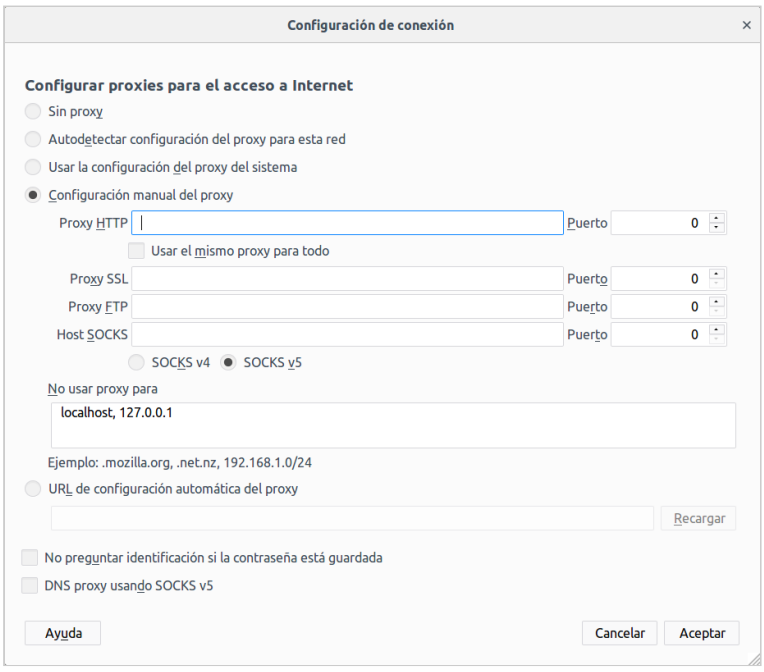
La configuración de un servidor Proxy en un cliente es bastante sencilla, simplemente es necesario localizar la zona de configuración de red. Los datos necesarios son los mismos, independientemente del navegador que estemos configurando, o la aplicación que haga uso del servidor Proxy para funcionar. Veamos un ejemplo de configuración de el navegador Firefox, concretamente en su versión 57.0.1 (64 bits).

En primer lugar deberemos ir a las preferencias del navegador, para ello podemos utilizar el botón hamburguesa . En la nueva pestaña que se abre, nos desplazaremos hasta la parte inferior, donde encontraremos la sección `Proxy de red`, pulsamos sobre el botón `Configuración...` para acceder a las opciones de configuración.





En la ventana que aparece a continuación deberemos escribir los datos necesarios para la conexión al Proxy, dirección IP o URL y el puerto necesario. Generalmente se utiliza un mismo Proxy para todo los tipos de conexiones, pero puede darse el caso que tengamos distintos servidores para según que servicio.



4.2.9. Módem ADSL y cable-módem

Estos dispositivos permiten el acceso remoto a la red y desde ella. Permiten a los paquetes de las redes LAN cambiar de segmento. Tradicionalmente se utilizaban módems analógicos, pero la llegada de la banda ancha hizo que se sustituyeran por los módems ADSL y de cable.

4.2.9.1. Tecnología ADSL

Las siglas DSL son Digital Subscriber Line, y delante de ellas se coloca la sigla que identifica a la familia a la que pertenece, por lo que en general nos referiremos a éstas como tecnologías xDSL.

En el caso de **ADSL**, se trata de aprovechar el cableado telefónico analógico ya existente para la transmisión de datos a Internet a alta velocidad. Esta tecnología establece dos canales de comunicación sobre la misma red física, para ello, se utiliza un dispositivo llamado *splitter*.

Los ***splitters*** son capaces de separar la señal de voz de la señal de datos, estos se utilizaban en las primeras instalaciones de ADSL. Era necesario personal especializado para su instalación.

Los **microfiltros** han sustituido a los *splitters* por su facilidad de instalación, además permiten que el *router* pueda se cambiado de roseta, ya que el microfiltro se instala en el teléfono, y no en el *router*. En una instalación doméstica podríamos tener hasta tres microfiltros.

Existe una gran variedad de tecnologías xDSL, pero nuestro principal caso de estudio será el ADSL, ya que es el que principalmente se ha instalado por las compañías telefónicas.

En este caso, la A de ADSL significa *Asymmetric*, lo que quiere decir que las velocidades de subida y descarga no son iguales, generalmente, la velocidad de descarga es mucho mayor a la velocidad de subida.

4.2.9.2. Cable-módem

También conocidos como módem de cable, nos permiten la conexión a Internet a alta velocidad mediante uso de las redes de televisión.

Los usuarios de este tipo de dispositivos reciben la señal de televisión a la vez que pueden transmitir o recibir datos de Internet.

Las velocidades de transmisión son muy variables con esta tecnología, inicialmente, se disponían de velocidades de entre 300 Kbps hasta los 10 Mbps, pero en la actualidad pueden alcanzarse los 200 o 300 Mbps[4].

Ejercicios propuestos

4.2.1. Rellena la tabla para cada uno de los siguientes dispositivos.

Dispositivo	Capa OSI	¿Es multipuerto?	¿Es local?	¿Segmenta dominios de colisión?	¿Segmenta dominios de broadcast?
Repetidor					
Concentrador					
Puente					
Conmutador					
Enrutador					

4.2.2. Desde una máquina en Linux, realiza las siguientes operaciones.

- Muestra la tabla de rutas de la máquina Linux, haz una captura de pantalla e indica el comando utilizado.
- Añade una ruta indicando que todos los paquetes deben dirigirse a una dirección IP de la red que no sea la puerta de enlace del aula (no persistente). Muestra la tabla con la nueva ruta y haz una captura, además, indica el comando utilizado.
- ¿Qué ocurre al añadir la nueva ruta?

Reinicia el sistema operativo para comprobar que la ruta ya no está.

4.2.3. Realiza la práctica 3 de Packet Tracer.

4.2.4. Realiza la práctica 4 de Packet Tracer.

4.2.5. Di si las siguientes afirmaciones son verdaderas o falsas, explica la respuesta:

a) Los conmutadores son más rápidos que los concentradores.

b) Un conmutador es siempre local.

c) Un proxy transparente debe ser configurado por el usuario para poder navegar.

d) El tiempo de convergencia es lo que tarda un switch en encontrar un camino alternativo en caso de fallo de la red.

e) Las pasarelas no suelen realizar tareas de traducción de direcciones.

f) Los routers de frontera se encargan de conectar únicamente routers interiores entre sí.

g) Las DMZ están formadas por ordenadores que se encuentran exclusivamente dentro de la red corporativa, supuestamente segura.

h) La tecnología ADSL establece dos canales de comunicación sobre la misma red física.

4.3. Dispositivos de interconexión de redes inalámbricas

Entenderemos como comunicación inalámbrica a la comunicación que se lleva a cabo sin utilizar cables para la interconexión entre los participantes.

En este punto se van a detallar los elementos más habituales para la interconexión de redes inalámbricas, en concreto nos centraremos en las redes WLAN, cuyo estándar de comunicación utilizado es la norma IEEE 802.11.

► Router Wi-Fi

Este dispositivo implementa las mismas funcionalidades que un router normal, trabajando de igual manera en la capa de red del modelo OSI, pero añade la funcionalidad inalámbrica.

► Puntos de acceso inalámbricos

Estos dispositivos, también se conocen como AP, permiten la creación de redes locales inalámbricas (WLAN). Los AP se conectan a otros dispositivos como *routers*, *switches* o *hubs* mediante un cable *Ethernet* y crea una señal Wi-Fi en la zona en cuestión.

► Repetidores inalámbricos o extensores de red

Los repetidores o extensores de redes inalámbricas permiten propagar la señal inalámbrica, mejorando y potenciando así la señal, ampliando así la cobertura. Podemos dividir estos dispositivos en tres.

- **Repetidor Wi-Fi:** es el más básico, se sincroniza con el router y reenvía de manera inalámbrica la señal Wi-Fi alcanzando así una mayor distancia.
- **Amplificador Wi-Fi:** aumentan o amplifican la señal, haciendo que la intensidad aumente. Se pueden encontrar dispositivos que repitan y amplíen la señal simultáneamente.
- **Repetidor PLC:** (*Power Line Communications*) estos dispositivos no amplifican la señal por el aire, sino que utilizan el cableado eléctrico para hacer llegar a los lugares que no llega el Wi-Fi.

► Antenas Wi-Fi

Las antenas Wi-Fi las definiremos como elementos pasivos que, no añaden potencia adicional a la señal y que simplemente reorientan la energía de ésta. Esta reorientación permite que exista mayor energía en la dirección señalada y menos en el resto.

Mediante el uso de antenas se consigue mayor ganancia (incremento de la potencia en la señal), dirección y polarización (orientación del campo eléctrico radiado por una antena, ésta puede ser vertical, horizontal, circular o elíptica).

4.4. Redes virtuales (VLAN)

Las redes de área local virtuales (*virtual LAN*) son un método que permite la creación de redes lógicas independientes dentro una una misma red física. Dentro de un mismo conmutador físico (*switch*), o red física, pueden existir varias VLAN.

La creación de redes virtuales permiten reducir el tamaño del dominio de *broadcast* (o difusión) y ayudan a la administración de la red. Se pueden crear segmentos lógicos de una red de área local para, por ejemplo, separar departamentos de una empresa que no deban intercambiar información mediante la red, aunque pueden utilizar un router para ello.

Además, se consigue una mejora en la velocidad por una mejor gestión de los puertos, y se aumenta la seguridad de la red por la segregación o aislamiento de conexiones.

4.4.1. Tipos de VLAN

Podemos clasificar las VLAN de varias formas, según la construcción utilizada, según el tráfico, según el uso que se haga de los datos, etc. Veamos unas cuantas.

Según sea la forma de construir la VLAN, sería la clasificación más sencilla.

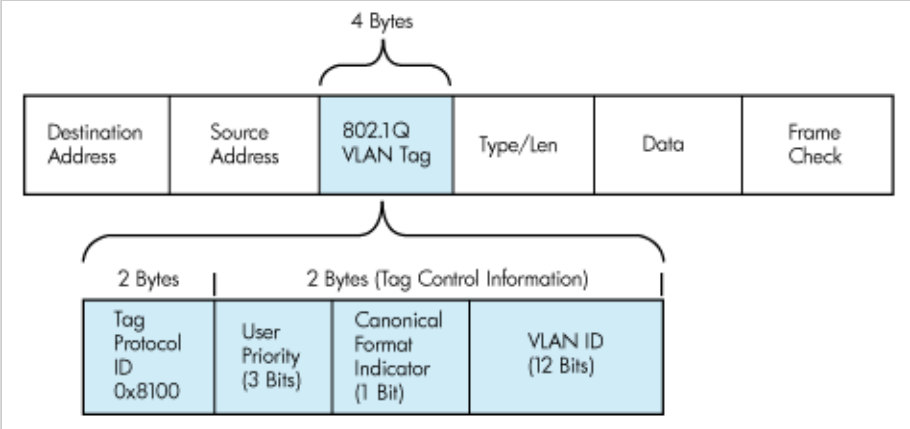
- **VLAN mediante asignación de direcciones MAC**: se crean grupos lógicos utilizando las direcciones MAC en los *switches*. De esta forma, cuando un equipo cambia su ubicación sigue manteniendo su MAC, por lo tanto, sigue perteneciendo al mismo grupo.
- **VLAN con asignaciones de puertos**: parecida a la agrupación anterior, pero en este caso, las agrupaciones se realizan utilizando los puertos del *switch* en lugar de las direcciones MAC. El equipo conectado a un puerto asociado a un segmento asociado a una VLAN pertenece a dicha VLAN.
- **VLAN por direccionamiento virtual**: las agrupaciones se constituirán sobre un sistema de direccionamiento compartido, utilizando para ello las máscaras de red. Este tipo de VLAN serían de nivel 3 de OSI (nivel de red).

Según sea la función que cumplen.

- **VLAN predeterminada**: todos los puertos del *switch* forman parte de la VLAN predeterminada, por lo que cualquier equipo conectado al *switch* puede comunicarse con cualquier otro.
- **VLAN de datos o de usuario**: configuradas para transportar únicamente el tráfico del usuario. No se considerará tráfico de usuario al tráfico de administración o a los datos de voz. Se suelen utilizar para crear grupos de usuarios o dispositivos.
- **VLAN nativa**: están asignadas a un puerto troncal 802.1Q. Este tipo de puertos admiten el tráfico que llega de las VLAN, conocido como tráfico etiquetado. Pero también llega tráfico que no pertenece a una VLAN, tráfico no etiquetado. Este tipo de VLAN se utilizan para identificar los extremos opuestos de un enlace troncal.
- **VLAN de administración**: estas VLAN se configuran para tener acceso de administración y/o configuración de los *switches*.

IEEE 802.1Q o **VLAN *Tagging*** es el estándar más común para la creación de VLAN. Gracias a éste se pueden definir VLAN independientemente del fabricante. El estándar lleva asociada una numeración de VLAN[5] a la que pertenecerá con independencia de su ubicación de red y que registrará en la cabecera de cada una de sus tramas, esto se conoce como *tagging*. La configuración de la VLAN se encuentra en la tarjeta de red, por lo que ésta debe ser compatible con IEEE 802.1Q.

El puerto del switch al que se conecten los nodos configurados mediante IEEE 802.1Q se marcarán como *"tags"*.



Ejercicios propuestos

4.4.1. Según lo que ya sabes sobre las VLAN, ¿cuáles serían la mayores diferencias o inconvenientes entre las VLAN mediante asignación de direcciones MAC y las VLAN con asignaciones de puertos?

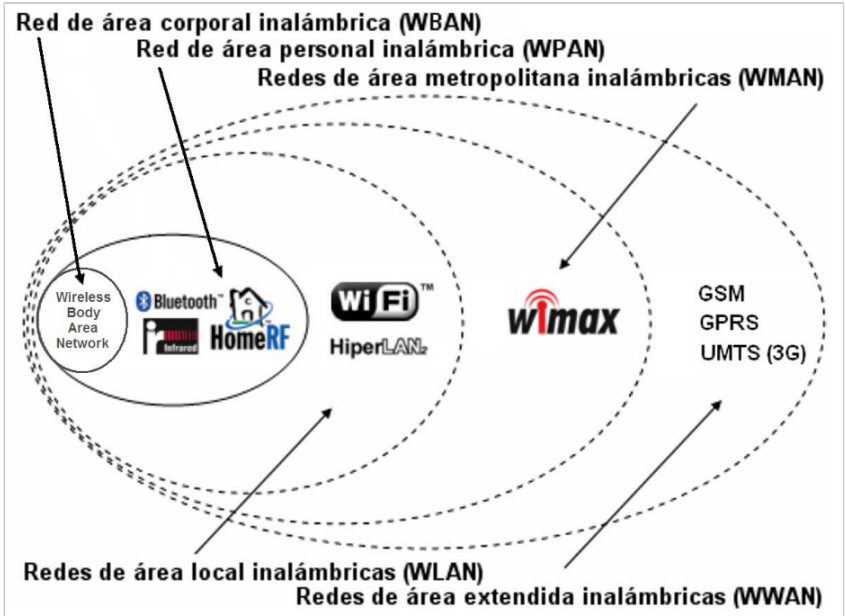
4.5. Redes mixtas

Actualmente, se tiende a pensar que la implantación de redes inalámbricas resuelven muchos de los problemas de conectividad para los administradores, pero deben tenerse en cuenta factores como el ancho de banda, que es menor en las conexiones inalámbricas, y la seguridad, que puede ser un punto muy vulnerable en las conexiones inalámbricas.

Cuando se habla de redes mixtas, podemos hablar varias topologías dentro de una misma red (bus, anillo, estrella, malla) o de redes con diferentes tecnologías dentro de la propia red. Éste último será el caso de estudio que nos atañe en este punto.

4.5.1. Tecnologías inalámbricas

Existen diferentes tecnologías inalámbricas, todas ellas en función del uso y/o cobertura que cubran. Actualmente, el estándar más extendido es el Wi-Fi (IEEE 802.11).



La siguiente tabla muestra una comparativa entre las diferentes normas reguladas por la Alianza Wi-Fi[6] y otras como Bluetooth (IEEE 802.15) o *HomeRF* que no están reguladas por ella. Existen más tecnologías inalámbricas que no aparecen aquí como la tecnología IrDA.

	Velocidad	Frecuencia	Ámbito*	Alcance
Bluetooth**	3-720 Kbps	2,4-2,48 Ghz	Redes personales	10 a 20 metros
HomeRF	1-10 Mbps	2,4 Ghz	SOHO***	50 metros
IEEE 802.11b	11 Mbps	2,4 Ghz	SOHO	Hasta 100 metros
IEEE 802.11g	54 Mbps	2,4 Ghz	SOHO	Hasta 100 metros
IEEE 802.11n	300 Mbps	2,4 Ghz	SOHO	Hasta 100 metros
IEEE 802.11ac**	433 Mbps	5 Ghz	SOHO	Hasta 100 metros

*** Ámbito aproximado, depende de otros muchos factores (características del medio, velocidad de transmisión, antenas, etc).**

**** Los datos para Bluetooth son una aproximación a la versión 5.0 de 2017.**

***** SOHO (_Small Office, Home Office_) Hace referencia a empresas pequeñas, de hasta 20 empleados.**

****** Es una mejora sobre la versión 802.11n, actualmente conocido como WiFi 5.**

4.5.1.1. Bluetooth

Esta iniciativa permite la interconexión inalámbrica entre dispositivos de uso personal como teléfonos móviles, ordenadores portátiles, etc. Se utiliza una potencia de transmisión baja, limitando así su alcance y con una velocidad de transmisión baja.

Bluetooth utiliza una banda de frecuencia de 2,4 GHz y una señalización FHSS (*Frequency Hopping Spread Spectrum*, Espectro extendido por salto de frecuencia), lo que permite que la señal vaya saltando entre múltiples frecuencias dentro de la banda según un patrón de sincronización conocido únicamente por el emisor y el receptor.

Los dispositivos Bluetooth se clasifican en tres tipos según sea la potencia de transmisión, esto está regulado por la norma IEEE 802.15 que detalla las comunicaciones personales inalámbricas (WPAN).

	Potencia máxima permitida (mW*)	Potencia máxima permitida (dBm**)	Alcance aproximado
Clase 1	100 mW	20 dBm	100 metros
Clase 2	2,5 mW	4 dBm	5-10 metros
Clase 3	1 mW	0 dBm	1 metro

*** milivatios.**

**** decibelios relativos a los milivatios.**

También se puede encontrar una clasificación según sea la capacidad del canal, aquí entran en juego las diferentes versiones que podemos encontrar de Bluetooth.

	Ancho de banda
Versión 1.2	1 Mbits / s
Versión 2.0 + EDR*	3 Mbits / s
Versión 3.0 + HS**	24 Mbits / s
Versión 4.0	32 Mbits / s
Versión 5.0	256 Mbits / s

*** EDR (*Enhanced Data Rate*) mayor velocidad de transmisión de datos.**

**** HS (*High Speed*) Indica que el dispositivo Bluetooth 3.0 tiene soporte de alta velocidad 802.11.**

En enero de 2019 se ha lanzado la versión 5.1 de Bluetooth, pero todavía no tenemos disponibles las características. Como una de las posibles nuevas características, se habla de la posibilidad de conocer la ubicación de los dispositivos conectados, pero no tendría la misma precisión que el GPS.

¿Cómo funcionan las redes Bluetooth?

Cuando hablemos de redes WPAN, en concretamente las que utilizan tecnología Bluetooth, debemos hablar de ***piconet***, este tipo de redes son aquellas en las que los nodos se conectan mediante tecnología Bluetooth.

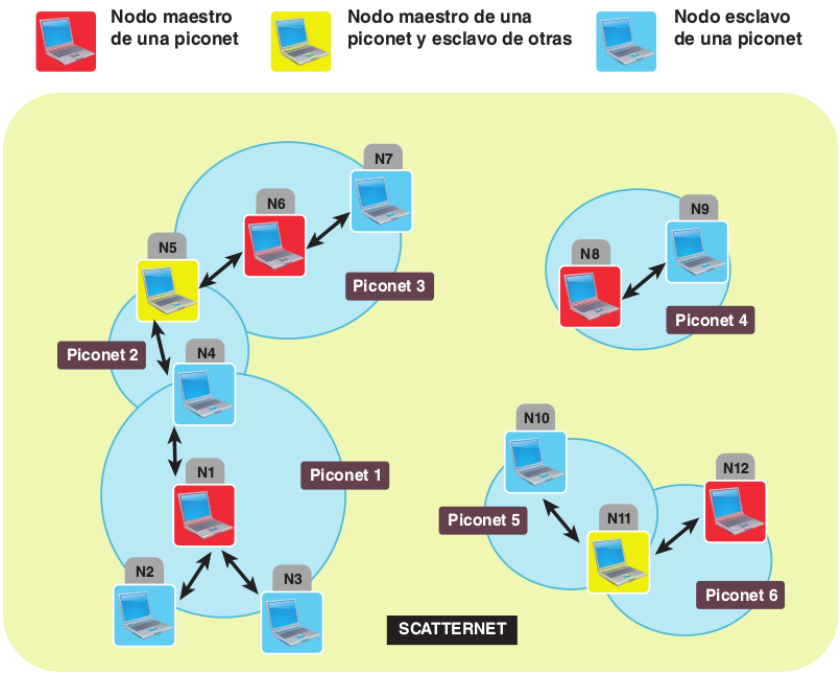
Las *piconet* son redes que tendrán siempre entre dos y siete dispositivos, en las cuales siempre existirá un nodo **maestro** y el resto serán **esclavos**. El establecimiento de las conexión se realizan de manera ad-hoc, es decir, cada emisor y receptor deben ponerse de acuerdo. ¿Qué deben cumplir las *piconet*?

1. Todo dispositivo Bluetooth debe permanecer a una *piconet*, compartiendo canal y sincronizado mediante un reloj común que establecerá la secuencia de saltos. Un extremo será el maestro, y el otro el esclavo.

2. Pueden existir varios canales, cada uno de ellos con su propio reloj, maestro y secuencia de saltos.

3. Una *piconet* únicamente puede tener un solo maestro, aunque un esclavo puede formar parte de varias *piconets*.

4. El maestro de una *piconet* puede ser a su vez esclavo en otra u otras *piconets* en las que el no es maestro. A este solapamiento de maestros y esclavos se le conoce como *scatternet* (red dispersa).



4.5.1.2. Redes Wi-Fi

Esta tecnología surge como sistemas propietarios con velocidades de transmisión inferiores a los 1,5 Mbps, algo insuficiente para las redes de área local. Actualmente la WECA (*Wireless Ethernet Compatibility Alliance*) o *Wi-Fi Alliance* se encarga de certificar las compatibilidades entre dispositivos IEEE 802.11.

Al hablar de Wi-Fi estamos haciendo referencia a la comunicación inalámbrica mediante ondas de radio, el mismo sistema que pueden utilizar los teléfonos móviles, la televisión o la radio en sí.

En las conexiones Wi-Fi intervienen dos elementos principalmente:

- El **adaptador Wi-Fi**, generalmente conectado a un ordenador (aunque también puede ser de un teléfono móvil, tablet, etc), se encarga de recibir las ondas de radio y traducirlas para que éstas sean comprendidas por el dispositivo.
- El **punto de acceso** o ***router* Wi-Fi**, se encarga de recibir las señales y transformarlas para que puedan salir hacia la LAN o Internet.

La conexión Wi-Fi es bidireccional, por lo que este proceso se realiza en ambos sentidos. También debe tenerse en cuenta que esta tecnología está pensada para distancias cortas, por lo que no es recomendable hacer uso de ella más allá de 100 metros.

Por otro lado, la tecnología Wi-Fi utiliza diferentes técnicas de modulación según el estándar elegido. Las más utilizadas son las siguientes.

- **DSSS** (*Direct-Sequence Spread Spectrum*): Espectro ensanchado por secuencia directa, esta técnica añade redundancia a la señal, creando un patrón de bits redundante por cada uno de los bits que forman la señal.
- **FHSS** (*Frequency Hopping Spread Spectrum*): Espectro ensanchado por salto de frecuencia, al igual que la técnica anterior, se añade redundancia a la señal, pero esta vez la señal va saltando de frecuencia

cada tiempo determinado, generalmente un tiempo inferior a 400 ms.

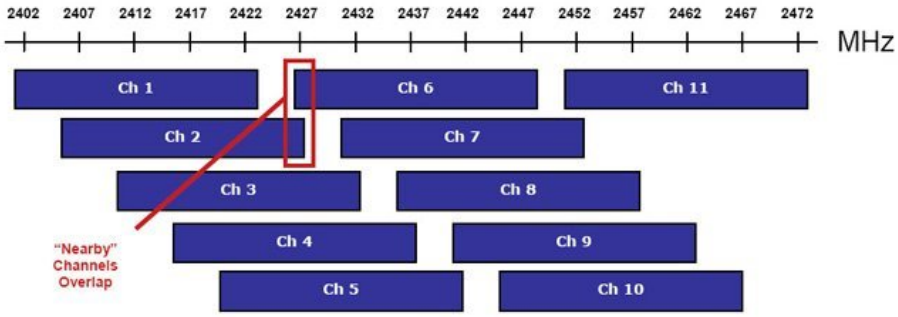
- **OFDM** (*Orthogonal Frequency Division Multiplexing*): Multiplexación por división de frecuencias ortogonales, consiste en la división de la señal portadora en varias frecuencias, cada una de ellas transportando información.

Existen una serie de datos que se deben conocer a la hora de configurar un punto de acceso o un *router* WiFi[7].

- **SSID** (*Service Set Identifier*): será un valor de hasta 32 caracteres alfanuméricos, como máximo, que identifica los puntos de acceso inalámbricos a la red. Todos los dispositivos que formen parte de la misma red y compartan información deben tener el mismo SSID.
- **BSSID** (*Basic Service Set Identifier*): tiene la misma función que el SSID, con la diferencia que los BSSID sólo pueden utilizarse en un único punto de acceso en una misma red.
- **Frecuencia**: se indica la frecuencia a la que se transmitirán las señales. Actualmente existen dispositivos que nos permiten emitir a 2,4 GHz y a 5 GHz.

	Ventajas	Inconvenientes
2,4 Ghz	- Abarca una mayor distancia. - Hay más dispositivos compatibles.	- Frecuencia con mayor interferencias debido a la cantidad de dispositivos que trabajan en ella.
5 Ghz	- Tiene un mayor ancho de banda. - Menos interferencias, es una frecuencia menos abarrotada.	- Menor distancia. - Pocos dispositivos admiten esta frecuencia.

- **Canal**: permite seleccionar el canal dentro de la frecuencia. Generalmente se utiliza el modo automático, para que se seleccione el canal más libre en ese momento. Cuando la conexión falla, lo más lógico es buscar un canal menos ocupado. Debemos tener en cuenta que los canales se solapan, por ejemplo, el canal 1 se solapa al 2, 3, 4 y 5, por lo que pueden producir interferencias.



- **Modo**: se utiliza para seleccionar el tipo de conexión con los dispositivos, por ejemplo 802.11a para 5 GHz, 802.11b para 2,4 GHz, etc. Si todos los dispositivos utilizan la misma tecnología puede ser útil, pero si tenemos dispositivos de distintas tecnologías se utiliza la opción mixta.

4.5.1.3. Estándar WiMAX

WiMAX (*Worldwide Interoperability for Microwave Access*) es el estándar de transmisión de datos inalámbrica por medio de microondas. Se basa sobre el IEEE 802.16 que comenzó a desarrollarse en 2002. El nombre de WiMAX era en realidad el nombre del foro en el que participaban varios fabricantes, entre ellos Intel y Nokia.

WiMAX proporciona acceso inalámbrico en áreas con un radio de 50 km, sin necesidad de tener una visión directa del punto de acceso. Funciona por debajo de los 11 GHz y es capaz de alcanzar velocidades de hasta 70 Mbps.

Las características principales de WiMAX las podemos resumir como sigue.

- Mayor ancho de banda a mayor distancia (hasta 50 km), por lo que ofrece mayor cobertura.
- No se necesita una visión directa del punto de acceso.
- Sistema escalable. El sistema es capaz de aumentar el número de usuario fácilmente y permite una adaptación cómoda de las frecuencias según la legislación.
- Permite utilizar mecanismos QoS (Quality of Service) para garantizar la calidad de la transmisión.
- Permite un despliegue de cobertura fácil en zonas metropolitanas.

4.6. Seguridad básica en redes

Las conexiones a Internet actuales son un gran avance, permitiendo, en el ámbito laboral, una mayor aumento de la productividad, reduciendo tiempos de espera y facilitando la comunicación entre usuarios. Por otro lado, la comodidad que proporciona el ancho de banda puede convertirse en un gran problema de seguridad si no se toman medidas.

Los principales problemas que pueden producirse en una red de área local pueden ser los ataques producidos por *hackers* y los virus informáticos.

Evidentemente, el bien más preciado que se debe proteger es la información, ya que un acceso indebido a ella puede producir daños económicos, laborales y de ámbito personal (*phishing*, robo de identidad).

Centremos ahora nuestra atención en aspectos más relacionados con las redes y su seguridad directamente.

4.6.1. Redes cableadas

A nivel de cableado, el principal problema lo encontramos en la conexión directa a Internet, por lo que debe controlarse tanto la entrada como la salida. Veamos algunas tecnologías que pueden ayudarnos en la protección de nuestros equipos.

- **Tecnología de servidor de seguridad *software***: esta técnica sería la más básica, consiste en la instalación se *software* de protección en los equipos de la red (antivirus, cortafuegos, etc), dejando a cada cliente ser responsable de su propia seguridad. Para redes muy grandes, esta técnica puede no resultar ser muy útil debido al manteniendo que conlleva.

- **Tecnología NAT**: esta tecnología se implementa mediante el uso *routers* principalmente. Como ya se ha visto, NAT se encarga de la traducción de direcciones. A nivel de seguridad, oculta las direcciones de

los equipos de la red al exterior, por lo que un atacante únicamente ve la dirección pública y no sabe que puede haber detrás. Básicamente, NAT oculta la red.

- **Tecnología SPI**: *Stateful Packet Inspection*, o filtrado de paquetes. Esto son un tipo de *firewall* o *proxy*, capaz de examinar el contenido de los paquetes que circulan en la red, y mediante el uso de reglas permite o deniega los accesos, tanto de entrada como de salida. Muchos de ellos permiten mantener un historial de los casos producidos para ayudar a la detección del origen del problema. Esta tecnología la podemos encontrar en los *routers*, pero también puede instalarse en servidores dedicados a dicha tarea, como *Squid*[8] por ejemplo.

4.6.2. Redes inalámbricas

Las tecnologías de seguridad aplicadas a las redes cableadas también se aplicarán a las redes inalámbricas. Aquí, el principal problema es el punto de acceso en sí. Debemos tener en cuenta que la tecnología Wi-Fi utiliza un sistema de autenticación de sistema abierto y clave compartida, y conocida la clave por personas ajenas pueden producirse accesos indebidos. Centremos en la seguridad de los puntos de acceso Wi-Fi.

- **Ocultación del SSID**: se parte de lo más básico, ocultar el nombre del punto de acceso, esto hace que no sea visible a búsquedas de redes Wi-Fi y sólo puedan conectarse aquellos que conozcan el SSID, una conexión a una red oculta. Esto se consigue desactivando el **SSID *broadcasting*** del *router* o punto de acceso.

- **WEP**: *Wired Equivalent Privacy*, privacidad equivalente al cableado. Sistema básico de seguridad para las redes inalámbricas incluido en el IEEE 802.11. Este sistema permite encriptar la información que se envía. Utiliza el algoritmo de cifrado RC4 de 64 o 128 bits. Se presentó en 1999 y, debido a las vulnerabilidades que se detectaron, fue rápidamente reemplazado por WPA en 2003.

- **WPA**: *Wi-Fi Protected Access*, tiene la misma función que WEP, es más, sigue utilizando el algoritmo de cifrado RC4 para encriptar la información, pero surge para corregir las carencias que mostraba su antecesor. Fue creado como intermediario hasta la corrección del sistema WEP en la 802.11i. Es habitual el uso de WPA-Personal más el protocolo de integridad de clave temporal (TKIP) para la encriptación, estas claves van variando dinámicamente a medida que se utilizan.

- **WPA2**: aparece en 2004 y mejora la versión anterior añadiendo el uso del estándar avanzado de cifrado (AES). La Wi-Fi Alliance nombra la versión WPA2-Personal a la autenticación con clave pre-compartida y WPA2-Enterprise a la versión con autenticación 802.1x/EAP[9]. En 2017 se demostró una vulnerabilidad en WPA2[10].

- **Radius**: *Remote Access Dial In User Service*, éste es el protocolo utilizado por las versiones Enterprise para la autenticación de usuarios. Mediante éste sistema, el usuario que pretende acceder al servicio, se autentica directamente contra un servidor dedicado a ello, en vez de contra el punto de acceso como ocurriría en las versiones *Personal*.

- **Filtrado por MAC**: esta puede ser otra medida de seguridad a implementar para evitar accesos no deseados. Puede utilizarse de dos maneras, ambas creando una lista con direcciones MAC. Una vez creada dicha lista, se especifica si, se permite el acceso a las direcciones que hay en esa lista o si se deniega. Siempre es más sencillo de administrar la lista si ésta es para permitir el acceso.

La versión WPA3[11], con fecha de salida prevista para principios de 2018, pasará de una clave de cifrado de 128 bits a 192 bits.

> **Ejercicios propuestos**
>
> **4.6.1.** Para este ejercicio, deberás realizar una configuración básica en un router inalámbrico doméstico, configurar la dirección IP del router en su parte LAN, cambiar el SSID por uno que te identifique y activar el DHCP, modifica el rango para que únicamente se sirvan 20 direcciones IP y asegúrate que la dirección de la puerta de enlace es la correcta.
>
> Crea un documento de texto con las capturas de pantalla necesarias, explicando que has modificado y porqué. Utiliza para el ejercicio el router Tp-Link TL-WDR4300 (Hogar) con versión de firmware 130319 que encontrarás en la web de emuladores de Tp-Link[7:1]. Recuerda que no se puede guardar la configuración, por lo tanto, una vez tengas segura la configuración, haz una captura de pantalla.
>
> **4.6.2.** Añade seguridad WEP a un router inalámbrico doméstico, también deberás cambiar el SSID por uno que te identifique.
>
> Crea un documento de texto con las capturas de pantalla necesarias, explicando que has modificado y porqué. Utiliza para el ejercicio el router Tp-Link[7:2] TL-WR840N (Hogar) con versión de firmware 161011 que encontrarás en la web de emuladores de Tp-Link. Recuerda que no se puede guardar la configuración, por lo tanto, una vez tengas segura la configuración, haz una captura de pantalla.
>
> **4.6.3.** Añade seguridad WPA2-PSK con encriptación AES a un router inalámbrico doméstico, también deberás cambiar el SSID por uno que te identifique y modificar el ancho del canal para que sea fijo a 40 Mhz y utilizar un canal fijo.
>
> Crea un documento de texto con las capturas de pantalla necesarias, explicando que has modificado y porqué.
>
> Utiliza para el ejercicio el router Tp-Link[7:3] Archer C60 (Hogar) con versión de firmware 161206 que encontrarás en la web de emuladores de Tp-Link. Recuerda que no se puede guardar la configuración, por lo tanto, una vez tengas segura la configuración, haz una captura de pantalla.

Trabajos de ampliación

Tecnología xDSL

Entrega un documento de LibreOffice Writer, debidamente formateado, en el que trates los siguientes puntos.

- Breve descripción de la tecnología xDSL.
- Tabla en la que detalles las diferentes versiones o tipos de xDSL.
- Enumera diferentes ISP que ofrezcan alguno de los tipos xDSL.

Protocolos de enrutamiento

Crea un documento e investiga cuales son los protocolos que existen para enrutamiento, agrupados en IGP y EGP. Describe cada uno de los protocolos, indicando sus características. Algunos de los protocolos son RIP,

BGP, OSPF, IS-IS, etc.

Recuerda que el trabajo debe tener portada, índice y la *webgrafía* al final del documento. Así como un encabezado con tu nombre, el nombre de la asignatura y el nombre del trabajo.

Manual de antenas Wi-Fi

Crea un documento e investiga la forma de crear una antena Wi-Fi casera, realiza un trabajo de documentación exhaustivo, pensando en que el lector no sabe nada sobre el tema en cuestión.

Como añadido, intenta crear la antena para presentarla en clase.

Recuerda que el trabajo debe tener portada, índice y la webgrafía al final del documento. Así como un encabezado con tu nombre, el nombre de la asignatura y el nombre del trabajo.

---

1. **ARP** (*Address Resolution Protocol*, protocolo de resolución de direcciones). ↩
2. **Ruta por defecto** (*default gateway*) es la ruta a la que se envía un paquete cuando ninguna otra ruta es apropiada. También se conoce como puerta de enlace y generalmente es la dirección IP de un *router*. ↩
3. **Norma RFC 1631** Describe la funcionalidad de NAT ver aquí. ↩
4. ONO rompe la barrera con una conexión con ¡500 Mbps de bajada! ↩
5. **VLAN *numbering***: cada VLAN 802.1Q se identifica mediante 12 bits llamados VID, el rango utilizado será desde 1 a 4094, los valores 0 y 4095 están reservados y no se utilizan. ↩
6. Wi-Fi Alliance Organización sin ánimo de lucro que encargada de promover la tecnología Wi-Fi y certificar productos para que éstos se ajusten a las normas de interoperabilidad fijadas en la IEEE 802.11. ↩
7. Emuladores tp-link. ↩ ↩ ↩ ↩
8. Squid. ↩
9. **802.1x/EAP** es un sistema de autenticación de usuarios para acceso a la red (inalámbrica o cableada) mediante el uso de un servidor de autenticación. El protocolo EAP es el encargado de controlar el acceso. ↩
10. **Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse** (https://www.krackattacks.com/) El protocolo WPA2 ha sido *hackeado*: la seguridad de las redes WiFi queda comprometida artículo Xataka. ↩
11. WPA3 ↩